FlexPod ソリューション

FlexPod

NetApp
March 25, 2024

目次

FlexPod ソリューション

FlexPod の定義

FlexPod Express 技術仕様

TR-4293 ：『 FlexPod Express Technical Specifications 』

ネットアップ、 Karthick Radhakrinan 、 Arvind Ramakrinan 、 Lindsey Street 、 Savita Kumari

FlexPod Express は、 Cisco Unified Computing System （ Cisco UCS ）と Cisco Nexus ファミリーのスイッチ上に構築された、ベストプラクティスに基づく事前設計済みのアーキテクチャであり、ストレージレイヤは NetApp FAS または NetApp E シリーズストレージを使用して構築されます。FlexPod Express は、さまざまな仮想ハイパーバイザーやベアメタルオペレーティングシステム（ OS ）やエンタープライズワークロードを実行するのに適したプラットフォームです。

FlexPod Express は、ベースライン構成だけでなく、さまざまなユースケースや要件に対応できるよう、サイズ設定と最適化が可能な柔軟性も備えています。このドキュメントでは、使用しているストレージシステム、NetApp FAS を使用した FlexPod Express 、および E シリーズを使用した FlexPod Express に基づいて FlexPod Express 構成を分類します。

FlexPod プラットフォーム

FlexPod プラットフォームには、次の 3 つがあります。

- * FlexPod データセンター。 * このプラットフォームは、ワークロードエンタープライズアプリケーション、仮想化、 VDI 、パブリックおよびプライベートクラウドに適した、拡張性にきわめて優れた仮想データセンターインフラストラクチャです。FlexPod データセンターには、独自の仕様があります。詳細については、を参照してください "TR-4036 ：『 FlexPod Datacenter Technical Specifications 』"。
- * FlexPod Express. * このプラットフォームは、リモートオフィスやエッジのユースケース向けのコンパクトな統合インフラストラクチャです。

本ドキュメントでは、 FlexPod Express プラットフォームの技術仕様について説明します。

FlexPod ルール

FlexPod の設計により、多数の異なるコンポーネントとソフトウェアバージョンを含む柔軟なインフラが実現します。

ルールセットは、有効な FlexPod 構成を構築またはアセンブルするためのガイドとして使用します。このドキュメントに記載されている番号とルールは、 FlexPod の最小要件です。これらの番号とルールは、環境やユースケースに応じて、付属の製品ファミリーで拡張することができます。

サポート対象の FlexPod 構成と検証済みの 構成の比較

FlexPod のアーキテクチャは、本ドキュメントで説明する一連のルールで定義されています。ハードウェアコンポーネントとソフトウェアの設定は、 Cisco Hardware Compatibility List （ HCL ；ハードウェア互換性リスト）およびでサポートされている必

要があります "ネットアップの Interoperability Matrix Tool （ IMT ）"。

各 Cisco Validated Design （ CVD ）または NetApp Verified Architecture （ NVA ）は、 FlexPod 構成の可能性があります。Cisco とネットアップは、これらの構成の組み合わせを文書化し、広範なエンドツーエンドのテストで検証しています。このドキュメントのガイドラインに従っている場合、 FlexPod の導入は完全にサポートされており、すべてのコンポーネントが Cisco HCL とネットアップで互換性があると記載されています "IMT"。

たとえば、ストレージコントローラや Cisco UCS サーバを追加し、ソフトウェア、ハードウェア、構成がこのドキュメントで定義されているガイドラインを満たしている場合は、ソフトウェアを新しいバージョンにアップグレードすることが完全にサポートされます。

ストレージソフトウェア

FlexPod Express は、 NetApp ONTAP または SANtricity オペレーティングシステムを実行するストレージシステムをサポートしています。

NetApp ONTAP

NetApp ONTAP ソフトウェアは、 AFF および FAS ストレージシステムで稼働するオペレーティングシステムです。ONTAP は、ノンストップオペレーション、無停止アップグレード、即応性に優れたデータインフラを実現する、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。

ONTAP の詳細については、を参照してください "ONTAP の製品ページ"。

E シリーズ SANtricity ソフトウェア

E シリーズ SANtricity ソフトウェアは、 E シリーズストレージシステムで動作するオペレーティングシステムです。SANtricity は、多様なアプリケーションニーズに対応する柔軟性に優れたシステムで、組み込みの高可用性機能とさまざまなデータ保護機能を提供します。

詳細については、を参照してください "SANtricity の製品ページ"。

ハードウェアの最小要件

ここでは、 FlexPod Express の各バージョンに必要なハードウェアの最小要件について説明します。

FlexPod Express with NetApp FAS 』を参照してください

基盤となるストレージにネットアップの FAS コントローラを使用する FlexPod Express ソリューションのハードウェア要件として、このセクションで説明する構成があります。

CIMC ベースの設定（スタンドアロンラックサーバ）

Cisco Integrated Management Controller （ CIMC ）の設定には、次のハードウェアコンポーネントが含まれています。

- 冗長構成の10Gbps標準イーサネットスイッチ×2（Cisco Nexus 31108を推奨、Cisco Nexus 3000および9000モデルをサポート）

- Cisco UCS C シリーズスタンドアロンラックサーバ
- AFF C190 、 AFF A250 、 FAS2600 、または FAS 2700 シリーズのコントローラが 2 ノードクラスタとして導入されたハイアベイラビリティ（ HA ）ペア構成で 2 台

Cisco UCS で管理される構成

Cisco UCS が管理する確認には、次のハードウェアコンポーネントが含まれます。

- 冗長構成の 10Gbps 標準イーサネットスイッチ × 2 （ Cisco Nexus 3524 を推奨）
- Cisco UCS 5108 交流（ AC ）ブレードサーバシャーシ 1 台
- Cisco UCS 6324 ファブリックインターコネクト × 2
- Cisco UCS B シリーズサーバ（ Cisco UCS B200 M5 ブレードサーバ × 4 以上）
- HA ペア構成の AFF C190 、 AFF A250 、 FAS2750 、 FAS2720 コントローラ × 2 （コントローラごとに使用可能なユニファイドターゲットアダプタ 2 つ UTA2 ポートが 2 つ必要）

FlexPod Express と **E** シリーズ

E シリーズのスターター構成を使用した FlexPod Express のハードウェア要件は次のとおりです。

- Cisco UCS 6324 ファブリックインターコネクト × 2
- Cisco UCS Mini シャーシ 5108 AC2 または DC2 （ Cisco UCS 6324 ファブリックインターコネクトは AC2 および DC2 シャーシでのみサポート）
- Cisco UCS B シリーズサーバ（ Cisco UCS B200 M4 ブレードサーバ × 2 以上）
- E シリーズ E2824 ストレージシステムの HA ペア構成 × 1 。 12 本以上のディスクドライブを搭載
- 冗長構成の 10Gbps 標準イーサネットスイッチ × 2 （データセンター内の既存のスイッチを使用可能）

これらのハードウェアコンポーネントは、解決策のスターター構成を構築するために必要です。必要に応じて、ブレードサーバとディスクドライブを追加できます。E シリーズ E2824 ストレージシステムは、上位のプラットフォームに交換することも、オールフラッシュシステムとして実行することもできます。

最小ソフトウェア要件

ここでは、 FlexPod Express の各バージョンに最低限必要なソフトウェアについて説明します。

ネットアップの **AFF** または **FAS** を使用する **FlexPod Express** のソフトウェア要件

ネットアップ FAS を使用した FlexPod Express のソフトウェア要件は次のとおりです。

- ONTAP 9.1 以降
- Cisco NX-OS バージョン 7.0(3) I6(1) 以降
- Cisco UCS で管理される構成では、 Cisco UCS Manager UCS 4.0(1b)

すべてのソフトウェアがにリストされ、サポートされている必要があります "NetApp IMT"。一部のソフトウェア機能では、以前のアーキテクチャに示されている最小要件よりも新しいバージョンのコードが必要になる場合があります。

E シリーズを使用する FlexPod Express のソフトウェア要件

E シリーズを使用する FlexPod Express のソフトウェア要件は次のとおりです。

- E シリーズ SANtricity ソフトウェア 11.30 以降
- Cisco UCS Manager 4.0(1b)

すべてのソフトウェアがにリストされ、サポートされている必要があります "NetApp IMT"。

接続要件

ここでは、 FlexPod Express の各バージョンの接続要件について説明します。

FAS Express と NetApp FlexPod の接続要件

FAS Express と NetApp FlexPod の接続要件は次のとおりです。

- NetApp FAS ストレージコントローラは、 Cisco Nexus スイッチに直接接続する必要があります。ただし、 Cisco UCS で管理される構成では、ストレージコントローラがファブリックインターコネクトに接続されます。
- FlexPod のコアコンポーネント間には、追加の機器をインラインで配置できません。
- Cisco Nexus 3000/9000 シリーズスイッチとネットアップストレージコントローラの接続には、仮想ポートチャネル（ vPC ）が必要です。
- 必須ではありませんが、環境全体でジャンボフレームのサポートを有効にすることを推奨します。

FlexPod Express と NetApp E シリーズの接続要件

E シリーズを使用した FlexPod Express の接続要件は次のとおりです。

- E シリーズストレージコントローラは、ファブリックインターコネクトに直接接続されている必要があります。
- FlexPod のコアコンポーネント間には、追加の機器をインラインで配置しないでください。
- vPC は、ファブリックインターコネクトとイーサネットスイッチの間に必要です。

AFF Express と NetApp FlexPod の接続要件

AFF Express と NetApp FlexPod の接続要件は次のとおりです。

- NetApp AFF ストレージコントローラは、 Cisco Nexus スイッチに直接接続する必要があります。ただし、 Cisco UCS で管理される構成では、ストレージコントローラがファブリックに接続されます。インターコネクト：
- FlexPod のコアコンポーネント間には、追加の機器をインラインで配置できません。
- Cisco Nexus 3000/9000 シリーズスイッチとネットアップストレージコントローラの接続には、仮想ポートチャネル（ vPC ）が必要です。
- 必須ではありませんが、環境全体でジャンボフレームのサポートを有効にすることを推奨します。

その他の要件

FlexPod Express のその他の要件は次のとおりです。

- 次の項目を含むすべての機器について、有効なサポート契約が必要です。
  - シスコ機器に対する SMARTnet サポート
  - ネットアップ機器に対する SupportEdge Advisor または SupportEdge Premium のサポート
- すべてのソフトウェアコンポーネントがにリストされ、サポートされている必要があります "NetApp IMT"。
- すべてのネットアップハードウェアコンポーネントがに一覧表示され、サポートされている必要があります "NetApp Hardware Universe の略"。
- すべての Cisco ハードウェアコンポーネントがにリストされ、でサポートされている必要があります "Cisco HCL"。

オプション機能

このセクションでは、 FlexPod Express のオプション機能について説明します。

iSCSI ブートオプション

FlexPod Express アーキテクチャは iSCSI ブートを使用します。iSCSI ブートオプションの最小要件は次のとおりです。

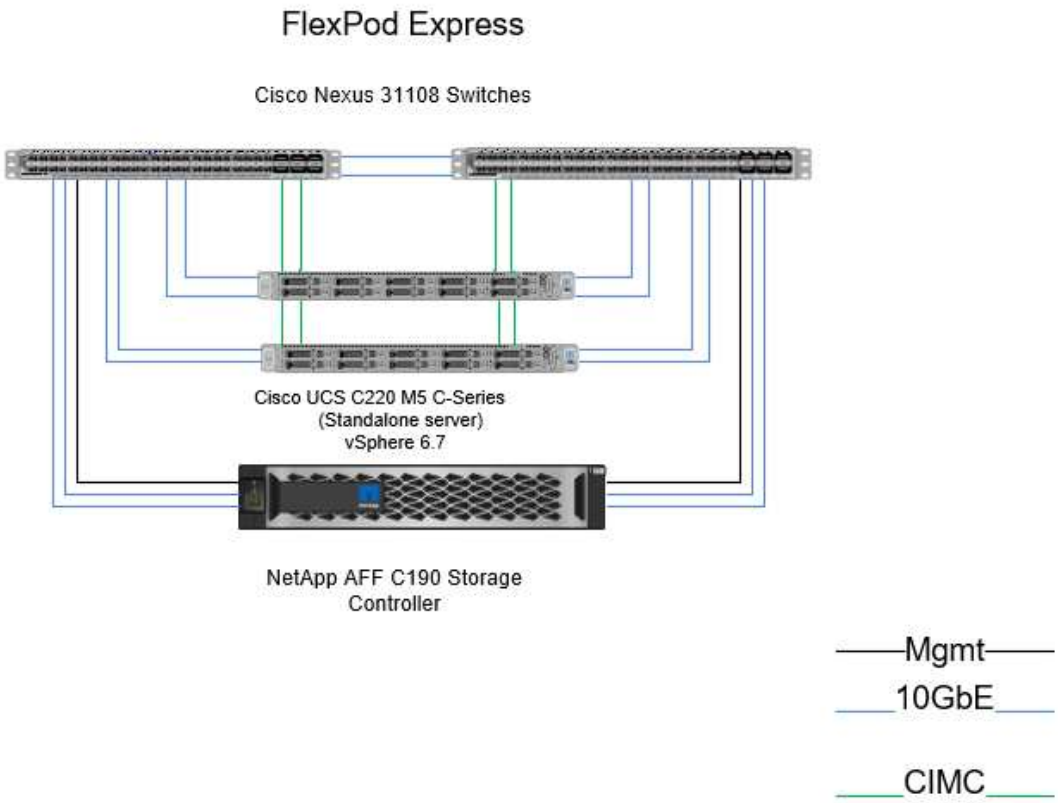
- ネットアップストレージコントローラでアクティブ化された iSCSI ライセンス / 機能
- ネットアップストレージコントローラ HA ペアの各ノードに、 2 ポート 10Gbps イーサネットアダプタを搭載します
- iSCSI ブートに対応した Cisco UCS サーバ内のアダプタ

設定オプション

このセクションでは、 FlexPod エクスプレスアーキテクチャで必要とされる設定と検証済みの設定について詳しく説明します。

FlexPod Express と **Cisco UCS C** シリーズおよび **AFF C190** シリーズ

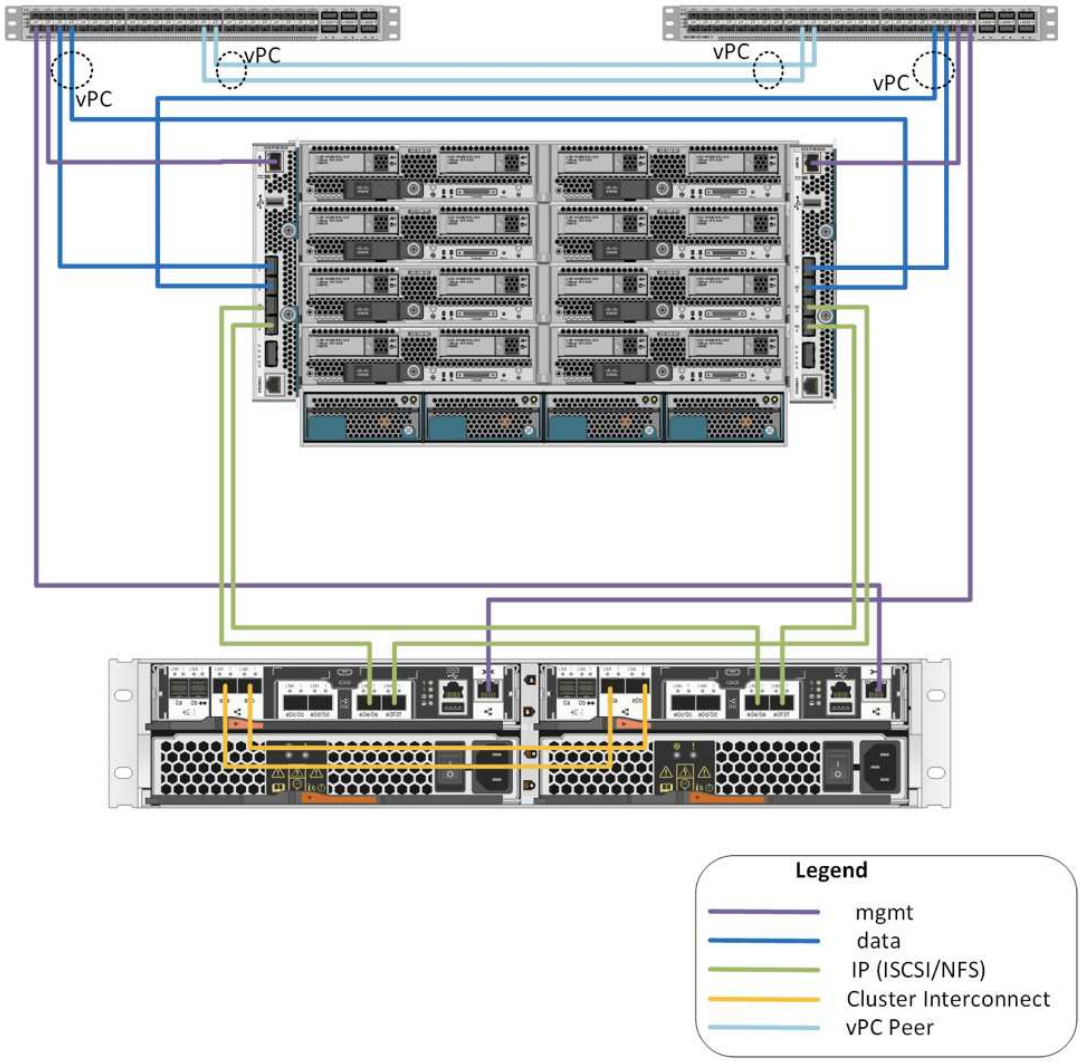
次の図に、 Cisco UCS C シリーズおよび AFF C190 シリーズ解決策を使用した FlexPod Express を示します。この解決策は、両方の 10GbE アップリンクをサポートします。



この構成の詳細については、『 FlexPod Express with VMware vSphere 6.7 』および『 NetApp AFF C190 NVA 導入ガイド』（現在）を参照してください。

Cisco UCS Mini と AFF A220 および FAS 2750/2720 を使用した FlexPod Express

次の図に、 FlexPod Express と Cisco UCS で管理される構成を示します。



この設定の詳細については、を参照してください "FlexPod Express と VMware vSphere 6.7U1 、および直接接続型の IP ベースストレージを搭載した NetApp AFF A220"。

シスコのコンポーネント

シスコは、 FlexPod Express の設計およびアーキテクチャに大きく貢献しており、解決策のコンピューティングおよびネットワーキングレイヤに貢献しています。ここでは、 FlexPod Express で使用できる Cisco UCS および Cisco Nexus コンポーネントについて説明します。

Cisco UCS B シリーズブレードサーバのオプション

Cisco UCS Mini プラットフォームで現在サポートされている Cisco UCS B シリーズブレードは、 B200 M5 および B420 M4 です。その他のブレードは、 Cisco UCS Mini プラットフォームでサポートされるようになるため、次の表に記載されます。

Cisco UCS B シリーズサーバ	パーツ番号	技術仕様
Cisco UCS B200 M5	UCSB-B2005-M5	https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-b200-m5-blade-server/model.html
Cisco UCS B200 M4	UCSB-B2004-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b200m4-specsheet.pdf
Cisco UCS B420 M4	UCSB-B420-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b420m4-spec-sheet.pdf

Cisco UCS C シリーズラックサーバのオプション

Cisco UCS C シリーズブレードには、 1 ラックおよび 2 ラックユニット（ RU ）のさまざまな種類があり、 CPU 、メモリ、 I/O のオプションもさまざまです。次の表に示す部品番号は、ベースサーバのものです。 CPU 、メモリ、ディスクドライブ、 PCIe カード、 Cisco FEX は含まれません。FlexPod では、複数の設定オプションを使用でき、サポートされています。

Cisco UCS C シリーズラックサーバ	パーツ番号	技術仕様
Cisco UCS C220 M4	UCSC-C220 - M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
Cisco UCS C240 M4	UCSC-C240 - M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c240m4-sff-spec-sheet.pdf
Cisco UCS C460 M4	UCSC-C460-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c460m4_specsheet.pdf

Cisco Nexus スイッチ

すべての FlexPod Express アーキテクチャに冗長スイッチが必要です。

AFF Express with FlexPod または FAS アーキテクチャは、 Cisco Nexus 31108 スイッチで構築されます。Cisco UCS Mini （ Cisco UCS で管理される）アーキテクチャを搭載した FlexPod Express は、 Cisco Nexus 3524 スイッチを使用して検証されます。この構成は、標準スイッチを使用して導入することもできます。

E シリーズを搭載した FlexPod Express は、標準スイッチとして導入できます。

次の表に、 Cisco Nexus シリーズシャーシの部品番号を示します。これらの部品番号には、追加の SFP モジュールやアドオンモジュールは含まれていません。

Cisco Nexus シリーズスイッチ	パーツ番号	技術仕様
Cisco Nexus 3048	N3K-C3048TP-1GE	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-685363.html
Cisco Nexus 31108	N3K-C31108PC-V	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 9396	N9K-C9396PX	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-729405.html
Cisco Nexus 3172	N3K-C3172.	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-729483.html

シスコのサポートライセンスオプション

FlexPod Express アーキテクチャのすべてのシスコ機器について、有効な SMARTnet サポート契約が必要です。

> 必要なライセンスとこれらのライセンスのパーツ番号は、製品によって異なる場合があるため、営業担当者が確認する必要があります。

次の表に、シスコのサポートライセンスオプションを示します。

Cisco Support のライセンス	ライセンスガイド
SMARTnet 24X7x4	http://www.cisco.com/web/services/portfolio/product-technical-support/smartnet/index.html

NetApp コンポーネント

ネットアップストレージコントローラは、ブートとアプリケーションデータストレージの両方を実現する FlexPod Express アーキテクチャのストレージ基盤を提供します。このセクションでは、 FlexPod Express アーキテクチャのさまざまなネットアップオプションについて説明します。

ネットアップストレージコントローラのオプション

NetApp FAS

AFF Express アーキテクチャでは、冗長構成の AFF C190 、 FlexPod A220 、または FAS2750 シリーズのコントローラが必要です。コントローラは ONTAP ソフトウェアを実行します。ストレージコントローラの注文時に、優先されるソフトウェアバージョンをコントローラにプリロードすることができます。ONTAP の場合、クラスタは、クラスタインターコネクトスイッチのペアを使用して導入することも、スイッチレスクラスタ構成に導入することもできます。

次の表に示すパーツ番号は、空のコントローラのものです。選択したストレージプラットフォームに応じて、さまざまなオプションや設定を使用できます。これらの追加コンポーネントの詳細については、営業担当者にお問い合わせください。

ストレージコントローラ	**FAS** パーツ番号	技術仕様
FAS2750	選択した個々のオプションに基づきます	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
FAS2720	選択した個々のオプションに基づきます	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
AFF C190	選択した個々のオプションに基づきます	https://www.netapp.com/us/products/entry-level-aff.aspx
AFF A220	選択した個々のオプションに基づきます	https://www.netapp.com/us/documentation/all-flash-fas.aspx
FAS2620	選択した個々のオプションに基づきます	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
FAS2650	選択した個々のオプションに基づきます	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx

E-Series ストレージ

FlexPod Express アーキテクチャには、 NetApp E2800 シリーズコントローラの HA ペアが必要です。コントローラは SANtricity OS を実行します。

次の表に示すパーツ番号は、空のコントローラのものです。選択したストレージプラットフォームに応じて、さまざまなオプションや設定を使用できます。これらの追加コンポーネントの詳細については、営業担当者にお問い合わせください。

ストレージコントローラ	パーツ番号	技術仕様
E2800	選択した個々のオプションに基づきます	http://www.netapp.com/us/products/storage-systems/e2800/e2800-tech-specs.aspx

ネットアップのイーサネット拡張モジュール

NetApp FAS

次の表に、 NetApp FAS10GbE アダプタオプションを示します。

コンポーネント	パーツ番号	技術仕様
NetApp X1117A	X1117A-R6	https://library.netapp.com/ecm/ecm_download_file/ECMM1280307

FAS2500 シリーズおよび 2600 シリーズのストレージシステムはオンボード 10GbE ポートを備えています。

NetApp X1117A アダプタは FAS8020 ストレージシステム用です。

E-Series ストレージ

次の表に、 E シリーズ 10GbE アダプタオプションを示します。

コンポーネント	パーツ番号
10GbE iSCSI / 16Gb FC 4 ポート	X-56025-00-0E-C
10GbE iSCSI / 16Gb FC 2 ポート	X-56024-00-0E-C

E2824 シリーズストレージシステムには、オンボード 10GbE ポートがあります。

10GbE iSCSI / 16Gb FC の 4 ポートホストインターフェイスカード（ HIC ）を使用してポート密度を高めることができます。

オンボードポートと HIC は、 SANtricity OS でアクティブ化された機能に応じて、 iSCSI アダプタまたは FC アダプタとして機能します。

サポートされているアダプタオプションの詳細については、の「アダプタ」セクションを参照してください "NetApp Hardware Universe の略"。

ネットアップのディスクシェルフとディスク

NetApp FAS

ストレージコントローラには、 1 台以上のネットアップディスクシェルフが必要です。選択したネットアップシェルフタイプによって、そのシェルフ内で使用可能なドライブタイプが決まります。

FAS2700 および FAS2600 シリーズのコントローラは、デュアルストレージコントローラと同じシャーシに搭載されたディスクを含む構成として提供されます。この構成には SATA ドライブまたは SAS ドライブを使用できます。そのため、パフォーマンスや容量の要件によってスピンドル数が制限されないかぎり、外付けディスクシェルフを追加する必要はありません。

ディスクシェルフの部品番号は、 AC PSU を 2 台搭載した空のシェルフのものです。その他のパーツ番号については、営業担当者にお問い合わせください。

ディスクドライブのパーツ番号は、購入するディスクのサイズとフォームファクタによって異なります。その他のパーツ番号については、営業担当者にお問い合わせください。

次の表に、ネットアップのディスクシェルフオプションと、 NetApp Hardware Universe に搭載されている各シェルフタイプでサポートされるドライブを示します。Hardware Universe リンクに従って、使用している ONTAP のバージョンを選択し、シェルフタイプを選択します。シェルフイメージの下の Supported Drives をクリックすると、特定のバージョンの ONTAP およびディスクシェルフでサポートされるドライブが表示されます。

ディスクシェルフ	パーツ番号	技術仕様
DS212C	DS212C 0-12	"NetApp Hardware Universe のディスクシェルフとストレージメディア技術仕様サポートされているドライブ"
DS224C	DS224C - 0 ~ 24	"NetApp Hardware Universe のディスクシェルフとストレージメディア技術仕様サポートされているドライブ"
DS460C	DS460C - 0~60	"NetApp Hardware Universe のディスクシェルフとストレージメディア技術仕様サポートされているドライブ"
DS2246	X559A-R6	"NetApp Hardware Universe のディスクシェルフとストレージメディア技術仕様サポートされているドライブ"
DS4246	X24M-R6	"NetApp Hardware Universe のディスクシェルフとストレージメディア技術仕様サポートされているドライブ"
DS4486	DS4486 - 144TB - R5-C	"NetApp Hardware Universe のディスクシェルフとストレージメディア技術仕様サポートされているドライブ"

E-Series ストレージ

シャーシにドライブを格納していないストレージコントローラには、少なくとも 1 台のネットアップディスクシェルフが必要です。選択したネットアップシェルフタイプによって、そのシェルフ内で使用可能なドライブタイプが決まります。

E2800 シリーズのコントローラは、デュアルストレージコントローラと、サポート対象のディスクシェルフに格納されたディスクを含む構成として提供されます。この構成は SSD または SAS ドライブで提供されます。

> ディスクドライブのパーツ番号は、購入するディスクのサイズとフォームファクタによって異なります。その他のパーツ番号については、営業担当者にお問い合わせください。

次の表に、ネットアップのディスクシェルフオプション、および各シェルフタイプでサポートされるドライブを示します。これらは、 NetApp Hardware Universe に搭載されています。Hardware Universe リンクに従って、使用している ONTAP のバージョンを選択し、シェルフタイプを選択します。シェルフイメージの下の Supported Drives をクリックすると、特定のバージョンの ONTAP およびディスクシェルフでサポートされるドライブが表示されます。

ディスクシェルフ	パーツ番号	技術仕様
DE460C	E-X5730A-DM-0E-C	"NetApp Hardware Universe のディスクシェルフ技術仕様サポートされているドライブ"
DE224C	E-X5721A-DM-0E-C	"NetApp Hardware Universe のディスクシェルフ技術仕様サポートされているドライブ"
DE212C	E-X5723A-DM-0E-C	"NetApp Hardware Universe のディスクシェルフ技術仕様サポートされているドライブ"

ネットアップのソフトウェアライセンスオプション

NetApp FAS

次の表に、 NetApp FAS ソフトウェアのライセンスオプションを示します。

ネットアップソフトウェアライセンス	パーツ番号	技術仕様
ベースクラスタライセンス	ライセンスについて詳しくは、ネットアップの営業チームにお問い合わせください。	

E-Series ストレージ

次の表に、 E シリーズソフトウェアのライセンスオプションを示します。

ネットアップソフトウェアライセンス	パーツ番号	技術仕様
標準装備	ライセンスについて詳しくは、ネットアップの営業チームにお問い合わせください。	
プレミアム機能		

ネットアップサポートのライセンスオプション

SupportEdge Premium ライセンスが必要です。これらのライセンスのパーツ番号は、 FlexPod Express デザインで選択されたオプションによって異なります。

NetApp FAS

次の表に、ネットアップがサポートする NetApp FAS のライセンスオプションを示します。

ネットアップサポートライセンス	パーツ番号	技術仕様
SupportEdge Premium4 時間オンサイト、月数 :36	： cs -O2-4HR	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf

E-Series ストレージ

次の表に、 E シリーズストレージのネットアップサポートライセンスオプションを示します。

ネットアップサポートライセンス	パーツ番号	技術仕様
ハードウェアサポート Premium ： 4 時間以内（オンサイト）、月数： 36	SVC-O2-4HR-E	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf
ソフトウェアサポート	SW-SSP-O2-4HR-E	
初期インストール	SVC-INST-O2-4HR-E	

電源とケーブル接続の要件

このセクションでは、 FlexPod Express デザインの電源要件および最小ケーブル要件について説明します。

電力要件

電力要件は米国に基づいていますAC 電源の仕様と使用を前提としています。他の国では、電力要件が異なる場合があります。直流（ DC ）電源オプションは、ほとんどのコンポーネントで使用できます。必要な最大電力およびその他の詳細な電力情報の詳細については、各ハードウェアコンポーネントの詳細な技術仕様を参照してください。

Cisco UCS の電力データの詳細については、を参照してください "Cisco UCS Power Calculator"。

次の表に、各デバイスに必要な電源ポートを示します。

Cisco Nexus スイッチ	電源ケーブルが必要です
Cisco Nexus 3048	Cisco Nexus 3000 シリーズスイッチごとに C13-C14 電源ケーブル × 2
Cisco Nexus 3524	Cisco Nexus 3000 シリーズスイッチごとに C13-C14 電源ケーブル × 2
Cisco Nexus 9396	Cisco Nexus 9000 シリーズスイッチごとに C13-C14 電源ケーブル × 2

Cisco UCS シャーシ	電源ケーブルが必要です
Cisco UCS 5108	Cisco UCS シャーシごとに 2 つの CAB-US515P-C19-US/CAB-US520-c19-US

Cisco UCS B シリーズサーバ	電源ケーブルが必要です
Cisco UCS B200 M4	N/A 。ブレードサーバはシャーシから電源供給されます
Cisco UCS B420 M4	N/A 。ブレードサーバはシャーシから電源供給されます
Cisco UCS B200 M5	N/A 。ブレードサーバはシャーシから電源供給されます
Cisco UCS B480 M5 の場合	N/A 。ブレードサーバはシャーシから電源供給されます

Cisco UCS C シリーズサーバ	電源ポートが必要です
Cisco UCS C220 M4	Cisco UCS サーバごとに C13-C14 電源ケーブル × 2
Cisco UCS C240 M4	
Cisco UCS C460 M4 Cisco UCS C220 M5 Cisco UCS C240 M5 Cisco UCS C480 M5	

NetApp FAS コントローラ	必要な電源ポート（ **HA** ペアごと）
FAS2554 のこと	C13-C14 × 2
FAS2552	C13-C14 × 2
FAS2520	C13-C14 × 2
FAS8020	C13-C14 × 2

E シリーズコントローラ	必要な電源ポート（ **HA** ペアごと）
E2824	C14 / C20 × 2

NetApp FAS ディスクシェルフ	電源ポートが必要です
DS212C	C13-C14 × 2
DS224C	C13-C14 × 2
DS460C	C13-C14 × 2
DS2246	C13-C14 × 2
DS4246	C13-C14 × 4

E-Series ディスクシェルフ	電源ポートが必要です
DE460C	C14 / C20 × 2
DE224C	C14 / C20 × 2
DE212C	C14 / C20 × 2

ケーブルの最小要件

ここでは、 FlexPod Express デザインの最小ケーブル要件について説明します。ほとんどの FlexPod 環境では追加のケーブルが必要ですが、構成数は導入規模と範囲によって異なります。

次の表に、各デバイスに必要なケーブルの最小数を示します。

Cisco Nexus 3000 シリーズスイッチ	ケーブルが必要です
Cisco Nexus 31108	スイッチごとに 10GbE ファイバケーブルまたは Twinax ケーブルが少なくとも 2 本必要です
Cisco Nexus 3172PQ の場合	
Cisco Nexus 3048	
Cisco Nexus 3524	
Cisco Nexus 9396	
DS212C	
DS2246	SAS ケーブルの数は、ディスクシェルフの構成によって異なります
DS460C	
DS224C	
DS4246	
E2800	• コントローラ 1 台につき、管理用のギガビットイーサネット（ 1GbE ）ケーブルが少なくとも 1 本必要です • コントローラ 1 台につき 10GbE ケーブル 2 本以上（ iSCSI の場合）または FC ケーブル 2 本以上で、速度要件が同じです
DE460C	ディスクシェルフ 1 台につき、 Mini-SAS HD ケーブル 2 本
DE224C	ディスクシェルフ 1 台につき、 Mini-SAS HD ケーブル 2 本
DE212C	ディスクシェルフ 1 台につき、 Mini-SAS HD ケーブル 2 本

技術仕様と参考資料

このセクションでは、 FlexPod Express の各コンポーネントに関するその他の重要な技術仕様について説明します。

Cisco UCS B シリーズブレードサーバ

次の表に、 Cisco UCS B シリーズブレードサーバのオプションを示します。

コンポーネント	**Cisco UCS B200 M4**	**Cisco UCS B420 M4**	**Cisco UCS B200 M5**
プロセッサのサポート	Intel Xeon E5-2600	Intel Xeon E5-4600	インテル ® Xeon ® スケーラブル・プロセッサー
最大メモリ容量	DIMM × 24 、最大 768GB	DIMM × 48 、最大 3TB	最大 3072GB の DIMM を 24 枚

コンポーネント	**Cisco UCS B200 M4**	**Cisco UCS B420 M4**	**Cisco UCS B200 M5**
メモリのサイズと速度	32GB DDR4 、 2133MHz	64GB DDR4 、 2400MHz	16GB 、 32GB 、 64GB 、 128GB DDR4 、 2666MHz
SAN ブートサポート	はい。	はい。	はい。
メザニン I/O アダプタスロット	2.	3.	GPU サポートを含む、前面と背面の 2 つのポートを備えています
I/O の最大スループット	80GBps です	160GBps です	80GBps です

Cisco UCS C シリーズラックサーバ

次の表に、 Cisco UCS C シリーズラックサーバのオプションを示します。

コンポーネント	**Cisco UCS C220 M4**	**Cisco UCS C240 M4**	**Cisco UCS C460 M4**	**Cisco UCS C220 M5**
プロセッサのサポート	1 または 2 個の Intel E5-2600 シリーズ	Intel Xeon E5-2600 シリーズ 1 台または 2 台	Intel Xeon E7-4800/8800 シリーズ × 2 または 4	インテル ® Xeon ® スケーラブル・プロセッサー（ 1 または 2 ）
最大メモリ容量	1.5GB	1.5 TB	6 TB	3072GB
PCIe スロット	2.	6.	10.	2.
フォームファクタ	1RU	2RU	4RU	1 RU

次の表に、 Cisco UCS C シリーズラックサーバオプションのデータシートを示します。

コンポーネント	**Cisco UCS** データシート
Cisco UCS C220 M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
Cisco UCS C240 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m4-rack-server/datasheet-c78-732455.html
Cisco UCS C460 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c460-m4-rack-server/datasheet-c78-730907.html
Cisco UCS C220 M5	https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m5-sff-specsheet.pdf

Cisco Nexus 3000 シリーズスイッチ

次の表に、 Cisco Nexus 3000 シリーズスイッチのオプションを示します。

コンポーネント	**Cisco Nexus 3048**	**Cisco Nexus 3524**	**Cisco Nexus 31108**	**Cisco Nexus 3172PQ** の場合
フォームファクタ	1RU	1RU	1RU	1 RU
1Gbps ポートの最大数	48	24	48 （ 10/40/100Gbps ）	1 / 10GbE ポート × 72 、または 1 / 10GbE ポート × 48 、 40GbE ポート × 6
転送レート	132MBps	360Mbps	1.2Bpps	1 、 pps
ジャンボフレームのサポート	はい。	はい。	はい。	はい。

次の表に、 Cisco Nexus 3000 シリーズスイッチオプションのデータシートを示します。

コンポーネント	**Cisco Nexus** データシート
Cisco Nexus 31108	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 3172PQ の場合	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3048	https://www.cisco.com/c/en/us/products/switches/nexus-3048-switch/index.html
Cisco Nexus 3172PQ-XL	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3548 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html
Cisco Nexus 3548	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html

次の表に、 Cisco Nexus 9000 シリーズのスイッチオプションを示します。

コンポーネント	**Cisco Nexus 9396**	**Cisco Nexus 9372**
フォームファクタ	2RU	1RU
最大ポート数	60	54
10Gbps SFP+ アップリンクポート	48	48

次の表に、 Cisco Nexus 9000 シリーズスイッチオプションのデータシートを示します。

コンポーネント	**Cisco Nexus** データシート
Cisco Nexus 9396	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Cisco Nexus 9372	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Nexus 9396X	https://www.cisco.com/c/en/us/products/switches/nexus-9396px-switch/index.html?dtid=osscdc000283

NetApp FAS ストレージコントローラ

次の表に、ネットアップ FAS の現在のストレージコントローラオプションを示します。

現在のコンポーネント	**FAS2620**	**FAS2650**
設定	2U シャーシに 2 台のコントローラを搭載できます	4U シャーシに 2 台のコントローラを搭載します
最大物理容量	1440TB	1243TB
内蔵ドライブ	12.	24
最大ドライブ数（内蔵および外付け）	144	144
最大ボリュームサイズ	100TB	
最大アグリゲートサイズ	4TB	
LUN の最大数	コントローラあたり 2 、 048	
サポートするストレージネットワークプロトコル	iSCSI 、 FC 、 FCoE 、 NFS 、 CIFS	
NetApp FlexVol の最大ボリューム数	コントローラあたり 1 、 000	
NetApp Snapshot コピーの最大数	コントローラあたり 25 、 000	
NetApp Flash Pool インテリジェントなデータキャッシングを最大限に活用	24 TB	

FAS ストレージコントローラオプションの詳細については、を参照してください "FAS モデル" Hardware Universe のセクション。AFF の場合は、を参照してください "AFF モデル" セクション。

次の表に、 FAS8020 コントローラシステムの特性を示します。

コンポーネント	**FAS8020**
設定	3U シャーシに 2 台のコントローラを搭載します
最大物理容量	2880TB

コンポーネント	**FAS8020**
ドライブの最大数	480
最大ボリュームサイズ	70TB
最大アグリゲートサイズ	324TB
LUN の最大数	コントローラあたり 8 、 192
サポートするストレージネットワークプロトコル	iSCSI 、 FC 、 NFS 、 CIFS
FlexVol の最大数	コントローラあたり 1 、 000
Snapshot コピーの最大数	コントローラあたり 25 、 000
NetApp Flash Cache によるインテリジェントなデータキャッシングを最大限に活用	3TB
Flash Pool の最大データキャッシング	24 TB

次の表に、ネットアップストレージコントローラのデータシートを示します。

コンポーネント	ストレージコントローラのデータシート
FAS2600 シリーズ	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
FAS2500 シリーズ	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8000 シリーズ	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

ネットアップ **FAS** イーサネットアダプタ

次の表に、ネットアップ FAS 10GbE アダプタを示します。

コンポーネント	**X1117A-R6**
ポート数	2.
アダプタタイプ	SFP+ （ファイバ使用

FAS8000 シリーズコントローラでは X1117A-R6 SFP+ アダプタがサポートされます。

FAS2600 および FAS2500 シリーズストレージシステムはオンボード 10GbE ポートを備えています。詳細については、を参照してください "NetApp 10GbE アダプタのデータシート"。

> AFF または FAS モデルに基づくアダプタの詳細については、を参照してください "アダプタセクション" を参照してください。 Hardware Universe

NetApp FAS ディスクシェルフ

次の表に、ネットアップ FAS のディスクシェルフオプションの最新情報を示します。

コンポーネント	DS460C	DS224C	DS212C	DS2246	DS4246
フォームファクタ	4RU	2RU	2RU	2RU	4RU
エンクロージャあたりのドライブ数	60	24	12.	24	24
ドライブのフォームファクタ	3.5 インチラージフォームファクタ	2.5 インチスモールフォームファクタ	3.5 インチラージフォームファクタ	2.5 インチスモールフォームファクタ	3.5 インチラージフォームファクタ
シェルフ I/O モジュール	デュアル IOM12 モジュール	デュアル IOM12 モジュール	デュアル IOM12 モジュール	デュアル IOM6 モジュール	デュアル IOM6 モジュール

詳細については、ネットアップディスクシェルフのデータシートを参照してください。

> ディスクシェルフの詳細については、『 NetApp Hardware Universe 』を参照してください "Disk Shelves セクション"。

NetApp FAS ディスクドライブ

ネットアップのディスクの技術仕様には、フォームファクタサイズ、ディスク容量、ディスク rpm 、サポートコントローラ、 Data ONTAP のバージョンなどがあり、これらはのドライブのセクションに記載されています "NetApp Hardware Universe の略"。

E シリーズストレージコントローラ

次の表に、現在の E シリーズストレージコントローラのオプションを示します。

現在のコンポーネント	E2812	E2824	E2860 となります
設定	2U シャーシに 2 台のコントローラを搭載できます	2U シャーシに 2 台のコントローラを搭載できます	4U シャーシに 2 台のコントローラを搭載します
最大物理容量	1 、 800TB	1756.8TB	1 、 800TB
内蔵ドライブ	12.	24	60
最大ドライブ数（内蔵および外付け）	180		
最大 SSD 数	120		
ディスクプールボリュームの最大ボリュームサイズ	1 、 024TB		
最大ディスクプール数	20		
サポートするストレージネットワークプロトコル	iSCSI および FC		
最大ボリューム数	512		

次の表に、最新の E シリーズストレージコントローラのデータシートを示します。

コンポーネント	ストレージコントローラのデータシート
E2800	http://www.netapp.com/us/media/ds-3805.pdf

E シリーズアダプタ

次の表に、 E シリーズのアダプタを示します。

コンポーネント	**X-56023-00-0E-C**	**X-56025-00-0E-C**	**X-56027-00-0E-C**	**X-56024-00-0E-C**	**X-56026-00-0E-C**
ポート数	2.	4.	4.	2.	2.
アダプタタイプ	10Gb Base-T の提供です	16G FC および 10GbE iSCSI	（ SAS ）。	16G FC および 10GbE iSCSI	（ SAS ）。

E-Series ディスクシェルフ

次の表に、 E シリーズのディスクシェルフオプションを示します。

コンポーネント	**DE212C**	**DE224C**	**DE460C**
フォームファクタ	2RU	2RU	4RU
エンクロージャあたりのドライブ数	12.	24	60
ドライブのフォームファクタ	2.5 インチスモールフォームファクタ 3.5 インチ	2.5 インチ	2.5 インチスモールフォームファクタ 3.5 インチ
シェルフ I/O モジュール	IOM12	IOM12	IOM12

E シリーズのディスクドライブ

ネットアップのディスクドライブの技術仕様には、フォームファクタサイズ、ディスク容量、ディスク rpm 、サポートコントローラ、 SANtricity のバージョンなどがあり、これらはのドライブセクションに記載されています "NetApp Hardware Universe の略"。

以前のアーキテクチャと機器

解決策は、 Cisco とネットアップが現在販売している既存の機器と新しい機器の両方を使用できる柔軟な FlexPod です。場合によっては、 Cisco とネットアップの両モデルの機器の販売終了が決まっています。

これらのモデルの機器は提供されなくなりましたが、販売終了日までにこれらのモデルのいずれかを購入したお客様は、 FlexPod 構成でその機器を使用できます。

さらに、 FlexPod Express アーキテクチャは定期的に更新され、 Cisco とネットアップの最新のハードウェアとソフトウェアを FlexPod Express 解決策に導入します。このセクションでは、以前に使用した FlexPod Express のアーキテクチャとハードウェアを示します。

以前の **FlexPod Express** アーキテクチャ

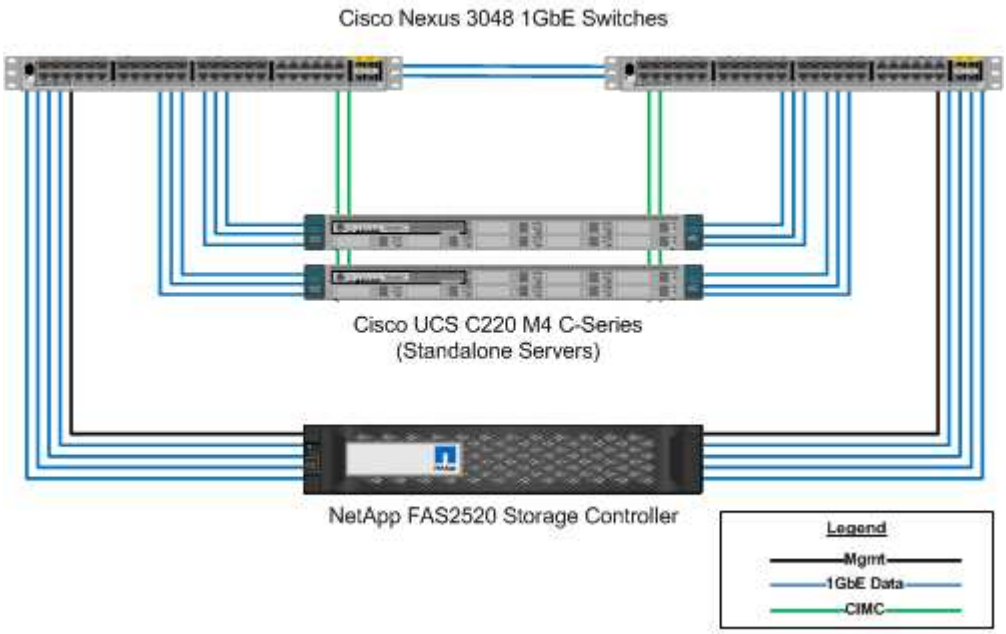
ここでは、これまでの FlexPod Express アーキテクチャについて説明します。

FlexPod Express の小規模および中規模構成

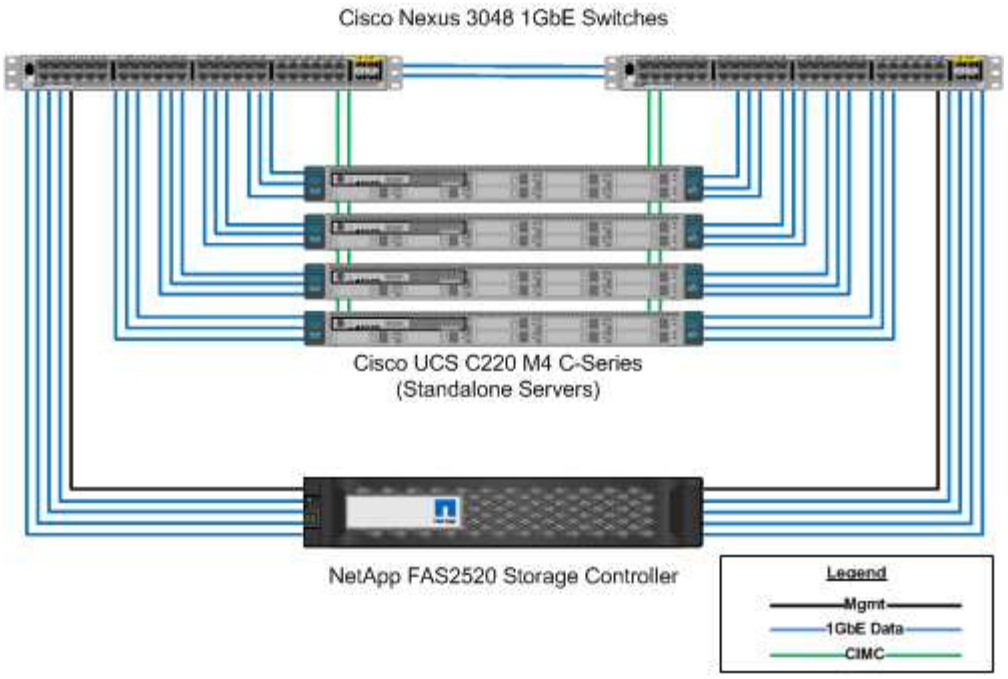
FlexPod Express の小規模および中規模構成には、次のコンポーネントが含まれます。

- 冗長構成の 2 台の Cisco Nexus 3048 スイッチ
- Cisco UCS C シリーズラックマウントサーバを 2 台以上
- HA ペア構成の場合、 2 台の FAS2200 または FAS2500 シリーズコントローラ

次の図に、 FlexPod Express の小規模構成を示します。



次の図は、 FlexPod Express の中規模構成を示しています。

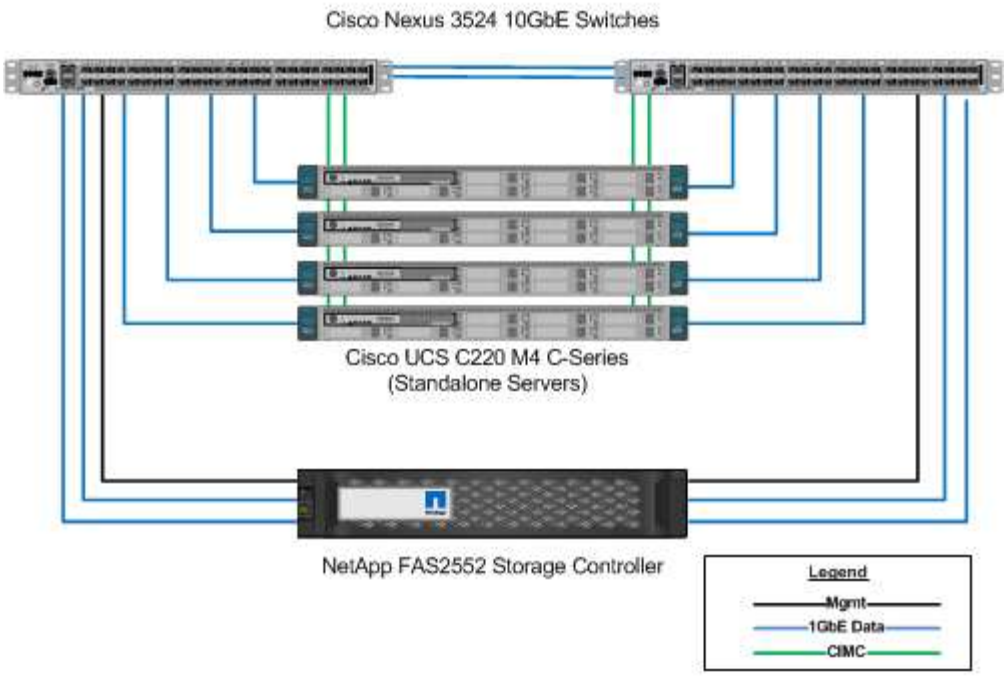


FlexPod Express の大規模構成

FlexPod Express の大規模構成には、次のコンポーネントが含まれます。

- 冗長構成の Cisco Nexus 3500 シリーズまたは Cisco Nexus 9300 シリーズスイッチ × 2
- Cisco UCS C シリーズラックマウントサーバを 2 台以上
- HA ペア構成の FAS2552 、 FAS2554 、または FAS8020 コントローラ × 2 （コントローラごとに 10GbE ポートが 2 つ必要）
- ネットアップディスクシェルフ × 1 （ FAS8020 を使用した場合）

次の図に、 FlexPod Express の大規模構成を示します。



以前の **FlexPod Express** 検証済みアーキテクチャ

以前の FlexPod Express 検証済みアーキテクチャも引き続きサポートされます。アーキテクチャと導入に関するドキュメントは、次のとおりです。

- "FlexPod Express 、 Cisco UCS C シリーズおよび NetApp FAS2500 シリーズ"
- "FlexPod Express with VMware vSphere 6.0 ：小規模および中規模構成"
- "FlexPod Express with VMware vSphere 6.0 ：大規模構成"
- "FlexPod Express with Microsoft Windows Server 2012 R2 Hyper-V ：小規模および中規模構成"
- "FlexPod Express with Microsoft Windows Server 2012 R2 Hyper-V ：大規模構成"

以前のハードウェア

次の表に、以前の FlexPod Express アーキテクチャで使用されていたハードウェアを示します。

以前のアーキテクチャで使用されていたハードウェア	技術仕様（利用可能な場合）
Cisco UCS C220 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c220-m3-rack-server/data_sheet_c78-700626.html
Cisco UCS C24 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706103.html
Cisco UCS C22 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706101.html
Cisco UCS C240 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m3-rack-server/data_sheet_c78-700629.html

以前のアーキテクチャで使用されていたハードウェア	技術仕様（利用可能な場合）
Cisco UCS C260 M2 の場合	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/c260m2_specsheet.pdf
Cisco UCS C420 M3 の場合	http://www.cisco.com/en/US/products/ps12770/index.html
Cisco UCS C460 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps11587/spec_sheet_c17-662220.pdf
Cisco UCS B200 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b200-m3-blade-server/data_sheet_c78-700625.html
Cisco UCS B420 M3 の特長を説明します	該当なし
Cisco UCS B22 M3	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b22m3_specsheet.pdf
Cisco Nexus 3524	http://www.cisco.com/c/en/us/products/switches/nexus-3524-switch/index.html
FAS2240	
FAS2220	http://www.netapp.com/us/products/storage-systems/fas2200/fas2200-tech-specs.aspx
DS4243	該当なし

レガシー機器

ネットアップの従来型ストレージコントローラオプションを次の表に示します。

ストレージコントローラ	**FAS** パーツ番号	技術仕様
FAS2520	選択した個々のオプションに基づきます	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	選択した個々のオプションに基づきます	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554 のこと	選択した個々のオプションに基づきます	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	選択した個々のオプションに基づきます	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

次の表に、 NetApp FAS で使用されている従来型のディスクシェルフオプションを示します。

ディスクシェルフ	パーツ番号	技術仕様
DE1600	E-X5682A-DM-0E-R6-C	"NetApp Hardware Universe のディスクシェルフ技術仕様サポートされているドライブ"
DE5600	E-X4041A-12-R6	"NetApp Hardware Universe のディスクシェルフ技術仕様サポートされているドライブ"
DE6600	X-48564-00-R6	"NetApp Hardware Universe のディスクシェルフ技術仕様サポートされているドライブ"

ネットアップの従来型 **FAS** コントローラ

次の表に、ネットアップの従来の FAS コントローラオプションを示します。

現在のコンポーネント	**FAS2554** のこと	**FAS2552**	**FAS2520**
設定	4U シャーシに 2 台のコントローラを搭載します	2U シャーシに 2 台のコントローラを搭載できます	2U シャーシに 2 台のコントローラを搭載できます
最大物理容量	576TB	509TB になります	336TB
内蔵ドライブ	24	24	12.
最大ドライブ数（内蔵および外付け）	144	144	84
最大ボリュームサイズ	60TB		
最大アグリゲートサイズ	120TB		
LUN の最大数	コントローラあたり 2 、 048		
サポートするストレージネットワークプロトコル	iSCSI 、 FC 、 FCoE 、 NFS 、 CIFS		iSCSI 、 NFS 、および CIFS
NetApp FlexVol の最大ボリューム数	コントローラあたり 1 、 000		
NetApp Snapshot コピーの最大数	コントローラあたり 25 、 000		

その他の NetApp FAS モデルについては、を参照してください "FAS モデルセクション" を参照してください。 Hardware Universe

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、次のドキュメントおよび Web サイトを参照してください。

- AFF および FAS システムドキュメントセンター

  "https://docs.netapp.com/platstor/index.jsp"

- AFF ドキュメントのリソースページ

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FAS ストレージシステムのドキュメントリソースページ

  "https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- NetApp のドキュメント

  "https://docs.netapp.com"

FlexPod データセンター技術仕様

TR-4036 ：『 FlexPod Datacenter Technical Specifications 』

ネットアップ、 Arvind Ramakrishnan 氏、 Jyh Shing Chen 氏

FlexPod プラットフォームは、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus ファミリースイッチ、およびネットアップストレージコントローラ（ AFF 、 ASA 、または FAS システム）を基盤として構築された、事前設計されたベストプラクティスのデータセンターアーキテクチャです。

FlexPod は、さまざまな仮想ハイパーバイザーや、ベアメタルのオペレーティングシステム、エンタープライズワークロードを実行するのに適したプラットフォームです。FlexPod は、ベースライン構成だけでなく、さまざまなユースケースや要件に対応できるよう、サイズ設定と最適化が可能な柔軟性も備えています。

> FlexPod の完全な設定を注文する前に、を参照してください "FlexPod 統合インフラ" これらの技術仕様の最新バージョンについては、 netapp.com のページを参照してください。

"次の例は、 FlexPod プラットフォームです。"

FlexPod プラットフォーム

FlexPod プラットフォームには、次の 2 つがあります。

- * FlexPod データセンター。 * このプラットフォームは、ワークロードエンタープライズアプリケーション、仮想化、仮想デスクトップインフラ（ VDI ）、パブリック、プライベート、ハイブリッドのクラウドワークロードに適した、拡張性にきわめて優れた仮想データセンターインフラストラクチャです。
- * FlexPod Express. * このプラットフォームは、リモートオフィスやエッジ向けのコンパクトな統合インフラストラクチャです。FlexPod Express には、に記載されている独自の仕様があります "FlexPod Express 技術仕様。"

本ドキュメントでは、 FlexPod データセンタープラットフォームの技術仕様について説明します。

FlexPod ルール

FlexPod の設計により、多数の異なるコンポーネントとソフトウェアバージョンを含む柔軟なインフラが実現します。

ルールセットは、有効な FlexPod 構成を構築またはアセンブルするためのガイドとして使用します。このドキュメントに記載されている番号とルールは、 FlexPod 構成の最小要件です。また、環境やユースケースに応じて、同梱されている製品ファミリー内で拡張することもできます。

サポート対象の FlexPod 構成と検証済みの 構成の比較

FlexPod アーキテクチャは、本ドキュメントで説明する一連のルールによって定義されています。ハードウェアコンポーネントとソフトウェア構成がでサポートされている必要があります "Cisco UCS ハードウェアおよびソフトウェア互換性リスト" および "ネットアップの Interoperability Matrix Tool （ IMT ）"。

各 Cisco Validated Design （ CVD ）または NetApp Verified Architecture （ NVA ）は、 FlexPod 構成の可能性があります。Cisco とネットアップは、これらの構成の組み合わせを文書化し、広範なエンドツーエンドのテストで検証しています。このドキュメントのガイドラインに従い、すべてのコンポーネントが Cisco UCS ハードウェアおよびソフトウェア互換性リストおよびネットアップに互換性があると記載されている場合、これらの構成から外れる FlexPod 環境は完全にサポートされます "IMT"。

たとえば、ストレージコントローラや Cisco UCS サーバを追加し、ソフトウェアを新しいバージョンにアップグレードする場合、ソフトウェア、ハードウェア、構成がこのドキュメントで定義されているガイドラインを満たしていれば、それらが完全にサポートされます。

NetApp ONTAP

NetApp ONTAP ソフトウェアは、すべてのネットアップ FAS 、 AFF 、および AFF All SAN Array （ ASA ）システムにインストールされます。FlexPod は、 ONTAP ソフトウェアとの検証済みで、ノンストップオペレーション、無停止アップグレード、即応性に優れたデータインフラを実現する、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。

ONTAP の詳細については、を参照してください "ONTAP データ管理ソフトウェア" 製品ページ。

Cisco Nexus スイッチング動作モード

特定の FlexPod 環境のスイッチングコンポーネントとして、さまざまな Cisco Nexus 製品を使用できます。これらのオプションのほとんどは、従来の Cisco Nexus OS または NX-OS ソフトウェアを利用しています。Cisco Nexus ファミリーのスイッチは、製品ライン内でさまざまな機能を提供します。これらの機能については、このドキュメントで後述します。

シスコが提供する Software-Defined ネットワーク分野の製品は、 Application Centric Infrastructure （ ACI ）と呼ばれています。ACI モードをサポートする Cisco Nexus 製品ラインは、ファブリックモードとも呼ばれ、 Cisco Nexus 9300 シリーズです。これらのスイッチは、 NX-OS またはスタンドアロンモードにも導入できます。

Cisco ACI は、特定のアプリケーションの要件に重点を置いたデータセンター導入をターゲットとしています。アプリケーションは、ホストまたは仮想マシン（ VM ）からネットワーク経由でストレージに接続できる一連のプロファイルと契約を通じてインスタンス化されます。

FlexPod は、 Cisco Nexus スイッチの両方の動作モードで検証されます。ACI モードと NX-OS モードの詳細については、次の Cisco のページを参照してください。

- "Cisco Application Centric Infrastructure の場合"
- "Cisco NX-OS ソフトウェア"

ハードウェアの最小要件

FlexPod データセンター構成には、スイッチ、ファブリックインターコネクト、サーバ、ネットアップストレージコントローラなど、最小限のハードウェア要件が含まれますが、これらに限定されません。

Cisco UCS サーバを使用する必要があります。事前検証済みの設計では、 C シリーズサーバと B シリーズサーバの両方を使用しています。Cisco Nexus ファブリックエクステンダ（ FEX ）は、 C シリーズサーバではオプションです。

FlexPod 構成には、ハードウェアに関する次の最小要件があります。

- 冗長構成の 2 台の Cisco Nexus スイッチこの構成は、 Cisco Nexus 5000 、 7000 、または 9000 シリーズの 2 台の冗長スイッチで構成できます。2 つのスイッチは同じモデルであり、同じ動作モードで設定する必要があります。

  ACI アーキテクチャを導入する場合は、次の追加要件を確認する必要があります。

  - Cisco Nexus 9000 シリーズスイッチをリーフスパイントポロジに導入する。
  - 3 つの Cisco Application Policy Infrastructure Controller （APIC; アプリケーションポリシーインフラストラクチャコントローラ）を使用します。
- 冗長構成の Cisco UCS 6200 、 6300 、または 6400 シリーズファブリックインターコネクト × 2
- Cisco UCS サーバ：
  - 解決策が B シリーズサーバを使用する場合は、 Cisco UCS 5108 B シリーズブレードサーバシャーシ 1 台と Cisco UCS B シリーズブレードサーバ 2 台と、 2104 、 2204/8 、 2408 、または 2304 I/O モジュール（ IOM ） 2 台を合わせます。
  - 解決策が C シリーズサーバを使用している場合は、 Cisco UCS C シリーズラックサーバを 2 台。

    Cisco UCS C シリーズラックサーバをより大規模に導入する場合は、 2232PP FEX モジュールのペアを選択できます。ただし、 2232PP はハードウェア要件ではありません。
- ハイアベイラビリティ（ HA ）ペア構成のネットアップストレージコントローラ × 2 ：

  この構成には、サポートされているネットアップの FAS 、 AFF 、または ASA シリーズのストレージコントローラが含まれます。を参照してください "NetApp Hardware Universe の略" サポートされている FAS 、 AFF 、 ASA の各コントローラモデルの最新リストを表示するためのアプリケーション。

  - HA 構成では、データアクセス用にコントローラごとに 2 つの冗長インターフェイスが必要です。インターフェイスは FCoE 、 FC 、 10 / 25 / 100Gb イーサネット（ GbE ）です。

- 解決策で NetApp ONTAP を使用している場合は、ネットアップの承認を受けたクラスタインターコネクトトポロジが必要です。詳細については、を参照してください "スイッチ" NetApp Hardware Universe のタブ。
- 解決策が ONTAP を使用している場合、データアクセスには、コントローラごとに最低 2 つの 10 / 25 / 100GbE ポートが追加で必要です。
- 2 ノード構成の ONTAP クラスタでは、 2 ノードスイッチレスクラスタを構成できます。
- ONTAP クラスタのノードが 3 つ以上の場合は、クラスタインターコネクトスイッチのペアが必要です。

- サポート対象のディスクタイプが設定されたネットアップディスクシェルフ × 1のシェルフタブを参照してください "NetApp Hardware Universe の略" サポートされるディスクシェルフモデルの最新のリストについては、を参照してください。

ソフトウェアの最小要件

FlexPod 構成には、次に示す最小ソフトウェア要件があります。

- NetApp ONTAP
  - ONTAP ソフトウェアのバージョンには ONTAP 9.1 以降が必要です
- Cisco UCS Manager リリース：
  - Cisco UCS 6200 シリーズファブリックインターコネクト - 2.2 （ 8a ）
  - Cisco UCS 6300 シリーズファブリックインターコネクト： 3.1 （ 1e ）
  - Cisco UCS 6400 シリーズファブリックインターコネクト： 4.0(1)
- Cisco Intersight 管理モード：
  - Cisco UCS 6400 シリーズファブリックインターコネクト– 4.1(2)
- Cisco Nexus 5000 シリーズスイッチの場合、 Cisco NX-OS ソフトウェアリリース 5.0(3)N1 （ 1c ）以降（ NX-OS 5.1.x を含む）
- Cisco Nexus 7000 シリーズスイッチの場合：
  - 4 スロットシャーシには、 Cisco NX-OS ソフトウェアリリース 6.1(2) 以降が必要です
  - 9 スロットシャーシには、 Cisco NX-OS ソフトウェアリリース 5.2 以降が必要です
  - 10 スロットシャーシには、 Cisco NX-OS ソフトウェアリリース 4.0 以降が必要です
  - 18 スロットシャーシには、 Cisco NX-OS ソフトウェアリリース 4.1 以降が必要です
- Cisco Nexus 9000 シリーズスイッチの場合は、 Cisco NX-OS ソフトウェアリリース 6.1(2) 以降が必要です

> FlexPod 構成で使用するソフトウェアがネットアップに表示され、サポートされている必要があります "IMT"。一部の機能では、リストされている機能よりも新しいリリースのソフトウェアが必要になる場合があります。

接続要件

FlexPod 構成には、次の接続要件があります。

- すべてのコンポーネントに対し、 100Mbps イーサネット / 1Gb イーサネットアウトオブバンド管理ネットワークがそれぞれ必要です。
- 環境全体でジャンボフレームのサポートを有効にすることを推奨しますが、必須ではありません。
- Cisco UCS ファブリックインターコネクトアプライアンスのポートは、 iSCSI 接続と NAS 接続にのみ使用することを推奨します。
- FlexPod のコアコンポーネント間に他の機器を配置することはできません。

アップリンク接続：

- 仮想ポートチャネル（ vPC ）をサポートするには、ネットアップストレージコントローラのポートを Cisco Nexus 5000 、 7000 、または 9000 シリーズスイッチに接続する必要があります。
- vPC は、 Cisco Nexus 5000 、 7000 、または 9000 シリーズスイッチとネットアップストレージコントローラの間で必要となります。
- vPC は、 Cisco Nexus 5000 、 7000 、または 9000 シリーズスイッチとファブリックインターコネクトの間で必要となります。
- vPC には少なくとも 2 つの接続が必要です。アプリケーションの負荷とパフォーマンスの要件に基づいて、 vPC 内の接続数を増やすことができます。

直接接続：

- ファブリックインターコネクトに直接接続されているネットアップストレージコントローラポートは、グループ化してポートチャネルを有効にすることができます。vPC はこの構成ではサポートされません。
- FCoE エンドツーエンドの設計では、 FCoE ポートチャネルが推奨されます。

SAN ブート：

- FlexPod ソリューションは、 iSCSI 、 FC 、または FCoE プロトコルを使用する SAN ブートアーキテクチャを中心に設計されています。SAN からのブートテクノロジを使用すると、データセンターインフラの柔軟な構成が可能になり、各インフラコンポーネントで使用できる豊富な機能を使用できます。SAN からのブートは最も効率的な構成ですが、ローカルサーバストレージからのブートは有効でサポートされている構成です。
- FC-NVMe での SAN ブートはサポートされていません。

その他の要件

FlexPod アーキテクチャには、相互運用性とサポート関連の次の要件が追加で含まれています。

- すべてのハードウェアコンポーネントとソフトウェアコンポーネントがネットアップに記載され、サポートされている必要があります "IMT"、 "Cisco UCS ハードウェアおよびソフトウェア互換性リスト"、および Cisco UCS Hardware and Software Interoperability Matrix Tool を参照してください。
- 次の項目を含むすべての機器について、有効なサポート契約が必要です。
  - シスコ機器の Smart Net Total Care （ SmartNet ）サポート
  - ネットアップ機器に対する SupportEdge Advisor または SupportEdge Premium のサポート

詳細については、ネットアップを参照してください "IMT"。

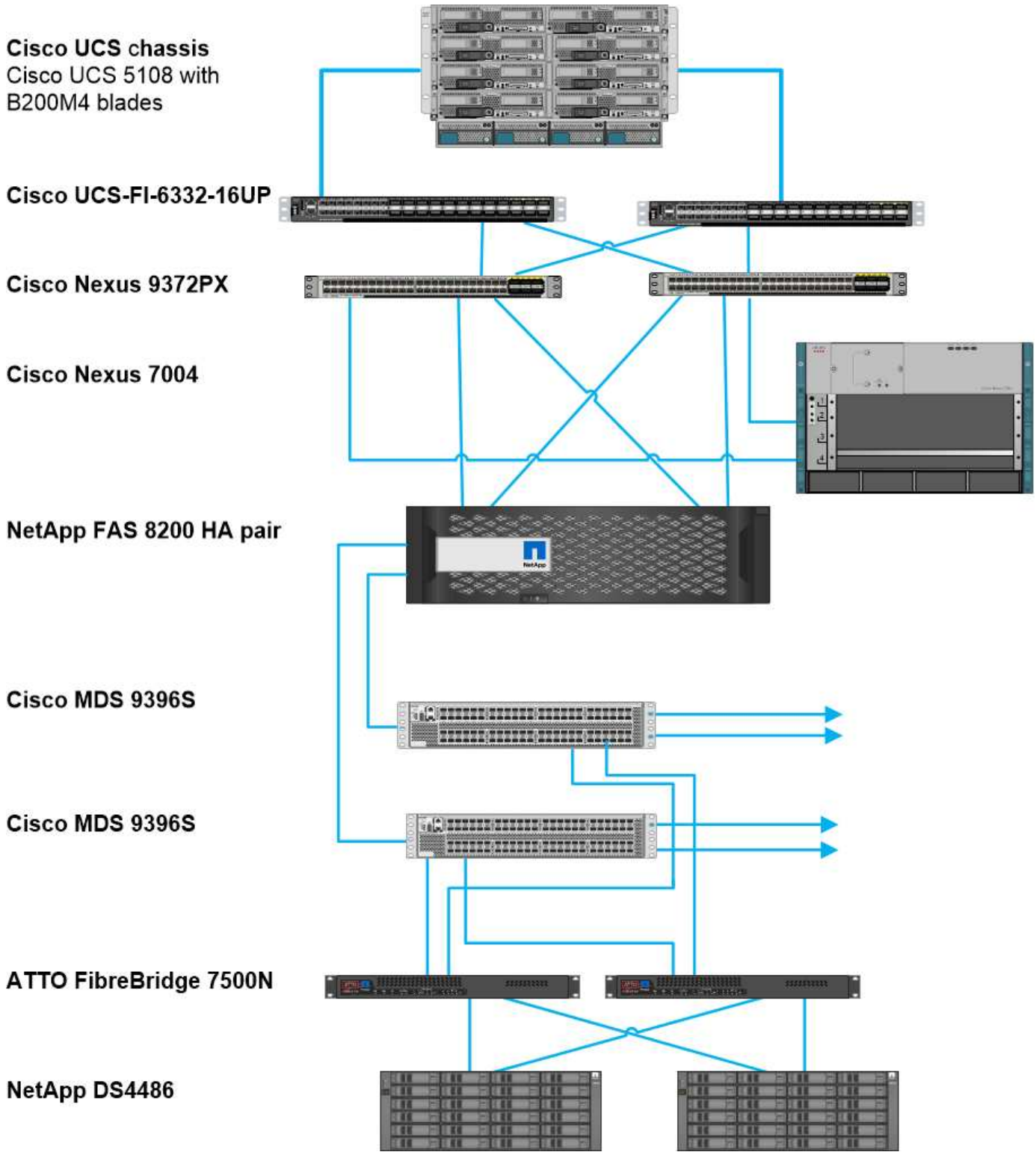
オプション機能

ネットアップは、 FlexPod データセンターのアーキテクチャをさらに強化するために、いくつかのオプションコンポーネントをサポートしてオプションコンポーネントについては、以降のサブセクションで説明します。

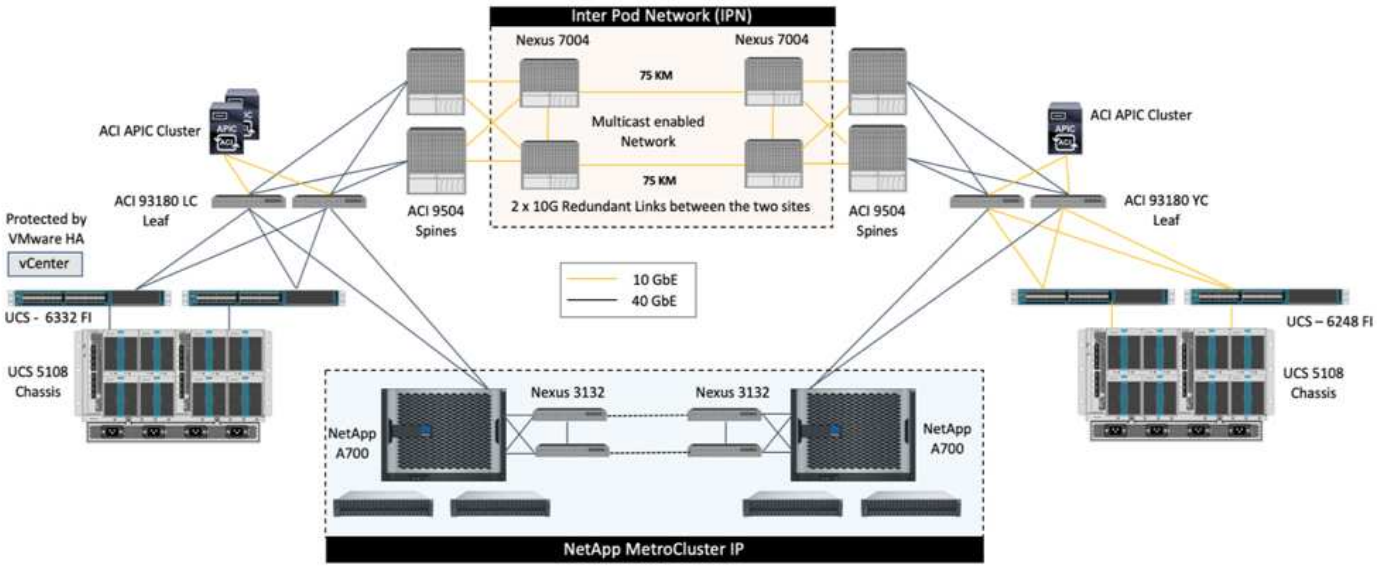
MetroCluster

FlexPod は、 2 ノードまたは 4 ノードのどちらのクラスタ構成でも、継続的可用性を実現する NetApp MetroCluster ソフトウェアのどちらかのバリエーションをサポートします。MetroCluster は、重要なワークロード向けに同期レプリケーションを提供します。Cisco スイッチに接続されたデュアルサイト構成が必要です。サイト間でサポートされる最大距離は、 MetroCluster FC の場合は約 186 マイル（ 300km ）、MetroCluster IP の場合は約 435 マイル（ 700km ）に増加します。次の図は、 FlexPod Datacenter with NetApp MetroCluster Architecture と FlexPod Datacenter with NetApp MetroCluster IP Architecture をそれぞれ示しています。

次の図は、ネットアップの MetroCluster アーキテクチャを備えた FlexPod データセンターを示しています。

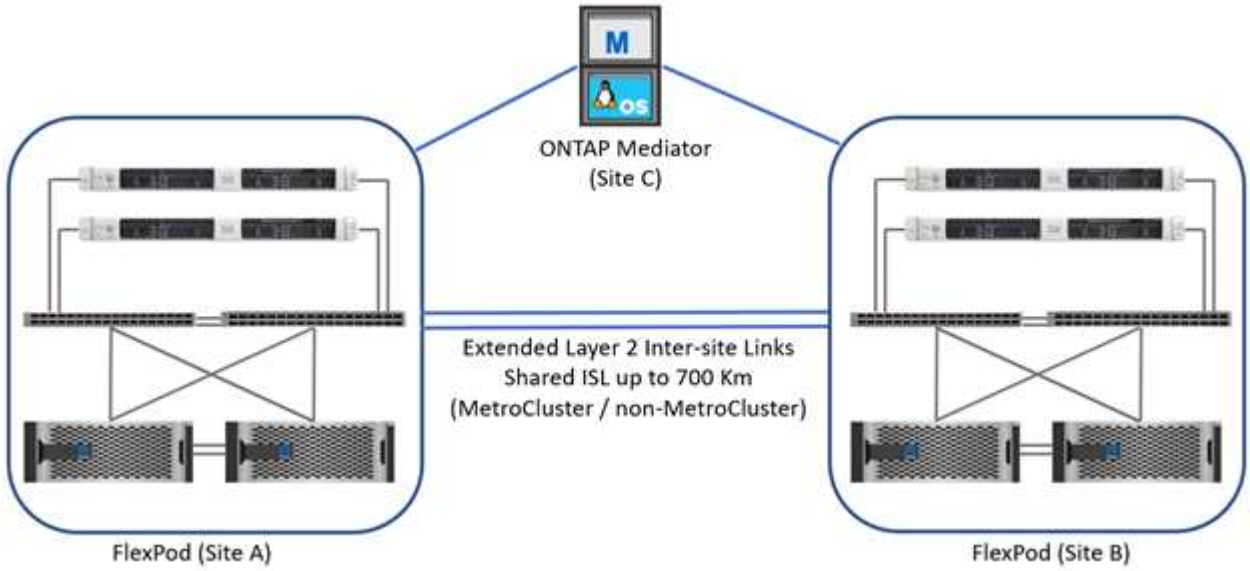


次の図は、ネットアップの MetroCluster IP アーキテクチャを備えた FlexPod データセンターを示しています。



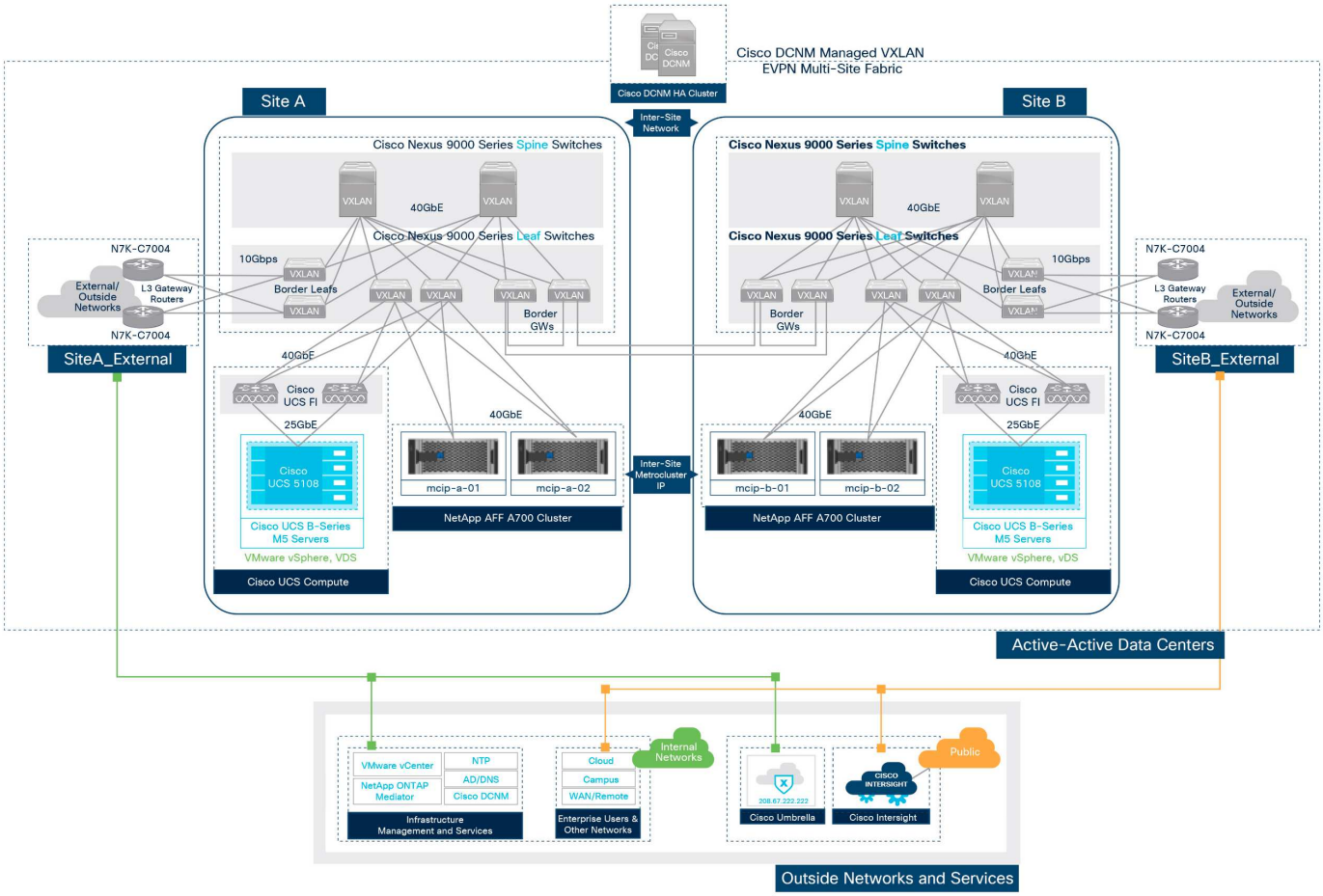
ONTAP 9.8 以降では、 MetroCluster メディエーターを第 3 のサイトに導入して解決策 IP ONTAP を監視し、サイト障害の発生時に自動計画外スイッチオーバーを実施できます。

拡張レイヤ 2 サイト間接続を使用する FlexPod MetroCluster IP 解決策環境では、次の図に示す要件を満たしている場合、 ISL を共有し、 MetroCluster スイッチを準拠 FlexPod IP スイッチとして使用することで、コストを削減できます。 この図は、解決策 IP FlexPod MetroCluster と ISL 共有および準拠スイッチを示しています。

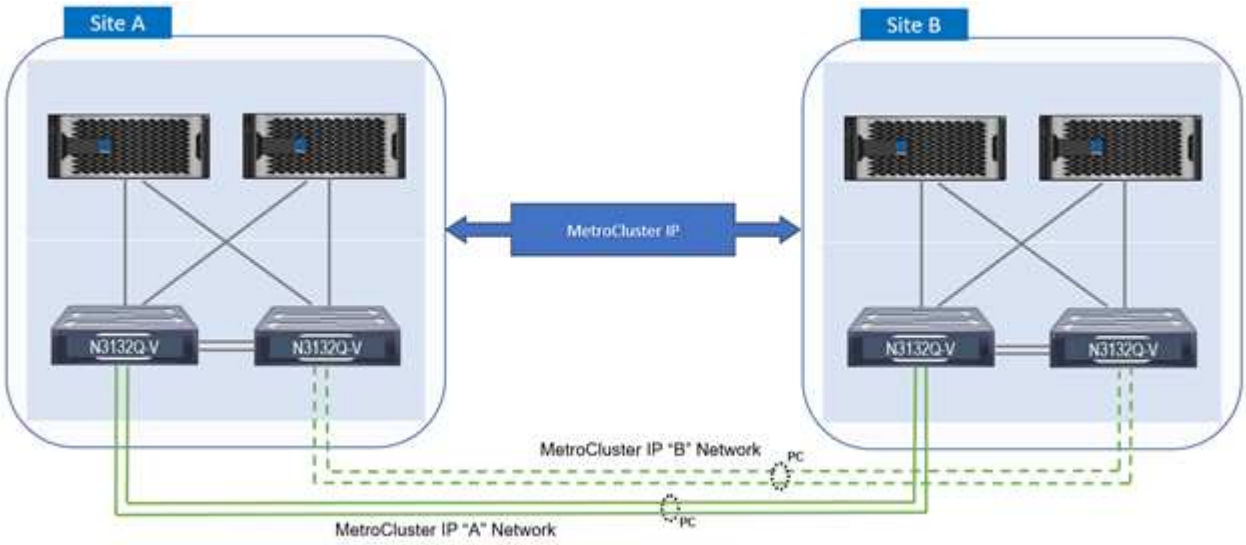


次の 2 つの図は、 VXLAN マルチサイトファブリックと、解決策 IP FlexPod MetroCluster と VXLAN マルチサイトファブリック導入のための MetroCluster IP ストレージファブリックを示しています。

- FlexPod MetroCluster IP 解決策用の VXLAN マルチサイトファブリック



- FlexPod MetroCluster IP 解決策用の MetroCluster IP ストレージファブリック



エンドツーエンドの **FC-NVMe**

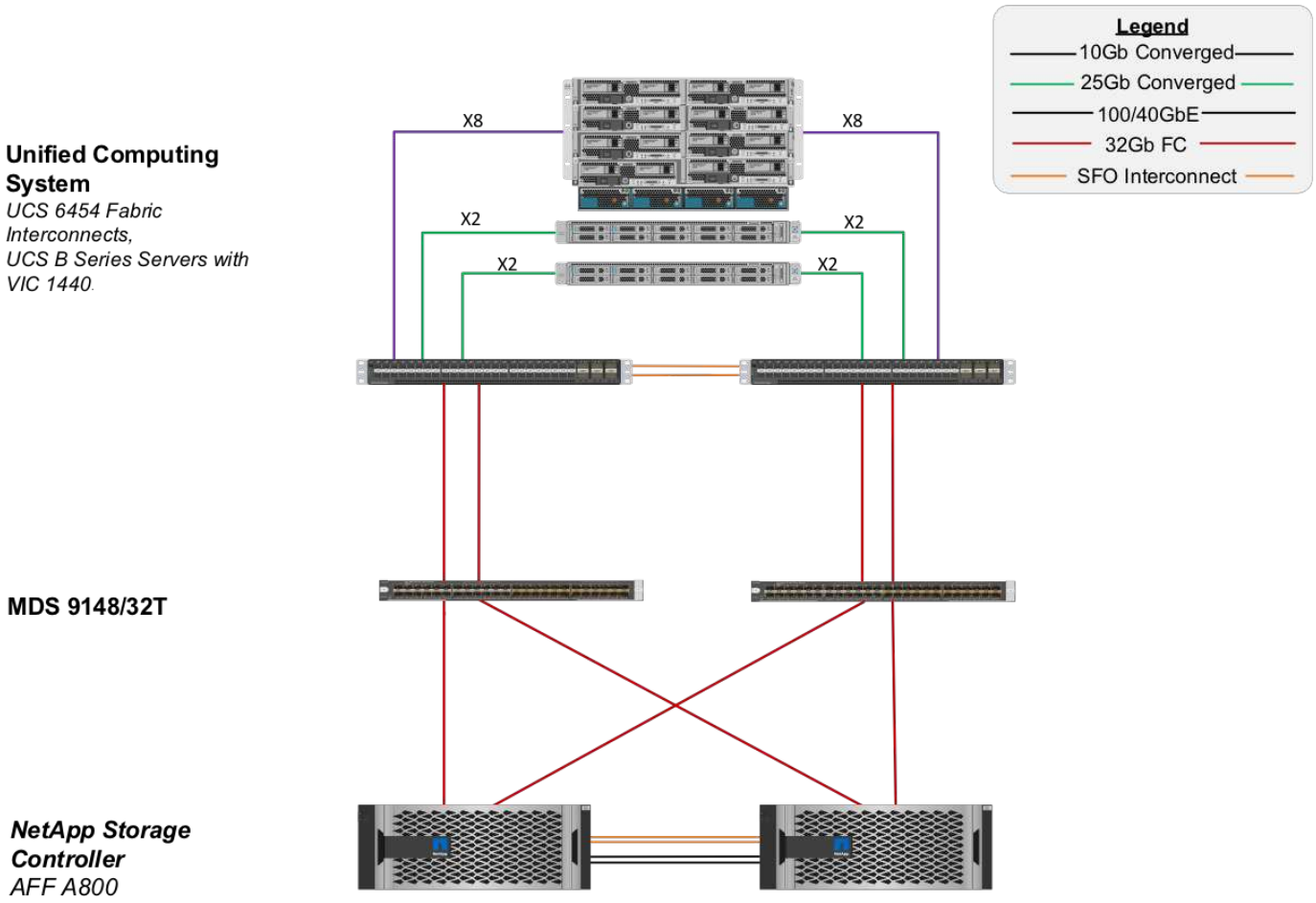
エンドツーエンドの FC-NVMe は、リアルタイムアプリケーション向けにお客様の既存の SAN インフラストラクチャをシームレスに拡張しながら、同時に、遅延を低減しながら IOPS とスループットを向上させます。

既存の 32G FC SAN 転送を使用して、 NVMe と SCSI の両方のワークロードを同時に転送できます。

次の図に、 FlexPod MDS を使用した FC の データセンターを示します。

FlexPod の構成とパフォーマンスのメリットの詳細については、を参照してください "ホワイトペーパー『 Introducing End-to-End NVMe for FlexPod 』"

ONTAP 実装の詳細については、を参照してください "TR-4684 『 Implementing and Configuring Modern SANs with NVMe 』"。



Cisco MDS を介した **FC SAN** ブート

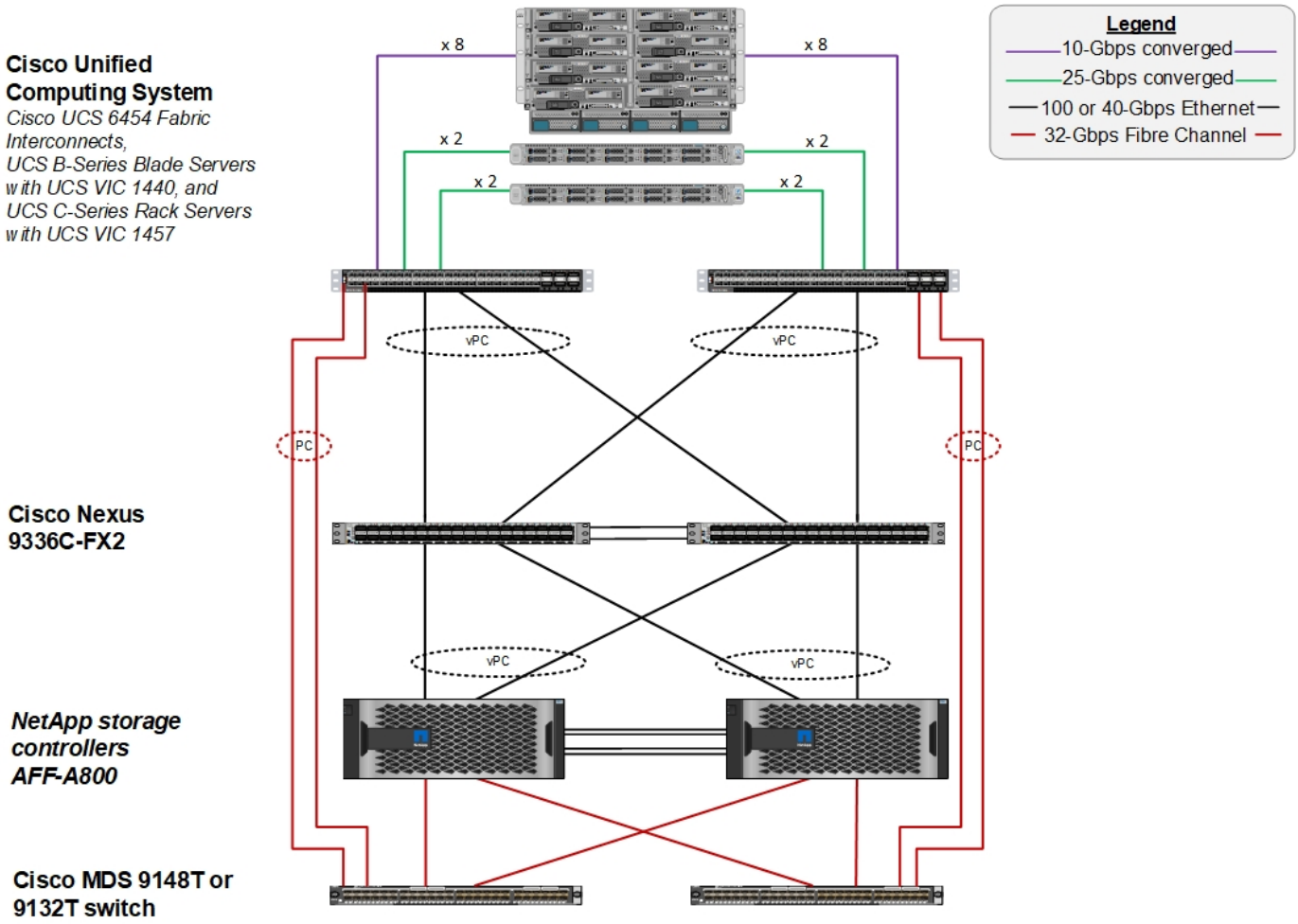
専用の SAN ネットワークを使用して拡張性を向上させるために、 FlexPod は Cisco MDS スイッチ経由で FC をサポートし、 Cisco Nexus 93108TC-FX などの FC スイッチをサポートしています。Cisco MDS の FC SAN ブートオプションには、次のライセンスおよびハードウェア要件があります。

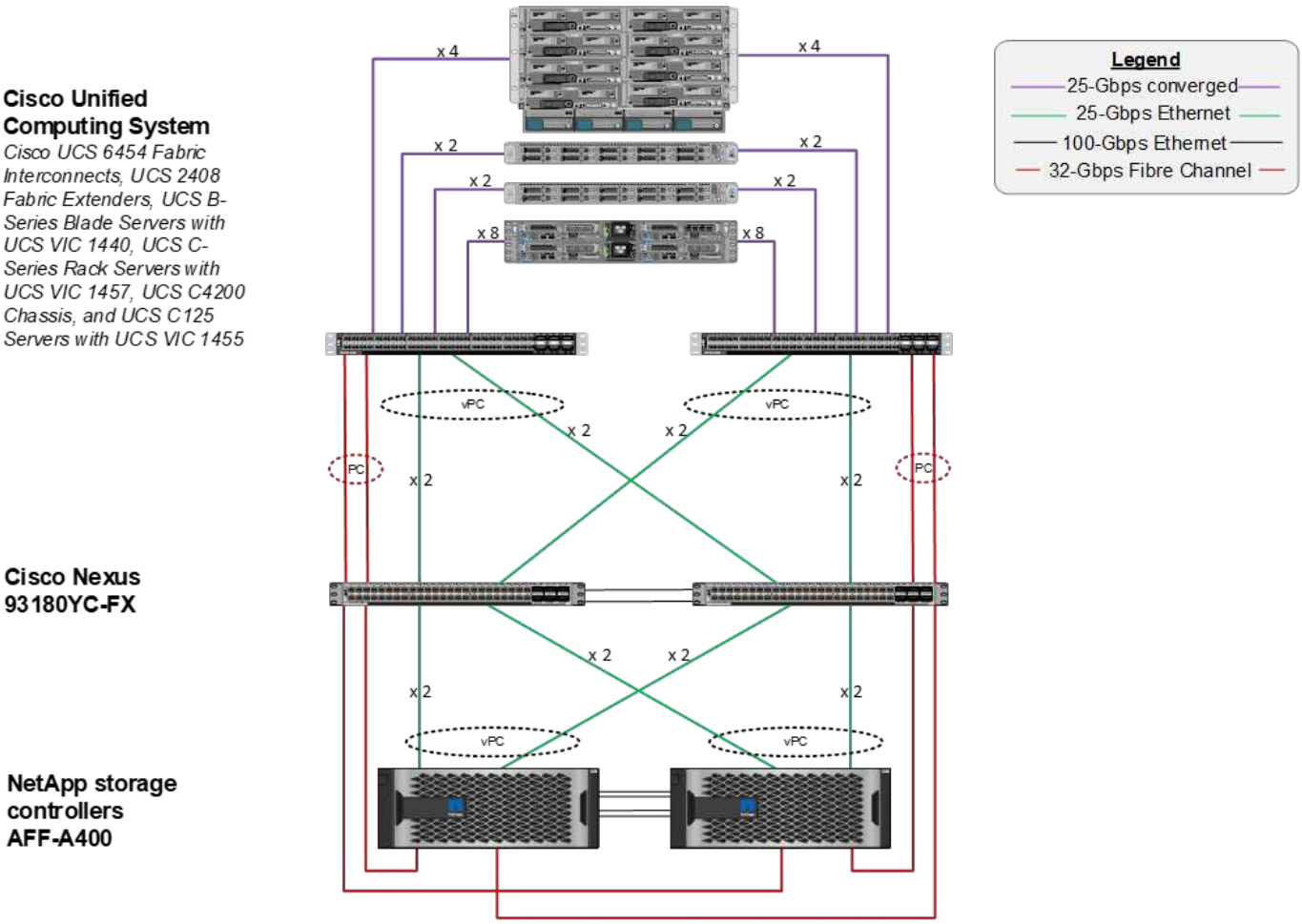
- ネットアップストレージコントローラごとに少なくとも 2 つの FC ポート。 SAN ファブリックごとに 1 つのポート
- 各ネットアップストレージコントローラに FC ライセンスが必要です
- ネットアップでサポートされている Cisco MDS スイッチおよびファームウェアのバージョン "IMT"

MDS ベースの設計の詳細については、 CVD を参照してください "『 FlexPod Datacenter with VMware vSphere 6.7U1 Fibre Channel and iSCSI Deployment Guide 』を参照してください"。

次の図は、 MDS 接続を備えた FlexPod Datacenter for FC と、 Cisco Nexus 93180YC-FX を使用した

FlexPod Datacenter for FC のそれぞれの例を示しています。





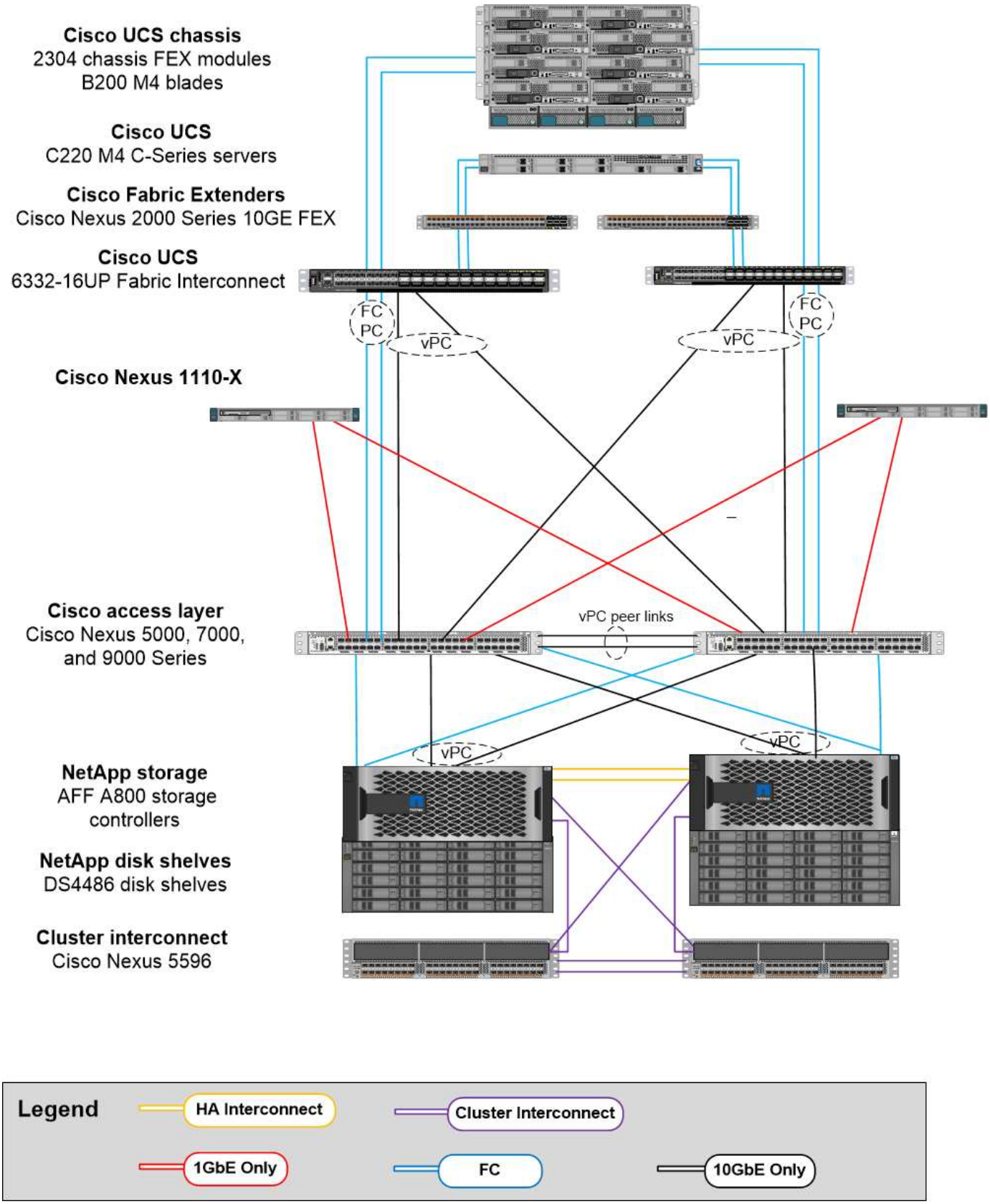
Cisco Nexus を使用した **FC SAN** ブート

従来の FC SAN ブートオプションには、ライセンスとハードウェアに関する次の要件があります。

- Cisco Nexus 5000 シリーズスイッチで FC ゾーニングを実行する場合は、 Cisco Nexus 5000 シリーズスイッチのストレージプロトコルサービスパッケージライセンス（ FC_FEATURES_PKG ）が必要です。
- Cisco Nexus 5000 シリーズスイッチで FC ゾーニングを実行する場合は、ファブリックインターコネクトと Cisco Nexus 5000 シリーズスイッチの間に SAN リンクが必要です。さらに冗長性を確保するため、リンク間に SAN ポートチャネルを配置することを推奨します。
- Cisco Nexus 5010 、 5020 、および 5548P スイッチには、 Cisco UCS ファブリックインターコネクトとネットアップストレージコントローラとの接続用に、個別の FC またはユニバーサルポート（ UP ）モジュールが必要です。
- Cisco Nexus 93180YC-FX で FC を有効にするには、 FC 機能のライセンスが必要です。
- ネットアップストレージコントローラごとに、接続用に少なくとも 2 つの 8 / 16 / 32Gb FC ポートが必要です。
- ネットアップストレージコントローラに FC ライセンスが必要です。

> Cisco Nexus 7000 または 9000 ファミリーのスイッチを使用すると、ファブリックインターコネクトで FC ゾーニングを実行しないかぎり、従来の FC を使用することはできません。この場合、スイッチへの SAN アップリンクはサポートされません。

次の図に、 FC 接続の構成を示します。



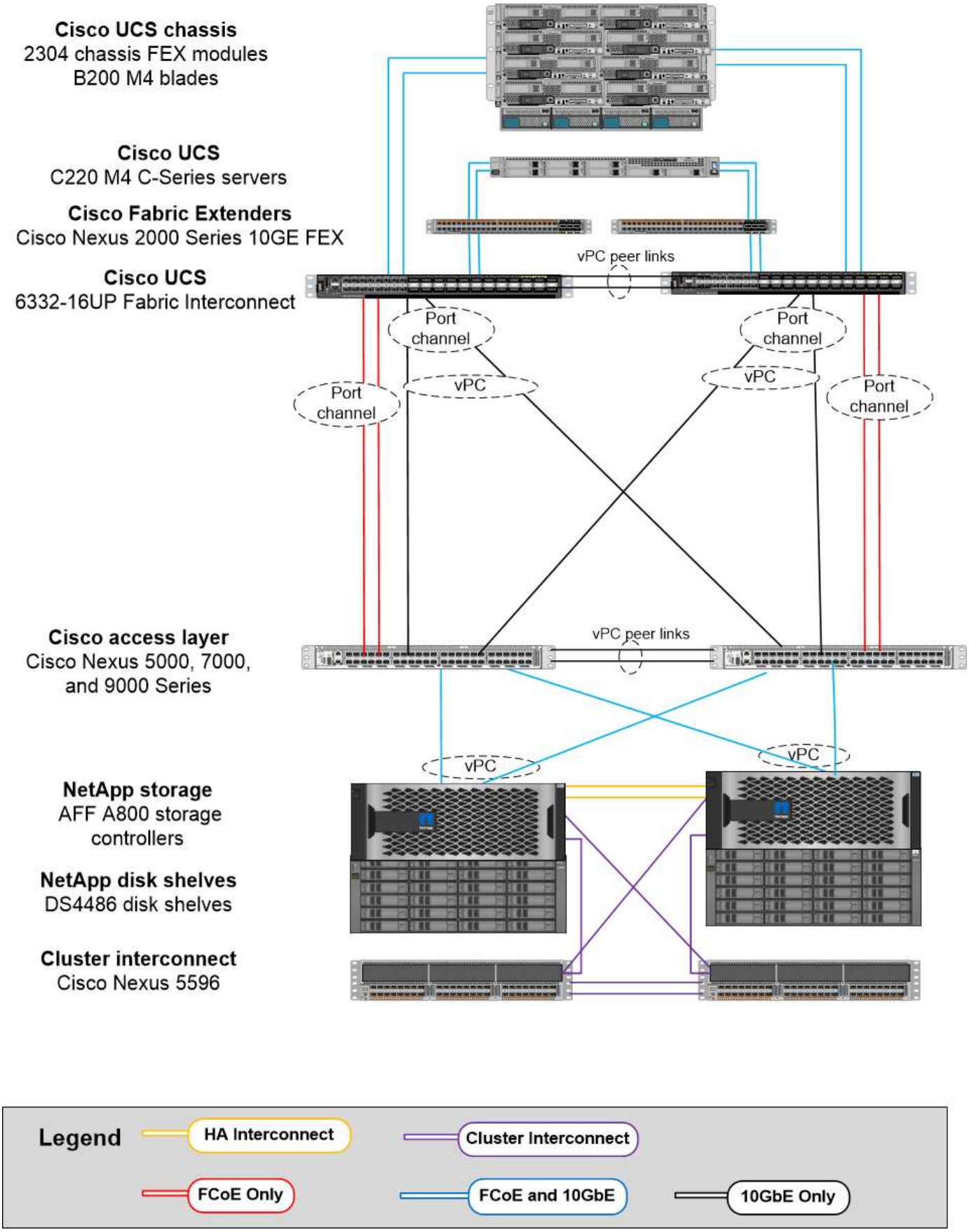
FCoE SAN ブートオプション

FCoE SAN ブートオプションには、ライセンスとハードウェアに関する次の要件があります。

- スイッチで FC ゾーニングを実行する場合は、 Cisco Nexus 5000 または 7000 シリーズスイッチ「（ FC_FEATURES_PKG ）」のストレージプロトコルサービスパッケージライセンスが必要です。
- スイッチで FC ゾーニングを実行する場合は、ファブリックインターコネクトと Cisco Nexus 5000 または 7000 シリーズスイッチ間に FCoE アップリンクが必要です。さらに冗長性を確保するために、リンク間で FCoE ポートチャネルを使用することも推奨されます。
- オンボードのユニファイドターゲットアダプタ 2 （ UTA2 ）ポートがないかぎり、各ネットアップストレージコントローラに、 FCoE 接続用のデュアルポートユニファイドターゲットアダプタ（ UTA ）アドオンカードが少なくとも 1 枚必要です。
- このオプションを使用するには、ネットアップストレージコントローラに FC ライセンスが必要です。
- Cisco Nexus 7000 シリーズスイッチを使用し、 FC ゾーニングをスイッチで実行する場合は、 FCoE に対応したラインカードが必要です。

> Cisco Nexus 9000 シリーズスイッチを使用すると、ファブリックインターコネクトで FC ゾーニングを実行し、アプライアンスポートでファブリックインターコネクトにストレージを接続していないかぎり、 FCoE を使用できなくなります。この場合、スイッチへの FCoE アップリンクはサポートされません。

次の図に、 FCoE ブートのシナリオを示します。

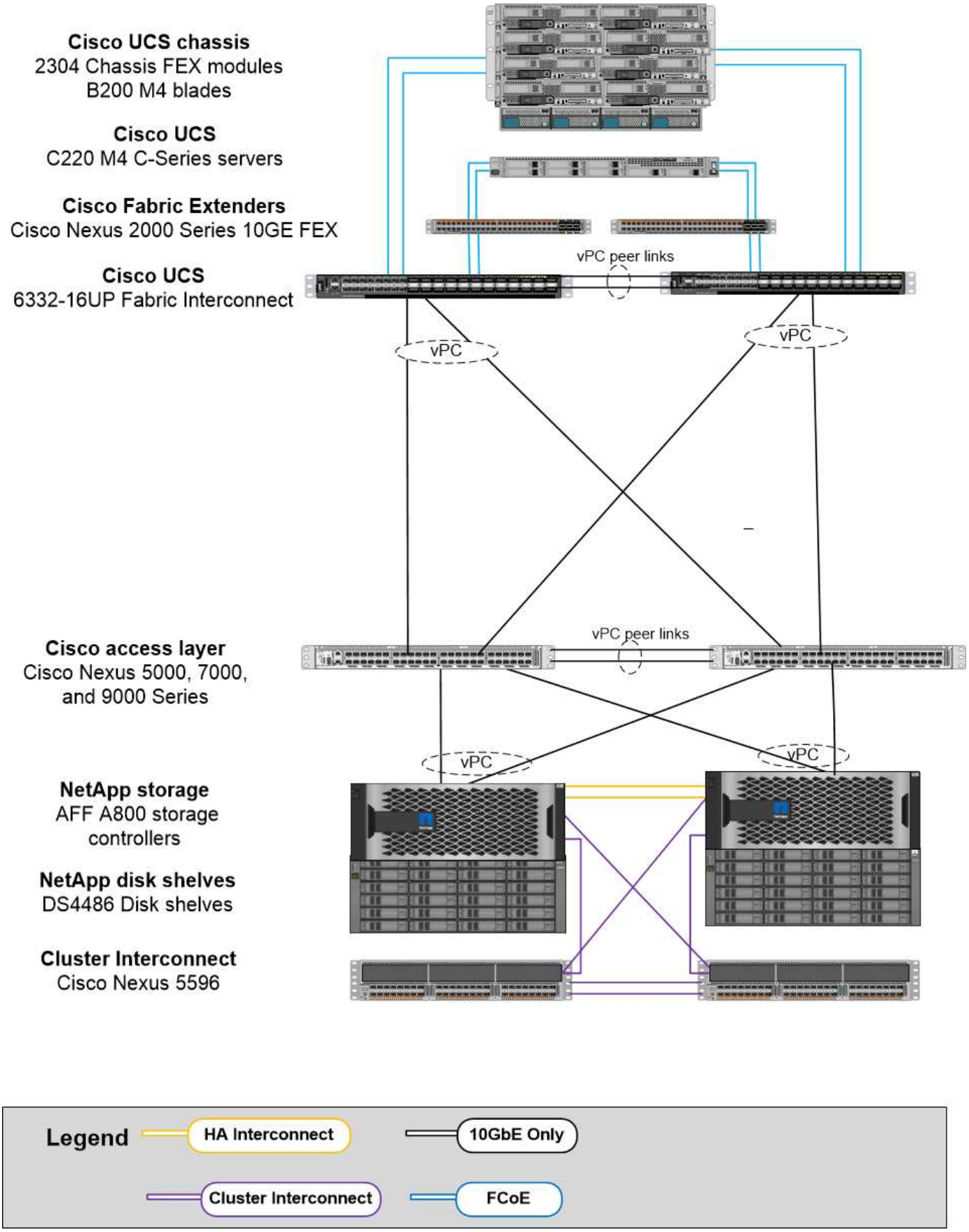

Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
vPC
Port channel
vPC
Port channel
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

iSCSI ブートオプション

iSCSI ブートオプションには、ライセンスとハードウェアに関する次の要件があります。

- ネットアップストレージコントローラに iSCSI ライセンスが必要です。
- iSCSI ブートに対応した Cisco UCS サーバのアダプタが必要です。
- ネットアップストレージコントローラには、 2 ポート 10Gbps イーサネットアダプタが必要です。

次の図は、 iSCSI でブートされるイーサネットのみの構成を示しています。


Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage
controllers
NetApp disk shelves
DS4486 Disk shelves
Cluster Interconnect
Cisco Nexus 5596
Legend
HA Interconnect
10GbE Only
Cluster Interconnect
FCoE

Cisco UCS はネットアップストレージと直接接続

NetApp AFF コントローラと FAS コントローラは、アップストリームの SAN スイッチを使用せずに、 Cisco UCS ファブリックインターコネクトに直接接続できます。

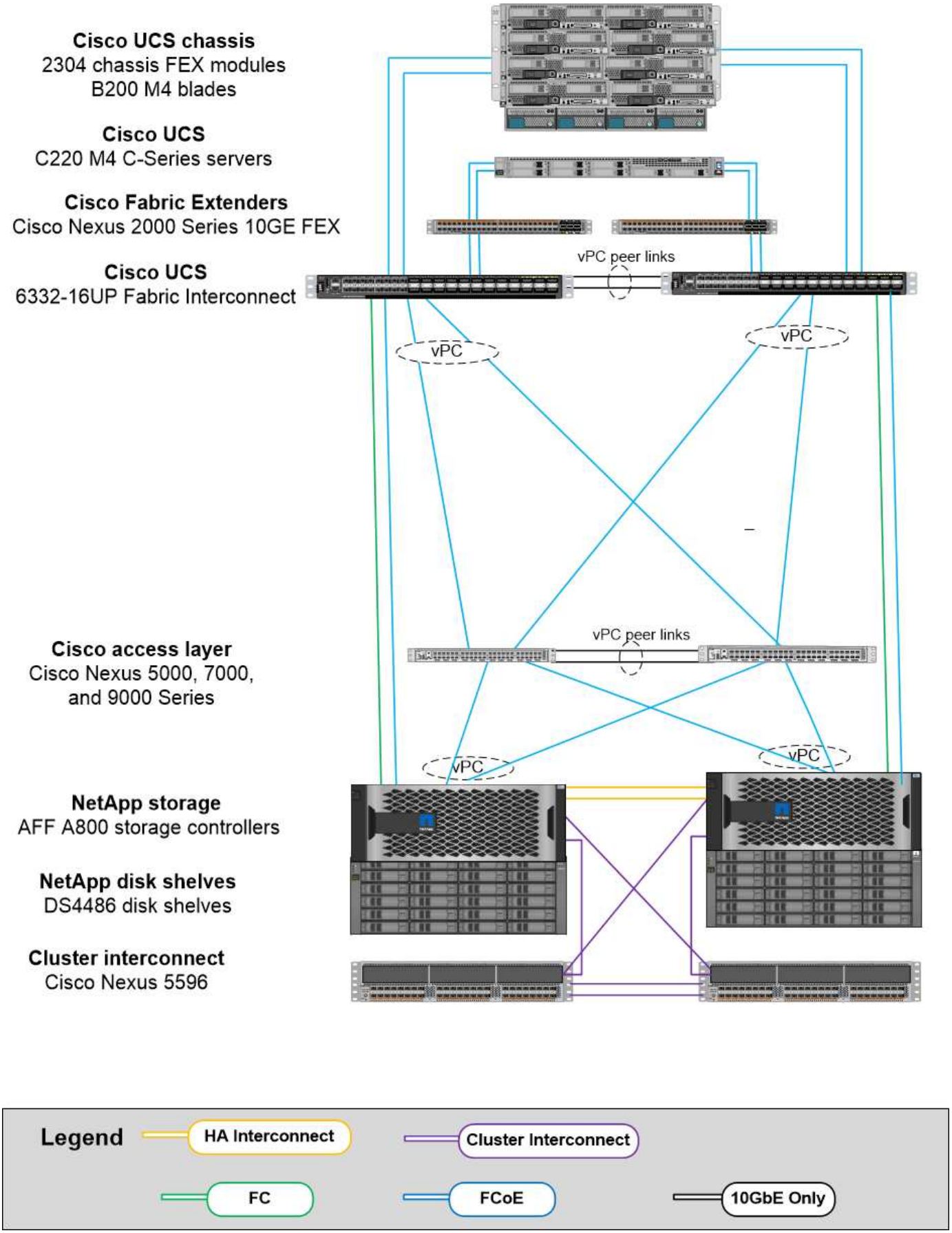
ネットアップストレージに直接接続する場合は、 Cisco UCS の次の 4 つのポートタイプを使用できます。

- * ストレージ FC ポート。 * ネットアップストレージの FC ポートに直接接続します。
- * ストレージ FCoE ポート。 * ネットアップストレージの FCoE ポートにこのポートを直接接続します。
- * アプライアンス・ポート。 * ネットアップ・ストレージ上の 10GbE ポートに、このポートを直接接続します。
- * ユニファイドストレージポート。 * このポートを NetApp UTA に直接接続できます。

ライセンスとハードウェアの要件は次のとおりです。

- ネットアップストレージコントローラにはプロトコルライセンスが必要です。
- サーバには Cisco UCS アダプタ（イニシエータ）が必要です。サポートされている Cisco UCS アダプタの一覧については、ネットアップを参照してください "IMT"。
- ネットアップストレージコントローラにはターゲットアダプタが必要です。

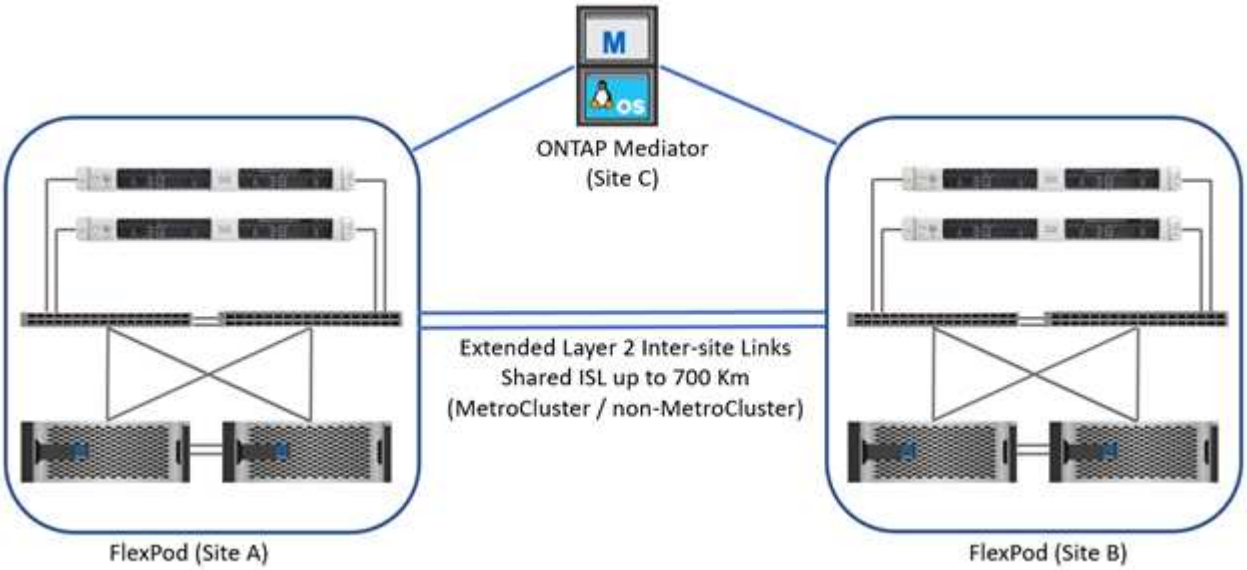
次の図に、 FC 直接接続構成を示します。


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

• 注：*

- Cisco UCS は FC スイッチングモードで設定されます。
- ターゲットからファブリックインターコネクトへの FCoE ポートは、 FCoE ストレージポートとして構成されます。
- ターゲットからファブリックインターコネクトへの FC ポートは、 FC ストレージポートとして構成されます。

次の図に、 iSCSI / ユニファイド IP の直接接続構成を示します。



- 注： *
- Cisco UCS はイーサネットスイッチングモードで設定されます。
- ターゲットからファブリックインターコネクトへの iSCSI ポートは、 iSCSI データ用のイーサネットストレージポートとして構成されます。
- ターゲットからファブリックインターコネクトへのイーサネットポートは、 CIFS / NFS データ用のイーサネットストレージポートとして構成されます。

シスコのコンポーネント

シスコは、解決策の設計とアーキテクチャに大きく貢献し、 FlexPod のコンピューティングレイヤとネットワーキングレイヤの両方をカバーしています。ここでは、 FlexPod で使用できる Cisco UCS および Cisco Nexus オプションについて説明します。FlexPod は、 Cisco UCS B シリーズと C シリーズの両方のサーバをサポートしています。

Cisco UCS ファブリックインターコネクトのオプション

FlexPod アーキテクチャには、冗長ファブリックインターコネクトが必要です。ファブリックインターコネクトのペアに複数の Cisco UCS シャーシを追加する場合、環境内のシャーシの最大数は、アーキテクチャとポートの両方の制限によって決定されることに注意してください。

次の表に、基本ファブリックインターコネクトのパーツ番号を示します。電源装置ユニット（ PSU ）、 SFP+ 、 QSFP+ 、拡張モジュールは含まれません。その他のファブリックインターコネクトもサポートされています。を参照してください "NetApp IMT" をクリックしてください。

Cisco UCS ファブリックインターコネクト	パーツ番号	技術仕様
Cisco UCS 6332UP	UCS-FI-6332 アップ	"Cisco UCS 6332 ファブリックインターコネクト"
Cisco UCS 6454	UCS-FI-6454-U	"Cisco UCS 6454 ファブリックインターコネクト"

Cisco UCS 6454

Cisco UCS 6454 シリーズは、ラインレート、低遅延、ロスレスの 10/25/40/100GbE イーサネットおよび FCoE 接続、およびイーサネットまたは FC の動作が可能なユニファイドポートを提供します。44 個の 10 / 25Gbps ポートは、 10Gbps または 25Gbps の統合イーサネットとして動作できます。このうちの 8 つのユニファイドポートは、 FC 用に 8 / 16 / 32Gbps で動作可能です。4 つのポートは従来の接続では 1/10/25Gbps で動作し、 6 つの QSFP ポートは 40/100Gbps アップリンクポートまたはブレークアウトポートとして機能します。100Gbps アダプタをサポートするネットアップストレージコントローラを使用して、 100Gbps エンドツーエンドのネットワーク接続を確立できます。アダプタおよびプラットフォームのサポートについては、を参照してください "NetApp Hardware Universe の略"。

ポートの詳細については、を参照してください "Cisco UCS 6454 ファブリックインターコネクト" データシート

100Gb QSFP データモジュールの技術仕様については、を参照してください "Cisco 100GBASE QSFP モジュールデータシート"。

Cisco UCS B シリーズシャーシオプション

Cisco UCS B シリーズブレードを使用するには、 Cisco UCS B シリーズシャーシが必要です。次の表では、Cisco UCS BSeries シャーシオプションについて説明します。

Cisco UCS B シリーズシャーシ	パーツ番号	技術仕様
Cisco UCS 5108	N20-C6508	"Cisco UCS 5100 シリーズブレードサーバシャーシ"

各 Cisco UCS 5108 ブレードシャーシには、ファブリックインターコネクトへの冗長接続を提供するために、2 つの Cisco UCS 2200/2300/2400 シリーズ IOM が必要です。

Cisco UCS B シリーズブレードサーバのオプション

Cisco UCS B シリーズブレードサーバには、さまざまな CPU 、メモリ、および I/O オプションを備えたハーフ幅およびフル幅の各種タイプが用意されています。次の表に示す部品番号は、ベースサーバー用です。CPU 、メモリ、ドライブ、メザニンアダプタカードは含まれません。FlexPod アーキテクチャでは、複数の構成オプションを使用でき、サポートされています。

Cisco UCS B シリーズブレード	パーツ番号	技術仕様
Cisco UCS B200 M6	UCSB-B2006-M6	"Cisco UCS B200 M6 ブレードサーバ"

旧世代の Cisco UCS B シリーズブレードがでサポートされていれば、 FlexPod アーキテクチャで使用できます "Cisco UCS ハードウェアおよびソフトウェア互換性リスト"。Cisco UCS B シリーズブレードサーバには、有効な SmartNet サポート契約も必要です。

Cisco UCS X シリーズシャーシオプション

Cisco UCS X シリーズのコンピューティングノードを使用するには、 Cisco UCS X シリーズシャーシが必要です。次の表では、 Cisco UCS X シリーズシャーシオプションについて説明します。

Cisco UCS X シリーズブレード	パーツ番号	技術仕様
Cisco UCS 9508 M6	UCSX-9508	"Cisco UCX9508 X シリーズシャーシ"

ファブリックインターコネクトへの冗長接続を提供するには、各 Cisco UCS 9508 シャーシに 2 つの Cisco UCS 9108 Intelligent Fabric Module （ IFM ）が必要です。

Cisco UCS X シリーズデバイスのオプション

Cisco UCS X シリーズのコンピューティングノードには、 CPU 、メモリ、 I/O の各種オプションが用意されています。次の表に、ベースノードのパーツ番号を示します。CPU 、メモリ、ドライブ、メザニンアダプタカードは含まれません。FlexPod アーキテクチャでは、複数の構成オプションを使用でき、サポートされています。

Cisco UCS X シリーズコンピューティングノード	パーツ番号	技術仕様
Cisco UCS X210c M6	UCSX-210C - M6	"Cisco UCS X210c M6 コンピューティングノード"

Cisco UCS C シリーズラックサーバのオプション

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 2 種類があり、さまざまな CPU 、メモリ、 I/O オプションが用意されています。下の 2 番目の表に記載されている部品番号は、ベースサーバー用です。CPU 、メモリ、ドライブ、 Peripheral Component Interconnect Express （ PCIe ）カード、または Cisco Fabric Extender は含まれません。FlexPod アーキテクチャでは、複数の構成オプションを使用でき、サポートされています。

次の表に、 Cisco UCS C シリーズラックサーバのオプションを示します。

Cisco UCS C シリーズラックサーバ	パーツ番号	技術仕様
Cisco UCS C220 M6	UCSC-C220 - M6	"Cisco UCS C220 M6 ラックサーバ"
Cisco UCS C225 M6	UCSC-C225-M6	"Cisco UCS C225 M6 ラックサーバ"
Cisco UCS C240 M6	UCSC-C240 -M6	"Cisco UCS C240 M6 ラックサーバ"
Cisco UCS C245 M6	UCSC-C245-M6	"Cisco UCS C245 M6 ラックサーバ"

旧世代の Cisco UCS C シリーズサーバは、でサポートされていれば、 FlexPod アーキテクチャで使用できます "Cisco UCS ハードウェアおよびソフトウェア互換性リスト"。Cisco UCS C シリーズサーバには、有効な SmartNet サポート契約も必要です。

Cisco Nexus 5000 シリーズスイッチのオプション

FlexPod アーキテクチャには、冗長構成の Cisco Nexus 5000 、 7000 、または 9000 シリーズスイッチが必要です。次の表に示す部品番号は、 Cisco Nexus 5000 シリーズシャーシのものです。 SFP モジュール、アドオン FC 、イーサネットモジュールは含まれていません。

Cisco Nexus 5000 シリーズスイッチ	パーツ番号	技術仕様
Cisco Nexus 56128P	N5K-C56128P	"Cisco Nexus 5600 プラットフォームスイッチ"
Cisco Nexus 5672UP.16G	N5K-C5672UP.16G	
Cisco Nexus 5596UP	N5k-c5596UP FA	"Cisco Nexus 5548 および 5596 スイッチ"
Cisco Nexus 5548UP	N5K-C5548UP - FA	

Cisco Nexus 7000 シリーズスイッチオプション

FlexPod アーキテクチャには、冗長構成の Cisco Nexus 5000 、 7000 、または 9000 シリーズスイッチが必要です。次の表に示す部品番号は、 Cisco Nexus 7000 シリーズシャーシのものです。 SFP モジュール、ラインカード、電源装置は含まれませんが、ファントレイも含まれます。

Cisco Nexus 7000 シリーズスイッチ	パーツ番号	技術仕様
Cisco Nexus 7004	N7K-C7004	"Cisco Nexus 7000 4 スロットスイッチ"
Cisco Nexus 7009	N7K-C7009	"Cisco Nexus 7000 9 スロットスイッチ"
Cisco Nexus 7702	N7K-C7702	"Cisco Nexus 7700 2 スロットスイッチ"
Cisco Nexus 7706	N77-C7706	"Cisco Nexus 7700 6 スロットスイッチ"

Cisco Nexus 9000 シリーズのスイッチオプション

FlexPod アーキテクチャには、冗長構成の Cisco Nexus 5000 、 7000 、または 9000 シリーズスイッチが必要です。次の表に示す部品番号は、 Cisco Nexus 9000 シリーズシャーシのもので、 SFP モジュールやイーサネットモジュールは含まれていません。

Cisco Nexus 9000 シリーズスイッチ	パーツ番号	技術仕様
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Cisco Nexus 9300 シリーズスイッチ"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Cisco Nexus 9336PQ ACI スパイン	N9K-C9336PQ	
Cisco Nexus 9332PQ の場合	N9K-C9332PQ	
Cisco Nexus 9336C-FX2	N9K-C9336C-FX2	

Cisco Nexus 9000 シリーズスイッチ	パーツ番号	技術仕様
Cisco Nexus 92304QC	N9K-C92304QC	"Cisco Nexus 9200 シリーズスイッチ"
Cisco Nexus 9236C	N9K-9236C	

一部の Cisco Nexus 9000 シリーズスイッチには、他のモデルもあります。これらのバリアントは、 FlexPod 解決策の一部としてサポートされています。Cisco Nexus 9000 シリーズスイッチの一覧については、を参照してください "Cisco Nexus 9000 シリーズスイッチ" シスコの Web サイトで入手できます。

Cisco APIC オプション

Cisco ACI を導入する際には、の項目に加えて、 3 つの Cisco APIC を設定する必要があります "Cisco Nexus 9000 シリーズスイッチ"。Cisco APIC のサイズの詳細については、を参照してください "Cisco Application Centric Infrastructure のデータシート。"

APIC 製品仕様の詳細については、の表 1 〜 3 を参照してください "Cisco Application Policy Infrastructure Controller データシート"。

Cisco Nexus ファブリックエクステンダのオプション

C シリーズサーバを使用する大規模な FlexPod アーキテクチャでは、冗長構成の Cisco Nexus 2000 シリーズラックマウント FEX が推奨されます。次の表に、 Cisco Nexus FEX のいくつかのオプションを示します。代替 FEX モデルもサポートされています。詳細については、を参照してください "Cisco UCS ハードウェアおよびソフトウェア互換性リスト"。

Cisco Nexus ラックマウント **FEX**	パーツ番号	技術仕様
Cisco Nexus 2232PP	N2K-C2232PP	"Cisco Nexus 2000 シリーズファブリックエクステンダ"
Cisco Nexus 2232TM-E	N2K-C2232TM-E です	
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Cisco Nexus 2300 プラットフォームファブリックエクステンダ"
Cisco Nexus 2348TQCisco Nexus 2348TQ-E	N2K-C2348TQN2K-C2348TQ-E	

Cisco MDS のオプション

Cisco MDS 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。FC SAN に Cisco MDS スイッチを実装する場合、冗長 SAN スイッチファブリックが必要です。次の表に、サポートされている Cisco MDS スイッチのサブセットのパーツ番号と詳細を示します。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。

Cisco MDS 9000 シリーズスイッチ	パーツ番号	説明
Cisco MDS 9148T	DS-C9148T-24IK	"Cisco MDS 9100 シリーズスイッチ"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Cisco MDS 9300 シリーズスイッチ"

シスコのソフトウェアライセンスオプション

Cisco Nexus スイッチでストレージプロトコルを有効にするには、ライセンスが必要です。Cisco Nexus 5000 および 7000 シリーズのスイッチでは、いずれのスイッチも SAN ブート実装で FC プロトコルまたは FCoE プロトコルを有効にするためにストレージサービスライセンスが必要です。Cisco Nexus 9000 シリーズスイッチでは、現在 FC と FCoE はサポートされていません。

これらのライセンスに必要なライセンスと製品番号は、 FlexPod 解決策の各コンポーネントで選択するオプションによって異なります。たとえば、ソフトウェアライセンスの製品番号は、ポートの数や、選択する Cisco Nexus 5000 または 7000 シリーズスイッチによって異なります。正確なパーツ番号については、営業担当者にお問い合わせください。次の表に、シスコのソフトウェアライセンスオプションを示します。

Cisco ソフトウェアライセンス	パーツ番号	ライセンス情報
Cisco Nexus 5500 ストレージライセンス、 8 、 48 、 96 ポート	N55-8P-SSK9/ N55-48P-SSK9/ N55-96P-SSK9	"Cisco NX-OS ソフトウェア機能のライセンス"
Cisco Nexus 5010/5020 ストレージプロトコルライセンス	N5010 - SSK9/ N5020 - SSK9	
Cisco Nexus 5600 ストレージプロトコルライセンス	N56-16P-SSK9/N5672-72P-SSK9/N56128-128P-SSK9	
Cisco Nexus 7000 Storage Enterprise ライセンス	N7K-SAN1K9	
Cisco Nexus 9000 Enterprise Services ライセンス	N95-LAN1K9/ N93-LAN1K9	

シスコはライセンスオプションをサポートしています

FlexPod アーキテクチャのすべてのシスコ機器について、有効な SmartNet サポート契約が必要です。

必要なライセンスおよびこれらのライセンスのパーツ番号は、製品によって異なる場合があるため、営業担当者が確認する必要があります。次の表に、シスコのサポートライセンスオプションを示します。

Cisco Support のライセンス	ライセンスガイド
Smart Net Total Care Onsite Premium	"Cisco Smart Net Total Care サービス"

NetApp コンポーネント

ネットアップのストレージコントローラは、ブートとアプリケーションデータストレージの両方に関して、 FlexPod アーキテクチャのストレージ基盤を提供します。ネットアップのコンポーネントには、ストレージコントローラ、クラスタインターコネクトスイッチ、ドライブとディスクシェルフ、ライセンスオプションがあります。

ネットアップストレージコントローラのオプション

FlexPod アーキテクチャには、冗長な NetApp FAS 、 AFF 、または AFF ASA コントローラが必要です。コントローラは ONTAP ソフトウェアを実行します。ストレージコントローラを購入した場合は、優先バージョンのソフトウェアをコントローラにプリロードすることができます。ONTAP の場合は、クラスタ全体を発注した。クラスタ全体には、ストレージコントローラのペアとクラスタインターコネクト（スイッチまたはスイッチレス）が含まれます。

選択したストレージプラットフォームに応じて、さまざまなオプションや設定を使用できます。これらの追加コンポーネントの詳細については、営業担当者にお問い合わせください。

次の表に示すコントローラファミリーは、解決策データセンター FlexPod での使用に適しています。 Cisco Nexus スイッチへの接続はシームレスであるためです。を参照してください "NetApp Hardware Universe の略" 各コントローラモデルの互換性の詳細については、を参照してください。

ストレージコントローラファミリー	技術仕様
AFF A シリーズ	"AFF A-Series のドキュメント"
AFF ASA A シリーズ	"AFF ASA A シリーズのドキュメント"
FAS シリーズ	"FAS シリーズのドキュメント"

クラスタインターコネクトスイッチのオプション

次の表に、 FlexPod アーキテクチャで使用できる Nexus クラスタインターコネクトスイッチを示します。また、導入する ONTAP のバージョンに互換性がある場合、 ONTAP は、他社製スイッチを含む FlexPod 対応のすべてのクラスタスイッチをサポートします。を参照してください "NetApp Hardware Universe の略" で、特定のスイッチモデルの互換性の詳細を確認できます。

クラスタインターコネクトスイッチ	技術仕様
Cisco Nexus 3132Q-V の 2 つのポートを設定します	"ネットアップのマニュアル： Cisco Nexus 3132Q-V switches"
Cisco Nexus 9336C-FX2	"ネットアップのマニュアル： Cisco Nexus 9336C-FX2 switches"

ネットアップのディスクシェルフとドライブのオプション

すべてのストレージコントローラに、少なくとも 1 台のネットアップディスクシェルフが必要です。

選択したネットアップシェルフタイプによって、そのシェルフ内で使用可能なドライブタイプが決まります。

> すべてのディスクシェルフとディスクのパーツ番号については、営業担当者にお問い合わせください。

サポートされているドライブの詳細については、次の表の「 NetApp Hardware Universe 」リンクをクリックし、サポートされているドライブを選択してください。

ディスクシェルフ	技術仕様
DS224C	"NetApp Hardware Universe でサポートされているディスクシェルフとストレージメディアドライブ"
DS212C	
DS460C	
NS224	

ネットアップのソフトウェアライセンスオプション

次の表に、 FlexPod データセンターアーキテクチャで使用できるネットアップのソフトウェアライセンスオプションを示します。ネットアップソフトウェアのライセンスは、 FAS および AFF のコントローラレベルで提供されます。

ネットアップソフトウェアライセンス	パーツ番号	技術仕様
SW 、完全 NDL （コントローラ）、 -C	SW-8XXX-COMP-BNDL-C	"Product Library A-Z"
SW 、 ONTAP Essentials （コントローラ）、 -C	sw-8XXX-ONTAP9-C	

ネットアップはライセンスオプションをサポートしています

SupportEdge Premium アーキテクチャには NetApp FlexPod ライセンスが必要ですが、これらのライセンスのパーツ番号は FlexPod 設計で選択したオプションによって異なります。たとえば、ソフトウェアライセンスのパーツ番号は、選択する FAS コントローラによって異なります。個々のサポートライセンスの正確なパーツ番号については、営業担当者にお問い合わせください。次の表に、 SupportEdge ライセンスの例を示します。

ネットアップサポートライセンス	パーツ番号	技術仕様
SupportEdge Premium 4 時間オンサイト—月数： 36	： cs -O2-4HR	"NetApp SupportEdge Premium の略"

電源とケーブル接続の要件

FlexPod 設計には、電源とケーブル配線の最小要件があります。

電力要件

FlexPod データセンターの電力要件は、 FlexPod データセンター構成のインストール場所によって異なります。

必要な最大電力およびその他の詳細な電力情報の詳細については、に記載されている各ハードウェアコンポーネントの技術仕様を参照してください "技術仕様と参考資料：ハードウェアコンポーネント"。

Cisco UCS の電力データの詳細については、を参照してください "Cisco UCS Power Calculator"。

ネットアップストレージコントローラの電力データについては、を参照してください "NetApp Hardware Universe の略"。プラットフォームで、構成に使用するストレージプラットフォーム（ FAS/V シリーズまたは AFF ）を選択します。ONTAP バージョンとストレージコントローラを選択し、 [結果の表示] ボタンをクリックします。

ケーブルの最小要件

必要なケーブルとアダプタの数と種類は、 FlexPod データセンターの導入環境によって異なります。ケーブルのタイプ、トランシーバのタイプ、および番号は、デザインプロセス中に要件に基づいて決定されます。次の表に、必要なケーブルの最小数を示します。

ハードウェア	モデル番号	ケーブルが必要です
Cisco UCS シャーシ	Cisco UCS 5108	Cisco UCS 2104XP 、 2204XP 、または 2208XP モジュールごとに 2 本以上のツイン同軸ケーブルを使用する
Cisco UCS ファブリックインターコネクト	Cisco UCS 6248UP	• 管理ポート用 Cat5e ケーブル × 2 • ファブリックインターコネクトのペアごとに、 L1 と L2 の 2 本の Cat5e ケーブル • ファブリックインターコネクトごとに 4 本以上のツイン同軸ケーブル • ファブリックインターコネクトごとに少なくとも 4 本の FC ケーブル
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• 管理ポート用 Cat5e ケーブル × 2 • ファブリックインターコネクトのペアごとに、 L1 と L2 の 2 本の Cat5e ケーブル • ファブリックインターコネクトごとに 4 本以上のツイン同軸ケーブル	Cisco UCS 6324
	• 10/100/1000Mbps 管理ポート × 2 • ファブリックインターコネクトごとに 2 本以上のツイン同軸ケーブル	Cisco Nexus 5000 および 7000 シリーズスイッチ
	Cisco Nexus 5000 シリーズ	
• スイッチごとに少なくとも 2 本の 10GbE ファイバケーブルまたはツイン同軸ケーブルが必要です • スイッチごとに少なくとも 2 本の FC ケーブル（ FC / FCoE 接続が必要な場合）	Cisco Nexus 7000 シリーズ	Cisco Nexus 9000 シリーズスイッチ

ハードウェア	モデル番号	ケーブルが必要です
Cisco Nexus 9000 シリーズ	各スイッチに少なくとも 2 本の 10GbE ケーブル	NetApp FAS コントローラ
AFF A シリーズ	• ストレージコントローラごとに 1 組の SAS ケーブルまたは SATA ケーブル • 従来の FC を使用している場合、コントローラごとに少なくとも 2 本の FC ケーブル • 各コントローラに 10GbE ケーブルが少なくとも 2 本必要です • コントローラごとに管理用の GbE ケーブルが少なくとも 1 本必要です • ONTAP では、クラスタインターコネクトスイッチのペアごとに 8 本の短いツイン同軸ケーブルが必要です	
FAS シリーズ	NetApp ディスクシェルフ	DS212C
ディスクシェルフ 1 台につき、SAS 、 SATA 、または FC ケーブル 2 本		DS224C
		DS460C
		NS224

技術仕様および参考資料

技術仕様は、シャーシ、 FEX 、サーバ、スイッチなど、 FlexPod 解決策のハードウェアコンポーネントに関する詳細を提供します。 ストレージコントローラを指定できます。

Cisco UCS B シリーズブレードサーバシャーシ

次の表に示す Cisco UCS B シリーズブレードサーバシャーシの技術仕様には、次のコンポーネントが含まれています。

- ラックユニット数
- ブレードの最大数
- ユニファイドファブリック機能
- サーバあたりのミッドプレーン I/O 帯域幅
- FEX の I/O ベイの数

コンポーネント	**Cisco UCS 5100** シリーズブレードサーバシャーシ
ラックユニット	6.
最大全幅ブレード	4.
ハーフ幅ブレードの最大数	8.
ユニファイドファブリックに対応しています	はい。
ミッドプレーン I/O	サーバあたり最大 80Gbps の I/O 帯域幅
FEX 用の I/O ベイ	Cisco UCS 2104XP 、 2204/8XP 、 2408XP 、および 2304 FEX 用のベイが 2 つあります

詳細については、を参照してください "Cisco UCS 5100 シリーズブレードサーバシャーシのデータシート"。

Cisco UCS B シリーズブレードサーバ

次の表に示す Cisco UCS B シリーズブレードサーバの技術仕様には、次のコンポーネントが含まれています。

- プロセッサソケットの数
- プロセッサのサポート
- メモリ容量
- サイズと速度
- SAN ブートサポート
- メザニンアダプタスロットの数
- I/O の最大スループット
- フォームファクタ
- シャーシあたりのサーバの最大数

コンポーネント	**Cisco UCS** データシート
Cisco UCS B200 M6	"Cisco UCS B200 M6 ブレードサーバ"

Cisco UCS C シリーズラックサーバ

Cisco UCS C シリーズラックサーバの技術仕様には、プロセッサのサポート、最大メモリ容量、 PCIe スロットの数、フォームファクタのサイズなどがあります。互換性のある UCS サーバモデルの詳細については、を参照してください "Cisco Hardware Compatibility の略" リスト次の表は、それぞれ C シリーズラックサーバデータシートと Cisco UCS C シリーズシャーシオプションを示しています。

コンポーネント	**Cisco UCS** データシート
Cisco UCS C220 M6	"Cisco UCS C220 M6 ラックサーバ"
Cisco UCS C225 M6	"Cisco UCS C225 M6 ラックサーバ"
Cisco UCS C240 M6	"Cisco UCS C240 M6 ラックサーバ"
Cisco UCS C245 M6	"Cisco UCS C245 M6 ラックサーバ"

Cisco UCS X シリーズシャーシ

次の表に示す Cisco UCS X シリーズシャーシの技術仕様には、次のコンポーネントが含まれています。

- ラックユニット数
- 最大ノード数
- ユニファイドファブリック機能
- IFM の I/O ベイの数

コンポーネント	**Cisco UCS 9508 X** シリーズコンピューティングノードシャーシ
ラックユニット	7.
最大ノード数	8.
ユニファイドファブリックに対応しています	はい。
IM 用 I/O ベイ	Cisco UCS 9108 Intelligent Fabric Module （ IFM ）用ベイ × 2

詳細については、を参照してください "Cisco UCS X9508 X シリーズシャーシのデータシート"。

Cisco UCS X シリーズコンピューティングノード

次の表に示す Cisco UCS X シリーズコンピューティングノードの技術仕様には、次のコンポーネントが含まれています。

- プロセッサソケットの数
- プロセッサのサポート
- メモリ容量
- サイズと速度
- SAN ブートサポート
- メザニンアダプタスロットの数
- I/O の最大スループット
- フォームファクタ
- シャーシあたりのコンピューティングノードの最大数

コンポーネント	Cisco UCS データシート
Cisco UCS X210c M6	"Cisco UCS X210c M6 コンピューティングノード"

GPU は **FlexPod AI** 、 **ML** 、 **DL** に最適です

次の表に示す Cisco UCS C シリーズラックサーバは、 AI 、 ML 、 DL のワークロードをホストする FlexPod アーキテクチャで使用できます。Cisco UCS C480 ML M5 サーバは、 AI 、 ML 、 DL のワークロード向けに設計されており、 NVIDIA の SXM2 ベースの GPU を使用し、他のサーバは PCIe ベースの GPU を使用します。

次の表に、これらのサーバで使用できる推奨 GPU も示します。

サーバ	**GPU**
Cisco UCS C220 M6	NVIDIA T4
Cisco UCS C225 M6	NVIDIA T4
Cisco UCS C240 M6	NVIDIA Tesla A10 、 A100
Cisco UCS C245 M6	NVIDIA Tesla A10 、 A100

Cisco UCS B シリーズブレードサーバ用の **Cisco UCS VIC** アダプタ

Cisco UCS B シリーズブレードサーバ用 Cisco UCS 仮想インターフェイスカード（ VIC ）アダプタの技術仕様には、次のコンポーネントが含まれています。

- アップリンクポートの数
- ポートあたりのパフォーマンス（ IOPS ）
- 電源
- ブレードポートの数
- ハードウェアオフロード
- シングルルート I/O 仮想化（ SR-IOV ）サポート

現在検証済みのすべての FlexPod アーキテクチャは、 Cisco UCS VIC を使用します。その他のアダプタは、ネットアップに記載されている場合はサポートされます "IMT" また、 FlexPod の導入と互換性がありますが、対応するリファレンスアーキテクチャに記載されているすべての機能が提供されるわけではありません。次の表は、 Cisco UCS VIC アダプタのデータシートを示しています。

コンポーネント	**Cisco UCS** データシート
Cisco UCS 仮想インターフェイスアダプタ	"Cisco UCS VIC データシート"

Cisco UCS ファブリックインターコネクト

Cisco UCS ファブリックインターコネクトの技術仕様には、フォームファクタサイズ、ポートと拡張スロットの総数、スループット容量などがあります。次の表に、 Cisco UCS ファブリックインターコネクトデータシートを示します。

コンポーネント	**Cisco UCS** データシート
Cisco UCS 6248UP	"Cisco UCS 6200 シリーズファブリックインターコネクト"
Cisco UCS 6296UP	
Cisco UCS 6324	"Cisco UCS 6324 ファブリックインターコネクト"
Cisco UCS 6300	"Cisco UCS 6300 シリーズファブリックインターコネクト"
Cisco UCS 6454	"Cisco UCS 6400 シリーズファブリックインターコネクト"

Cisco Nexus 5000 シリーズスイッチ

フォームファクタのサイズ、ポートの総数、レイヤ 3 モジュールおよびドーターカードのサポートなど、Cisco Nexus 5000 シリーズスイッチの技術仕様は、各モデルファミリのデータシートに記載されています。これらのデータシートは次の表にあります。

コンポーネント	**Cisco Nexus** データシート
Cisco Nexus 5548UP	"Cisco Nexus 5548UP スイッチ"
Cisco Nexus 5596UP （ 2U ）	"Cisco Nexus 5596UP スイッチ"
Cisco Nexus 56128P	"Cisco Nexus 56128P スイッチ"
Cisco Nexus 5672UP	"Cisco Nexus 5672UP スイッチ"

Cisco Nexus 7000 シリーズスイッチ

フォームファクタのサイズやポートの最大数など、 Cisco Nexus 7000 シリーズスイッチの技術仕様は、各モデルファミリのデータシートに記載されています。これらのデータシートは次の表にあります。

コンポーネント	**Cisco Nexus** データシート
Cisco Nexus 7004	"Cisco Nexus 7000 シリーズスイッチ"
Cisco Nexus 7009	
Cisco Nexus 7010	
Cisco Nexus 7018	
Cisco Nexus 7702	"Cisco Nexus 7700 シリーズスイッチ"
Cisco Nexus 7706	
Cisco Nexus 7710	
Cisco Nexus 7718	

Cisco Nexus 9000 シリーズスイッチ

Cisco Nexus 9000 シリーズスイッチの技術仕様については、各モデルのデータシートを参照してください。仕様には、フォームファクタのサイズ、スーパーバイザ、ファブリックモジュール、およびラインカードスロットの数、およびポートの最大数が含まれます。これらのデータシートは次の表にあります。

コンポーネント	**Cisco Nexus** データシート
Cisco Nexus 9000 シリーズ	"Cisco Nexus 9000 シリーズスイッチ"
Cisco Nexus 9500 シリーズ	"Cisco Nexus 9500 シリーズスイッチ"
Cisco Nexus 9300 シリーズ	"Cisco Nexus 9300 シリーズスイッチ"
Cisco Nexus 9336PQ ACI スパインスイッチ	"Cisco Nexus 9336PQ ACI スパインスイッチ"
Cisco Nexus 9200 シリーズ	"Cisco Nexus 9200 プラットフォームスイッチ"

Cisco Application Policy Infrastructure コントローラ

セクションの項目に加えて、 Cisco ACI を導入する "Cisco Nexus 9000 シリーズスイッチ"では、 3 つの Cisco APIC を設定する必要があります。次の表に、 Cisco APIC データシートを示します。

コンポーネント	**Cisco Application Policy Infrastructure** データシート
Cisco Application Policy Infrastructure Controller	"Cisco APIC データシート"

Cisco Nexus ファブリックエクステンダの詳細

Cisco Nexus FEX の技術仕様には、速度、固定ポートおよびリンクの数、およびフォームファクタサイズが含まれます。

次の表に、 Cisco Nexus 2000 シリーズ FEX データシートを示します。

コンポーネント	**Cisco Nexus** ファブリックエクステンダデータシート
Cisco Nexus 2000 シリーズファブリックエクステンダ	"Nexus 2000 シリーズ FEX データシート"

SFP モジュール

SFP モジュールの詳細については、次のリソースを参照してください。

- Cisco 10Gb SFP の詳細については、を参照してください "Cisco 10 ギガビットモジュール"。
- Cisco 25GB SFP の詳細については、を参照してください "Cisco 25 ギガビットモジュール"。
- Cisco QSFP モジュールの詳細については、を参照してください "Cisco 40GBASE QSFP モジュールデータシート"。
- Cisco 100Gb SFP の詳細については、を参照してください "Cisco 100 ギガビットモジュール"。
- Cisco FC SFP モジュールの詳細については、を参照してください "Cisco MDS 9000 ファミリ Pluggable Transceiver データシート"。
- サポートされているすべての Cisco SFP およびトランシーバモジュールについては、を参照してください "『 Cisco SFP and SFP+ Transceiver Module Installation Notes 』" および "Cisco トランシーバモジュール"。

ネットアップストレージコントローラ

ネットアップストレージコントローラの技術仕様には、以下のコンポーネントが含まれます。

- シャーシの構成
- ラックユニット数
- メモリの容量
- NetApp FlashCache のキャッシング
- アグリゲートのサイズ
- ボリュームサイズ

- LUN の数
- サポートされるネットワークストレージ
- NetApp FlexVol の最大ボリューム数
- サポートされる SAN ホストの最大数
- Snapshot コピーの最大数

FAS シリーズ

FAS データセンターでは、使用可能な FlexPod ストレージコントローラのすべてのモデルがサポートされます。FAS シリーズのすべてのストレージコントローラの詳細な仕様については、を参照してください "NetApp Hardware Universe の略"。特定の FAS モデルの詳細については、次の表に示すプラットフォーム固有のドキュメントを参照してください。

コンポーネント	**FAS** シリーズコントローラプラットフォームのマニュアル
FAS9000 シリーズ	"FAS9000 シリーズのデータシート"
FAS8700 シリーズ	"FAS8700 シリーズのデータシート"
FAS8300 シリーズ	"FAS8300 シリーズのデータシート"
FAS500f シリーズ	"FAS500f シリーズのデータシート"
FAS2700 シリーズ	"FAS2700 シリーズのデータシート"

AFF A シリーズ

最新モデルの NetApp AFF A シリーズストレージコントローラは、いずれも FlexPod で使用できます。追加情報はにあります "AFF 技術仕様" データシートおよびのデータシート "NetApp Hardware Universe の略"。特定の AFF モデルの詳細については、次の表に示すプラットフォーム固有のドキュメントを参照してください。

コンポーネント	**AFF A** シリーズコントローラプラットフォームのドキュメント
NetApp AFF A800	"AFF A800 プラットフォームのドキュメント"
NetApp AFF A700	"AFF A700 プラットフォームのドキュメント"
NetApp AFF A700s	"AFF A700s プラットフォームのドキュメント"
NetApp AFF A400	"AFF A400 プラットフォームのドキュメント"
NetApp AFF A250	"AFF A250 プラットフォームマニュアル"

AFF ASA A シリーズ

最新モデルの NetApp AFF ASA A シリーズストレージコントローラは、いずれも FlexPod で使用できます。追加情報については、『オール SAN アレイ』ドキュメント、『 ONTAP AFF オール SAN アレイシステム』テクニカルレポート、および『 NetApp Hardware Universe 』を参照してください。特定の AFF モデルの詳細については、次の表に示すプラットフォーム固有のドキュメントを参照してください。

コンポーネント	**AFF A** シリーズコントローラプラットフォームのドキュメント
NetApp AFF ASA A800	"AFF ASA A800 プラットフォームのドキュメント"
NetApp AFF ASA A700	"AFF ASA A700 プラットフォームのドキュメント"
NetApp AFF ASA A400	"AFF ASA A400 プラットフォームのドキュメント"
NetApp AFF ASA A250	"AFF ASA A250 プラットフォームマニュアル"
NetApp AFF ASA A220	"AFF ASA A220 プラットフォームのマニュアル"

NetApp ディスクシェルフ

ネットアップのディスクシェルフの技術仕様には、フォームファクタサイズ、エンクロージャあたりのドライブ数、シェルフ I/O モジュールなどが含まれます。このドキュメントは、次の表に記載されています。詳細については、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技術仕様" および "NetApp Hardware Universe の略"。

コンポーネント	**NetApp FAS / AFF** ディスクシェルフのドキュメント
NetApp DS212C ディスクシェルフ	"DS212C ディスクシェルフのマニュアル"
NetApp DS224C ディスクシェルフ	"DS224C ディスクシェルフのドキュメント"
NetApp DS460C ディスクシェルフ	"DS460C ディスクシェルフのドキュメント"
NetApp NS224 NVMe SSD ディスクシェルフ	"NS224 ディスクシェルフのドキュメント"

ネットアップのドライブ

ネットアップドライブの技術仕様には、フォームファクタサイズ、ディスク容量、ディスク rpm 、サポートするコントローラ、 ONTAP のバージョンなどがあります。これらの仕様は、の「ドライブ」セクションに記載されています "NetApp Hardware Universe の略"。

レガシー機器

FlexPod は、 Cisco とネットアップが現在販売している既存の機器と新しい機器を使用できる柔軟な解決策です。場合によっては、 Cisco とネットアップの機器の一部のモデルがサポート終了（ EOL ）に指定されていることがあります。

これらの機器モデルは提供されなくなりましたが、販売終了（ EOA ）の前にこれらのモデルのいずれかを購入した場合は、 FlexPod 構成でその機器を使用できます。FlexPod でサポートされていて、販売されなくなった従来の機器モデルの完全なリストは、で参照できます "ネットアップサービスおよびサポート製品プログラム可用性インデックス"。

シスコのレガシー機器の詳細については、のシスコ EOL および EOA に関する通知を参照してください "Cisco UCS C シリーズラックサーバ"、 "Cisco UCS B シリーズブレードサーバ"および "Nexus スイッチ"。

従来の FC ファブリックのサポートには、次のものが含まれます。

- 2GB ファブリック
- 4GB ファブリック

レガシーソフトウェアには次のものが含まれます。

- NetApp Data ONTAP 7-Mode 、 7.3.5 以降
- ONTAP 8.1.x 〜 9.0.x
- Cisco UCS Manager 1.3 以降
- Cisco UCS Manager 2.1 〜 2.2.7

追加情報の参照先

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。

- ネットアップの製品マニュアル

  "https://docs.netapp.com/"

- ネットアップサポートコミュニケーション

  "https://mysupport.netapp.com/info/communications/index.html"

- ネットアップの Interoperability Matrix Tool （ IMT ）

  "https://mysupport.netapp.com/matrix/#welcome"

- NetApp Hardware Universe の略

  "https://hwu.netapp.com/"

- ネットアップサポート

  "https://mysupport.netapp.com/"

FlexPod データセンター

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

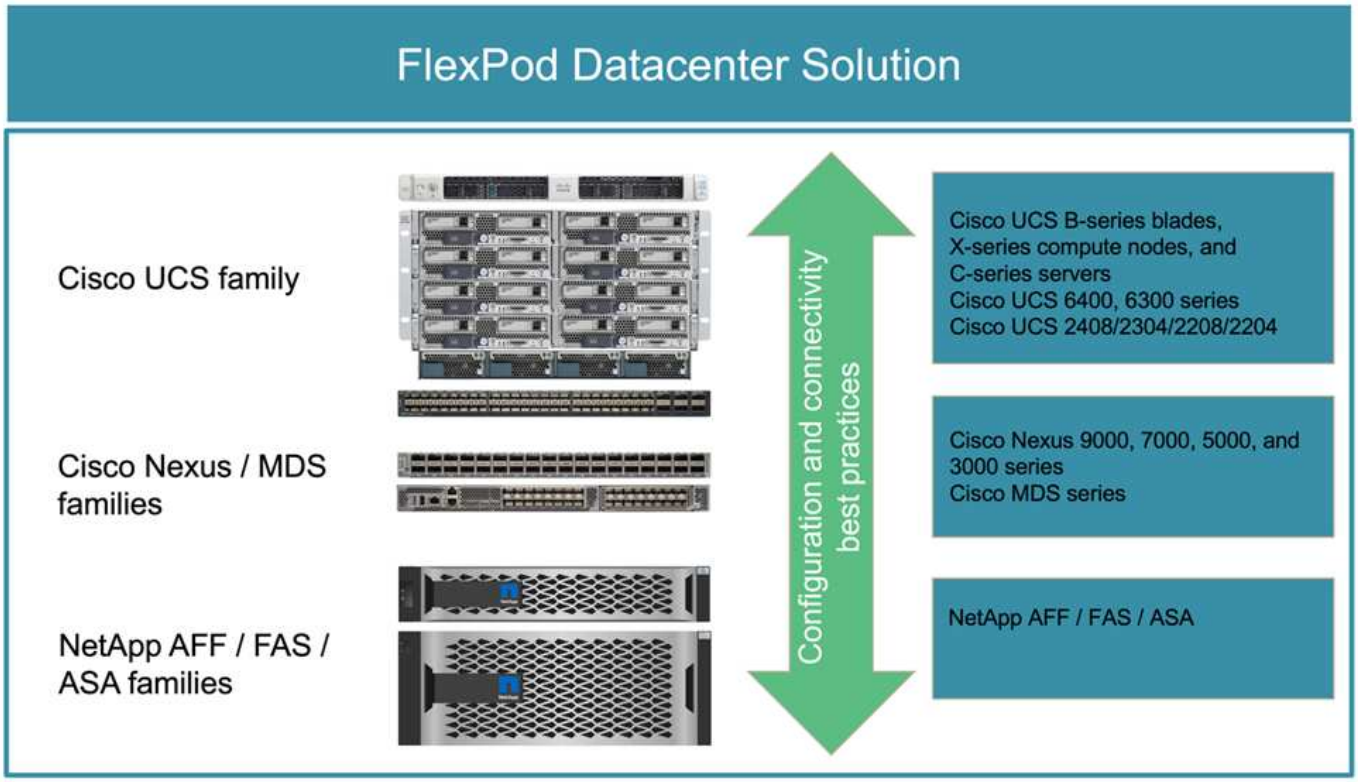
はじめに

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。

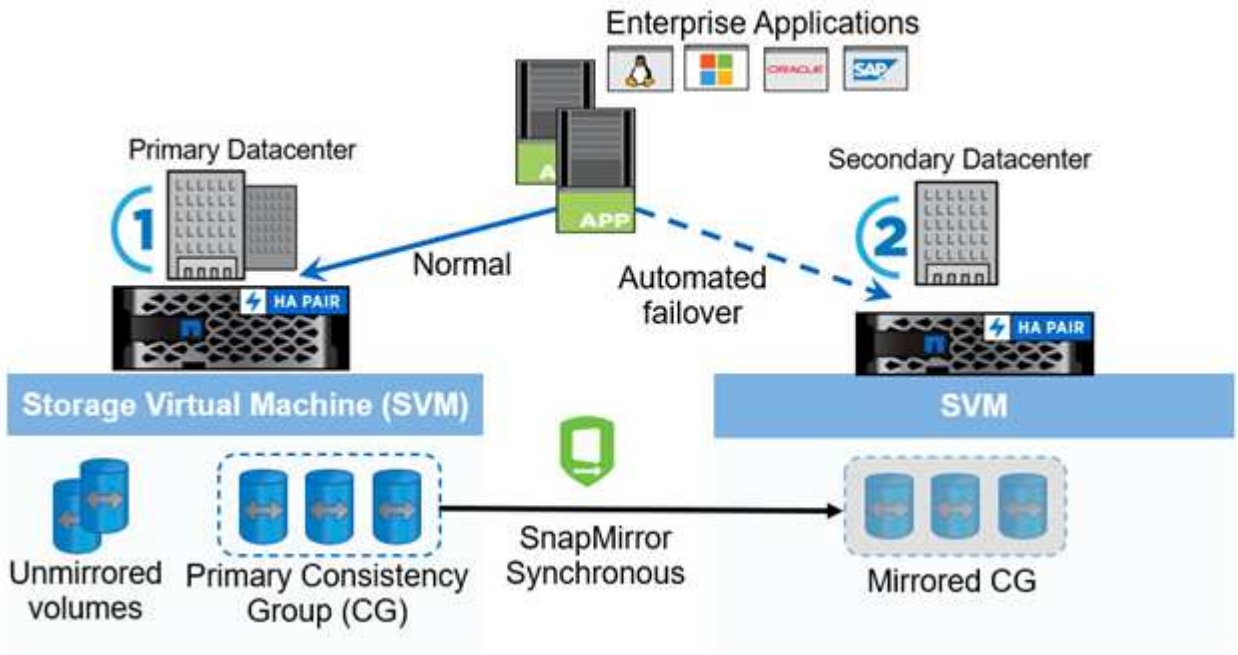
SM-BC です

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

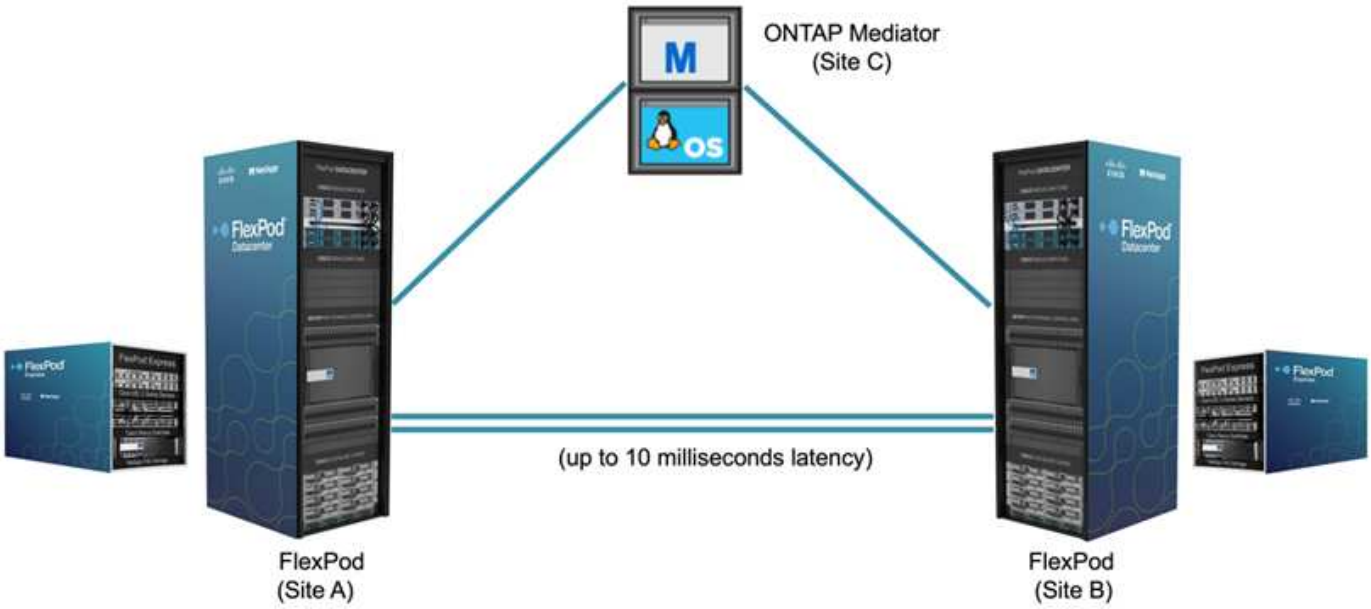
FlexPod SM-BC 解決策 は、高いレベルで 2 つの FlexPod システムで構成されています。これらのシステムは、ある程度離れた場所に設置され、接続され、ペアリングされているため、可用性が高く、柔軟性と信頼性に優れたデータセンター解決策 を提供し、サイト障害時にもビジネス継続性を提供できます。

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

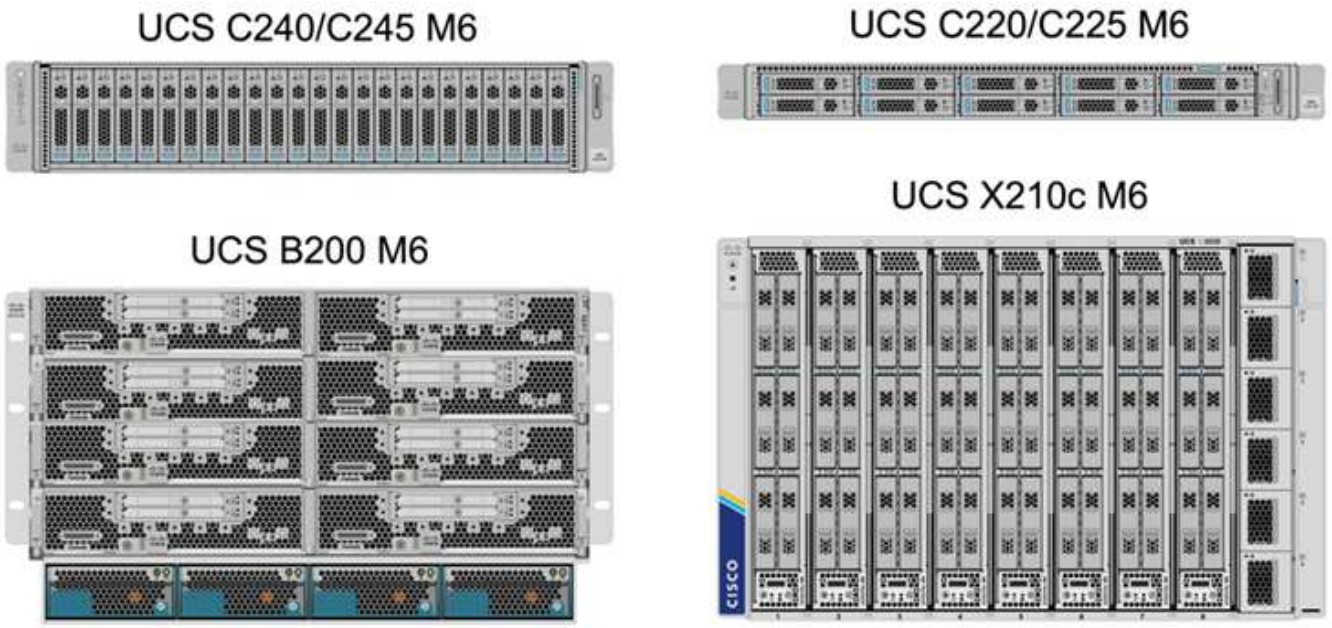
解決策コンポーネント

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。

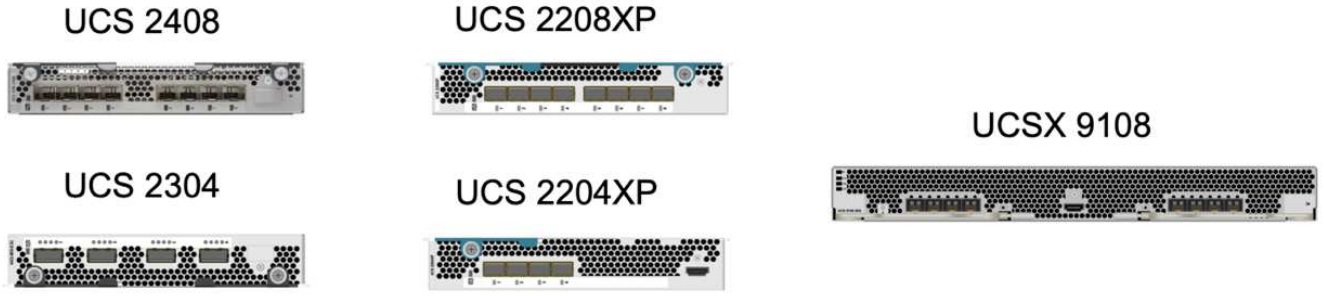
I/O モジュールおよびインテリジェントファブリックモジュール

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。

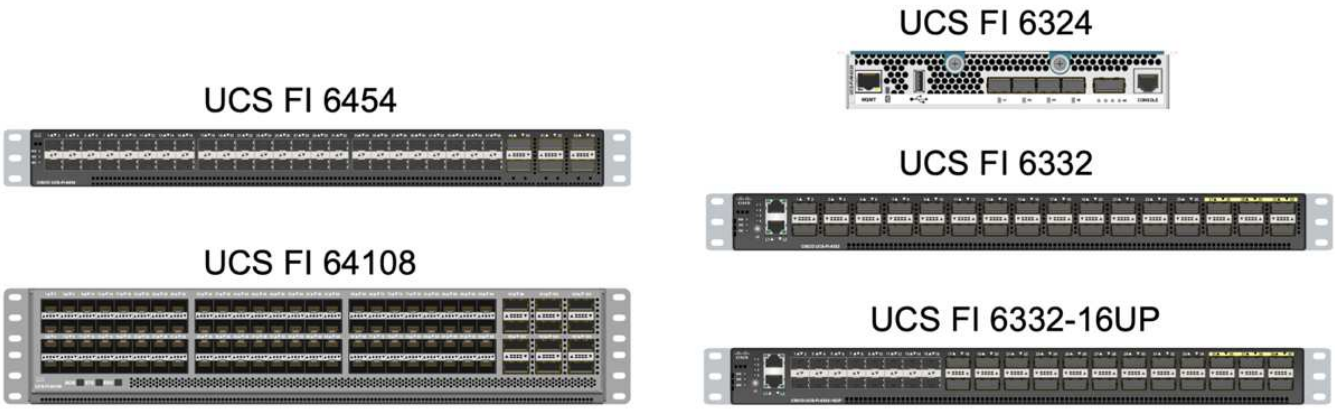
次の図は、 UCS 5108 シャーシの場合は UCS 2408 以前の IOM 世代、 X9508 シャーシの場合は 9108 IFM を示しています。



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。

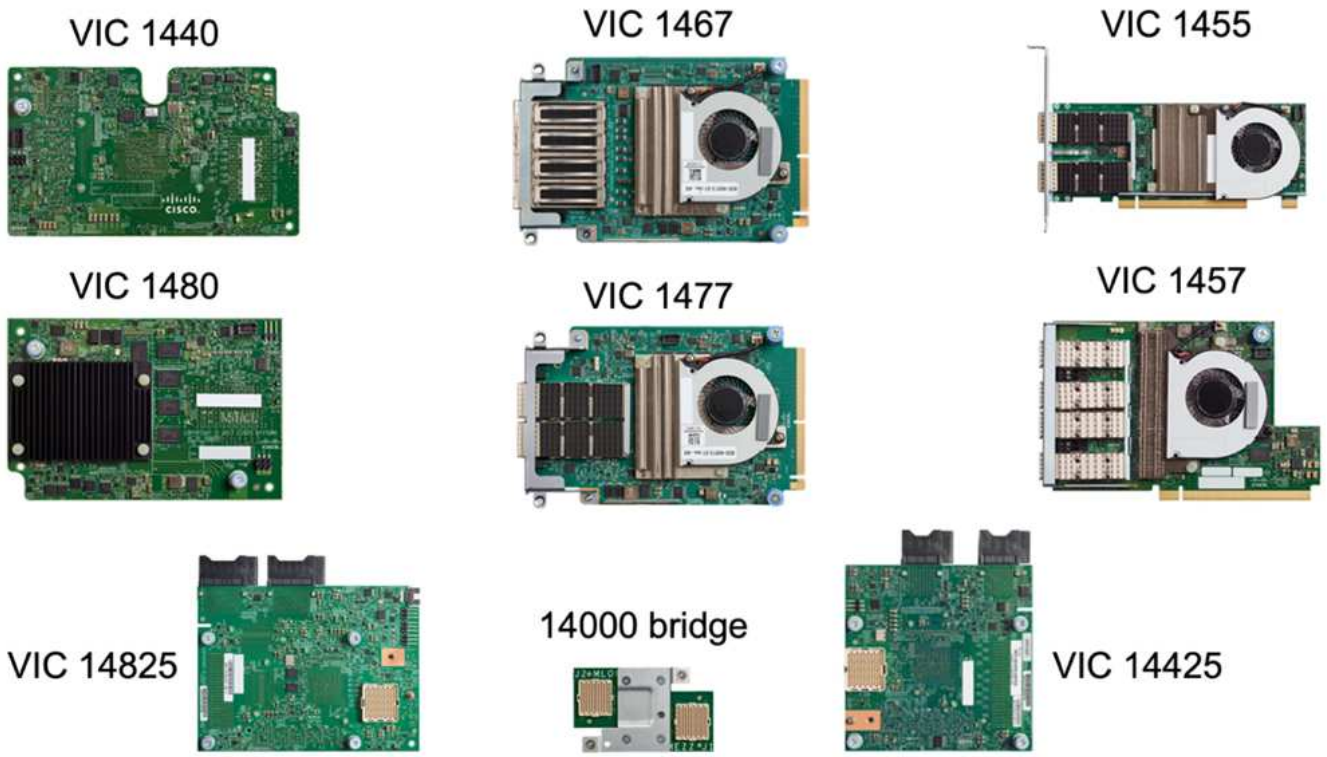


Cisco UCS X シリーズシャーシをサポートするには、 Intersight Managed Mode （ IMM ）で設定された第 4 世代のファブリックインターコネクトが必要です。ただし、 Cisco UCS 5108 B シリーズシャーシは、 IMM モードと UCSM 管理モードの両方でサポートできます。

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。

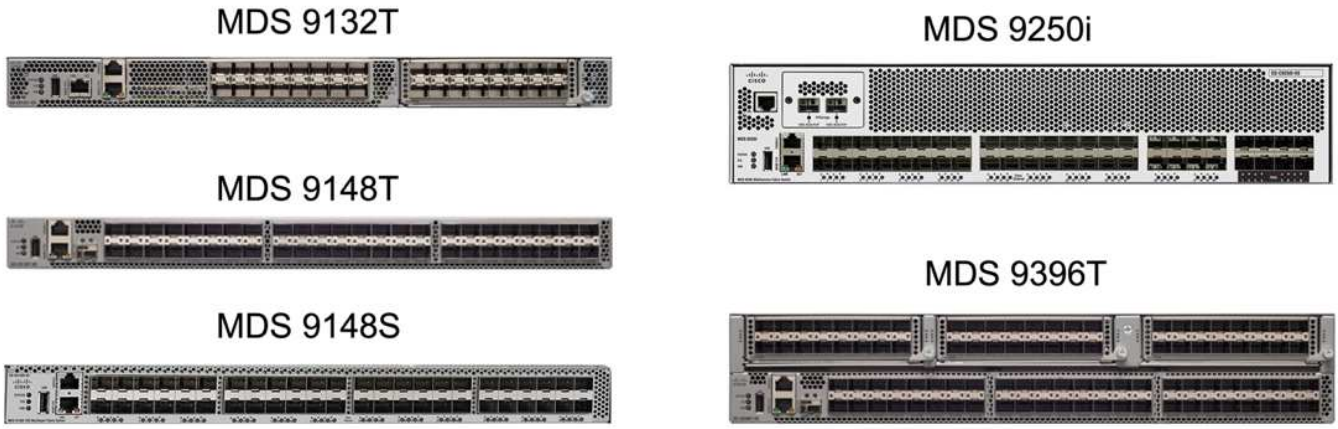
FlexPod 環境のスイッチモデルを選択する際には、パフォーマンス、ポート速度、ポート密度、スイッチング遅延など、さまざまな要因を考慮する必要があります。 また、 ACI や VXLAN などのプロトコルをサポートしているため、設計目的やスイッチのタイムスパンがサポートされます。

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。

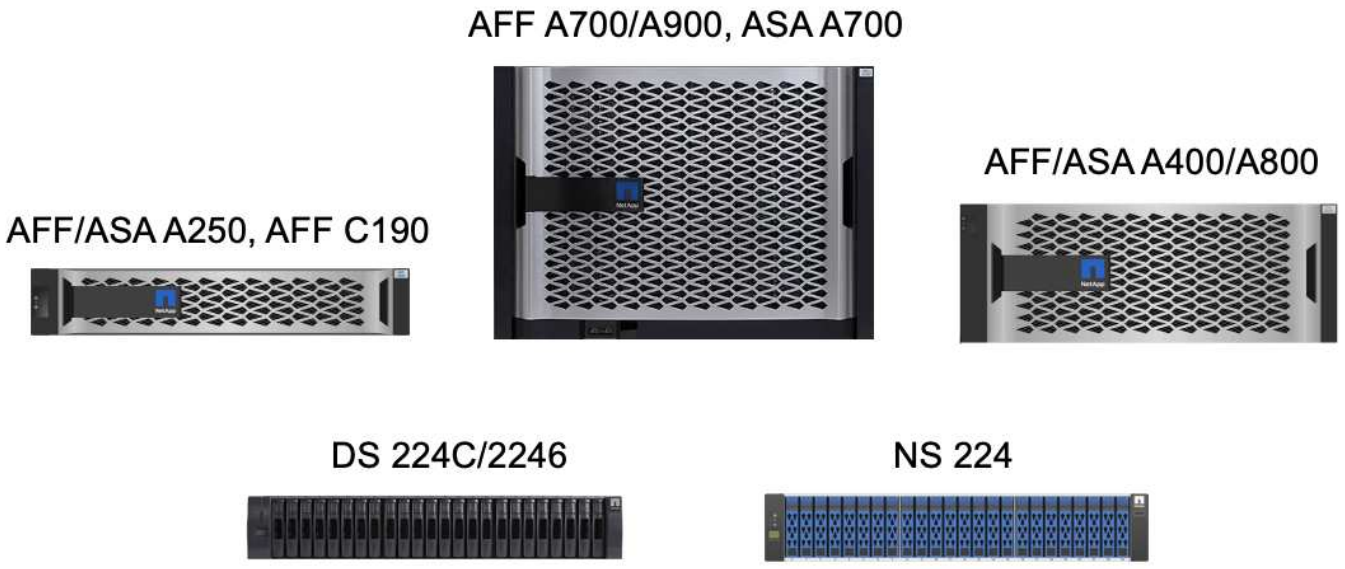
NetApp コンポーネント

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。

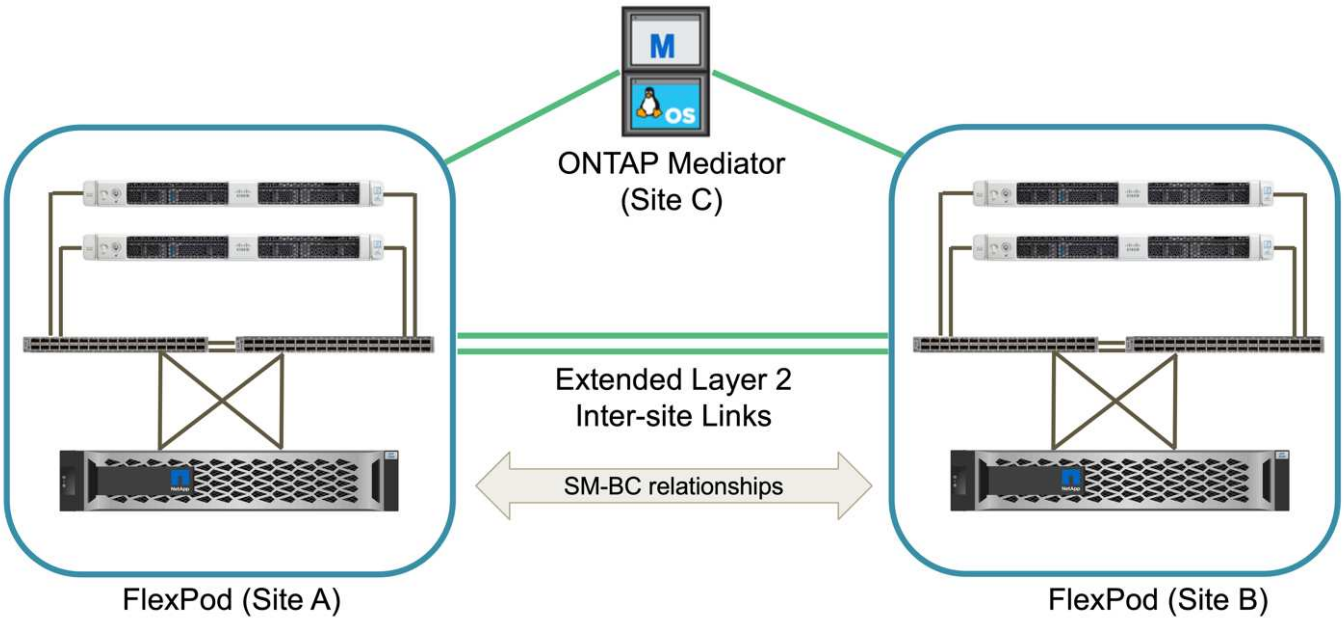


製品ファミリー	技術仕様
AFF シリーズ	"AFF シリーズのドキュメント"
ASA シリーズ	"ASA シリーズのドキュメント"

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。

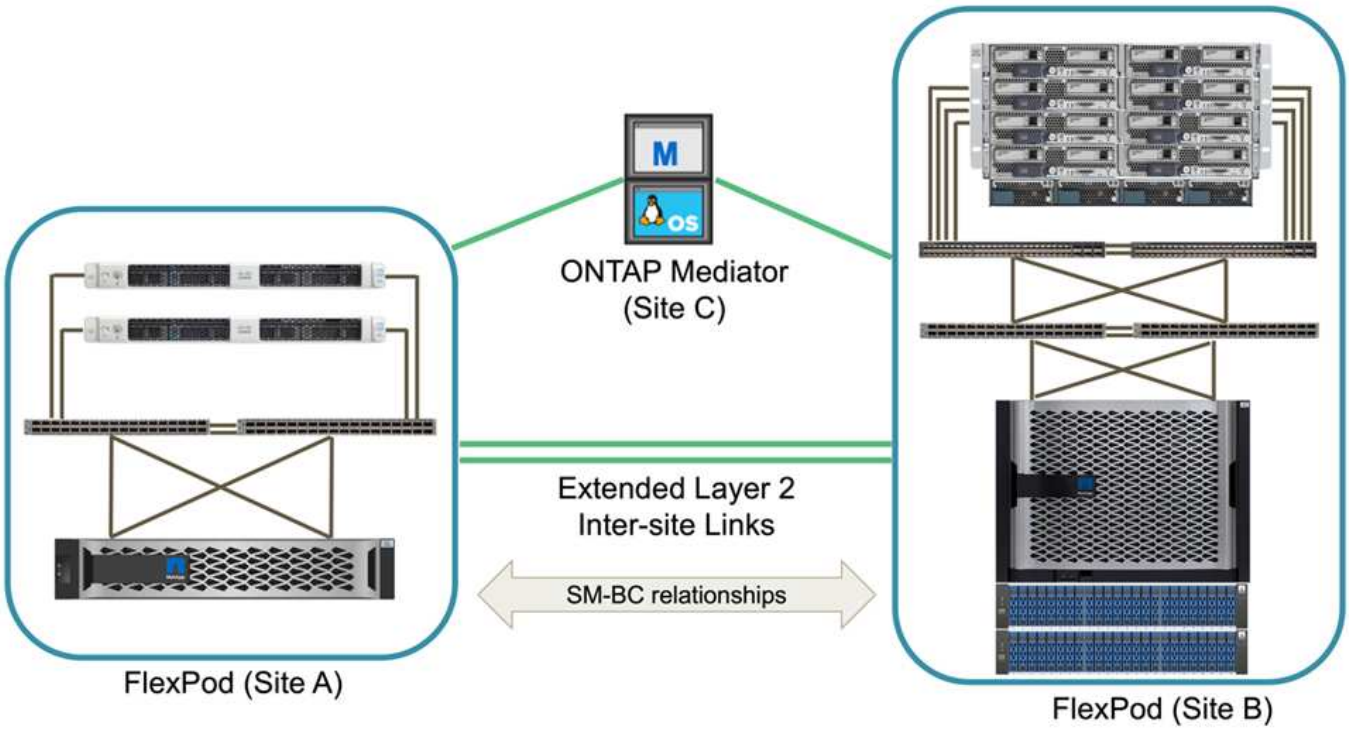
解決策 トポロジ

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。



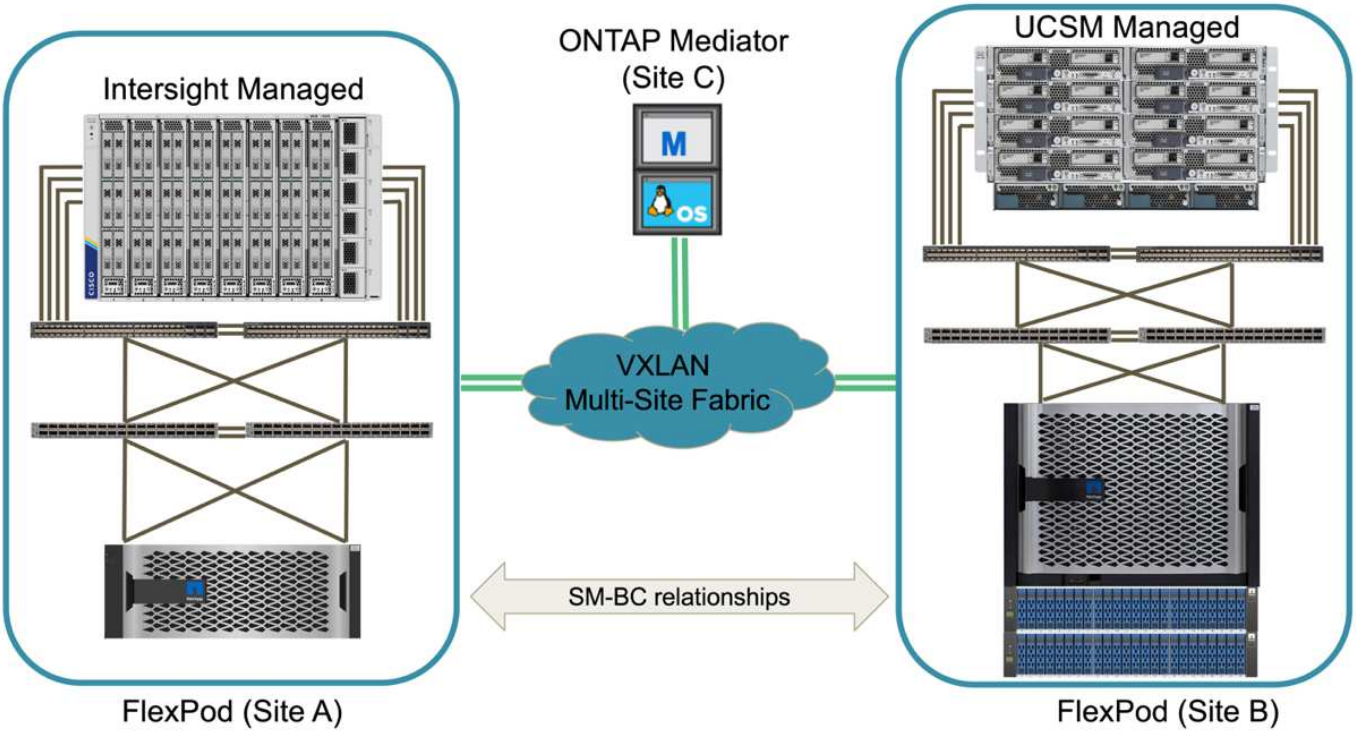
コンピューティング、ネットワーク、ストレージの冗長コンポーネントは、コンポーネント間の冗長な接続によって相互接続されます。この高可用性設計は、解決策 の耐障害性を提供し、単一点障害のシナリオに耐えることができます。マルチサイト設計と ONTAP SM-BC 同期データレプリケーション関係により、単一サイトのストレージ障害が発生しても、ビジネスクリティカルなデータサービスを提供します。

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。

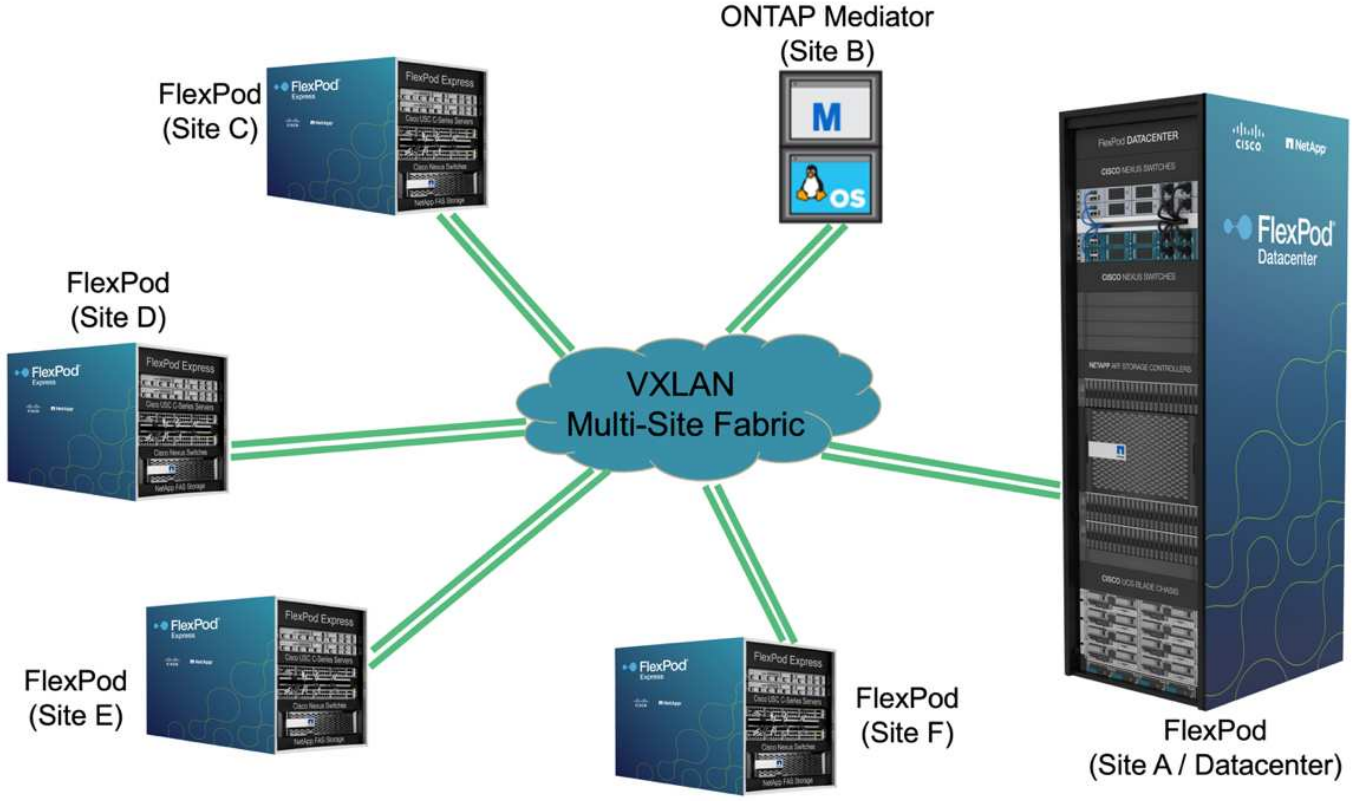


VXLAN ベースのマルチサイトファブリックを使用すると、コンピューティングリソースとストレージリソースの要件が大きくなり、複数のサイトにシームレスなネットワークファブリックを構築して、アプリケーションのモビリティを促進し、アプリケーションを任意のサイトから提供できるようになります。

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

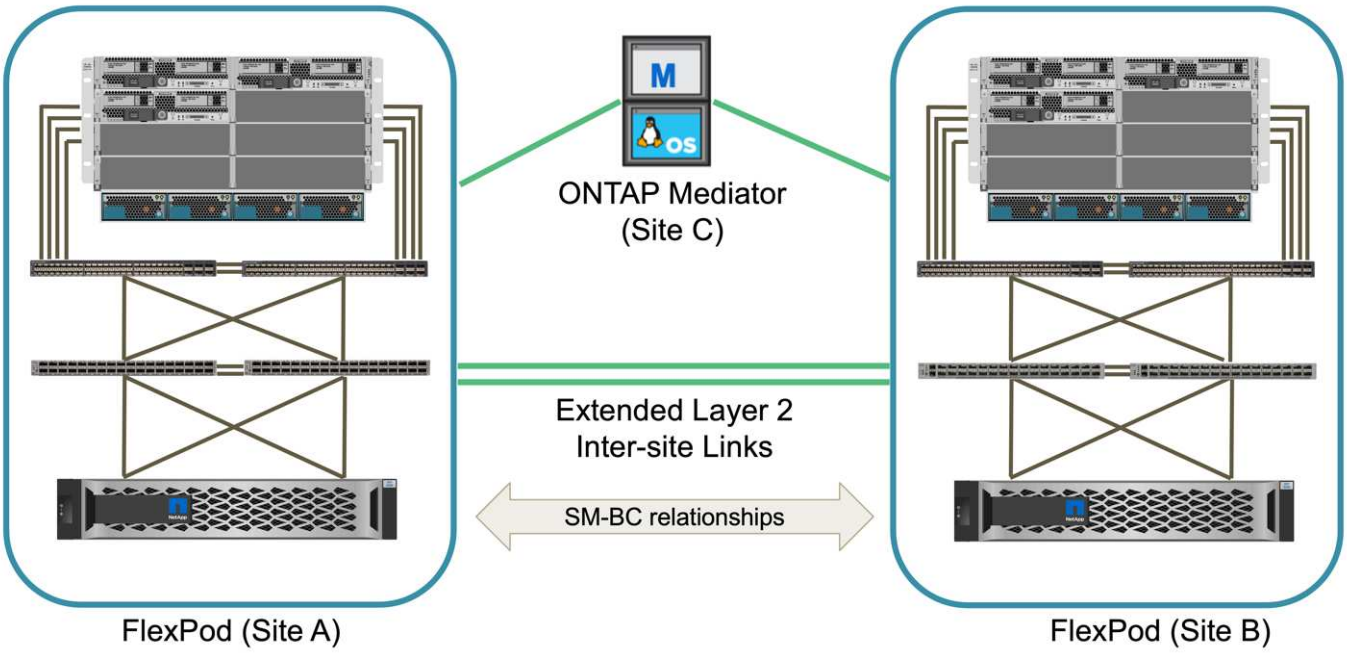
"前のページ： FlexPod SM-BC 解決策"

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）
	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.

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 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。"

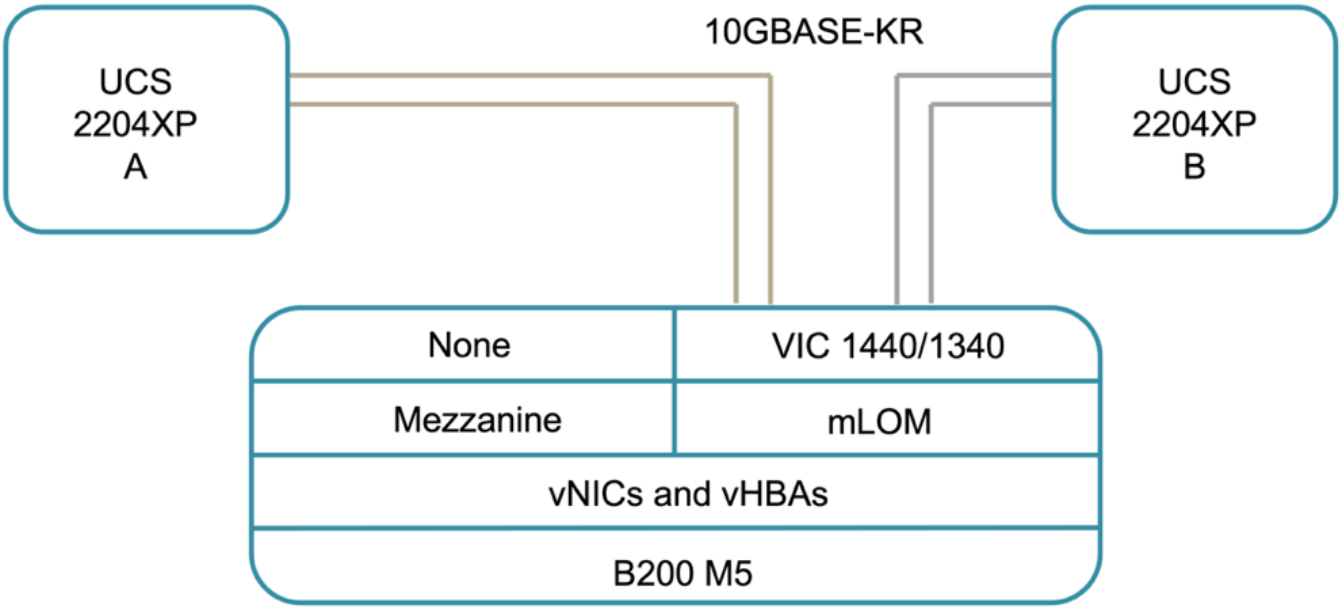
解決策 の検証 - コンピューティング

"事前定義：解決策 の検証 - 概要。"

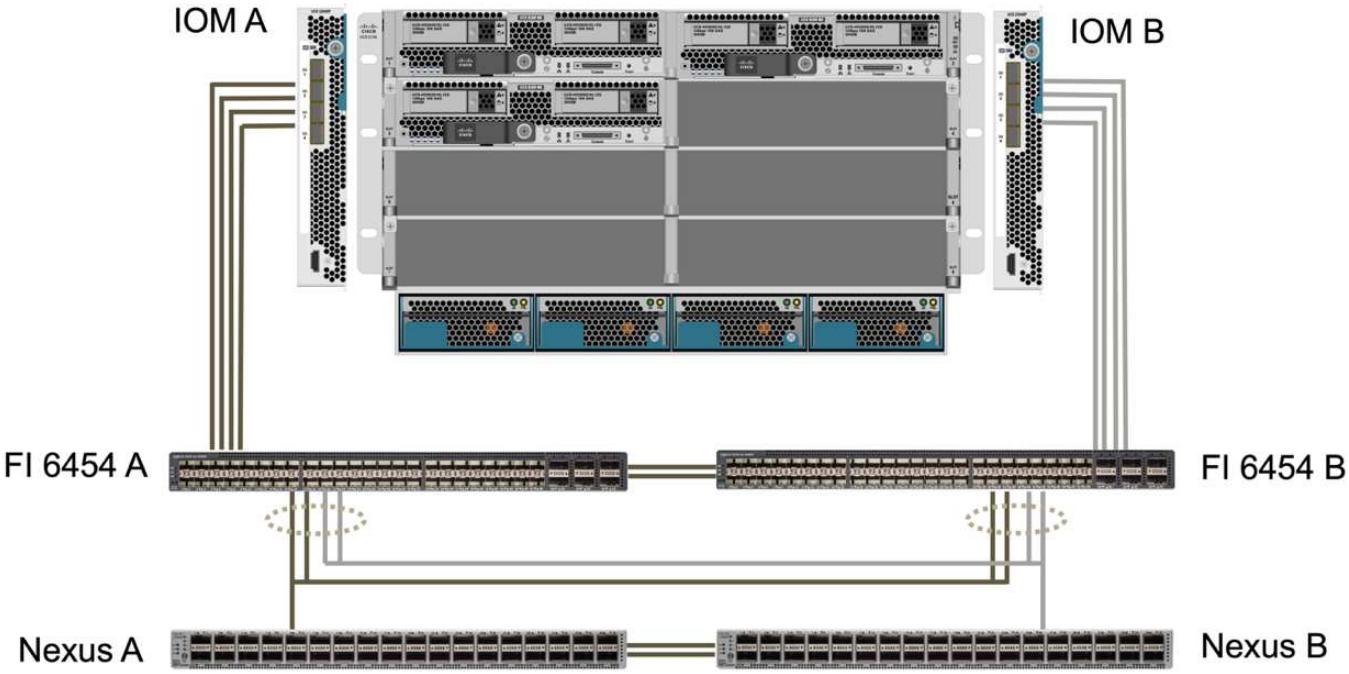
FlexPod SM-BC 解決策 のコンピューティング設定は、一般的な FlexPod 解決策 のベストプラクティスに従います。以降のセクションでは、検証に使用する接続と構成の一部を紹介します。また、 SM-BC に関連する考慮事項の一部は、実装のリファレンスとガイダンスを提供するために強調表示されています。

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.

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
	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。

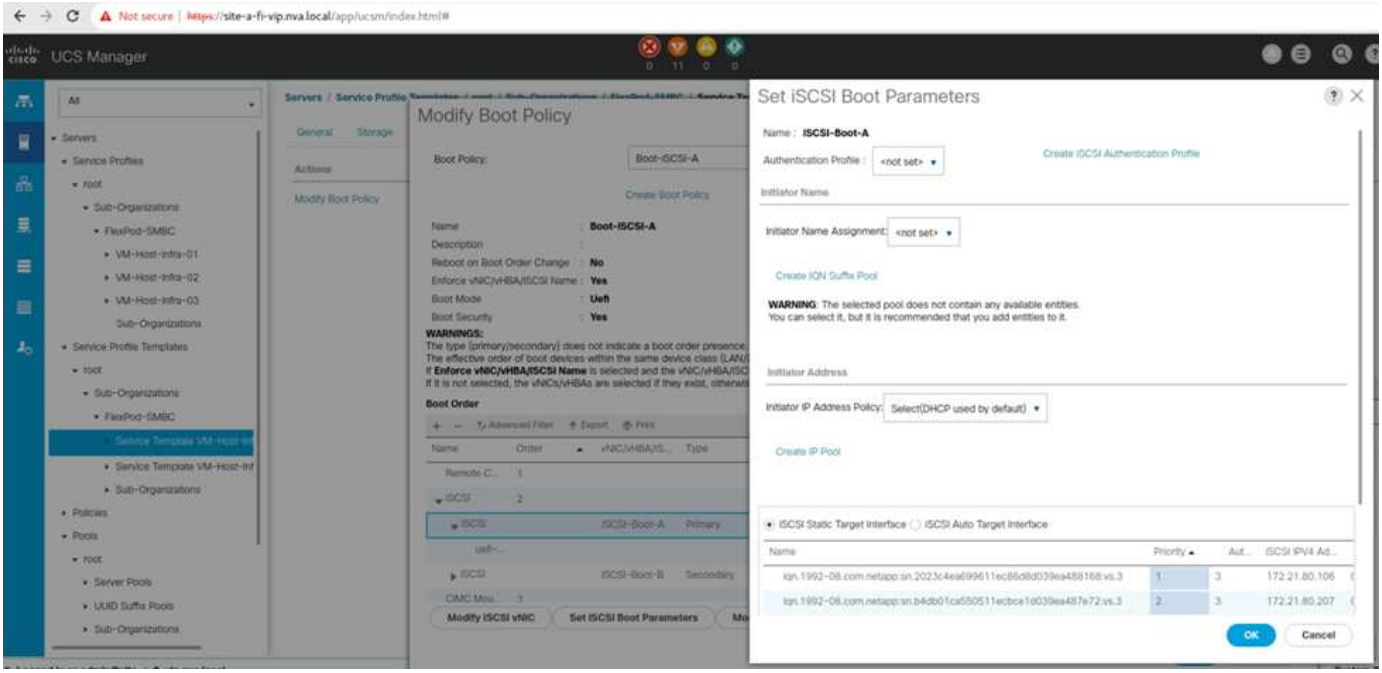
作成されるサービスプロファイルでは、 VMware ESXi ホストに対して次の情報がサポートされます。

- 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 ファブリック	優先度	iSCSI ターゲット	iSCSI 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

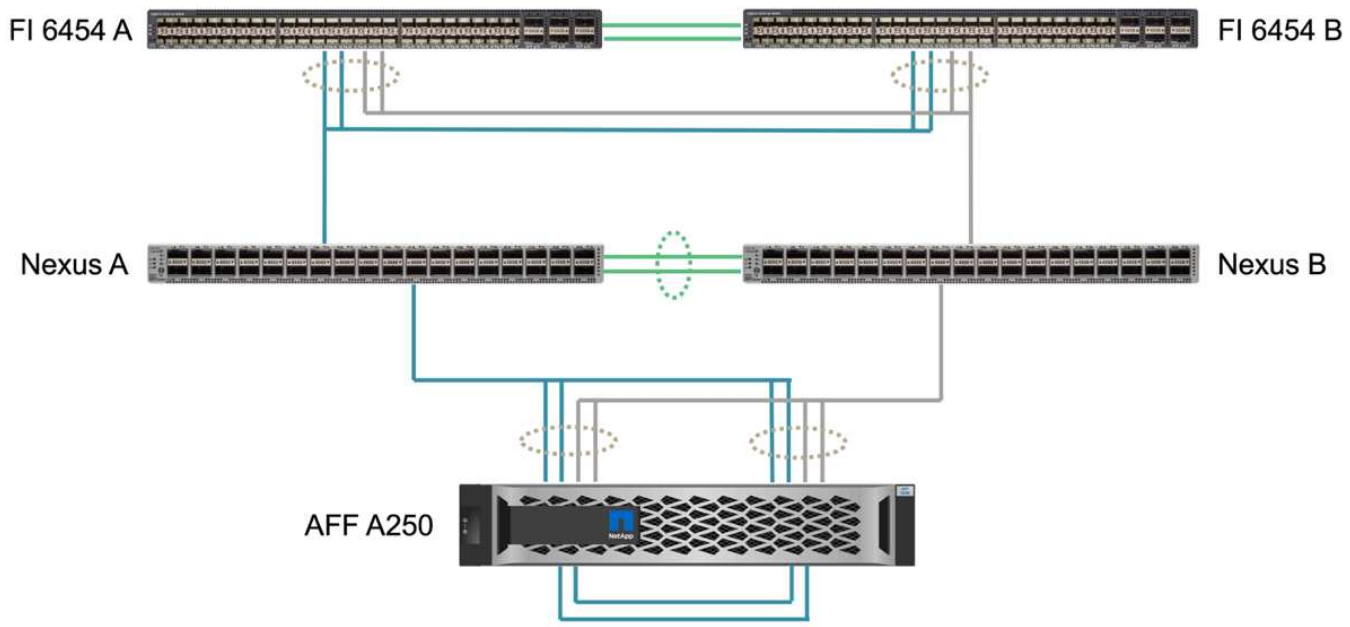
"前のバージョン：解決策 の検証 - コンピューティング。"

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。

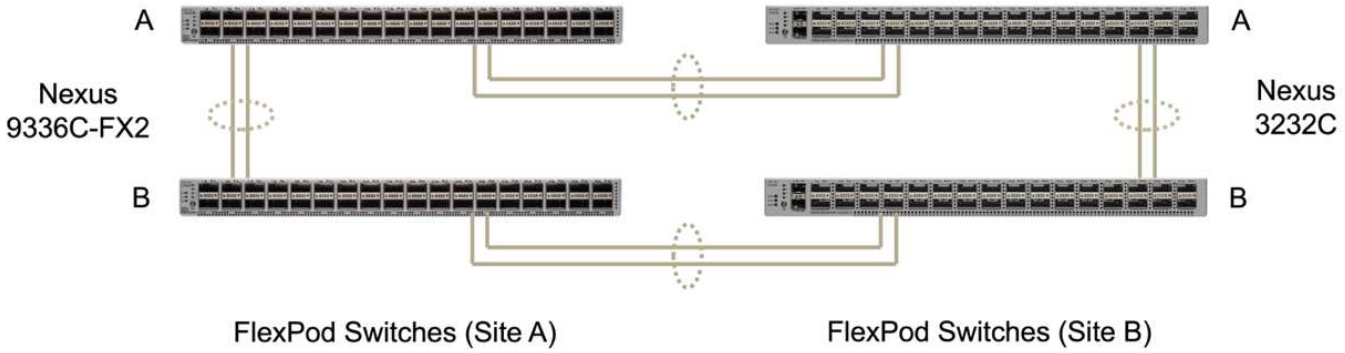
次の図は、各サイトでの Nexus スイッチのローカル接続を示しています。図に示されている内容に加えて、図に示されていない各コンポーネントのコンソールネットワーク接続と管理ネットワーク接続もあります。40G ~ 4 x 10G ブレークアウトケーブルは、 Nexus スイッチを UCS FI および ONTAP AFF A250 ストレージコントローラに接続するために使用します。また、 100G から 4 x 25G ブレークアウトケーブルを使用して、 Nexus スイッチと AFF A250 ストレージコントローラ間の通信速度を向上させることもできます。わかりやすいように、 2 台の AFF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

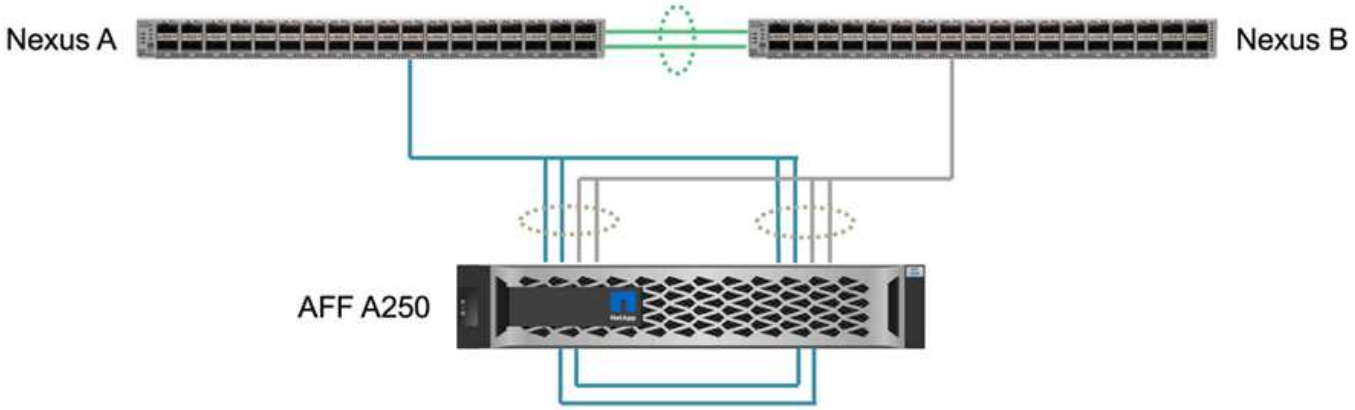
解決策 の検証 - ストレージ

"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。



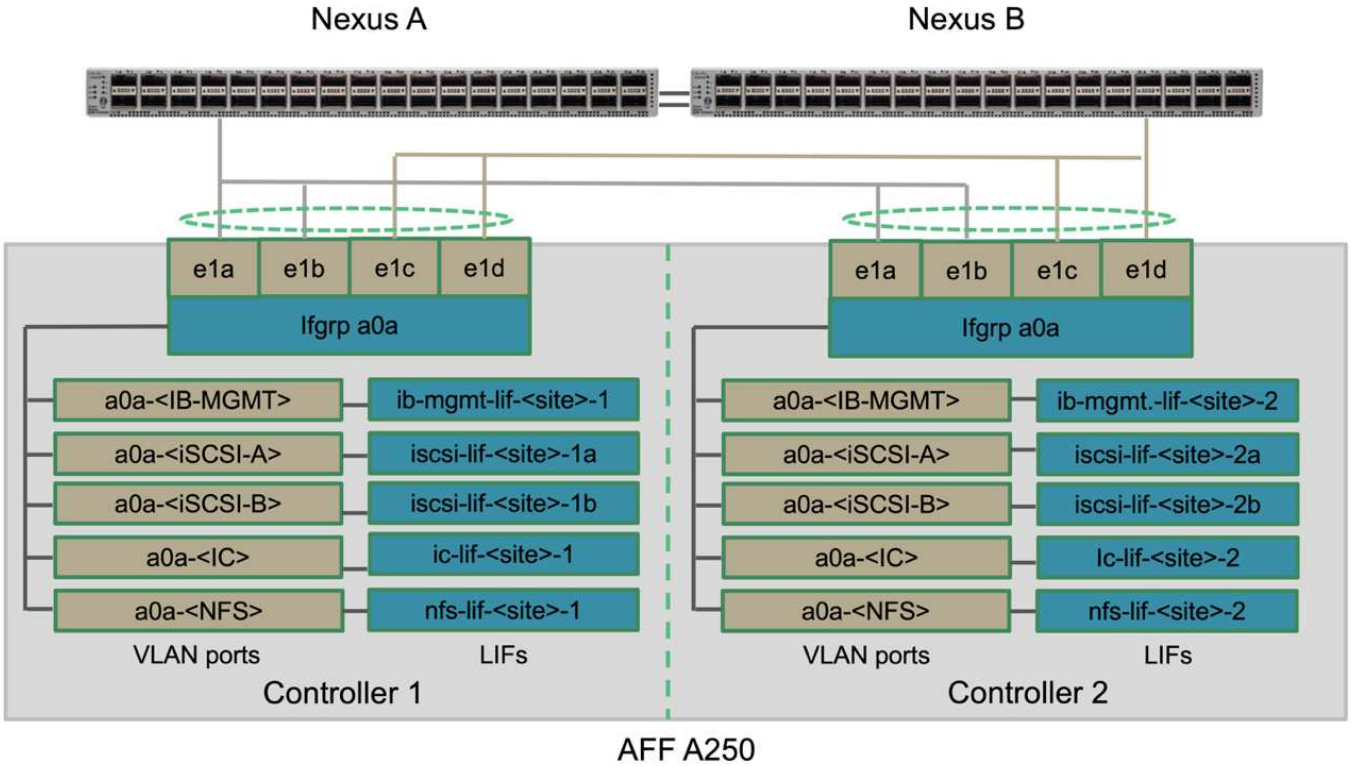
ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	E1A	Nexus A	1/10/1.
	e1b		1/10/2.
	E1C	Nexus B	1/10/1.

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。

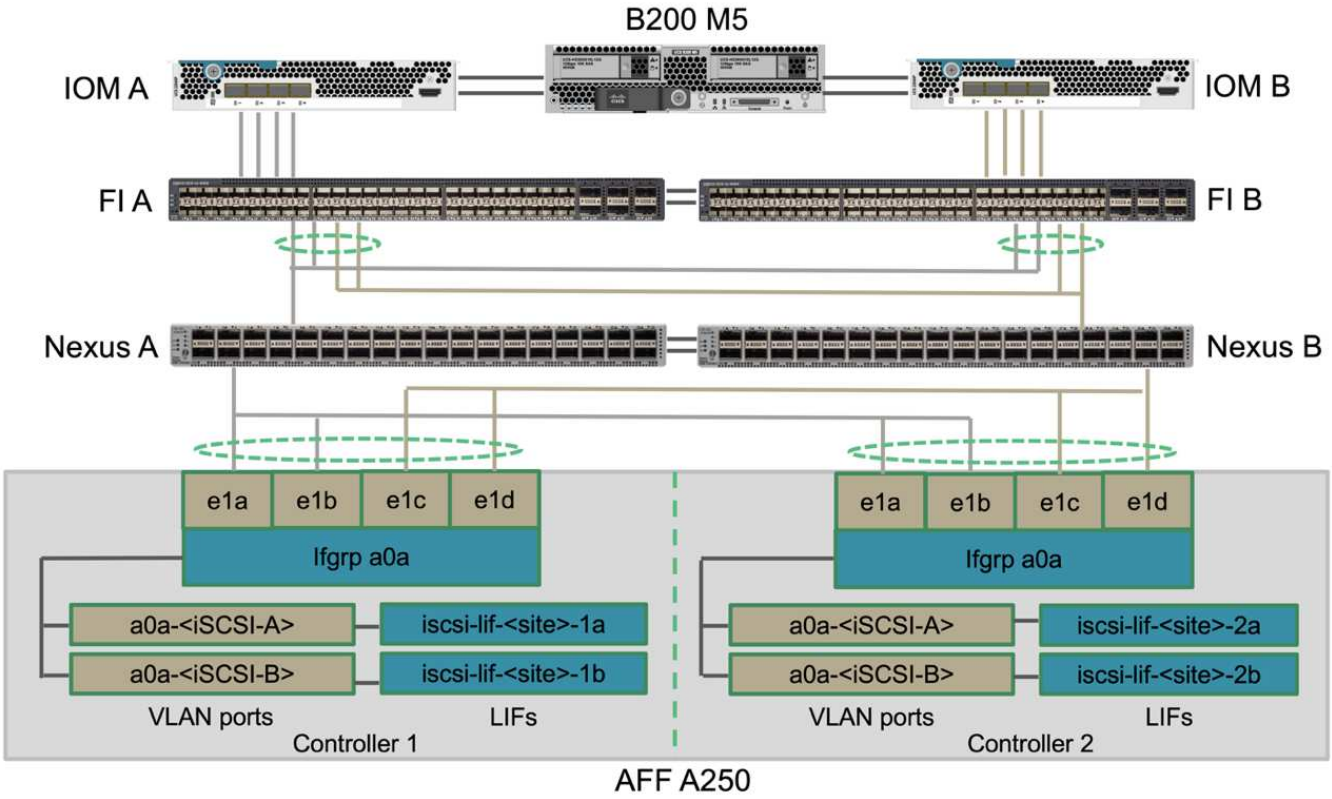


SAN ブート

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。

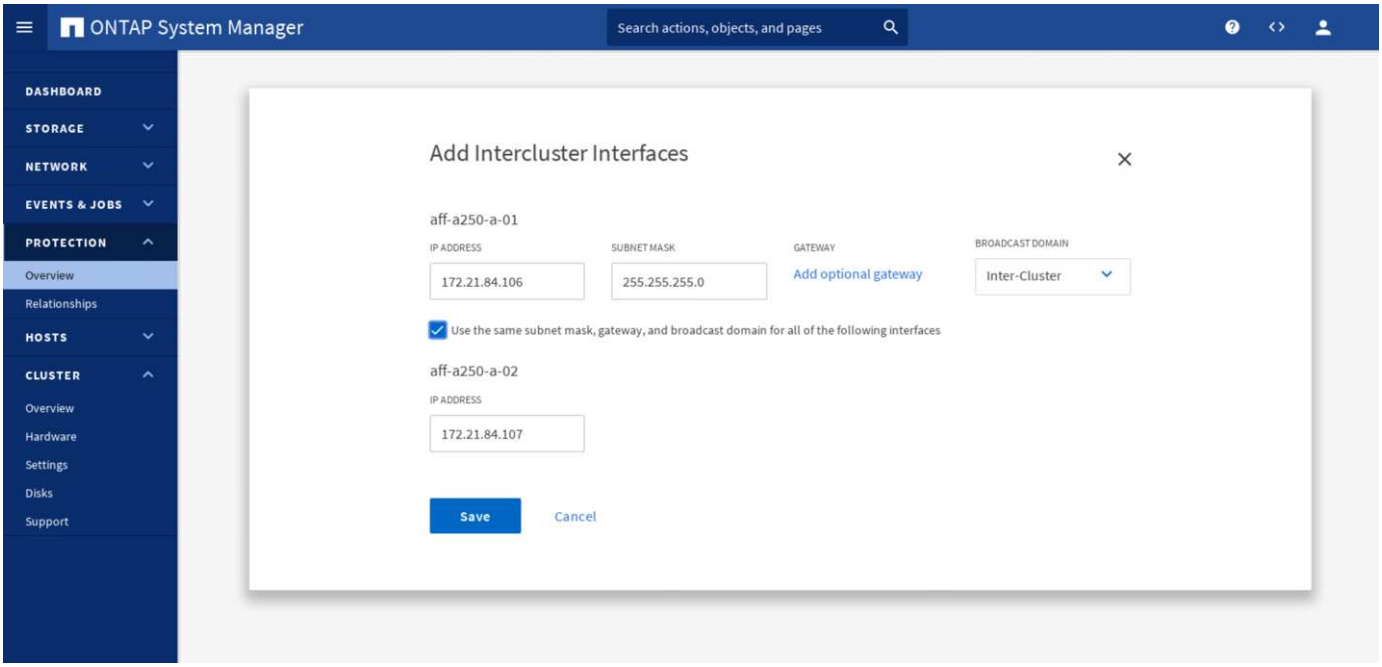
次の図は、ネットアップストレージから Cisco UCS サーバの iSCSI SAN ブートの接続を示しています。iSCSI SAN ブートでは、各 Cisco UCS サーバに 2 つの iSCSI vNIC （各 SAN ファブリックに 1 つずつ）が割り当てられ、サーバからストレージへの冗長接続が提供されます。Nexus スイッチに接続された 10 / 25 G イーサネットストレージポート（この例では e1a 、 e1b 、 e1c 、 e1d ）をグループ化して、 1 つのインターフェイスグループ（ ifgrp ）になります（この例では a0a ）。iSCSI VLAN ポートは ifgrp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



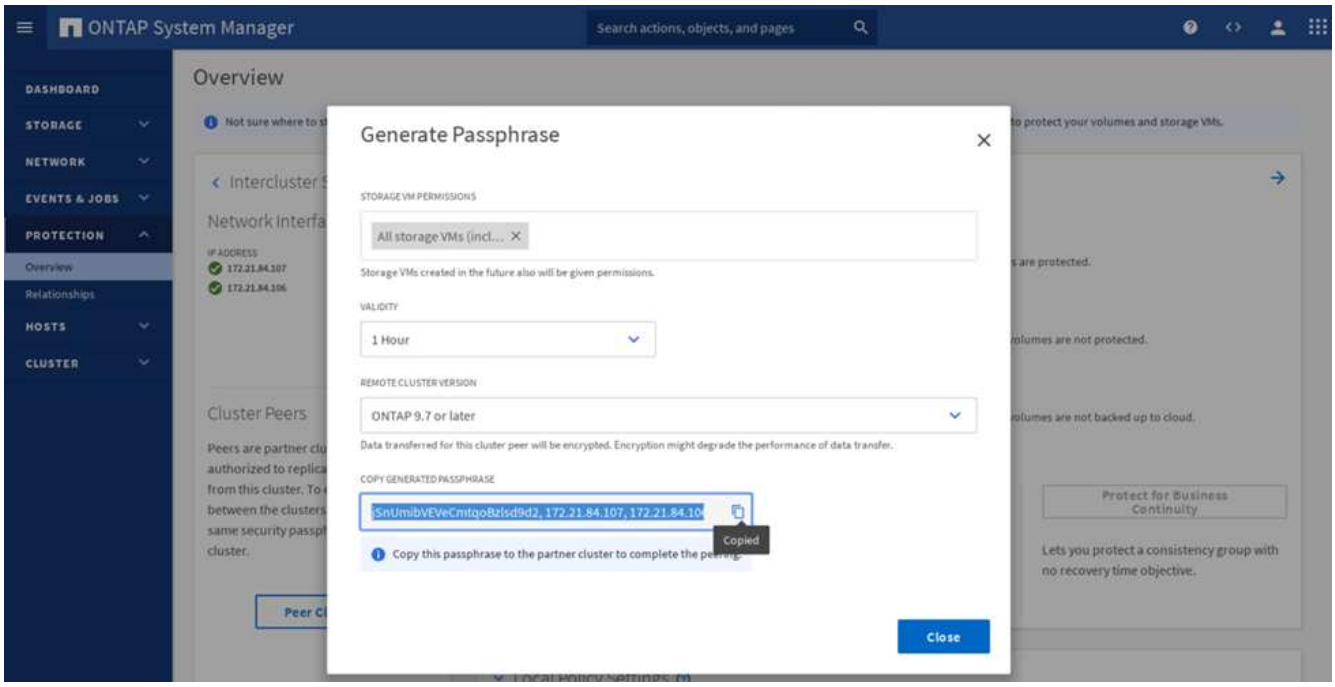
クラスタピアリング

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。

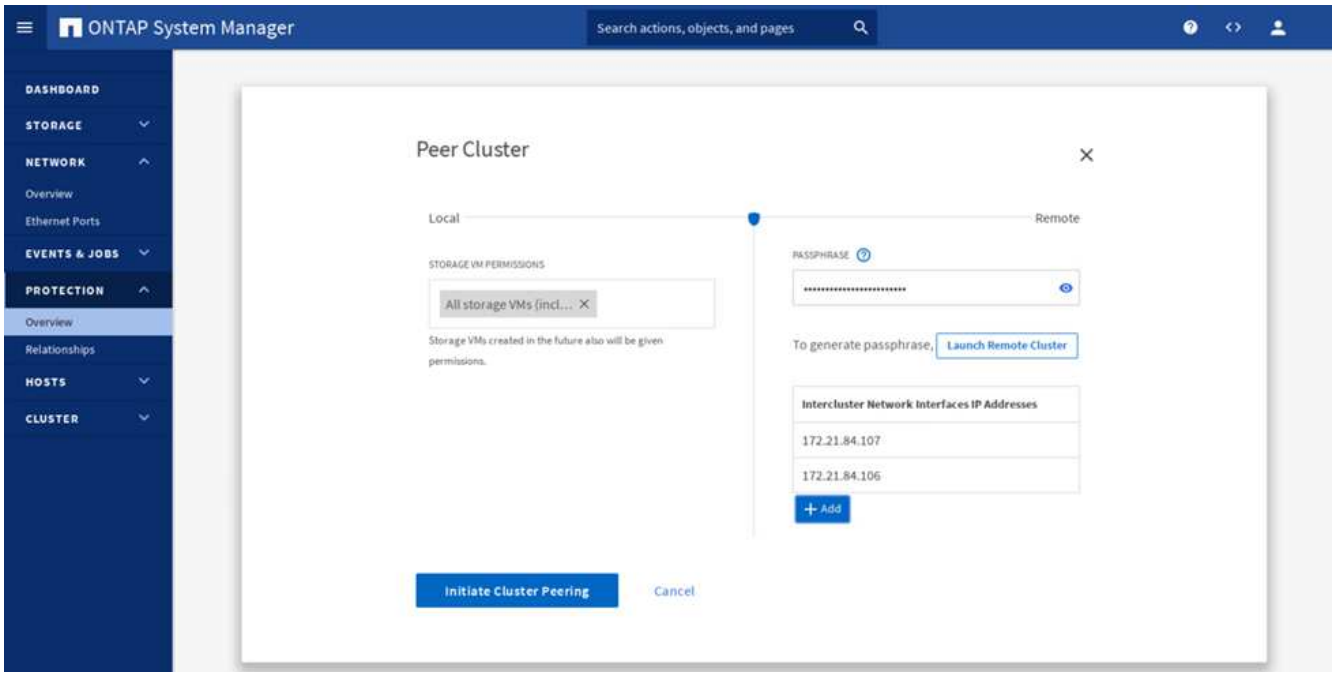


2 つのクラスタ間にピア関係を設定するには、次の手順を実行します。

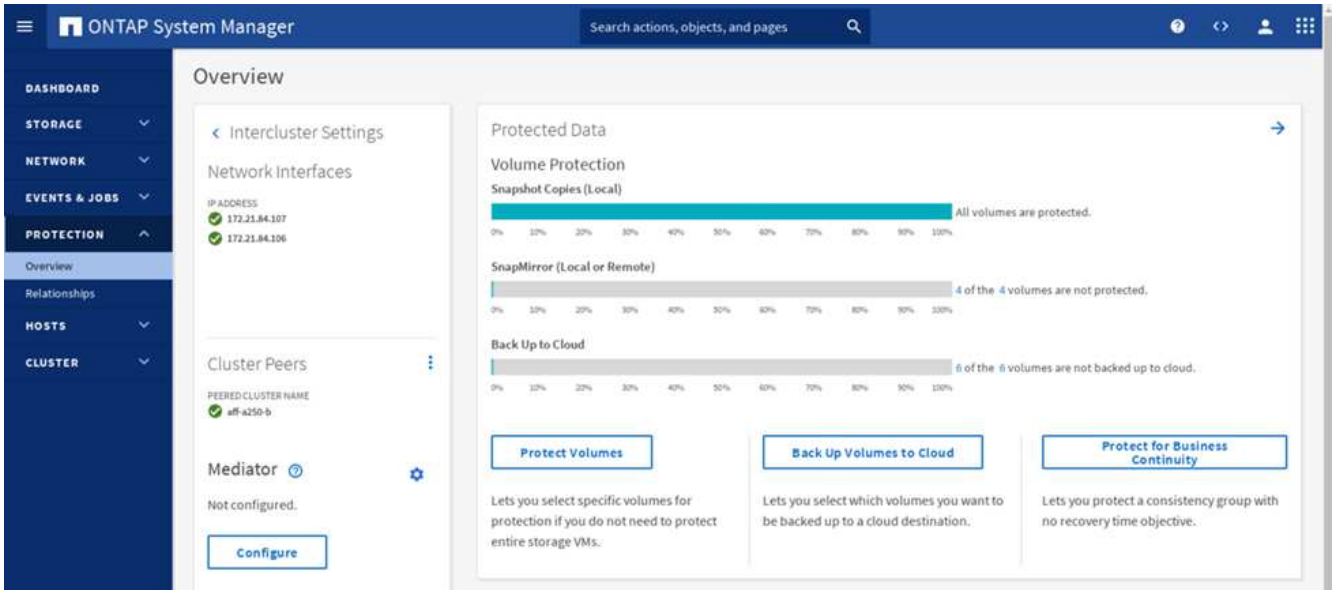
1. 1 つ目のクラスタでクラスタピアパスフレーズを生成



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。



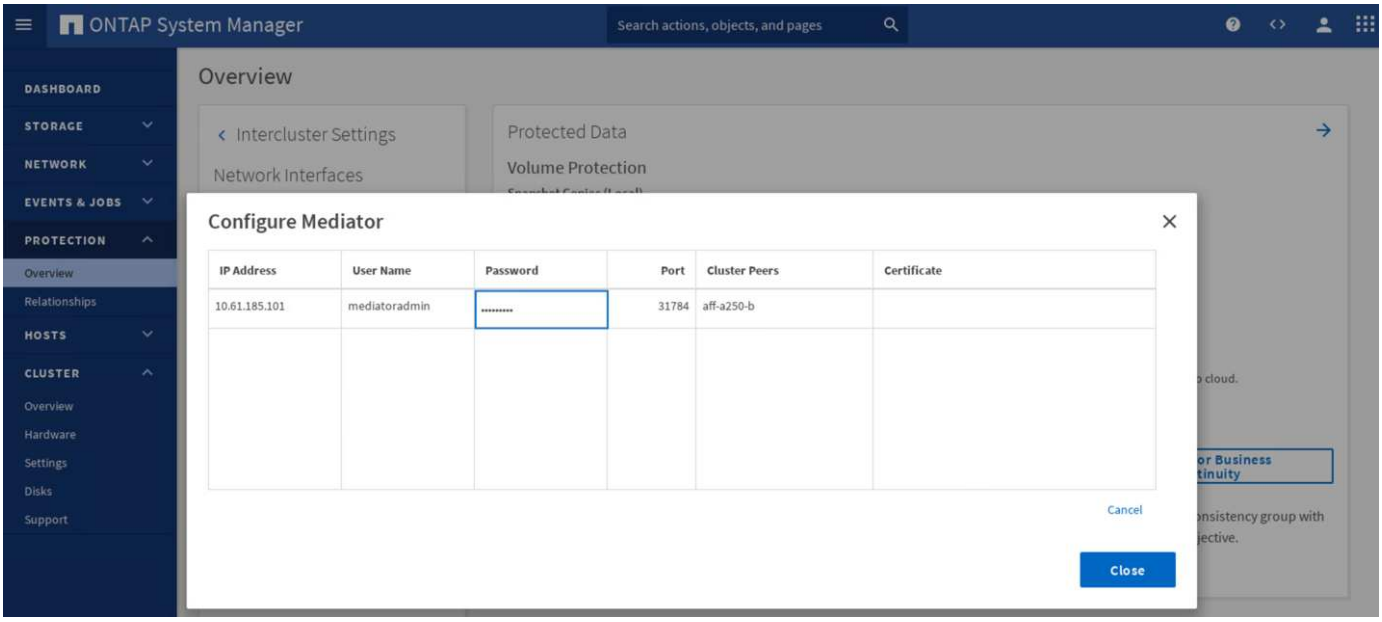
ONTAP メディエーターのインストールと設定

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。

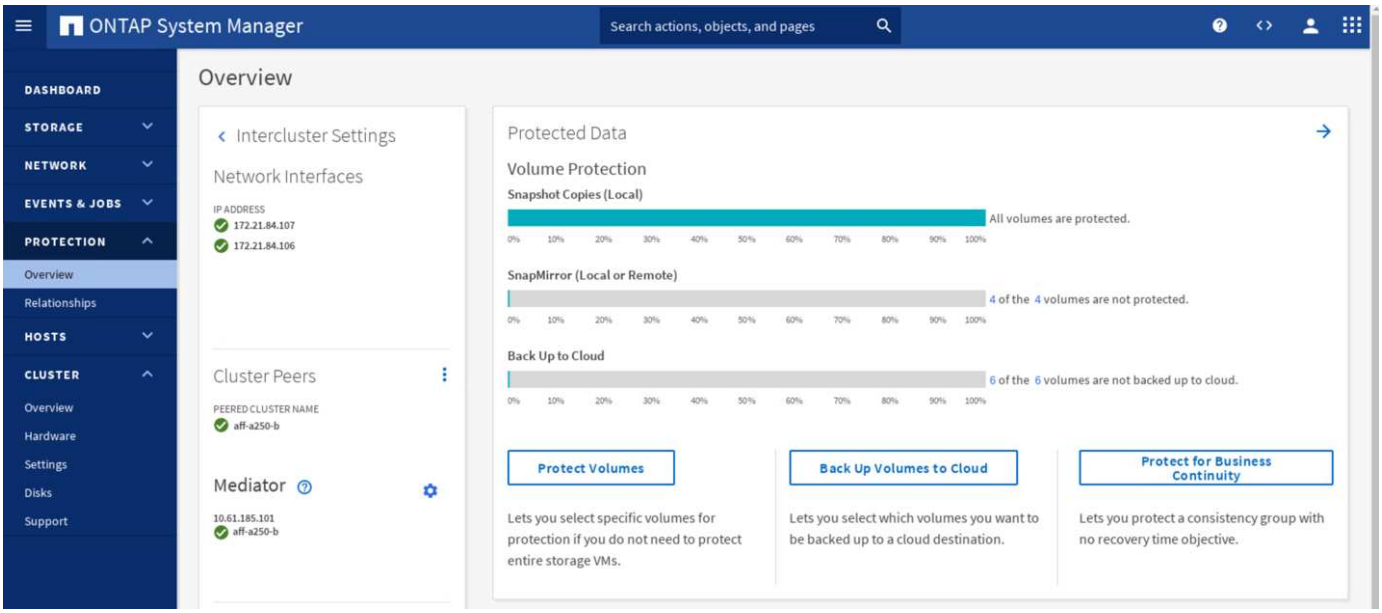
ONTAP メディエーターをインストールする前に、を確認します "ONTAP メディエーターサービスをインストールまたはアップグレードします" の各ページでは、前提条件、サポートされている Linux のバージョン、およびそれらをサポートされている各種 Linux オペレーティングシステムにインストールする手順について説明します。

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。



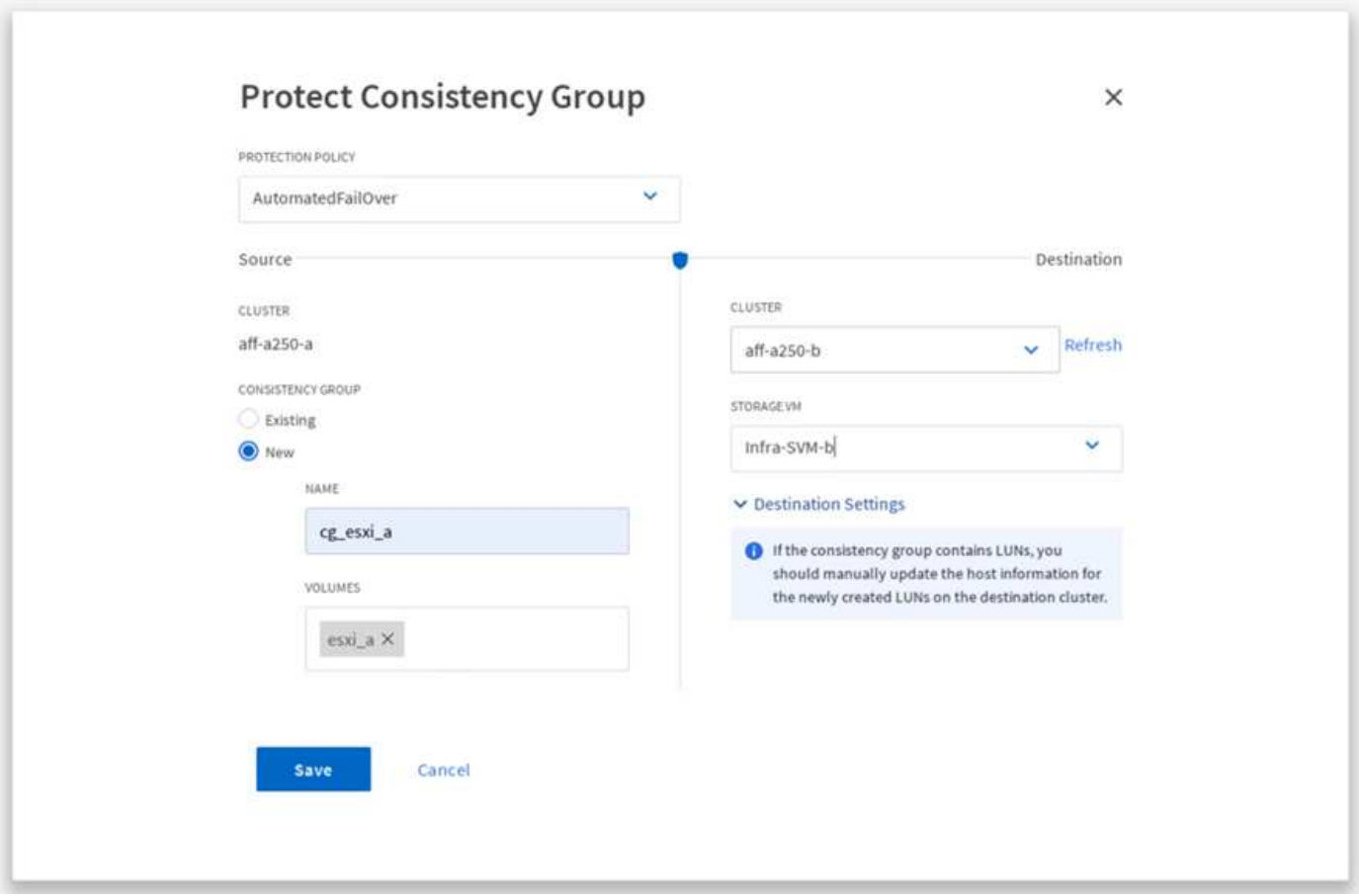
SM-BC 整合グループ

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。

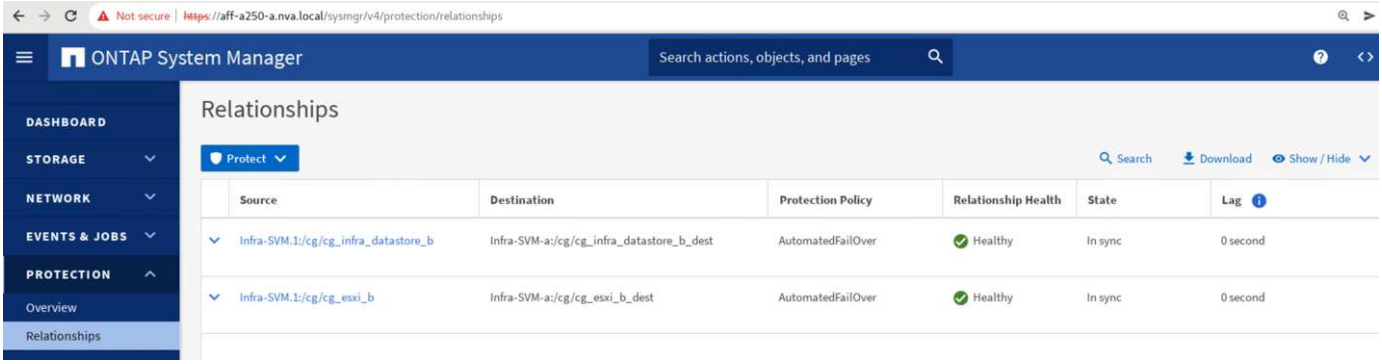


次の表に、検証テストで作成される 4 つの整合グループと各整合グループに含まれるボリュームを示します。

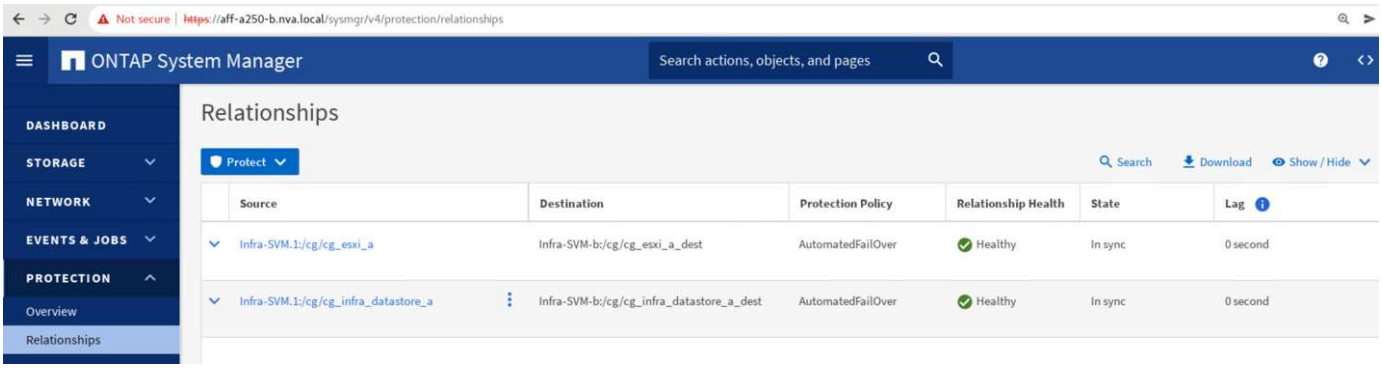
System Manager の略	整合グループ	個のボリューム
サイト A	CG_ESXi_a のようになります	esxi_a です
サイト A	cG_infra_a_a	infra_datastore_a_01 infra_a_02
サイト B	cG_esxi_b	esxi_b
サイト B	cG_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

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

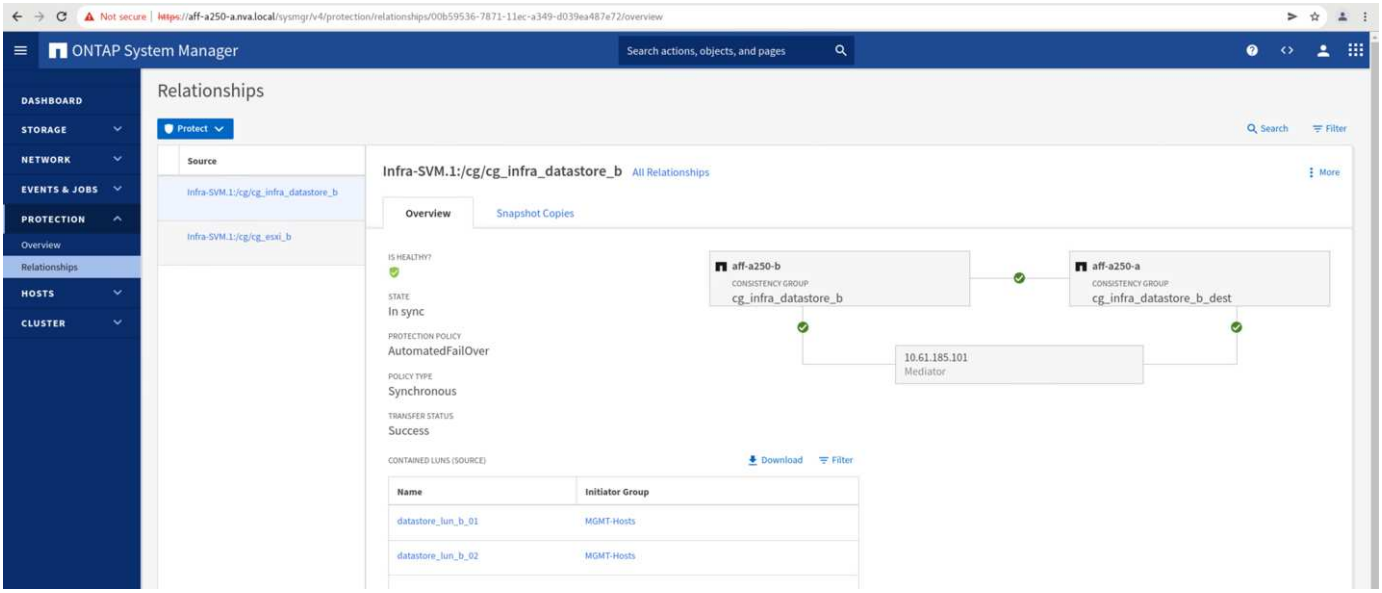
このスクリーンショットは、サイト A の整合グループ関係を示しています



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。"

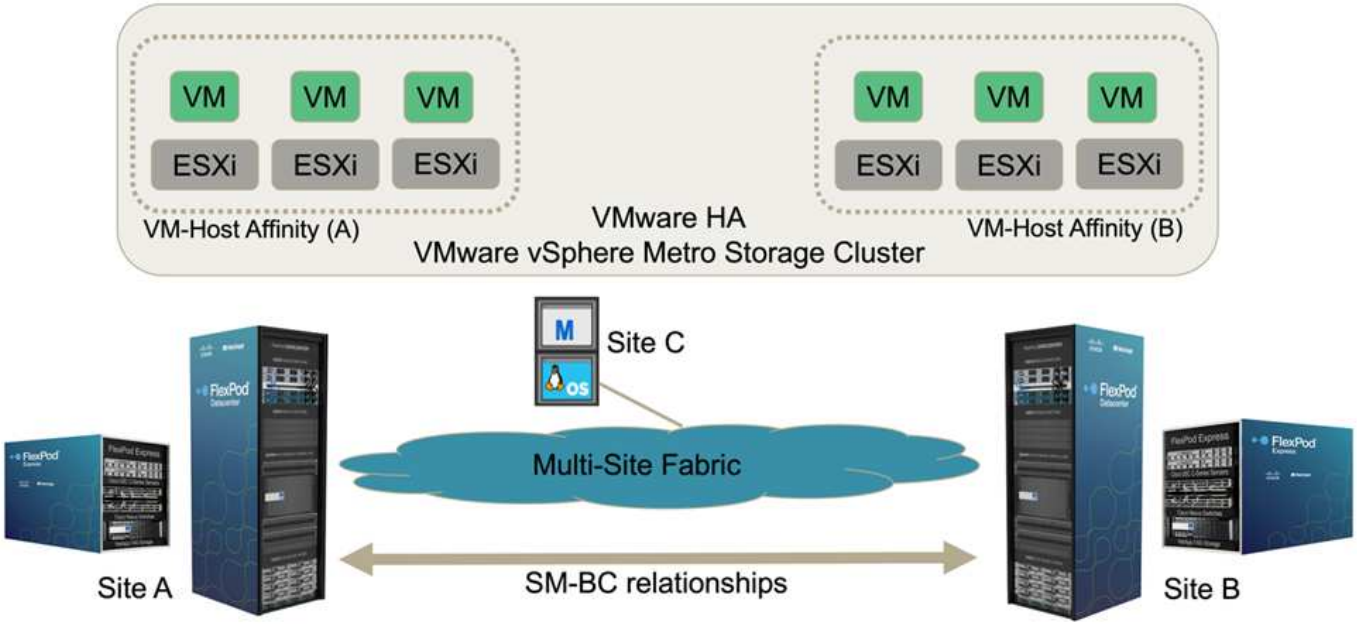
マルチサイトの FlexPod SM-BC 解決策 では、 1 つの VMware vCenter が解決策 全体の仮想インフラストラクチャリソースを管理します。両方のデータセンターのホストは、両方のデータセンターにまたがる単一の VMware HA クラスタに参加します。ホストは、 NetApp SM-BC 解決策 にアクセスできます。このでは、定義済みの SM-BC 関係にあるストレージに両方のサイトからアクセスできます。

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。

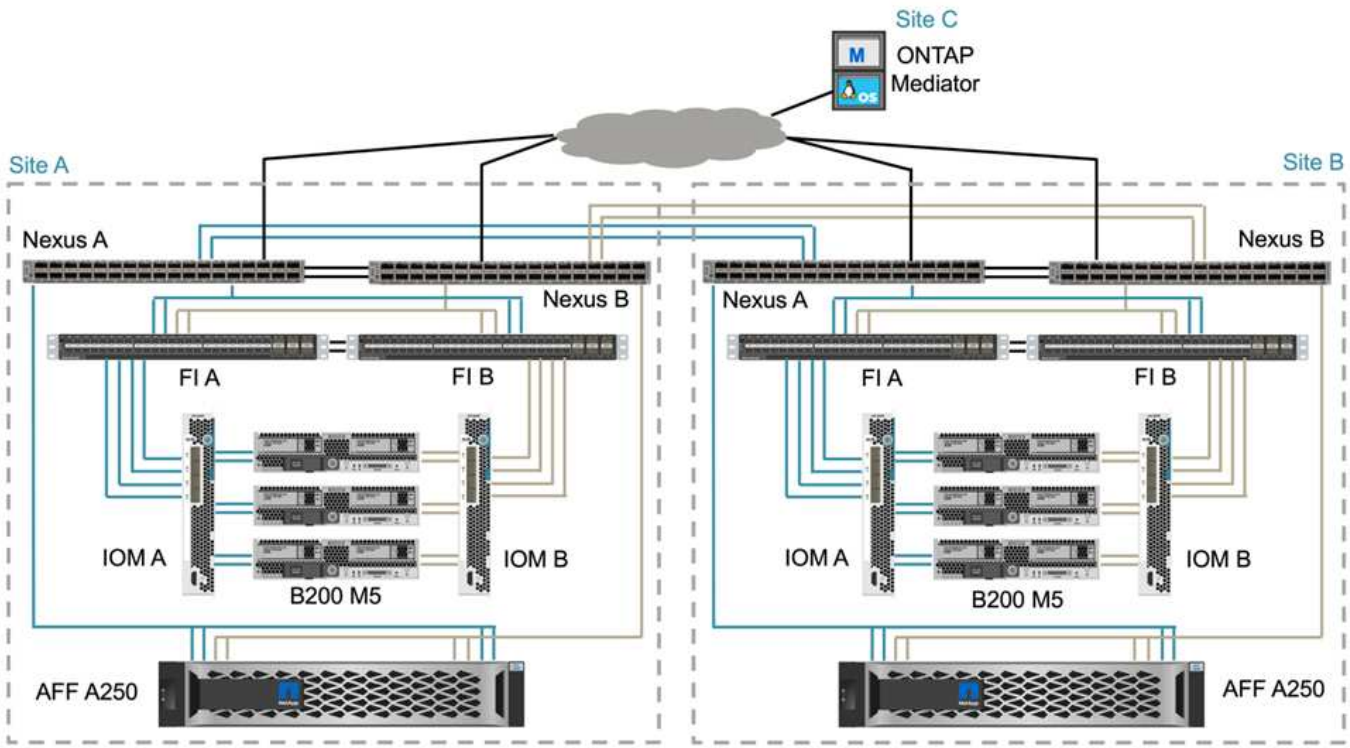
ただし、両方のサイトで VM を実行できる構成では、リモートサイトのホストで VMware HA によって VM を再起動し、解決策 の耐障害性を確保できます。両方のサイトで仮想マシンを実行する場合は、サイト間で仮想マシンの vMotion を円滑に実行するために、すべての ESXi ホストに iSCSI 共有データストアをマウントする必要があります。

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。



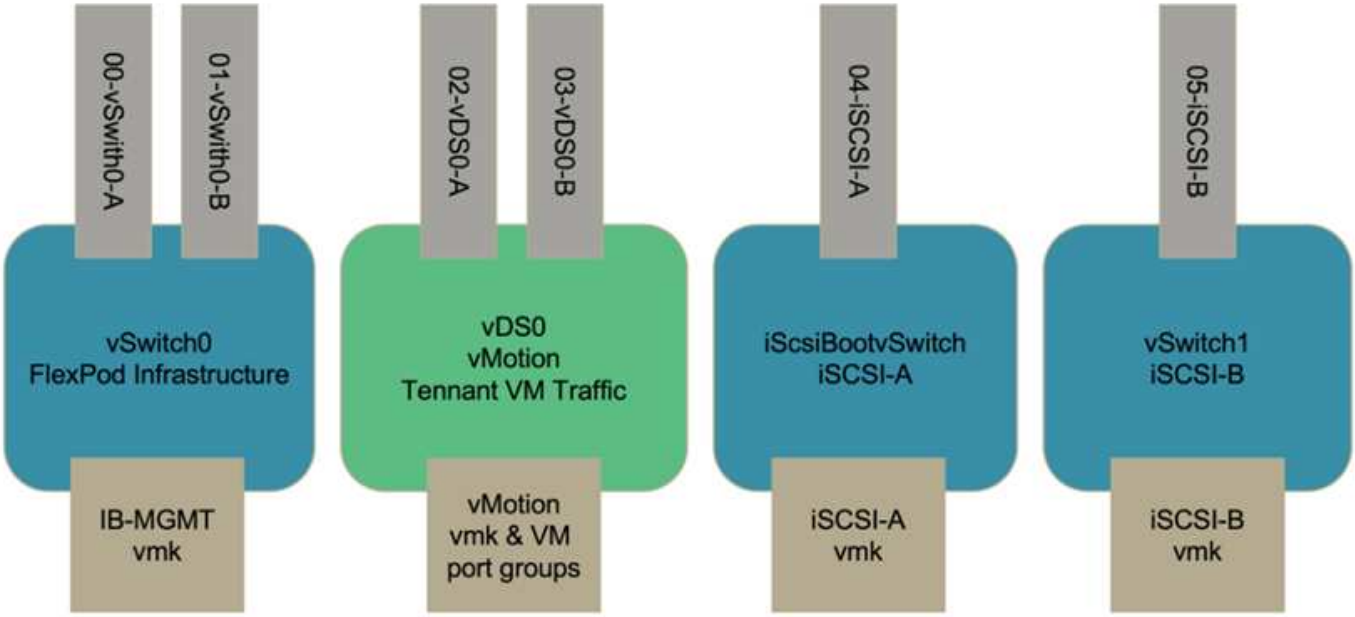
FlexPod の導入アーキテクチャは、この解決策 検証で各サイトで同じです。ただし、解決策 は非対称型の導入をサポートしており、要件を満たす既存の FlexPod ソリューションに追加することもできます。

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。

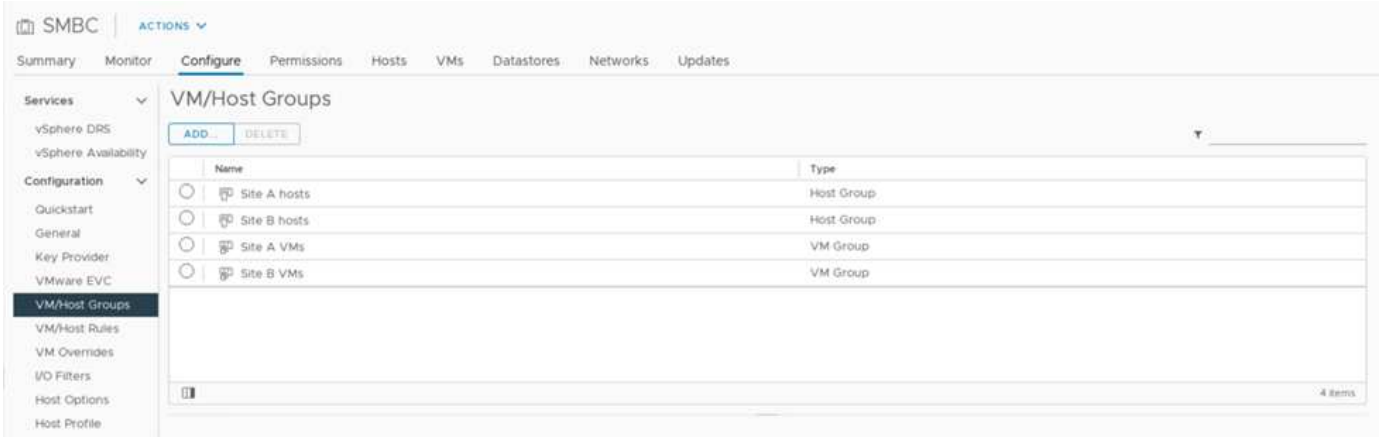
VM とホストのアフィニティグループとルール

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。

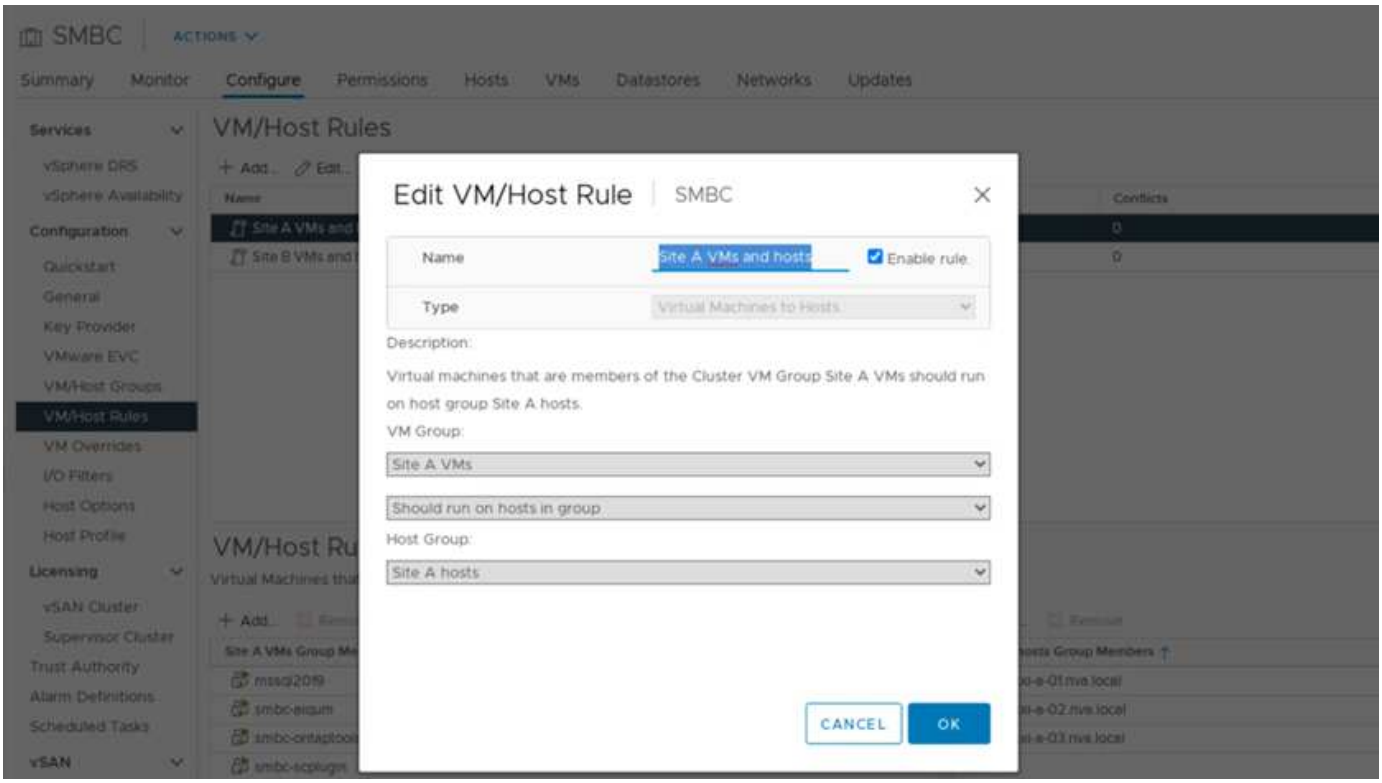
ローカルデータストアを使用する仮想マシンの場合、仮想ディスクがリモートサイトのホストに移行されると、仮想ディスクへのアクセスがリモートになり、サイト間の物理的な距離による読み取り処理のレイテンシが増加します。そのため、ローカルホストに仮想マシンを保持し、サイトでローカルストレージを利用することを推奨します。

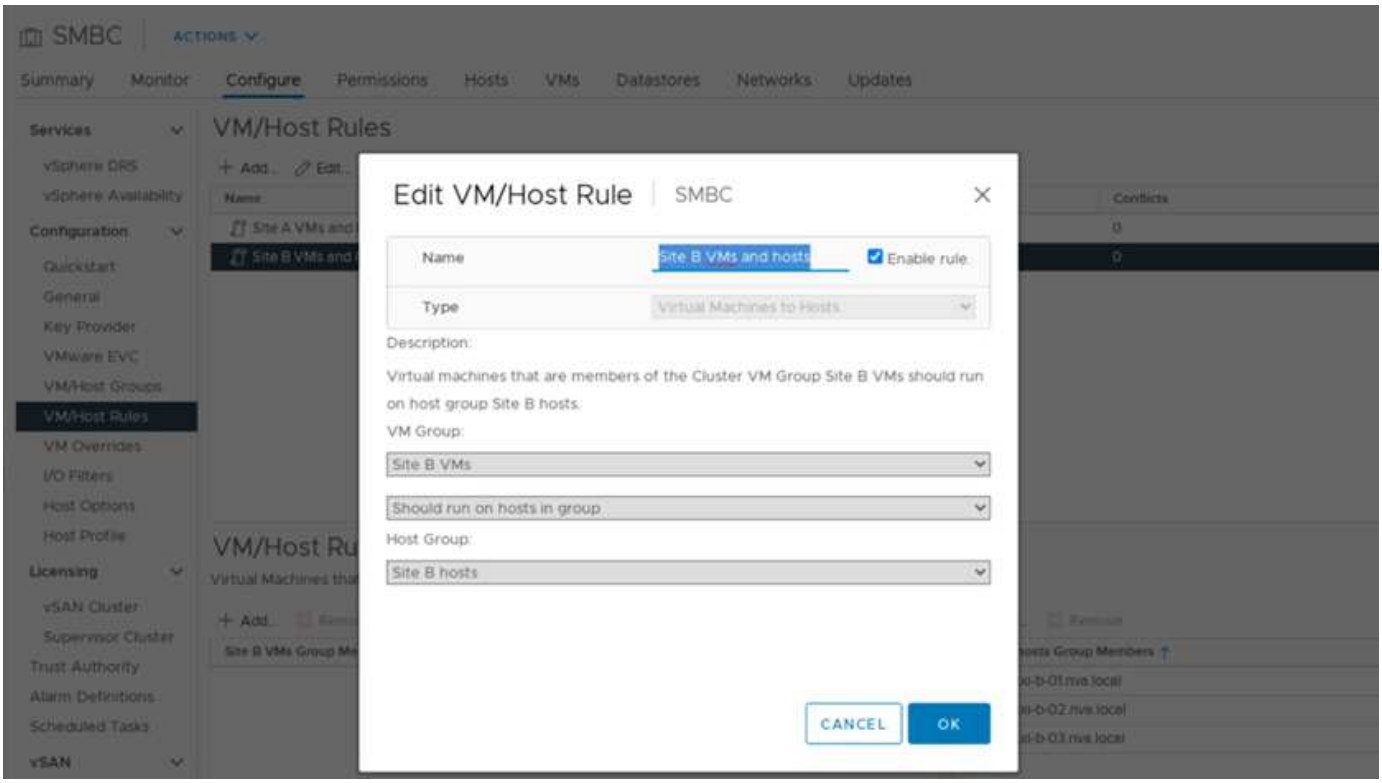
VM とホストのアフィニティメカニズムを使用すると、 VM / ホストグループを作成して、特定のサイトに配置された仮想マシンとホストの VM グループとホストグループを作成できます。VM/ ホストルールを使用して、 VM とホストが従うポリシーを指定できます。サイトのメンテナンスまたは災害時にサイト間で仮想マシンを移行できるようにするには、その柔軟性のため、「グループ内のホストで実行する」ポリシー仕様を使用します。

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。

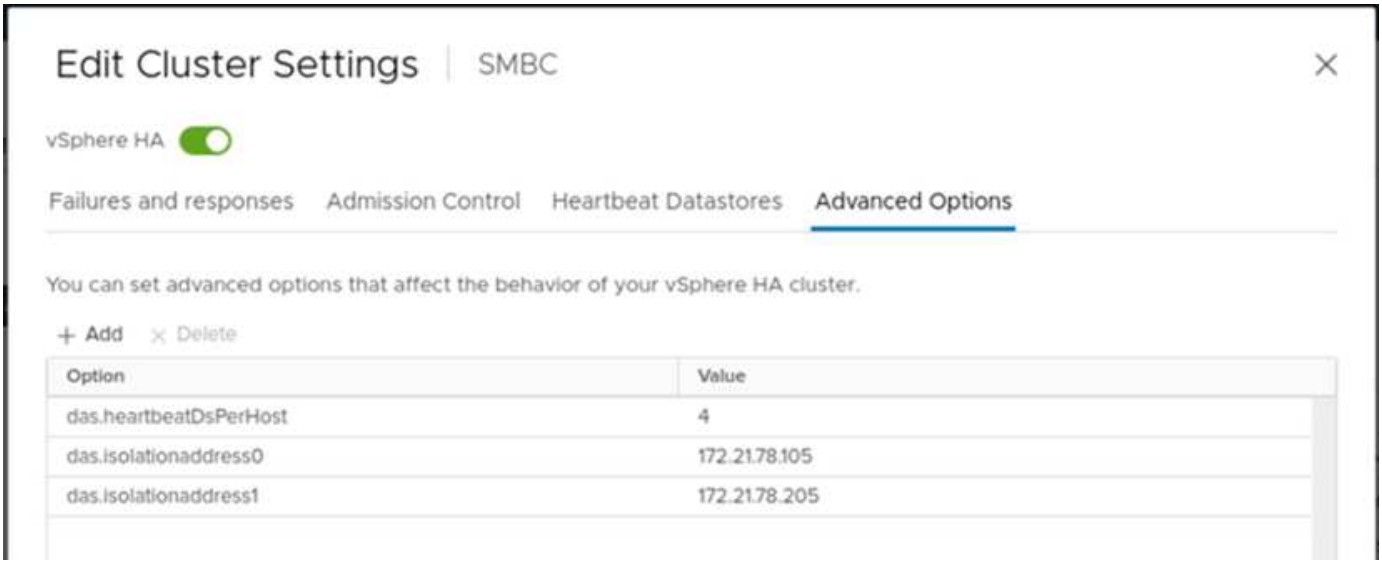




vSphere HA ハートビート

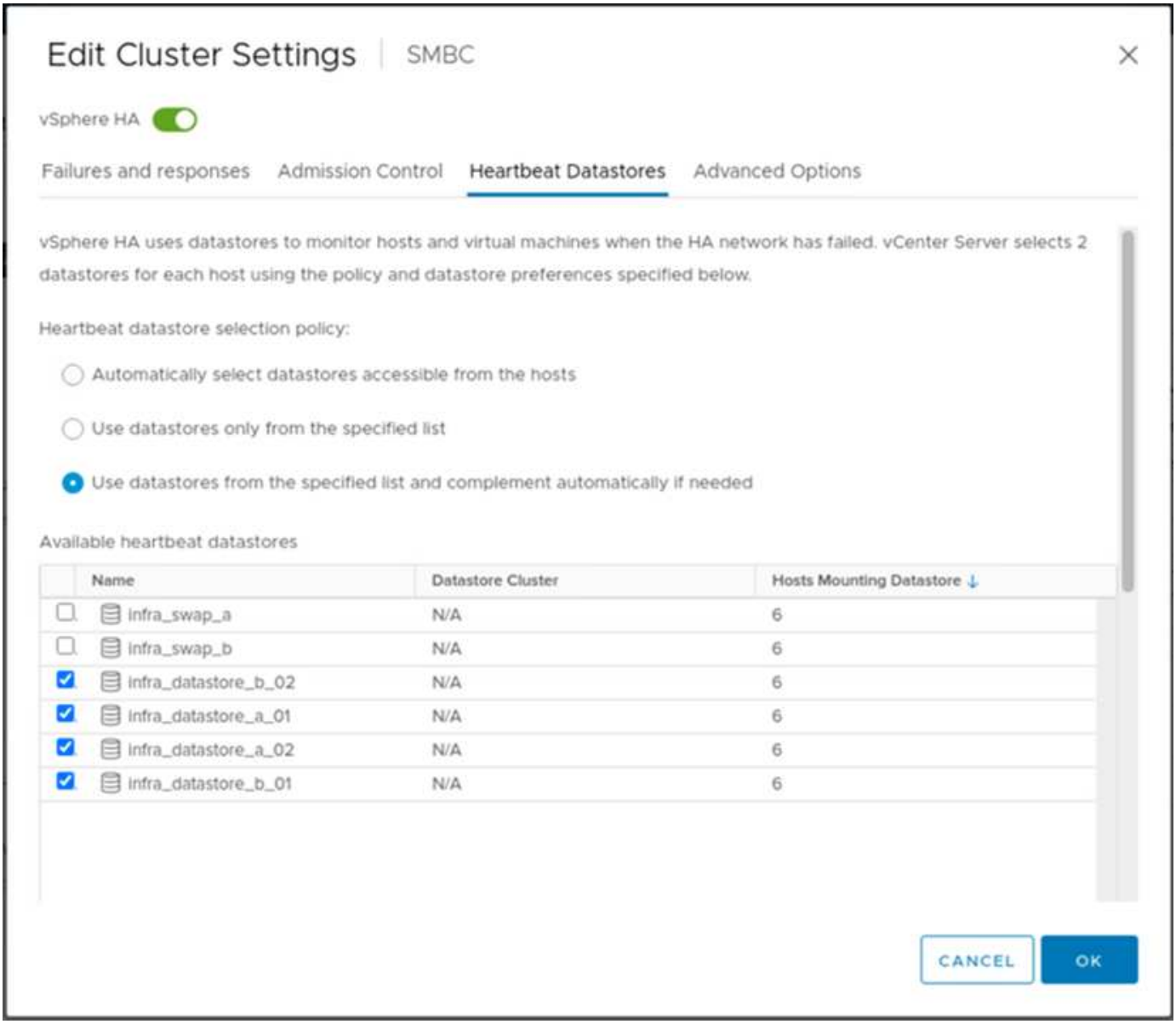
VMware vSphere HA は、ホストの状態を検証するためのハートビートメカニズムを備えています。一次ハートビートメカニズムはネットワーク経由で行われ、二次ハートビートメカニズムはデータストアを経由します。ハートビートを受信しない場合は、デフォルトゲートウェイに ping を送信するか、手動で設定した隔離アドレスに基づいて、ハートビートをネットワークから隔離するかを決定します。データストアのハートビートでは、ストレッチクラスタのハートビートデータストアを最小構成から 4 つに増やすことを推奨します。

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

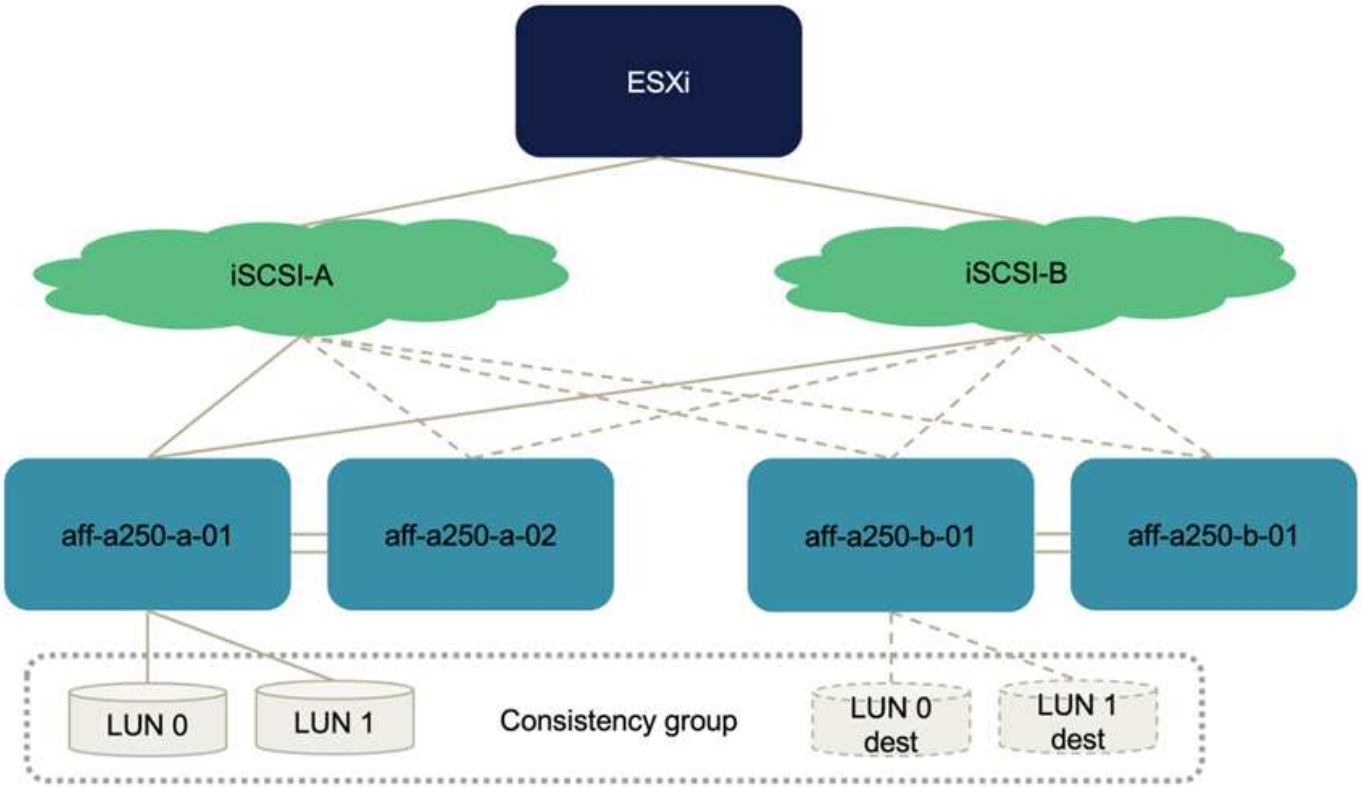
解決策 内の ESXi ホストは、 iSCSI SAN からブートするように設定されます。SAN ブートを使用すると、サーバを交換する際のサーバ管理が簡素化されます。これは、サーバのサービスプロファイルを新しいサーバに関連付けて、サーバが起動するために追加の設定変更を行う必要がないためです。

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。

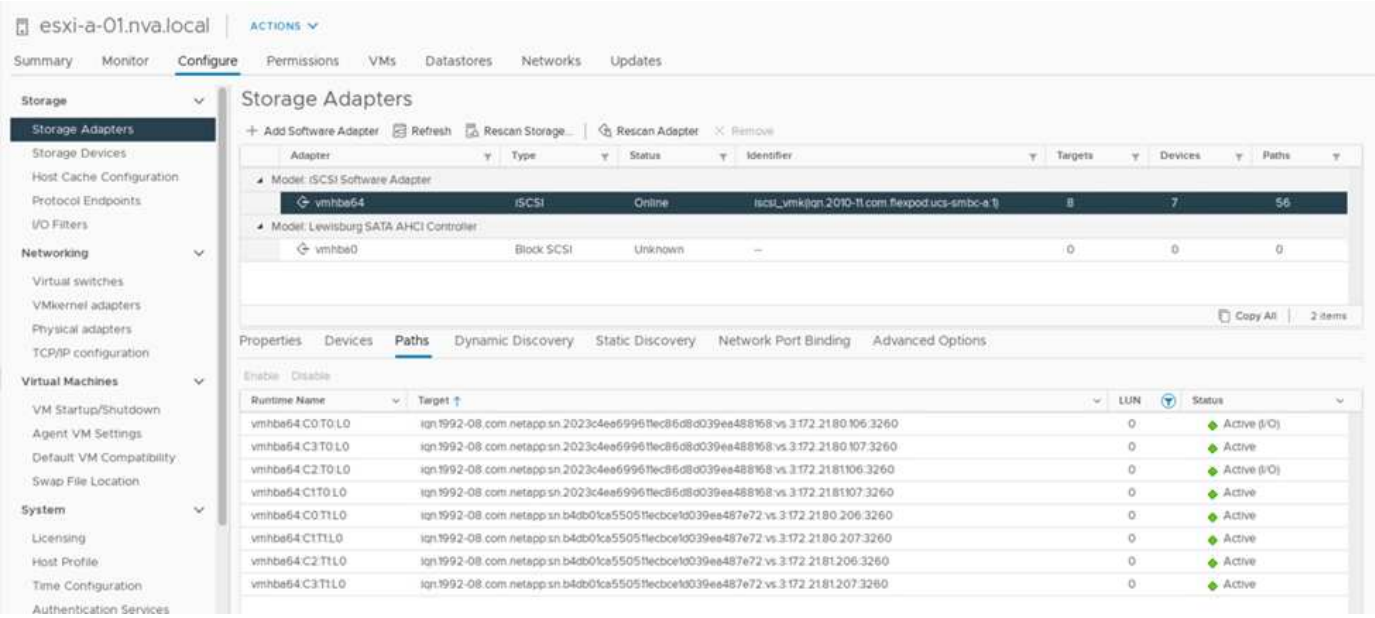
SM-BC 整合グループ関係を設定する前に、ストレージコントローラ HA ペアでホストされる iSCSI LUN には、ベストプラクティスの実装に基づいて、各 iSCSI ファブリックに 2 つずつ、合計 4 つのパスがあります。ホストは、 2 つの iSCSI VLAN / ファブリック経由で LUN にアクセスでき、 LUN ホスティングコントローラやコントローラのハイアベイラビリティパートナー経由で LUN にアクセスできます。

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。

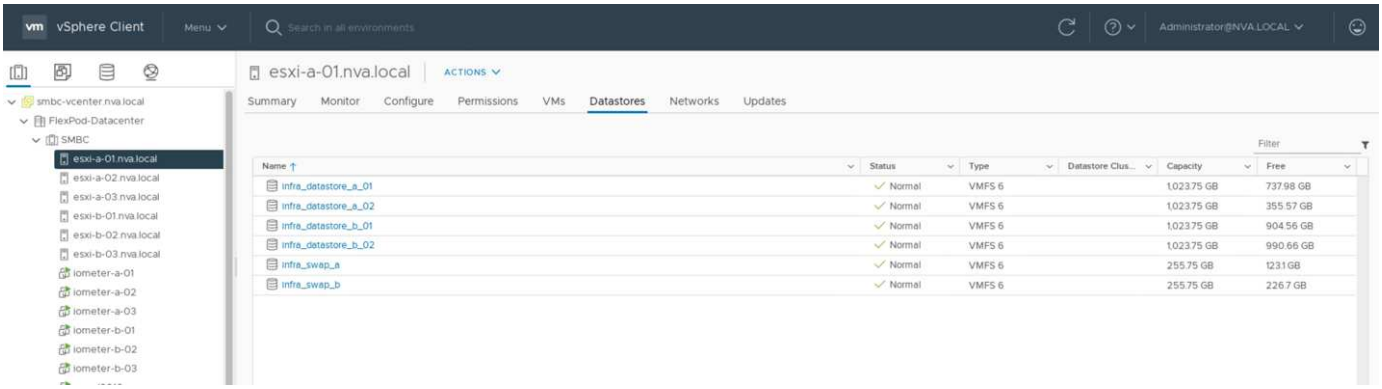
VMware vMotion と **VM** とホストのアフィニティテスト

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。

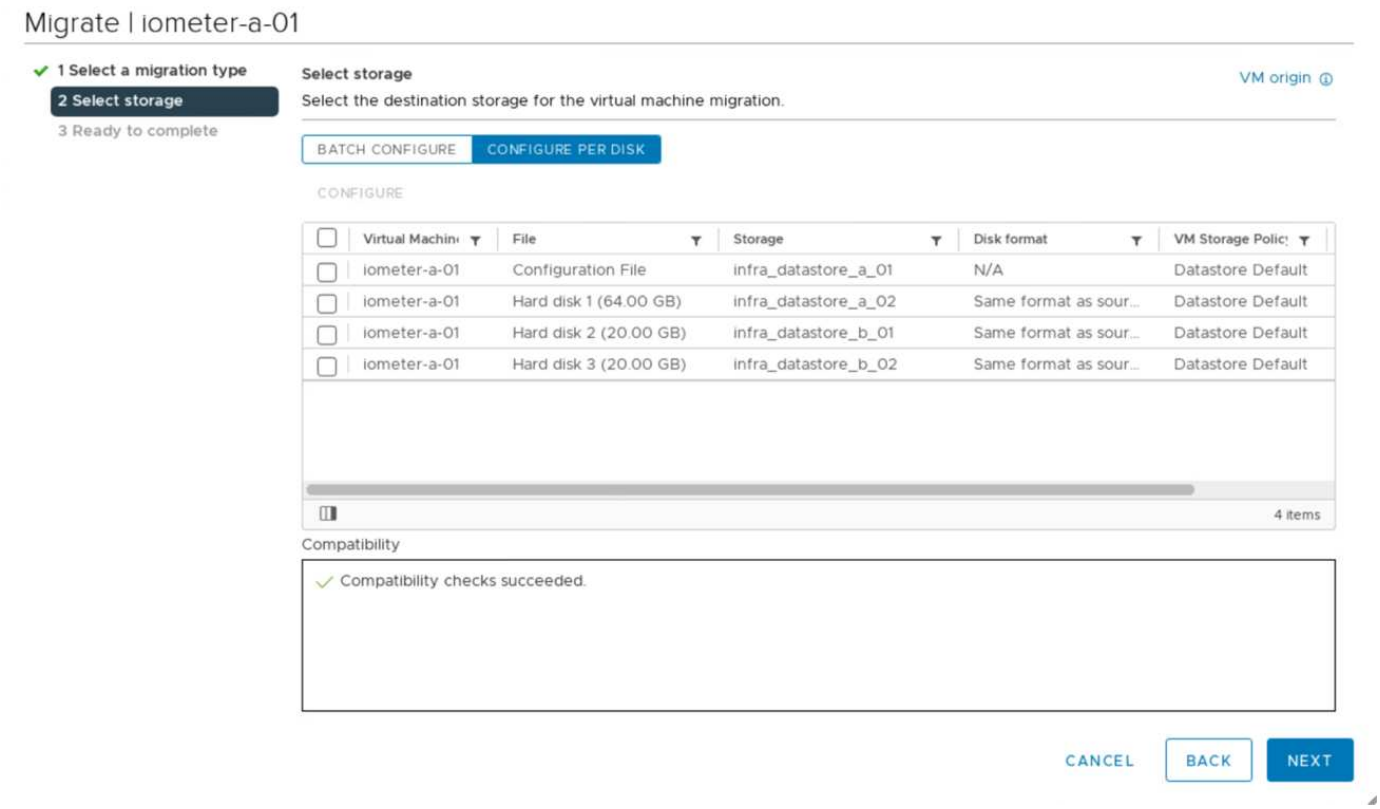
いずれかの SM-BC サイトのストレージサービスを仮想マシンで使用できるようにするには、 2 つのサイト間で仮想マシンを移行したり、災害時のフェイルオーバー・シナリオに備えて、両方のサイトの iSCSI データストアをクラスタ内のすべてのホストにマウントする必要があります。

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。



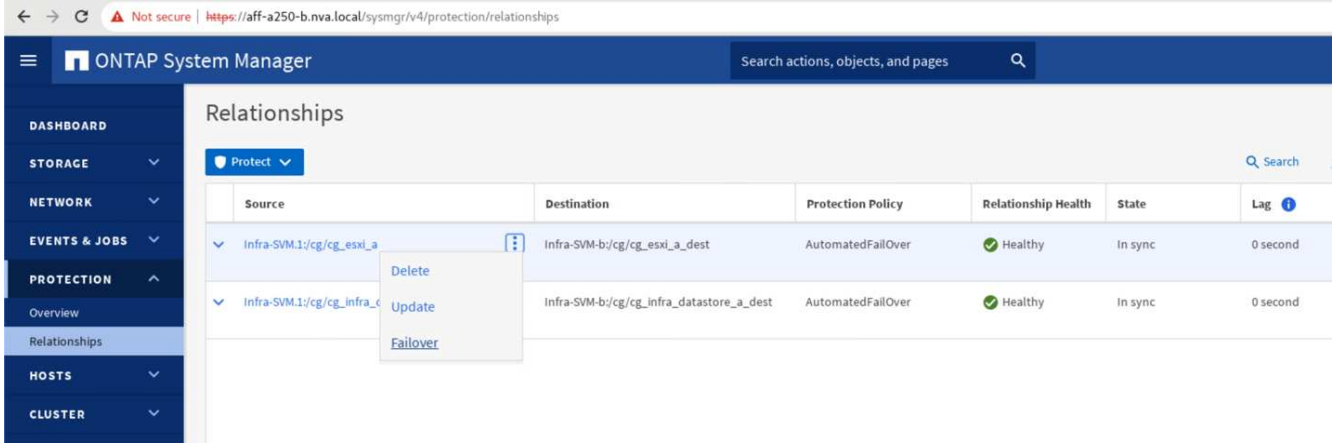
同じサイトにある別のホスト、およびサイト間で仮想マシンの vMotion をテストし、正常に実行された。サイト間で仮想マシンを手動で移行すると、 VM とホストのアフィニティルールがアクティブになり、仮想マシンが通常の状態にあるグループに移行されます。

ストレージのフェイルオーバーを計画

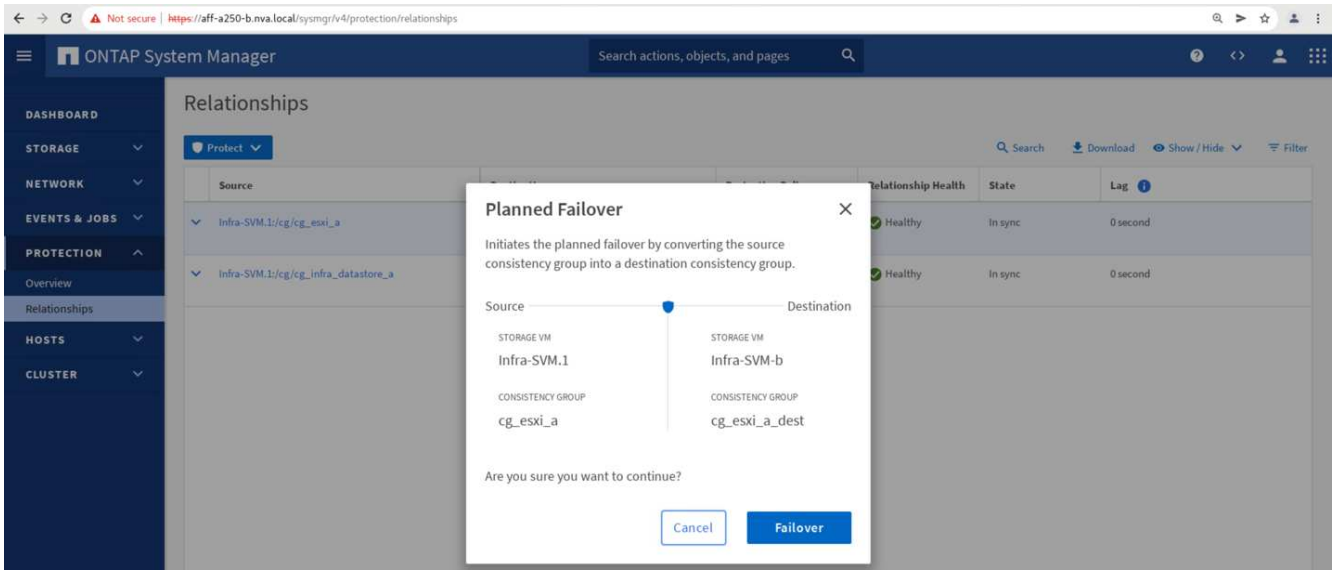
ストレージフェイルオーバー後に解決策 が適切に機能しているかどうかを確認するには、初期設定後に解決策 で計画的なストレージフェイルオーバー処理を実行する必要があります。このテストは、 I/O の停止を招く可能性のある接続や構成の問題を特定するのに役立ちます。接続や設定の問題を定期的にテストして解決することで、実際のサイトで障害が発生してもデータサービスを中断なく提供できます。計画的ストレージフェイルオーバーは、スケジュールされたストレージメンテナンスアクティビティの前にも使用できます。これにより、影響を受けないサイトからデータサービスを提供できます。

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。

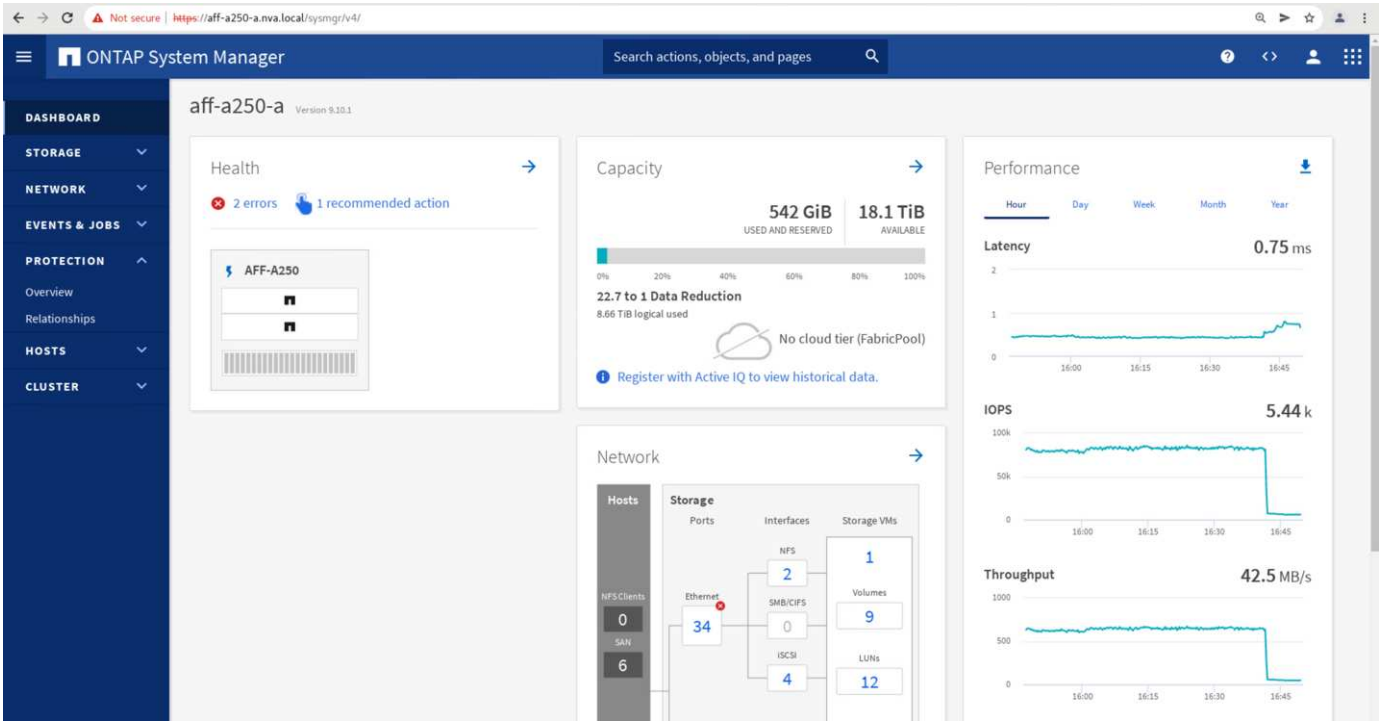
1. Protection > Relationships 画面に移動して ' コンシステンシ・グループの関係状態が In Sync' であることを確認しますまだ「同期中」状態の場合は、状態が「同期中」になるまで待ってからフェイルオーバーを実行します。
2. ソース名の横にあるドットを展開し、フェイルオーバーをクリックします。



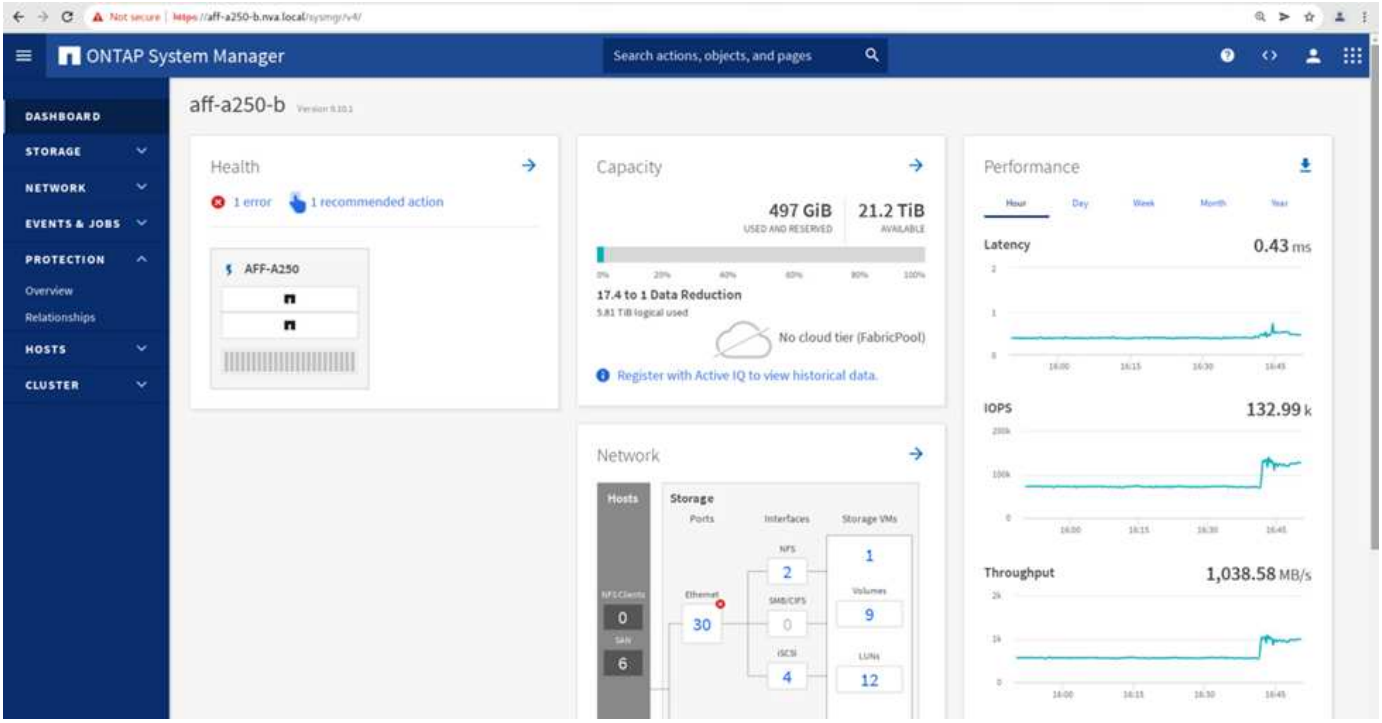
3. 処理を開始するには、フェイルオーバーを確認してください。



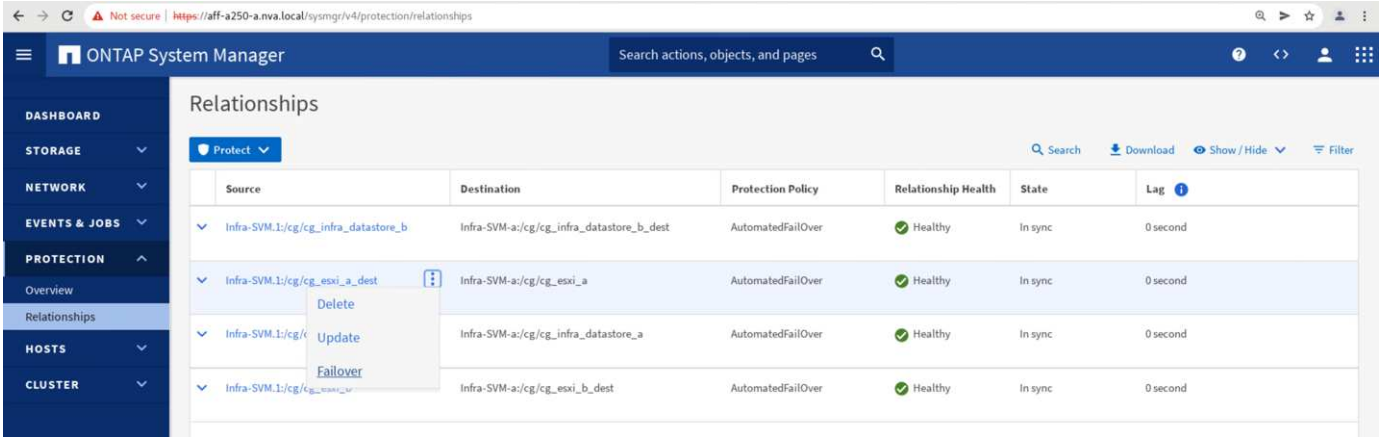
2 つのコンシステンシグループ「 cg_esxi_a 」および「 cg_infra_datastore_a 」のフェイルオーバーがサイト B の System Manager GUI で開始された直後に、これら 2 つのコンシステンシグループを処理するサイト A の I/O がサイト B に移動されましたそのため、サイト A の System Manager のパフォーマンスペインでは、サイト A の I/O が大幅に削減されました。



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。

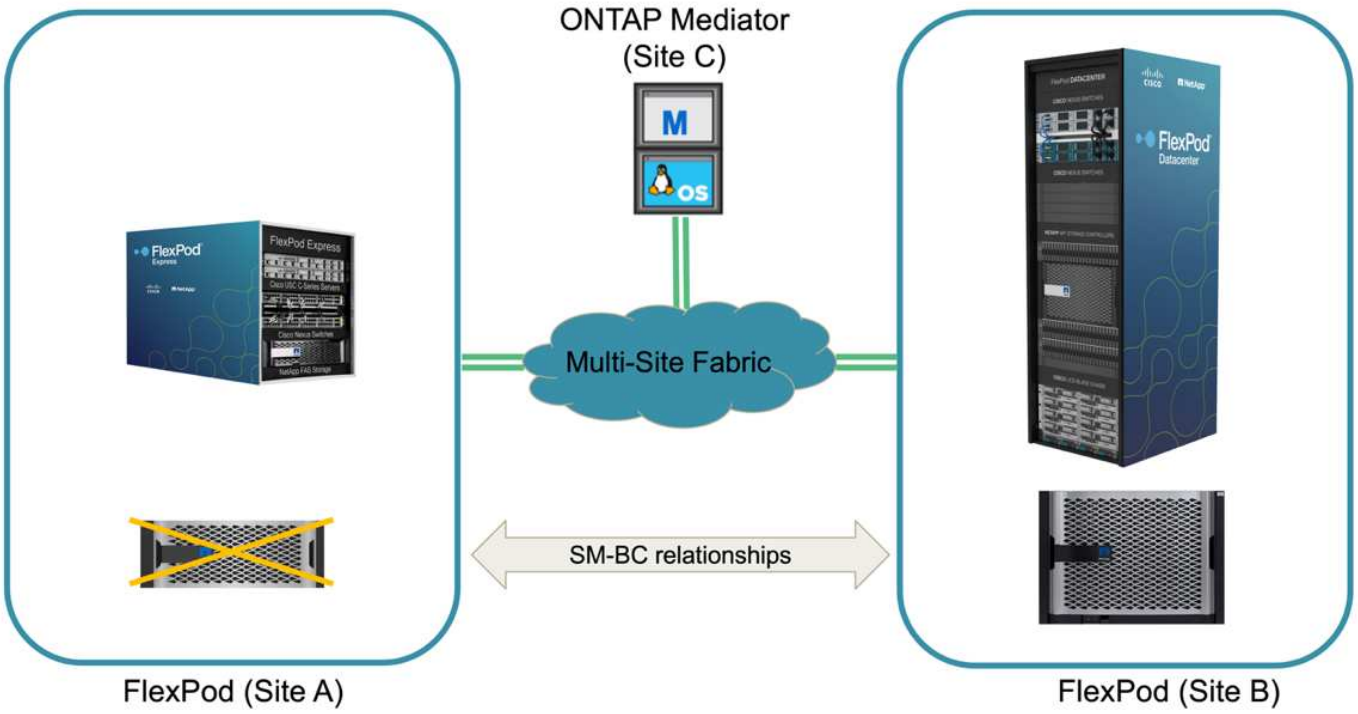


I/O をサイト A からサイト B に透過的に移行することで、計画的なメンテナンスのためにサイト A のストレージコントローラを停止できるようになります。メンテナンス作業またはテストが完了し ' サイト A のストレージ・クラスタが稼働状態に戻ったら ' フェイルオーバーを実行してサイト B からサイト A へのフェイルオーバー I/O を返す前に ' コンシステンシ・グループの保護状態が同期状態に戻るまでチェックして待機します メンテナンスまたはテストのためにサイトが停止される時間が長くなると ' データが同期されるまでの時間が長くなり ' コンシステンシ・グループは同期状態に戻ります



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

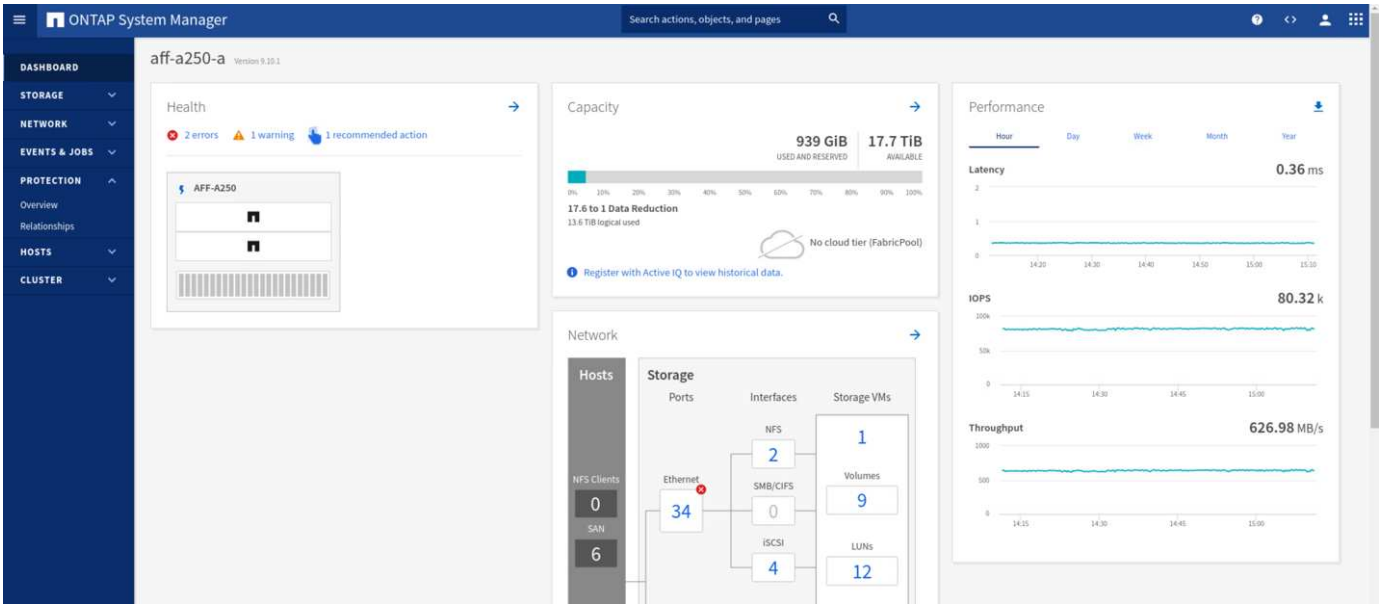


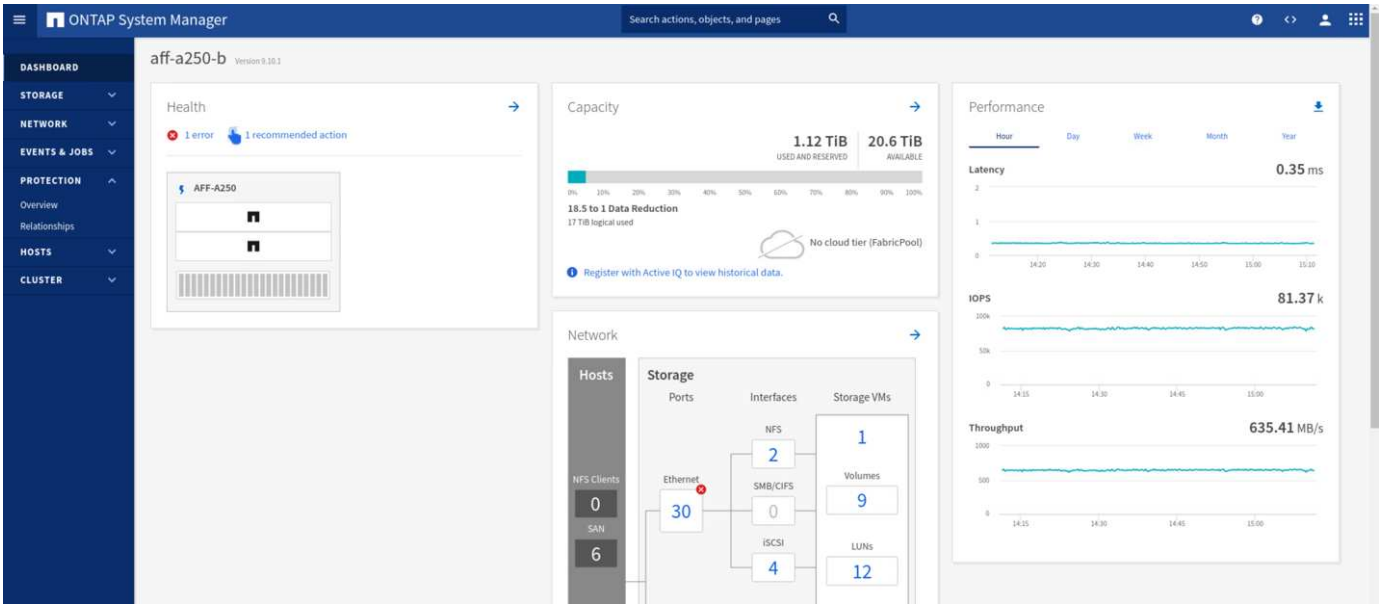
サイト A でストレージ災害をシミュレートするために、サイト A の両方のストレージコントローラの電源スイッチを物理的にオフにしてコントローラへの電源供給を停止することで、両方のコントローラの電源をオフにできます。 または、ストレージコントローラのサービスプロセッサの system power management コマンドを使用してコントローラの電源をオフにします。

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

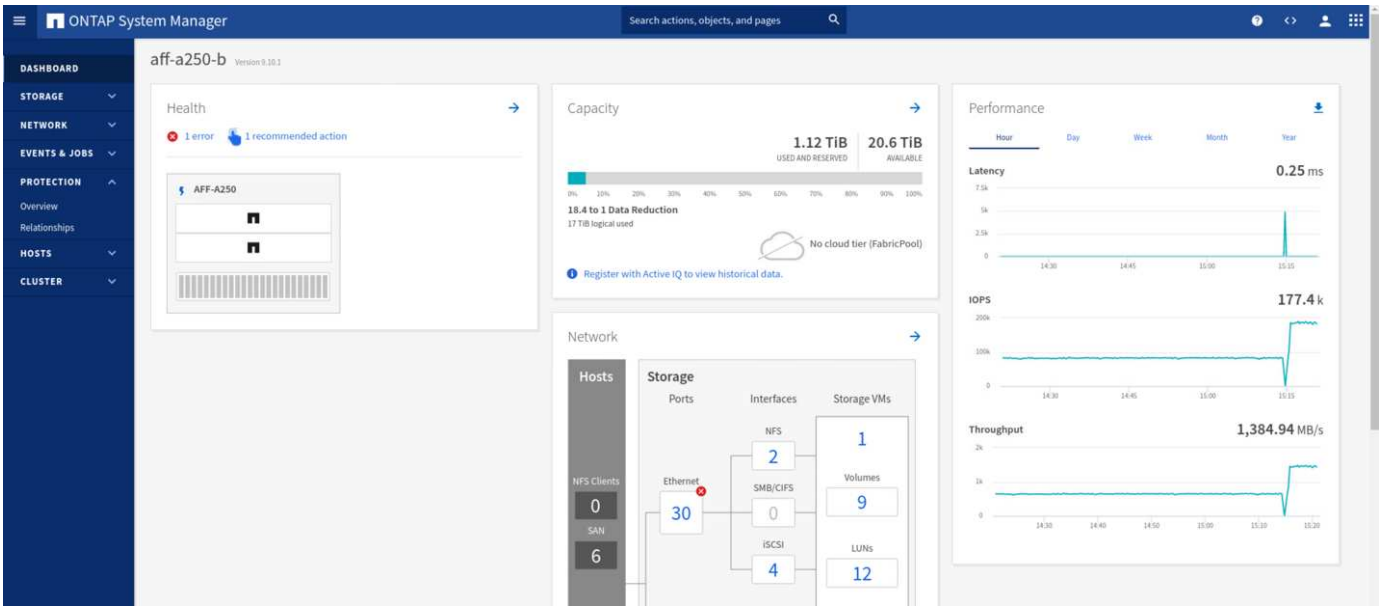
アプリケーション側では、オペレーティングシステムが LUN のパスステータスを確認し、稼働しているサイト B のストレージコントローラへの利用可能なパスで I/O を再開する間、データサービスは一時的に停止します。

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。

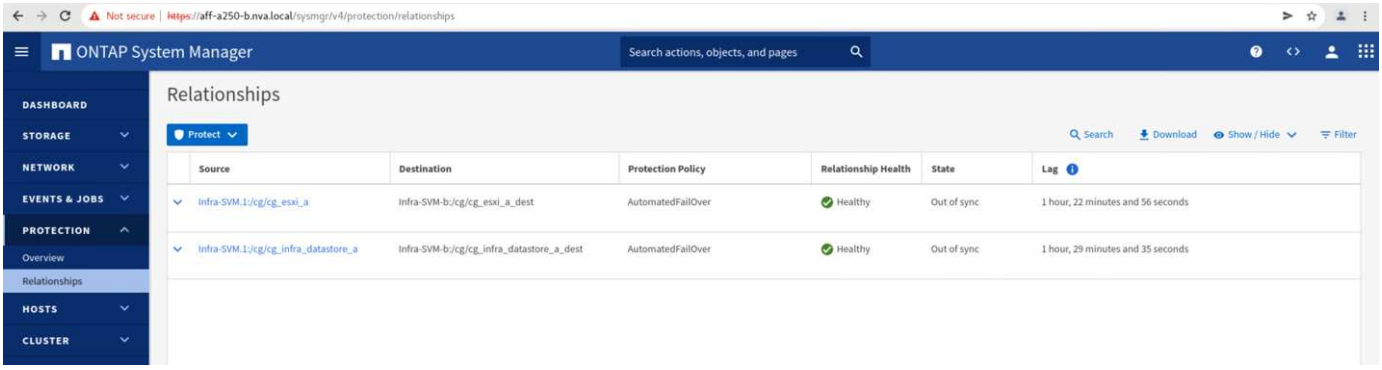




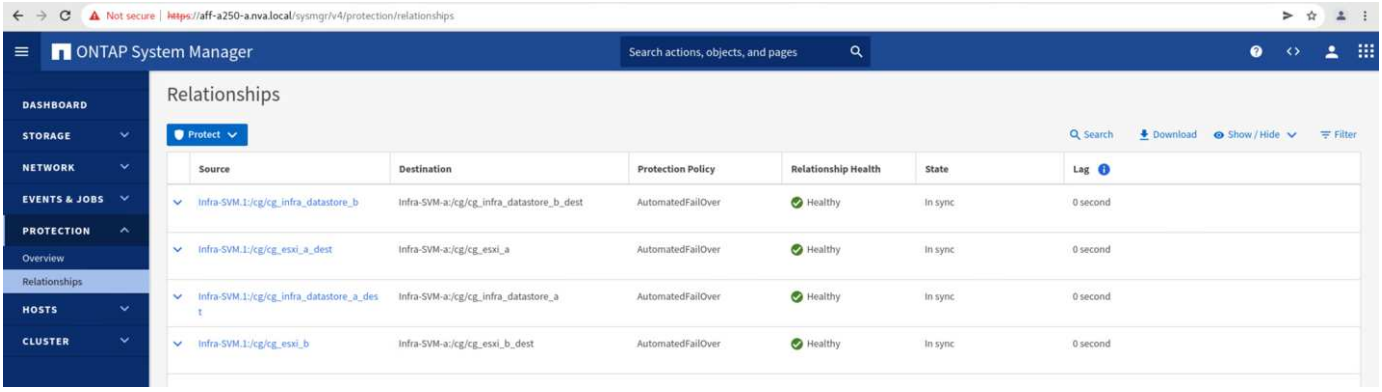
サイト A のストレージコントローラの電源をオフにしたあと、サイト A に代わって追加のデータサービスを提供するために、サイト B のストレージコントローラの I/O が大幅に増加したことを視覚的に確認できます（次の図を参照）。また、 IOMeter VM の GUI には、サイト A のストレージクラスタが停止しても I/O が継続することが示されました。SM-BC 関係で保護されていない LUN から作成されたデータストアがほかにもある場合、ストレージ災害の発生時にこれらのデータストアにアクセスできなくなります。そのため、さまざまなアプリケーションデータのビジネスニーズを評価し、ビジネス継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

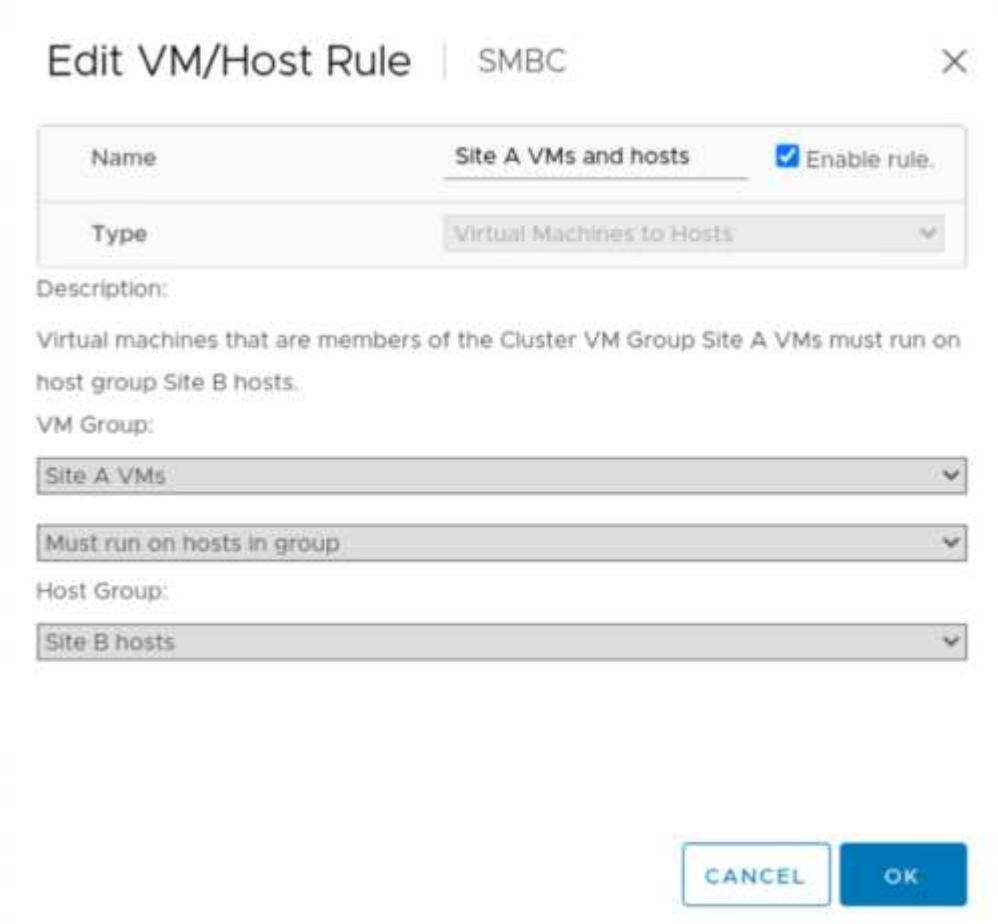


サイトのメンテナンスや停電が発生したり、ハリケーンや地震などの自然災害によって影響が及ぶ可能性があります。そのため、計画的および計画外のサイト障害シナリオを実施して、 FlexPod SM-BC 解決策 が、ビジネスクリティカルなすべてのアプリケーションおよびデータサービスでこのような障害が発生しても運用を継続できるように適切に設定されていることを確認することが重要です。検証されたサイト関連のシナリオは次のとおりです。

- 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。

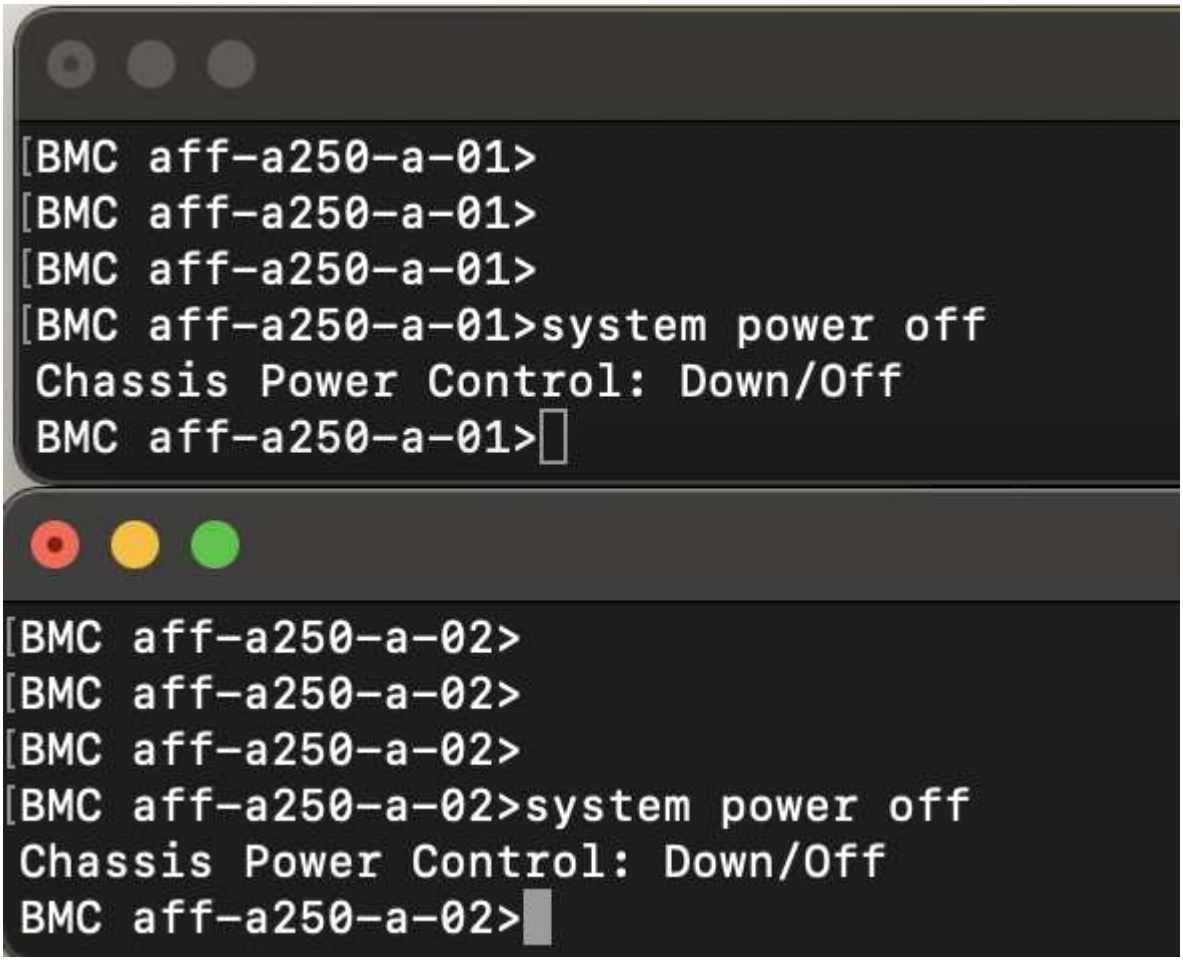
計画的な移行を実行する前に、 VM とホストのアフィニティルールを更新して、サイトで現在実行されている VM がメンテナンス中のサイトから自動的に移行されるようにします。次のスクリーンショットは、サイト A の VM とホストのアフィニティルールを変更し、サイト A からサイト B に VM を自動的に移行する例を示しています。VM をサイト B で実行するように指定する代わりに、アフィニティルールを一時的に無効にして VM を手動で移行することもできます。



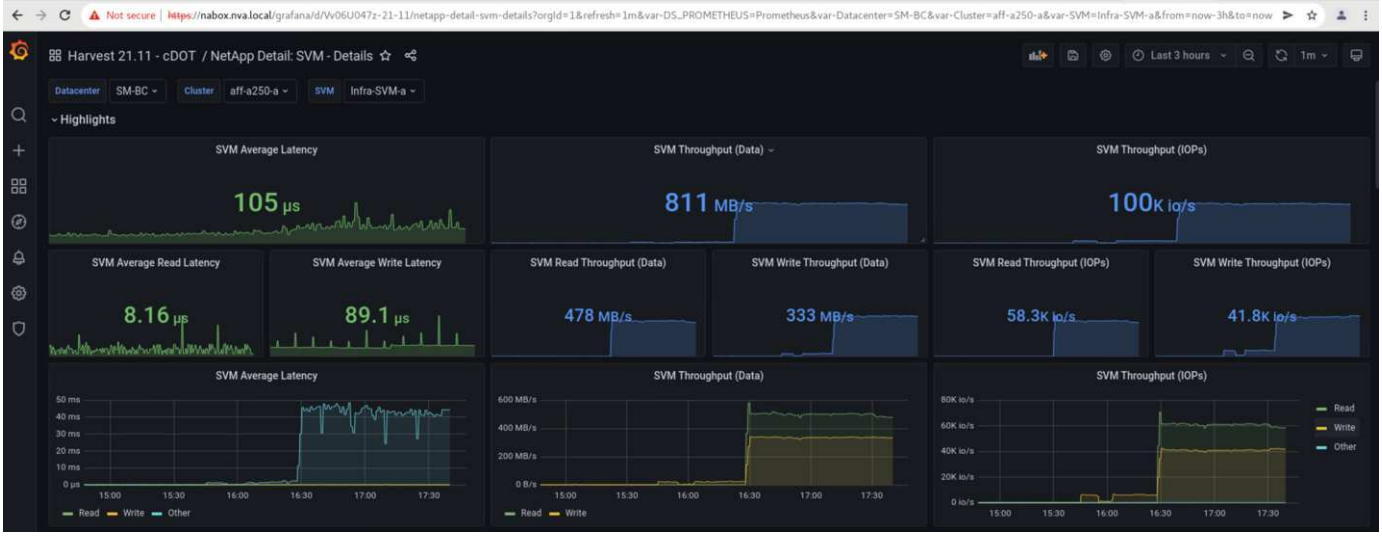
仮想マシンとストレージサービスの移行が完了したら、サーバ、ストレージコントローラ、ディスクシェルフ、およびスイッチの電源をオフにし、必要なサイトのメンテナンス作業を実行できます。サイトのメンテナンスが完了し、 FlexPod インスタンスが稼働状態に戻ったら、 VM のホストグループのアフィニティを変更して元のサイトに戻すことができます。その後、「グループ内のホストで実行する必要があります」 VM/ ホストサイトアフィニティルールを「グループ内のホストで実行する必要があります」に戻して、災害が発生した場合に、他のサイトのホストで仮想マシンを実行できるようにします。検証テストでは、すべての仮想マ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。

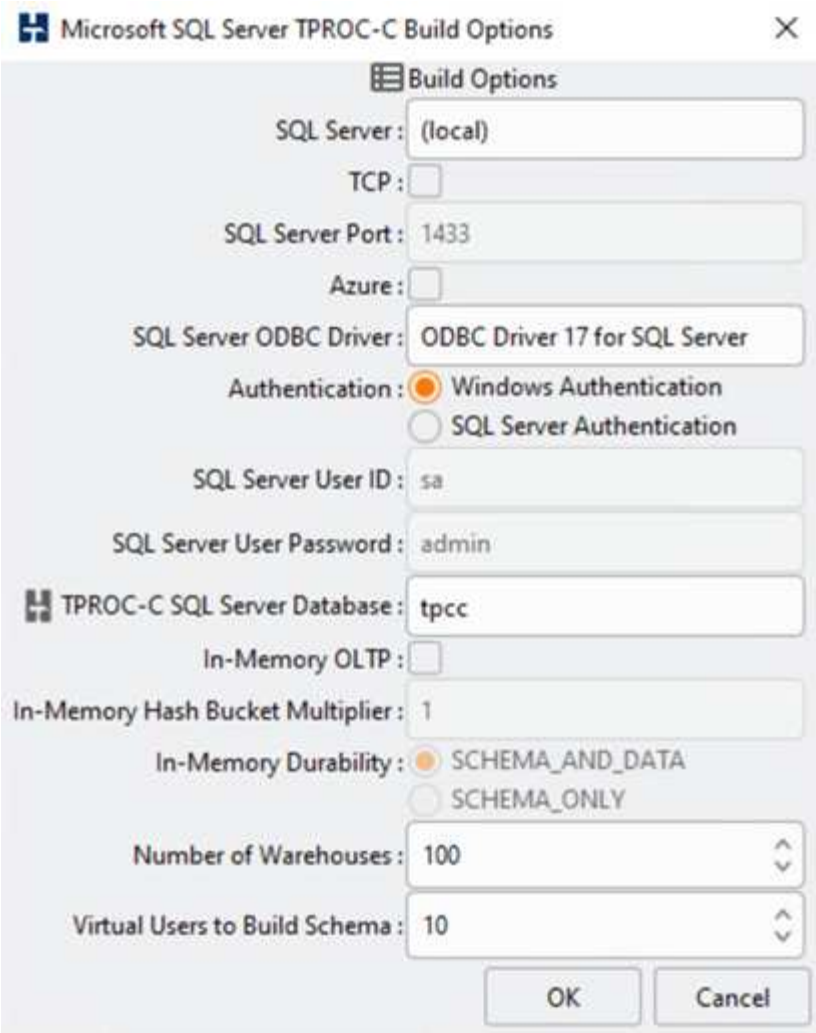


Microsoft SQL Server の場合

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。

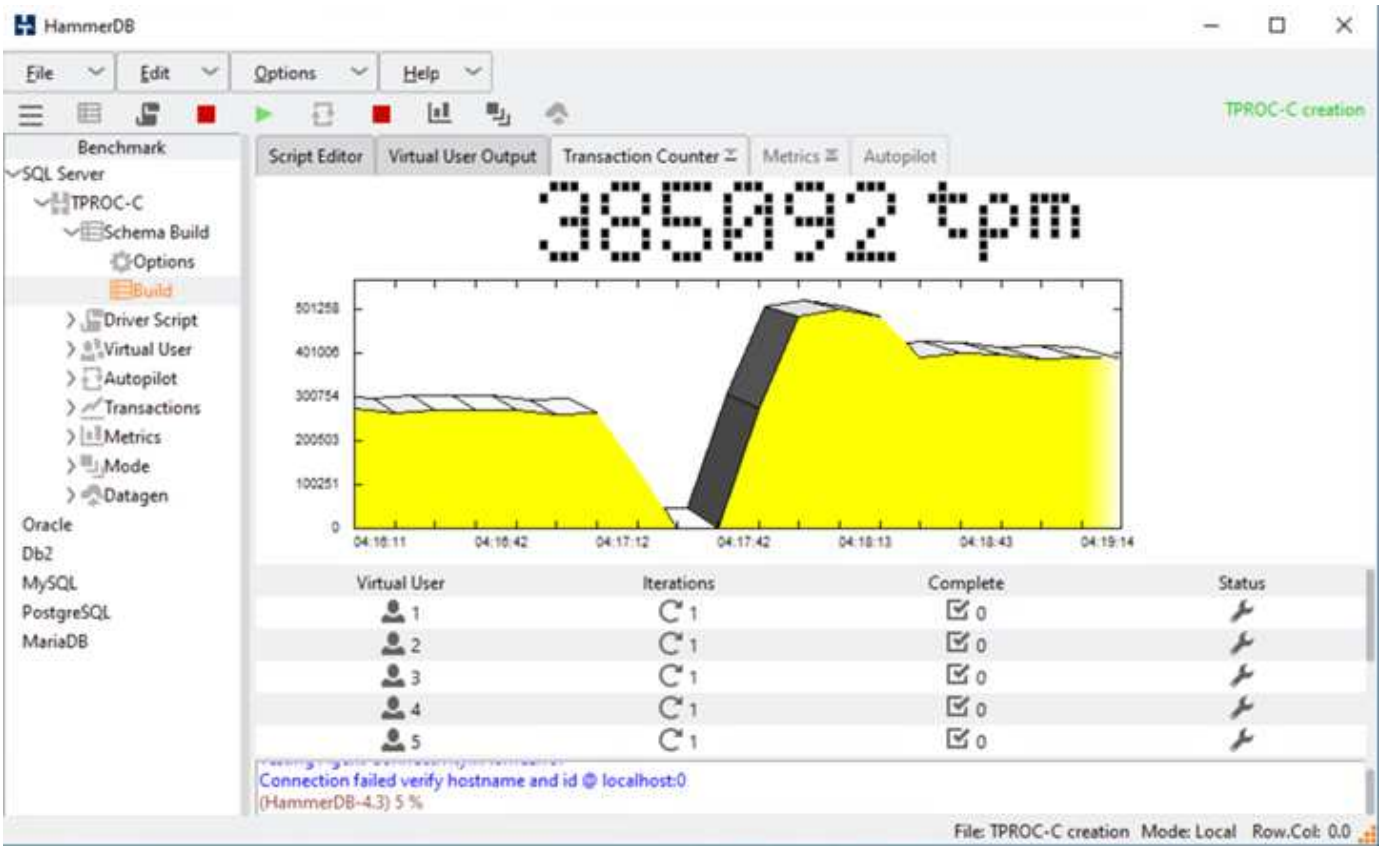
FlexPod SM-BC 解決策 のビジネスクリティカルなワークロード検証の一環として、 Windows Server 2022 VM にインストールされた Microsoft SQL Server 2019 が、 SM-BC が計画的および計画外のストレージフェイルオーバーテスト用の IOMeter VM に含まれています。Windows Server 2022 VM に SQL Server Management Studio をインストールして、 SQL Server を管理します。テストには、 HammerDB データベースツールを使用してデータベーストランザクションが生成されます。

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

FlexPod Datacenter with VMware vSphere 7.0、Cisco VXLAN Single-Site Fabric、and NetApp ONTAP 9.7-Design

ネットアップ、Ramesh Isaac、Cisco Abhinav Singh

Cisco Validated Design（CVD）は、お客様の導入を促進および改善するために設計、テスト、文書化されたシステムとソリューションで構成されています。これらの設計には、お客様のビジネスニーズに対応するために開発されたソリューションポートフォリオに、幅広いテクノロジと製品が組み込まれています。Ciscoとネットアップは提携して、さまざまなワークロードの基盤として機能するFlexPod を提供し、お客様の要件に対応できる堅牢性、効率性、拡張性に優れたアーキテクチャ設計を提供しています。FlexPod 解決策 は、Ciscoとネットアップのテクノロジや製品を導入して、プライベートクラウドとパブリッククラウドの共有インフラを構築するための検証済みのアプローチです。

"FlexPod Datacenter with VMware vSphere 7.0、Cisco VXLAN Single-Site Fabric、and NetApp ONTAP 9.7-

Design"

<xmt-block0>FlexPod</xmt-block> Datacenter with VMware vSphere 7.0 and NetApp<xmt-block1> ONTAP</xmt-block> 9.7 - Deploymentを参照してください

John George、Cisco Sree Lakshmi Lanka、ネットアップ

このドキュメントでは、NetApp AFF A400オールフラッシュストレージシステム、第2世代Intel Xeonスケーラブルプロセッサを搭載したCisco UCS Managerユニファイドソフトウェアリリース4.1(2)、およびVMware vSphere 7.0上でNetApp ONTAP 9.7を搭載したCiscoとNetApp FlexPod データセンターについて説明します。Cisco UCS Manager（UCSM）4.1(2)では、次のサポートが統合されています。

- 現行のすべてのCisco UCSファブリックインターコネクトモデル：6200、6300、6324（Cisco UCS Mini）
- 6400
- 2200/2300/2400シリーズIOM
- Cisco UCS B-Series
- Cisco UCS C-Series

また、Cisco IntersightとNetApp Active IQ SaaS管理プラットフォームも含まれます。

NetApp ONTAP 9.7、Cisco UCSユニファイドソフトウェアリリース4.1(2)、VMware vSphere 7.0を搭載したFlexPod データセンターは、Cisco Unified Computing System（Cisco UCS）、Cisco Nexus 9000スイッチファミリ、MDS 9000マルチレイヤファブリックスイッチ、 およびONTAP 9.7データ管理ソフトウェアを実行するNetApp AFF Aシリーズストレージアレイ。

"FlexPod Datacenter with VMware vSphere 7.0 and NetApp ONTAP 9.7 - Deploymentを参照してください"

FlexPod Datacenter with Cisco Intersight and NetApp ONTAP 9.7-Design

John George、Cisco Scott Kovacs、ネットアップ

本ドキュメントでは、Ciscoとネットアップのテクノロジを共有クラウドインフラとして導入するための検証済みのアプローチである、CiscoとネットアップのFlexPod 解決策について説明します。この検証済みの設計は、エンタープライズクラスのデータセンターで最も人気のある仮想化プラットフォームであるVMware vSphereをFlexPod 上に導入するためのフレームワークを提供します。

"FlexPod Datacenter with Cisco Intersight and NetApp ONTAP 9.7-Design"

<xmt-block0>FlexPod</xmt-block> Datacenter with Cisco Intersight and NetApp<xmt-block1> ONTAP</xmt-block> 9.7 - Deploymentを参照してください

John George、Cisco Scott Kovacs、ネットアップ

データセンター設計における業界の現在のトレンドは、共有インフラへの移行です。仮想化と事前検証済みのITプラットフォームを使用することで、大企業のお客様は、アプリケーションサイロから脱却し、迅速に導入できる共有インフラに移行することで、即応性の向上とコストの削減を実現しています。Ciscoとネットアップは提携してFlexPodを提供しています。は、業界最高水準のストレージ、サーバ、ネットワークコンポーネントを使用してさまざまなワークロードの基盤として機能し、迅速かつ確実に導入できる効率的なアーキテクチャ設計を実現しています。

"FlexPod Datacenter with Cisco Intersight and NetApp ONTAP 9.7 - Deploymentを参照してください"

FlexPod Datacenter with Cisco Intersight and NetApp ONTAP 9.7-Design

John George、Cisco Scott Kovacs、ネットアップ

このドキュメントでは、Ciscoとネットアップのテクノロジを共有クラウドインフラとして導入するための検証済みの解決策 について説明します。この検証済みの設計は、エンタープライズクラスのデータセンターで最も人気のある仮想化プラットフォームであるVMware vSphereをFlexPod 上に導入するためのフレームワークを提供します。

FlexPod は業界をリードする統合インフラで、幅広いエンタープライズワークロードとユースケースをサポートしています。この解決策 を使用すると、VMware vSphereベースのプライベートクラウドを統合インフラに迅速かつ確実に導入できます。

"FlexPod Datacenter with Cisco Intersight and NetApp ONTAP 9.7-Design"

FlexPod データセンターには、VMware vSphere 6.7 U2、Cisco UCS第4世代ファブリック、NetApp ONTAP 9.6が搭載されています

John George、Cisco Sree Lakshmi Lanka、ネットアップ

このドキュメントでは、NetApp ONTAP 9.6を搭載したCiscoとNetApp FlexPod データセンター、第2世代Intel Xeonスケーラブルプロセッサを搭載したCisco UCS Manager Unifiedソフトウェアリリース4.0(4)、およびVMware vSphere 6.7 U2について説明します。Cisco UCS Manager（UCSM）4.0(4)は、次の機能を統合的にサポートします。

- 現行のすべてのCisco UCSファブリックインターコネクトモデル：6200、6300、6324（Cisco UCS Mini）

- 6454
- 2200/2300/2400シリーズIOM
- Cisco UCS B-Series
- Cisco UCS Cシリーズ：

FlexPod Datacenter with NetApp ONTAP 9.6、Cisco UCSユニファイドソフトウェアリリース4.0(4)、およびVMware vSphere 6.7 U2は、Cisco Unified Computing System（Cisco UCS）、Cisco Nexus 9000スイッチファミリ、MDS 9000マルチレイヤファブリックスイッチを基盤とした、設計済みのベストプラクティスに基づくデータセンターアーキテクチャです。 およびONTAP 9を実行するNetApp AFF Aシリーズストレージアレイ。

"VMware vSphere 6.7 U2、Cisco UCS第4世代ファブリック、NetApp ONTAP 9.6を搭載したFlexPod データセンター"

FlexPod Datacenter with VMware vSphere 6.7 U1、Cisco UCS第4世代ファブリック、およびNetApp AFF Aシリーズ-設計

John George、Cisco Sree Lakshmi Lanka、ネットアップ

本ドキュメントでは、Ciscoとネットアップのテクノロジを共有クラウドインフラとして導入するための検証済みのアプローチである、CiscoとネットアップのFlexPod 解決策について説明します。この検証済みの設計は、エンタープライズクラスのデータセンターで最も人気のある仮想化プラットフォームであるVMware vSphereをFlexPod 上に導入するためのフレームワークを提供します。

FlexPod は業界をリードする統合インフラで、幅広いエンタープライズワークロードとユースケースをサポートしています。この解決策 を使用すると、VMware vSphereベースのプライベートクラウドを統合インフラに迅速かつ確実に導入できます。

推奨される解決策 アーキテクチャは、Cisco UCS Bシリーズブレードサーバおよび Cシリーズラックサーバ、Cisco UCS 6454ファブリックインターコネクト、Cisco Nexus 9000シリーズスイッチ、Cisco MDSファイバチャネルスイッチなど、Cisco UCSハードウェアプラットフォームをサポートするために、Cisco Unified Computing System（Cisco UCS）上に構築されています。 ネットアップのオールフラッシュシリーズストレージアレイにも対応しています。また、VMware vSphere 6.7 Update 1も含まれています。これは、ストレージ利用率を最適化し、プライベートクラウドを促進するための多数の新機能を提供します。

"FlexPod Datacenter with VMware vSphere 6.7 U1、Cisco UCS第4世代ファブリック、およびNetApp AFF Aシリーズ-設計"

FlexPod Datacenter with VMware vSphere 6.7 U1、Cisco UCS第4世代ファブリック、NetApp AFF Aシリーズ

John George、Cisco Scott Kovacs、ネットアップ

このドキュメントでは、Cisco UCS Manager Unifiedソフトウェアリリース4.0(2)およびVMware vSphere 6.7 U1を搭載したCiscoとNetApp FlexPod データセンターについて

説明します。Cisco UCS Manager（UCSM）4.0(2)は、現在のすべてのCisco UCSファブリックインターコネクトモデル（6200、6300、6324（Cisco UCS Mini））、6454、2200/2300シリーズIOM、Cisco UCS Bシリーズ、およびCisco UCS Cシリーズの統合サポートを提供します。Cisco UCSユニファイドソフトウェアリリース4.0(2)とVMware vSphere 6.7 U1を搭載したFlexPod データセンターは、Cisco Unified Computing System（UCS）、Cisco Nexus 9000ファミリスイッチ、MDS 9000マルチレイヤファブリックスイッチ、 およびONTAP 9ストレージOSを実行するNetApp AFF Aシリーズストレージアレイ。

"FlexPod Datacenter with VMware vSphere 6.7 U1、Cisco UCS第4世代ファブリック、NetApp AFF Aシリーズ"

FlexPod Datacenter with Cisco ACI Multi-Pod、NetApp MetroCluster IP、VMware vSphere 6.7 - Design

ネットアップ、Haseeb Niazi、Cisco Arvind Ramakrishnan

本ドキュメントでは、Cisco ACIマルチポッドとNetApp MetroCluster IP解決策をFlexPod データセンターに統合して、可用性の高いマルチデータセンター解決策 を実現する方法について説明します。マルチデータセンターアーキテクチャは、無停止でのワークロードモビリティを利用して2つのデータセンター間でワークロードを分散する機能を提供します。これにより、システム停止を維持することなく、サイト間でサービスを移行できます。

FlexPod with ACI Multi-PodおよびNetApp MetroCluster IP解決策 には、次のようなメリットがあります。

- データセンター間でワークロードをシームレスに移動
- サイト全体で一貫したポリシーを適用できます
- 地理的に分散したデータセンター全体にわたるレイヤ2拡張
- メンテナンス時のダウンタイム回避を強化しました
- 災害の回避とリカバリ

"FlexPod Datacenter with Cisco ACI Multi-Pod、NetApp MetroCluster IP、VMware vSphere 6.7 - Design"

<xmt-block0>FlexPod</xmt-block> Datacenter with Cisco ACI Multi-Pod with NetApp<xmt-block1> MetroCluster</xmt-block> IP and VMware vSphere 6.7 - Deploymentを参照してください

ネットアップ、Haseeb Niazi、Cisco Ramesh Issac、Cisco Arvind Ramakrishnan

Ciscoとネットアップは提携して、戦略的なデータセンタープラットフォームを実現する一連のFlexPod ソリューションを提供しています。FlexPod 解決策 は、コンピューティング、ストレージ、ネットワークのベストプラクティスを組み込んだ統合アーキテクチ

ャを提供します。そのため、統合アーキテクチャを検証してさまざまなコンポーネント間の互換性を確保することで、ITリスクを最小限に抑えることができます。また、解決策 は、導入のさまざまな段階（計画、設計、実装）で使用できる文書化された設計ガイダンス、導入ガイダンス、およびサポートを提供することで、ITの課題にも対処します。

"FlexPod Datacenter with Cisco ACI Multi-Pod with NetApp MetroCluster IP and VMware vSphere 6.7 - Deploymentを参照してください"

ハイブリッドクラウド

FlexPod ハイブリッドクラウドとCloud Volumes ONTAP for Epic

TR-4960：『FlexPod Hybrid Cloud with Cloud Volumes ONTAP for Epic』

協力：

Kamini Singh、ネットアップ

デジタル変革を実現するための鍵は、単にデータを活用してより多くのことを行うことにあります。病院では、組織を運営し、患者に効果的にサービスを提供するために、大量のデータが生成され、必要とされています。情報は、患者を治療し、スタッフのスケジュールと医療リソースを管理するときに収集および処理されます。

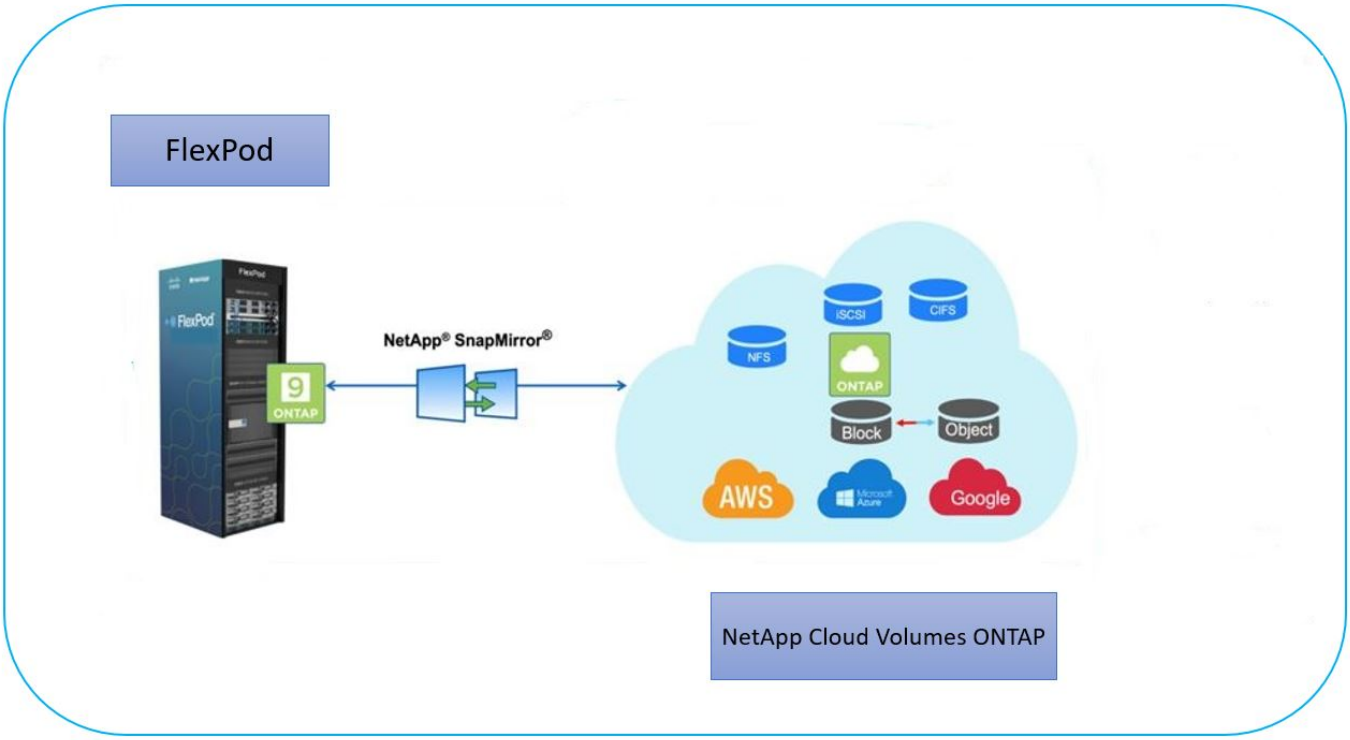
増え続ける医療データと、そのデータから得られる価値あるインサイトによって、医療データサービスとデータ保護が重要な課題となっています。まず、データリカバリ、医療ビジネス継続性、コンプライアンスの要件を満たすためには、医療データの可用性と保護の両方を確保する必要があります。

第2に、医療データを分析のためにすぐに利用できるようにする必要があります。多くの場合、この分析では人工知能（AI）ベースと機械学習（ML）ベースのアプローチを使用して、医療企業がソリューションを改善し、ビジネスバリューを創出できるよう支援します。

第3に、データサービスインフラとデータ保護手法は、医療ビジネスの成長に伴う医療データの増大に対応する必要があります。さらに、データ分析やアーカイブの目的で利用可能なリソースを使用するために、作成されたエッジからコアやクラウドにデータを移動する必要があるため、データモビリティの重要性がますます高まっています。

ネットアップは、ヘルスケアを含むエンタープライズアプリケーション向けに単一のデータ管理解決策 を提供しています。ネットアップは、病院のデジタル変革への道のりを支援することができます。NetApp Cloud Volumes ONTAP は、医療データ管理のための解決策 を提供します。FlexPod データセンターから、AWSなどのパブリッククラウドに導入されたCloud Volumes ONTAP にデータを効率的にレプリケートできます。

Cloud Volumes ONTAP は、対費用効果に優れたセキュアなパブリッククラウドリソースを活用することで、効率性に優れたデータレプリケーション、組み込みのStorage Efficiency機能、シンプルなDRテストによって、クラウドベースのディザスタリカバリ（DR）を強化します。これらのシステムは一元管理され、ドラッグアンドドロップで簡単に管理できるため、あらゆる種類のエラー、障害、災害に対する対費用効果の高い確実な保護が実現します。Cloud Volumes ONTAP は、NetApp SnapMirrorテクノロジをブロックレベルのデータレプリケーション用の解決策 として提供し、差分更新によってデスティネーションを最新の状態に維持します。



対象者

本ドキュメントは、ネットアップ、パートナー様のソリューションエンジニア（SE）、プロフェッショナルサービス担当者を対象としています。ネットアップは、読者が次の知識を有していることを前提としています。

- SANとNASの概念を十分に理解している
- NetApp ONTAP ストレージシステムに関する技術的な知識
- ONTAP ソフトウェアの構成と管理に関する技術的知識

解決策のメリット

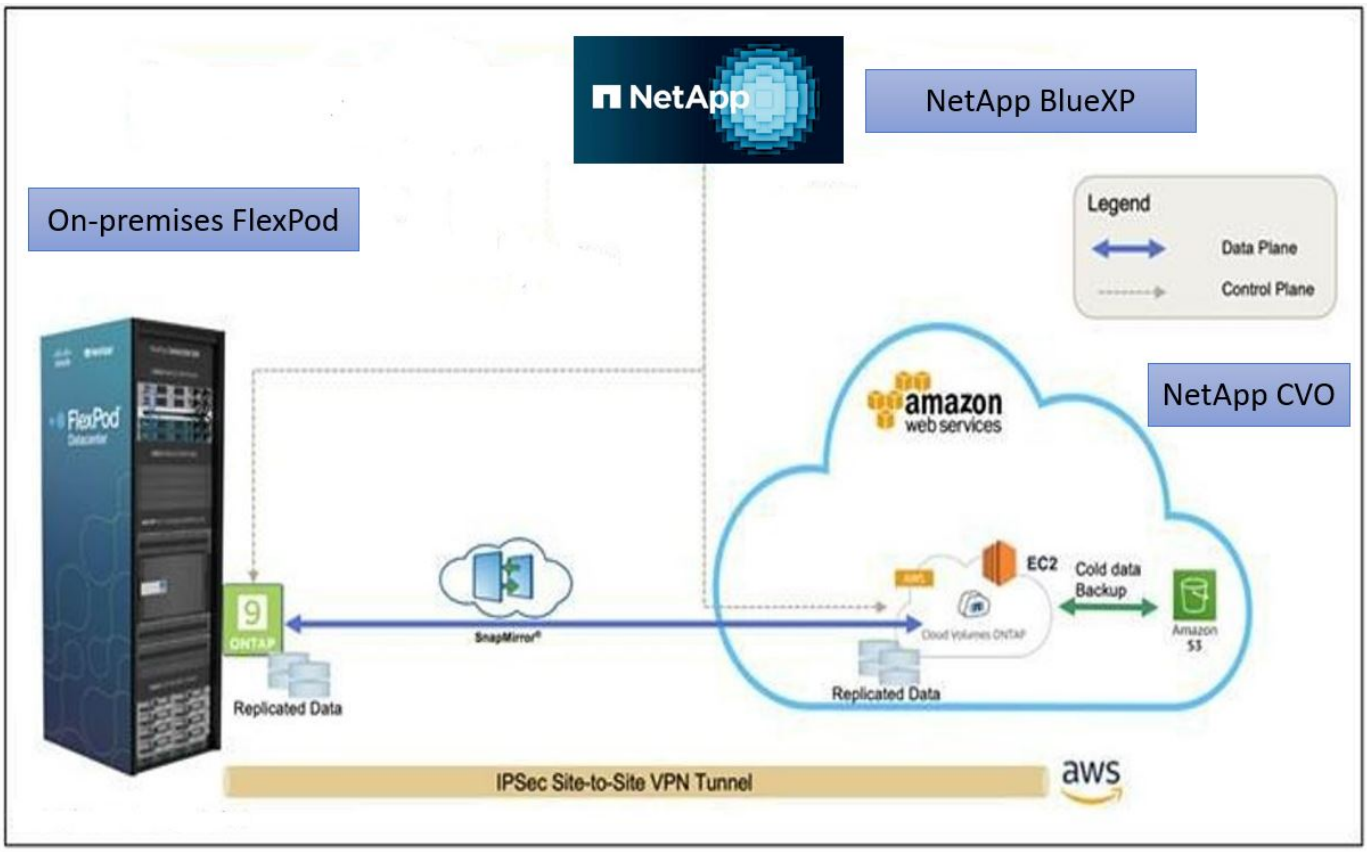
NetApp Cloud Volumes ONTAP と統合されたFlexPod Datacenterは、ヘルスケアワークロードに次のメリットをもたらします。

- カスタマイズされた保護。 Cloud Volumes ONTAP は、ONTAP からクラウドへのブロックレベルのデータレプリケーションを提供し、差分更新によってデスティネーションを最新の状態に維持します。同期スケジュールを指定して、ソースでの変更が転送されるタイミングを決定できます。これにより、あらゆる種類の医療データに対してカスタマイズされた保護が提供されます。
- *フェイルオーバーとフェイルバック*災害が発生した場合、ストレージ管理者はクラウドボリュームへのフェイルオーバーを迅速に設定できます。プライマリサイトがリカバリされると、DR環境で作成された新しいデータがソースボリュームに同期され、セカンダリデータレプリケーションが再確立されます。このようにして、システムを停止することなく医療データを簡単にリカバリできます。
- *効率性。*セカンダリクラウドコピーのストレージスペースとコストは、データ圧縮、シンプロビジョニング、重複排除を使用して最適化されます。医療データは、圧縮と重複排除が適用された形式でブロックレベルで転送されるため、転送速度が向上します。また、データは低コストのオブジェクトストレージに自動的に階層化され、DRシナリオなどでアクセスされたときにのみハイパフォーマンスストレージに戻されます。これにより、継続的なストレージコストを大幅に削減できます。

- ランサムウェア対策。 NetApp BlueXPのランサムウェア対策は、オンプレミス環境とクラウド環境にわたってデータソースをスキャンし、セキュリティの脆弱性を検出し、現在のセキュリティステータスとリスクスコアリングを提供します。次に、さらに調査して修正できる実践的な推奨事項が提示されます。このようにして、医療機関の重要なデータをランサムウェア攻撃から保護できます。

解決策 トポロジ

このセクションでは、解決策 の論理トポロジについて説明します。次の図は、FlexPod オンプレミス環境、Amazon Web Services（AWS）で実行されるNetApp Cloud Volumes ONTAP （CVO）、NetApp BlueXP SaaSプラットフォームで構成される解決策 トポロジを示しています。



コントロールプレーンとデータプレーンは、エンドポイント間で明確に示されます。データプレーンは、セキュアなサイト間VPN接続を利用して、FlexPod のオールフラッシュFAS で実行されるONTAP インスタンスとAWSのNetApp CVOインスタンスの間で実行されます。医療ワークロードのデータをオンプレミスのFlexPod データセンターからNetApp Cloud Volumes ONTAP にレプリケートするには、NetApp SnapMirror レプリケーションを使用します。この解決策 では、NetApp CVOインスタンスにあるコールドデータのバックアップとAWS S3への階層化（オプション）もサポートされています。

"次の例は、解決策 コンポーネントです。"

解決策コンポーネント

"前のページ：解決策 の概要"

FlexPod

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフト

ウェアの定義済みセットです。FlexPod には、NetApp ONTAP ストレージ、Cisco Nexusネットワーキング、Cisco MDSストレージネットワーキング、およびCisco Unified Computing System（Cisco UCS）が含まれます。

医療機関は、デジタル変革を容易にし、患者のエクスペリエンスと成果を向上させるための解決策 を求めています。FlexPod を使用すると、安全性と拡張性に優れたプラットフォームを利用して効率性を高め、より多くの情報に基づいた意思決定を迅速に行うことができるため、より優れた患者ケアを提供できます。

FlexPod には次のようなメリットがあるため、医療ワークロードのニーズに最適なプラットフォームです。

- 運用を最適化して分析情報を迅速に取得し、患者の転帰を改善
- 拡張性と信頼性に優れたインフラで画像処理アプリケーションを合理化
- EHRなどの医療に特化したアプリケーション向けの実証済みのアプローチを使用して、迅速かつ効率的に導入できます。

EHR

電子カルテ（EHR）は、中規模および大規模な医療グループ、病院、統合医療組織向けのソフトウェアを作成しています。顧客には、コミュニティ病院、学術施設、子供の組織、セーフティネットプロバイダー、マルチホスピタルシステムも含まれます。EHRに統合されたソフトウェアは、臨床、アクセス、収益の機能にまたがっており、家庭でも利用できます。

医療提供者組織は、業界をリードするEHRへの多額の投資から最大限の利益を得ることを求められ続けています。お客様は、EHRソリューションやミッションクリティカルなアプリケーション向けにデータセンターを設計する際に、データセンターアーキテクチャに関して次のような目標を特定することがよくあります。

- EHRアプリケーションの高可用性
- ハイパフォーマンス
- データセンターへのEHRの導入が容易
- 新しいEHRリリースやアプリケーションで成長を可能にする俊敏性と拡張性
- コスト効率
- 管理性、安定性、および容易なサポート
- 堅牢なデータ保護、バックアップ、リカバリ、ビジネス継続性

FlexPod はEHR検証済みで、Intel Xeonプロセッサ搭載のCisco UCS、Red Hat Enterprise Linux（RHEL）、VMware ESXiによる仮想化を含むプラットフォームをサポートしています。このプラットフォームは、ONTAP を実行するネットアップストレージとしてEHRが評価している「High Comfort Level」と組み合わせることで、お客様は、FlexPod を介してフルマネージドのプライベートクラウドで医療アプリケーションを実行できます。このクラウドは、いずれのパブリッククラウドプロバイダにも接続できます。

NetApp BlueXP

BlueXP（旧称NetApp Cloud Manager）は、エンタープライズクラスのSaaSベースの管理プラットフォームです。ITエキスパートやクラウドアーキテクトは、ネットアップのクラウドソリューションを使用してハイブリッドマルチクラウドインフラを一元管理できます。オンプレミスとクラウドのストレージを表示および管理する一元化されたシステムを提供し、ハイブリッドクラウド、複数のクラウドプロバイダ、アカウントをサポートします。詳細については、を参照してください "BlueXP"。

コネクタ

BlueXPはコネクタインスタンスを使用して、パブリッククラウド環境内のリソースとプロセスを管理できます。BlueXPで提供される機能の多くにはコネクタが必要であり、クラウドまたはオンプレミスのネットワークに導入できます。

Connectorは次の場所でサポートされます。

- Amazon Web Services の
- Microsoft Azure
- Google Cloud
- オンプレミス

コネクタの詳細については、を参照してください "コネクタページ"。

NetApp Cloud Volumes ONTAP の略

NetApp Cloud Volumes ONTAP は、クラウドでONTAP データ管理ソフトウェアを実行し、ファイルワークロードとブロックワークロードに高度なデータ管理を提供するSoftware-Defined Storageソリューションです。Cloud Volumes ONTAP を使用すると、データ保護、セキュリティ、コンプライアンスを強化しながら、クラウドストレージのコストを最適化し、アプリケーションのパフォーマンスを向上させることができます。

主なメリットは次のとおりです。

- * Storage Efficiency。*組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、瞬時のクローニングを活用して、ストレージコストを最小限に抑えます。
- *高可用性*クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を実現します。
- データ保護。 Cloud Volumes ONTAP は、業界をリードするネットアップのレプリケーションテクノロジであるSnapMirrorを使用してオンプレミスのデータをクラウドにレプリケートするため、複数のユースケースでセカンダリコピーを簡単に利用できます。また、Cloud Volumes ONTAP はCloud Backupと統合して、クラウドデータの保護と長期アーカイブのためのバックアップとリストアの機能を提供します。
- *データ階層化。*アプリケーションをオフラインにすることなく、高パフォーマンスと低パフォーマンスのストレージプールをオンデマンドで切り替えます。
- アプリケーションの整合性。 NetApp SnapCenter テクノロジを使用して、NetApp Snapshotコピーの整合性を提供します。
- データセキュリティ。 Cloud Volumes ONTAP はデータ暗号化をサポートし、ウイルスやランサムウェアからの保護を提供します。
- プライバシーコンプライアンス管理 Cloud Data Senseとの統合により、データのコンテキストを把握し、機密データを特定できます。

詳細については、を参照してください "Cloud Volumes ONTAP"。

NetApp Active IQ Unified Manager の略

NetApp Active IQ Unified Manager では、設計が刷新されたわかりやすい単一のインターフェイスからONTAPストレージクラスタを監視でき、集合知とAI分析から得た情報を提供します。ストレージ環境とストレージ環境で実行されている仮想マシンに関する、運用面、パフォーマンス面、プロアクティブな分析情報を包括的に

提供します。ストレージインフラで問題 が発生すると、Unified Managerから問題 の詳細情報を通知してルート原因 を特定できるようになります。仮想マシンダッシュボードではVMのパフォーマンス統計を確認でき、これにより、ネットワーク経由でダウンしているvSphereホストからストレージへのI/Oパス全体を調査できます。

一部のイベントには、問題 を修正するための対応策も用意されています。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントにカスタムアラートを設定できます。Active IQ Unified Manager を使用すると、容量と使用状況の傾向を予測してユーザのストレージ要件を計画できます。これにより、問題が発生する前に対処できるようになり、長期的に新たな問題につながる可能性のある、短期的な事後的な判断を回避できます。

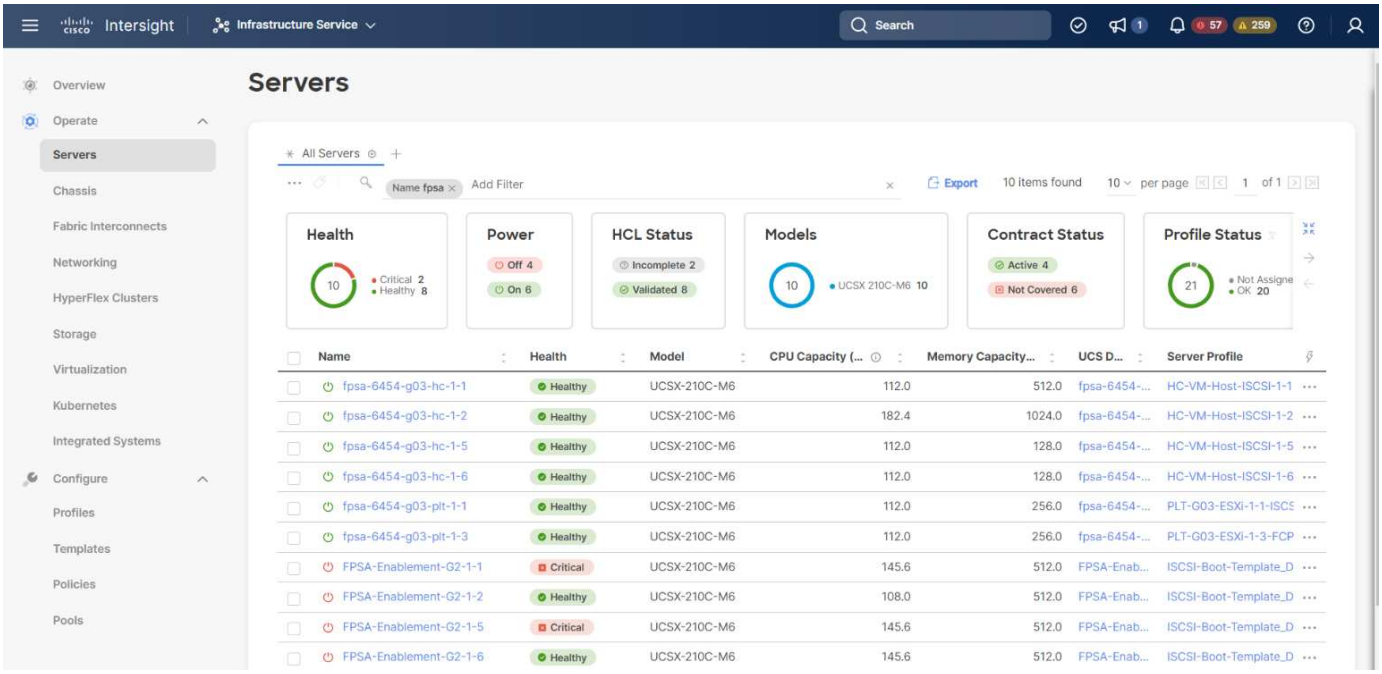
詳細については、を参照してください "Active IQ Unified Manager"。

Cisco Intersightの

Cisco Intersightは、従来のアプリケーションやクラウドネイティブなインフラに向けて、インテリジェントな自動化、オブザーバビリティ、最適化を実現するSaaSプラットフォームです。このプラットフォームは、ITチームの変化を促進し、ハイブリッドクラウド向けに設計された運用モデルを提供します。Cisco Intersightには、次のようなメリットがあります。

- 迅速な提供。 Intersightは、アジャイルベースのソフトウェア開発モデルにより、頻繁な更新と継続的なイノベーションにより、クラウドまたはお客様のデータセンターからサービスとして提供されます。このようにして、お客様は重要なビジネスニーズのサポートに集中できます。
- 運用の簡易化。 Intersightは、SaaSで提供される単一のセキュアなツールと共通のインベントリ、認証、APIを使用してフルスタックとすべての場所で機能し、チーム間のサイロを解消することで、運用を簡易化します。これにより、オンプレミスの物理サーバとハイパーバイザー、VM、Kubernetes、サーバレス、自動化、 オンプレミスとパブリッククラウドの両方で最適化とコスト管理を実現します。
- *継続的な最適化。*すべてのレイヤおよびCisco TACが提供するCisco Intersightのインテリジェンスを使用して、環境を継続的に最適化できます。このインテリジェンスは推奨される自動化可能なアクションに変換されるため、ワークロードの移動や物理サーバの健全性の監視から、使用するパブリッククラウドのコスト削減の推奨まで、あらゆる変更にリアルタイムで適応できます。

Cisco Intersightには、UCSM Managed Mode（UMM）とIntersight Managed Mode（IMM）という2つの管理操作モードがあります。ファブリックインターコネクトの初期セットアップ時に、ファブリック接続Cisco UCSシステムのネイティブUCSM Managed Mode（UMM）またはIntersight Managed Mode（IMM）を選択できます。この解決策 では、ネイティブIMMが使用されます。次の図は、Cisco Intersightダッシュボードを示しています。



ページを示しています。"]

VMware vSphere 7.0

VMware vSphereは、大規模なインフラストラクチャ（CPU、ストレージ、ネットワークなど）をシームレスで汎用性の高い動的な運用環境として包括的に管理するための仮想化プラットフォームです。個 々 のマシンを管理する従来のオペレーティングシステムとは異なり、VMware vSphereはデータセンター全体のインフラストラクチャを集約して、必要なアプリケーションに迅速かつ動的に割り当てることができるリソースを備えた単一のパワーハウスを作成します。

VMware vSphereとそのコンポーネントの詳細については、を参照してください "VMware vSphere の場合"。

VMware vCenter Server の各機能を使用し

VMware vCenter Serverでは、1つのコンソールからすべてのホストとVMを統合的に管理でき、クラスタ、ホスト、およびVMのパフォーマンス監視を集約できます。VMware vCenter Serverを使用すると、管理者は、コンピューティングクラスタ、ホスト、VM、ストレージ、ゲストOS、 仮想インフラストラクチャのその他の重要なコンポーネントVMware vCenterは、VMware vSphere環境で使用できる豊富な機能を管理します。

詳細については、を参照してください "VMware vCenter"。

ハードウェアおよびソフトウェアのリビジョン

このハイブリッドクラウド解決策 は、で定義されている、サポート対象のバージョンのソフトウェア、ファームウェア、ハードウェアを実行している任意のFlexPod 環境に拡張できます "NetApp Interoperability Matrix Tool で確認できます"、 "UCSハードウェアおよびソフトウェアの互換性"および "VMware Compatibility Guide 』を参照してください"。

次の表に、オンプレミスのFlexPod ハードウェアとソフトウェアのリビジョンを示します。

コンポーネント	プロダクト	バージョン
コンピューティング	Cisco UCS X210c M6	5.0（1b）

コンポーネント	プロダクト	バージョン
	Cisco UCSファブリックインターコネクト6454	4.2（2a）
ネットワーク	Cisco Nexus 9336C-FX2 NX-OS	9.3（9）
ストレージ	NetApp AFF A400	ONTAP 9.11.1P2
	NetApp ONTAP Tools for VMware vSphere の略	9.11
	NetApp NFS Plug-in for VMware VAAI	"2.0"
	NetApp Active IQ Unified Manager の略	9.11P1
ソフトウェア	VMware vSphere の場合	7.0（U3）
	VMware ESXi nenic イーサネットドライバ	1.0.35.0
	VMware vCenter Applianceの略	バージョン7.0.3
	Cisco Intersight Assist仮想アプライアンス	1.0.9-342

次の表に、NetApp BlueXPとCloud Volumes ONTAP のバージョンを示します。

ベンダー	プロダクト	バージョン
ネットアップ	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"次の記事：インストールと設定"

インストールと設定

"前の図：解決策 コンポーネント。"

NetApp Cloud Volumes ONTAP の導入

Cloud Volumes ONTAP インスタンスを設定するには、次の手順を実行します。

1. パブリッククラウドサービスプロバイダ環境の準備

   解決策 構成について、パブリッククラウドサービスプロバイダの環境の詳細を確認しておく必要があります。たとえば、Amazon Web Services（AWS）環境の準備では、AWSアクセスキー、AWSシークレットキー、およびその他のネットワークの詳細（リージョン、VPC、サブネットなど）が必要です。

2. VPCエンドポイントゲートウェイを設定します。

   VPCとAWS S3サービスの間の接続を有効にするには、VPCエンドポイントゲートウェイが必要です。これは、ゲートウェイタイプのエンドポイントであるCVOでバックアップを有効にするために使用されます。

3. NetApp BlueXPにアクセスします。

   NetApp BlueXPやその他のクラウドサービスにアクセスするには、に登録する必要があります "NetApp BlueXP"。BlueXPアカウントでワークスペースとユーザを設定するには、をクリックします "こちらをご覧ください"。BlueXPからクラウドプロバイダにコネクタを直接導入する権限を持つアカウントが必要です。BlueXPポリシーはからダウンロードできます "こちらをご覧ください"。

4. コネクタを展開します。

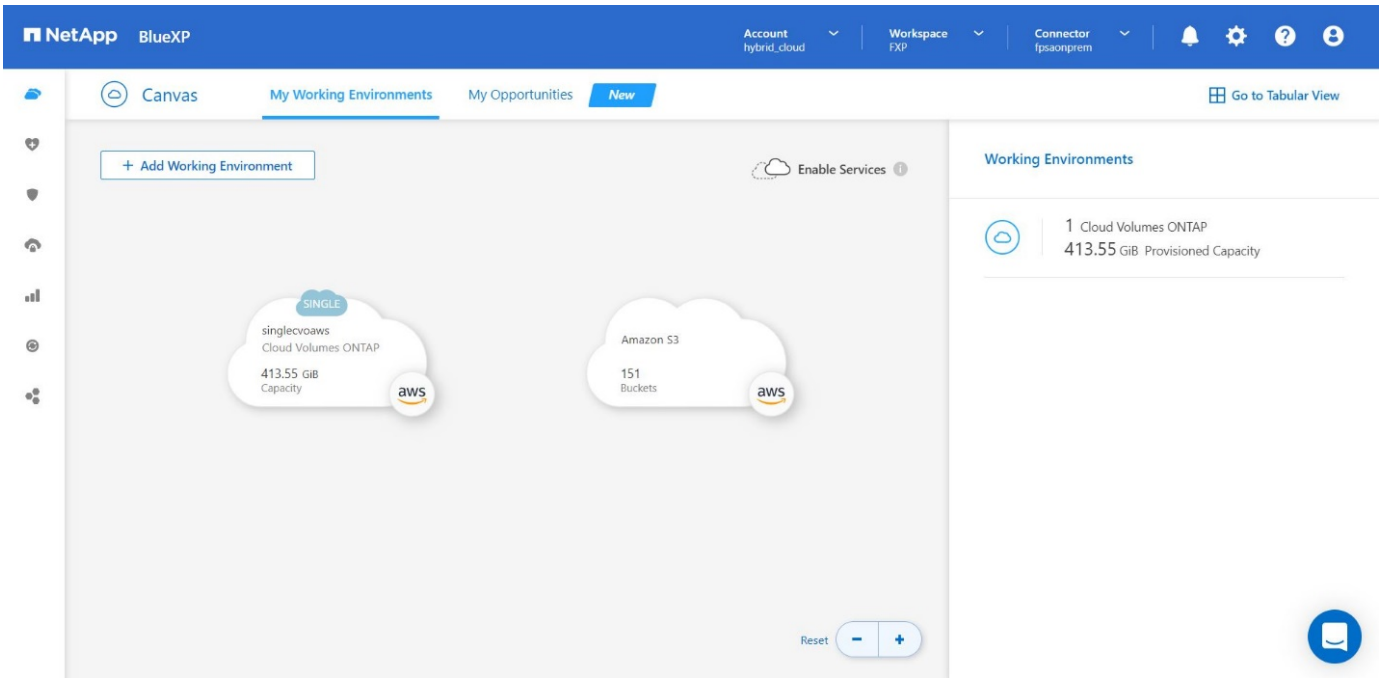
   Cloud Volume ONTAP 作業環境を追加する前に、コネクタを導入する必要があります。コネクタを配置せずに最初のCloud Volumes ONTAP 作業環境を作成しようとすると、プロンプトが表示されます。BlueXPからAWSにコネクタを導入する方法については、こちらを参照してください "リンク"。

5. AWSでCloud Volumes ONTAP を起動します。

   Cloud Volumes ONTAP は単一システム構成で起動することも、 AWS で HA ペアとして起動することもできます。 "ステップバイステップの手順をお読みください"。

   これらの手順の詳細については、を参照してください "AWSでのCloud Volumes ONTAP のクイックスタートガイド"。

   この解決策 では、AWSにシングルノードのCloud Volumes ONTAP システムを導入しました。次の図は、シングルノードCVOインスタンスを使用するNetApp BlueXPダッシュボードを示しています。



画面と[My Working Environments]を示しています。"]

オンプレミスの**FlexPod** 環境

FlexPod とUCS Xシリーズ、VMware、およびNetApp ONTAP の設計の詳細については、を参照してください "FlexPod データセンターとCisco UCS Xシリーズ" 設計ガイド：このドキュメントでは、Cisco Intersightが管理するUCS Xシリーズプラットフォームを FlexPod データセンターインフラに組み込むための設計ガイダンスを提供します。

オンプレミスのFlexPod インスタンスの導入については、を参照してください "この導入ガイドを参照してください"。

このドキュメントでは、Cisco Intersightが管理するUCS Xシリーズプラットフォームを FlexPod データセンターインフラに組み込むための導入ガイダンスを提供します。このドキュメントでは、導入を成功させるための構成とベストプラクティスの両方について説明します。

FlexPod は、UCS管理モードとCisco Intersight管理モード（IMM）の両方で導入できます。FlexPod をUCS管理モードで展開する場合は、こちらを参照してください "設計ガイド" そしてこれ "導入ガイド"。

FlexPod の導入は、Ansibleを使用してコードとしてインフラを使用して自動化できます。以下は、エンドツーエンドのFlexPod 展開のためのGitHubリポジトリへのリンクです。

- UCS管理モードでのCisco UCS、NetApp ONTAP 、VMware vSphereを使用したFlexPod のAnsible構成を確認できます "こちらをご覧ください"。
- IMM内のCisco UCS、NetApp ONTAP 、VMware vSphereを使用したFlexPod のAnsible構成を確認できます "こちらをご覧ください"。

オンプレミスの**ONTAP** ストレージ構成

ここでは、この解決策 に固有のONTAP の重要な設定手順をいくつか説明します。

1. iSCSIサービスを実行しているSVMを設定します。

```
1. vserver create -vserver Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security-
style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   クラスタの構成時にiSCSIライセンスがインストールされなかった場合は、iSCSIサービスを作成する前に必ずライセンスをインストールしてください。

2. FlexVol ボリュームを作成します。

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. iSCSIアクセス用のインターフェイスを追加します。

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> –status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
```

この解決策 では、4つのiSCSI論理インターフェイス（LIF）を作成しました（各ノードに2つずつ）。

vCenterを導入してFlexPod インスタンスを運用開始し、すべてのESXiホストを追加したら、NetApp ONTAP ストレージに接続してアクセスするサーバとして機能するLinux VMを導入する必要があります。この解決策 では、CentOS 8インスタンスをvCenterにインストールしました。

4. LUNを作成します。

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

EHR Operational Database（ODB；EHR運用データベース）、ジャーナル、およびアプリケーションのワークロードについては、ストレージをサーバにiSCSI LUNとして提供することを推奨します。また、対応しているAIXおよびRHELオペレーティングシステムのバージョンがある場合は、FCPとNVMe/FCの使用もサポートされるため、パフォーマンスが向上します。FCPとNVMe/FCは同じファブリックに共存できます。

5. igroupを作成します。

```
1. igroup create –vserver Healthcare_SVM –igroup ehr –protocol iscsi
–ostype linux –initiator iqn.1994-05.com.redhat:8e91e9769336
```

igroupは、サーバからLUNへのアクセスを許可するために使用されます。Linuxホストの場合、サーバIQNはファイルで確認できます `/etc/iscsi/initiatorname.iscsi`。

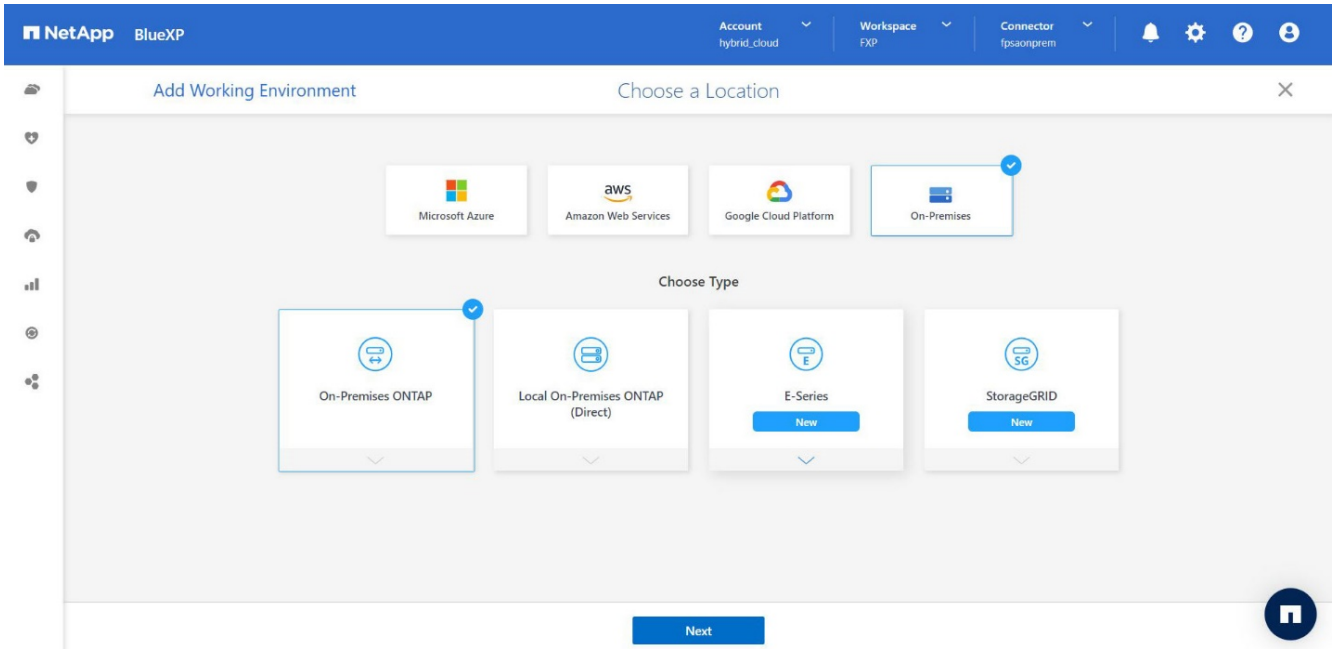
6. LUN を igroup にマッピングします。

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

オンプレミスの**FlexPod** ストレージを**BlueXP**に追加

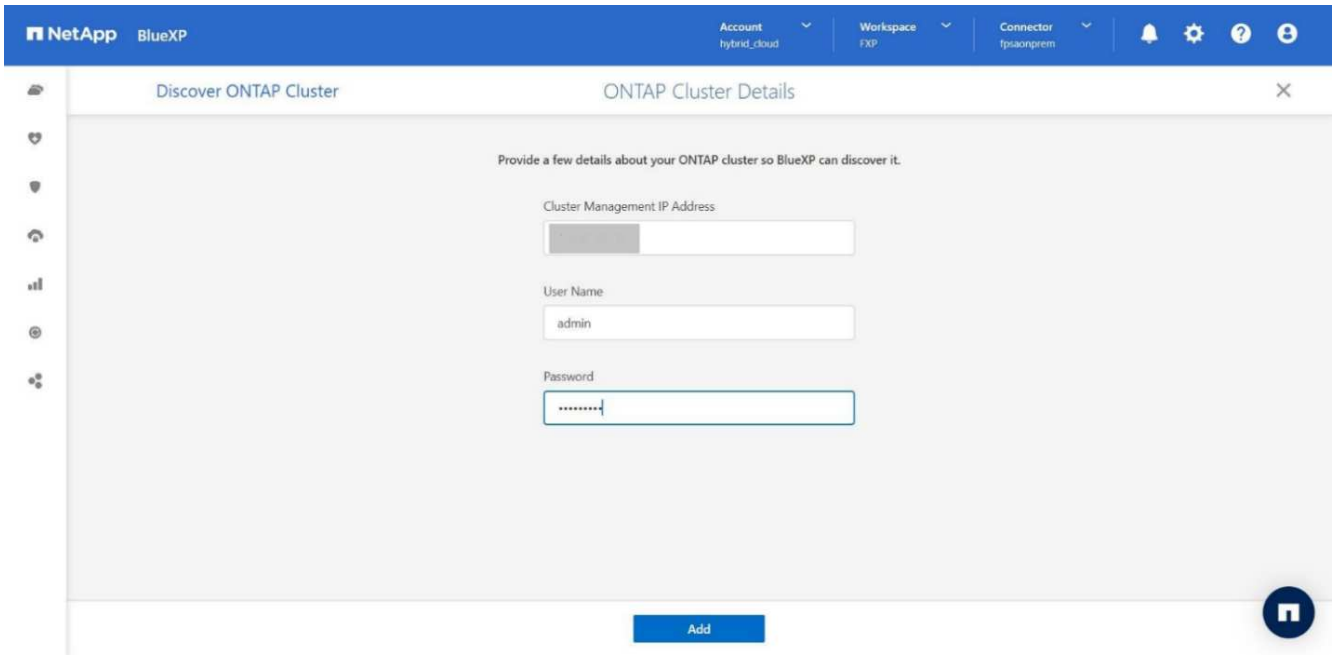
NetApp BlueXPを使用してFlexPod ストレージを作業環境に追加するには、次の手順を実行します。

1. ナビゲーションメニューから、**[**ストレージ**]**>*[キャンバス]*を選択します。
2. キャンバスページで、*作業環境の追加*をクリックし、*オンプレミス*を選択します。
3. オンプレミスONTAP *を選択します。「 * 次へ * 」をクリックします。



ページを示しています。オンプレミスのONTAP が選択されています。"]

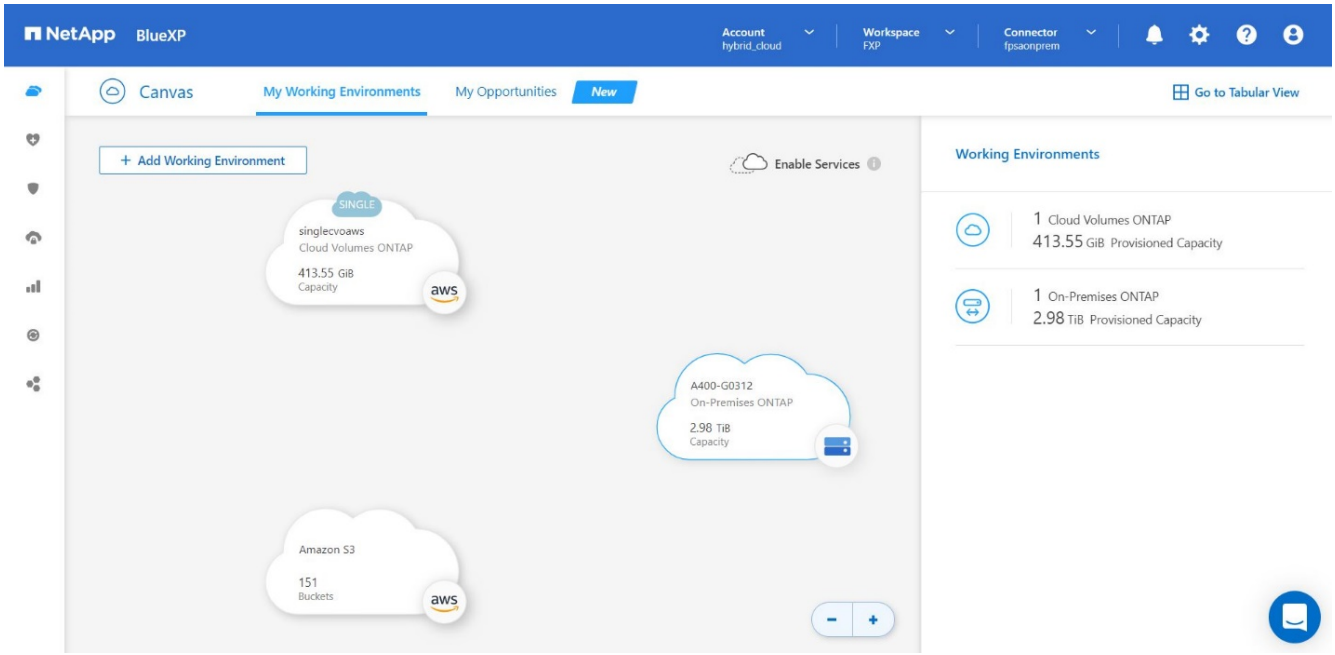
4. ONTAP のクラスタ詳細ページで、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードを入力します。次に*[追加]*をクリックします。



ページとONTAP の[Cluster Details]エントリを示しています。"]

5. [Details and Credentials]ページで、作業環境の名前と概要 を入力し、*[Go]*をクリックします。

   BlueXPがONTAP クラスタを検出し、Canvasの作業環境として追加します。



ページを示しています。最近追加した作業環境が右側に表示されます。"]

詳細については、ページを参照してください "オンプレミスのONTAP クラスタを検出"。

"次の記事：SANの構成"

SAN の設定

"前の手順：インストールと設定"

このセクションでは、EHRがネットアップストレージとの最適な統合を可能にするために必要なホスト側の構成について説明します。このセグメントでは、Linuxオペレーティングシステムのホスト統合について具体的に説明します。を使用します "ネットアップのInteroperability Matrix Tool （IMT）" ソフトウェアとファームウェアのすべてのバージョンを検証します。

以下は、この解決策 で使用したCentOS 8ホストに固有の設定手順です。

NetApp Host Utility Kitの略

ネットアップストレージシステムに接続されてアクセスしているホストのオペレーティングシステムに、NetApp Host Utility Kit（Host Utilities）をインストールすることを推奨します。ネイティブのMicrosoftマルチパスI/O（MPIO）がサポートされています。OSがマルチパス用にAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）に対応している必要があります。Host Utilitiesをインストールすると、ネットアップストレージのホストバスアダプタ（HBA）が設定されます。

NetApp Host Utilitiesをダウンロードできます "こちらをご覧ください"。この解決策 では、Linux Host Utilities 7.1をホストにインストールしました。

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

ONTAP ストレージを検出

ログインが発生するはずのときにiSCSIサービスが実行されていることを確認します。ターゲット上の特定のポータルまたはターゲット上のすべてのポータルに対してログインモードを設定するには、を使用します `iscsiadm` コマンドを実行します

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

今、あなたはを使うことができます `sanlun` をクリックして、ホストに接続されているLUNに関する情報を表示します。ホストにrootとしてログインしていることを確認します。

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                     device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
---
Healthcare_SVM                        /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                        /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

マルチパスを設定します

Device Mapper Multipathing（DM-Multipath）は、Linuxの標準マルチパスユーティリティです。冗長性を確保し、パフォーマンスを向上させるために使用できます。サーバとストレージ間の複数のI/Oパスを集約または結合するため、OSレベルで1つのデバイスを作成します。

1. システムにDM-Multipathを設定する前に、システムが更新され、が含まれていることを確認してください `device-mapper-multipath` パッケージ。

   ```
   [root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
   device-mapper-multipath-libs-0.8.4-31.el8.x86_64
   device-mapper-multipath-0.8.4-31.el8.x86_64
   ```

2. 構成ファイルはです `/etc/multipath.conf` ファイル。次のように設定ファイルを更新します。

   ```
   [root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
   defaults {
      path_checker      readsector0
      no_path_retry      fail
   }
   devices {
      device {
         vendor         "NETAPP  "
         product         "LUN.*"
         no_path_retry     queue
         path_checker      tur
      }
   }
   ```

3. マルチパスサービスを有効にして開始します。

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. ロード可能なカーネルモジュールを追加します `dm-multipath` をクリックし、マルチパスサービスを再起動します。最後に、マルチパスのステータスを確認します。

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

これらの手順の詳細については、を参照してください "こちらをご覧ください"。

物理ボリュームを作成します

を使用します `pvcreate` 物理ボリュームとして使用するブロックデバイスを初期化するコマンド。初期化は、ファイルシステムのフォーマットに似ています。

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

ボリュームグループを作成します

1つ以上の物理ボリュームからボリュームグループを作成するには、を使用します `vgcreate` コマンドを実行しますこのコマンドは、名前を指定して新しいボリュームグループを作成し、そのグループに少なくとも1つの物理ボリュームを追加します。

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

。 vgdisplay コマンドを使用すると、ボリュームグループのプロパティ（サイズ、エクステント、物理ボリューム数など）を固定形式で表示できます。

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

論理ボリュームを作成します

論理ボリュームを作成すると、ボリュームグループを構成する物理ボリューム上の空きエクステントを使用して、ボリュームグループから論理ボリュームが作成されます。

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

このコマンドは、という名前の論理ボリュームを作成します datalv ボリュームグループ内の未割り当てスペースをすべて使用します datavg。

ファイルシステムを作成します

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

マウントするフォルダを作成します

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

ファイルシステムをマウントします

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                 1K-blocks    Used Available Use% Mounted on
devtmpfs                     8072804       0   8072804   0% /dev
tmpfs                        8103272       0   8103272   0% /dev/shm
tmpfs                        8103272    9404   8093868   1% /run
tmpfs                        8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root         45496624 5642104  39854520  13% /
/dev/sda2                    1038336  258712    779624  25% /boot
/dev/sda1                     613184    7416    605768   2% /boot/efi
tmpfs                        1620652      12   1620640   1% /run/user/42
tmpfs                        1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

これらのタスクの詳細については、ページを参照してください "CLIコマンドを使用したLVM管理"。

データ生成

`Dgen.pl` は、EHRのI/Oシミュレータ（GenerateIO）用のPerlスクリプトデータジェネレータです。LUN内のデータはEHRを使用して生成されます
`Dgen.pl` スクリプト：スクリプトは、EHRデータベース内にあるものと同様のデータを作成するように設計されています。

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                 1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

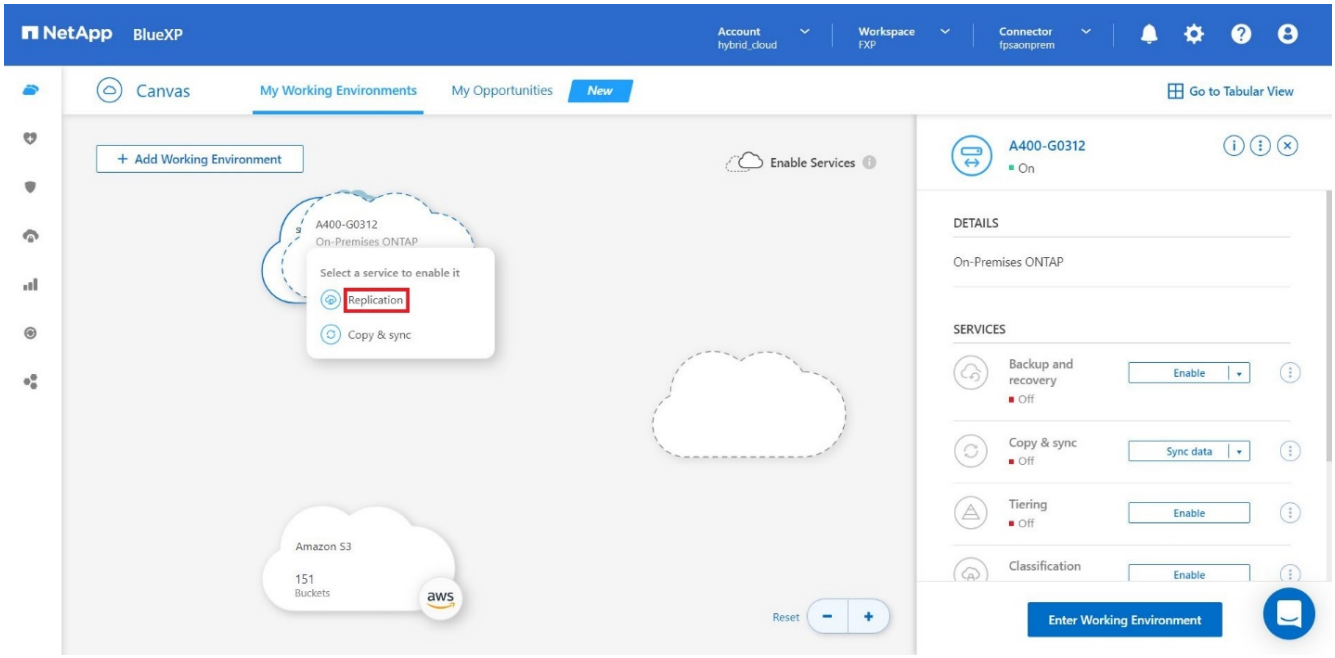
実行中は、 `Dgen.pl` スクリプトは、デフォルトでファイルシステムの85%をデータ生成に使用します。

オンプレミスの**ONTAP** と**Cloud Volumes ONTAP** の間に**SnapMirror**レプリケーションを設定

NetApp SnapMirror は、 LAN または WAN 経由でデータを高速でレプリケートするため、仮想環境と従来の環境の両方で、高いデータ可用性と高速なデータレプリケーションを実現できます。ネットアップストレージシステムにデータをレプリケートし、セカンダリデータを継続的に更新することで、データを最新の状態に保ちながら、必要なときにいつでもデータを利用できるようになります。外部レプリケーションサーバは必要ありません。

オンプレミスのONTAP システムとCVOの間にSnapMirrorレプリケーションを設定するには、次の手順を実行します。

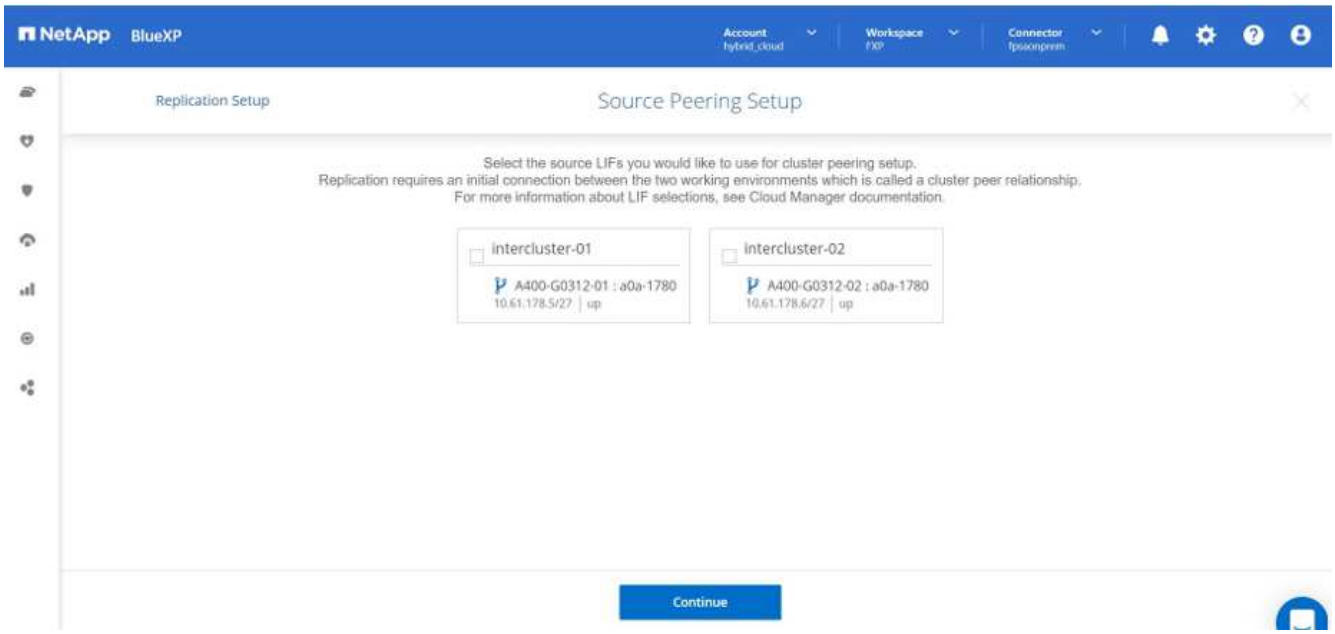
1. ナビゲーションメニューから、**[**ストレージ**]**>*[キャンバス]*を選択します。
2. Canvasで、ソースボリュームが含まれている作業環境を選択し、ボリュームのレプリケート先となる作業環境にソースボリュームをドラッグして、*[レプリケーション]*を選択します。



画面を示しています。オンプレミスのONTAP インスタンスのドロップダウンで[Replication]が選択されています。"]

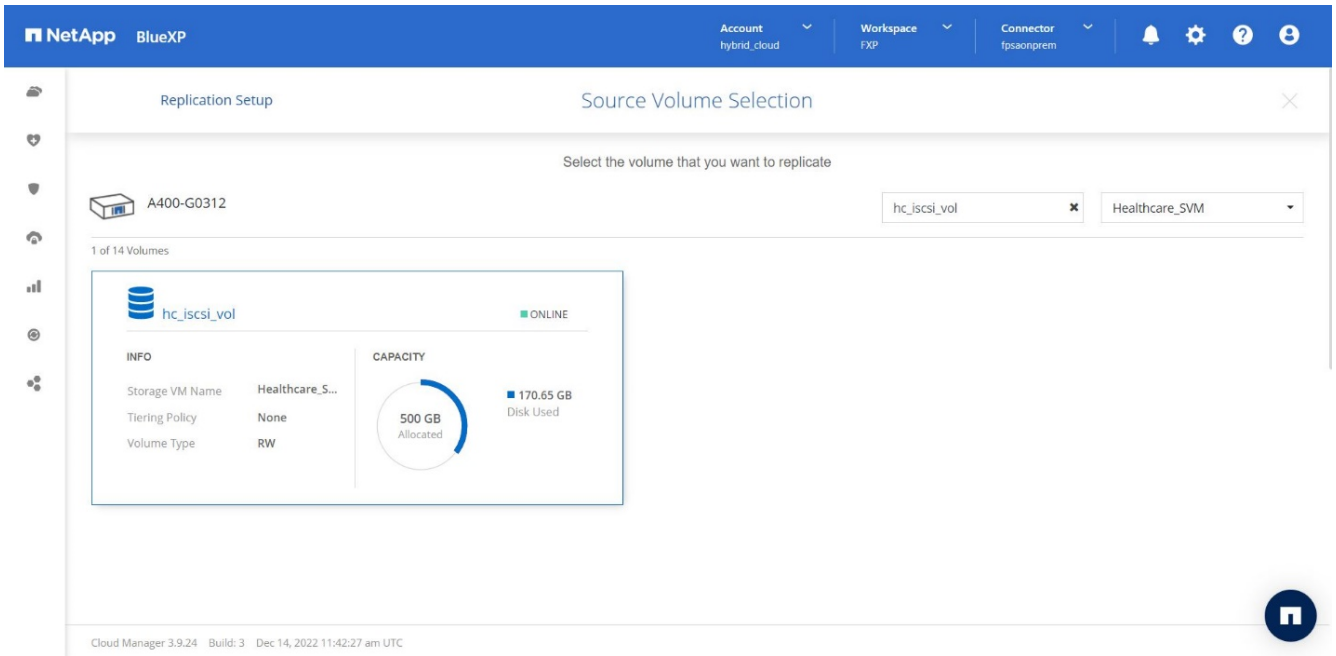
以降の手順では、Cloud Volumes ONTAP クラスタとオンプレミスのONTAP クラスタ間に同期関係を作成する方法について説明します。

3. *ソースとデスティネーションのピアリングのセットアップ。*このページが表示された場合は、クラスタピア関係に使用するすべてのクラスタ間LIFを選択します。



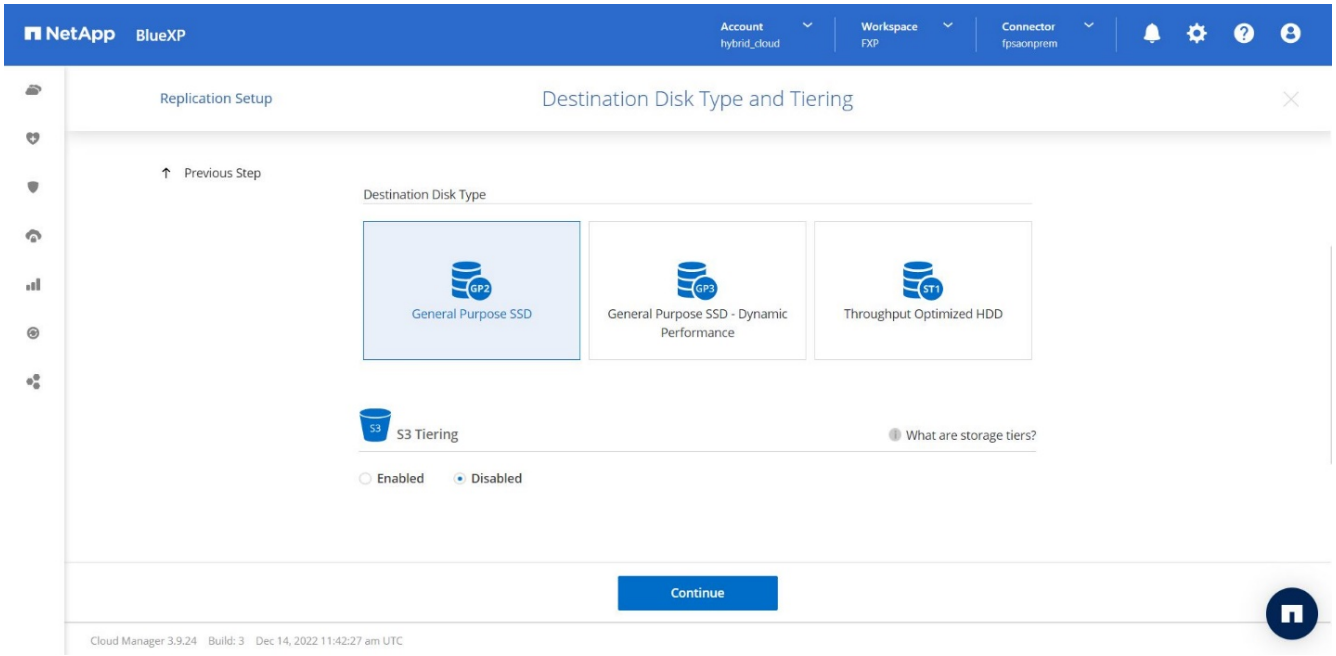
画面を示しています。"]

4. *ソースボリュームの選択。*レプリケートするボリュームを選択します。



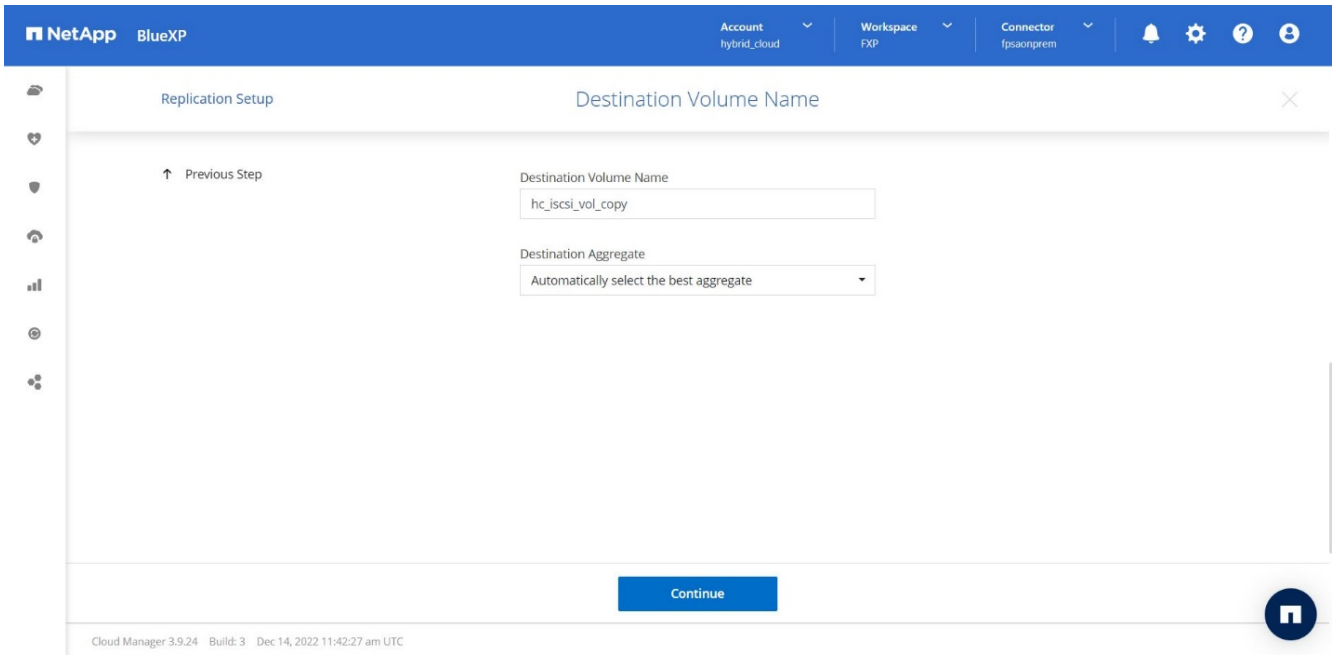
画面を示しています。1つのボリューム（14個）が表示されています。"]

5. *デスティネーションディスクの種類と階層化。*ターゲットがCloud Volumes ONTAP システムの場合は、デスティネーションディスクの種類を選択し、データ階層化を有効にするかどうかを選択します。



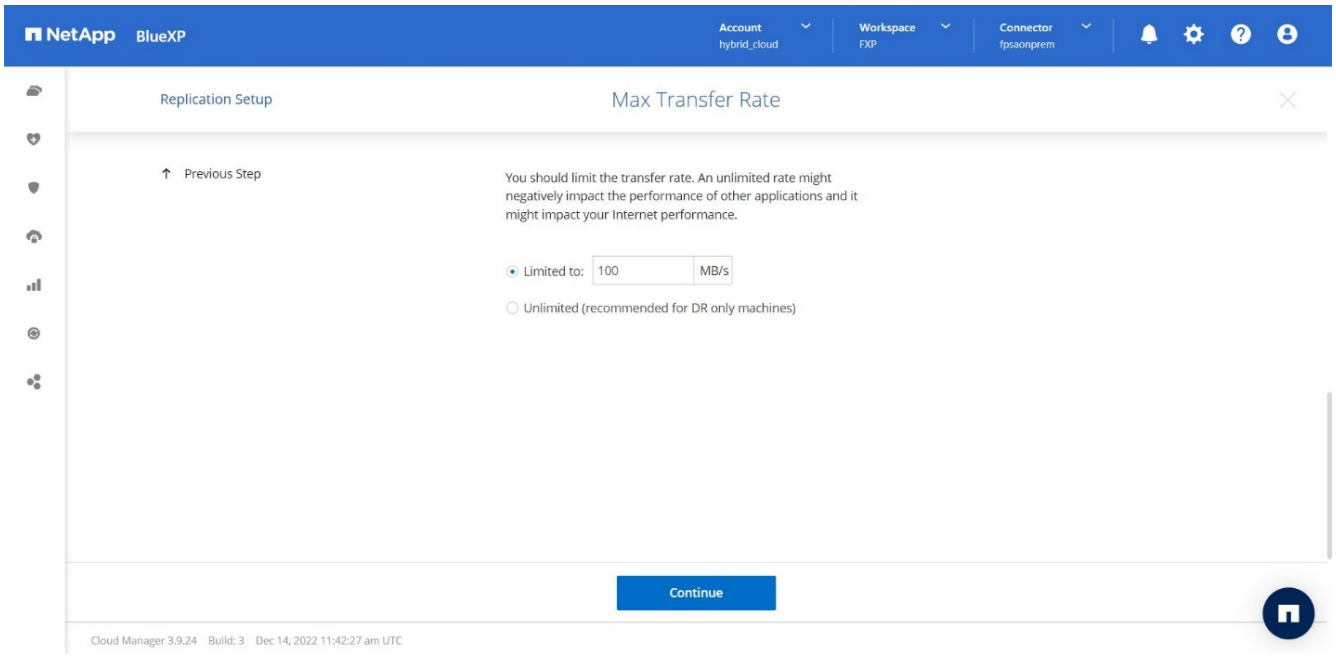
画面を示しています。"]

6. *デスティネーションボリューム名：*デスティネーションボリュームの名前を指定し、デスティネーションアグリゲートを選択してください。デスティネーションが ONTAP クラスタの場合は、デスティネーション Storage VM も指定する必要があります。



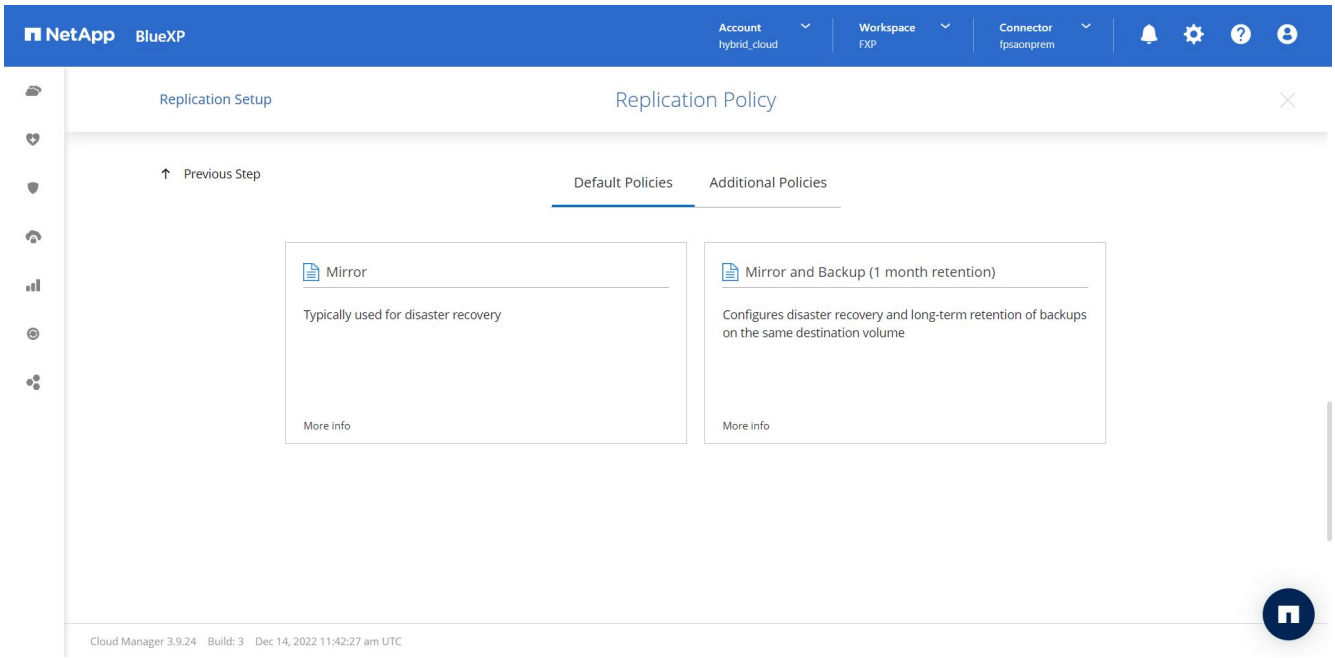
画面を示しています。関連する情報が入力されています。"]

7. *最大転送速度。*データを転送できる最大転送速度（1秒あたりのメガバイト数）を指定します。



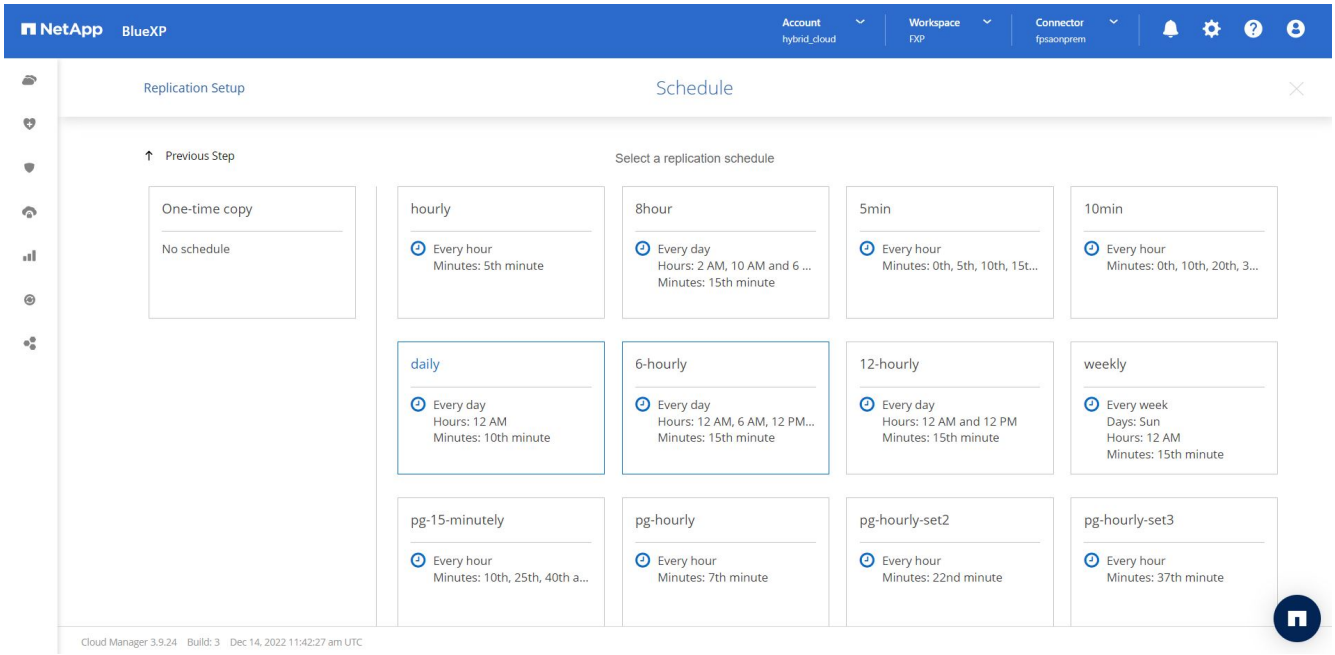
画面を示しています。100MB/sが入力されています。"]

8. レプリケーションポリシー。*デフォルトポリシーを選択するか[その他のポリシー]*をクリックし、いずれかの高度なポリシーを選択します。ヘルプを表示するには、 "レプリケーションポリシーについて説明します"。

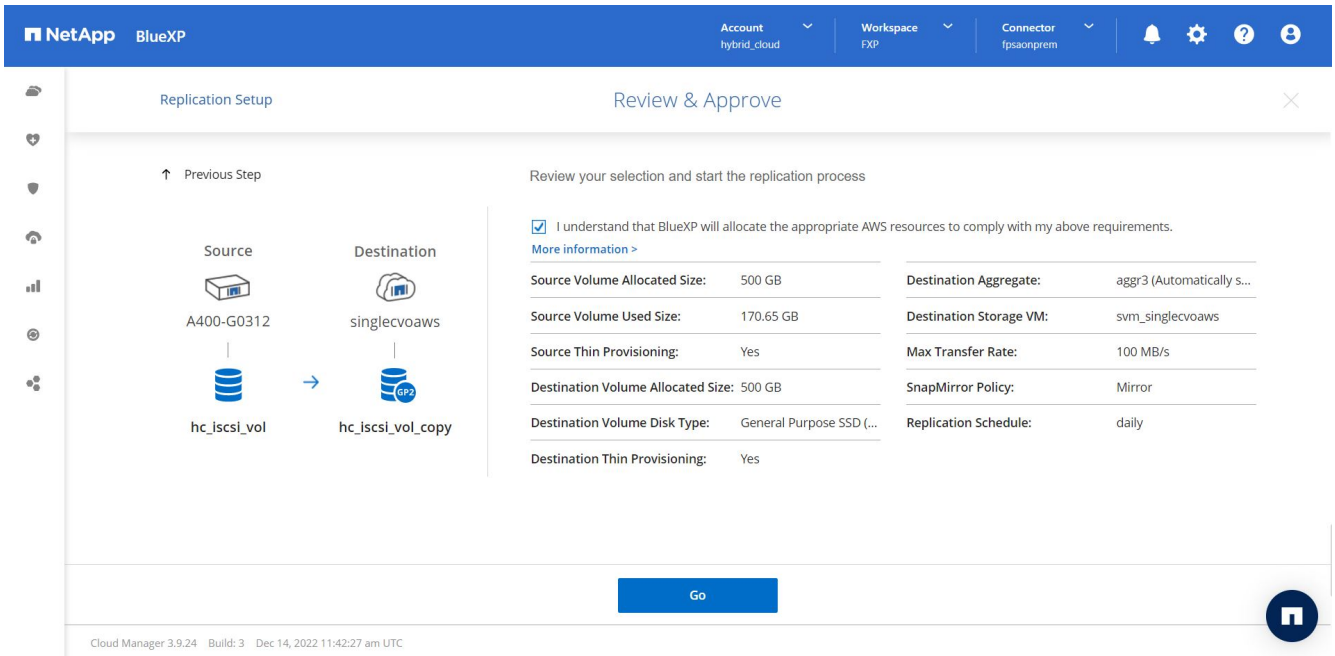


ページを示しています。デフォルトのポリシーである「Mirror」または「Mirror and Backup」が表示されています。"]

9. スケジュール。 1回限りのコピーまたは定期的なスケジュールを選択します。いくつかのデフォルトスケジュールを使用できます。別のスケジュールが必要な場合は、で新しいスケジュールを作成する必要があります `destination cluster` System Manager を使用



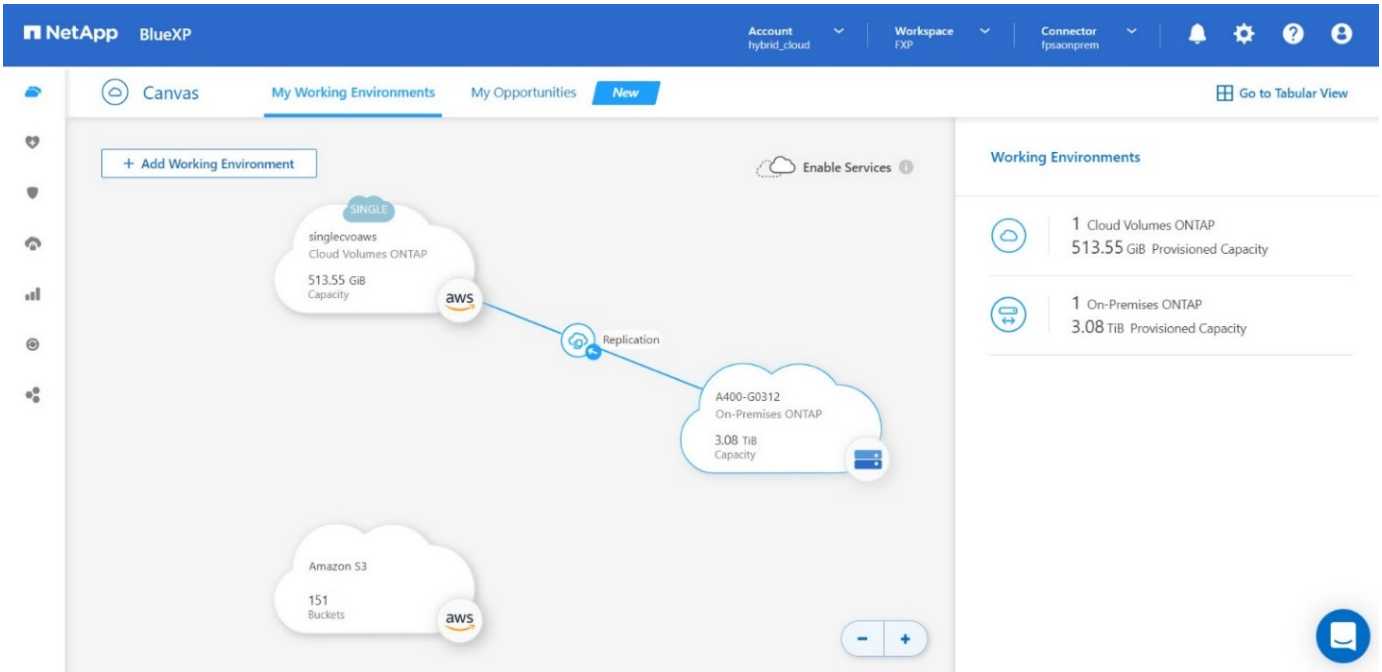
10. *確認。*選択内容を確認し、*移動*をクリックします。



画面を示しています。"]

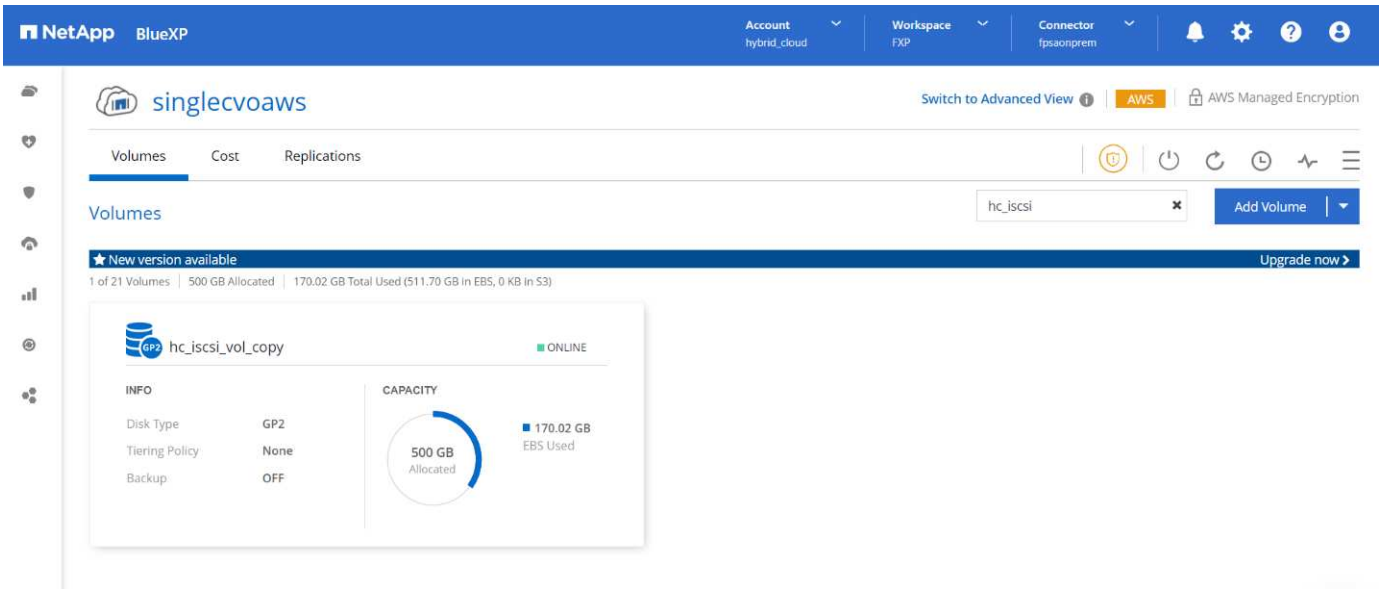
これらの設定手順の詳細については、を参照してください "こちらをご覧ください"。

BlueXPがデータレプリケーションプロセスを開始しますオンプレミスのONTAP システムとCloud Volumes ONTAP の間に確立された*レプリケーション*サービスを確認できます。



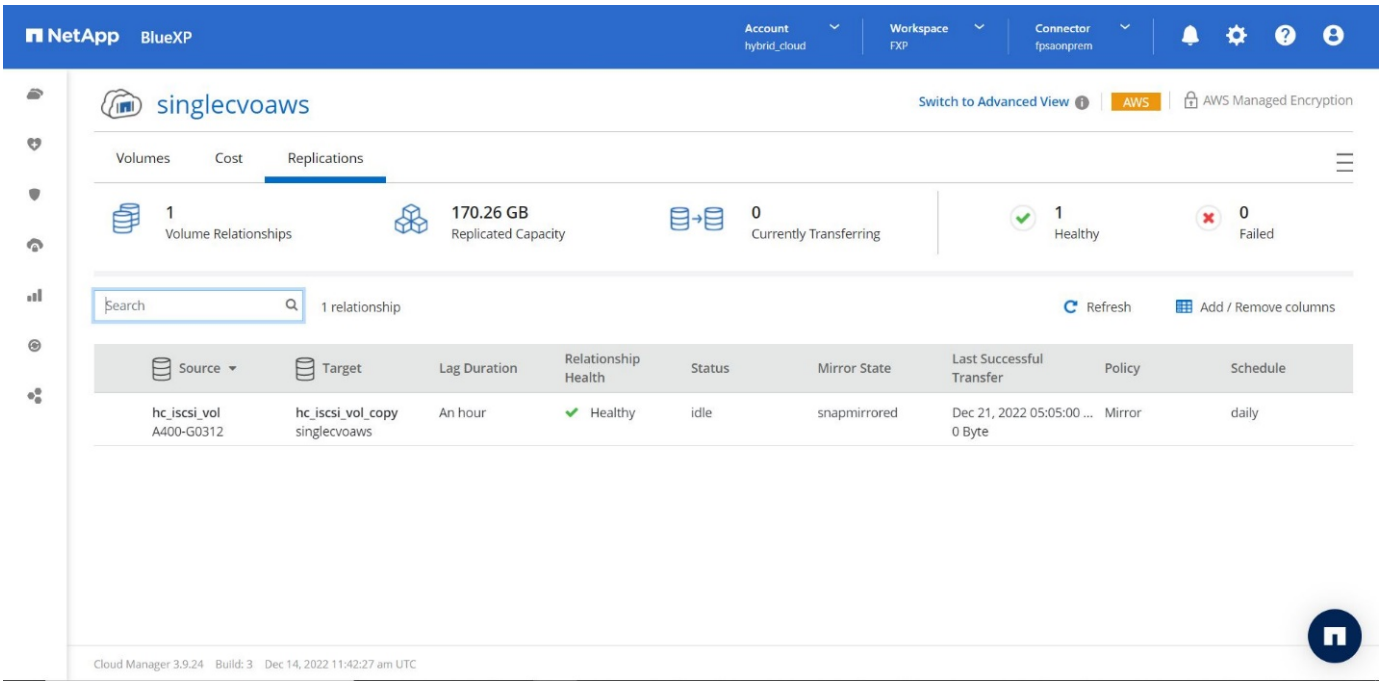
画面を示しています。レプリケーションサービスはCVOインスタンスとオンプレミスのONTAP インスタンスを結ぶ線で示されています。"]

Cloud Volumes ONTAP クラスタでは、新しく作成されたボリュームを確認できます。



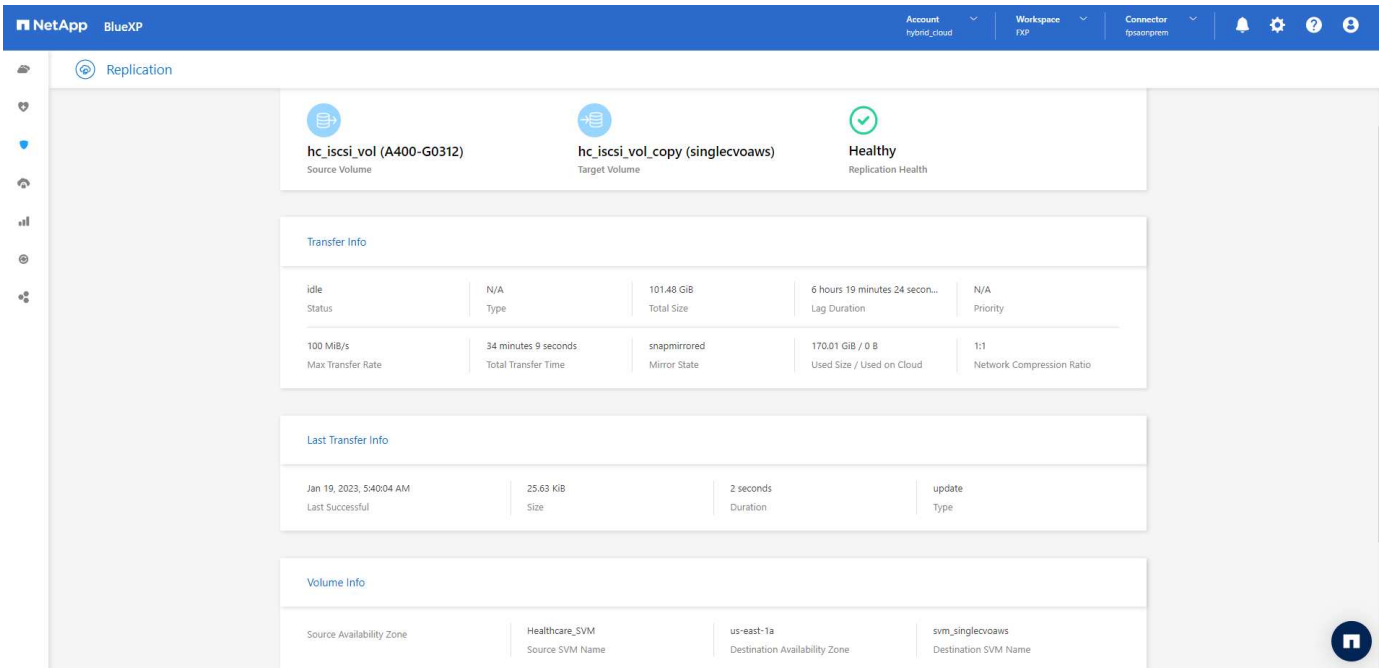
タブを示しています。新しいボリュームが表示されています。"]

オンプレミスボリュームとクラウドボリュームの間にSnapMirror関係が確立されたことを確認することもできます。



タブを示しており、作成したレプリケーション関係に関する情報が表示されています。"]

レプリケーションタスクの詳細については、*[レプリケーション]*タブを参照してください。



タブの下に詳細情報を示しています。"]

"次の例は、解決策の検証です。"

解決策の検証

"前の手順：SAN構成"

このセクションでは、解決策 のユースケースをいくつか確認します。

- SnapMirrorの主なユースケースの1つに、データバックアップがあります。SnapMirrorは、同じクラスタ内またはリモートターゲットにデータをレプリケートすることで、プライマリバックアップツールとして使用できます。
- DR環境を使用したアプリケーション開発テスト（開発とテスト）の実行
- 本番環境で災害が発生した場合のDR。
- データ配信とリモートデータアクセス：

注目すべき点として、この解決策 で検証された比較的少数のユースケースでは、SnapMirrorレプリケーションの全機能を網羅しているわけではありません。

アプリケーションの開発とテスト（開発とテスト）

レプリケートされたデータをDRサイトで迅速にクローニングし、開発/テストアプリケーションに使用することで、アプリケーションの開発期間を短縮できます。DR環境と開発/テスト環境をコロケーションすることで、バックアップやDR施設の利用率を大幅に向上できます。また、オンデマンドの開発/テスト用クローンにより、必要な数のデータコピーを迅速に本番環境に移行できます。

NetApp FlexCloneテクノロジを使用すると、セカンダリコピーの読み取り/書き込みアクセスを許可してすべての本番環境データが利用可能かどうかを確認する場合に、SnapMirrorデスティネーションFlexVol ボリュームの読み取り/書き込みコピーを迅速に作成できます。

DR環境を使用してアプリケーションの開発とテストを実行するには、次の手順を実行します。

1. 本番環境のデータのコピーを作成します。そのためには、オンプレミスボリュームのアプリケーションスナップショットを実行します。アプリケーションスナップショットの作成は、3つのステップで構成されます。 `Lock`、 `Snap`および `Unlock`。

   a. ファイルシステムを休止して、I/Oが中断され、アプリケーションの整合性が維持されるようにします。ファイルシステムにヒットするアプリケーションの書き込みは、手順cで休止解除コマンドが実行されるまで待機状態のままですステップa、b、cは透過的なプロセスまたはワークフローを通じて実行され、アプリケーションのSLAには影響しません。

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
   ```

   このオプションは、指定されたファイルシステムが新しい変更からフリーズされるように要求します。フリーズされたファイルシステムに書き込みを試みるプロセスは、ファイルシステムがフリーズ解除されるまでブロックされます。

   b. オンプレミスボリュームのSnapshotを作成

   ```
   A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
   hc_iscsi_vol -snapshot kamini
   ```

   c. ファイルシステムを休止解除してI/Oを再開します。

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
   ```

   このオプションは、ファイルシステムのフリーズを解除し、操作を続行できるようにするために使用します。フリーズによってブロックされたファイルシステムの変更はブロック解除され、完了することができます。

   アプリケーションと整合性のあるSnapshotは、前述のワークフローをSnapCenter の一部として完全にオーケストレーションしたNetApp SnapCenter を使用して実行することもできます。詳細については、を参照してください "こちらをご覧ください"。

2. SnapMirror更新処理を実行して、業務用システムとDRシステムの同期を維持します。

   ```
   singlecvoaws::> snapmirror update -destination-path
   svm_singlecvoaws:hc_iscsi_vol_copy -source-path
   Healthcare_SVM:hc_iscsi_vol

   Operation is queued: snapmirror update of destination
   “svm_singlecvoaws:hc_iscsi_vol_copy”.
   ```

   BlueXPのGUIの*[Replication]*タブから、SnapMirrorの更新を実行することもできます。

3. 前の手順で作成したアプリケーションSnapshotに基づいてFlexCloneインスタンスを作成します。

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

前のタスクでは、新しいSnapshotも作成できますが、アプリケーションの整合性を確保するには、上記と同じ手順を実行する必要があります。

4. FlexCloneボリュームをアクティブ化して、クラウドでEHRインスタンスを起動します。

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                    Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                 /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. クラウドのEHRインスタンスで次のコマンドを実行して、データまたはファイルシステムにアクセスします。
   a. ONTAP ストレージを検出マルチパスのステータスを確認します。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                     /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. ボリュームグループをアクティブ化します。

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. ファイル・システムをマウントし’ファイル・システム情報の概要を表示します

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

これにより、アプリケーションの開発とテストにDR環境を使用できるかどうかが検証されます。DRストレージでアプリケーションの開発とテストを実行すると、ほとんどの時間アイドル状態になる可

能性のあるリソースをより有効に活用できます。

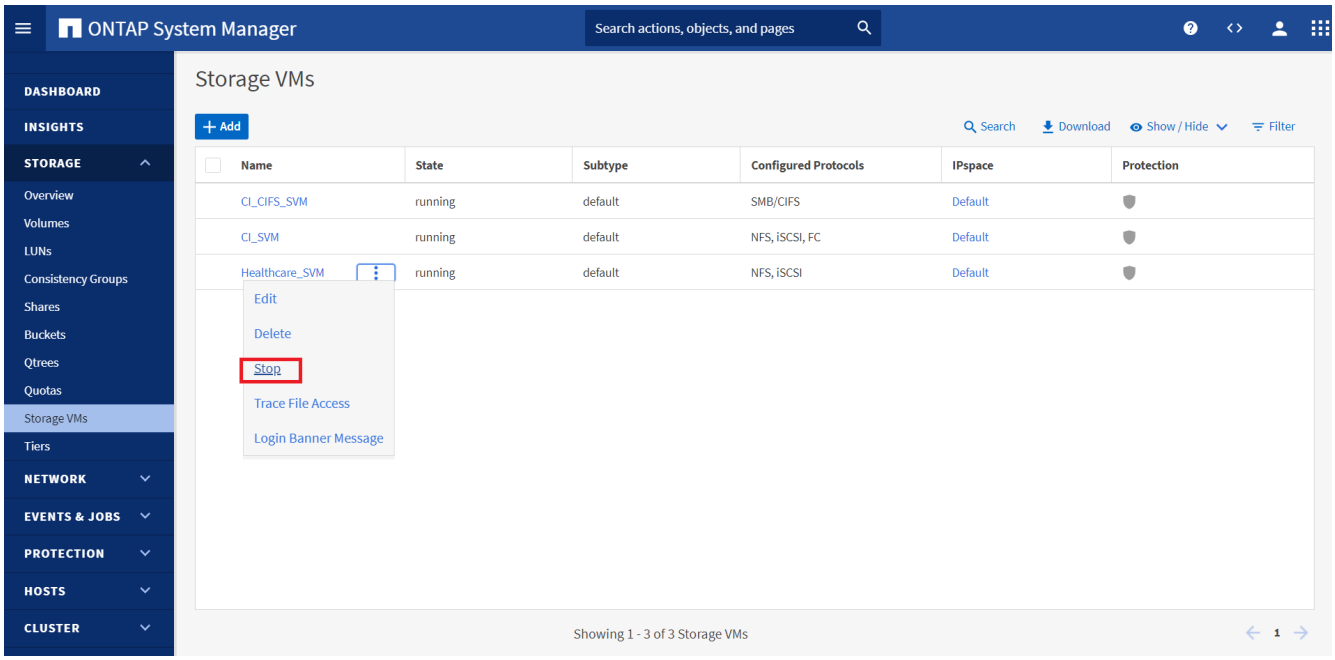
ディザスタリカバリ

SnapMirrorテクノロジは、DR計画の一部としても使用されます。重要なデータが物理的に別の場所にレプリケートされている場合、重大な災害が原因 発生しても、ビジネスクリティカルなアプリケーションで長期間データを使用できなくなることはありません。クライアントは、破損、偶発的な削除、自然災害などから本番サイトをリカバリするまで、レプリケートされたデータにネットワーク経由でアクセスできます。

プライマリサイトへのフェイルバックの場合、SnapMirrorを使用すると、SnapMirror関係をDRサイトからプライマリサイトに反転させるだけで、変更されたデータや新しいデータのみをDRサイトからプライマリサイトに転送して、DRサイトとDRサイトを効率的に再同期できます。プライマリサイトで通常のアプリケーション運用が再開されると、SnapMirrorは、ベースライン転送をもう1回行わずにDRサイトへの転送を続行します。

DRシナリオが成功するかどうかを検証するには、次の手順を実行します。

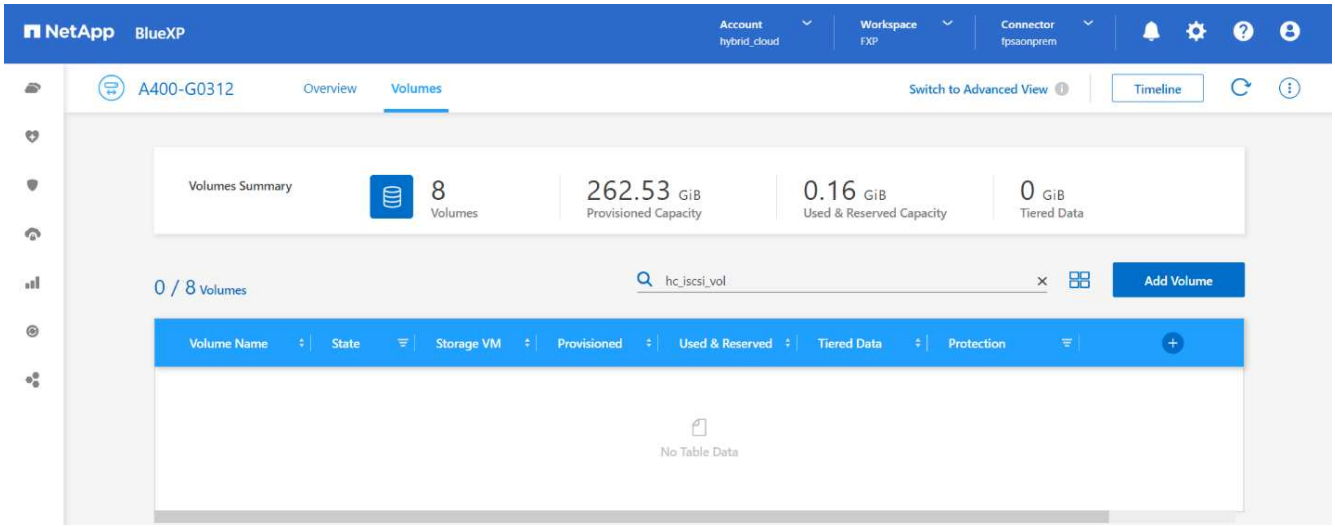
1. オンプレミスのONTAP ボリュームをホストするSVMを停止して、ソース（本番）側で災害をシミュレートします (`hc_iscsi_vol`）。



ドロップダウンにある[stop]オプションを示しています。"]

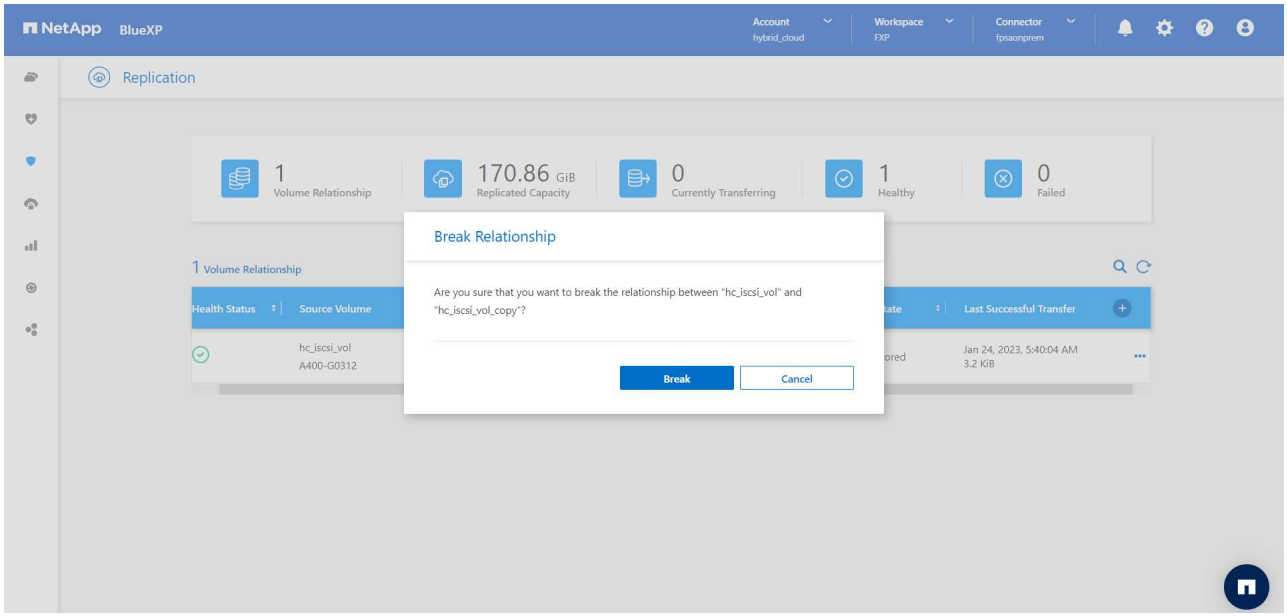
アプリケーションのSnapshotを頻繁に作成できるように、FlexPod インスタンスのオンプレミスONTAPとAWSのCloud Volumes ONTAP の間でSnapMirrorレプリケーションがすでに設定されていることを確認します。

SVMが停止したあと、 `hc_iscsi_vol` ボリュームはBlueXPに表示されません。



2. CVOでDRをアクティブ化

   a. オンプレミスのONTAP とCloud Volumes ONTAP の間のSnapMirrorレプリケーション関係を解除し、CVOのデスティネーションボリュームを昇格します (`hc_iscsi_vol_copy`）を本番環境に移行します。



   SnapMirror関係を解除すると、デスティネーションボリュームのタイプがデータ保護（DP）から読み書き可能（rw）に変わります。

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume             type
--------------- ----------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

   b. Cloud Volumes ONTAP でデスティネーションボリュームをアクティブ化し、クラウド内のEC2インスタンスでEHRインスタンスを起動します。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. クラウド内のEHRインスタンス上のデータとファイルシステムにアクセスするには、まずONTAP ストレージを検出し、マルチパスのステータスを確認します。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
---------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. ボリュームグループをアクティブ化します。

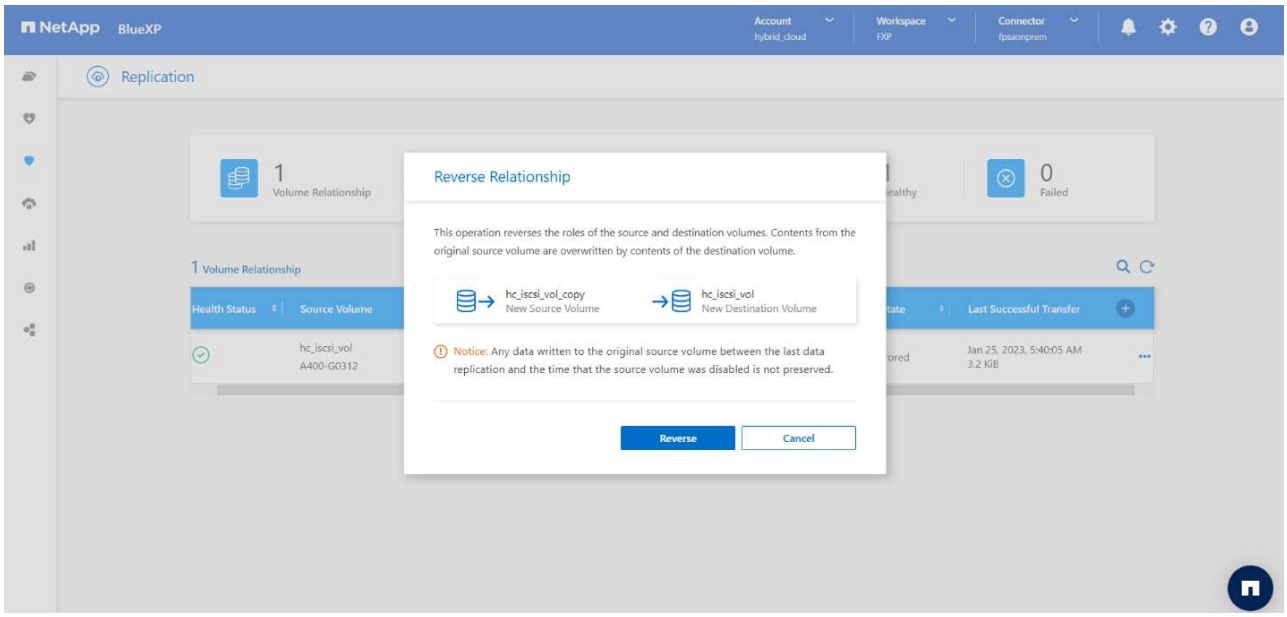
```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

e. 最後に、ファイルシステムをマウントし、ファイルシステム情報を表示します。

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                  1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

この出力は、災害から本番サイトがリカバリされるまで、ユーザがネットワーク経由でレプリケートされたデータにアクセスできることを示しています。

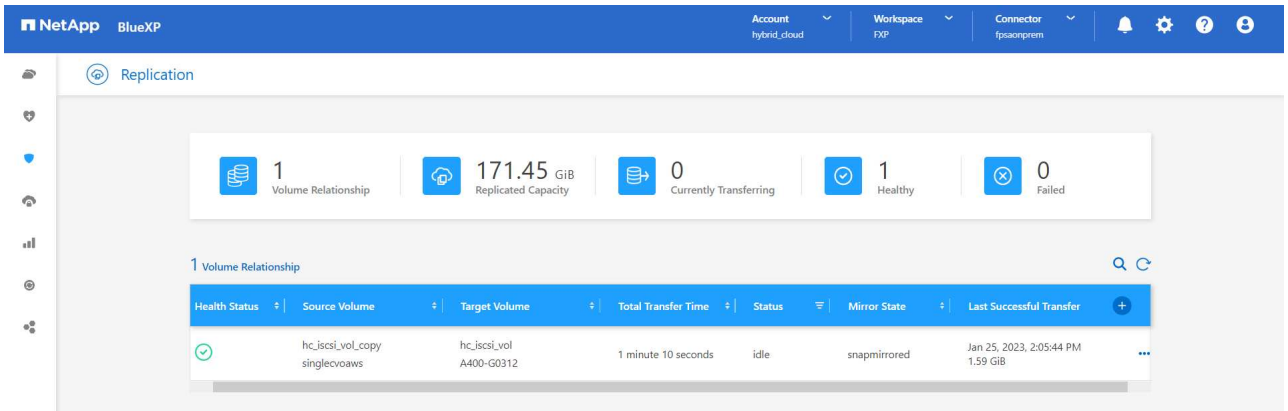
f. SnapMirror関係を反転します。この処理では、ソースボリュームとデスティネーションボリュームの役割が入れ替わります。



ボックスを示しています。"]

この処理を実行すると、元のソースボリュームの内容がデスティネーションボリュームの内容で上書きされます。これは、オフラインになったソースボリュームを再アクティブ化する場合に役立ちます。

CVOボリュームに移動します (`hc_iscsi_vol_copy`）がソースボリュームになり、オンプレミスボリュームになります (`hc_iscsi_vol`）がデスティネーションボリュームになります。



前回のデータレプリケーションからソースボリュームが無効になったまでの間に元のソースボリュームに書き込まれたデータは保持されません。

a. CVOボリュームへの書き込みアクセスを確認するには、クラウドのEHRインスタンスに新しいファイルを作成します。

```
cd /file1/
sudo touch newfile
```

業務用サイトが停止しても、クライアントは引き続きデータにアクセスし、Cloud Volumes ONTAP ボリューム（現在はソースボリューム）への書き込みも実行できます。

プライマリサイトへのフェイルバックの場合、SnapMirrorを使用すると、SnapMirror関係をDRサイトからプライマリサイトに反転させるだけで、変更されたデータや新しいデータのみをDRサイトからプライマリサイトに転送して、DRサイトとDRサイトを効率的に再同期できます。プライマリサイトで通常のアプリケーション運用が再開されると、SnapMirrorは、ベースライン転送をもう1回行わずにDRサイトへの転送を続行します。

このセクションでは、業務用サイトで災害が発生した場合のDRシナリオの適切な解決方法について説明します。これで、ソースサイトのリストア中にクライアントにサービスを提供できるアプリケーションが、データを安全に消費できるようになります。

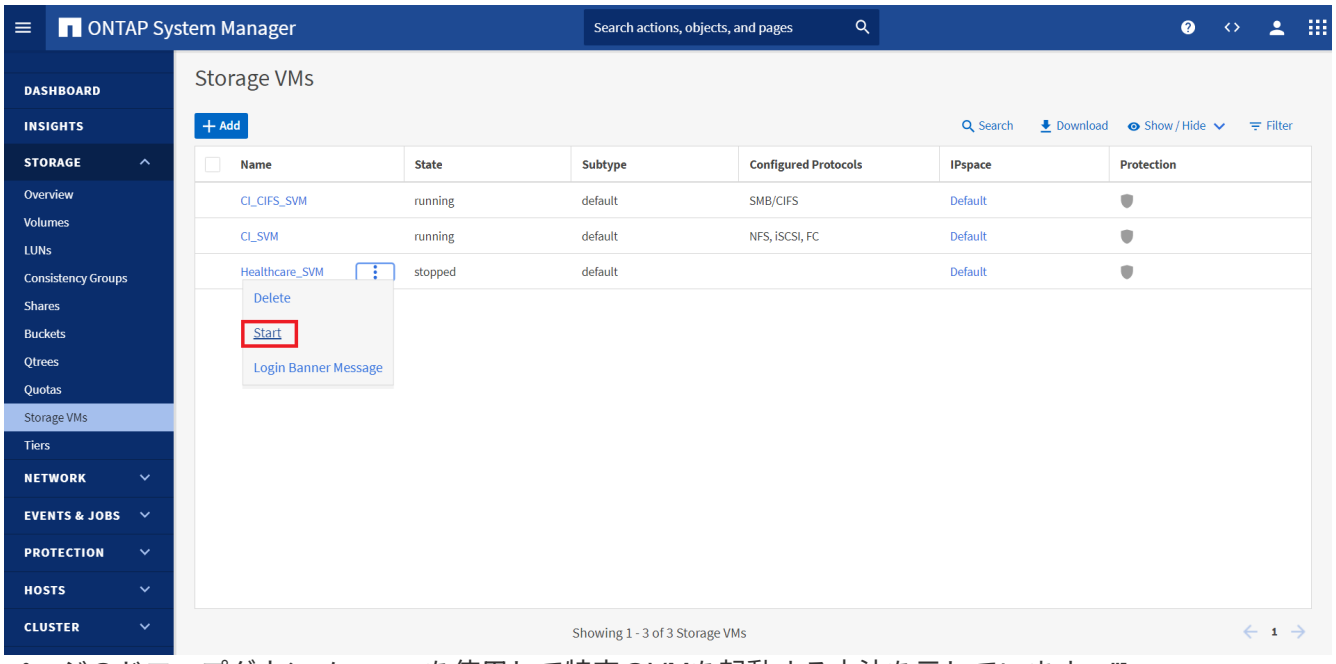
本番サイトでのデータの検証

業務用サイトをリストアしたら、元の構成がリストアされ、クライアントがソースサイトのデータにアクセスできることを確認する必要があります。

このセクションでは、ソースサイトを立ち上げ、オンプレミスのONTAP とCloud Volumes ONTAP 間のSnapMirror関係をリストアし、最後にソース側でデータ整合性チェックを実行します

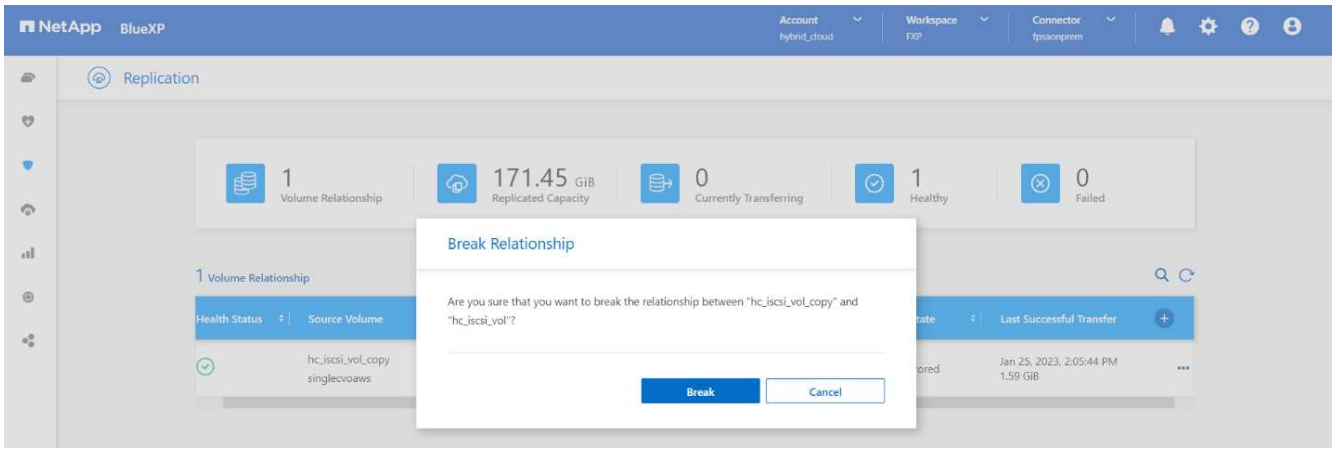
業務用サイトでは、次の手順 を使用してデータを検証できます。

1. ソースサイトが稼働していることを確認します。これを行うには、オンプレミスのONTAP ボリュームをホストするSVMを起動します (`hc_iscsi_vol`）。



ページのドロップダウンメニューを使用して特定のVMを起動する方法を示しています。"]

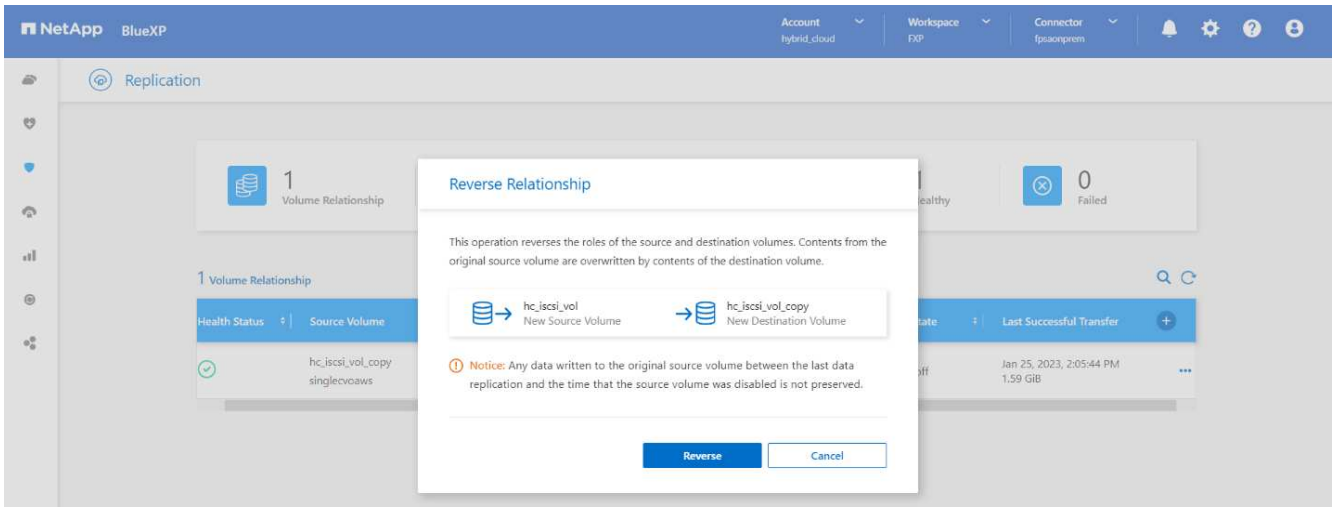
2. Cloud Volumes ONTAP とオンプレミスのONTAP 間のSnapMirrorレプリケーション関係を解除し、オンプレミスボリュームを昇格 (`hc_iscsi_vol`) を本番環境に戻します。



SnapMirror関係を解除すると、オンプレミスのボリュームタイプがデータ保護（DP）から読み取り/書き込み（RW）に変わります。

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver         volume        type
--------------- ------------- ----
Healthcare_SVM hc_iscsi_vol RW
```

3. SnapMirror関係を反転します。今度はオンプレミスのONTAP ボリュームです (`hc_iscsi_vol`) がソースボリュームになり、Cloud Volumes ONTAP ボリュームになります (`hc_iscsi_vol_copy`) がデスティネーションボリュームになります。



これらの手順を実行することで、元の構成が正常に復元されました。

4. オンプレミスのEHRインスタンスをリブートします。ファイルシステムをマウントし、を確認します `newfile` 本番環境がダウンしていたときにクラウドのEHRインスタンスに作成したものもここに存在します。

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37  dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77  kamini
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38  dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78  latest_file
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39  dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79  newfile
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40  dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80
```

ソースからデスティネーションへのデータレプリケーションが正常に完了し、データの整合性が維持されていると推測できます。これで、本番サイトでのデータの検証は完了です。

"次は終わりです"

まとめ

"前のバージョン：解決策 の検証。"

ほとんどの医療機関では、ハイブリッドクラウドの構築が、いつでもデータにアクセスできるようにすることを目標としています。この解決策 では、Cloud Volumes ONTAP を備えたFlexPod ハイブリッドクラウド解決策 を実装し、ネットアップのSnapMirrorレプリケーションテクノロジを活用して、ヘルスケアアプリケーションとワークロードのバックアップとリカバリのいくつかのユースケースを検証しました。

FlexPod は、Ciscoとネットアップの戦略的パートナーシップが提供する厳格なテストと検証済みの統合インフラです。予測可能な低レイテンシのシステムパフォーマンスと高可用性を実現するように設計されています。このアプローチにより、EHRの快適性レベルが高くなり、最終的にEHRシステムのユーザーにとって最適な応答時間が得られます。

ネットアップなら、オンプレミスのデータセンターでネットアップのストレージ機能を実行するのと同じように、本番環境のEHR、ディザスタリカバリ、バックアップ、階層化をクラウドで実行できます。ネットアップは、NetApp Cloud Volumes ONTAP を使用して、クラウドでEHRを効果的に実行するために必要なエンタープライズクラスの機能とパフォーマンスを提供します。ネットアップのクラウドオプションは、iSCSI経由のブロックとNFSまたはSMB経由のファイルを提供します。

この解決策 は、医療機関のニーズに応え、デジタル変革に向けた一歩を踏み出すためのものです。また、アプリケーションやワークロードを効率的に管理するのにも役立ちます。

"次へ：追加情報の検索場所。"

追加情報の参照先

"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 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"

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP の略

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- AWS での Cloud Volumes ONTAP のクイックスタート

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- SnapMirror レプリケーション

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- TR-3928：『NetApp Best Practices for Epic』

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- TR-4693 ：『 FlexPod Datacenter for Epic EHR Deployment Guide 』

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- FlexPod for Epicの略

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

- NetApp Interoperability Matrix Tool で確認できます

  "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.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- 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	2023年3月	初版

ネットアップのCloud Volumes ONTAP とCisco Intersightを活用したFlexPod ハイブリッドクラウドfor Google Cloud Platform

TR-4939：『FlexPod Hybrid Cloud for Google Cloud Platform with NetApp Cloud Volumes ONTAP and Cisco Intersight』

Ruchika Lahoti、ネットアップ

はじめに

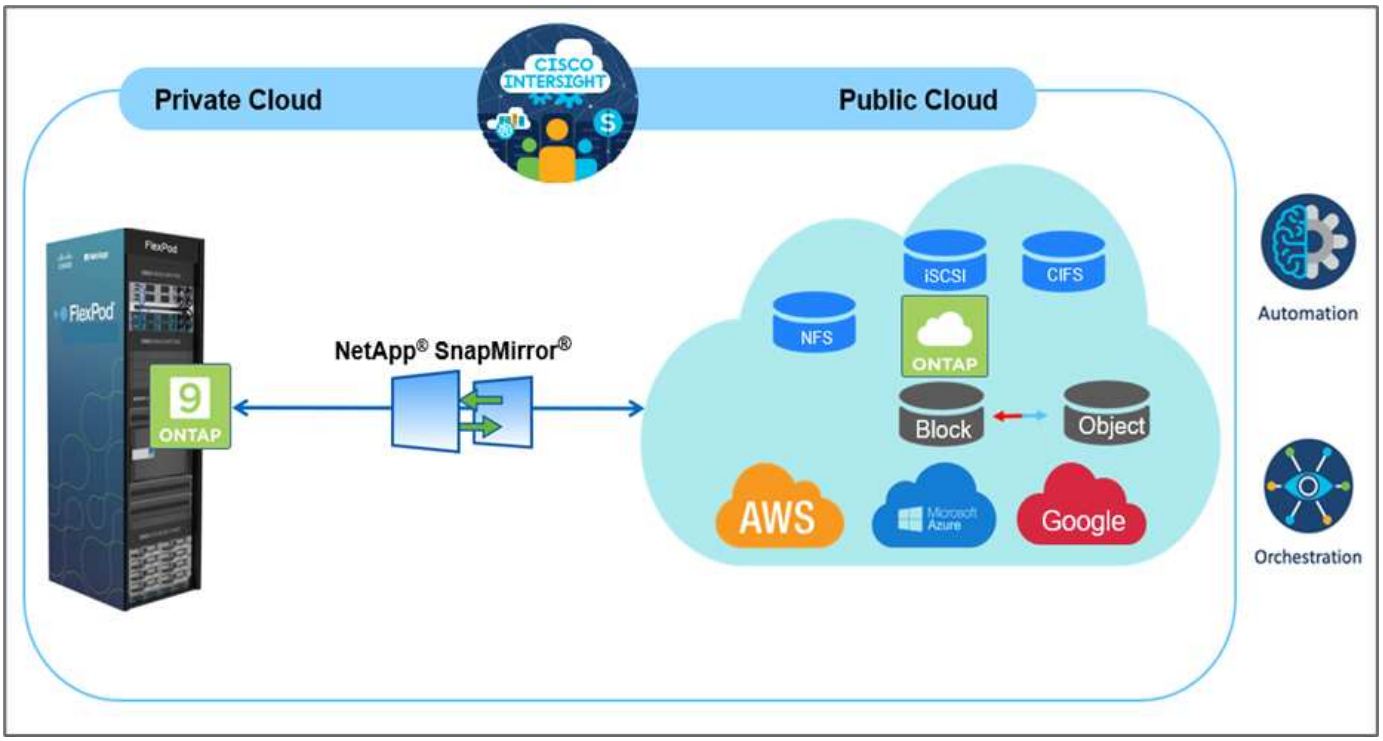
企業の継続性を確保するうえで重要な目標は、ディザスタリカバリ（DR）によってデータを保護することです。DRを使用すると、企業は業務をセカンダリサイトにフェイルオーバーし、あとでプライマリサイトに効率的かつ確実にリカバリおよびフェイルバックできます。自然災害、ネットワーク障害、ソフトウェアの脆弱性、人為的ミスなど、さまざまな懸念があるため、DR戦略を開発することがITの最優先事項となっています。

DRに関しては、プライマリサイトで実行しているすべてのワークロードを、DRサイトで忠実に再現する必要があります。組織には、データベース、ファイルサービス、NFS、iSCSIストレージなど、すべてのエンタープライズデータの最新コピーも必要です。本番環境のデータは常に更新されるため、変更は定期的にDRサイトに転送する必要があります。

DR環境の導入は、インフラやサイトに依存しないことが求められるため、ほとんどの組織にとって困難な課題です。必要なリソースの数や、セカンダリデータセンターのセットアップ、テスト、メンテナンスにかかるコストは、通常、本番環境全体のコストに迫ることがあります。データを継続的に同期し、シームレスなフェイルオーバーとフェイルバックを確立しながら、最小限のデータ容量で十分な保護を維持することは困難です。DRサイトを構築したら、本番環境からデータをレプリケートし、それを同期して先に進めるという課題に直面します。

このテクニカルレポートでは、FlexPod コンバージドインフラ解決策 、Google Cloud上のNetApp Cloud Volumes ONTAP 、およびCisco Intersightを統合して、DR用のハイブリッドクラウドデータセンターを形成しています。この解決策 では、Cisco Intersight Cloud Orchestratorを使用したオンプレミスONTAP ワークフローの設計と実行について説明します。また、ネットアップCloud Volumes ONTAP の導入、FlexPod とCloud Volumes ONTAP 間のデータレプリケーションおよびDRのオーケストレーションと自動化についても、Cisco Intersight Service for橋(Cisco Intersight Service for橋Corp Terraform)を使用して説明します。

次の図は、解決策 の概要を示しています。



この解決策 には、次のような複数の利点があります。

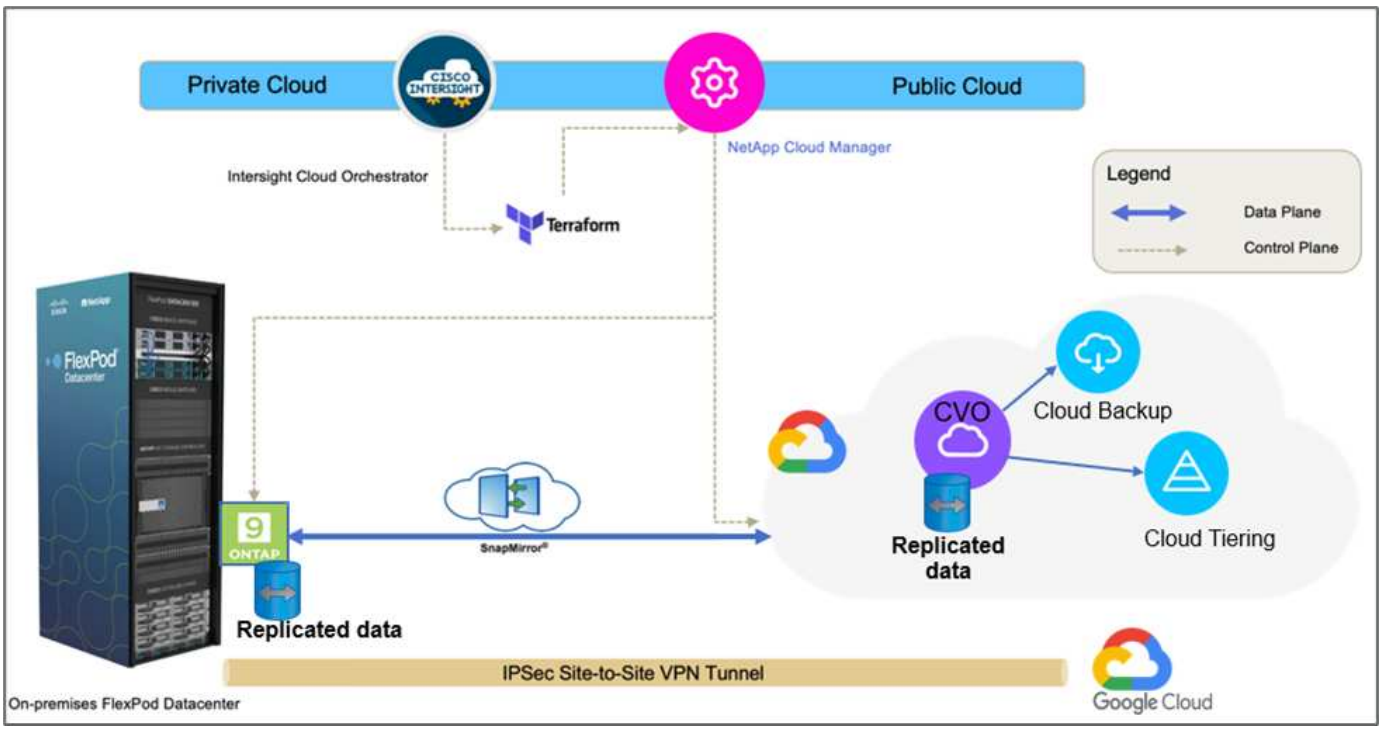
- オーケストレーションと自動化。 Cisco Intersightは、自動化を通じて提供される一貫したオーケストレーションフレームワークを提供することで、FlexPod ハイブリッドクラウドインフラの日常的な運用を簡易化します。
- カスタマイズされた保護。 Cloud Volumes ONTAP は、ONTAP からクラウドへのブロックレベルのデータレプリケーションを提供し、差分更新によってデスティネーションを最新の状態に維持します。ユーザは、たとえば、転送されるソースでの変更に基づいて、5分ごとまたは1時間ごとに同期スケジュールを指定できます。
- *シームレスなフェイルオーバーとフェイルバック。*災害が発生した場合、ストレージ管理者はCloud Volume に迅速にフェイルオーバーできます。プライマリサイトがリカバリされると、DR環境で作成された新しいデータがソースボリュームと同期され、セカンダリデータレプリケーションが再確立されます。
- *効率性：*データ圧縮、シンプロビジョニング、重複排除により、セカンダリクラウドコピー用のストレージスペースとコストを最適化します。データは圧縮と重複排除が行われた形式でブロックレベルで転送されるため、転送速度が向上します。また、データは低コストのオブジェクトストレージに自動的に階層化され、DRシナリオなどでアクセスされたときにのみハイパフォーマンスストレージに戻されます。これにより、継続的なストレージコストを大幅に削減できます。
- * ITの生産性向上。* Intersightをインフラストラクチャおよびアプリケーションのライフサイクル管理向けの単一のセキュアなエンタープライズクラスのプラットフォームとして使用することで、解決策 の構成管理と手動タスクの自動化が容易になります。

対象者

本ドキュメントが対象とする主な読者は、セールスエンジニア、フィールドコンサルタント、プロフェッショナルサービス、ITマネージャ、 パートナー様のエンジニア、サイト信頼性エンジニア、クラウドアーキテクト、クラウドエンジニア、お客様が、ITの効率化とITイノベーションの実現のために構築されたインフラを活用したいと考えています。

解決策 トポロジ

このセクションでは、解決策 の論理トポロジについて説明します。次の図は、オンプレミスのFlexPod 環境、Google Cloudで実行されているNetApp Cloud Volumes ONTAP 、Cisco Intersight、NetApp Cloud Managerの解決策 トポロジを示しています。



コントロールプレーンとデータプレーンは、エンドポイント間で明確に示されます。データプレーンは、セキュアなサイト間VPN接続を使用して、FlexPod All Flash FAS で実行されているONTAP インスタンスをGoogle Cloud上のNetApp Cloud Volumes ONTAP インスタンスに接続します。

FlexPod からNetApp Cloud Volumes ONTAP へのワークロードデータのレプリケーションはNetApp SnapMirrorによって処理され、オンプレミス環境とクラウド環境の両方でCisco Intersight Cloud Orchestrator を使用して全体的なプロセスが調整されます。Cisco Intersight Cloud OrchestratorはNetApp Cloud Managerのリソースプロバイダとして、NetApp Cloud Volumes ONTAP の導入に関連する処理を実行し、データレプリケーション関係を確立します。

> この解決策 では、NetApp Cloud Volumes ONTAP インスタンスにあるコールドデータのバックアップと階層化もオプションでサポートされています。

"次の例は、解決策 コンポーネントです。"

解決策コンポーネント

"Previous ：解決策の概要を示します。"

FlexPod

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフトウェアの定義済みセットです。FlexPod には、NetApp ONTAP ストレージ、Cisco Nexusネットワーク、Cisco MDSストレージネットワーク、Cisco Unified Computing System（Cisco UCS）が含まれています。この設計は、ネットワーク、コンピューティング、ストレージを1つのデータセンターラックに収容でき

る柔軟性を備えています。また、お客様のデータセンター設計に従って導入することもできます。ポート密度を使用すると、ネットワークコンポーネントは複数の構成に対応できます。

Cisco Intersightの

Cisco Intersightは、従来のアプリケーションやクラウドネイティブなインフラに向けて、インテリジェントな自動化、オブザーバビリティ、最適化を実現するSaaSプラットフォームです。このプラットフォームは、ITチームの変化を促進し、ハイブリッドクラウド向けに設計された運用モデルを提供します。Cisco Intersightには、次のようなメリットがあります。

- *迅速な提供。*俊敏性に優れたソフトウェア開発モデルにより、クラウドまたはお客様のデータセンターからサービスとして提供され、頻繁な更新と継続的な技術革新を実現します。このようにして、お客様は基幹業務へのサービス提供の高速化に注力できます。
- *運用の簡素化。*共通のインベントリ、認証、APIを備えた単一のセキュアなSaaS提供ツールを使用して、スタック全体とすべての場所で作業できるようにし、チーム間のサイロを排除し、運用を簡素化します。オンプレミスの物理サーバやハイパーバイザーの管理からVM、Kubernetes、サーバレス、自動化、オンプレミスとパブリッククラウドの両方にわたって最適化とコスト管理を実現
- 継続的な最適化。 Cisco Intersightが提供するインテリジェンスを、Cisco TACだけでなくすべてのレイヤで使用して、環境を継続的に最適化します。このインテリジェンスは、推奨される自動化可能なアクションに変換されるため、ワークロードの移動や物理サーバの状態の監視から、コスト削減へと、お客様が使用するパブリッククラウドの推奨まで、あらゆる変化にリアルタイムで適応できます。

Cisco Intersightには、UCSM Managed Mode（UMM）とIntersight Managed Mode（IMM）という2つの管理操作モードがあります。ファブリックインターコネクトの初期セットアップ中に、ファブリック接続Cisco UCSシステムにネイティブUmmまたはIMMを選択できます。この解決策 では、ネイティブIMMが使用されます。

Cisco Intersightのライセンス

Cisco Intersightは、複数の階層を含むサブスクリプションベースのライセンスを使用しています。

Cisco Intersightのライセンスレベルは次のとおりです。

- * Cisco Intersight Essential.*には、すべての基本機能に加えて次の機能が含まれています。
  - Cisco UCS Centralの特長です
  - Cisco IMC Supervisorの使用権
  - サーバプロファイルを使用したポリシーベースの設定
  - ファームウェア管理
  - ハードウェア互換性リスト（HCL）との互換性の評価
- * Cisco Intersight Advantage *には、Essentials階層の機能に加え、次の機能が含まれます。
  - 物理コンピューティング、ネットワーク、ストレージ、VMware仮想化、AWSパブリッククラウド全体で、ウィジェット、インベントリ、容量、利用率、ドメイン間のインベントリ相関関係を確認できます。
  - お客様が重要なセキュリティアラートを受信し、影響を受けるエンドポイントデバイスに関するフィールド通知を受け取ることができるシスコセキュリティアドバイザリサービス。
- * Cisco Intersight Premierは、Advantageレベルで提供される機能に加えて、次の機能を提供します。
  - Ciscoとサードパーティのコンピューティング、ネットワーク、ストレージ、統合システム、仮想化向

けのIntersight Cloud Orchestrator（ICO） コンテナ、パブリッククラウドの各プラットフォームで実現できます

- Cisco UCS Directorのフルサブスクリプションを追加料金なしでご利用いただけます。

Intersightのライセンスと各ライセンスでサポートされる機能の詳細については、こちらをご覧ください "こちらをご覧ください"。

> この解決策 では、インテル®Intersightクラウド・オーケストレーション・サービスとインテル®Intersightサービスを使用して、これらの機能は、Intersight Premierライセンスを持つユーザが利用できるため、このライセンス層を有効にする必要があります。

クラウドと**ICO**の統合

Cisco Intersight Cloud Orchestrator（ICO）を使用すると、Terraform Cloud（TFC）APIと呼ばれるワークフローを作成、実行できます。Web API要求の呼び出しタスクは、Terraform Cloudをターゲットとしてサポートし、HTTPメソッドを使用してTerraform Cloud APIで構成できます。そのため、このワークフローでは、汎用のAPIタスクやその他の操作を使用して、複数のTerraform Cloud APIを呼び出すタスクを組み合わせることができます。ICO機能を使用するには、プレミアライセンスが必要です。

Cisco Intersight Assistの導入

Cisco Intersight Assistを使用すると、エンドポイントデバイスをCisco Intersightに追加できます。データセンターには、Cisco Intersightに直接接続できない複数のデバイスが存在する場合があります。Cisco Intersightでサポートされているが、直接接続されていないデバイスには、接続メカニズムが必要です。Cisco Intersight Assistは、この接続メカニズムを提供し、Cisco Intersightへのデバイスの追加を支援します。

Cisco Intersight Assistは、Cisco Intersight Virtual Appliance内で利用できます。これは、Open Virtual Appliance（OVA；オープン仮想アプライアンス）ファイル形式に含まれる展開可能な仮想マシンとして配布されます。アプライアンスはESXiサーバにインストールできます。詳細については、を参照してください "『Cisco Intersight Virtual Appliance Getting Started Guide』"。

Intersight AssistをIntersightに請求した後、[Claim Through Intersight Assist]オプションを使用してエンドポイントデバイスを請求できます。詳細については、を参照してください "はじめに"。

NetApp Cloud Volumes ONTAP の略

- 組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、クローニングを活用して、ストレージコストを最小限に抑えます。
- クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を実現します。
- Cloud Volumes ONTAP では、業界をリードするレプリケーションテクノロジであるNetApp SnapMirrorを使用して、オンプレミスのデータをクラウドにレプリケートすることで、複数のユースケースでセカンダリコピーを簡単に利用できます。
- また、Cloud Volumes ONTAP はCloud Backup Service との統合により、クラウドデータの保護と長期保管のためのバックアップおよびリストア機能も提供します。
- アプリケーションをオフラインにすることなく、ハイパフォーマンスとローパフォーマンスのストレージプールをオンデマンドで切り替えます。
- NetApp SnapCenter を使用してSnapshotコピーの整合性を確保する。
- Cloud Volumes ONTAP は、データ暗号化をサポートし、ウィルスやランサムウェアからの保護を提供し

ます。

- クラウドデータセンスとの統合により、データコンテキストを把握し、機密データを識別できます。

Cloud Central にアクセスできます

Cloud Centralは、ネットアップのクラウドデータサービスにアクセスして管理するための一元的な場所を提供します。これらのサービスを利用すると、重要なアプリケーションをクラウドで実行したり、自動化されたDR サイトを作成したり、 SaaS データをバックアップしたり、複数のクラウド間でデータを効果的に移行および制御したりすることができます。詳細については、を参照してください "Cloud Central にアクセスできます"。

クラウドマネージャ

Cloud Managerは、エンタープライズクラスのSaaSベースの管理プラットフォームです。ITエキスパートやクラウドアーキテクトは、ネットアップのクラウドソリューションを使用してハイブリッドマルチクラウドインフラを一元管理できます。オンプレミスとクラウドのストレージを表示および管理する一元化されたシステムを提供し、複数のハイブリッドクラウドプロバイダとアカウントをサポートします。詳細については、を参照してください "クラウドマネージャ"。

コネクタ

Connectorを使用すると、Cloud Managerでパブリッククラウド環境内のリソースやプロセスを管理できます。コネクタインスタンスは、Cloud Managerが提供するさまざまな機能を使用するために必要です。クラウドまたはオンプレミスのネットワークに導入できます。Connectorは次の場所でサポートされます。

- AWS
- Microsoft Azure
- Google Cloud
- オンプレミス

NetApp Active IQ Unified Manager の略

NetApp Active IQ Unified Manager では、設計を一新したわかりやすいインターフェイスからONTAP ストレージクラスタを監視でき、集合知やAI分析から得た情報を活用できます。運用、パフォーマンス、プロアクティブな分析情報を提供し、ストレージ環境と仮想マシン上で実行される環境を包括的に分析します。ストレージインフラで問題 が発生すると、Unified Managerから問題 の詳細情報を通知してルート原因 を特定できるようになります。仮想マシンダッシュボードではVMのパフォーマンス統計を確認でき、これにより、ネットワーク経由でダウンしているvSphereホストからストレージへのI/Oパス全体を調査できます。

一部のイベントには、問題 を修正するための対応策も用意されています。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントにカスタムアラートを設定できます。Active IQ Unified Manager を使用すると、容量や使用状況の傾向を予測して問題が発生する前にプロアクティブに対処することができるため、長期的な問題につながる短期的な事後対処策を実施する必要がなくなり、ユーザのストレージ要件に合わせて計画を立てることができます。

VMware vSphere の場合

VMware vSphereは、大量のインフラ（CPU、ストレージ、ネットワークなどのリソース）をシームレスで汎用性に優れた動的な運用環境として包括的に管理する仮想化プラットフォームです。個々のマシンを管理する従来のオペレーティングシステムとは異なり、VMware vSphereはデータセンター全体のインフラストラクチャを集約して、必要なアプリケーションに迅速かつ動的に割り当てられるリソースを備えた単一の強力なサー

バを作成します。

VMware vSphereの詳細については、を参照してください "リンクをクリックしてください"。

VMware vSphere vCenterの場合

VMware vCenter Serverでは、1つのコンソールからすべてのホストとVMを統合的に管理でき、クラスタ、ホスト、およびVMのパフォーマンス監視を集約できます。VMware vCenter Serverを使用すると、管理者は、コンピューティングクラスタ、ホスト、VM、ストレージ、ゲストOS、 仮想インフラストラクチャのその他の重要なコンポーネントVMware vCenterは、VMware vSphere環境で使用できる豊富な機能を管理します。

ハードウェアとソフトウェアのバージョン

このハイブリッドクラウド解決策 は、サポート対象のバージョンのソフトウェア、ファームウェア、ハードウェアを実行しているFlexPod 環境に拡張できます。このバージョンは、NetApp Interoperability Matrix ToolおよびCisco UCSハードウェア互換性リストで定義されています。

ネットアップのオンプレミス環境でベースラインプラットフォームとして使用されているFlexPod 解決策は、前述のガイドラインと仕様に従って導入されています "こちらをご覧ください"。

この環境内のネットワークはACIベースです。詳細については、を参照してください "こちらをご覧ください"。

- 詳細については、次のリンクを参照してください。
- "NetApp Interoperability Matrix Tool で確認できます"
- "VMware Compatibility Guide 』を参照してください"
- "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"

次の表に、FlexPod のハードウェアとソフトウェアのリビジョンを示します。

コンポーネント	プロダクト	バージョン
コンピューティング	Cisco UCS X210-M6	5.0（1b）
	Cisco UCSファブリックインターコネクト6454	4.2（2a）
ネットワーク	Cisco Nexus 9332C（スパイン）	14.2（7秒）
	Cisco Nexus 9336C-FX2（リーフ）	14.2（7秒）
	Cisco ACI	4.2（7秒）
ストレージ	NetApp AFF A220	9.11.1
	NetApp ONTAP Tools for VMware vSphere の略	9.10
	NetApp NFS Plugin for VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
ソフトウェア	vSphere ESXiの場合	7.0（U3）

コンポーネント	プロダクト	バージョン
	VMware vCenter Applianceの略	バージョン7.0.3
	Cisco Intersight Assist仮想アプライアンス	1.0.11-306

Terraformの構成の実行は、Terraform Cloud for Businessアカウントで行われます。Terraformの構成では、NetApp Cloud ManagerのTerraformプロバイダを使用しています。

次の表に、ベンダー、製品、およびバージョンを示します。

コンポーネント	プロダクト	バージョン
橋本（橋本	テラフォーム	1.2.7

次の表に、Cloud ManagerとCloud Volumes ONTAP のバージョンを示します。

コンポーネント	プロダクト	バージョン
ネットアップ	Cloud Volumes ONTAP	9.11
	クラウドマネージャ	3.9.21

"次の手順：インストールと設定- FlexPod を導入します。"

インストールと設定

FlexPod を導入します

"前の図：解決策 コンポーネント。"

設計のさまざまな要素の構成や関連するベストプラクティスなど、FlexPod の設計および導入の詳細については、を参照してください "FlexPod 向けのシスコ検証済み設計"。

FlexPod は、UCS管理モードとCisco Intersight管理モードの両方に導入できます。FlexPod をUCS管理モードで導入している場合は、最新のCisco Validated Designが見つかります "こちらをご覧ください"。

Cisco Unified Compute System（Cisco UCS）Xシリーズは、まったく新しいモジュラ型コンピューティングシステムであり、クラウドから構成、管理できます。最新のアプリケーションのニーズを満たし、柔軟性に優れた、将来に対応できるモジュラ設計によって運用効率、即応性、拡張性を向上させるように設計されています。Cisco Intersightが管理するUCS XシリーズプラットフォームをFlexPod インフラに組み込むための設計ガイダンスを提供します "こちらをご覧ください"。

FlexPod とCisco ACIの導入方法が用意されています "こちらをご覧ください"。

"次の例は、Cisco Intersightの設定です。"

Cisco Intersightの設定

"前の手順：FlexPod を導入します。"

Cisco IntersightとIntersight Assistを設定する方法については、「Cisco Validated Design

for FlexPod 」を参照してください "こちらをご覧ください"。

"次のステップ：クラウド統合とICOの統合の前提条件"

クラウド統合と**ICO**の統合の前提条件

"前の手順：Cisco Intersightの設定。"

手順 **1**：**Cisco Intersight**と**Terraform Cloud**を接続します

1. Terraform Cloudアカウントの詳細情報を提供して、クラウドターゲットを請求または作成します。
2. プライベートクラウド用のTerraform Cloud Agentターゲットを作成して、お客様がデータセンターにエージェントをインストールし、Terraform Cloudと通信できるようにします。

   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"。

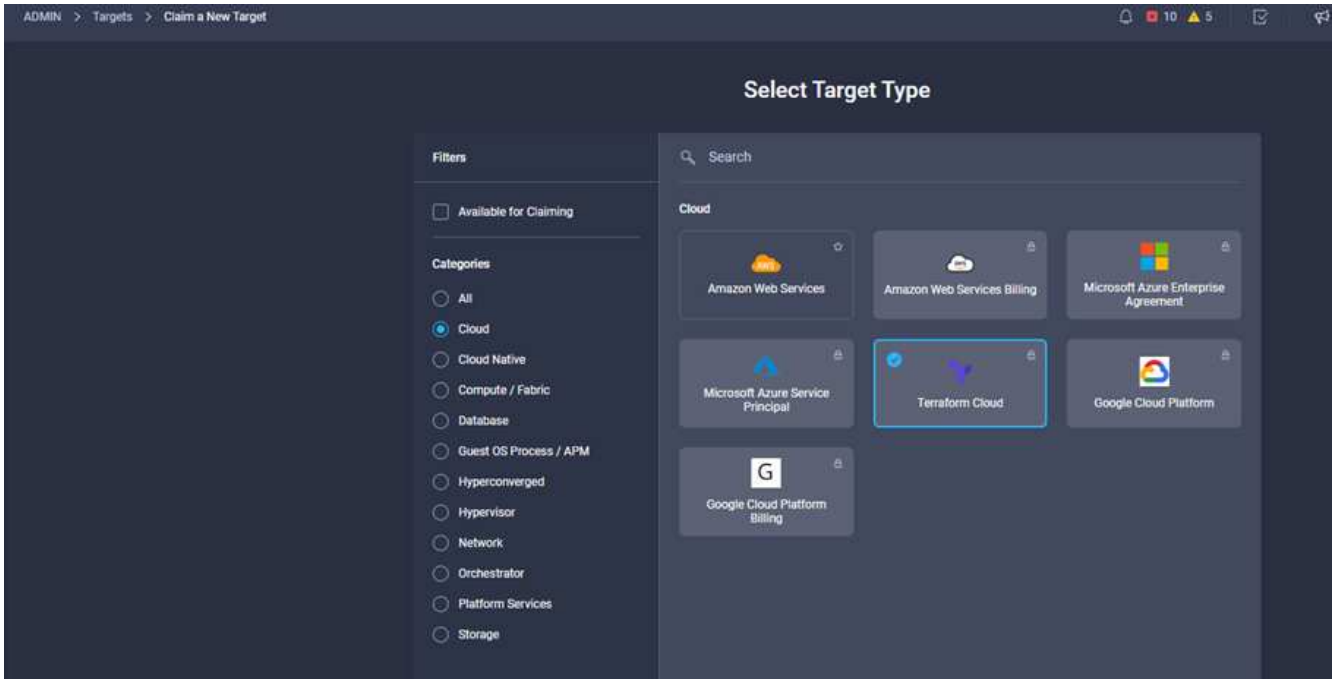
手順 **2:**ユーザートークンを生成します

Terraform Cloudのターゲットを追加する際には、Terraform Cloud設定ページからユーザー名とAPIトークンを入力する必要があります。

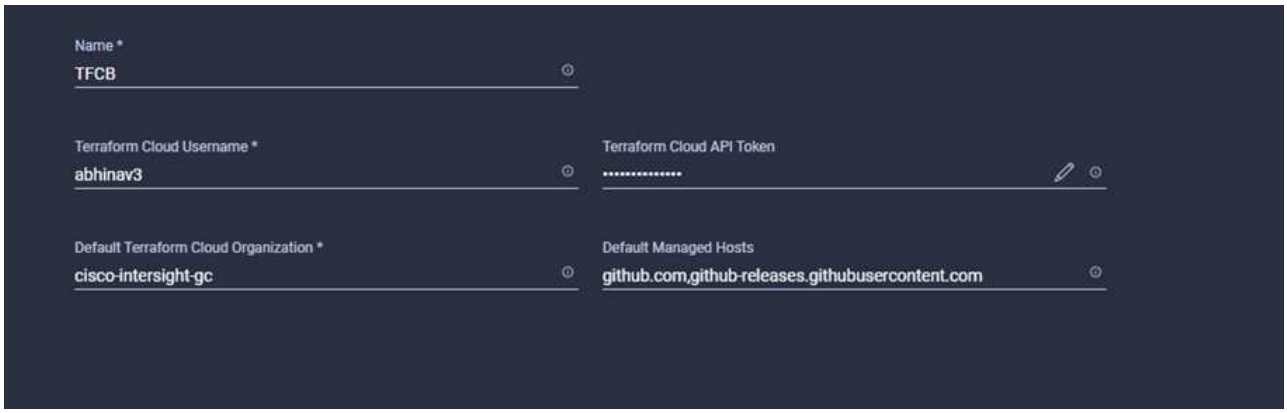
1. Terraform Cloudにログインし、* User Tokens *にアクセスします。"https://app.terraform.io/app/settings/tokens"。
2. [新しい**API**トークンの作成]をクリックします。
3. トークンを覚えて安全な場所に保存するための名前を割り当てます。

手順 **3**：クラウドターゲットを要求

1. アカウント管理者、デバイス管理者、またはデバイス技術者の権限でIntersightにログインします。
2. [管理者]、[ターゲット]、[新しいターゲットの請求]の順に移動します。*
3. 「カテゴリ」で、「クラウド」をクリックします。
4. [**Terraform Cloud**]をクリックし、[**Start**]をクリックします。



5. 次の図に示すように、ターゲットの名前、Terraform Cloudのユーザー名、APIトークン、およびTerraform Cloudのデフォルトの組織を入力します。
6. [*Default Managed Hosts]フィールドに、他の管理対象ホストと一緒に次のリンクを追加してください。
   - github.com
   - github-releases.githubusercontent.com



すべてが正しく入力されていれば、[* Intersight Targets]セクションにTerraform Cloudターゲットが表示されます。

手順 **4**：クラウドエージェントを追加します

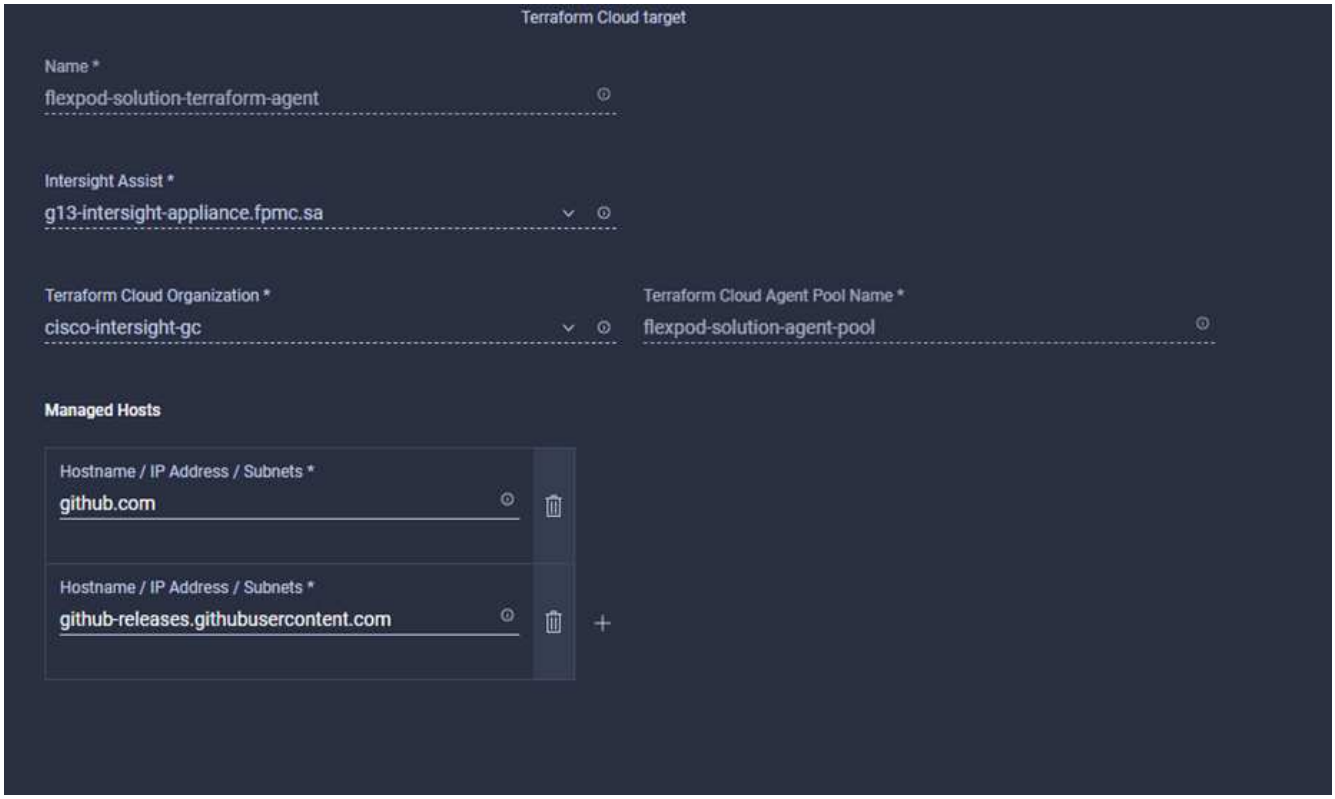
前提条件

- クラウドのターゲットをクラウド化
- Terraform Cloud Agentを展開する前に、Intersight AssistをIntersightに主張。

> 各アシストに対して請求できるエージェントは5人だけです。

Terraformへの接続を作成したら、Terraform Agentをスピンアップして Terraformコードを実行する必要があります。

1. Terraform Cloudターゲットのドロップダウンリストから*Claim Terraform Cloud Agent *をクリックします。
2. Terraformクラウドエージェントの詳細を入力します。次のスクリーンショットは、Terraformエージェントの構成の詳細を示しています。



任意のTerraform Agentプロパティを更新できます。ターゲットが「接続されていない」状態で、「接続されていない」状態になっていない場合、Terraformエージェントに対してトークンが生成されていません。

エージェントの検証が成功し、エージェントトークンが生成された後、組織やエージェントプールを再構成することはできません。Terraformエージェントが正常に配備された場合、ステータスは* Connected *と表示されます。

Terraform Cloud統合を有効にして主張したら、Cisco Intersight Assistで1つ以上のTerraform Cloudエージェントを導入できます。Terraform Cloudエージェントは、クラウドターゲットの子ターゲットとしてモデル化されています。エージェント目標を要求すると、ターゲット請求が進行中であることを示すメッセージが表示されます。

数秒後、ターゲットは「接続済み」状態に移行し、Intersightプラットフォームはエージェントから Terraform CloudゲートウェイにHTTPSパケットをルーティングします。

Terraform Agentは正しく請求され、ターゲットの下に「* Connected *」と表示されます。

"次の手順：パブリッククラウドサービスプロバイダを設定します。"

パブリッククラウドサービスプロバイダを設定

"前：Terraform Cloud Integration with ICOの前提条件"

手順 **1**：**NetApp Cloud Manager**にアクセスします

NetApp Cloud Managerおよびその他の クラウド サービス にアクセスするには、にサインアップする必要があります "NetApp Cloud Central"。

> Cloud Centralアカウントでワークスペースとユーザを設定する場合は、をクリックします "こちらをご覧ください"。

手順 **2**：コネクタを配置します

Google CloudにConnectorを導入するには、こちらを参照してください "リンク"。

"次のステップ：ハイブリッドクラウドネットアップストレージの自動導入"

ハイブリッドクラウドネットアップストレージの導入を自動化

"前のページ：パブリッククラウドサービスプロバイダを設定"

Google Cloud

最初にAPIを有効にし、コネクタまたは異なるプロジェクトにあるCloud Volumes ONTAP システムを導入および管理する権限をCloud Managerに付与するサービスアカウントを作成する必要があります。

Google CloudプロジェクトにConnectorを導入する前に、Connectorがオンプレミスまたは別のクラウドプロバイダで実行されていないことを確認してください。

Cloud Manager からコネクタを直接導入するには、次の 2 組の権限が必要です。

- Cloud ManagerからConnector VMインスタンスを起動する権限があるGoogleアカウントを使用してConnectorを導入する必要があります。
- Connectorを導入する場合は、VMインスタンスを選択するよう求められます。Cloud Manager は、サービスアカウントから権限を取得して、 Cloud Volumes ONTAP システムを代わりに作成および管理します。権限は、サービスアカウントにカスタムロールを割り当てることによって提供されます。ユーザーとサービスアカウントに必要な権限を含むYAMLファイルを2つ設定する必要があります。の使用方法について説明します "権限を設定するYAMLファイル" こちらをご覧ください。

を参照してください "この詳細なビデオをご覧ください" を参照してください。

Cloud Volumes ONTAP の導入モードとアーキテクチャ

Cloud Volumes ONTAP は、シングルノードシステムとして、またハイアベイラビリティ（HA）ペアのノードとしてGoogle Cloudで利用できます。要件に基づいて、Cloud Volumes ONTAP 導入モードを選択できます。シングルノードシステムの HA ペアへのアップグレードはサポートされていません。シングルノードシステムとHAペアを切り替える場合は、新しいシステムを導入し、既存のシステムから新しいシステムにデータをレプリケートする必要があります。

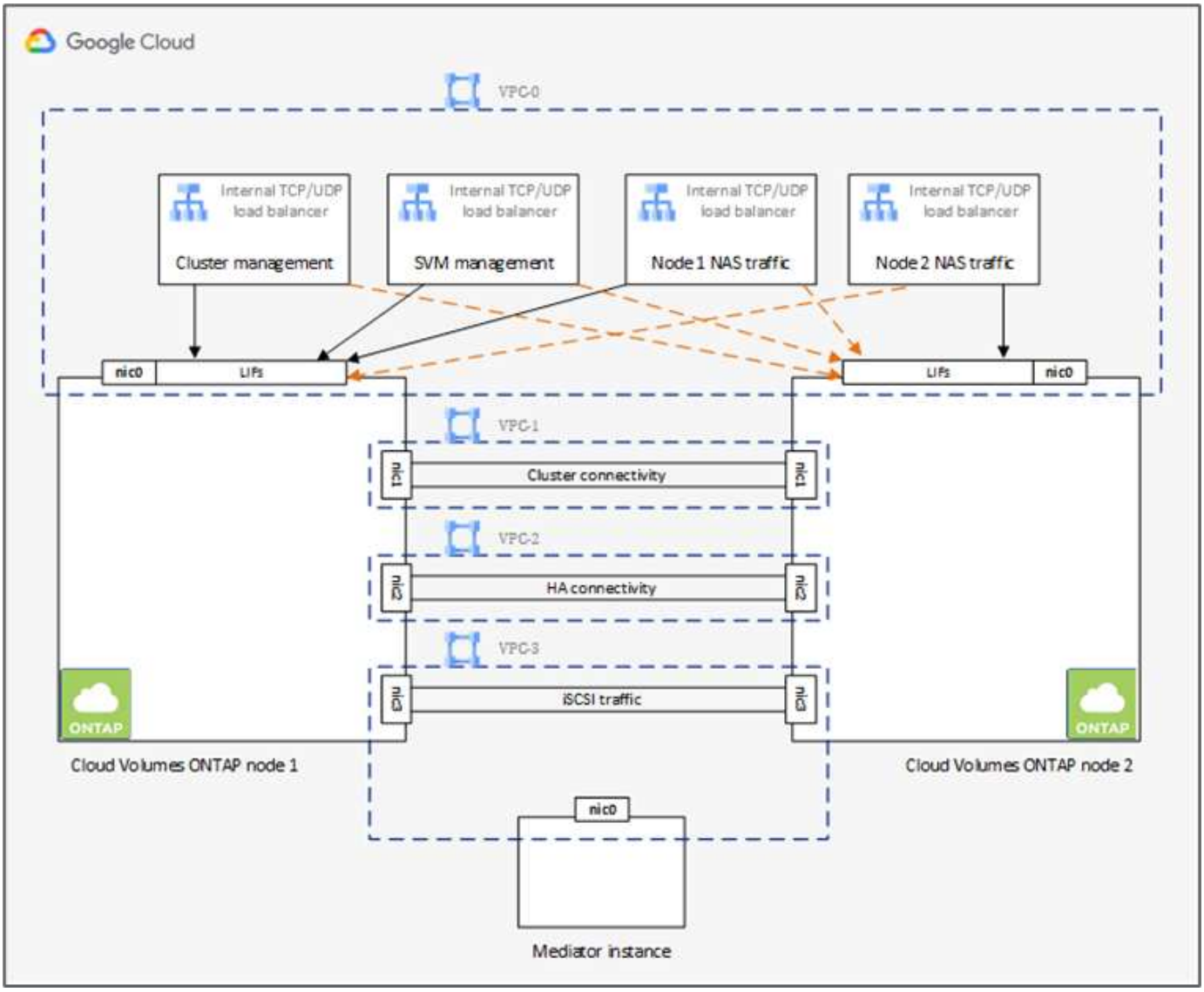
Google Cloudの高可用性Cloud Volumes ONTAP

Google Cloudでは、複数の地域や1つの地域内の複数のゾーンにまたがるリソースの導入をサポートしています。HA導入は、Google Cloudで利用できる強力なn1-standardまたはn2標準のマシンタイプを使用する2つのONTAP ノードで構成されます。2つのCloud Volumes ONTAP ノード間でデータが同期的にレプリケートされ、障害発生時の可用性が確保されます。Cloud Volumes ONTAP のHA導入では、VPCごとに4つのVPCとプライベートサブネットが必要です。4つのVPC内のサブネットは、重複しないCIDR範囲でプロビジョニングする必要があります。

4つのVPCは次の目的に使用されます。

- vPC 0は、データノードおよびCloud Volumes ONTAP ノードへのインバウンド通信を可能にします。
- vPC 1は、Cloud Volumes ONTAP ノード間のクラスタ接続を提供します。
- vPC 2を使用すると、ノード間でNVRAM（不揮発性RAM）レプリケーションを実行できます。
- vPC 3は、HAメディエーターインスタンスへの接続、およびノードの再構築のためのディスクレプリケーショントラフィックに使用されます。

次の図は、Goggle Cloudで高可用性Cloud Volumes ONTAP を示しています。



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"。

Google CloudでのCloud Volumes ONTAP のネットワーク要件については、を参照してください "リンクをクリックしてください"。

データ階層化の詳細については、を参照してください "リンクをクリックしてください"。

環境の前提条件を設定する

Cloud Volumes ONTAP クラスタの自動作成、オンプレミスボリュームとクラウドボリューム間のSnapMirror設定、クラウドボリュームの作成などが、Terraform設定を使用して実行されます。これらのTerraform構成は、Terraform Cloud for Businessアカウントでホストされています。Intersight Cloud Orchestratorを使用すると、Terraform Cloud for Businessアカウントでのワークスペースの作成、ワークスペースへの必要な変数の追加、Terraformプランの実行などのタスクをオーケストレーションできます。

これらの自動化タスクとオーケストレーションタスクには、以降のセクションで説明するように、いくつかの要件とデータが必要になります。

GitHub リポジトリ

TerraformコードをホストするにはGitHubアカウントが必要です。Intersight Orchestratorは、Terraform Cloud for Businessアカウントに新しいワークスペースを作成します。このワークスペースには、バージョン管理ワークフローが設定されています。そのためには、Terraformの構成をGitHubリポジトリに保持し、ワークスペースの作成時に入力として提供する必要があります。

"このGitHubリンク" は、さまざまなリソースを使用したTerraformの構成を提供します。このリポジトリを作成し、GitHubアカウントにコピーを作成できます。

このリポジトリでは'providator.tf'は'必要なTerraformプロバイダの定義を持っていますNetApp Cloud ManagerのTerraformプロバイダが使用されています。

「variable.tf」には、すべての変数宣言が含まれています。これらの変数の値は、Intersight Cloud Orchestratorのワークフロー入力として入力されます。これにより、値をワークスペースに渡し、Terraform設定を実行するのに便利な方法が提供されます。

「resources.tf」では、作業環境へのオンプレミスONTAP の追加、Google CloudでのシングルノードCloud Volumes ONTAP クラスタの作成、オンプレミスとCloud Volumes ONTAP 間のSnapMirror関係の確立、Cloud Volumes ONTAP でのクラウドボリュームの作成などに必要なさまざまなリソースを定義します。

このリポジトリの内容は次のとおりです

- 「providator.tf」には、必要なTerraformプロバイダの定義としてNetApp Cloud Managerが含まれています。
- 「variables .tf」には、Intersight Cloud Orchestratorワークフローの入力として使用される変数宣言が含まれています。これにより、値をワークスペースに渡し、Terraform設定を実行する便利な方法が提供されます。
- 「resources.tf」では、オンプレミスONTAP を作業環境に追加するためのさまざまなリソースを定義し、Google Cloud上でシングルノードCloud Volumes ONTAP クラスタを作成し、オンプレミスとCloud Volumes ONTAP 間のSnapMirror関係を確立し、Cloud Volumes ONTAP 上にクラウドボリュームを作成します。

Cloud Volumes ONTAP 上に複数のボリュームを作成する場合は'リソース・ブロックを追加するか'Terraform

構造体ごとにcountまたは'for _を使用できます

Terraformのワークスペース、モジュール、およびポリシーセットを、Terraformの構成を含むgitリポジトリに接続するには、Terraform CloudがGitHubレポジトリにアクセスする必要があります。

クライアントを追加すると、そのクライアントのOAuthトークンIDがIntersight Cloud Orchestratorのワークフロー入力の1つとして使用されます。

1. Terraform Cloud for Businessアカウントにログインします。[設定]>[プロバイダ]に移動します。
2. [VCSプロバイダの追加*]をクリックします。
3. バージョンを選択します。
4. 「プロバイダの設定」の手順に従います。
5. 追加したクライアントが* VCS Providers *に表示されます。OAuthトークンIDをメモします。

NetApp Cloud Manager API処理のトークンを更新します

Cloud Manager には、 Web ブラウザインターフェイスに加えて、 SaaS インターフェイスを介して Cloud Manager 機能に直接アクセスできるようにする REST API が用意されています。Cloud Manager サービスは、拡張可能な開発プラットフォームをまとめた複数のコンポーネントで構成されます。リフレッシュトークンを使用すると、API呼び出しごとにAuthorizationヘッダーに追加するアクセストークンを生成できます。

APIを直接呼び出すことなく、cloudmanagerプロバイダは更新トークンを使用し、Terraformリソースを対応するAPI呼び出しに変換します。NetApp Cloud Manager API処理の更新トークンを生成する必要があります "NetApp Cloud Central"。

Cloud Volumes ONTAP クラスタの作成、SnapMirrorの設定などのリソースをCloud Managerで作成するには、Cloud Manager ConnectorのクライアントIDが必要です。

1. Cloud Managerにログインします。 "https://cloudmanager.netapp.com/"。
2. コネクター（ * Connector ）をクリックします。
3. [* コネクターの管理 *] をクリックします。
4. 省略記号をクリックし、コネクタIDをコピーします。

Cisco Intersight Cloud Orchestratorのワークフローの開発

Cisco Intersight Cloud Orchestratorは、次の場合にCisco Intersightで利用できます。

- Intersight Premierのライセンスがインストールされている。
- お客様は、アカウント管理者、ストレージ管理者、仮想化管理者、またはサーバ管理者であり、少なくとも1台のサーバを割り当て済みであることが必要です。

ワークフローデザイナ

ワークフローデザイナを使用すると、新しいワークフロー(タスクおよびデータ型)の作成や、既存のワークフローの編集を行って、Cisco Intersightでターゲットを管理できます。

Workflow Designerを起動するには、[* Orchestration（オーケストレーション）**]>[Workflows *（ワークフロー）**]ダッシュボードには、[マイワークフロー*]、[サンプルワークフロー*]、[すべてのワークフロー*]タブの下に以下の詳細が表示されます。

- 検証ステータス
- 前回の実行ステータス
- 実行数別上位ワークフロー
- 上位のワークフローカテゴリ
- システム定義ワークフローの数
- Top Workflows by Targets（ターゲット別の上位ワークフロー

ダッシュボードを使用すると、タブを作成、編集、クローニング、または削除できます。独自のカスタムビュータブを作成するには、*+*をクリックし、名前を指定し、列、タグ列、ウィジェットに表示する必要があるパラメータを選択します。タブに*ロック*アイコンがない場合は、タブの名前を変更できます。

ダッシュボードの下には、次の情報を表示するワークフローが表形式のリストとして表示されます。

- 表示名
- 説明
- システム定義
- デフォルトバージョン
- 実行
- 前回の実行ステータス
- 検証ステータス
- 前回の更新
- 組織

Actionsカラムでは、次の操作を実行できます。

- *実行。*ワークフローを実行します。
- *履歴。*ワークフローの実行履歴を表示します。
- *バージョンの管理。*ワークフローのバージョンを作成および管理します。
- *削除。*ワークフローを削除します。
- *再試行*失敗したワークフローを再試行します。

ワークフロー

次の手順で構成されるワークフローを作成します。

- *ワークフローの定義。*表示名、概要 、およびその他の重要な属性を指定します。
- *ワークフローの入力とワークフローの出力を定義します。*ワークフローの実行に必要な入力パラメータと、正常に実行されたときに生成される出力を指定します
- *ワークフロータスクを追加します。*ワークフローデザイナで、ワークフローの機能を実行するために必要なワークフロータスクを1つ以上追加します。
- *ワークフローを検証します。*ワークフローを検証して、タスク入出力の接続にエラーがないことを確認します。

オンプレミスの**FlexPod** ストレージ用のワークフローを作成

オンプレミスのFlexPod ストレージのワークフローを設定するには、を参照してください "リンクをクリックしてください"。

"次：DRワークフロー："

DRワークフロー

"前：ハイブリッドクラウドネットアップストレージの自動導入。"

手順は次のとおりです。

1. ワークフローを定義します。
   - ディザスタリカバリワークフローなど、ワークフローにわかりやすい短い名前を作成します。
2. ワークフローの入力を定義します。このワークフローでは、以下の情報を入力します。
   - ボリュームオプション（ボリューム名、マウントパス）
   - ボリューム容量
   - 新しいデータストアに関連付けられているデータセンター
   - データストアがホストされているクラスタ
   - vCenterで作成する新しいデータストアの名前
   - 新しいデータストアのタイプとバージョン
   - Terraform組織の名前
   - Terraformワークスペース
   - Terraformワークスペースの概要
   - Terraform設定を実行するために必要な変数（機密性および非機密）
   - 計画を開始する理由
3. ワークフロータスクを追加します。

   FlexPod の処理に関連するタスクは次のとおりです。

   - FlexPod でボリュームを作成します。
   - 作成したボリュームにストレージエクスポートポリシーを追加します。
   - VMware vCenterで、新しく作成したボリュームをデータストアにマッピングします。

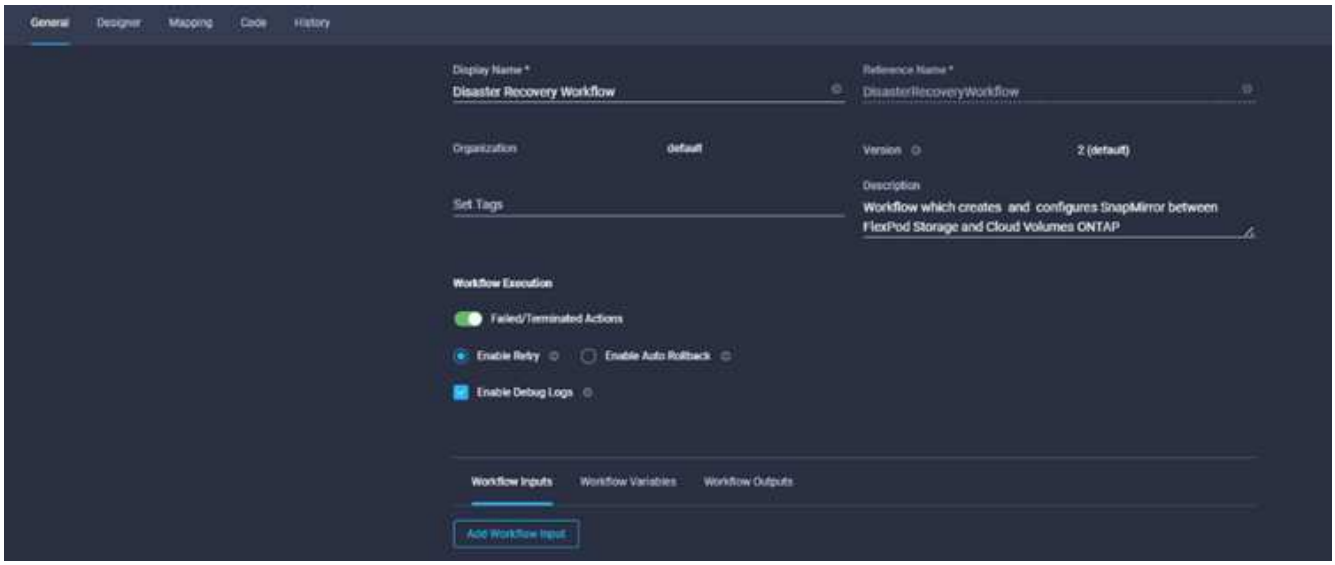
     Cloud Volumes ONTAP クラスタの作成に関連するタスクは次のとおりです。

   - Terraformワークスペースを追加します
   - Terraform変数を追加します
   - Terraformの機密変数を追加します
   - 新しいTerraformプランを開始します
   - Terraformの実行を確認します

4. ワークフローを検証します。

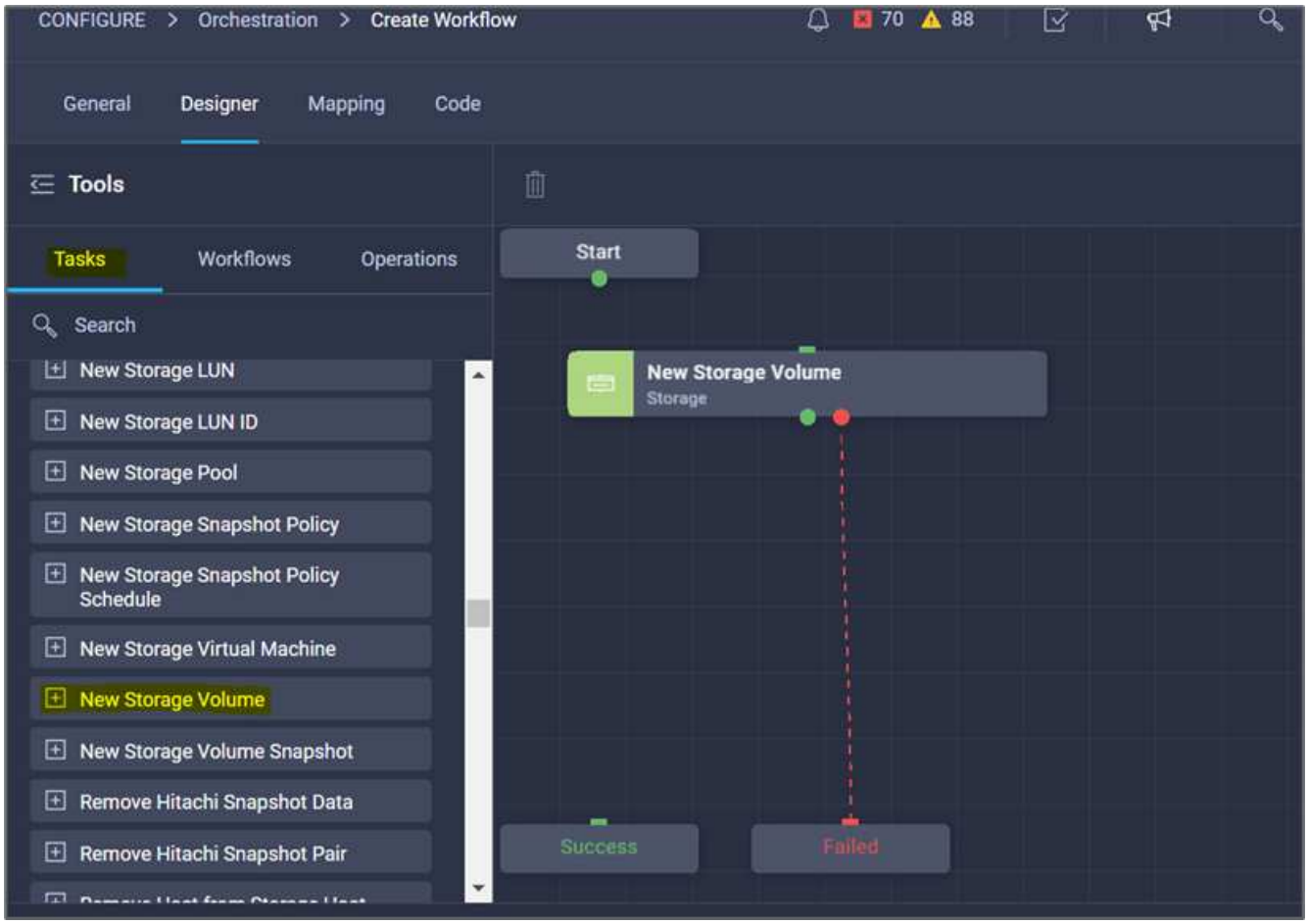
手順 **1**：ワークフローを作成します

1. 左側のナビゲーションペインで[* Orchestration（オーケストレーション）**]**をクリックし、**[** Create Workflow*]をクリックします。
2. [一般*（General *）]タブで、次のように
   a. 表示名を指定します（ディザスタリカバリワークフロー）。
   b. 組織を選択し、タグを設定し、概要 を指定します。
3. [保存] をクリックします .

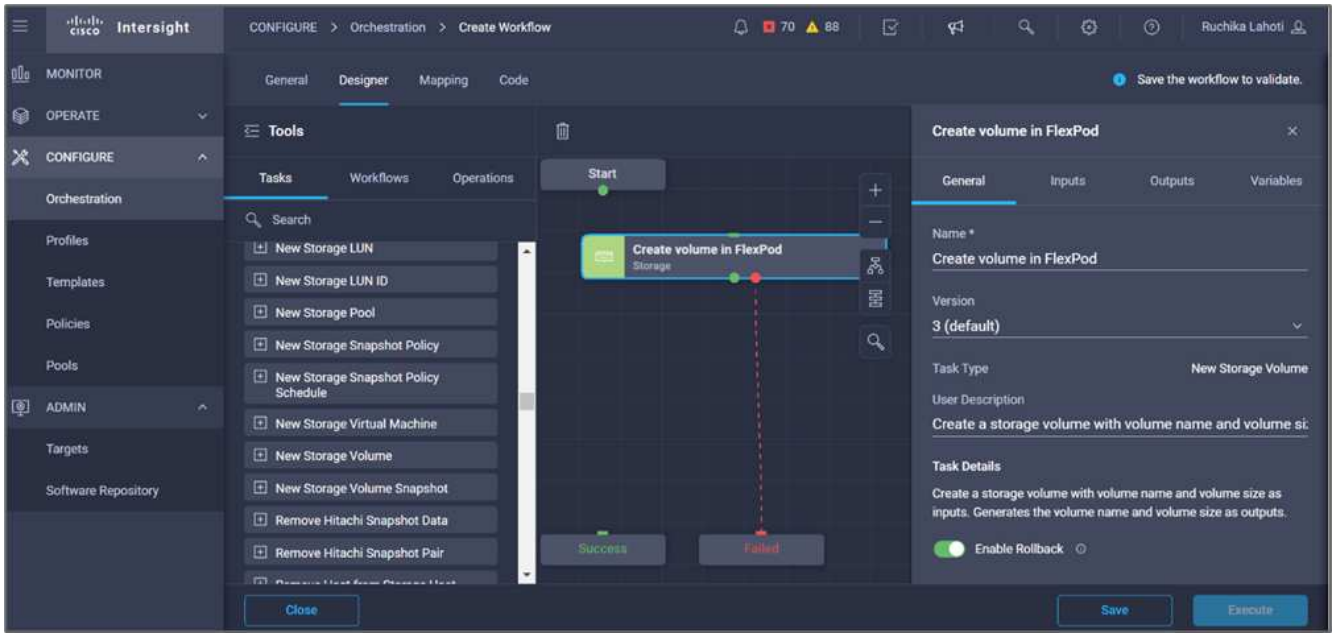


手順 **2.FlexPod** で新しいボリュームを作成します

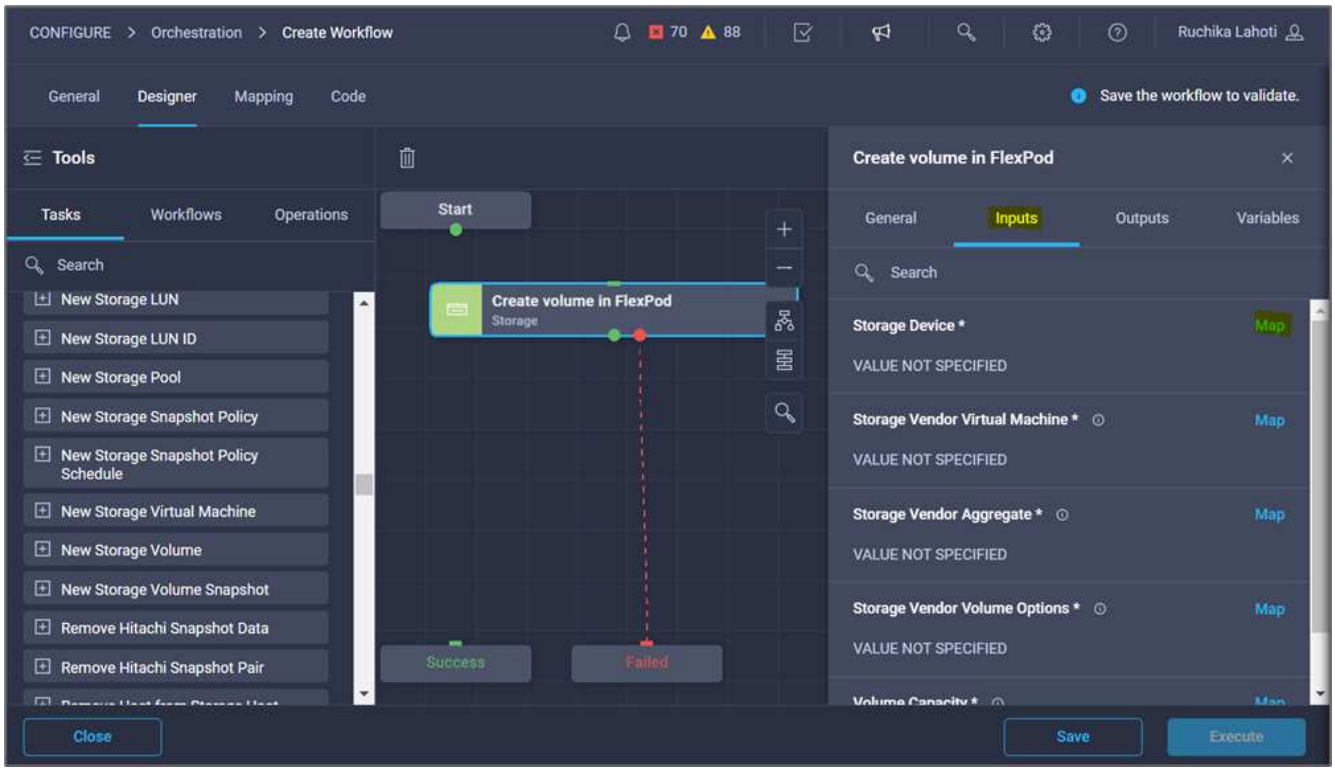
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. [ツール]セクションから[デザイン]領域に*ストレージ>新規ストレージボリューム*タスクをドラッグアンドドロップします。
3. [New Storage Volume]をクリックします。



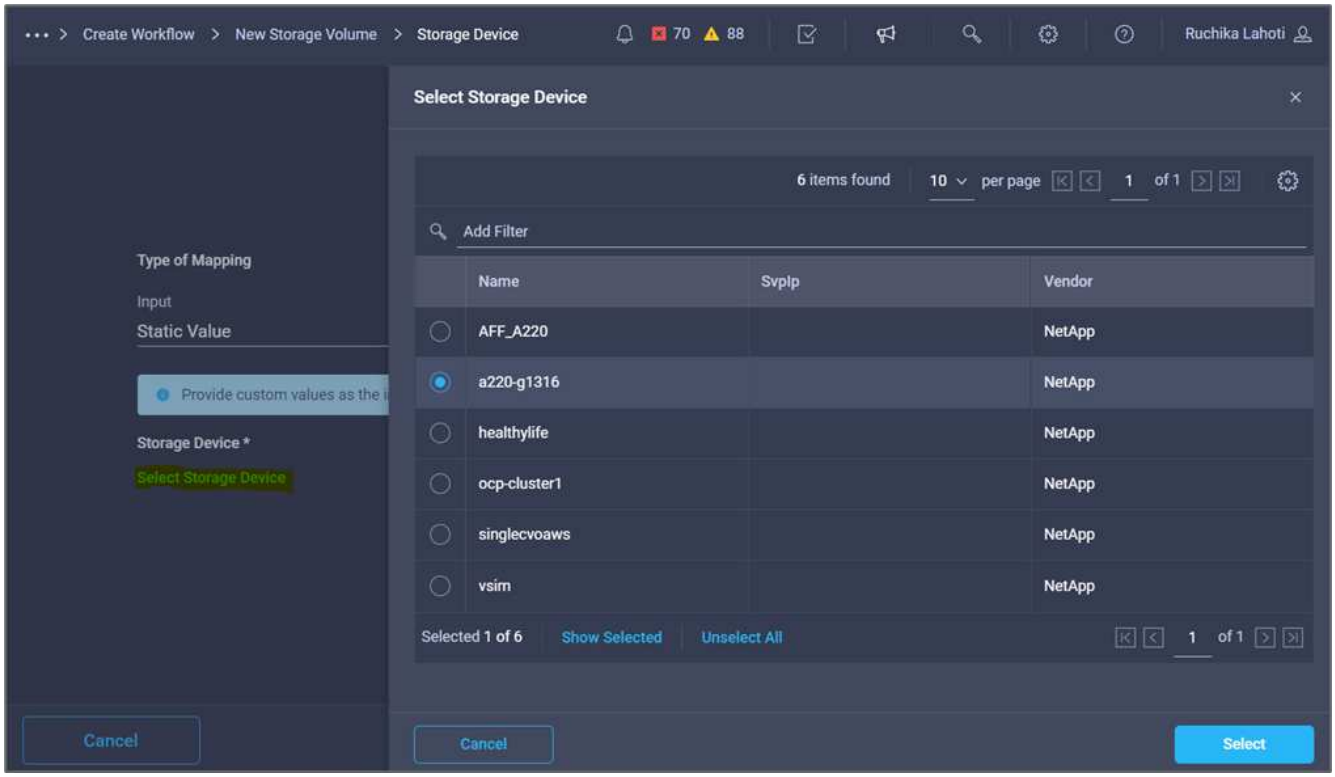
4. [タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前は* FlexPod でのボリュームの作成*です。



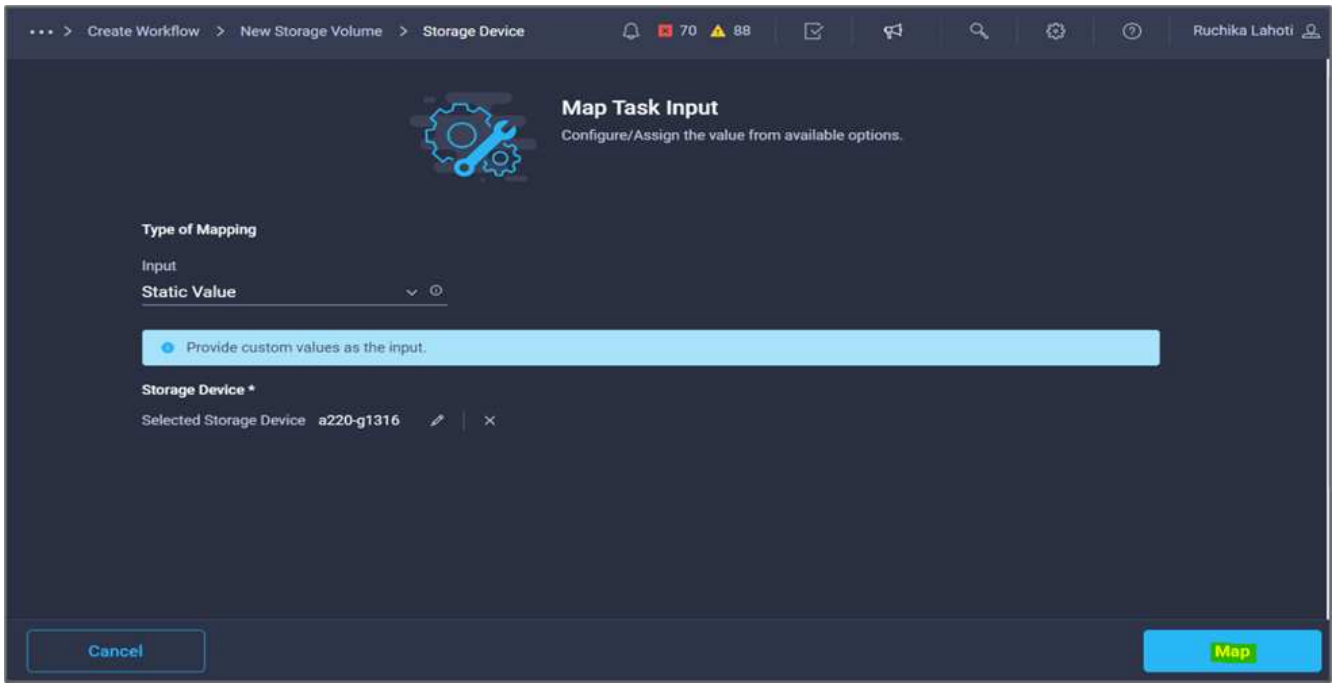
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. [ストレージデバイス]フィールドで[マップ]をクリックします。



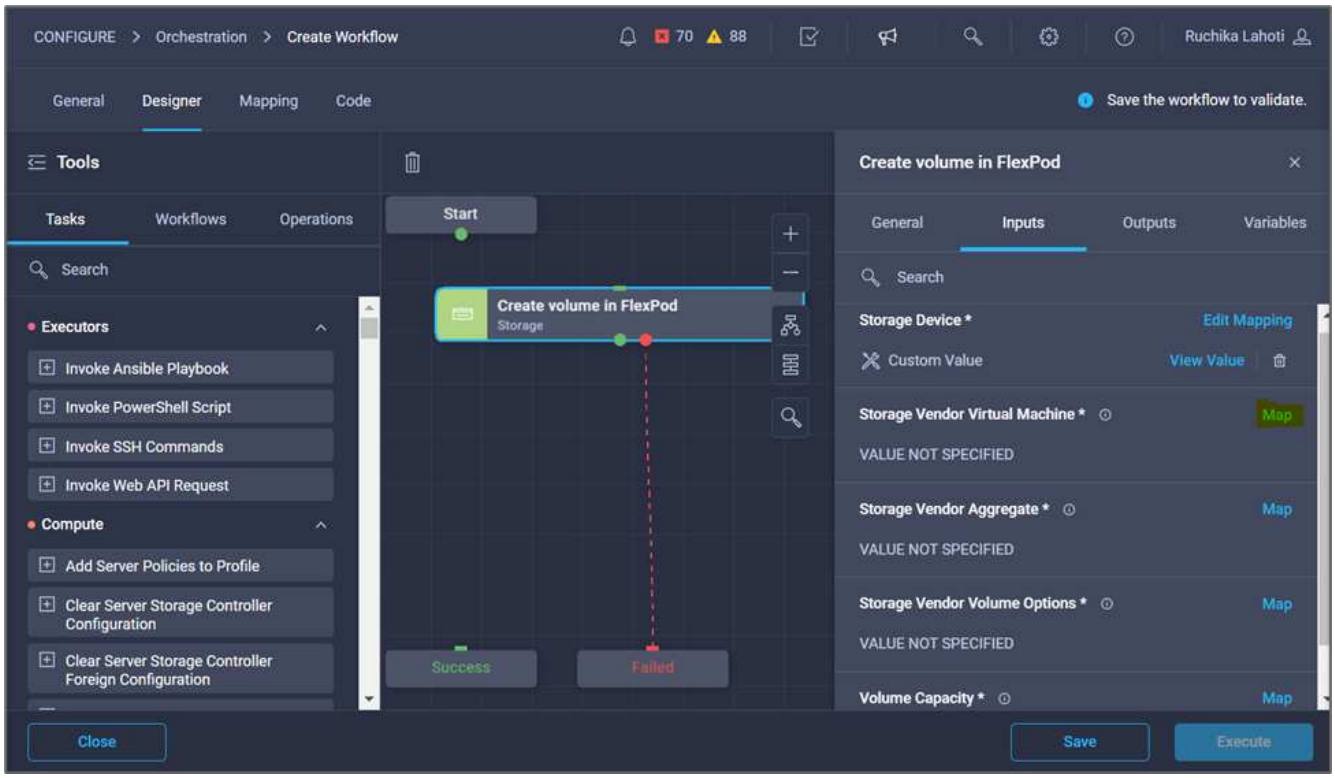
7. 「* Static Value 」を選択し、「 Select Storage Device *」をクリックします。
8. 追加したストレージターゲットをクリックし、* Select *をクリックします。



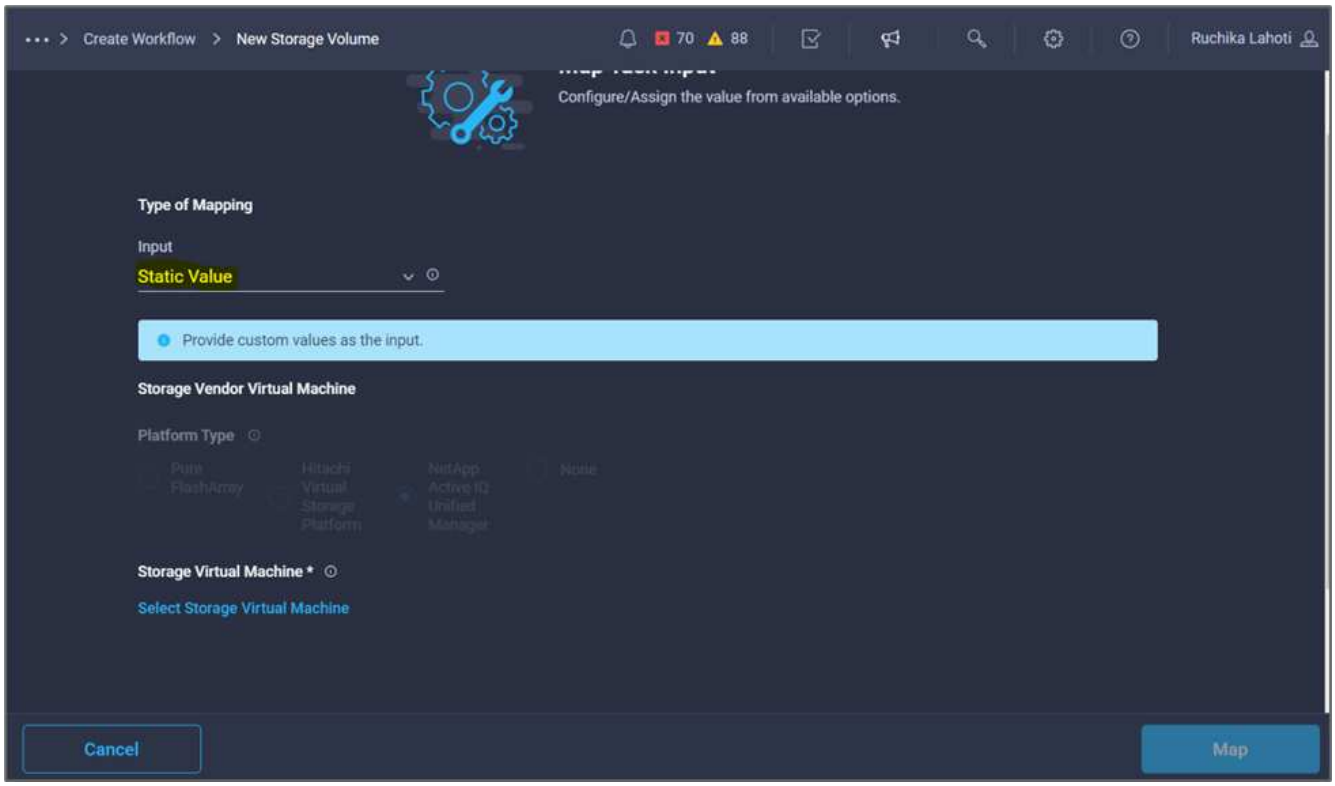
9. [マップ]をクリックします。



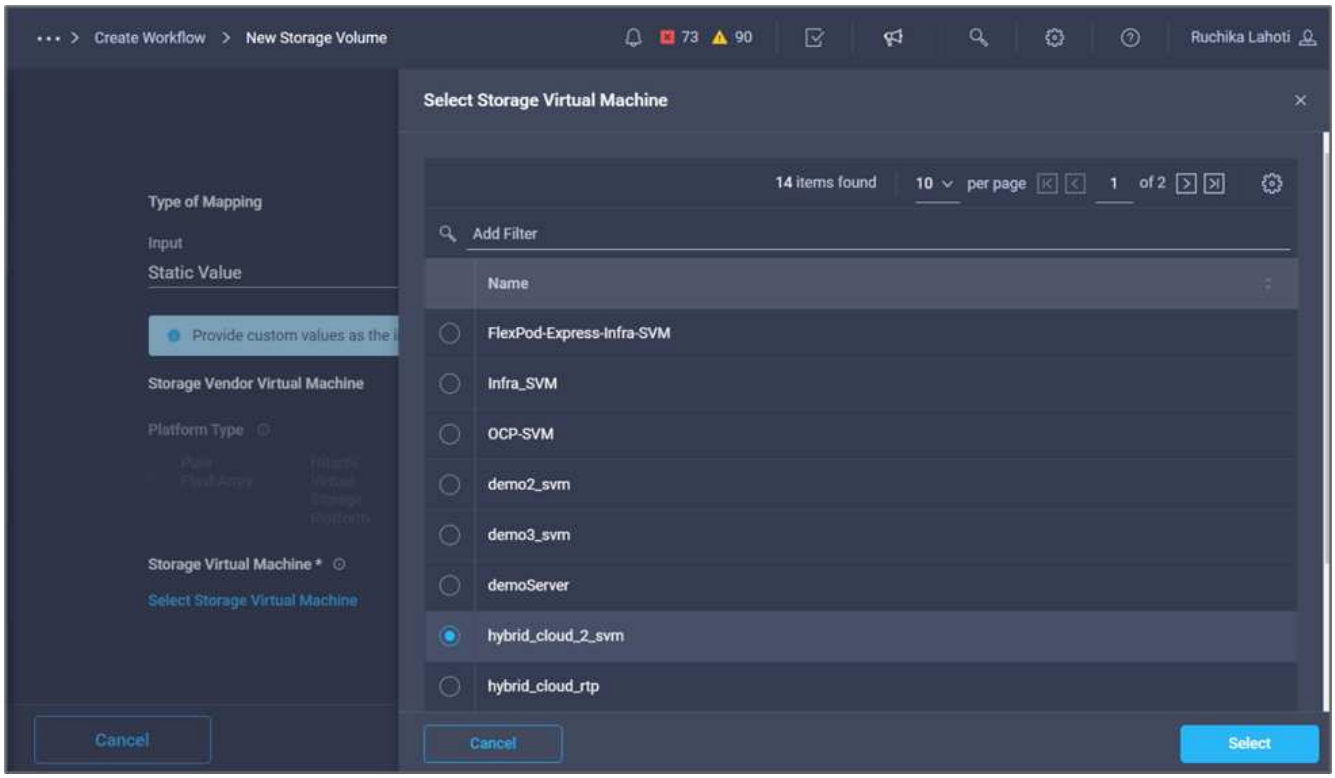
10. Storage Vendor Virtual Machine フィールドで Map *をクリックします。



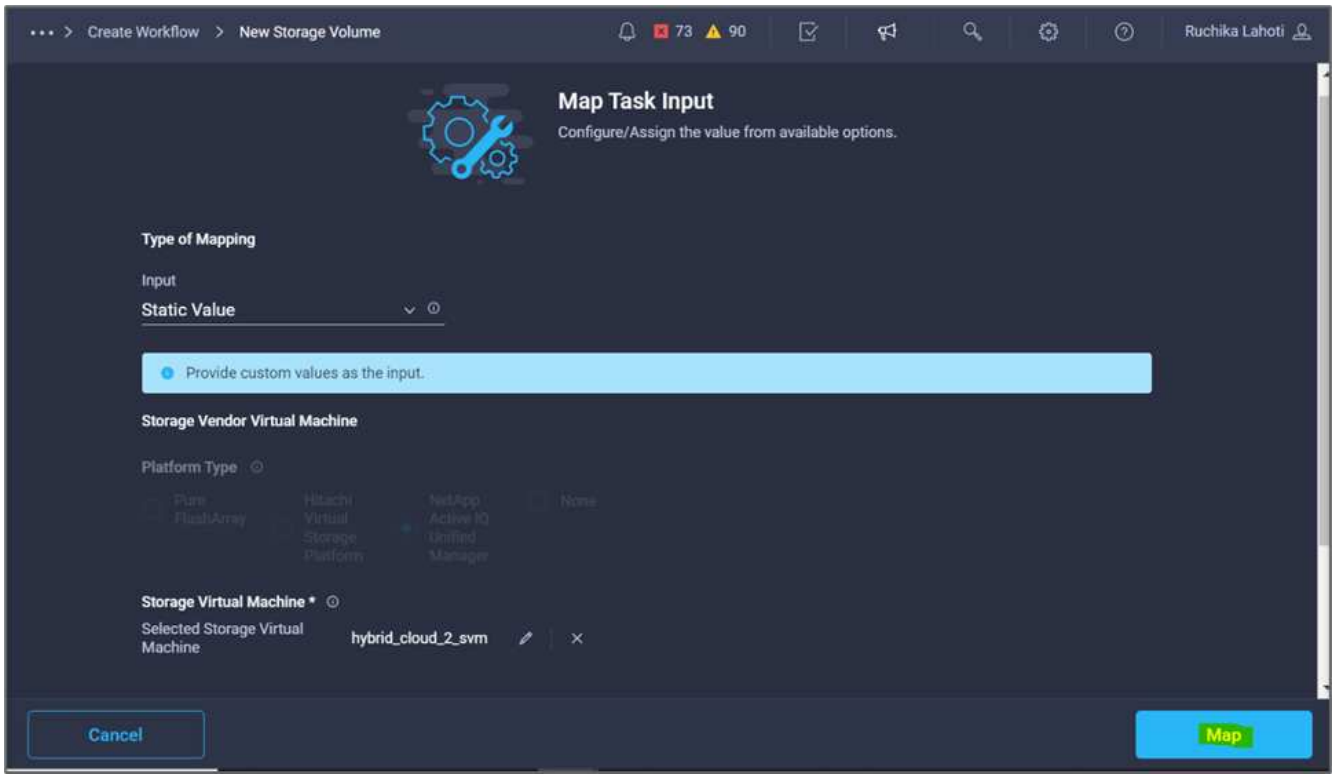
11. 「* Static Value 」を選択し、「 Storage Virtual Machineの選択*」をクリックします。



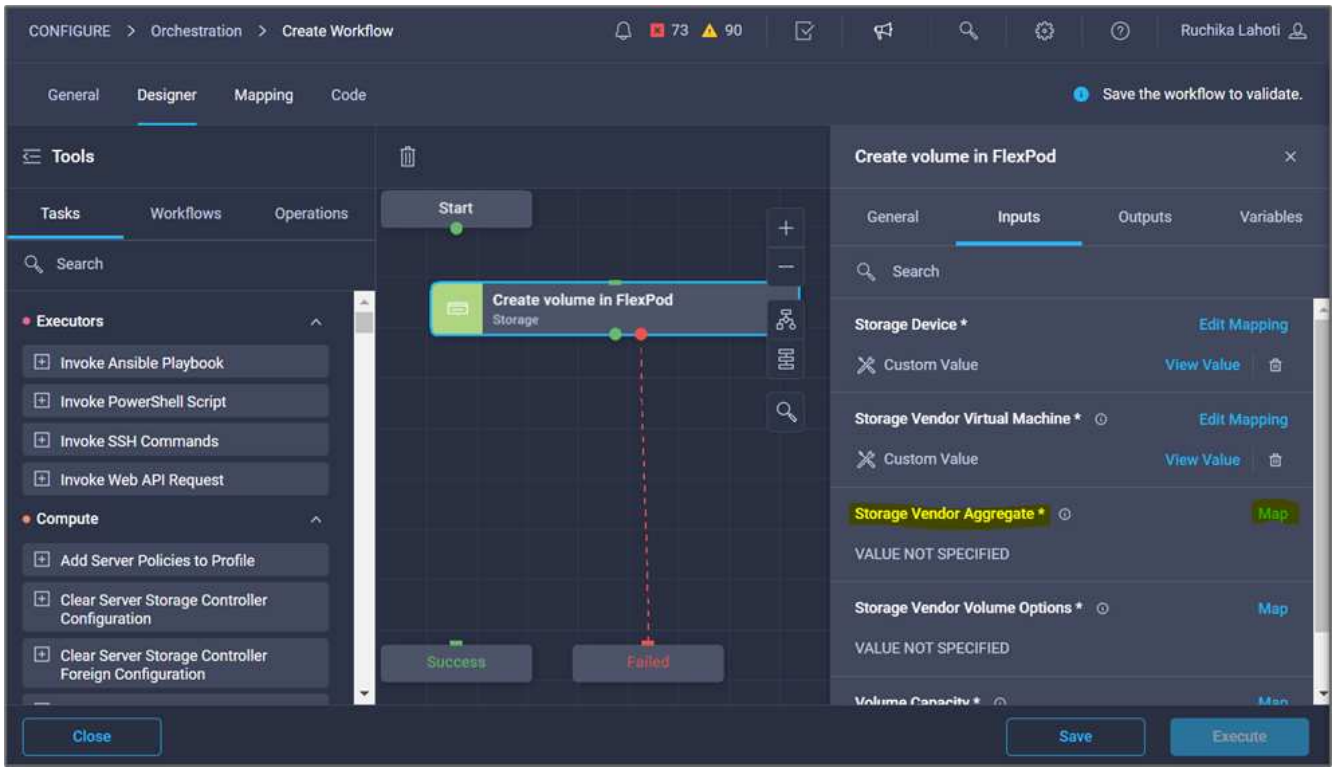
12. ボリュームを作成するStorage Virtual Machineを選択し、* Select *をクリックします。



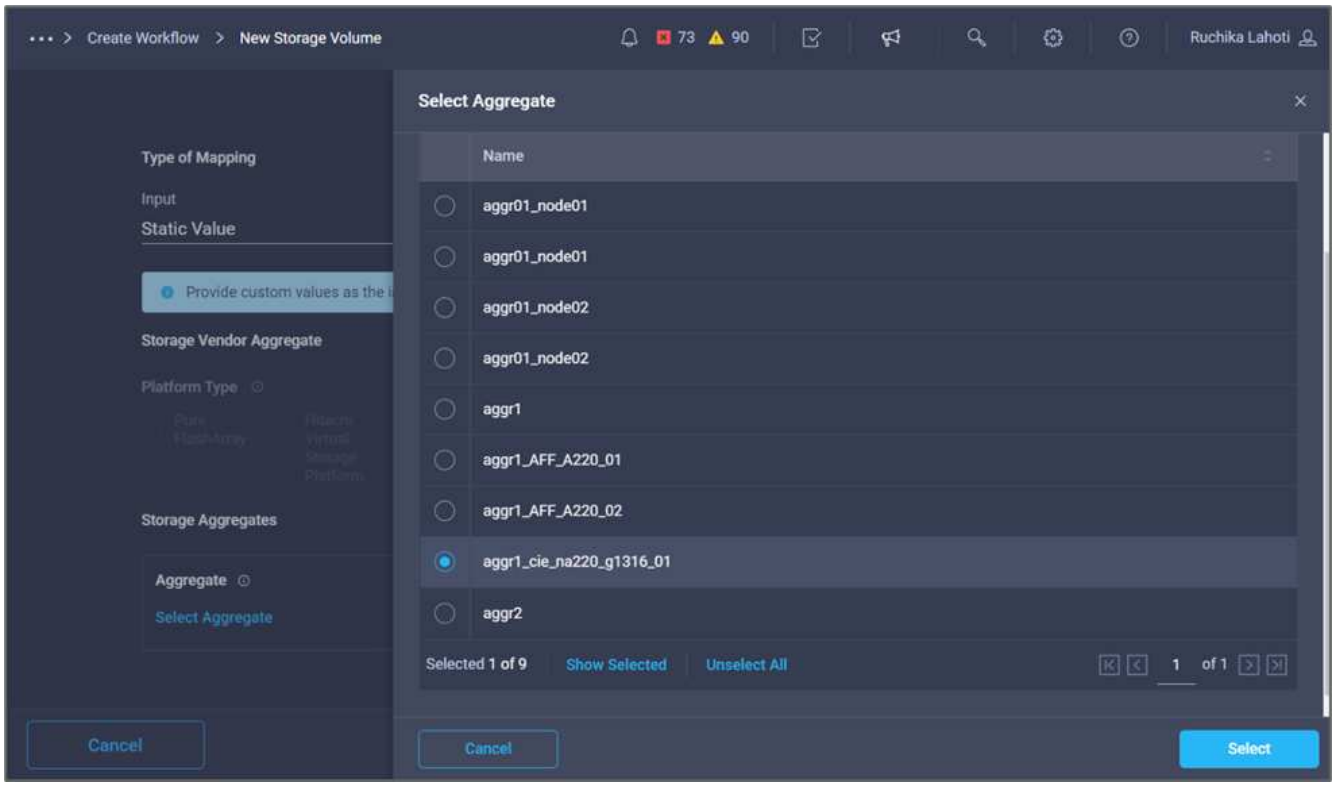
13. [マップ]をクリックします。



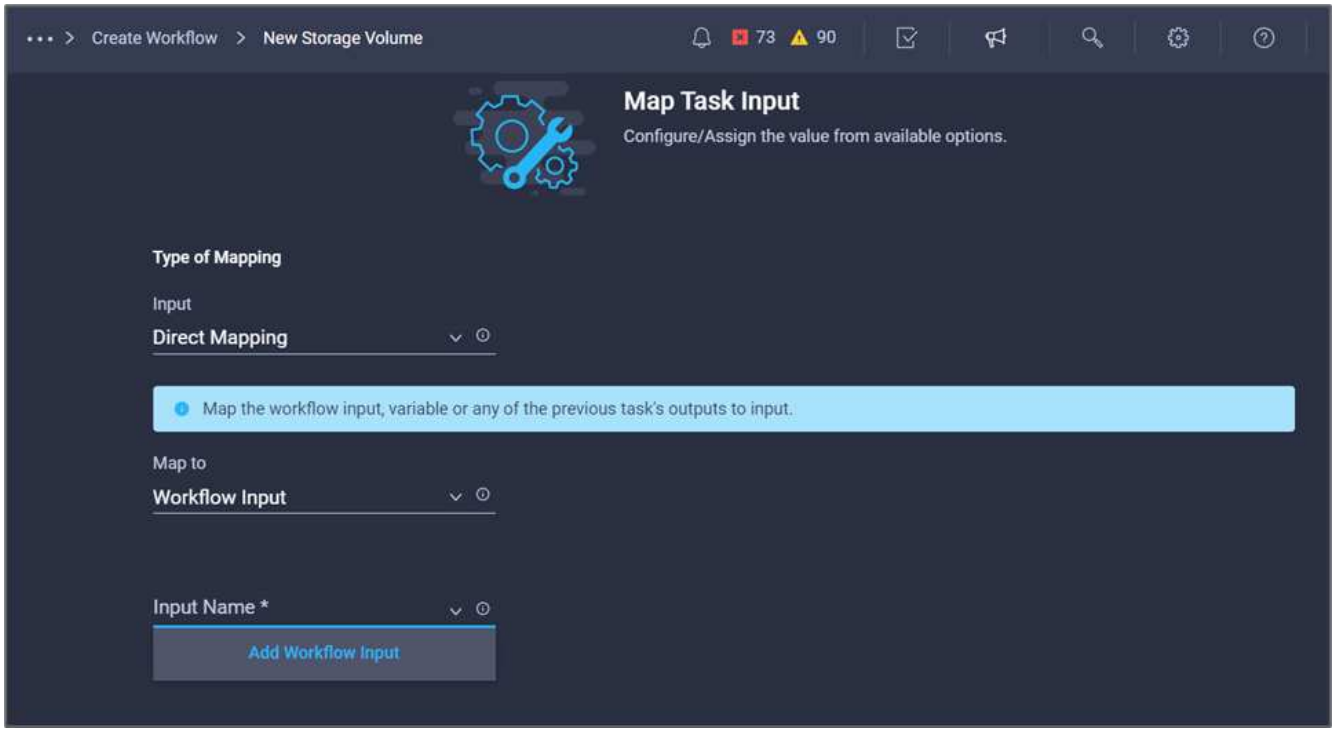
14. Storage Vendor Aggregate フィールドで Map *をクリックします。



15. 「静的値」を選択し、「*ストレージアグリゲートの選択」をクリックします。アグリゲートを選択し、Select *をクリックします。



16. [マップ]をクリックします。
17. Storage Vendor Volume Options （ストレージベンダーボリュームオプション）フィールドで* Map *をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。



19. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。

b. タイプ*でストレージ・ベンダーのボリューム・オプション*が選択されていることを確認します。

c. [デフォルト値の設定]と[オーバーライド*]をクリックします。

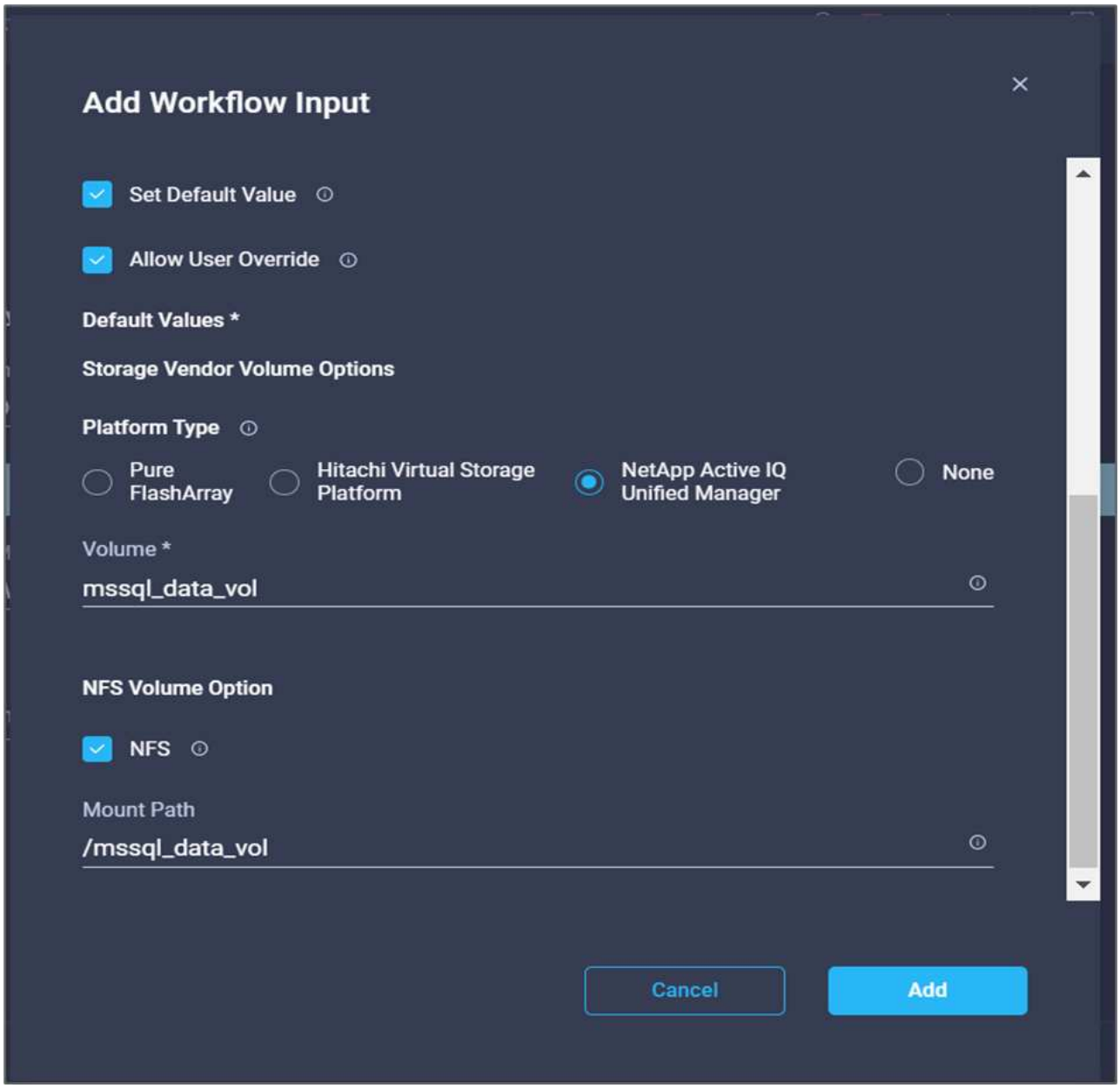
d. [必須]をクリックします。

e. プラットフォームのタイプ*をNetApp Active IQ Unified Manager *に設定します。

f. 作成したボリュームのデフォルト値を* Volume *で指定します。

g. [**NFS**]をクリックします。NFSが設定されている場合は、NFSボリュームが作成されます。この値をfalseに設定すると、SANボリュームが作成されます。

h. マウントパスを指定し、* Add *をクリックします。

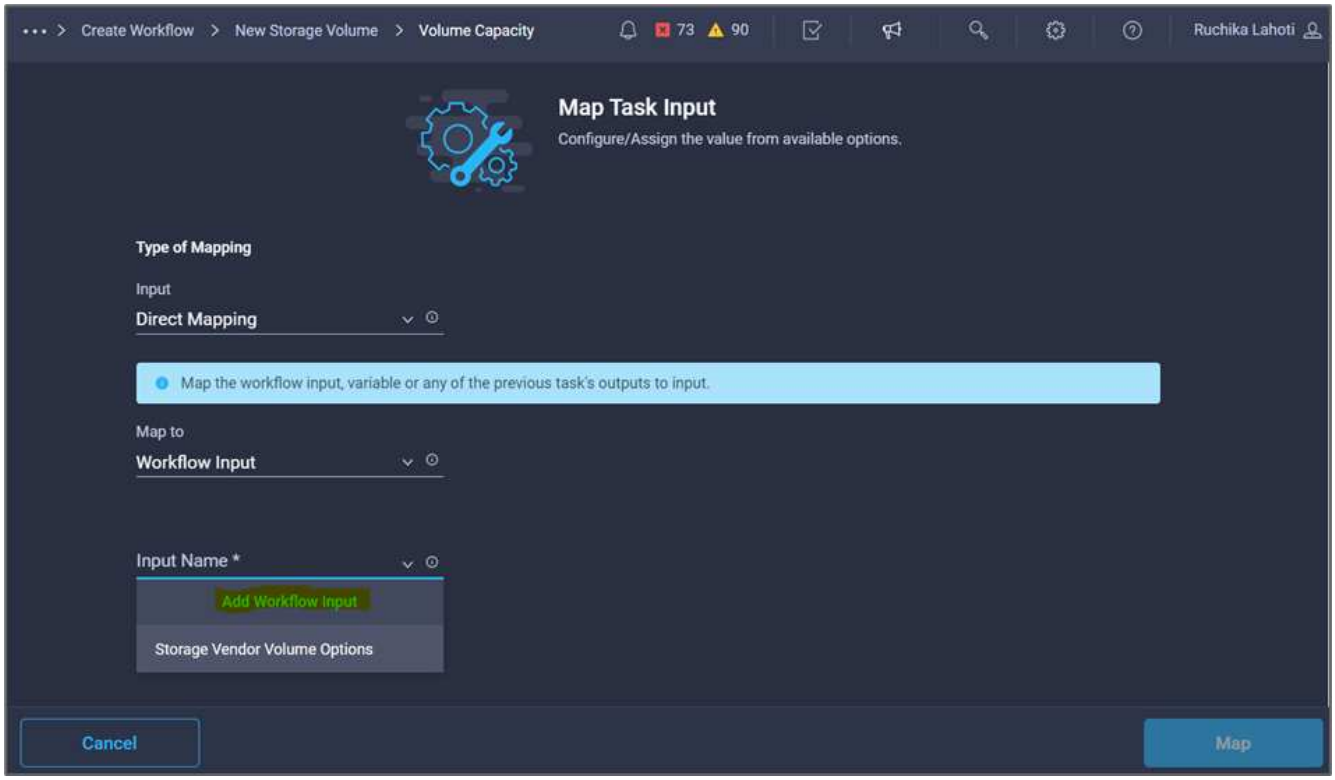


20. [マップ]をクリックします。

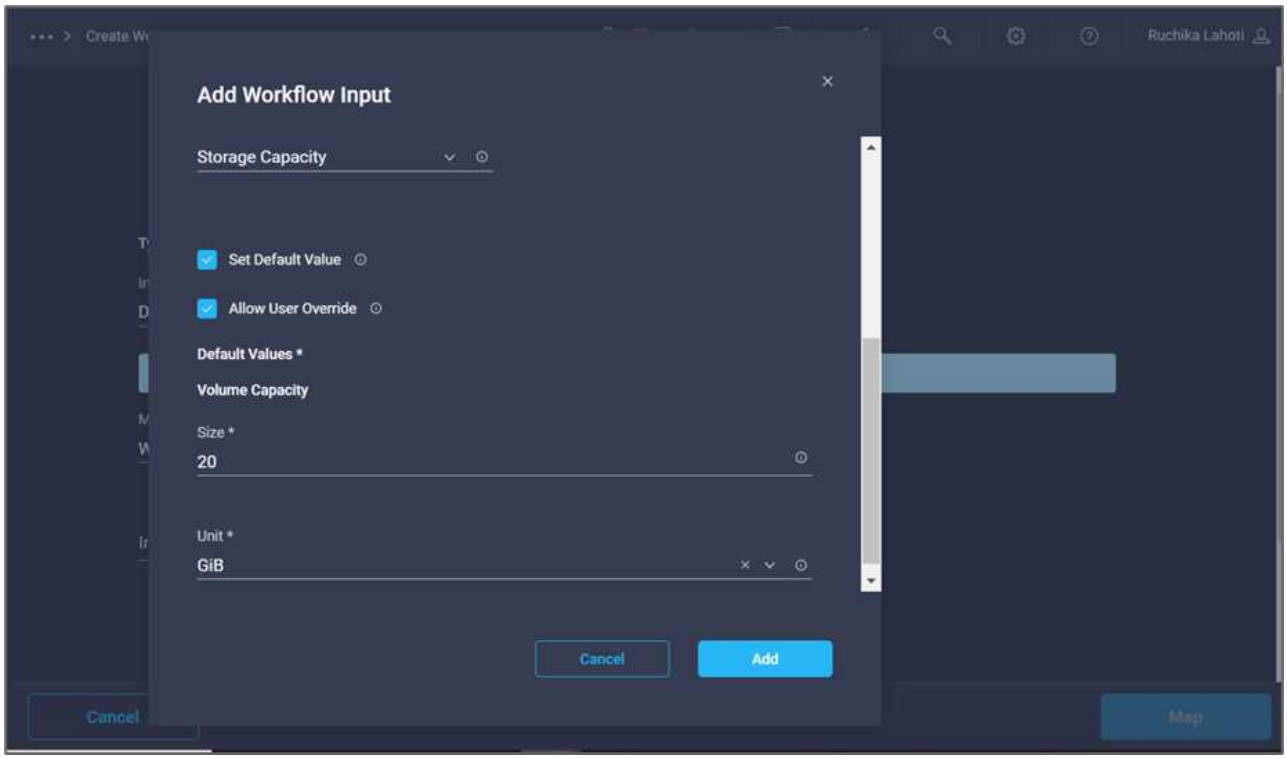
21. [* Volume Capacity*（ボリューム容量*）]フィールドで[* Map]*をクリックします。

22. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。

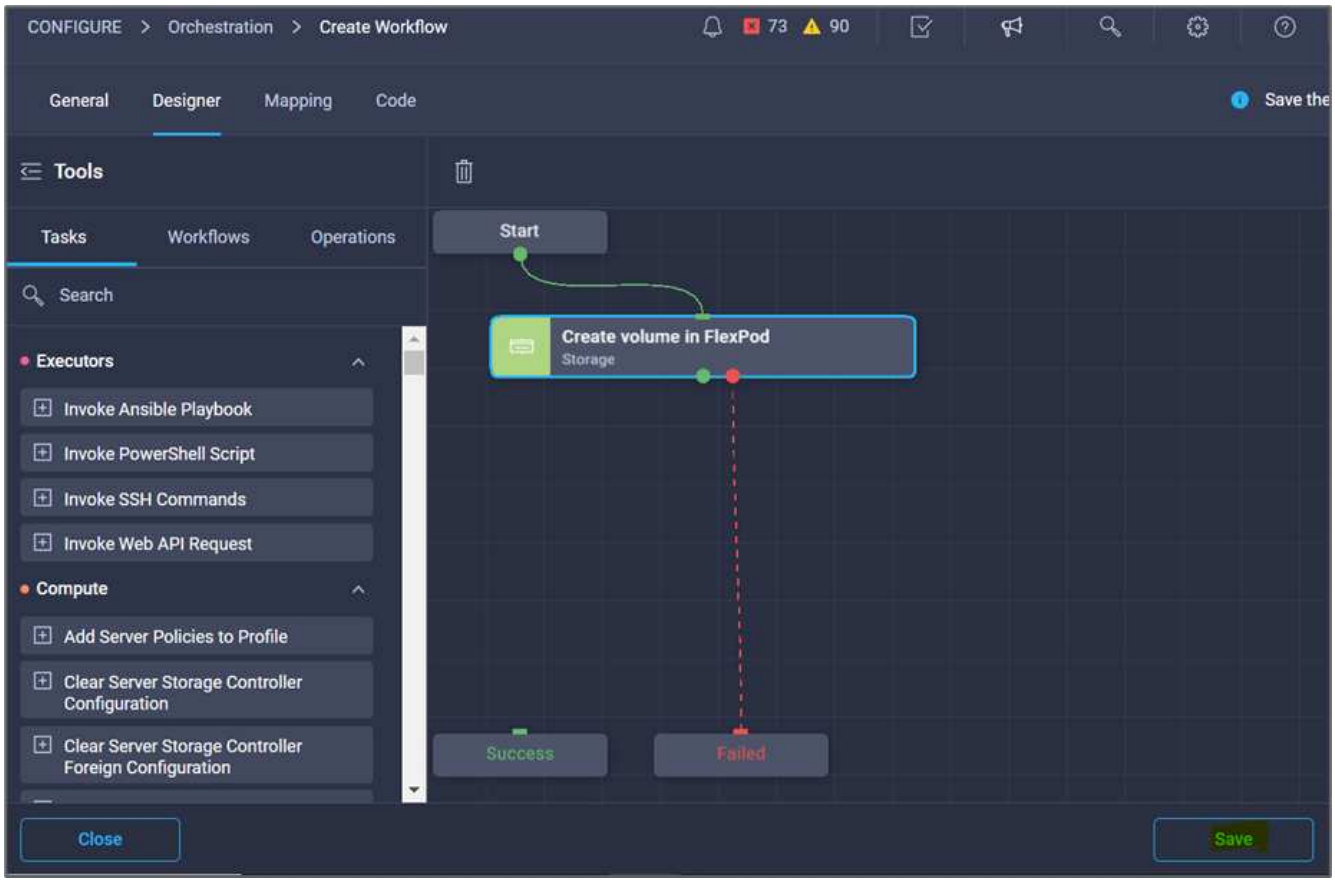
23. [入力名]および[ワークフロー入力の作成]をクリックします。



24. 入力の追加ウィザードで、次の操作を行います。
    a. 表示名と参照名を入力します（オプション）。
    b. [必須]をクリックします。
    c. 「タイプ」で、「ストレージ容量」を選択します。
    d. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    e. ボリュームのサイズと単位をデフォルトで指定します。
    f. [追加（ Add ）] をクリックします。



25. [マップ]をクリックします。
26. コネクターを使用して、FlexPod *タスクで*スタート*と*ボリュームの作成*の間に接続を作成し、*保存*をクリックします。

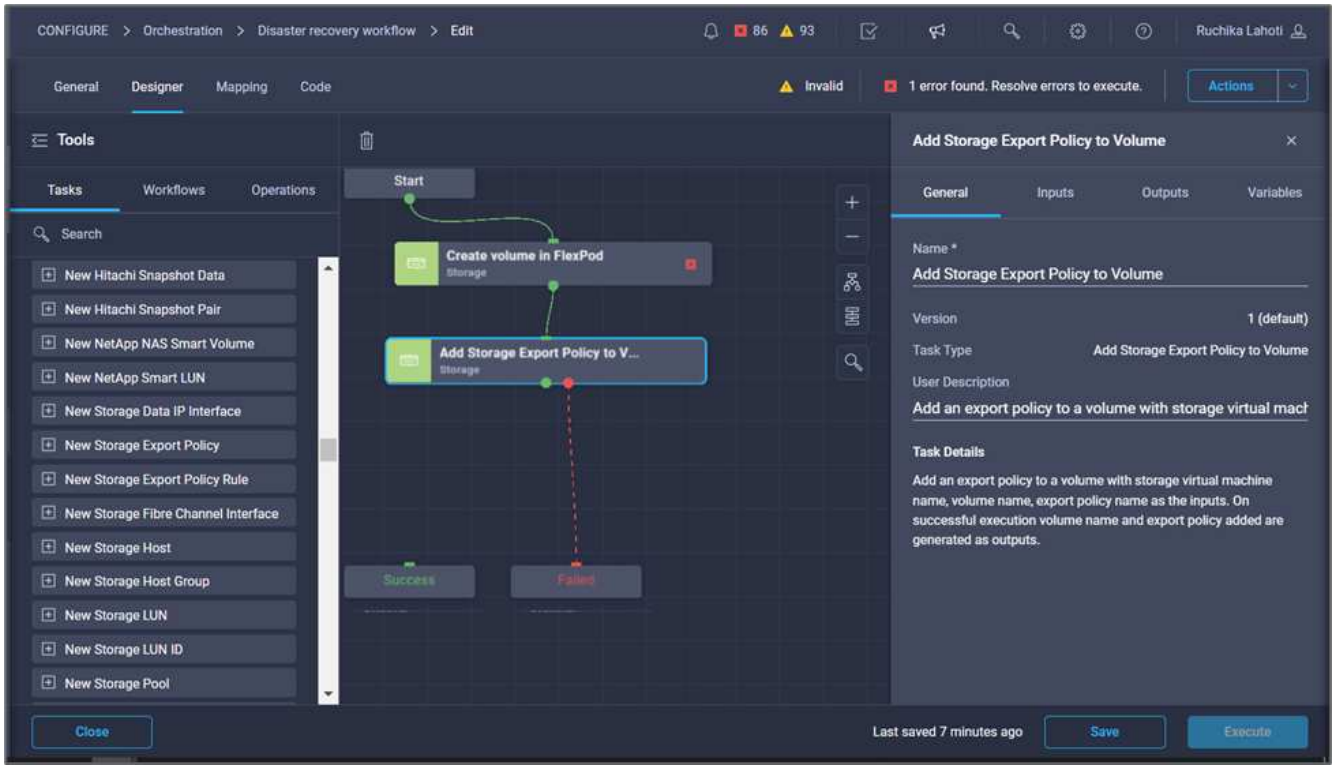


と[ボリュームの作成]の間に接続を作成する方法を示しています。"]

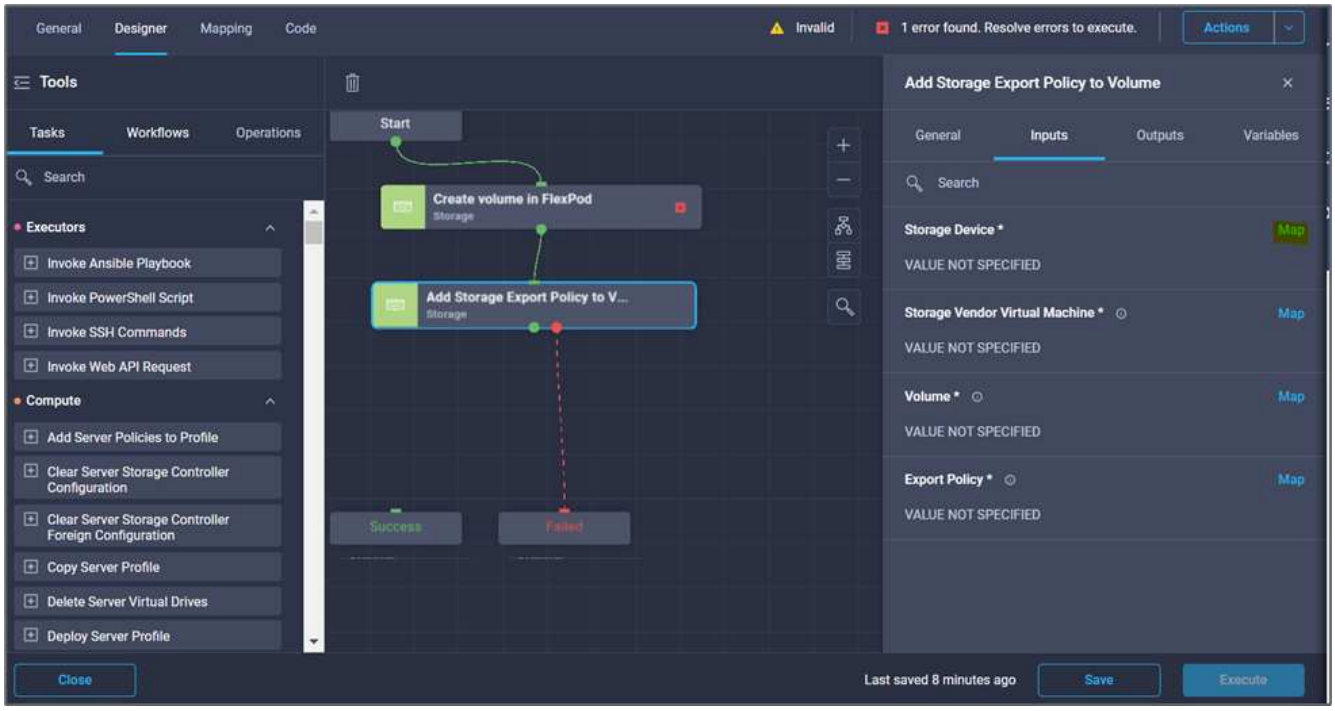
今はエラーを無視してください。このエラーは、成功した移行を指定するために必要なタスク* FlexPod でのボリュームの作成*と* Success *の間に接続がないことが原因で表示されます。

手順 **3**：ストレージエクスポートポリシーを追加します

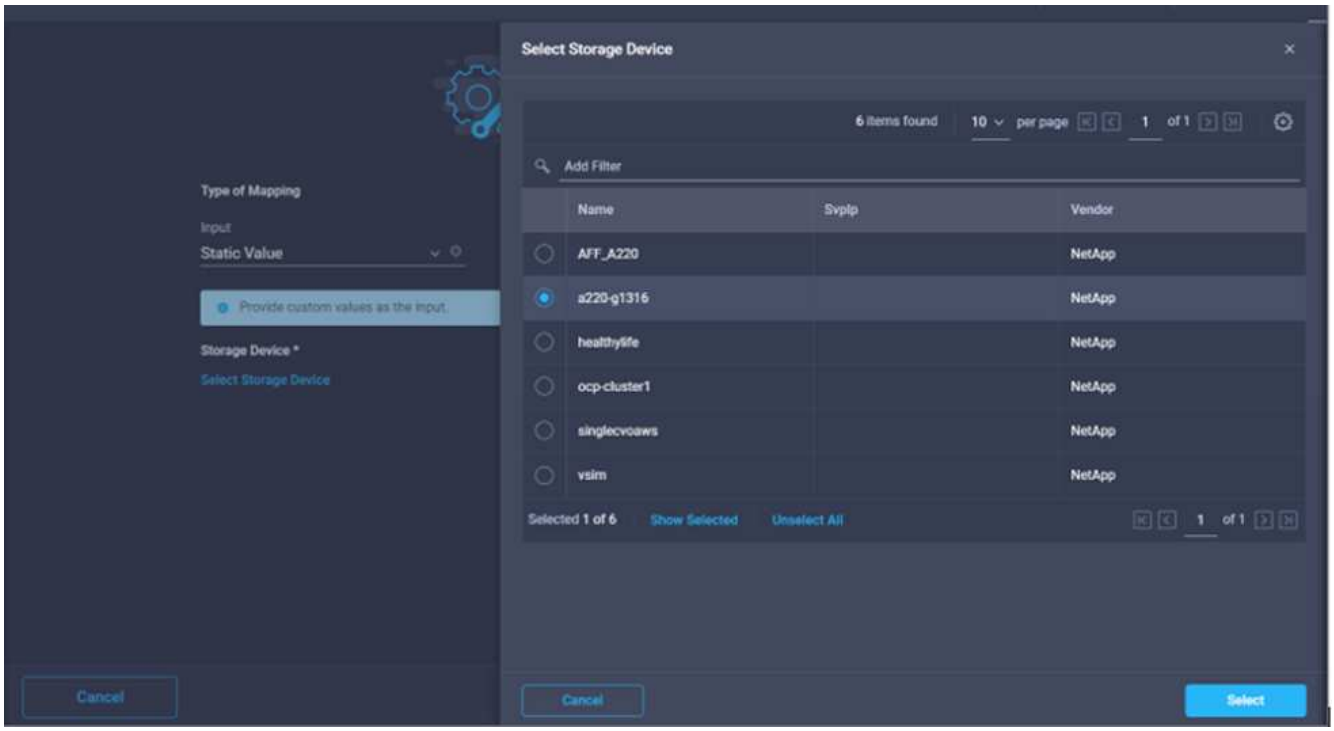
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. デザイン*領域の*ツール*セクションから、*ストレージ>ボリュームへのストレージエクスポートポリシーの追加タスクをドラッグ・アンド・ドロップします。
3. Add Storage Export Policy to Volume（ボリュームへのストレージエクスポートポリシーの追加）をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前はAdd Storage Export Policyです。
4. コネクターを使用して、FlexPod *でのタスク*ボリュームの作成と*ストレージエクスポートポリシーの追加*との間に接続を確立します。[保存（ Save ）] をクリックします。



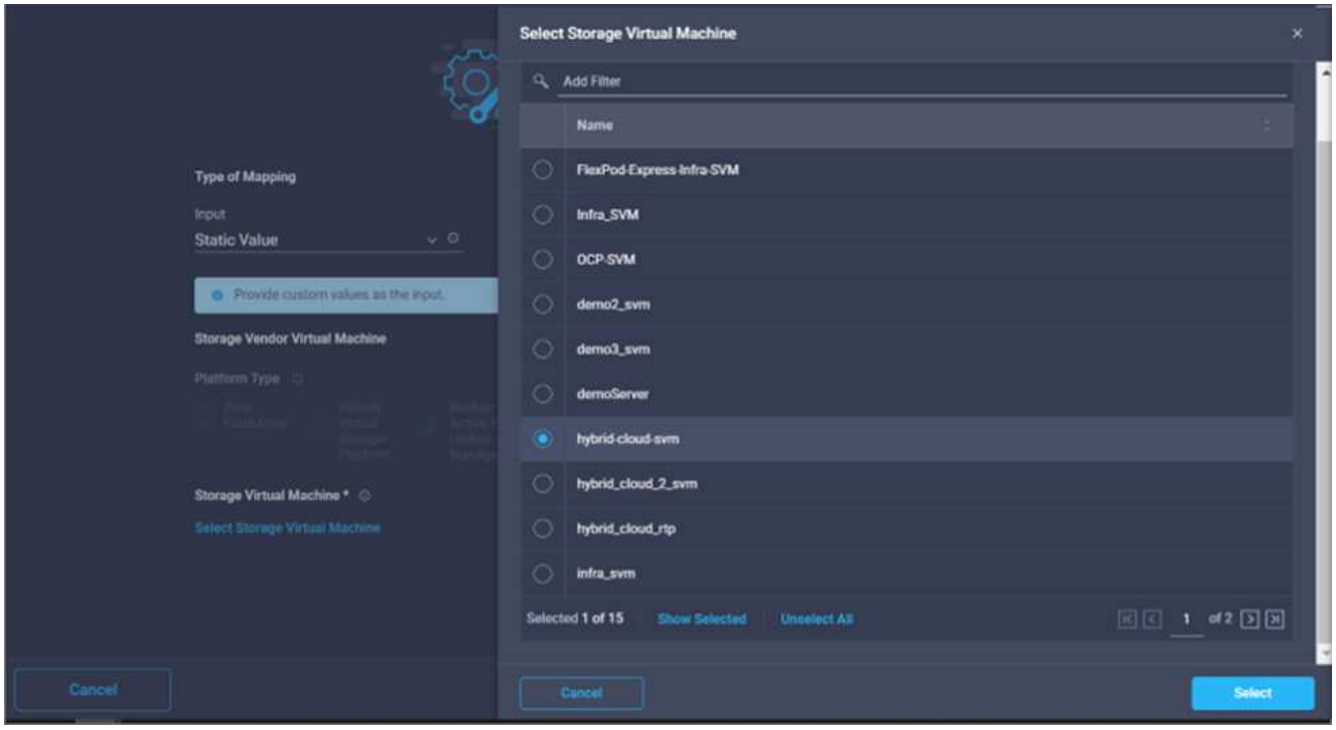
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. [ストレージデバイス]フィールドで[マップ]をクリックします。



7. 「* Static Value 」を選択し、「 Select Storage Device *」をクリックします。新しいストレージボリュームを作成する前のタスクで追加したのと同じストレージターゲットを選択します。
8. [マップ]をクリックします。

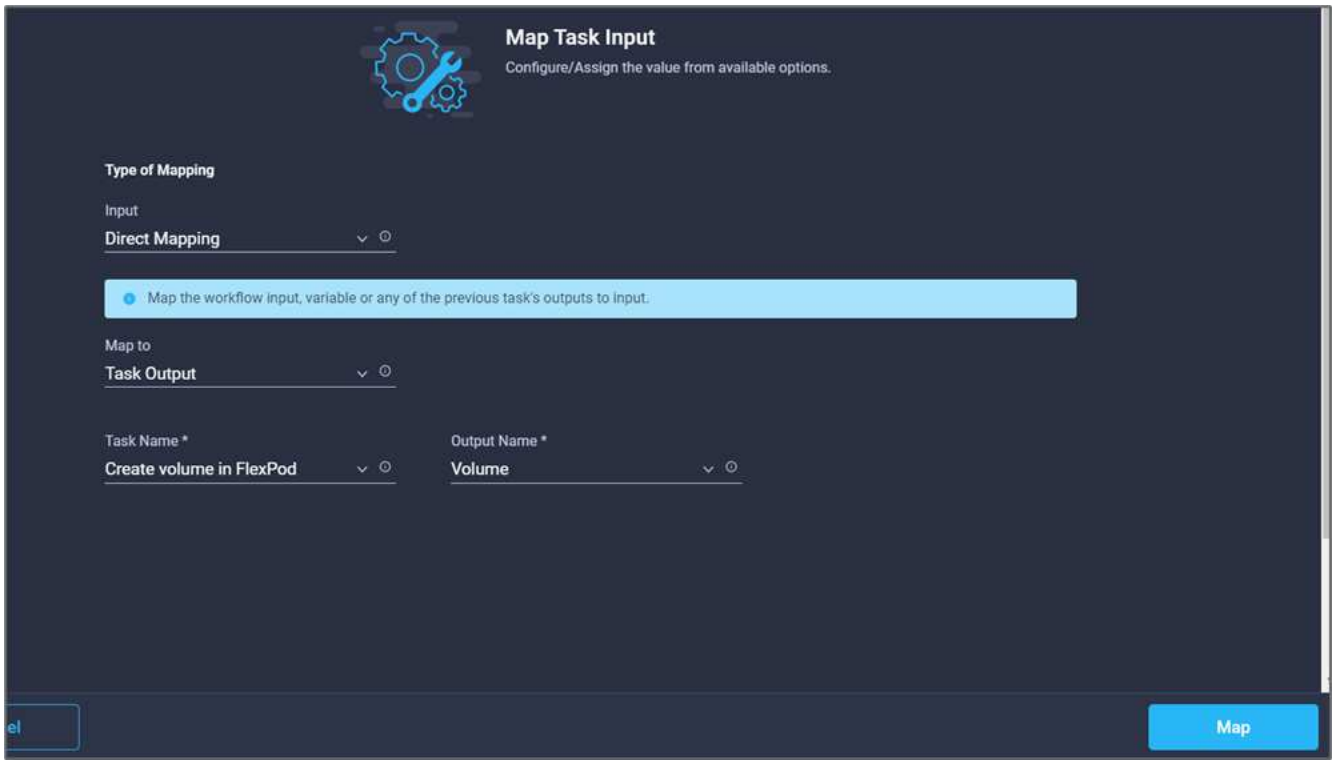


9. Storage Vendor Virtual Machine フィールドで Map *をクリックします。
10. 「* Static Value 」を選択し、「 Storage Virtual Machineの選択*」をクリックします。新しいストレージボリュームを作成する前のタスクの作成時に追加したのと同じStorage Virtual Machineを選択してください。

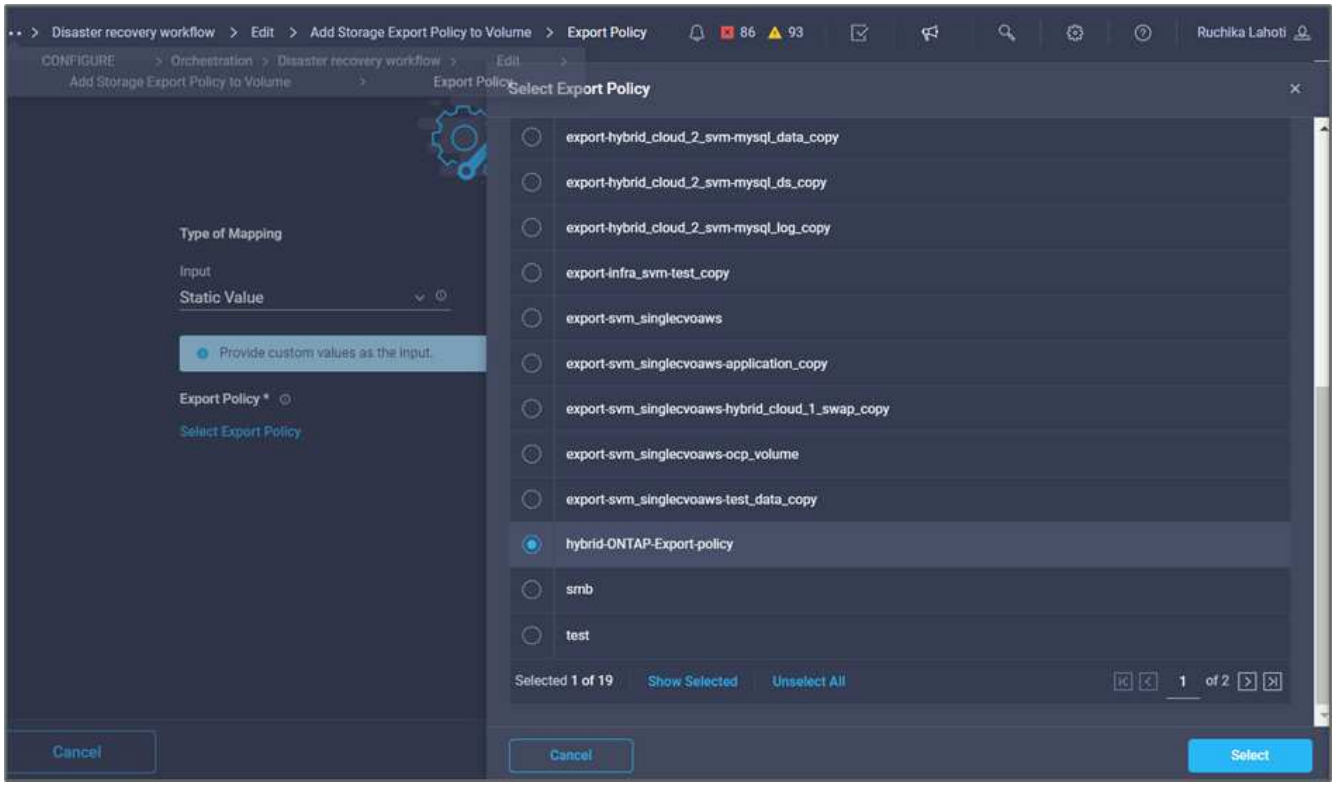


11. [マップ]をクリックします。
12. [* Volume*（ボリューム*）]フィールドの[マップ（* Map *）]をクリック
13. タスク名*をクリックし、FlexPod でボリュームを作成をクリックします。**[***出力名]、[ボリューム]の順にクリックします。

> Cisco Intersight Cloud Orchestratorでは、前のタスクの出力を新しいタスクの入力として指定できます。この例では、「FlexPod でのボリュームの作成」タスクの入力として「ボリューム」の詳細がタスク*ストレージエクスポートポリシーの追加」から提供されています。



14. [マップ]をクリックします。
15. [エクスポートポリシー]フィールドで[マップ]をクリックします。
16. 「* Static Value 」を選択し、「*エクスポートポリシーの選択」をクリックします。作成したエクスポートポリシーを選択します。

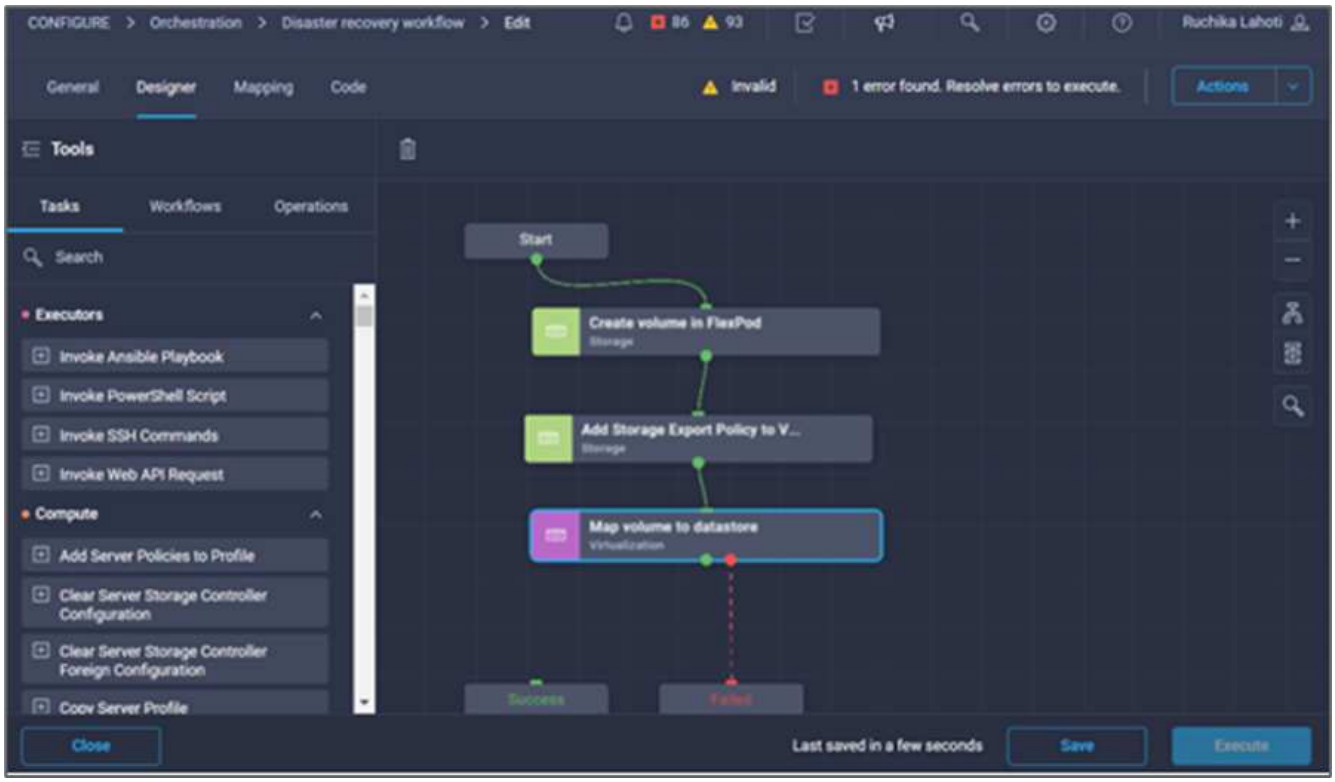


17. [マップ]、[保存]の順にクリックします。

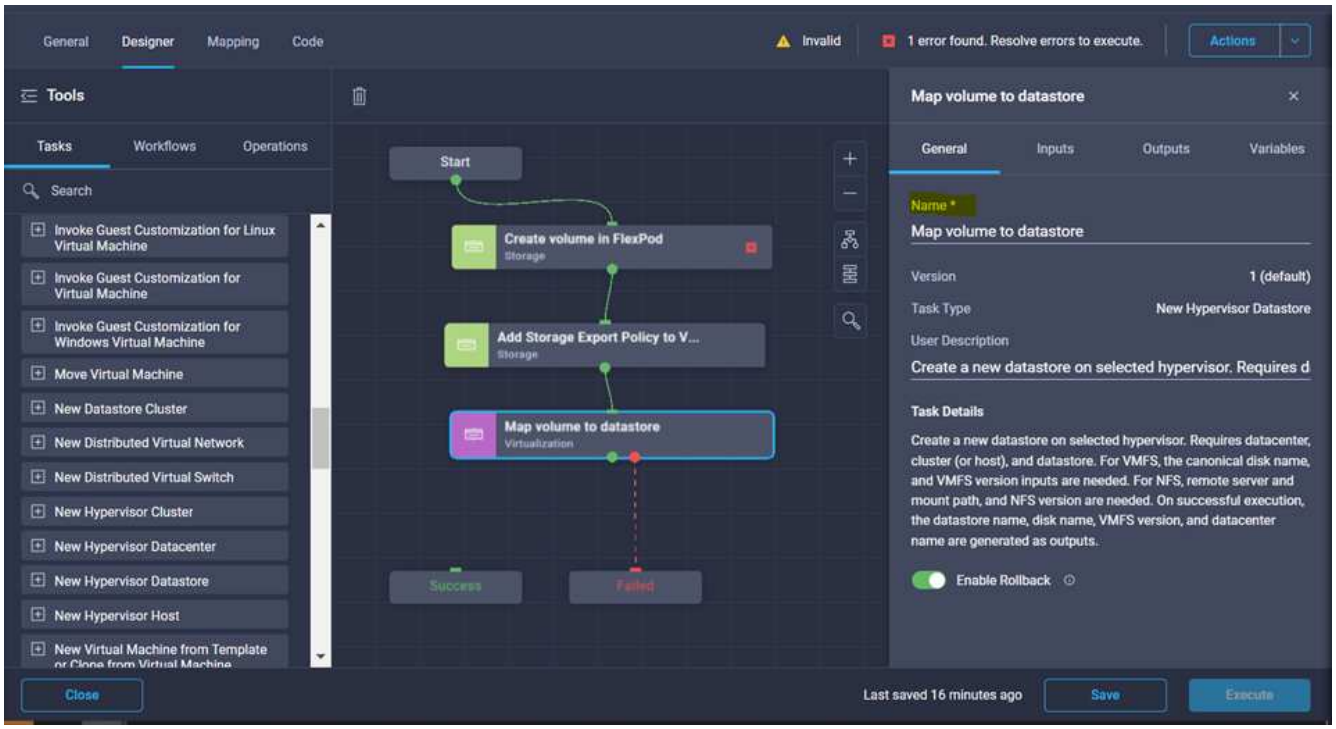
これで、ボリュームへのエクスポートポリシーの追加は完了です。次に、作成したボリュームをマッピングする新しいデータストアを作成します。

手順 **4**：**FlexPod** ボリュームをデータストアにマッピングする

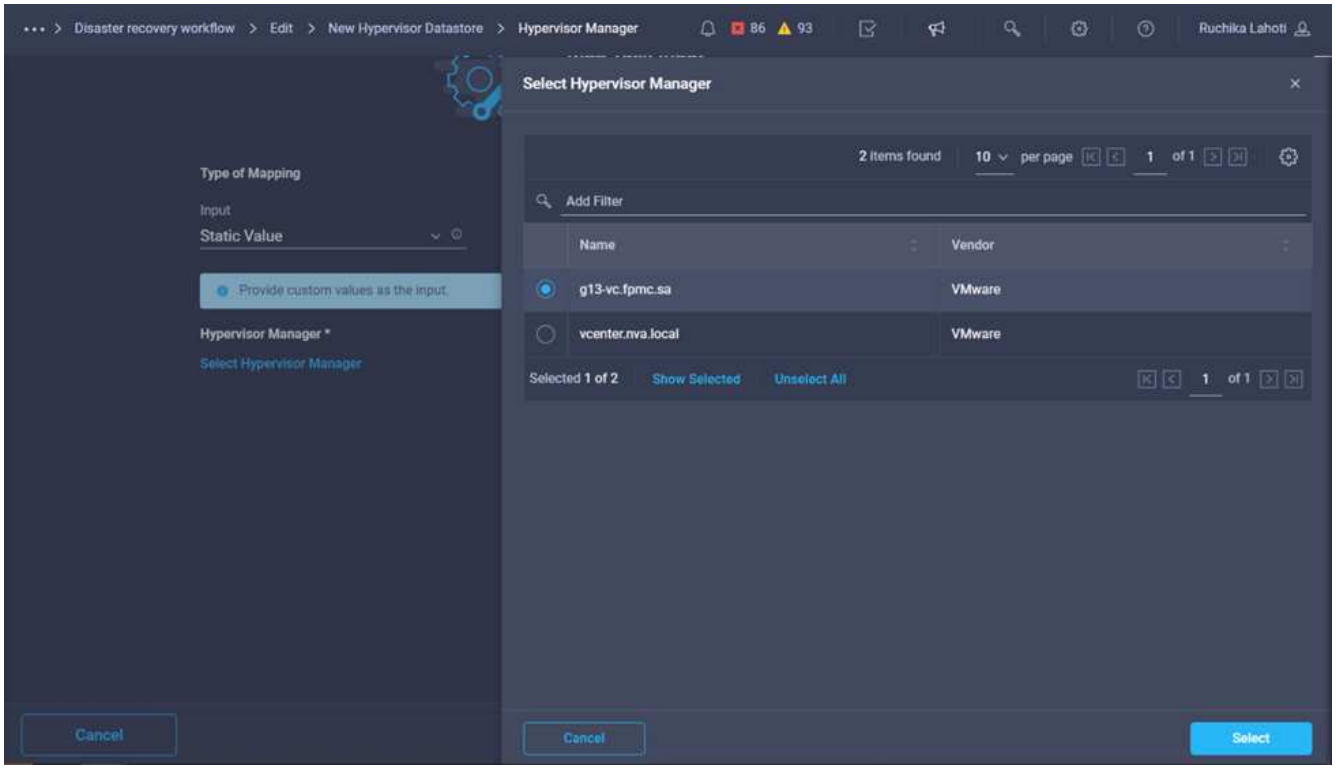
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. 「デザイン」領域の「ツール*」セクションから*「仮想化」>「新しいハイパーバイザー・データストア*」タスクをドラッグアンド・ドロップします。
3. コネクタを使用して、*ストレージエクスポートポリシーの追加*タスクと*新しいハイパーバイザーデータストア*タスクを接続します。[保存（ Save ）] をクリックします。



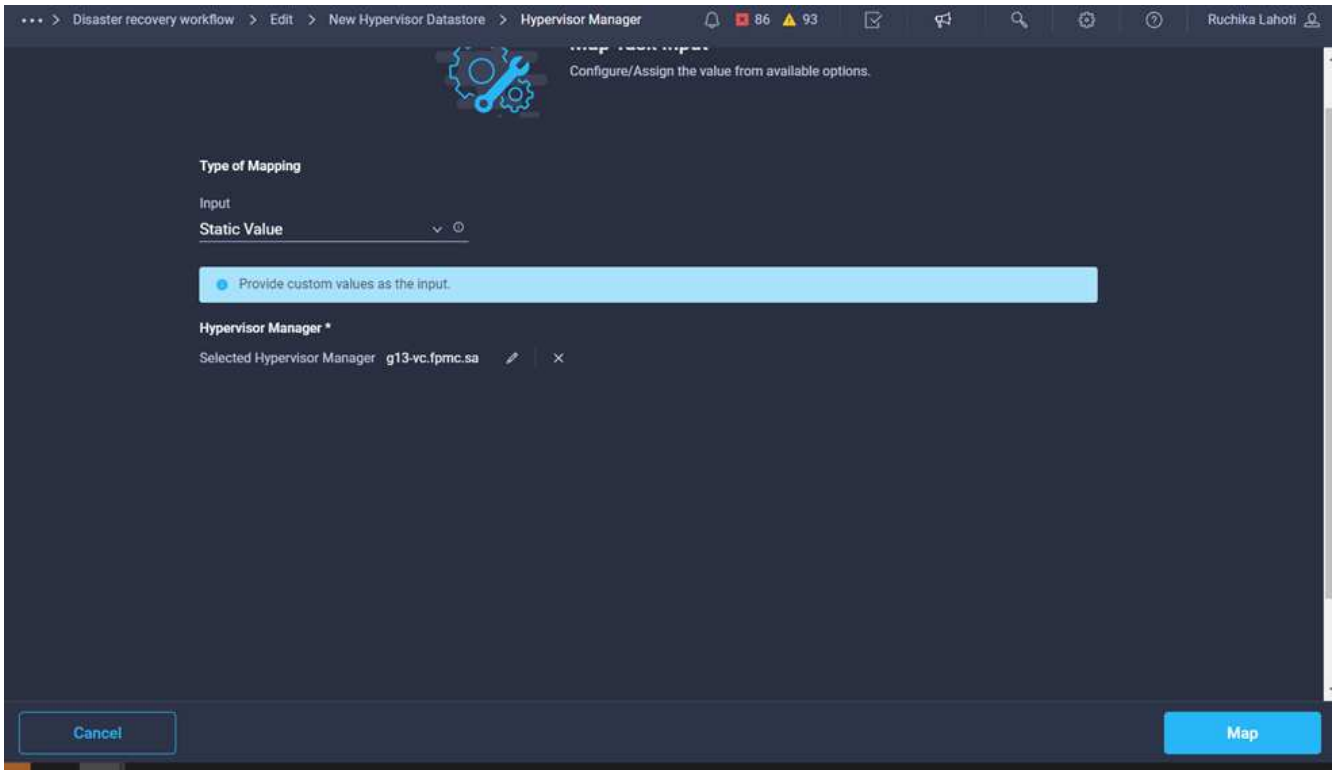
4. [New Hypervisor Datastore]をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前は*ボリュームをデータストアにマッピング*です。



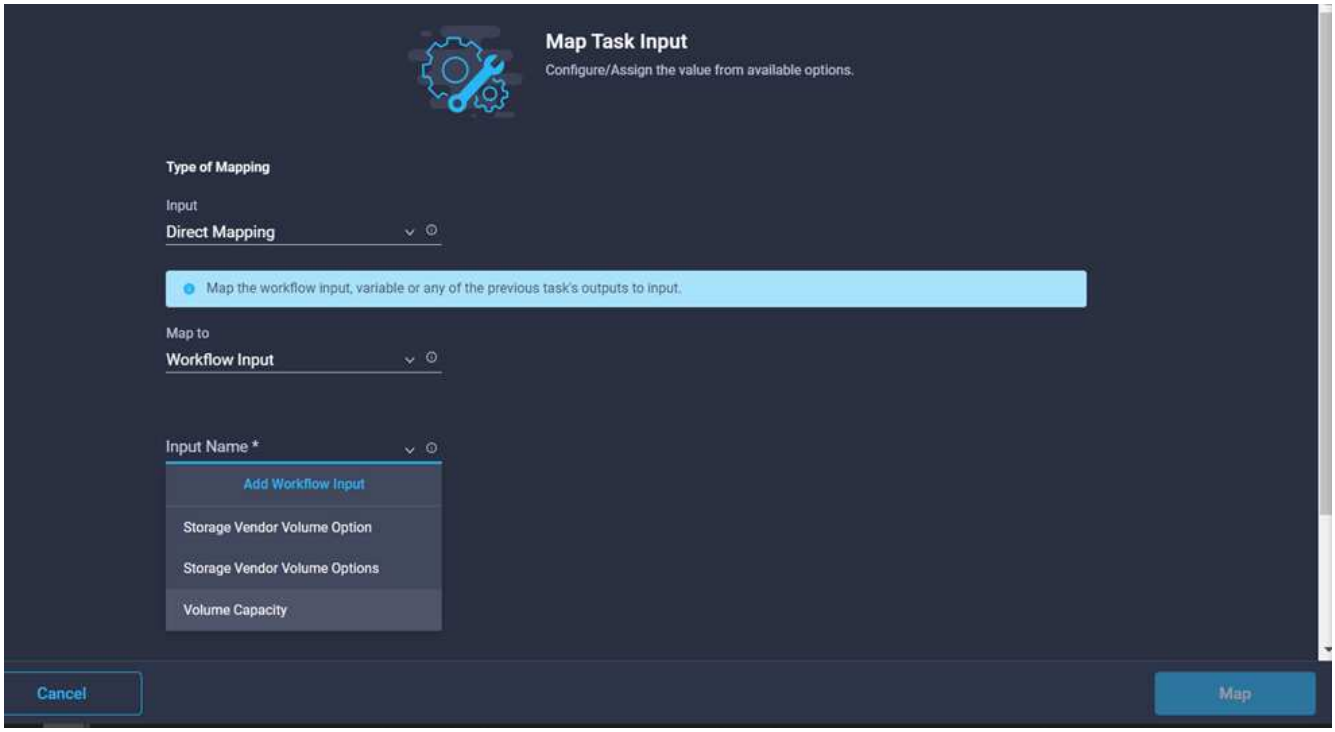
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. [* Hypervisor Manager*]フィールドで[* Map]をクリックします。
7. 「* Static Value 」を選択し、「*ハイパーバイザーマネージャーの選択」をクリックします。VMware vCenterターゲットをクリックします。



8. [マップ]をクリックします。



9. [データセンター]フィールドで[マップ]をクリックします。新しいデータストアに関連付けられているデータセンターです。
10. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
11. [入力名]、[ワークフロー入力の作成]の順にクリックします。



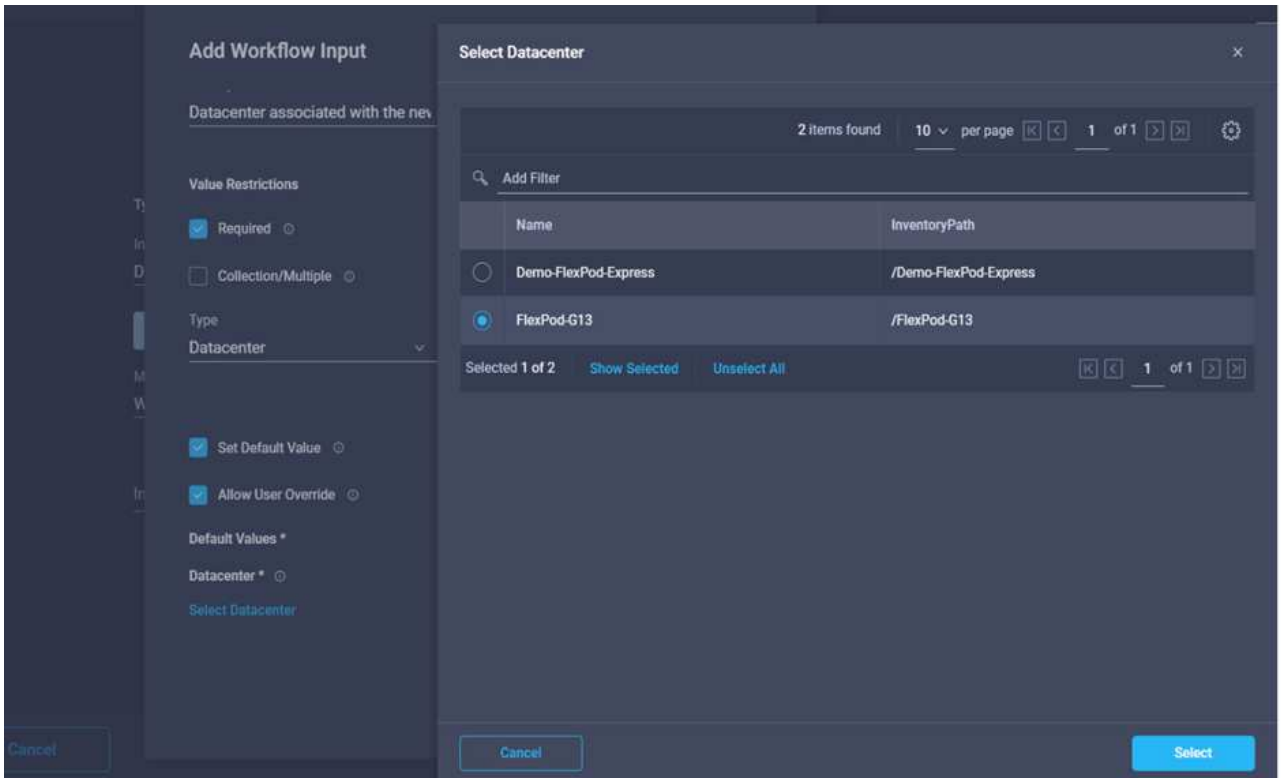
12. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。

b. タイプとして* Datacenter *を選択します。

c. [デフォルト値の設定]と[オーバーライド*]をクリックします。

d. [データセンターの選択]をクリックします。

e. 新しいデータストアに関連付けられているデータセンターをクリックし、* Select *をクリックします。

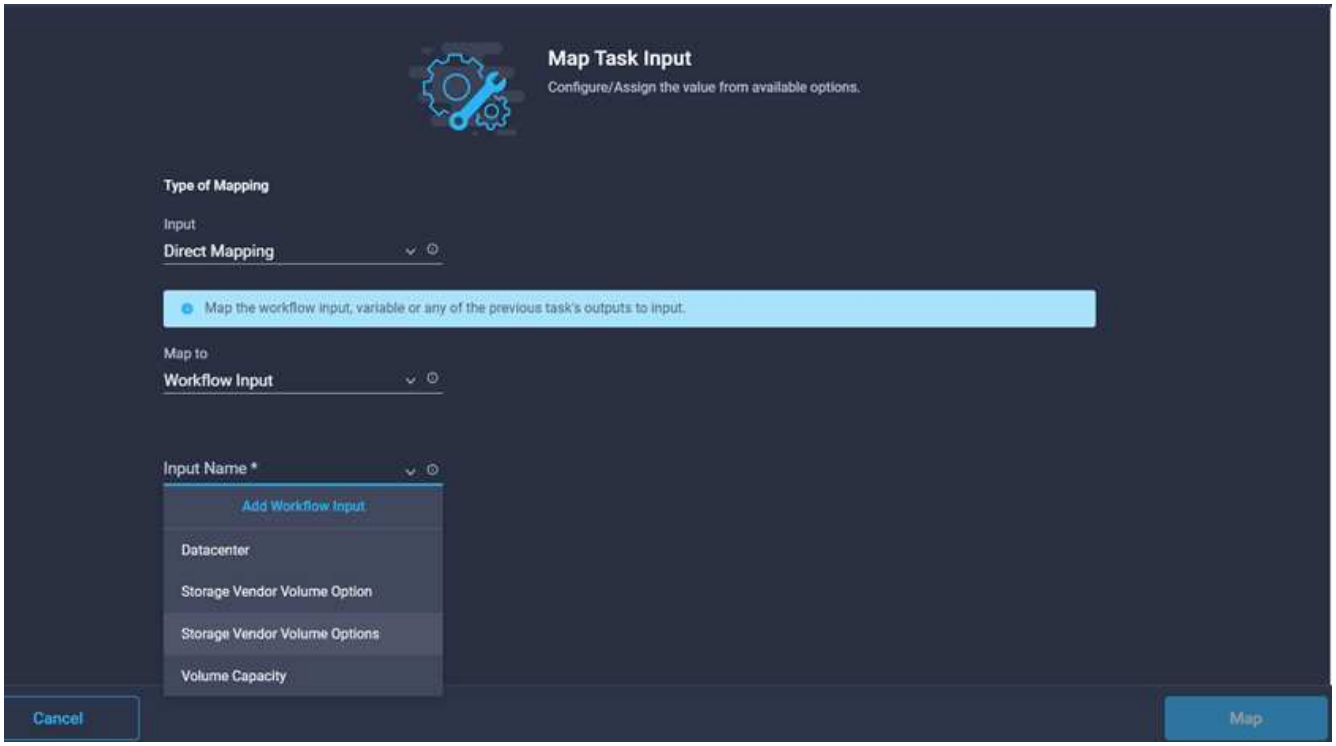


- [追加（ Add ）] をクリックします。

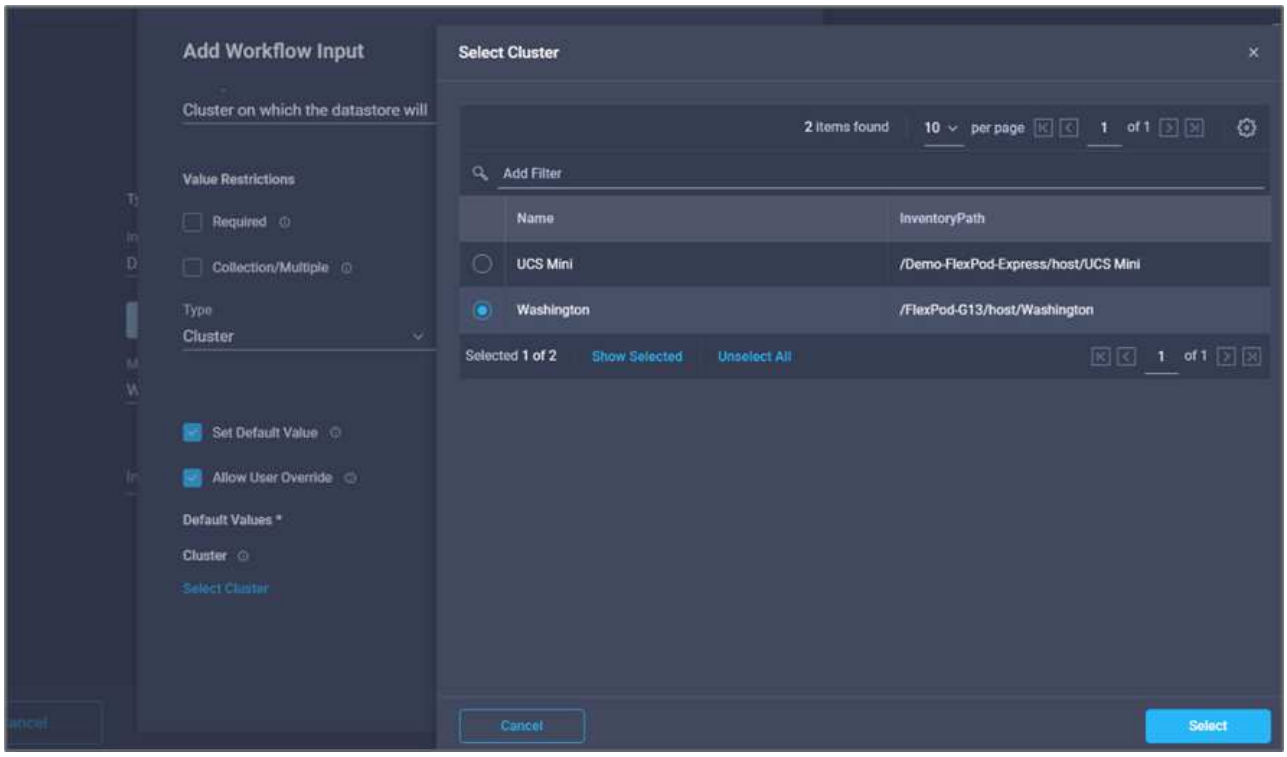
13. [マップ]をクリックします。

14. [**Cluster**]フィールドで[**Map**]をクリックします。

15. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。



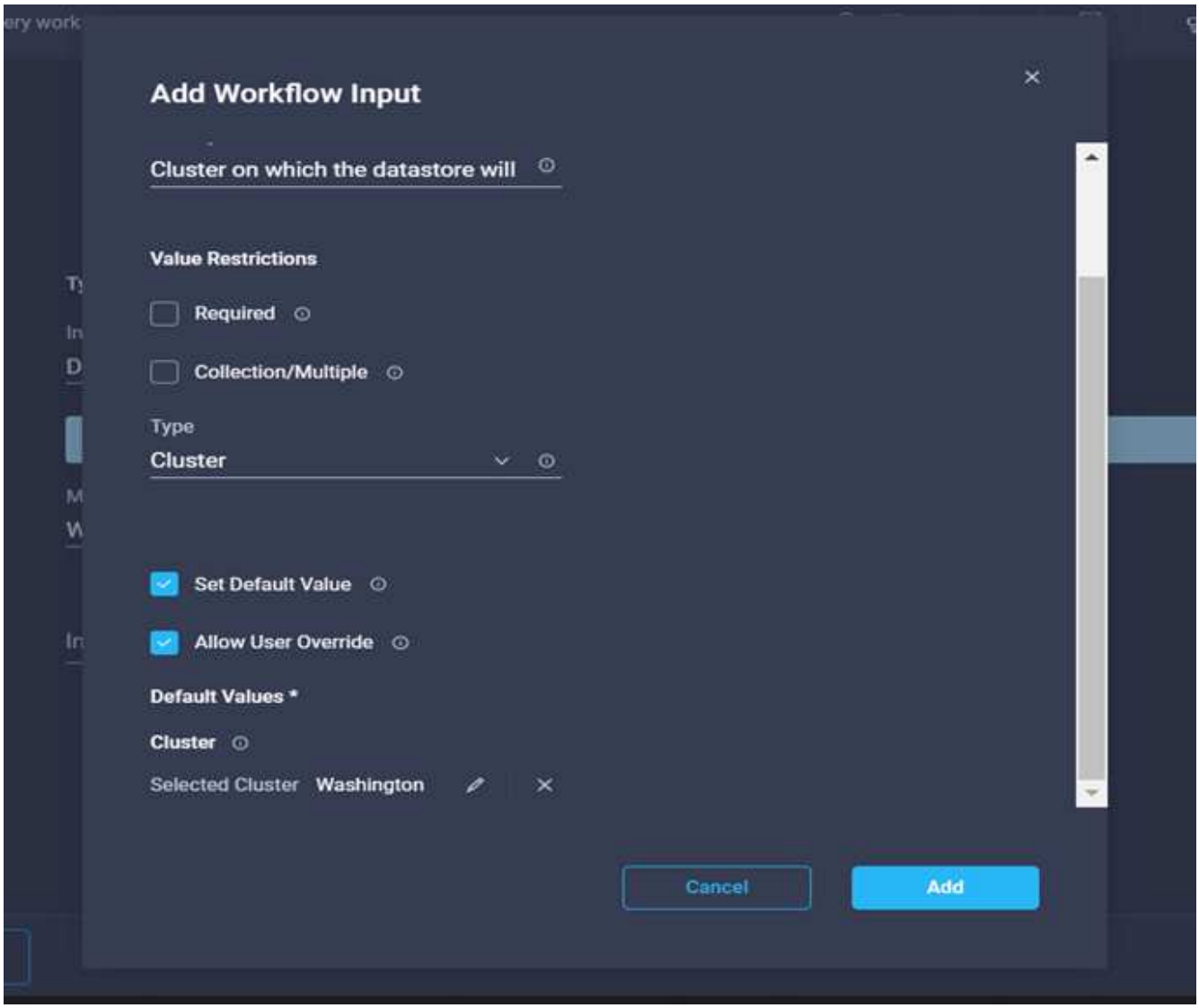
16. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [必須]をクリックします。
    c. タイプとしてClusterを選択します。
    d. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    e. Select Cluster（クラスタの選択）*をクリックします。
    f. 新しいデータストアに関連付けられているクラスタをクリックします。
    g. [* 選択 *] をクリックします。



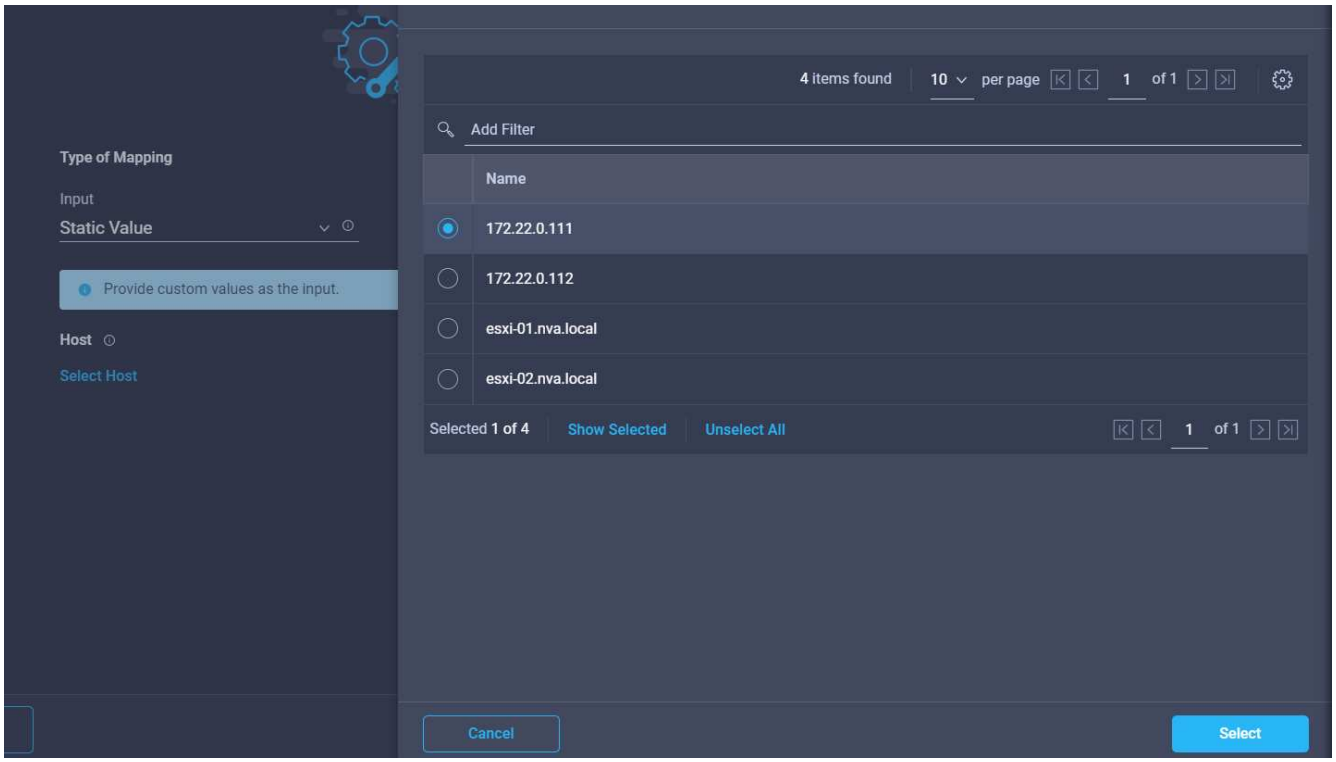
h. [追加（ Add ）] をクリックします。

17. [マップ]をクリックします。

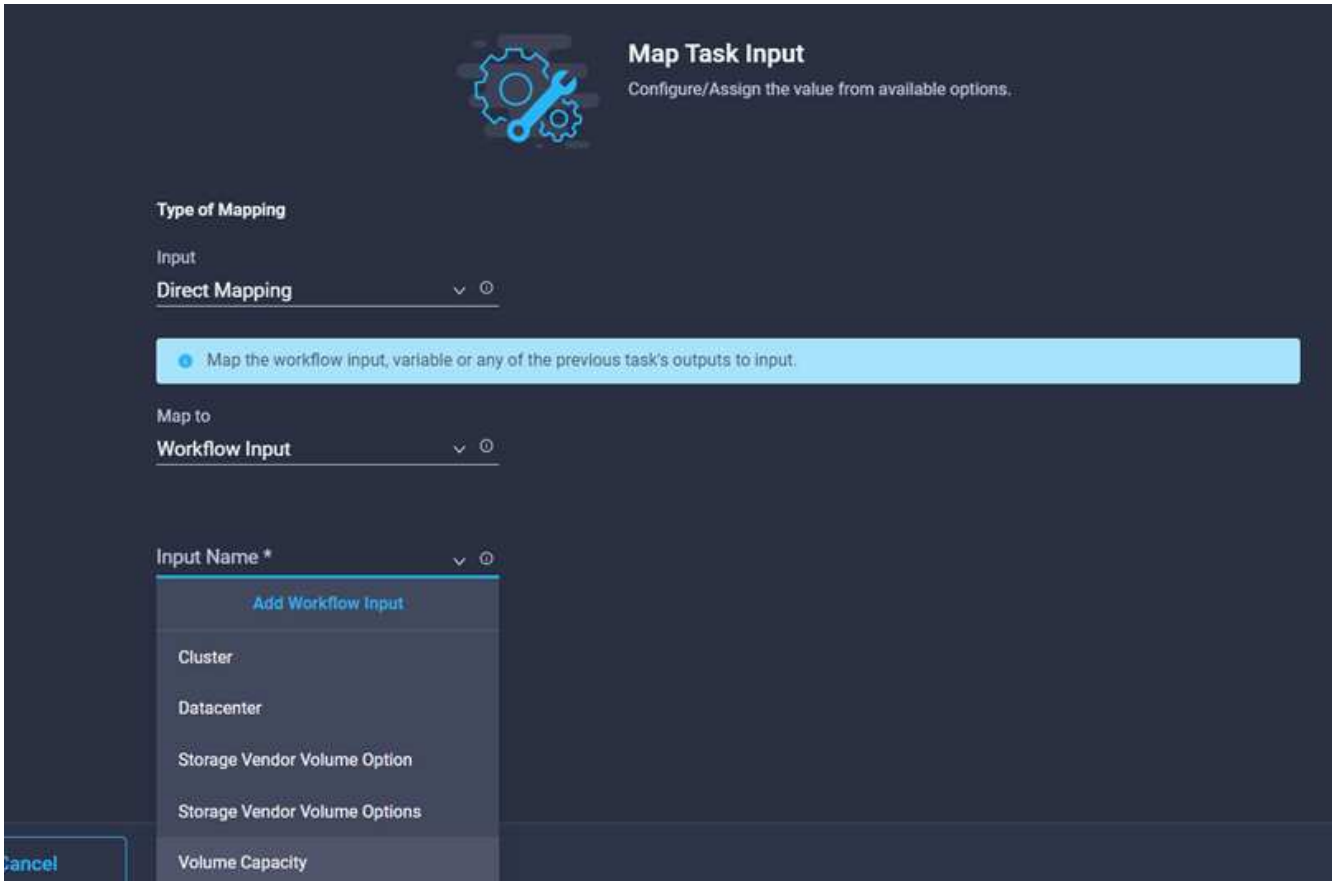
18. [**Host**]フィールドの[**Map**]をクリックします。



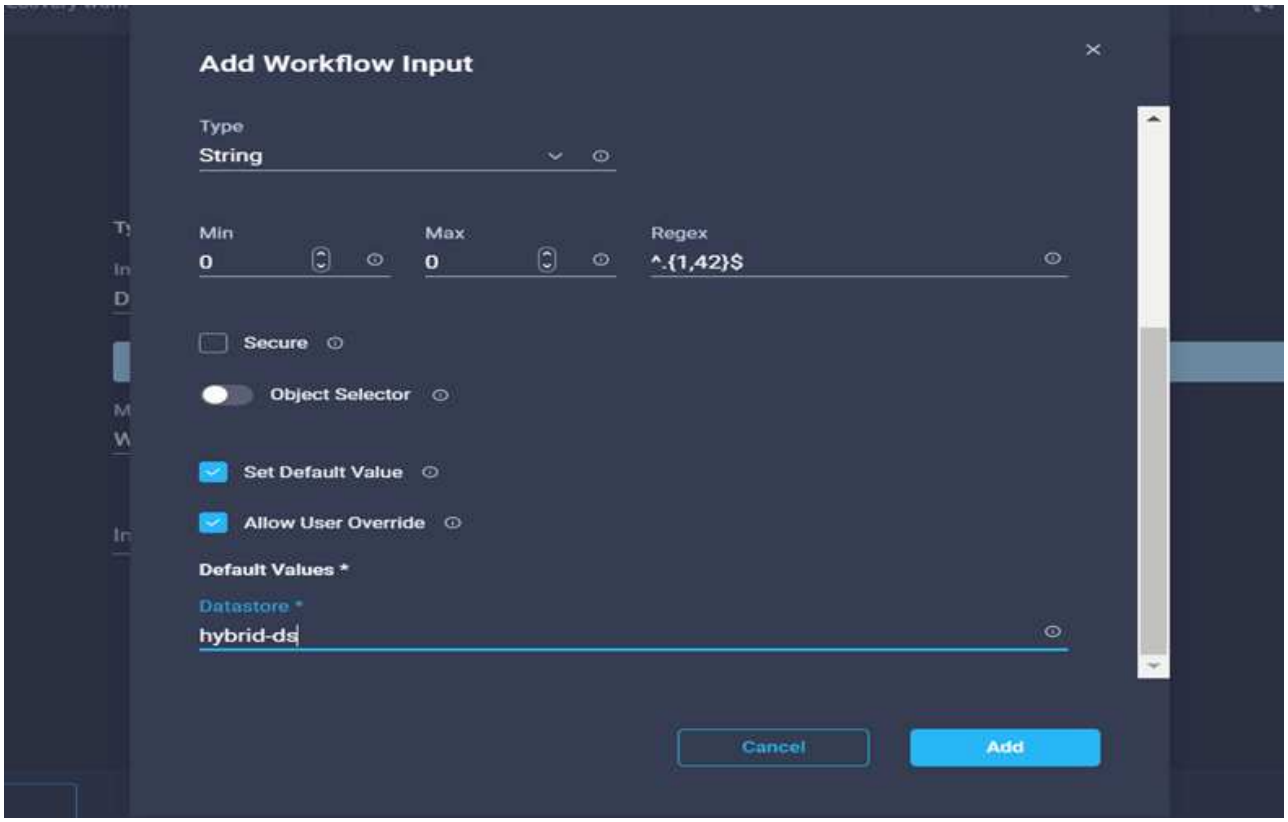
19. 「* Static Value *」を選択し、データストアをホストするホストをクリックします。クラスタを指定した場合、ホストは無視されます。



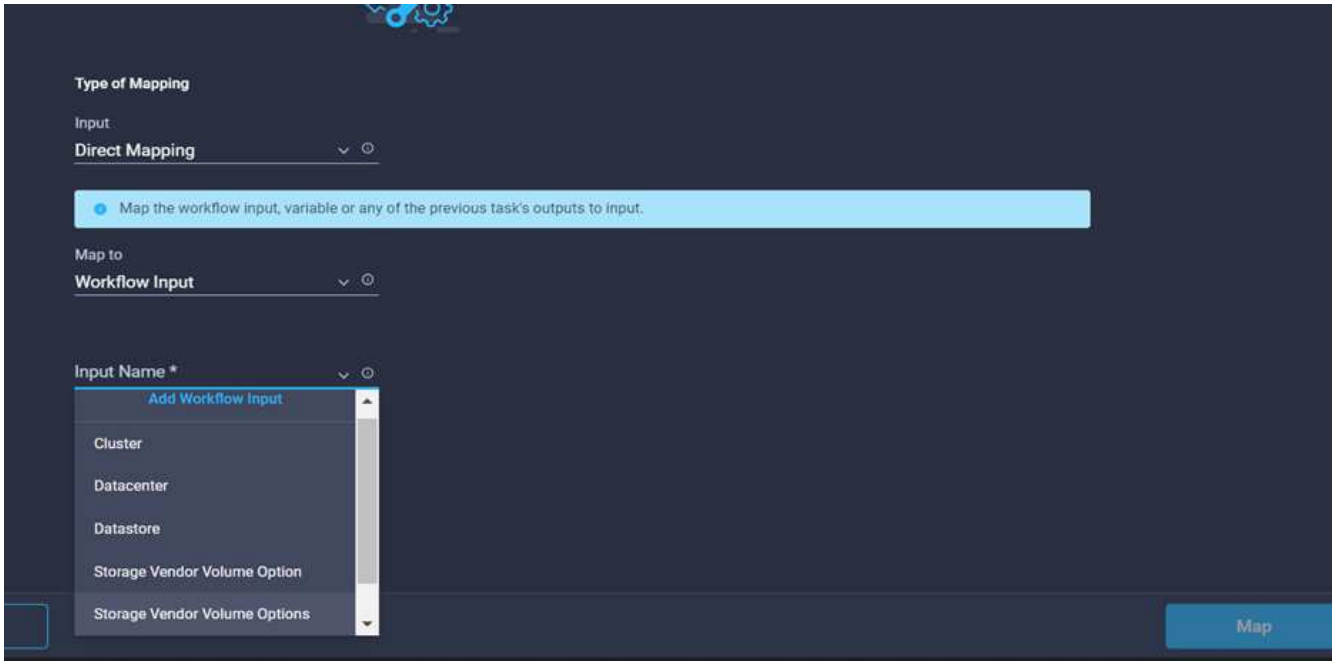
20. [選択してマップ]をクリックします。
21. **[Datastore](**データストア**)**フィールドで**[*Map](**マップ)をクリックします。
22. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
23. [入力名]および[ワークフロー入力の作成]をクリックします。



24. 入力の追加ウィザードで、次の操作を行います。
    a. 表示名と参照名を指定します（オプション）。
    b. [必須]をクリックします。
    c. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    d. データストアのデフォルト値を指定し、* Add *をクリックします。

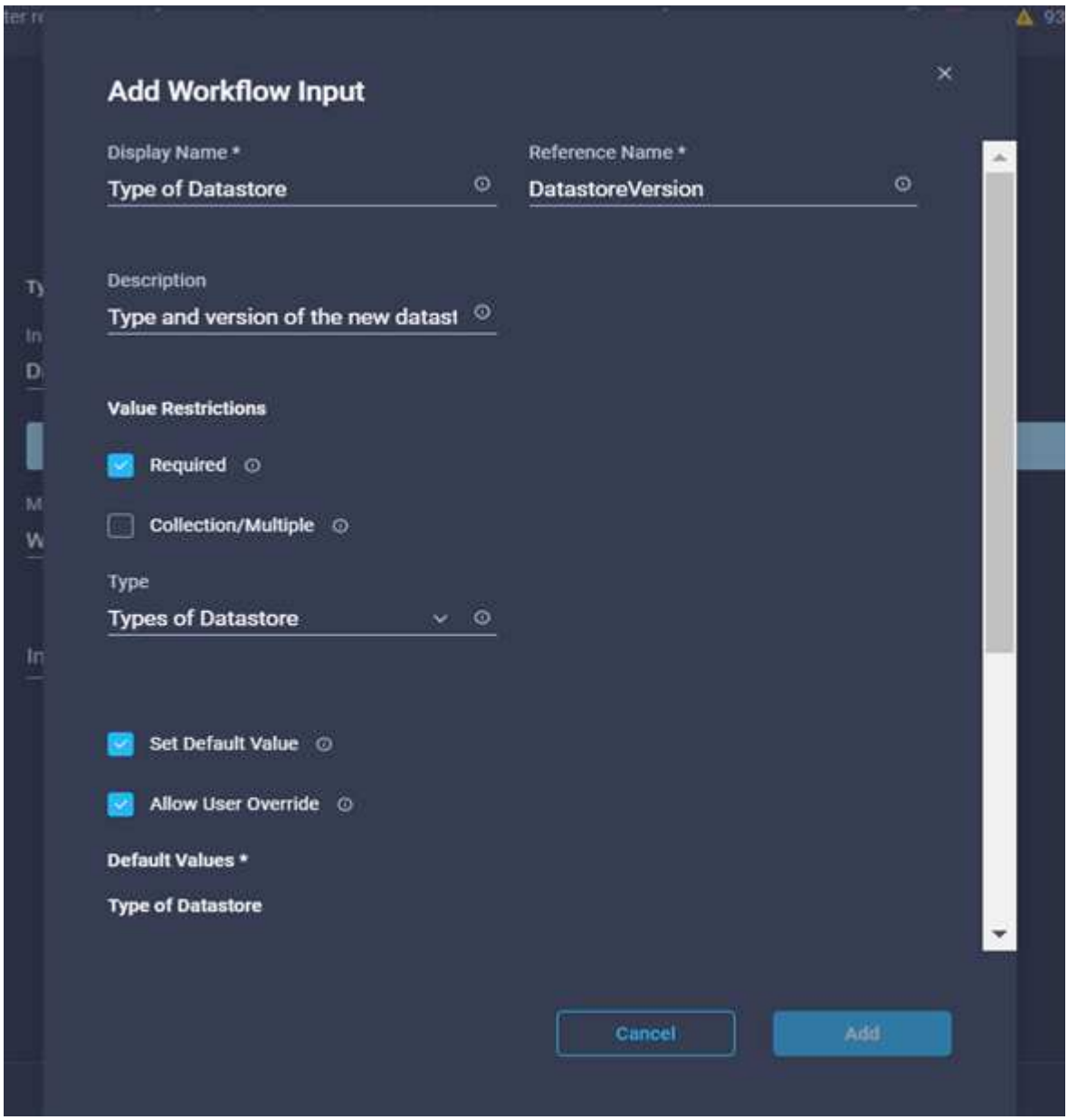


25. [マップ]をクリックします。
26. 入力フィールド*データストアのタイプ*で*マップ*をクリックします。
27. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
28. [入力名]および[ワークフロー入力の作成]をクリックします。



29. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を入力し（オプション）、*必須*をクリックします。

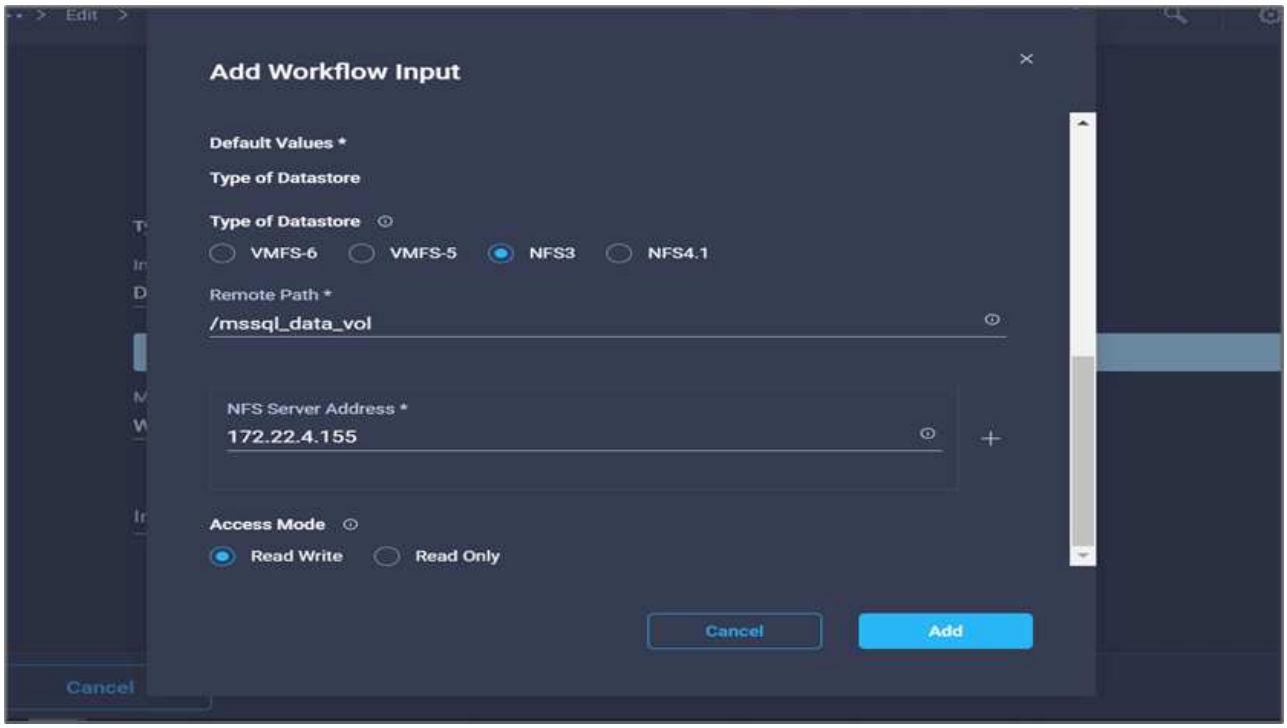
b. タイプ*タイプのデータストア*を選択し、*デフォルト値の設定と上書き*をクリックしてください。



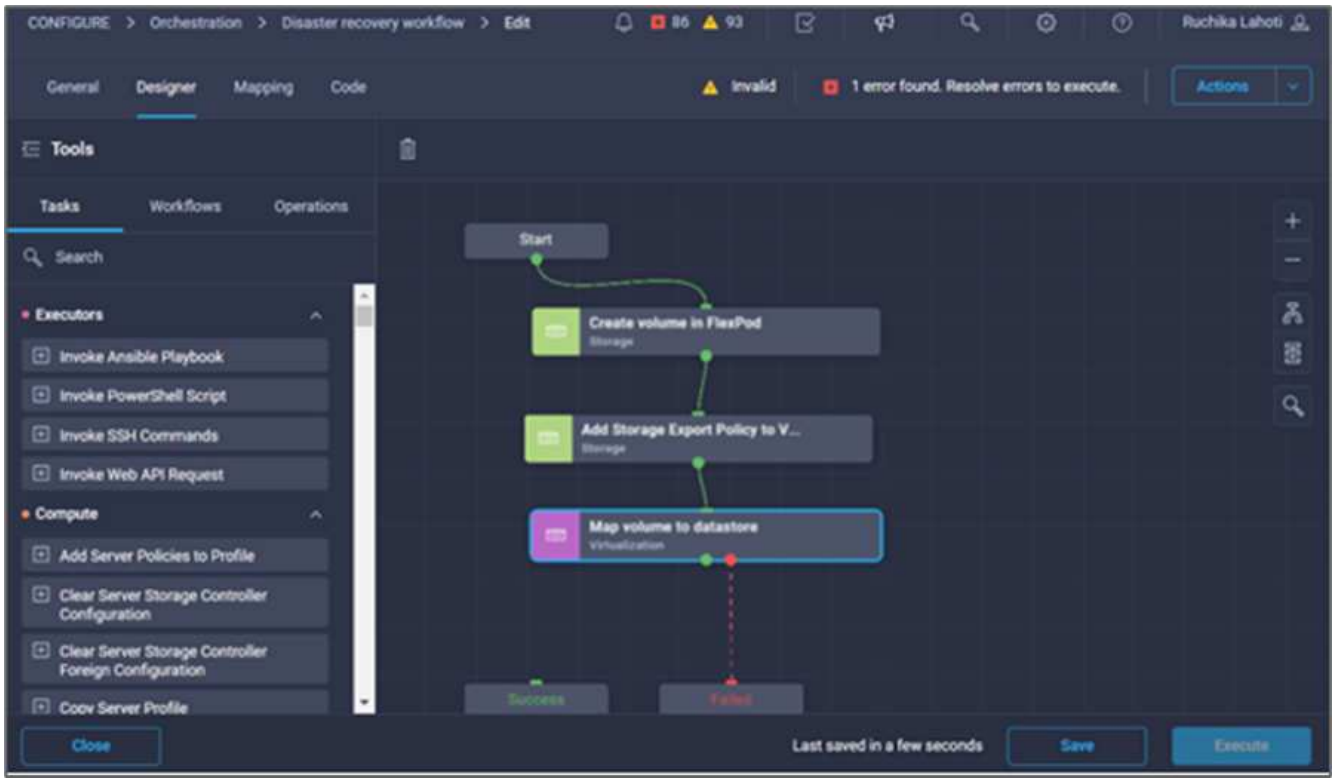
c. リモートパスを指定します。NFSマウントポイントのリモートパスです。

d. NFSサーバアドレスにリモートNFSサーバのホスト名またはIPアドレスを入力します。

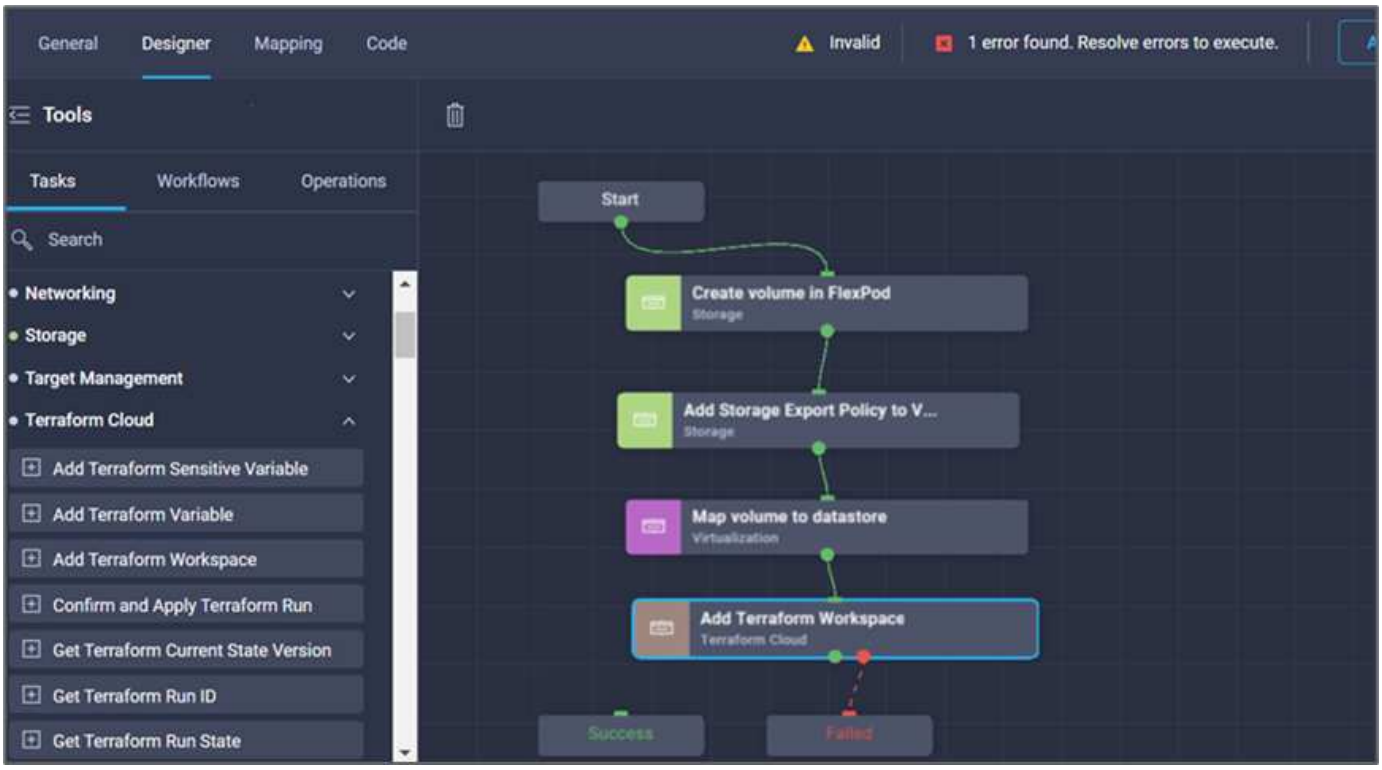
e. [アクセスモード*]をクリックします。アクセスモードはNFSサーバ用です。ボリュームが読み取り専用としてエクスポートされている場合は、[読み取り専用]をクリックします。[追加（ Add ）] をクリックします。



30. [マップ]をクリックします。
31. [保存（ Save ）] をクリックします。

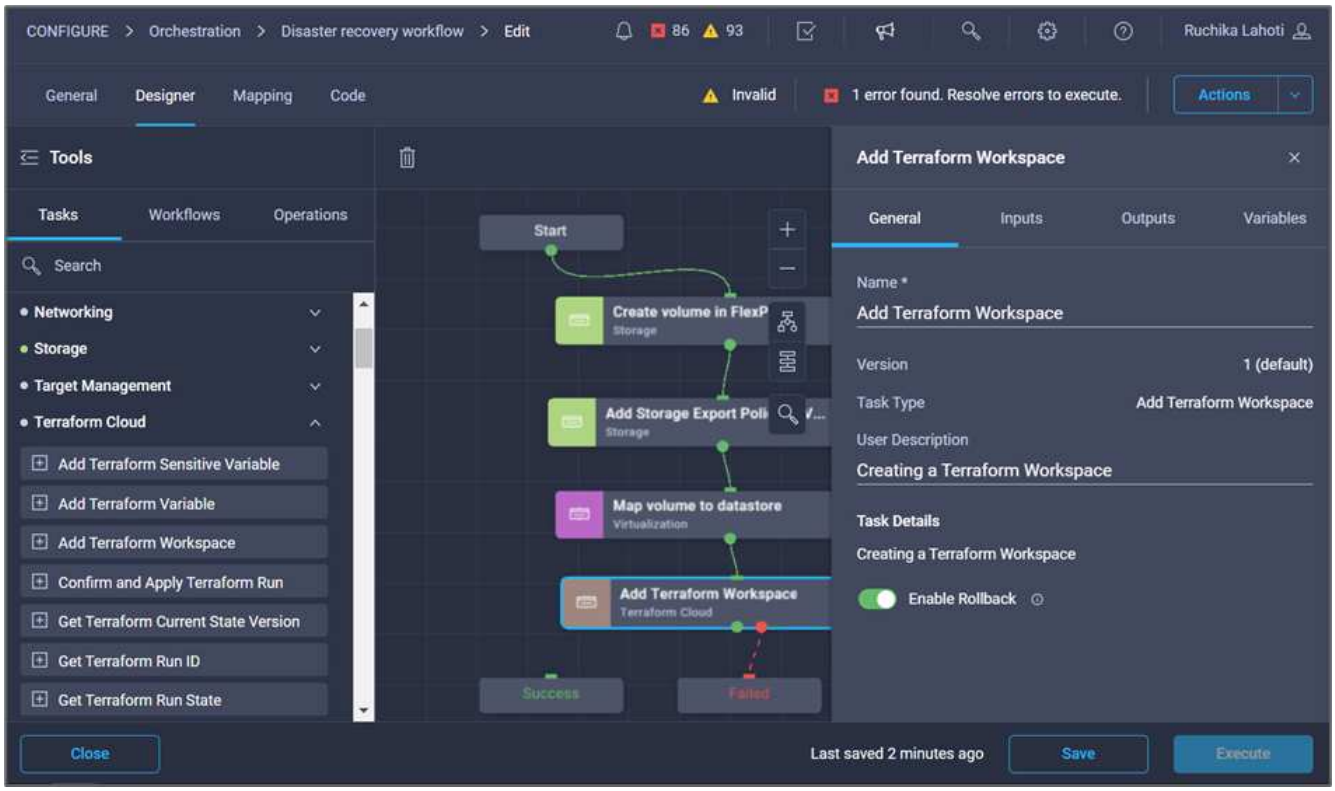


これでデータストアの作成は完了です。オンプレミスのFlexPod データセンターで実行されるすべてのタスクが完了します。

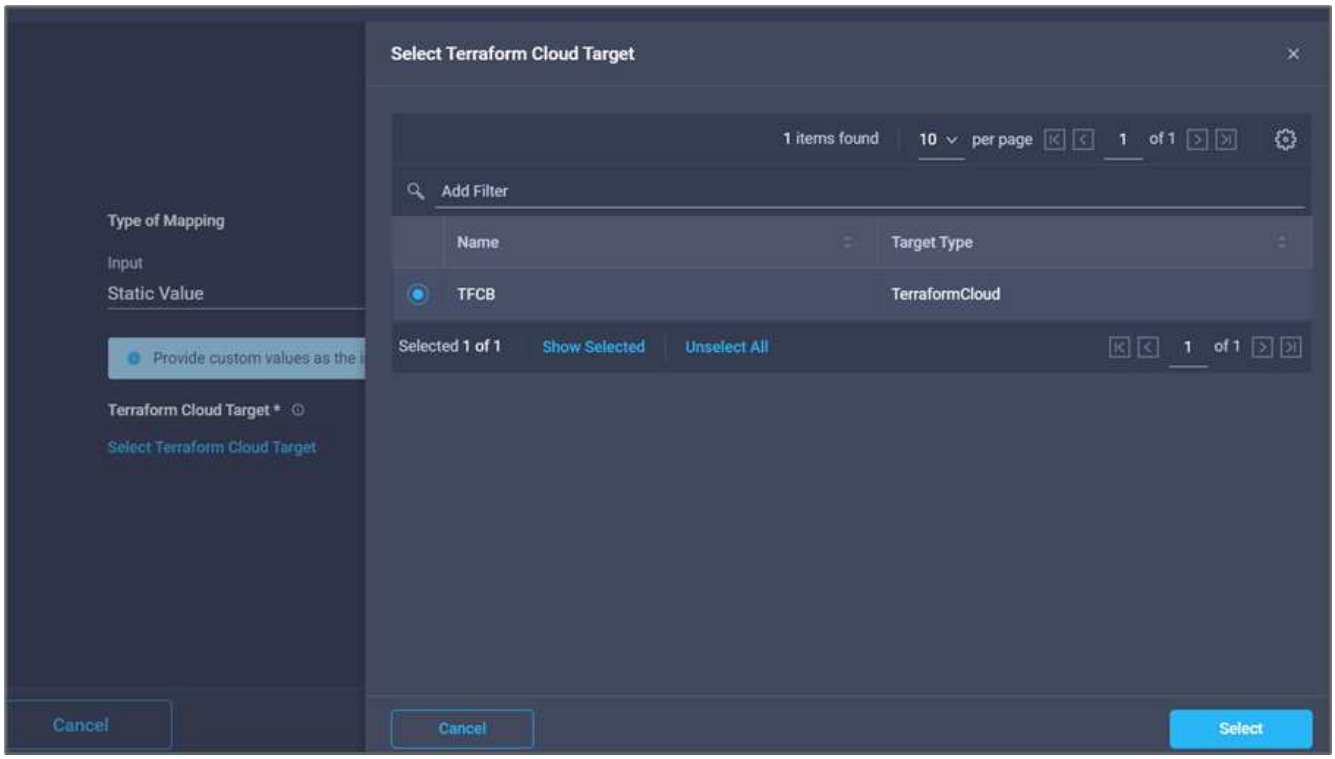


手順 **5:**新しい**Terraform**ワークスペースを追加します

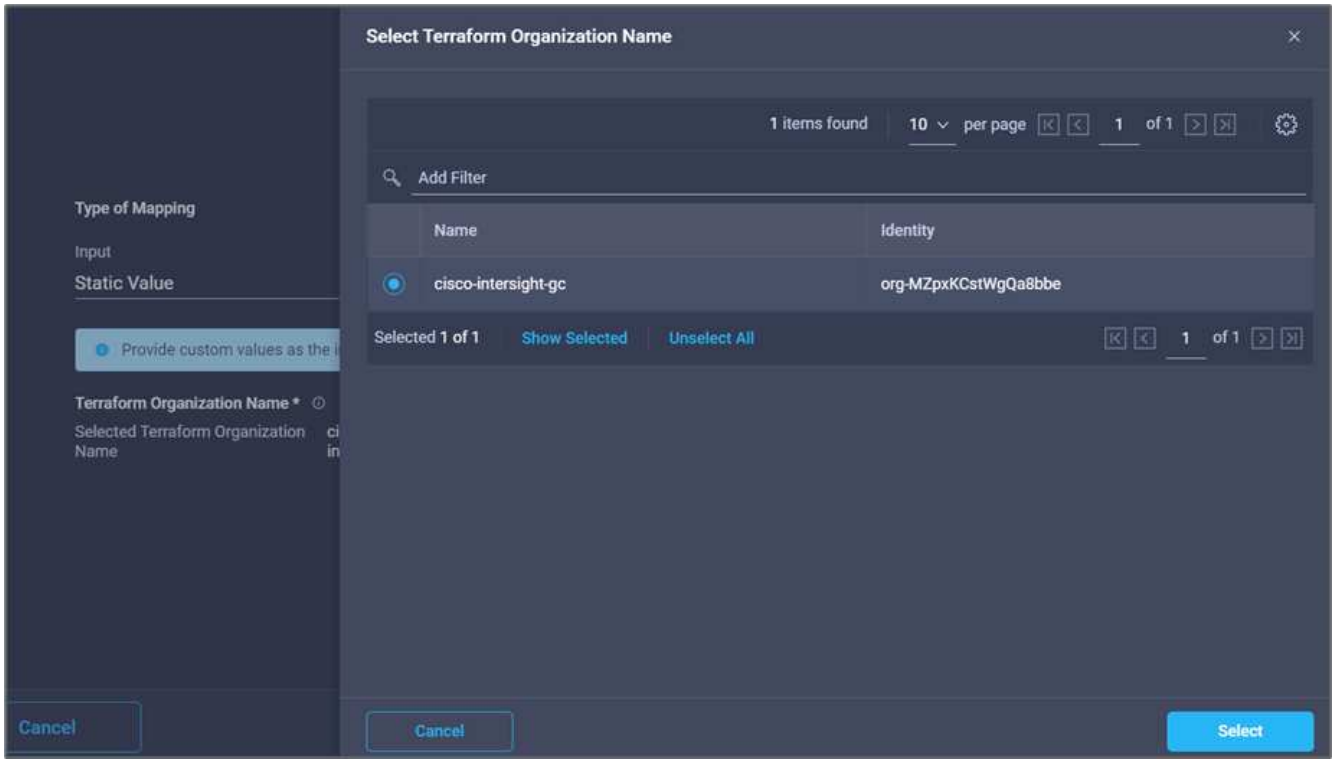
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. [デザイン]領域の[ツール]セクションから、[*Terraform Cloud]>[Add Terraform Workspace]タスクをドラッグアンドドロップします。
3. コネクターを使用して、*マップボリュームをデータストア*に接続し、*テラフォームワークスペースの追加*タスクを実行し、*保存*をクリックします。
4. [**Add Terraform Workspace]**をクリックします。**[**タスクのプロパティ**]**領域で、**[**一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。



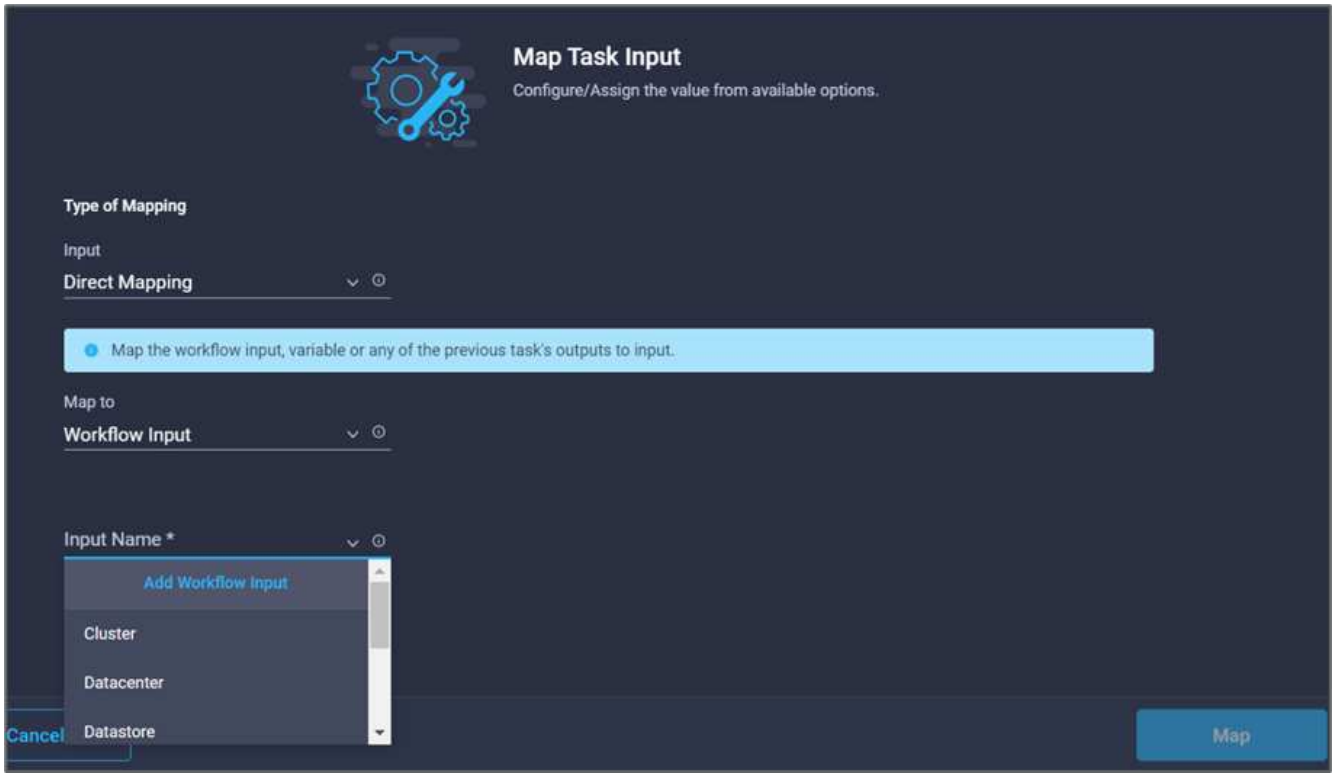
5. [タスクプロパティ]領域で、[入力]をクリックします。
6. 入力フィールド* Terraform Cloud Target で Map *をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。の説明に従って追加された、Terraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"。」。



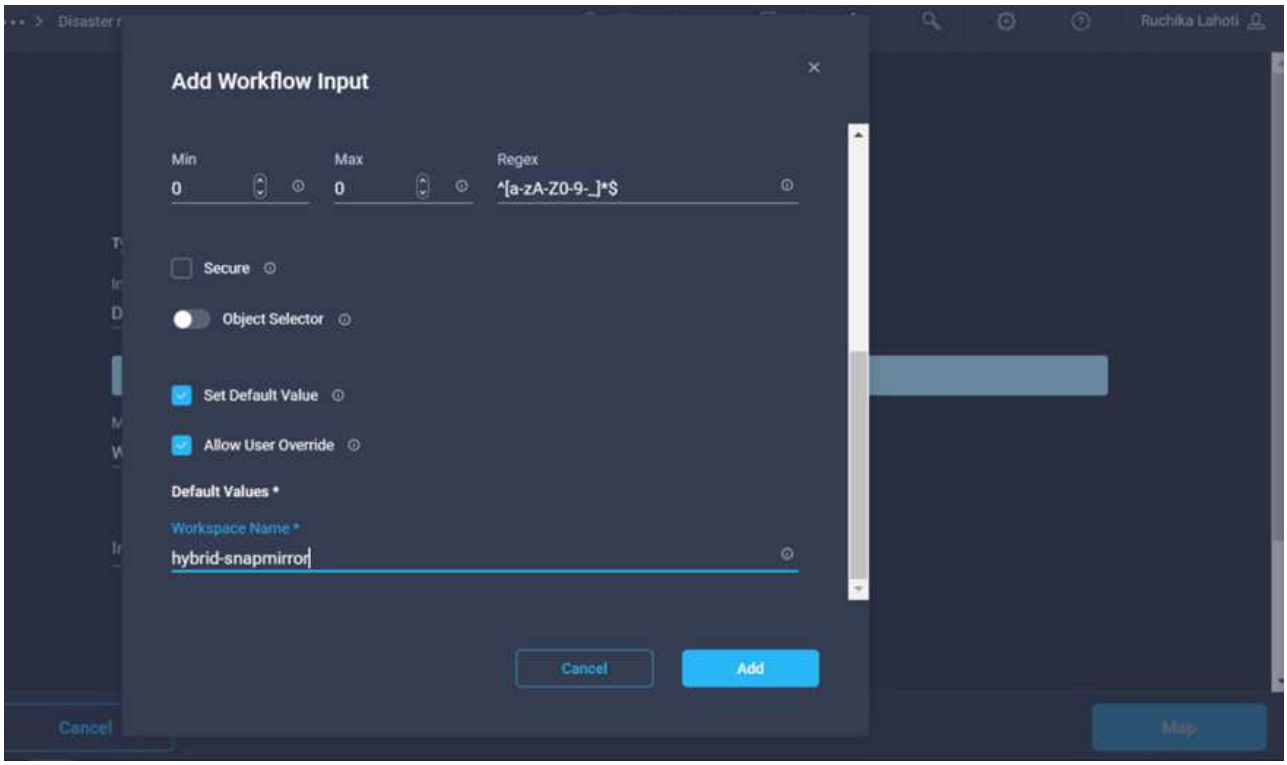
8. [マップ]をクリックします。
9. 入力フィールド*Terraform組織名*の*Map*をクリックします。
10. [静的値*]を選択し、[**Select Terraform Organization**]をクリックします。Terraform Cloud for Businessアカウントに含まれるTerraform Organizationの名前を選択します。



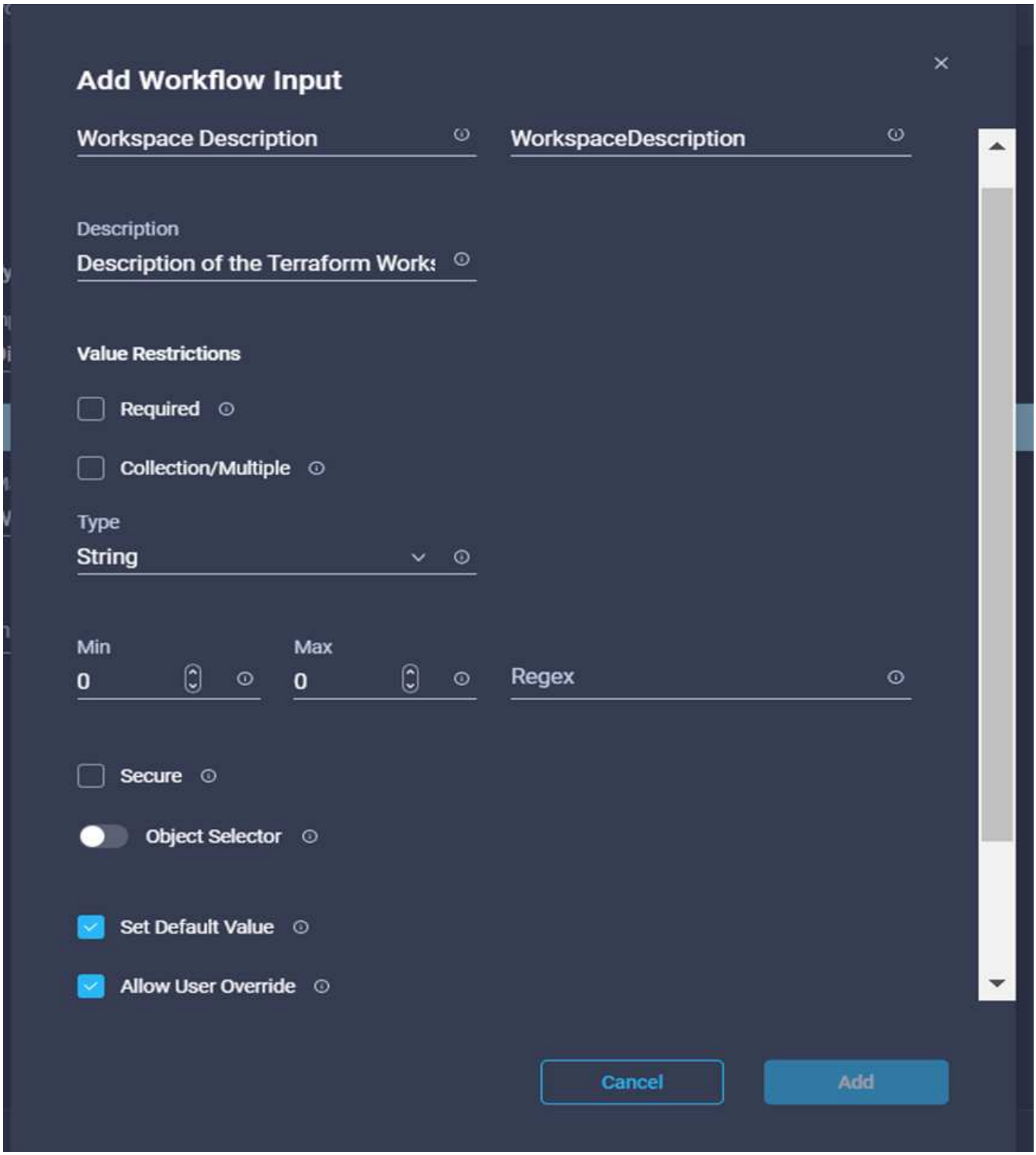
11. [マップ]をクリックします。
12. [**Terraform**ワークスペース名]フィールドの[**Map**]をクリックします。これは、Terraform Cloud for Businessアカウントの新しいワークスペースです。
13. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
14. [入力名]および[ワークフロー入力の作成]をクリックします。



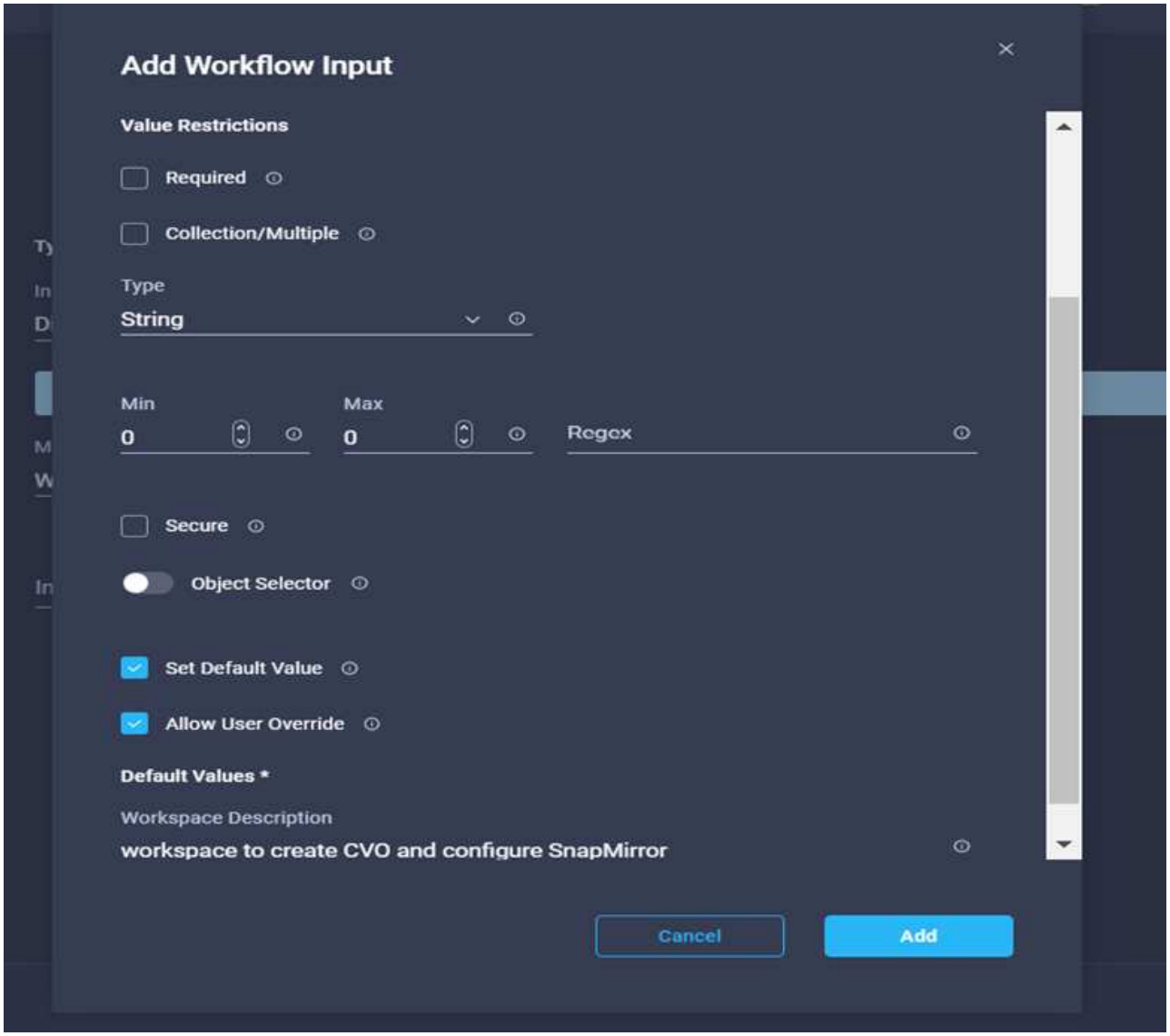
15. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [必須]をクリックします。
    c. [タイプ（* Type）]に[文字列（* String）]を選択してください。
    d. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    e. ワークスペースのデフォルト名を指定します。
    f. [追加（ Add ）] をクリックします。



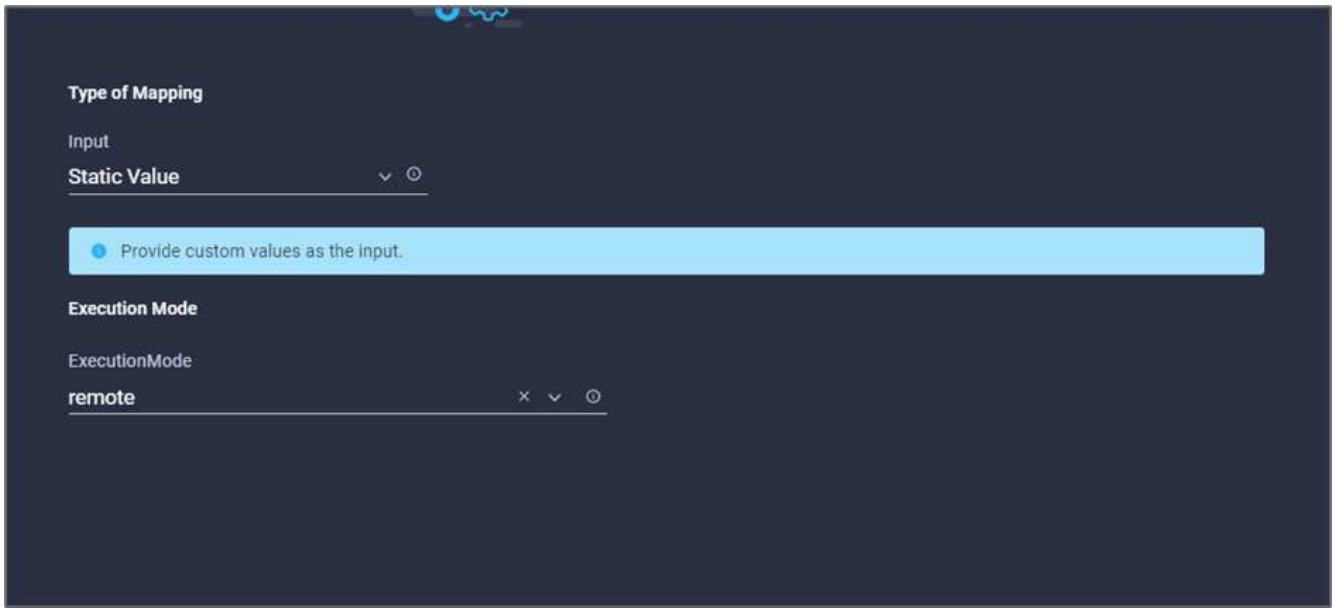
16. [マップ]をクリックします。
17. [* Workspace概要 （ワークスペースのマップ）]フィールドで[マップ]をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
19. [入力名]および[ワークフロー入力の作成]をクリックします。



20. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [タイプ（* Type）]に[文字列（* String）]を選択してください。
    c. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    d. ワークスペース概要 を提供し、*追加*をクリックします。



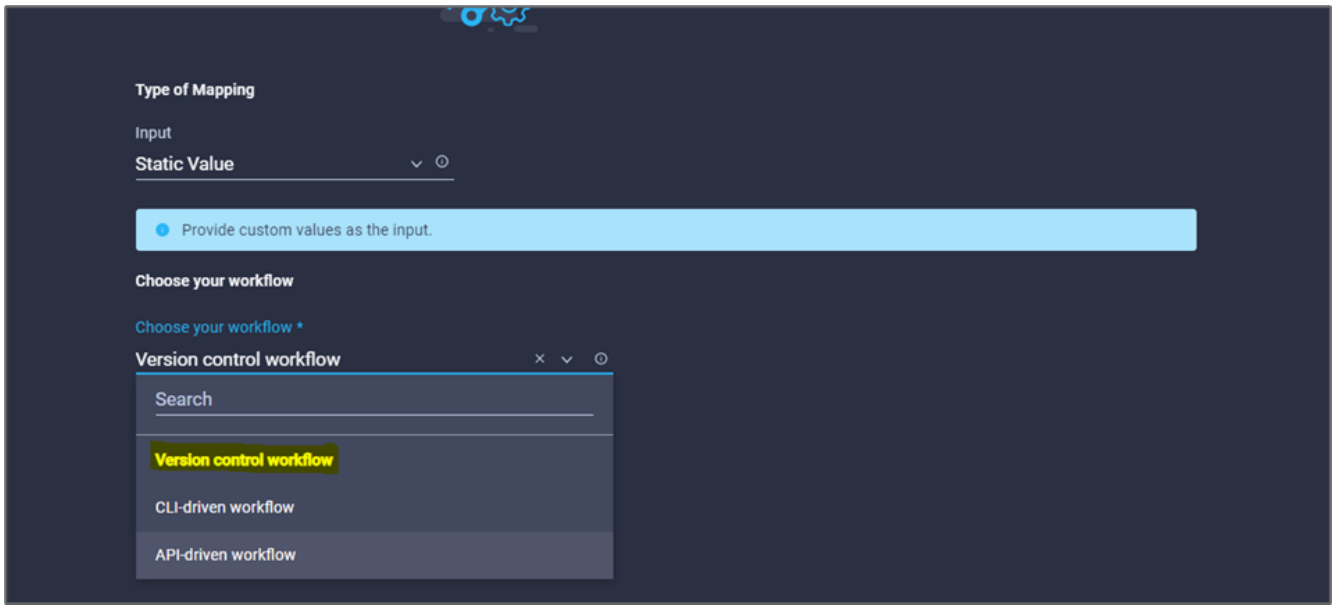
21. [マップ]をクリックします。
22. [実行モード*]フィールドの[マップ*]をクリックします。
23. *静的値*を選択し、*実行モード*をクリックして、*リモート*をクリックします。



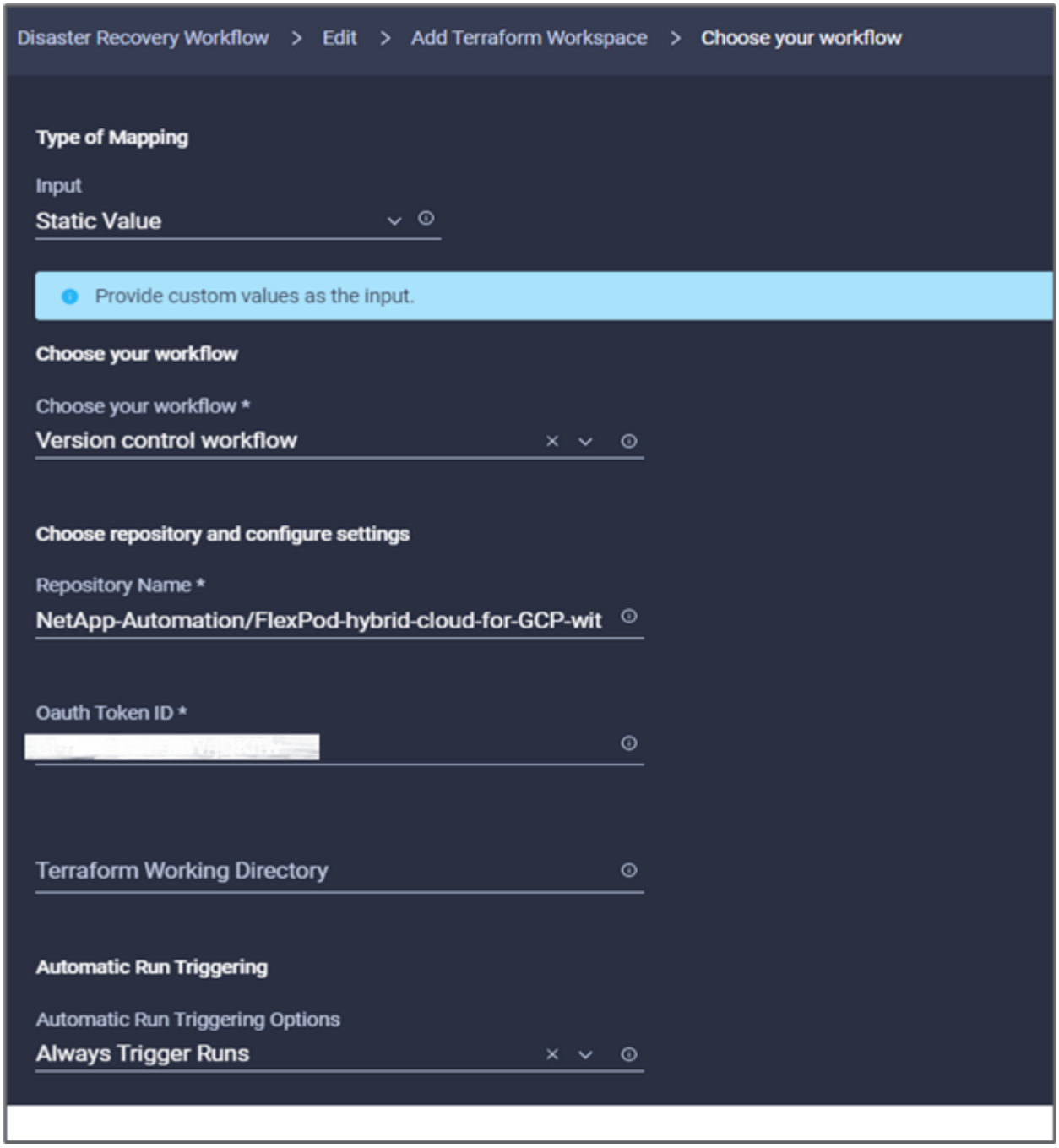
24. [マップ]をクリックします。
25. [メソッドの適用]フィールドで[マップ]をクリックします。
26. 「* Static Value 」を選択し、「 Apply Method *」をクリックします。*手動適用*をクリックします。

27. [マップ]をクリックします。
28. [ユーザーインタフェース]フィールドで[マップ]をクリックします。
29. 「* Static Value 」を選択し、「 User Interface 」をクリックします。**[***コンソール**UI**]をクリックします。

30. [マップ]をクリックします。
31. 入力フィールドで*マップ*をクリックし、ワークフローを選択します。
32. 「静的値」を選択し、「ワークフローの選択」をクリックします。[バージョン管理ワークフロー]をクリックします。



33. GitHubリポジトリについて、次の詳細情報を入力します。
    a. [リポジトリ名*]に'セクションで詳細に説明したリポジトリの名前を入力します "「環境の前提条件の設定」"。
    b. セクションの説明に従って、OAuthトークンIDを指定します "「環境の前提条件の設定」"。
    c. [自動実行トリガー（* Automatic Run Triggering）]オプションを選択します。



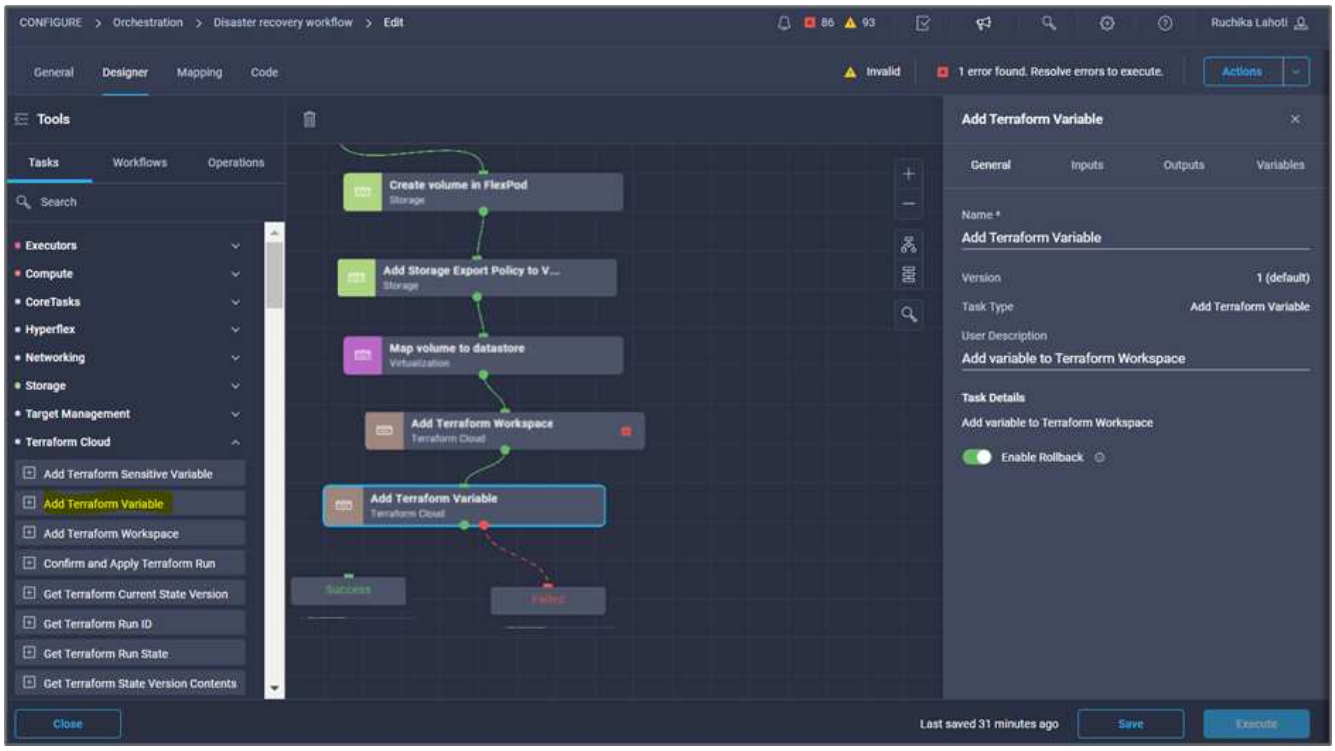
34. [マップ]をクリックします。
35. [保存（ Save ）] をクリックします。

これで、Terraform Cloud for Businessアカウントでワークスペースを作成するタスクは完了です。

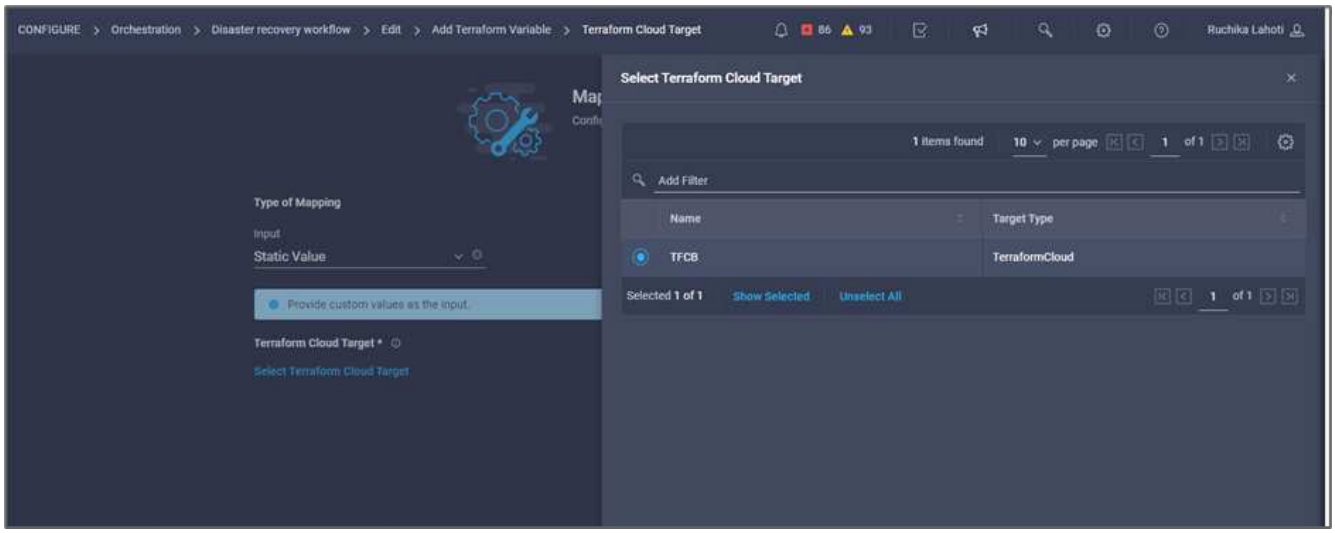
手順 **6**：ワークスペースに非機密変数を追加します

1. **[Designer]**タブに移動し、**[**ツールからのワークフロー]セクションをクリックします。
2. [**Design**]領域の[**Tools**]セクションから、[**Terraform]>[Add Terraform Variables**]ワークフローをドラッグアンドドロップします。
3. コネクターを使用して、*テラフォームワークスペースの追加*および*テラフォーム変数の追加*タスクを接続します。[保存（ Save ）] をクリックします。

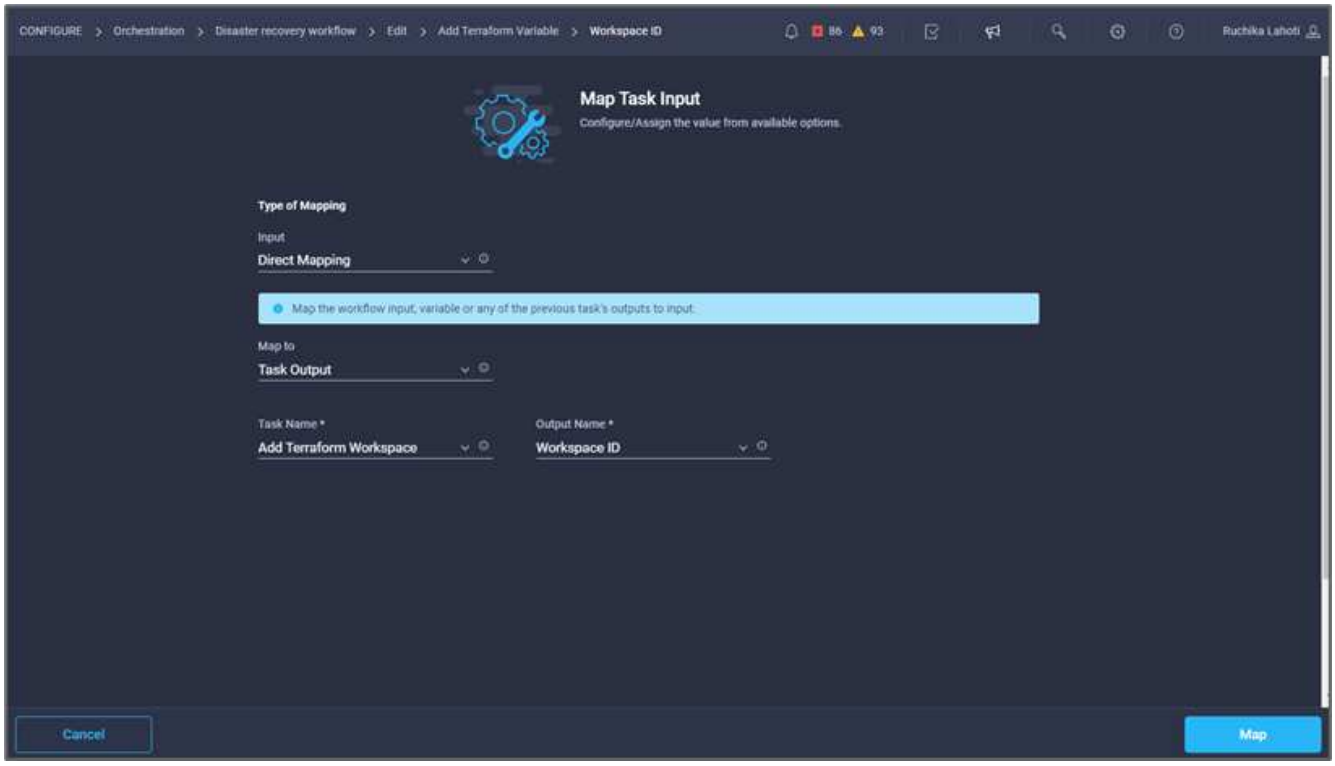
4. [**Add Terraform Variables**]をクリックします。[ワークフローのプロパティ*]領域で、[一般*]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。



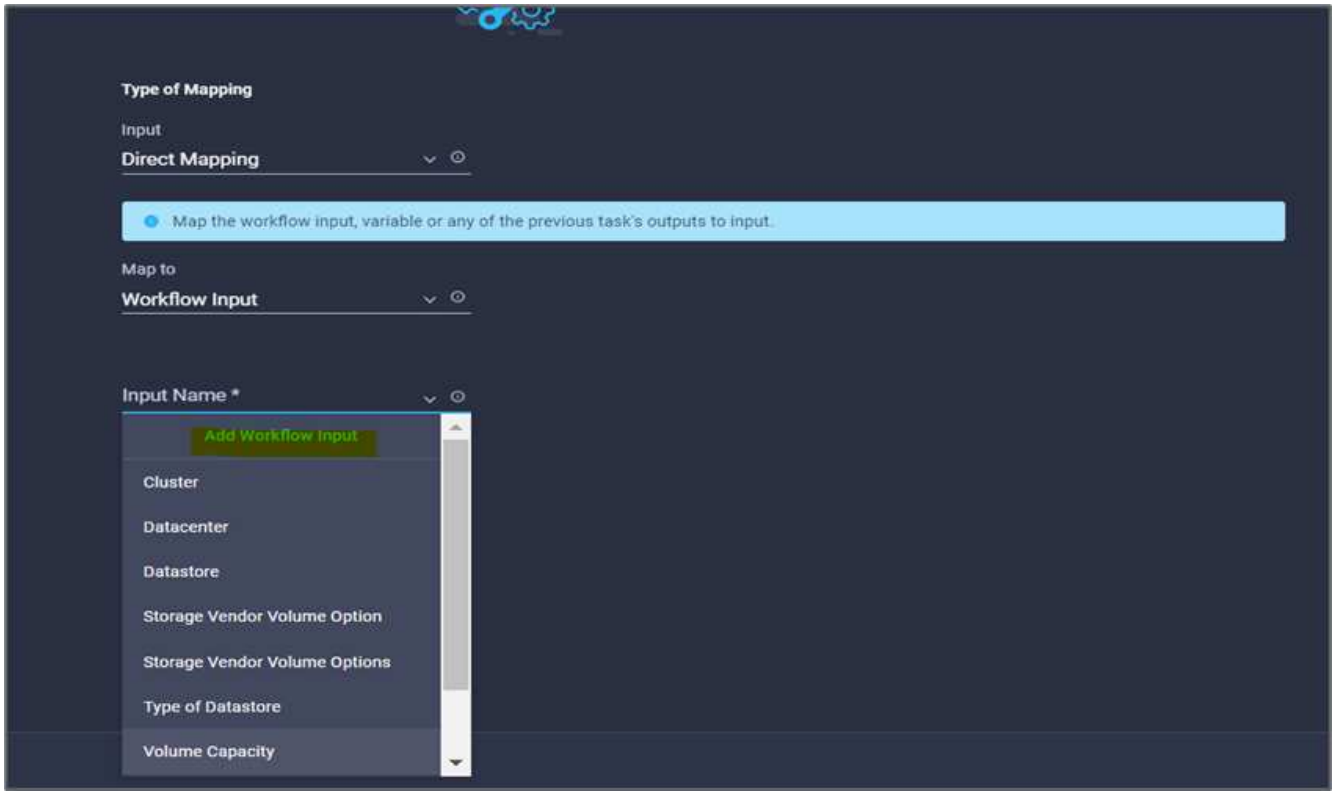
5. [ワークフロープロパティ]領域で、[入力]をクリックします。
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。の説明に従って追加された、Terraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"。」。



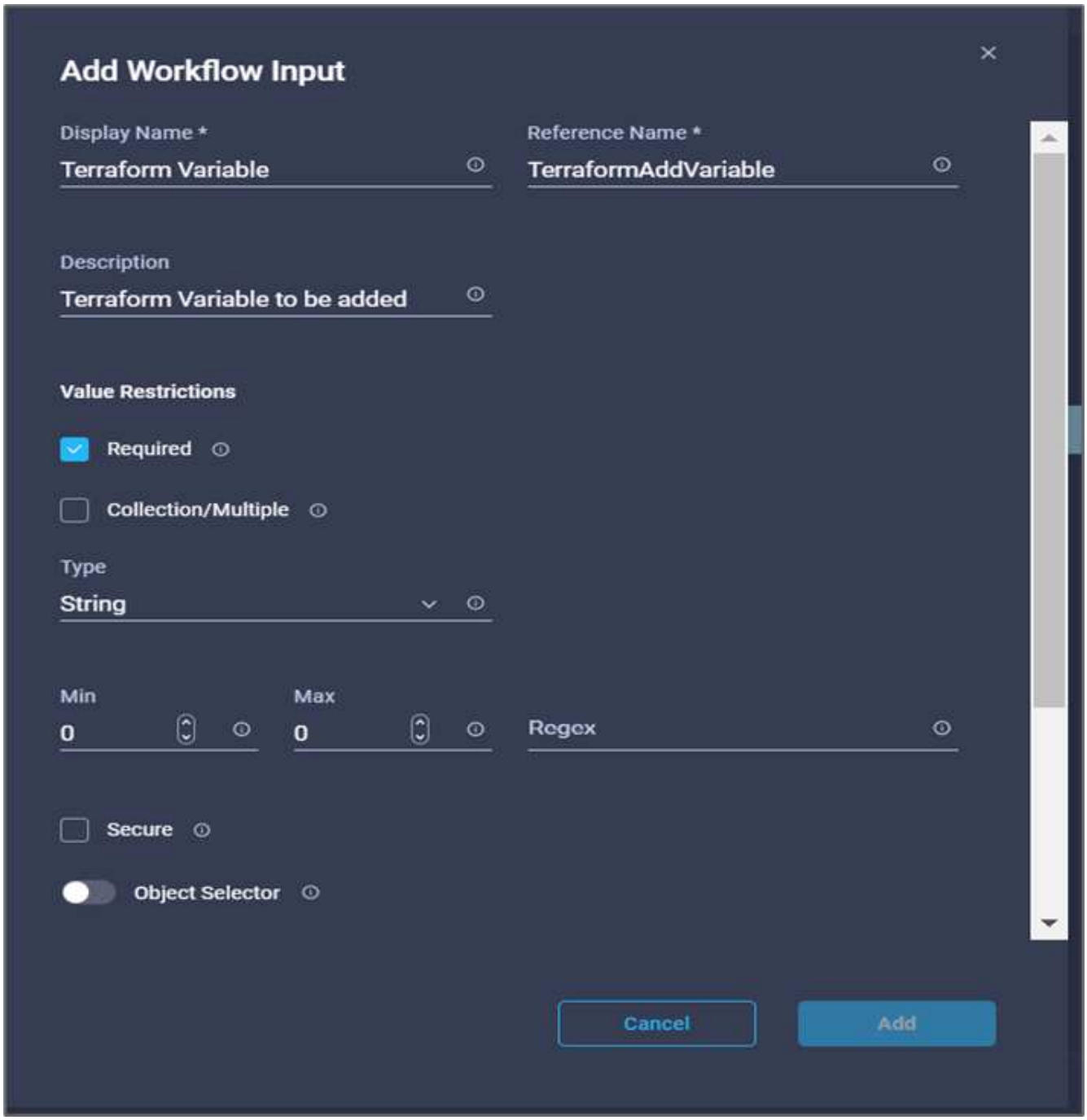
8. [マップ]をクリックします。
9. [**Terraform Organization Name**]フィールドの[**Map**]をクリックします。
10. 「静的値」を選択し、「テラフォームの組織を選択」をクリックします。Terraform Cloud for Businessアカウントに含まれるTerraform Organizationの名前を選択します。



11. [マップ]をクリックします。
12. [**Terraform**ワークスペース名]フィールドの[**Map**]をクリックします。
13. [直接マッピング]を選択し、[タスク出力]をクリックします。
14. タスク名*をクリックし、*テラフォームワークスペースの追加*をクリックします。



15. 出力名*をクリックし、*ワークスペース名*をクリックします。
16. [マップ]をクリックします。
17. [変数オプションの追加*]フィールドで[**Map**]をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
19. [入力名]および[ワークフロー入力の作成]をクリックします。

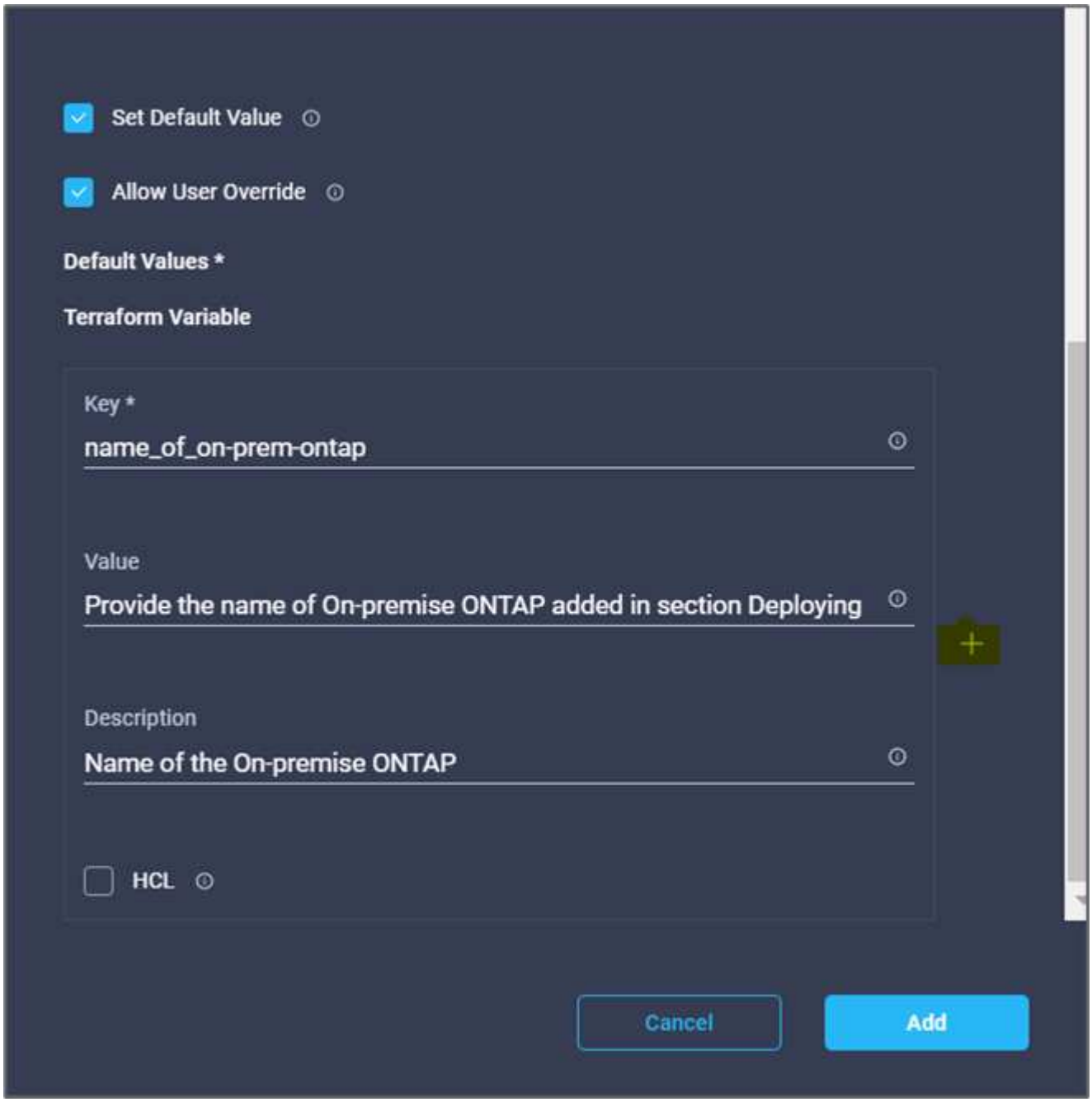


20. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [タイプ（* Type）]に[文字列（ String）]を選択してください。

c. [デフォルト値の設定]と[オーバーライド*]をクリックします。

d. 変数タイプ*をクリックし、*非機密変数*をクリックします。

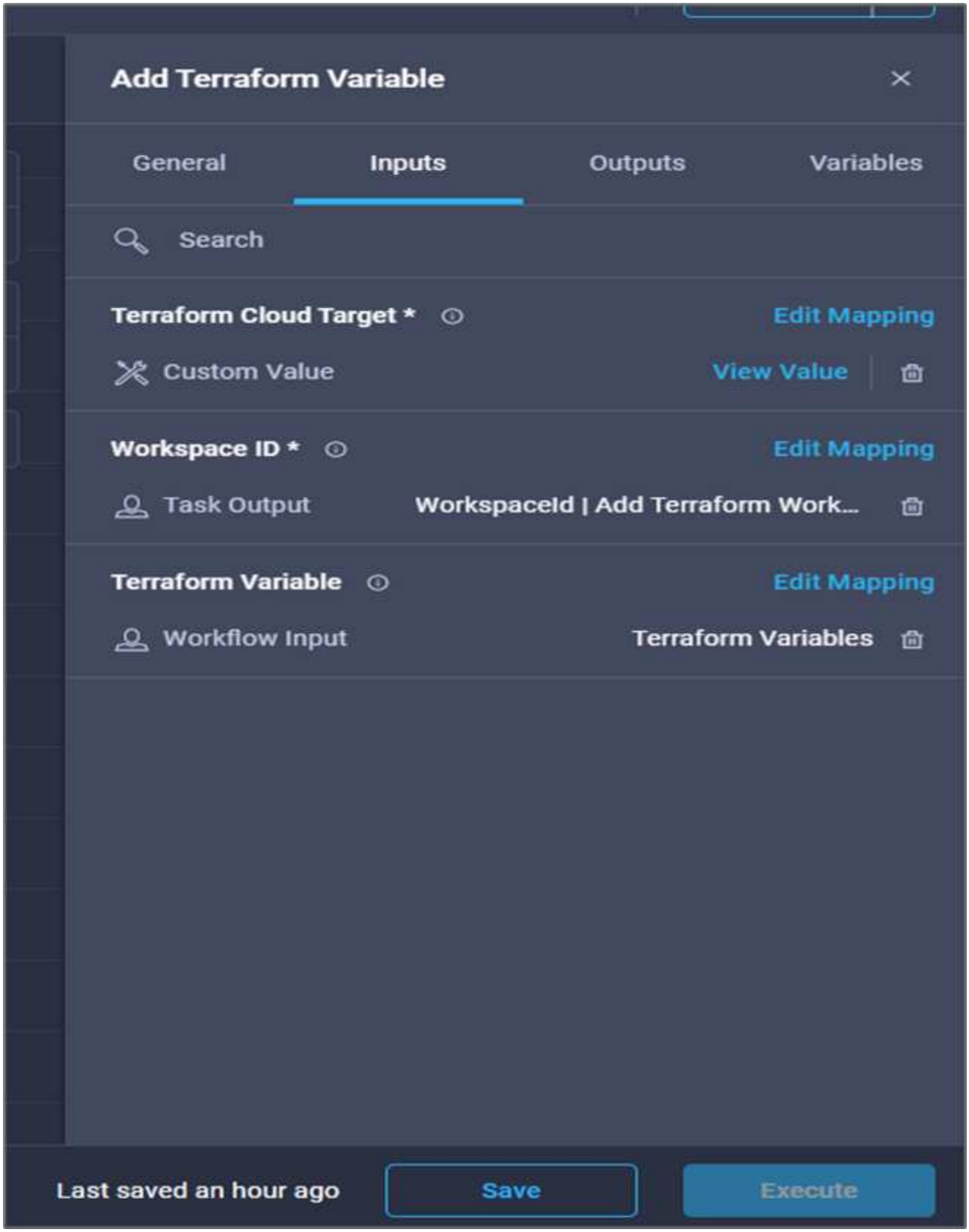
21. [**Add Terraform Variables**]セクションで、次の情報を入力します。
    - * Key.*'name_OF_OF_OLIプレ ミス-ONTAP'
    - *値。*オンプレミスONTAP の名前を指定します。
    - *概要 。*オンプレミスONTAP の名前。
22. 追加の変数を追加するには、*+*をクリックします。



23. 次の表に示すように、すべてのTerraform変数を追加します。デフォルト値を指定することもできます。

Terraform変数名	説明
名前オンプレミス- ONTAP	オンプレミスONTAP （FlexPod ）の名前
オンプレミス- ONTAP_cluster_IP	ストレージクラスタ管理インターフェイスのIPアドレスです
オンプレミス- ONTAP_user_name	ストレージクラスタの管理ユーザ名
ゾーン	作業環境を作成するGCPリージョン
subnet_idの値	作業環境を作成するGCPサブネットID
vPC_id	作業環境を作成するVPC ID
capacity_package_nameのようになりました	使用するライセンスのタイプ
source_volumeを指定します	ソースボリュームの名前
source_storage_vm_name	ソースSVMの名前
destination_volumeに指定します	Cloud Volumes ONTAP 上のボリュームの名前
レプリケーションのスケジュール	デフォルトは1時間です
name_OF_VOLUME _TO _CREATE _on_CVO	クラウドボリュームの名前
Workspace_idをクリックします	作業環境を作成するワークスペースID
project_idに割り当てられます	作業環境を作成するproject_id
名前_OF_CVO-cluster	Cloud Volumes ONTAP 作業環境の名前
GCP_SERVICE_ACCOUNT	Cloud Volumes ONTAP 作業環境のGCP_SERVICE_ACCOUNT

24. [マップ]、[保存]の順にクリックします。



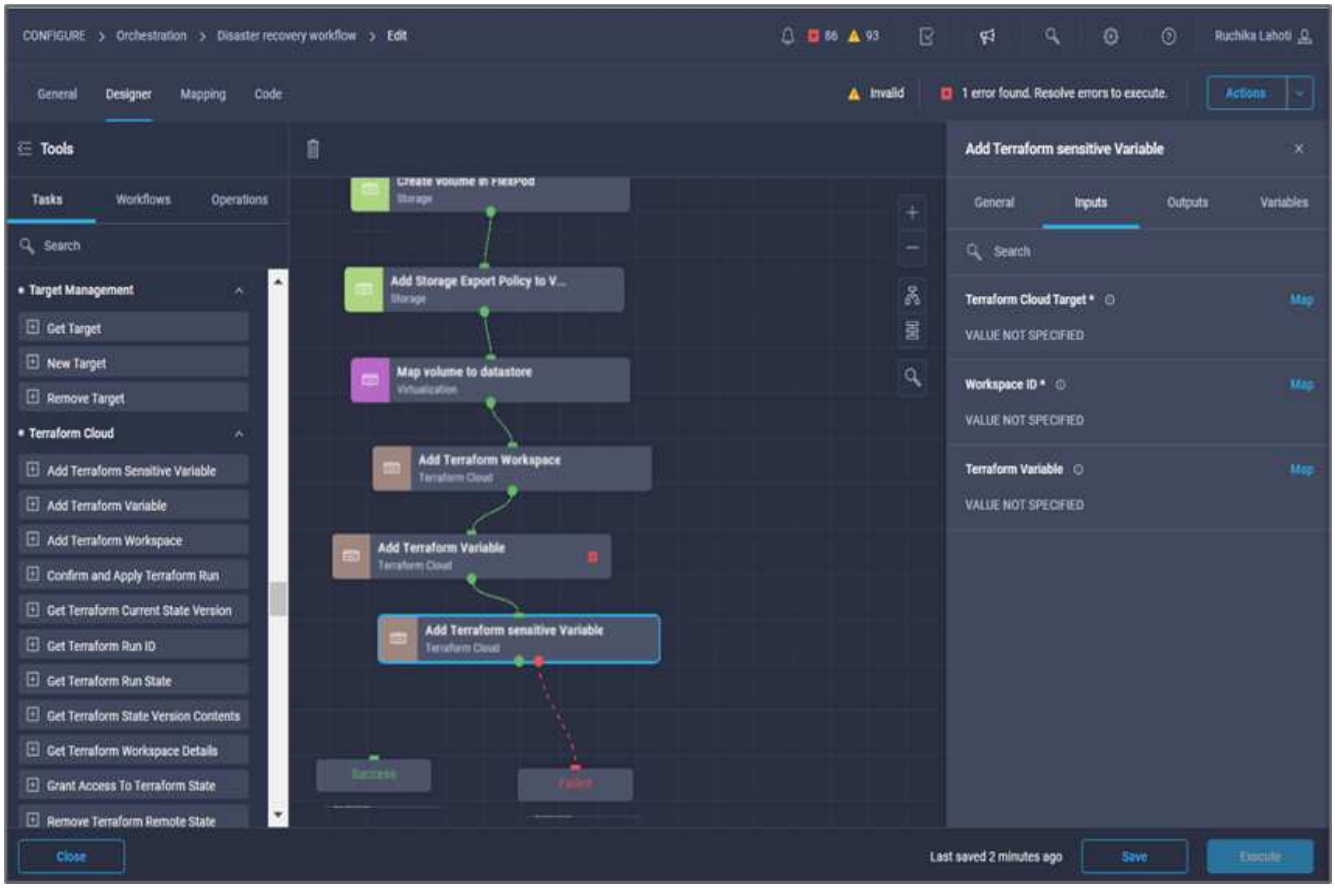
これで、必要なTerraform変数をワークスペースに追加する作業は完了です。次に、必要なセンシティブTerraform変数をワークスペースに追加します。両方を1つのタスクに組み合わせることもできます。

手順 **7:**ワークスペースに機密変数を追加します

1. [*Designer]タブに移動し、[*Tools]セクションから[*Workflows]をクリックします。
2. [**Design**]領域の[**Tools**]セクションから、[**Terraform]>[Add Terraform Variables**]ワークフローをドラッグアンドドロップします。
3. コネクターを使用して、2つの*テラフォームワークスペースの追加*タスクを接続します。[保存（ Save ）] をクリックします。

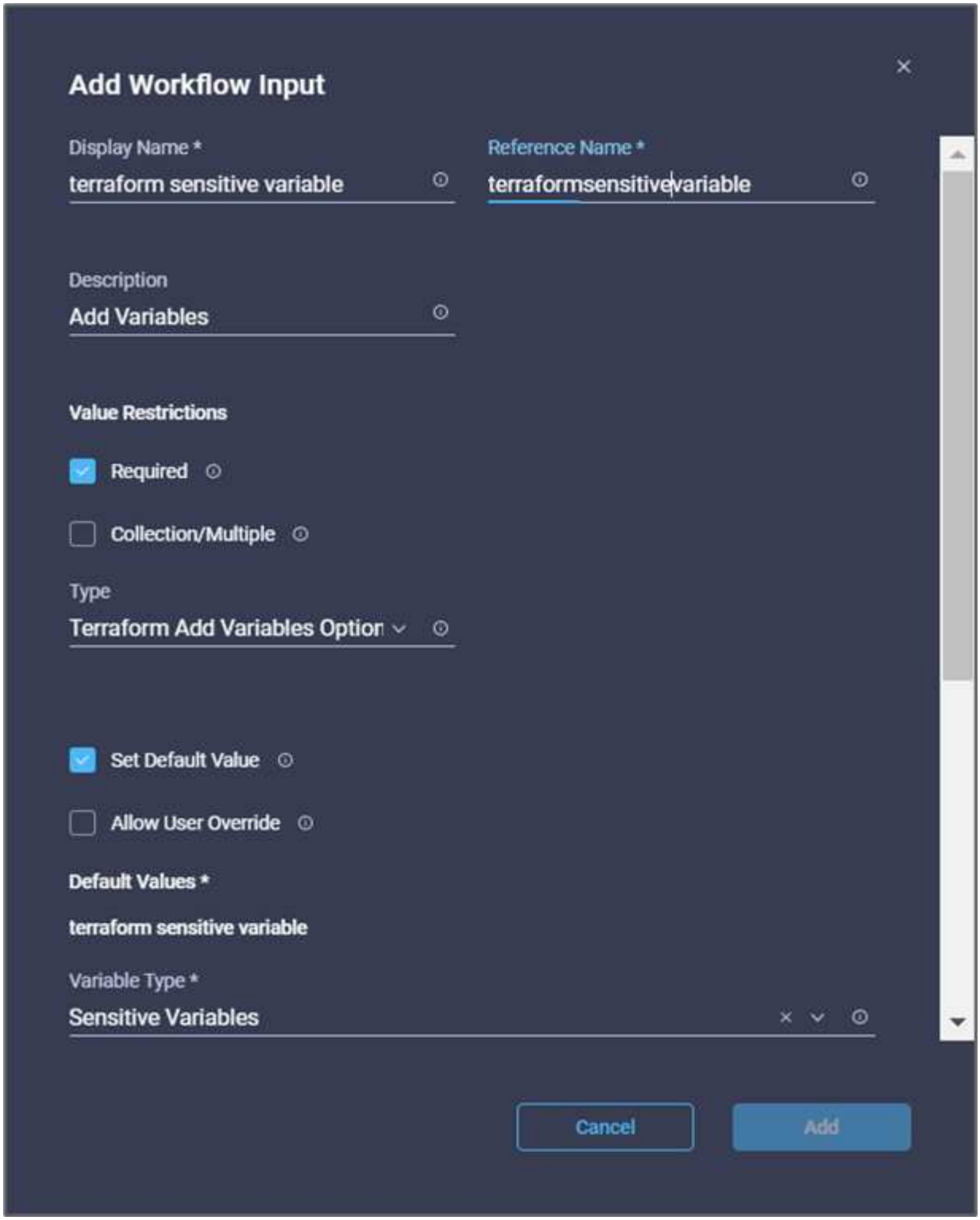
> 2つのタスクの名前が同じであることを示す警告が表示されます。次の手順でタスク名を変更したため、エラーは無視してください。

4. [**Add Terraform Variables**]をクリックします。[ワークフローのプロパティ*]領域で、[一般*]タブをクリックします。名前を*Add Terraform Sensitive Variables*に変更します。



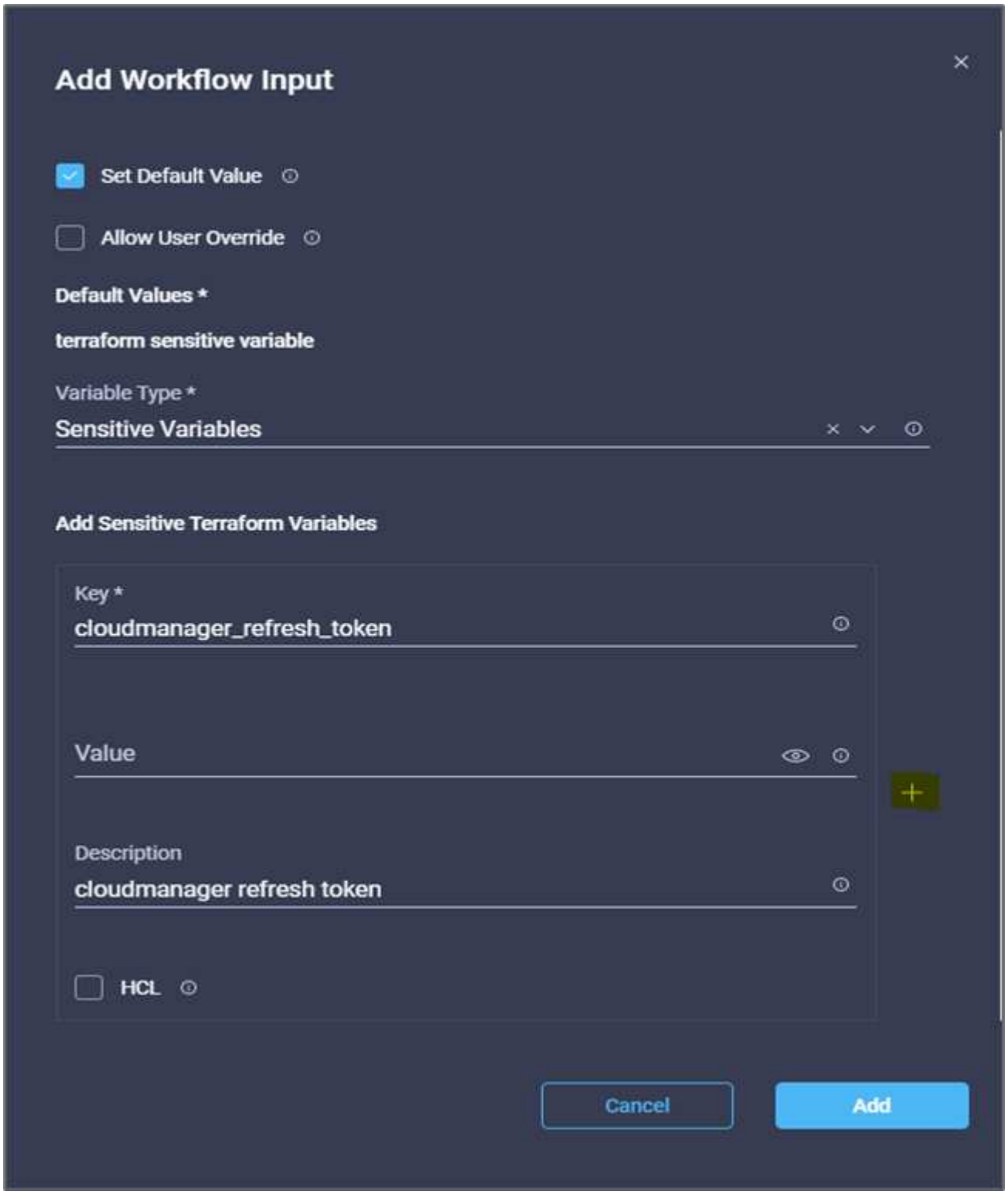
5. [ワークフロープロパティ]領域で、[入力]をクリックします。
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。セクションに追加されたTerraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"」
8. [マップ]をクリックします。
9. [**Terraform Organization Name**]フィールドの[**Map**]をクリックします。
10. 「静的値」を選択し、「テラフォームの組織を選択」をクリックします。Terraform Cloud for Businessアカウントに含まれるTerraform Organizationの名前を選択します。

11. [マップ]をクリックします。
12. [**Terraform**ワークスペース名]フィールドの[**Map**]をクリックします。
13. [直接マッピング]を選択し、[タスク出力]をクリックします。
14. [タスク名*]をクリックし、[**Add Terraform Workspace**]をクリックします。
15. 出力名*をクリックし、出力*ワークスペース名*をクリックします。
16. [マップ]をクリックします。
17. [変数オプションの追加*]フィールドで[**Map**]をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
19. [入力名]および[ワークフロー入力の作成]をクリックします。
20. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. タイプには必ず* Terraform「変数オプションを追加」*を選択してください。
    c. *デフォルト値の設定*をクリックします。
    d. [変数の種類*]をクリックし、[変数の影響を受ける変数]をクリックします。
    e. [追加（ Add ）] をクリックします。



21. [**Add Terraform Variables**]セクションで、次の情報を入力します。
    - * Key.*`cloudmanager_refresh_ctoken`.
    - 値。 NetApp Cloud Manager API処理の更新トークンを入力します。
    - *概要 。*リフレッシュトークン。

NetApp Cloud Manager API処理用の更新トークンの取得方法の詳細については、セクションを参照してください "「環境の前提条件を設定する」"



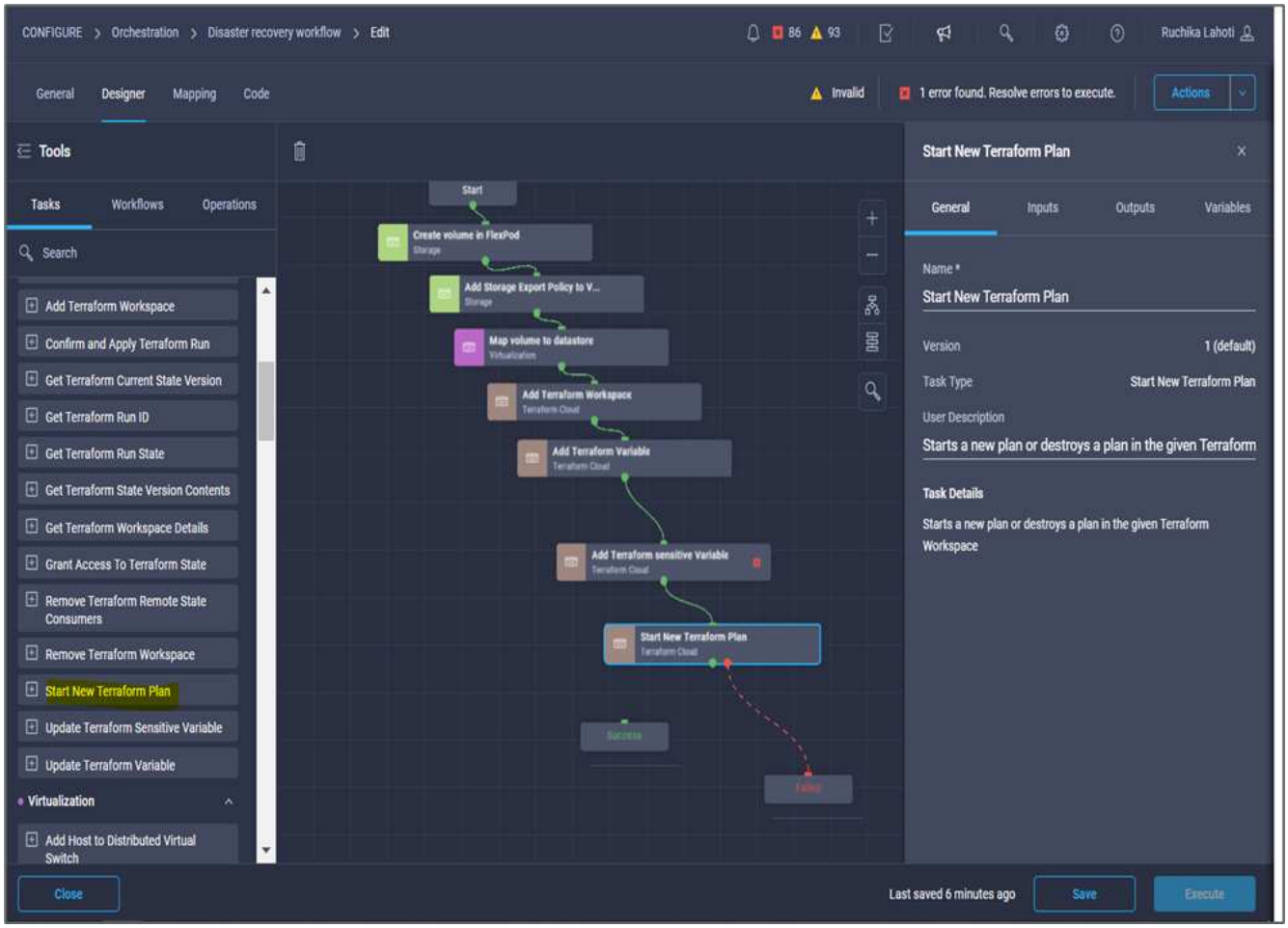
22. 次の表に示すように、すべてのTerraform機密変数を追加します。デフォルト値を指定することもできます。

Terraformの変数名	説明
cloudmanager_refresh_ctoken	トークンをリフレッシュします。次の場所から入手してください。
connector_id	Cloud Manager ConnectorのクライアントID。から入手します
CVO-admin_passwordのように入力します	Cloud Volumes ONTAP の管理パスワード
オンプレミス- ONTAP_user_password	ストレージクラスタの管理パスワード

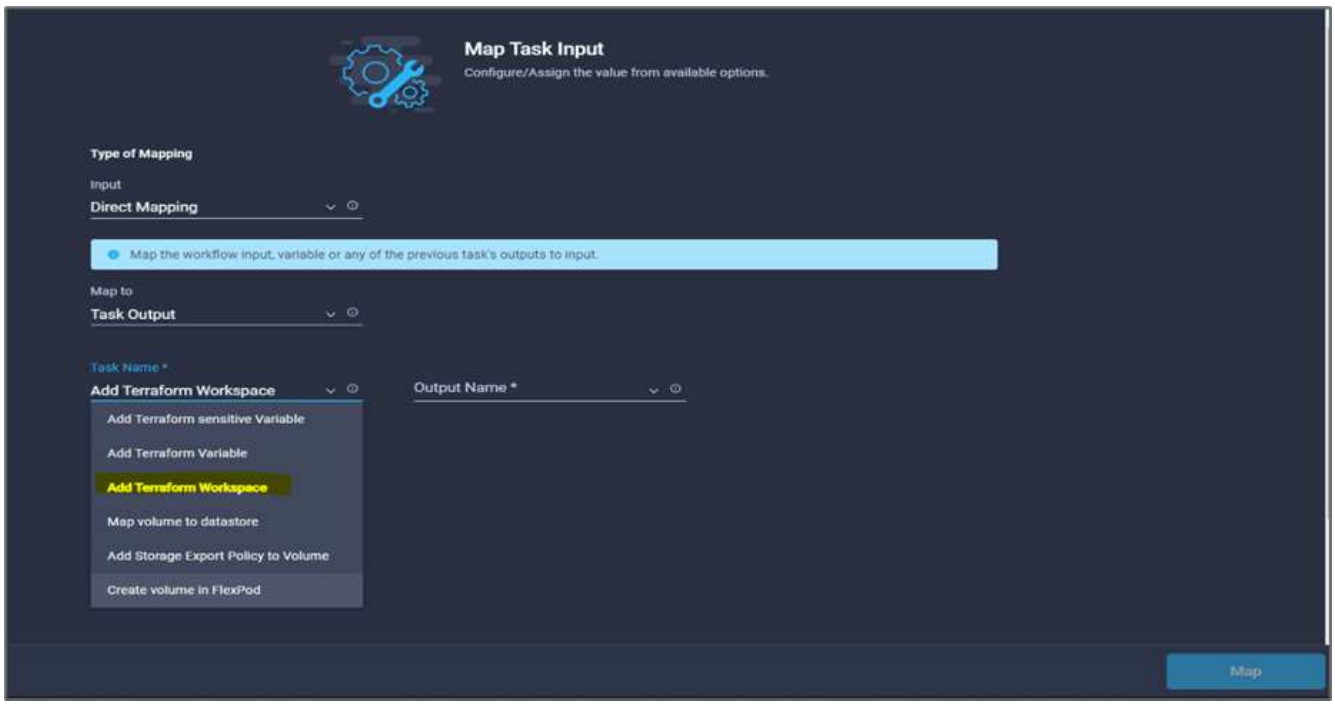
23. [**Map**]をクリックします。これで、必要なTerraformの機密変数をワークスペースに追加するタスクが完了します。次に、設定したワークスペースで新しいTerraformプランを開始します。

手順 **8:**新しい**Terraform**計画を開始します

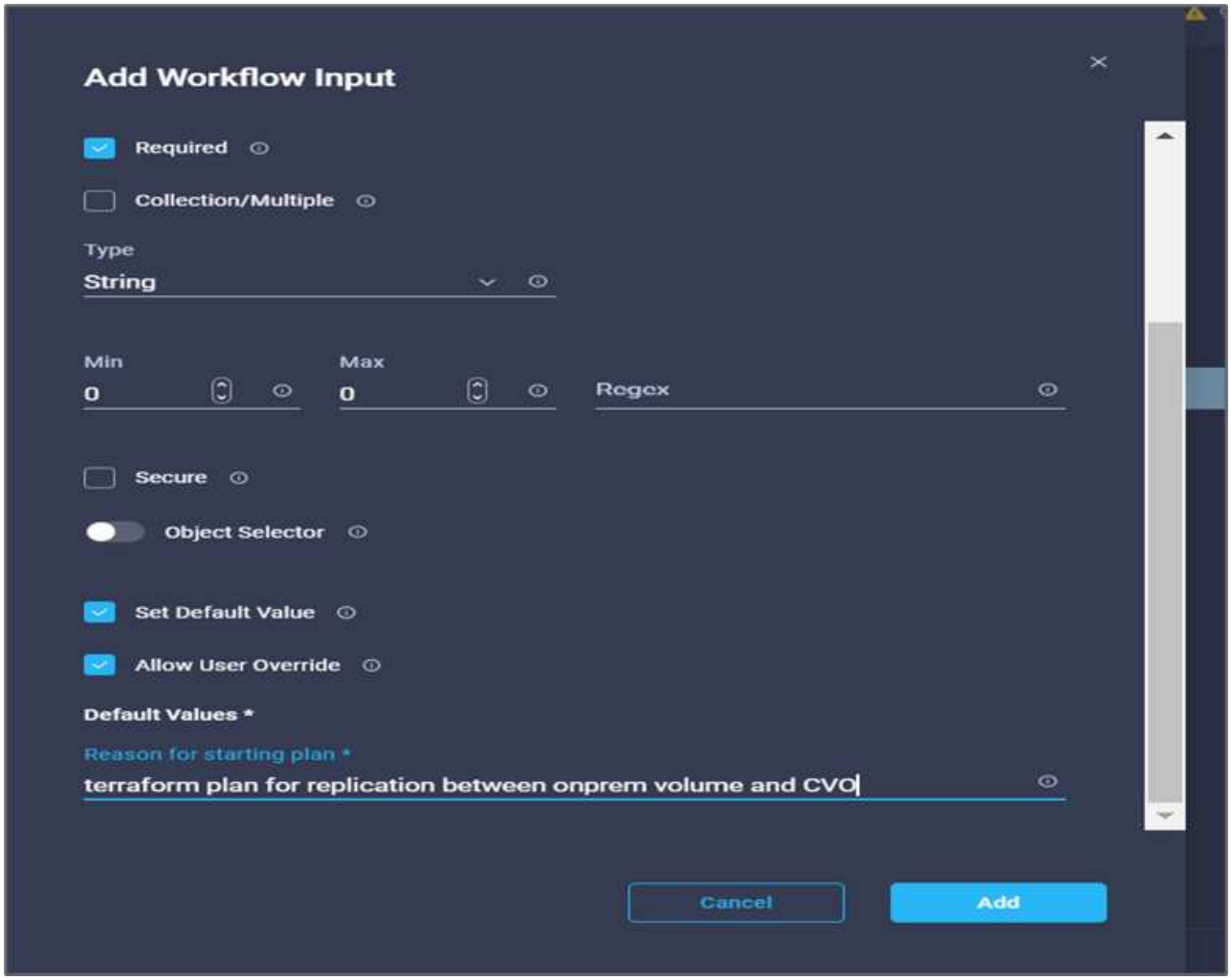
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. デザイン*領域の*ツール*セクションから*テラフォーム・クラウド>新規テラフォームプラン開始*タスクをドラッグ・アンド・ドロップします。
3. コネクターを使用して、タスク*テラフォームのセンシティブ変数の追加*と*新しいTerraformプランタスクの開始*を接続します。[保存（ Save ）] をクリックします。
4. [新しいTerraformプランを開始する*]をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。



5. [タスクプロパティ（Task Properties ）**]**領域で、**[***入力（Inputs *）]をクリックする
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。「Configuring Cisco Intersight Service for Corp’Terraform」の項に追加されたTerraform Cloud for Businessアカウントを選択します。
8. [マップ]をクリックします。
9. [ワークスペース**ID**]フィールドで[マップ]をクリックします。
10. [直接マッピング]を選択し、[タスク出力]をクリックします。
11. [タスク名*]をクリックし、[**Add Terraform Workspace**]をクリックします。



12. [出力名*]、[ワークスペース**ID**]、[マップ]の順にクリックします。
13. [開始計画の理由*]フィールドで[**Map**]をクリックします。
14. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
15. [入力名]、[ワークフロー入力の作成]の順にクリックします。
16. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [タイプ（* Type）]に[文字列（ String）]を選択してください。
    c. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    d. 開始計画の理由*のデフォルト値を入力し、*追加*をクリックします。



17. [マップ]をクリックします。
18. [計画操作]フィールドで[マップ]をクリックします。
19. 「静的値」を選択し、「計画操作」をクリックします。[新しい計画*]をクリックします。

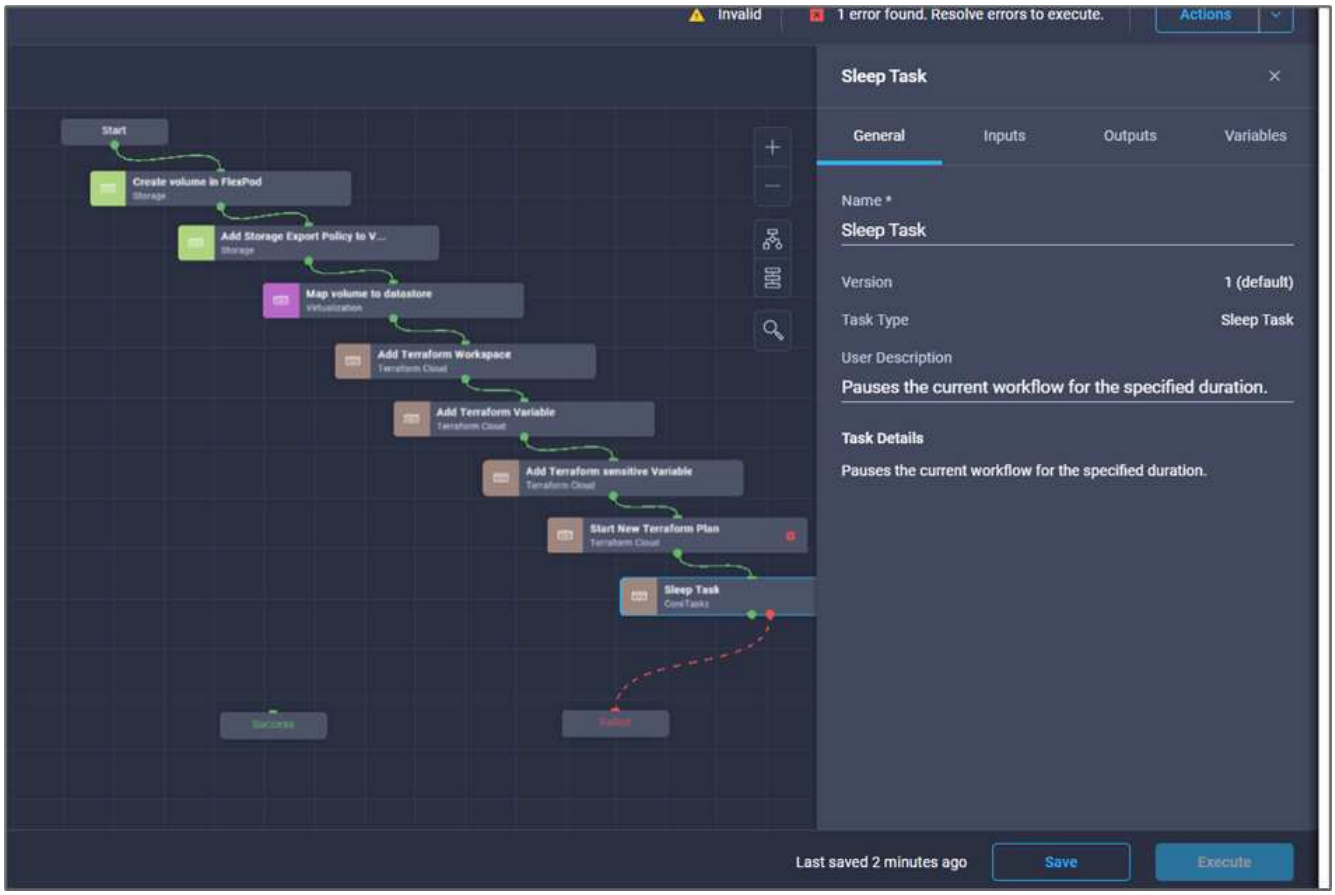
20. [マップ]をクリックします。
21. [保存（ Save ）] をクリックします。

これで、Terraform Cloud for BusinessアカウントにTerraformプランを追加する作業は完了です。次に、スリープタスクを数秒間作成します。

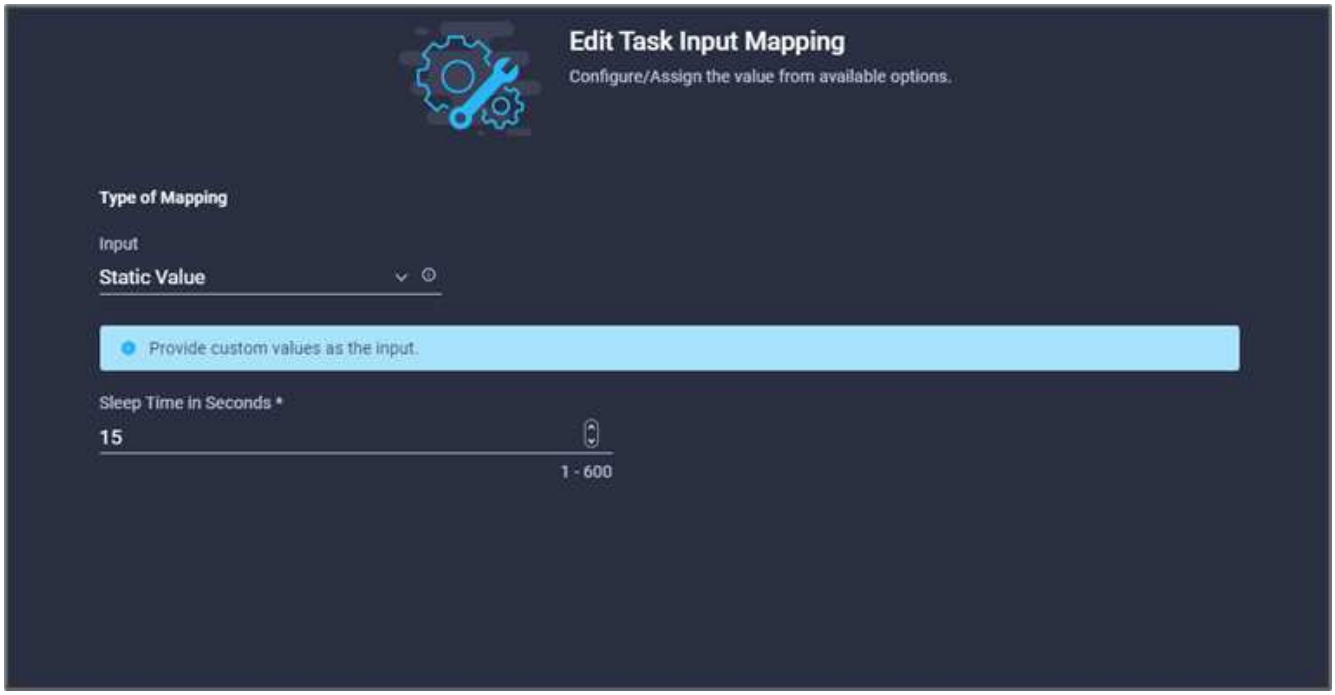
手順 **9**：同期のためのスリープタスク

Terraform ApplyにはRunIDが必要です。RunIDはTerraform Planタスクの一部として生成されます。Terraform PlanとTerraform Applyアクションの間に数秒待機することで、タイミングの問題を回避できます。

1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. デザイン*領域の*ツール*セクションから*コアタスク>スリープ・タスク*をドラッグ・アンド・ドロップします。
3. コネクターを使用して、タスク*新しいTerraformプランの開始*と*スリープタスク*を接続します。[保存（ Save ）] をクリックします。



4. スリープタスク*をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前は* Synchronize *です。
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. スリープ時間（秒）*フィールドで*マップ*をクリックします。
7. スリープ時間（秒）*に*静的値*と入力 15 *を選択します。

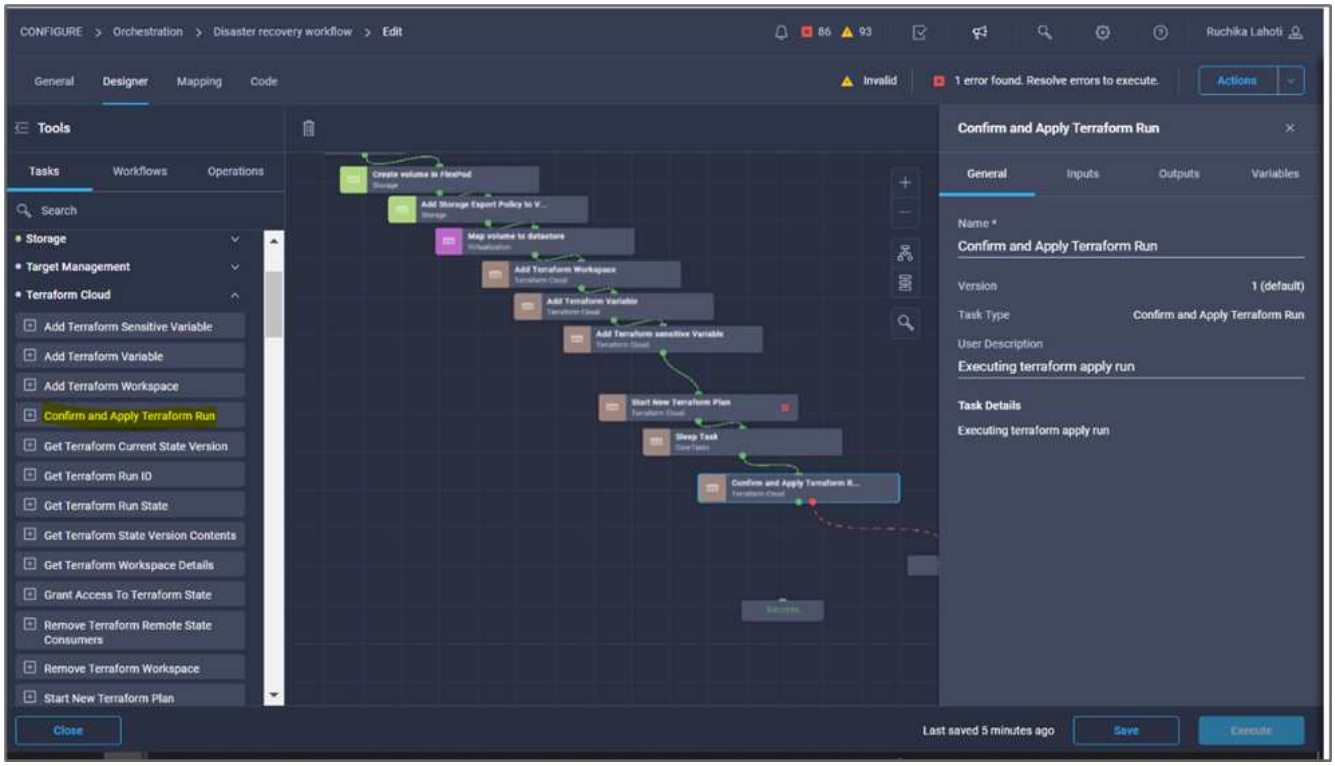


8. [マップ]をクリックします。
9. [保存（ Save ）] をクリックします。

これでスリープタスクは完了です。次に、このワークフローの最後のタスクを作成し、Terraform Runを確認して適用します。

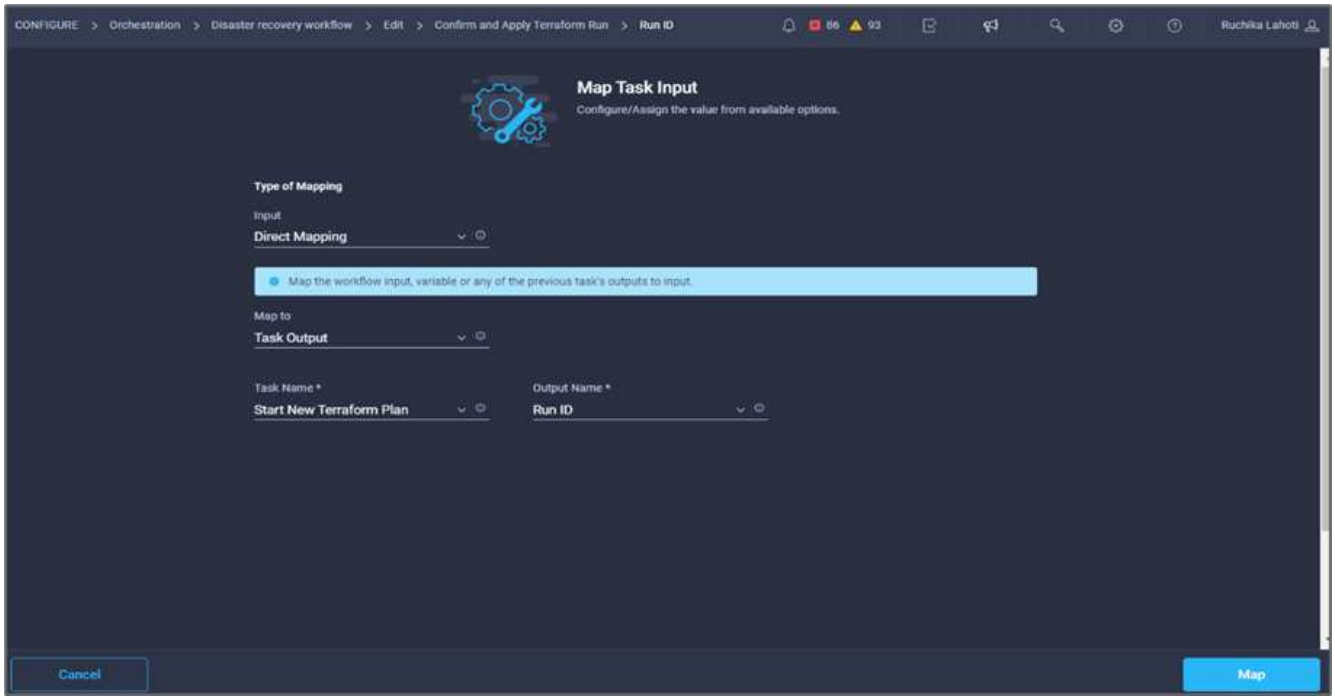
手順 **10: Terraform Run**を確認して適用します

1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. [**Design**]領域の[**Tools**]セクションから**[*Terraform Cloud]>[Confirm and Apply Terraform Run**]タスクをドラッグアンドドロップします。
3. コネクターを使用して、タスク*同期化*および*確認とテラフォーム実行の適用*を接続します。[保存（ Save ）] をクリックします。
4. [確認]と[* Terraform実行の適用*]をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。

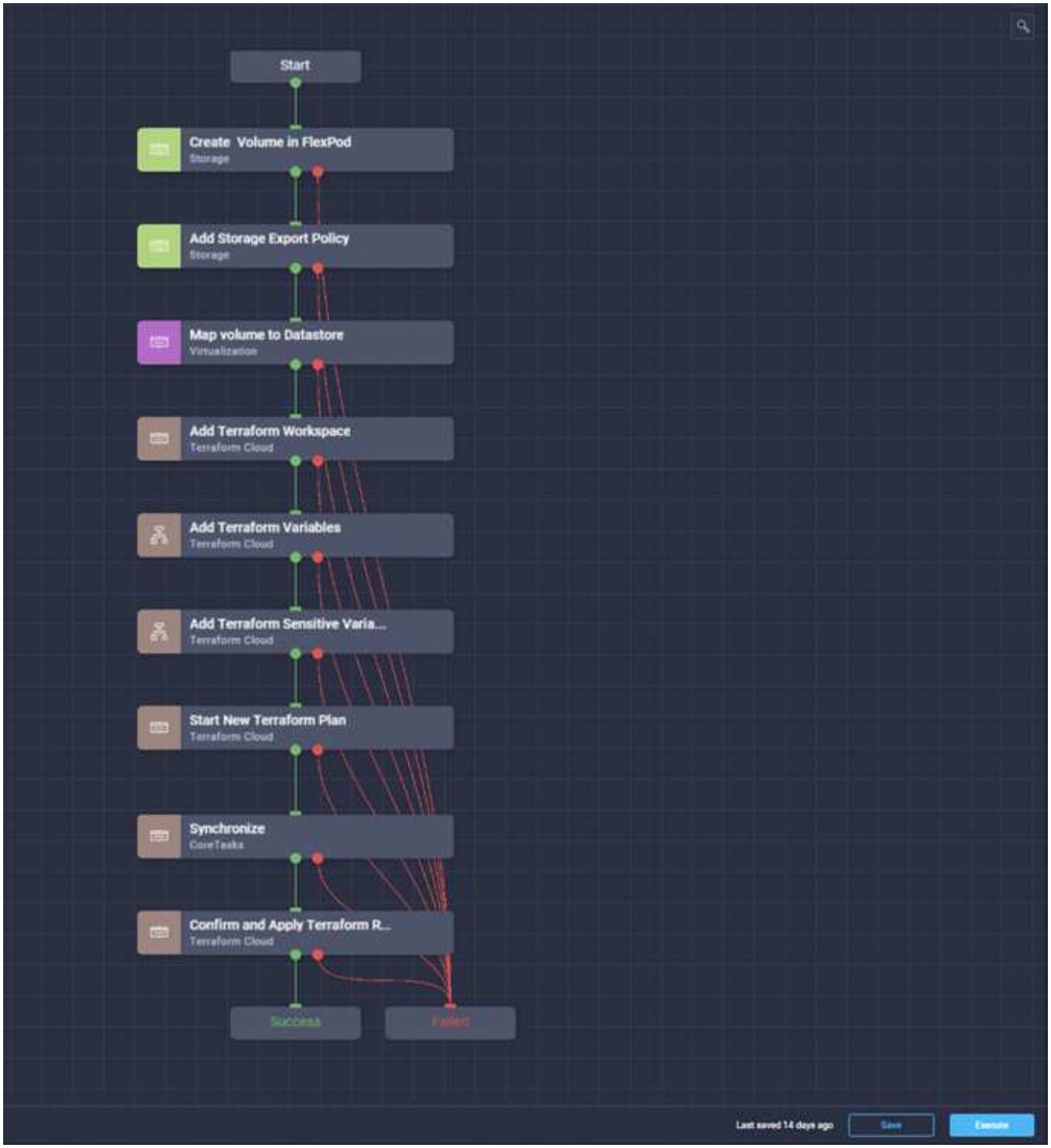


5. [タスクプロパティ（Task Properties ）**]**領域で、**[***入力（Inputs *）]をクリックする
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。で追加したTerraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"」
8. [マップ]をクリックします。
9. [ファイル名を指定して実行ID **]**フィールドの**[*Map**]をクリックします。
10. [直接マッピング]を選択し、[タスク出力]をクリックします。
11. [タスク名*]をクリックし、[新しいTerraformプランの開始*]をクリックします。

12. [出力名*]をクリックし、[**Run ID**]をクリックします。



13. [マップ]をクリックします。
14. [保存（ Save ）] をクリックします。
15. すべてのタスクが整列されるように、*ワークフローの自動整列*をクリックします。[保存（ Save ）] をクリックします。



これで、確認と実行の適用タスクは完了です。コネクターを使用して、**Confirm**タスクと**Apply Terraform Run***タスクと***Success**/*Failed*タスクを接続します。

手順 **11**：シスコが構築したワークフローをインポートします

Cisco Intersight Cloud Orchestratorを使用すると、ワークフローをCisco Intersightアカウントからシステムにエクスポートし、別のアカウントにインポートできます。JSONファイルは、アカウントにインポート可能なビルドワークフローをエクスポートすることで作成されました。

ワークフローコンポーネントのJSONファイルは、で確認できます "GitHub リポジトリ"。

"次の例は、コントローラからのTerraformの実行です。"

コントローラからの**Terraform**の実行

"前の手順：DRワークフロー"

コントローラを使用してTerraformプランを実行できます。ICOワークフローを使用してTerraformプランをすでに実行している場合は、このセクションを省略できます。

前提条件

解決策 のセットアップは、まずインターネットにアクセスできる管理ワークステーションと、Terraformの実際のインストールから始まります。

Terraformをインストールするためのガイドがあります "こちらをご覧ください"。

クローン**GitHub**リポジトリをリポジトリします

このプロセスの最初のステップでは、GitHubリポジトリを管理ワークステーションの新しい空のフォルダにクローニングします。GitHubリポジトリのクローンを作成するには、次の手順を実行します。

1. 管理ワークステーションから、プロジェクトの新しいフォルダを作成します。このフォルダ内に'/root/snapmirror-CVO'という名前の新しいフォルダを作成し'GitHubリポジトリをクローンします
2. 管理ワークステーションでコマンドラインインターフェイスまたはコンソールインターフェイスを開き、作成した新しいフォルダにディレクトリを変更します。
3. 次のコマンドを使用してGitHubコレクションをクローニングします。

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. ディレクトリを「snapmirror-CVO'」という新しいフォルダに変更します。
    - Terraformの実行*

- * Init.*(local) Terraform環境を初期化します。通常、1回のセッションで1回のみ実行されます。
- *計画。*テラフォームの状態をクラウドの現状と比較し、実行計画を作成して表示します。これによって導入環境が変更されることはありません（読み取り専用）。
- *適用。*計画フェーズから計画を適用します。これにより、導入環境（読み取りと書き込み）が変更される可能性があります。
- *破棄。*この特定のテラフォーム環境によって管理されるすべてのリソース。

詳細については、を参照してください "こちらをご覧ください"。

"次の例は、解決策の検証です。"

解決策の検証

"前のバージョン：コントローラからのTerraformの実行。"

このセクションでは、サンプルのデータレプリケーションワークフローを使用して解決策 を再確認し、測定値をいくつか確認して、FlexPod で実行されているNetApp ONTAP インスタンスからGoogle Cloudで実行されているNetApp Cloud Volumes ONTAP へのデータレプリケーションの整合性を検証します。

この解決策 では、Cisco Intersightワークフローオーケストレーションツールを使用しており、今回のユースケースで引き続き使用します。

特に、この解決策 で使用される限定的なCisco Intersightのワークフローは、Cisco Intersightに含まれるすべてのワークフローを表しているわけではありません。独自の要件に基づいてカスタムワークフローを作成し、Cisco Intersightからトリガーされるようにすることができます。

DRシナリオが成功するかどうかを検証するために、最初にSnapMirrorを使用して、FlexPod に含まれるONTAP のボリュームからCloud Volumes ONTAP にデータを移動します。その後、Googleクラウドコンピューティングインスタンスからデータにアクセスし、データ整合性チェックを実行できます。

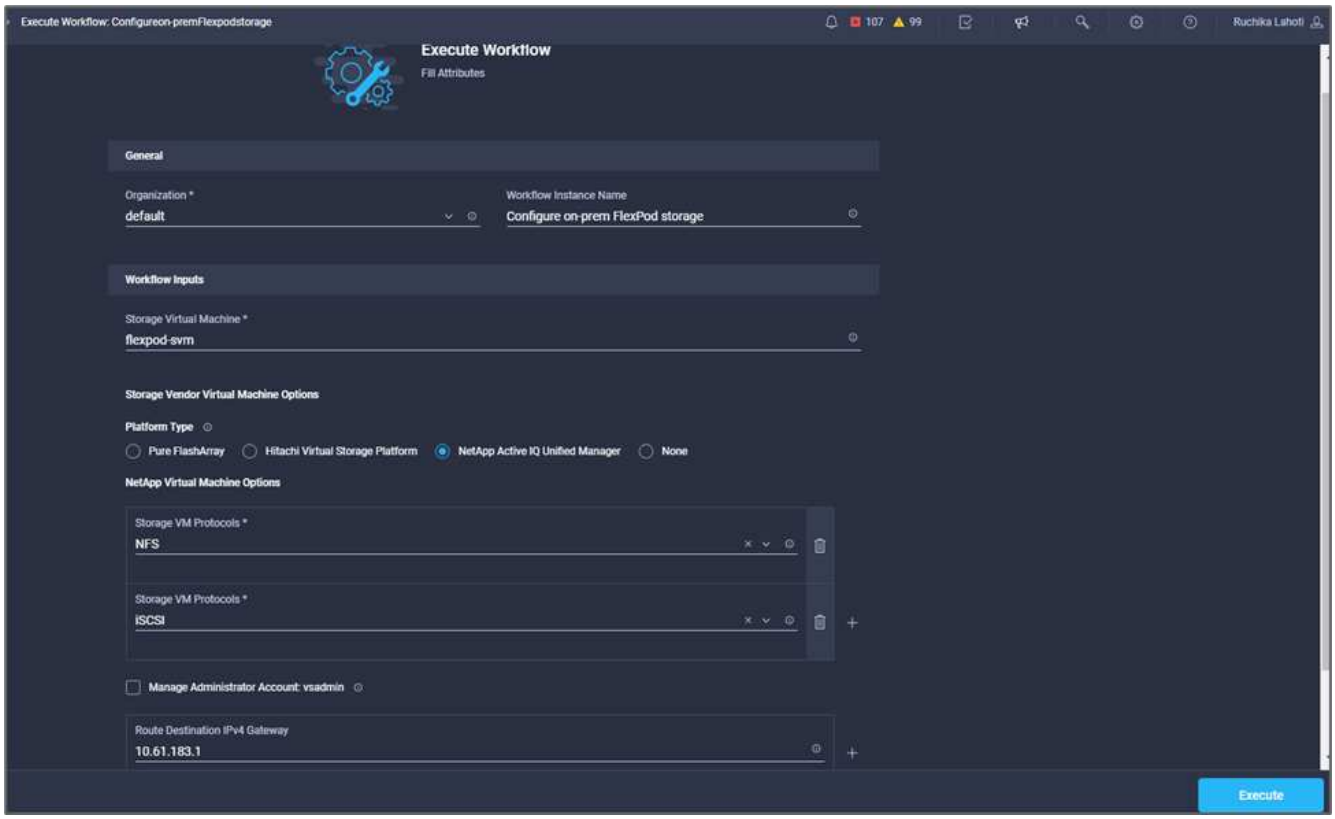
次に、この解決策 の成功基準を確認する手順の概要を示します。

1. FlexPod のONTAP ボリュームにあるサンプルデータセットでSHA256チェックサムを生成します。
2. FlexPod のONTAP とCloud Volumes ONTAP の間にVolume SnapMirror関係を設定します。
3. サンプルデータセットをFlexPod からCloud Volumes ONTAP にレプリケートします。
4. SnapMirror関係を解除し、Cloud Volumes ONTAP 内のボリュームを本番環境に昇格します。
5. Cloud Volumes ONTAP ボリュームとデータセットをGoogle Cloudのコンピューティングインスタンスにマッピングします。
6. Cloud Volumes ONTAP のサンプルデータセットでSHA256チェックサムを生成します。
7. ソースとデスティネーションのチェックサムを比較します。両方のチェックサムが一致していると考えられます。

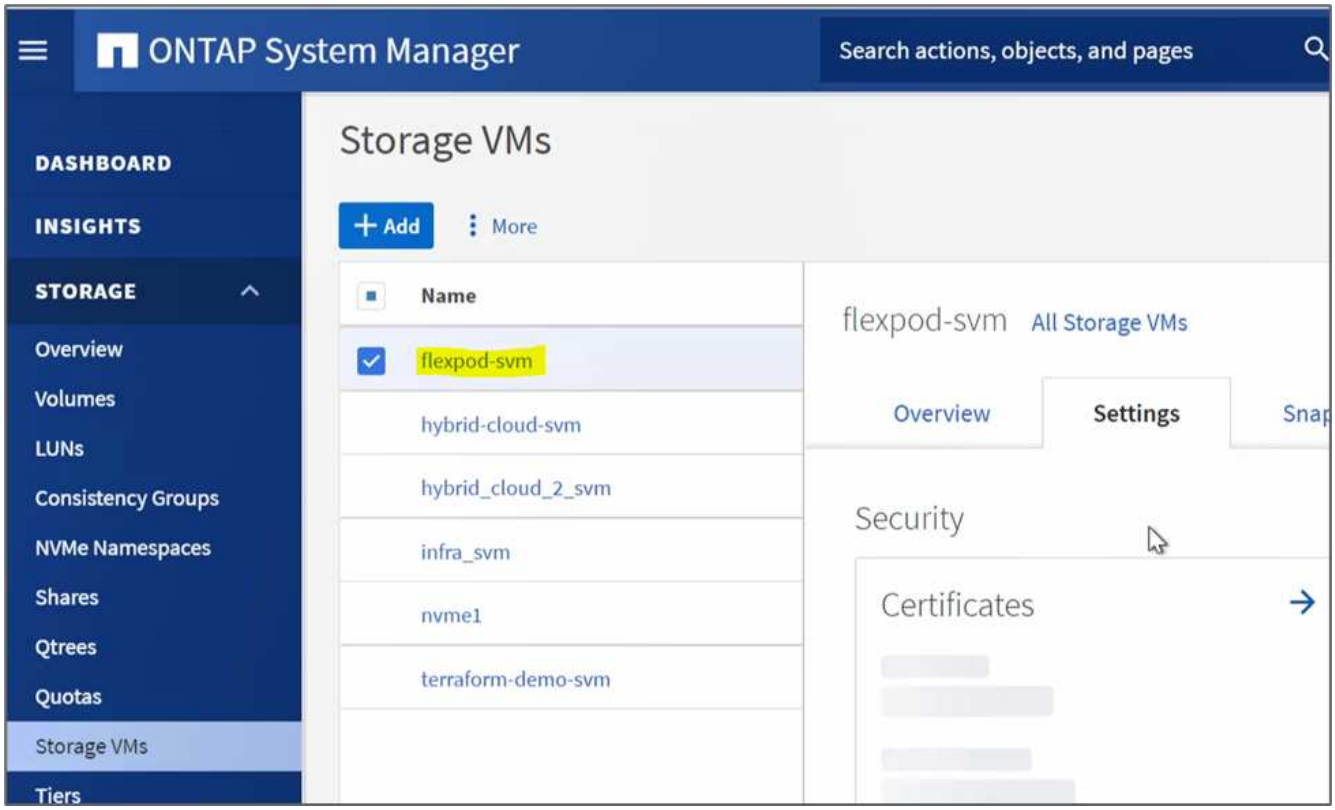
オンプレミスワークフローを実行するには、次の手順を実行します。

1. オンプレミスFlexPod のIntersightでワークフローを作成

2. 必要な入力を指定し、ワークフローを実行します。

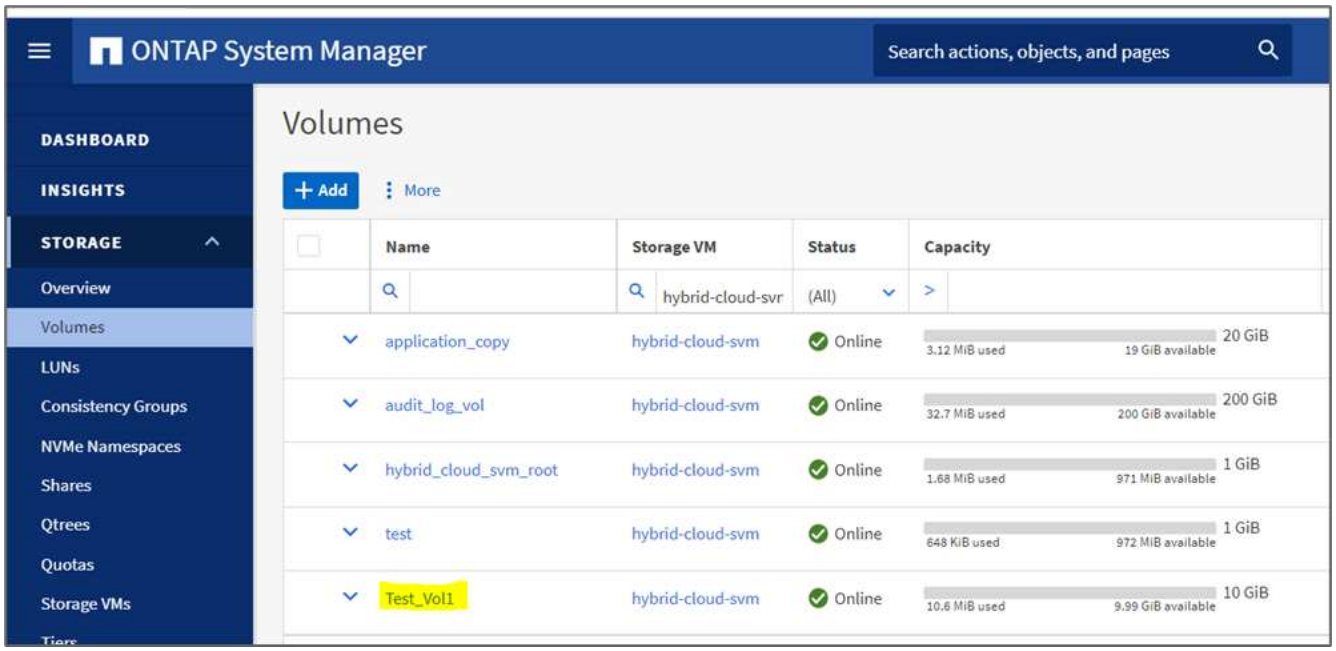


3. システムマネージャで、新しく作成したSVMを確認します。



4. 別のディザスタリカバリワークフローを作成して実行し、オンプレミスのFlexPod にボリュームを作成して、FlexPod とCloud Volumes ONTAP でこのボリューム間にSnapMirror関係を確立します。

5. ONTAP システムマネージャで、新しく作成したボリュームを確認します。

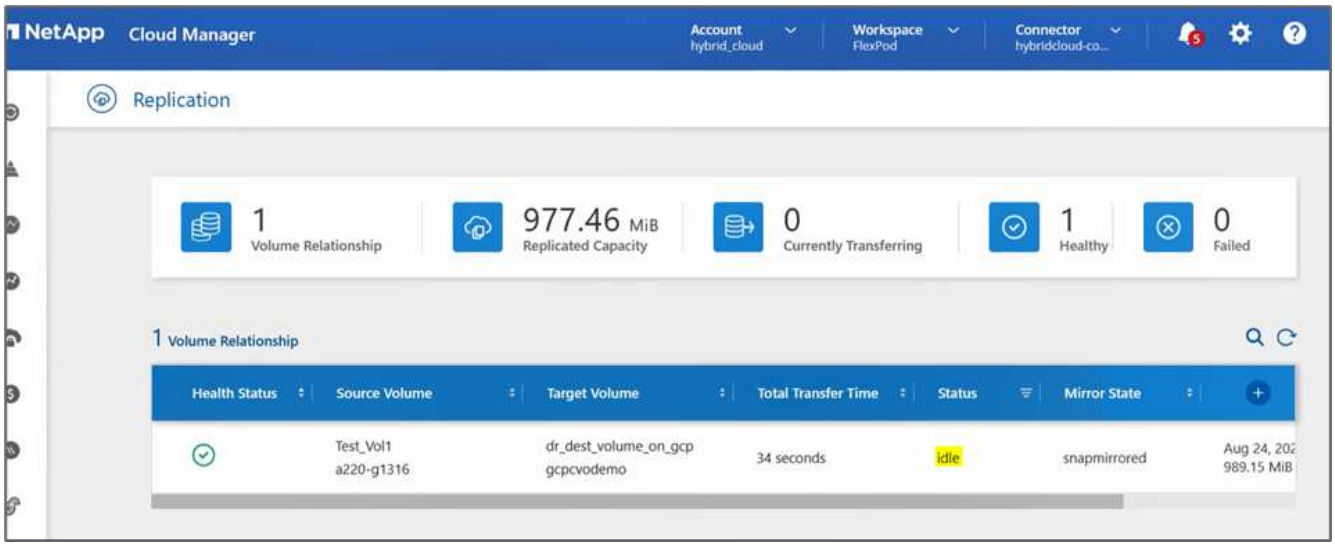


6. 同じNFSボリュームをオンプレミスの仮想マシンにマウントし、サンプルデータセットをコピーしてチェックサムを実行します。

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

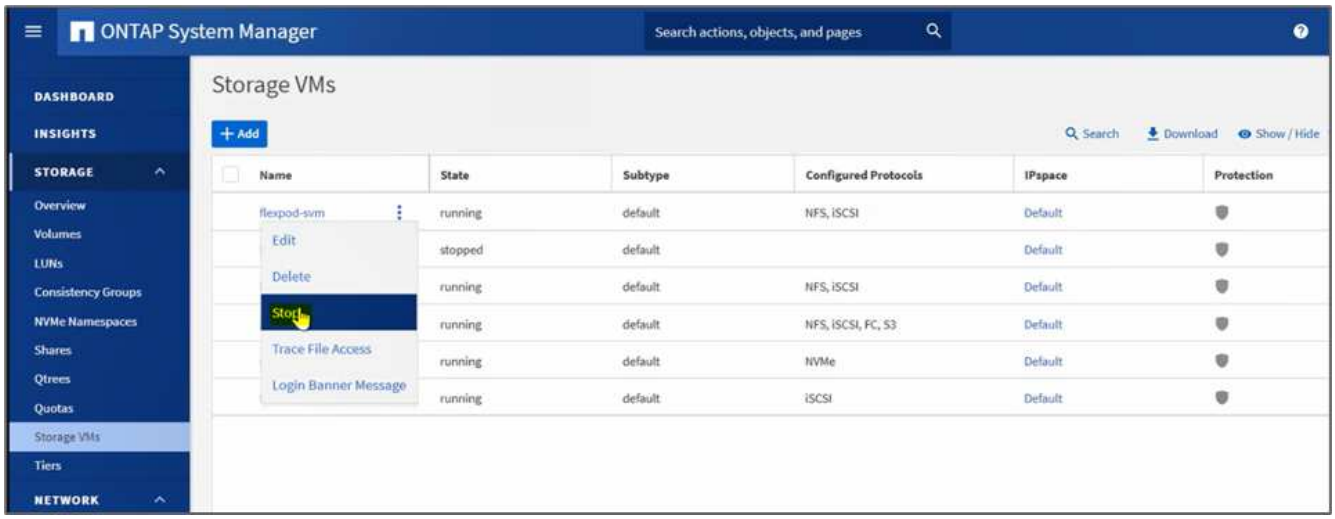
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Cloud Managerでレプリケーションステータスを確認します。データのサイズによっては、データ転送に数分かかることがあります。完了すると、SnapMirrorのステータスが* Idle *と表示されます。

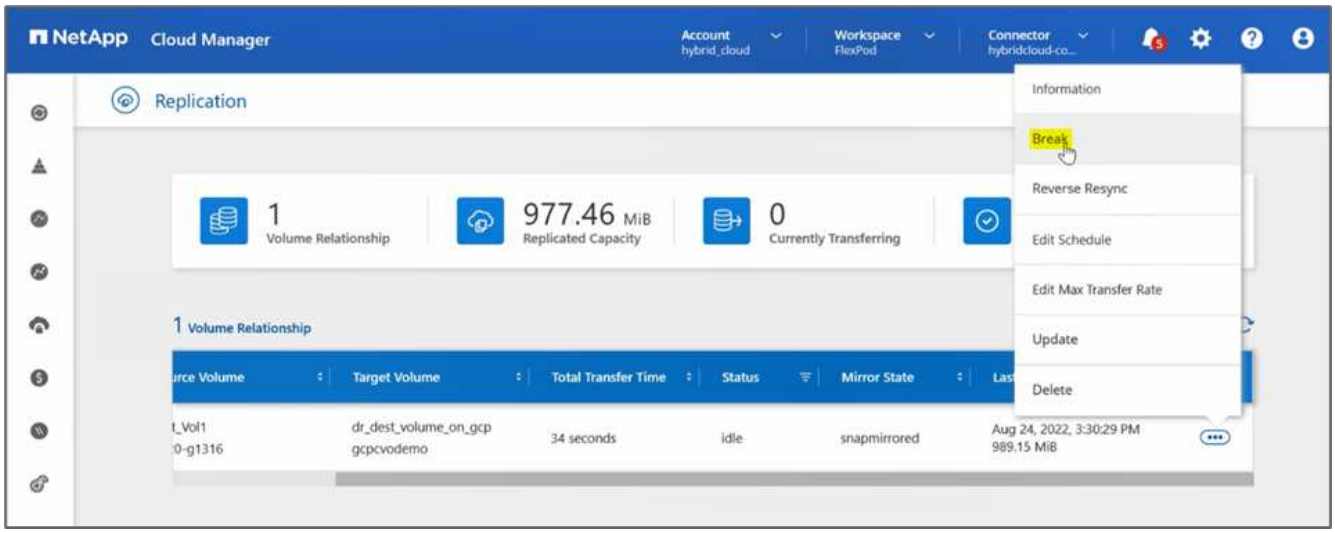


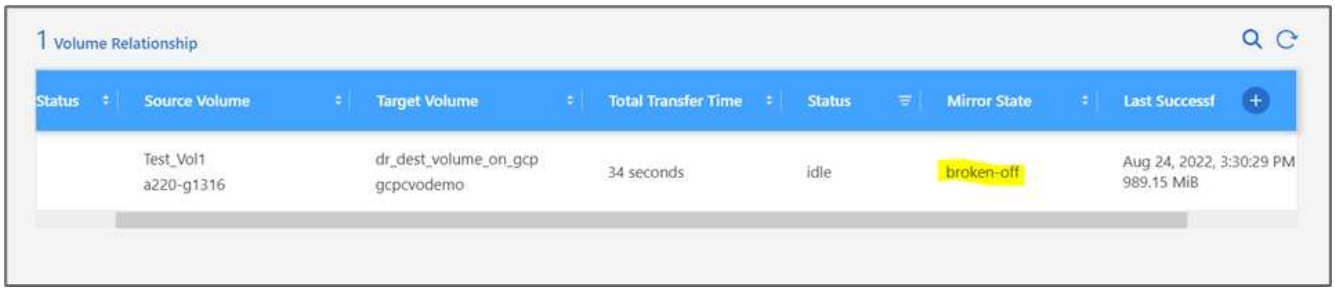
8. データ転送が完了したら、「Test_vol1」ボリュームをホストしているSVMを停止して、ソース側の災害をシミュレートします。

   SVMの停止後、「Test_vol1」ボリュームはCloud Managerに表示されません。

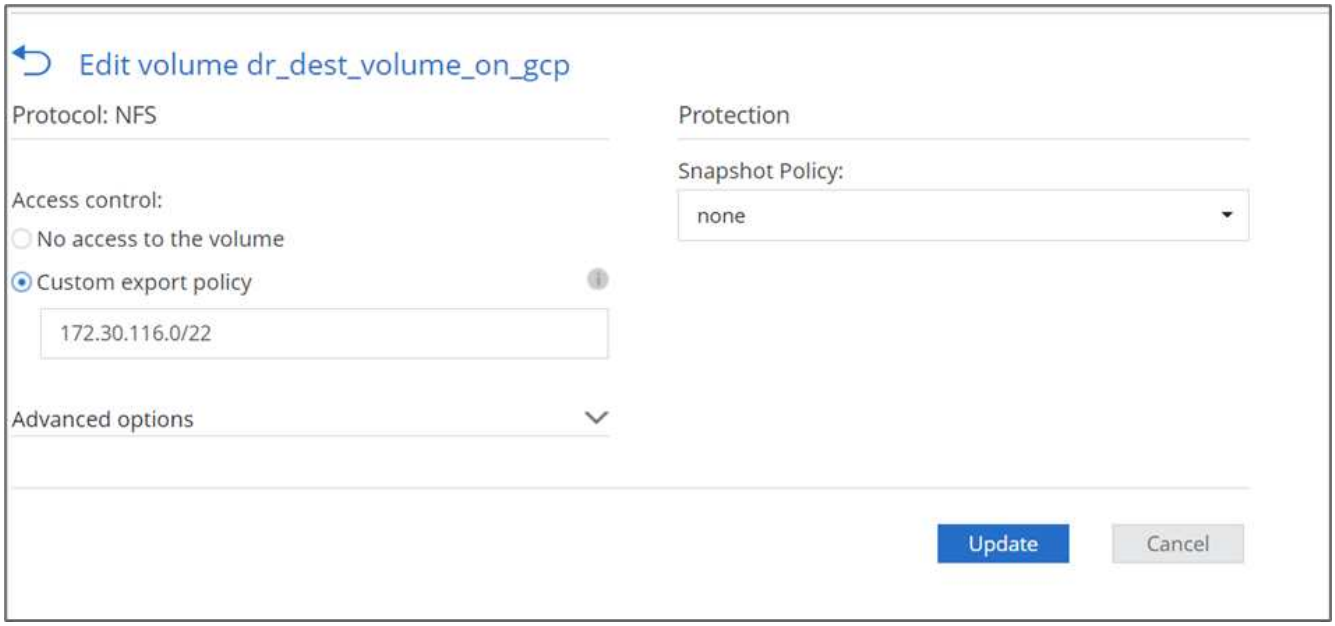


9. レプリケーション関係を解除し、Cloud Volumes ONTAP デスティネーションボリュームを本番環境に昇格

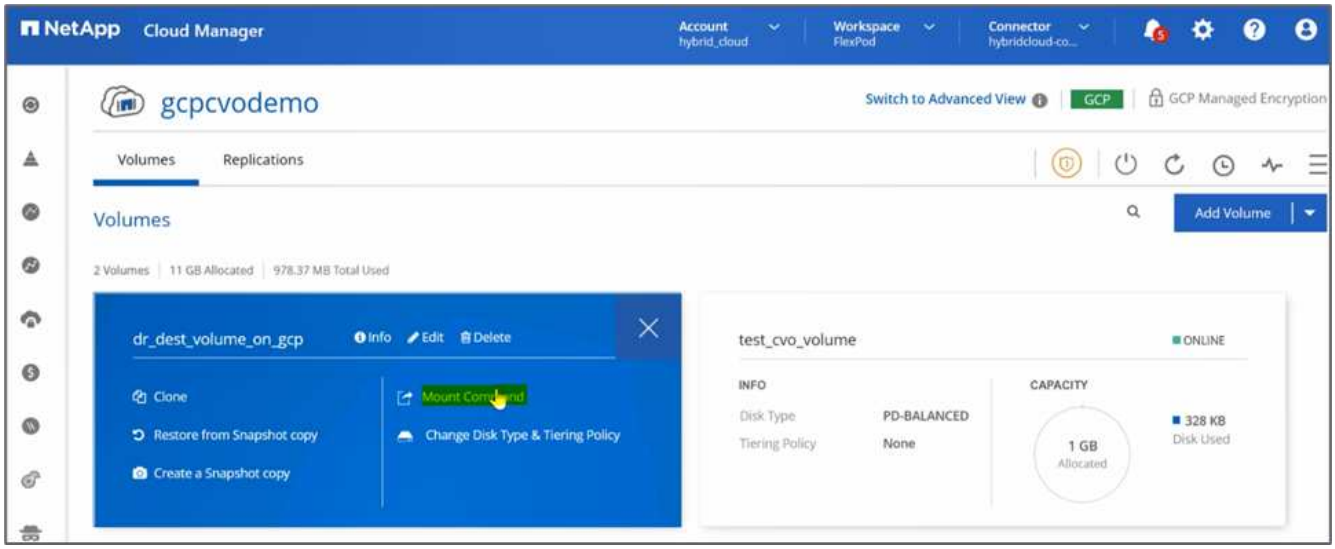




10. ボリュームを編集し、エクスポートポリシーに関連付けてクライアントアクセスを有効にします。



11. ボリュームの使用準備が完了しているマウントコマンドを取得します。



12. コンピューティング・インスタンスにボリュームをマウントし'デスティネーション・ボリュームにデータが存在することを確認して'sample_dataset_s2GB'ファイルのSHA256チェックサムを生成します

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. ソース（FlexPod ）とデスティネーション（Cloud Volumes ONTAP ）の両方でチェックサム値を比較します。
14. チェックサムはソースとデスティネーションのチェックサムと同じです。

ソースからデスティネーションへのデータレプリケーションが正常に完了し、データの整合性が維持されていることを確認できます。このデータは、ソースサイトがリストアを実行している間に、アプリケーションがクライアントにデータを提供するために安全に使用できるようになりました。

"次は終わりです"

まとめ

"前のバージョン：解決策 の検証。"

この解決策 では、ネットアップのクラウドデータサービス、Cloud Volumes ONTAP 、FlexPod データセンターインフラを使用して、Cisco Intersightクラウドオーケストレーションツールを基盤とするパブリッククラウドを使用したDR解決策 を構築しました。FlexPod 解決策 は絶えず進化しており、お客様はアプリケーションやビジネス提供プロセスを最新化できるようになっています。この解決策 を使用すると、DR解決策 のコストを低く抑えながら、短期またはフルタイムのDR計画のための移動先としてパブリッククラウドを使用してBCDR計画を構築できます。

オンプレミスのFlexPod とNetApp Cloud Volumes ONTAP 間のデータレプリケーションは、実績のあるSnapMirrorテクノロジによって処理されましたが、お客様のデータ移動要件には、Cloud Sync などの他のネットアップのデータ転送ツールや同期ツールも選択できます。TLS/AESをベースとする暗号化テクノロジが組み込まれているため、転送中のデータのセキュリティを確保できます。

アプリケーション向けの一時的なDRプランでも、企業向けのフルタイムのDRプランでも、この解決策 で使用される製品ポートフォリオは、両方の要件を大規模に満たすことができます。Cisco Intersight Workflow Orchestratorを活用することで、構築済みのワークフローを利用して同じワークフローを自動化できます。プロセスの再構築が不要になるだけでなく、BCDRプランの実装も高速化されます。

解決策 を使用すると、Cisco Intersight Cloud Orchestratorが提供する自動化とオーケストレーションによって、ハイブリッドクラウド全体でFlexPod オンプレミスとデータレプリケーションを非常に簡単かつ便利に管理できます。

追加情報の参照先

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。

GitHub

- 使用されているすべてのTerraform設定

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- ワークフローをインポートするためのJSONファイル

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersightの

- Cisco Intersightのヘルプセンター

  "https://intersight.com/help/saas/home"

- Cisco Intersight Cloud Orchestratorのドキュメント：

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service for橋（橋本）Terraform Documentation

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Cisco Intersightのデータシート

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Cisco Intersight Cloud Orchestratorデータシート

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Cisco Intersight Service for橋（Cisco Intersight Service for橋）Terraformデータシート

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

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

  "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"

- FlexPod データセンターとCisco UCS Xシリーズ

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

相互運用性

- NetApp Interoperability Matrix Tool で確認できます

  "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.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

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

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

NetApp Cloud Volumes ONTAP の参考資料

- NetApp Cloud Manager の略

"https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Cloud Volumes ONTAP TCO計算ツール

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP サイジングツール

  "https://cloud.netapp.com/cvo-sizer"

- クラウド評価ツール

  https://cloud.netapp.com/assessments

- ネットアップのハイブリッドクラウド

  https://cloud.netapp.com/hybrid-cloud

- Cloud Manager API ドキュメント

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

問題のトラブルシューティング

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

テラフォーム

- クラウドをテラフォーム

  "https://www.terraform.io/cloud"

- Terraformドキュメント

  "https://www.terraform.io/docs/"

- NetApp Cloud Managerレジストリ

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- GCPのONTAP ハイアベイラビリティ

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- GCPの永続的なサイト

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

ネットアップのAstraとCisco Intersightを活用したFlexPod ハイブリッドクラウドをRed Hat OpenShiftに活用

TR-4936：『FlexPod hybrid cloud with NetApp Astra and Cisco Intersight for Red Hat OpenShift』

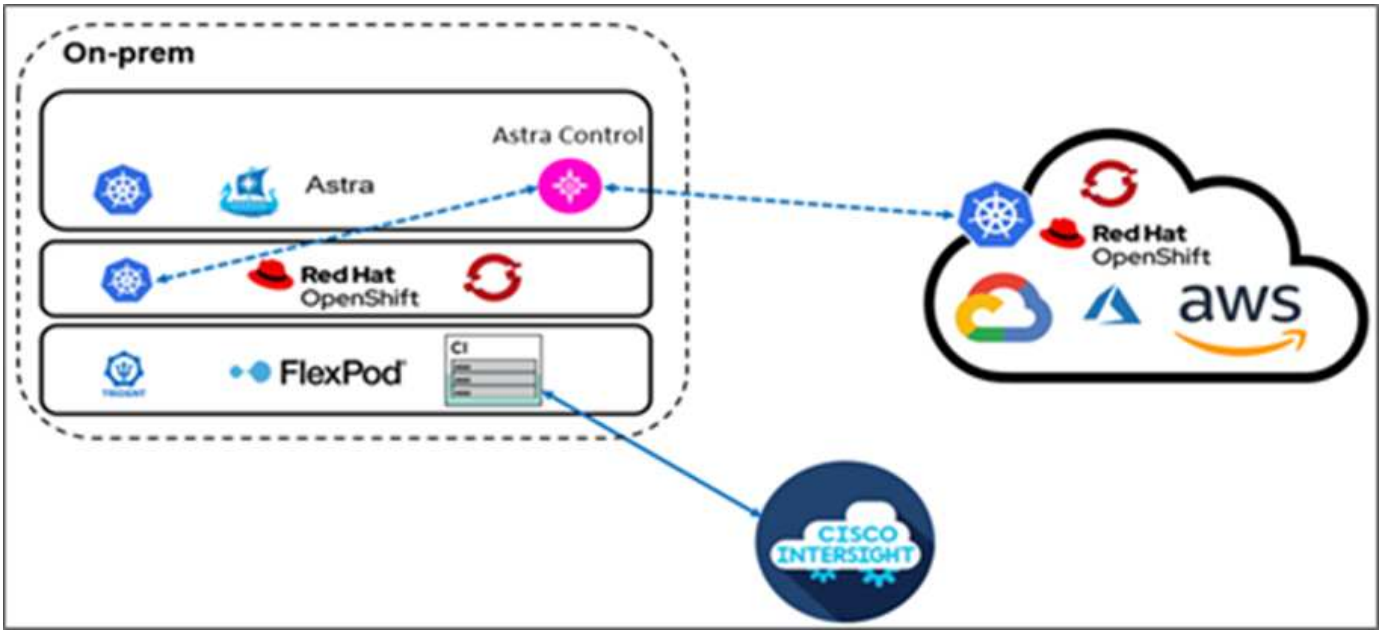
Abhinav Singhの

はじめに

コンテナ化されたアプリケーションの開発、導入、実行、管理、拡張のための事実上の選択肢となるコンテナとKubernetesは、ビジネスクリティカルなアプリケーションを実行する企業の増加に伴いつつあります。ビジネスクリティカルなアプリケーションは、状態に大きく依存しています。ステートフルアプリケーションには、状態、データ、および設定情報が関連付けられており、ビジネスロジックを実行する前のデータトランザクションに依存します。Kubernetes上で実行されるビジネスクリティカルなアプリケーションには、従来型アプリケーションのような可用性とビジネス継続性の要件が引き続きあります。サービスの停止は、収益の損失、生産性、会社の評判に深刻な影響を与える可能性があります。そのため、Kubernetesワークロードをクラスタ、オンプレミスデータセンター、ハイブリッドクラウド環境内およびクラスタ間で迅速かつ容易に保護、リカバリ、移動することが非常に重要です。企業は、ビジネスをハイブリッドクラウドモデルに移行し、アプリケーションをクラウドネイティブなフォームファクタに刷新するメリットを高く挙げています。

このテクニカルレポートでは、FlexPod コンバージドインフラ解決策 上にNetApp Astra Control CenterとRed Hat OpenShift Container Platformを統合し、Amazon Web Services（AWS）に拡張してハイブリッドクラウドデータセンターを構築しました。使い慣れたことに基づいて作成されています "FlexPod とRed Hat OpenShift"このドキュメントでは、ネットアップのAstra Control Centerについて説明します。インストール、設定、アプリケーション保護ワークフロー、オンプレミスとクラウド間でのアプリケーション移行から始まります。また、Red Hat OpenShiftで実行されるコンテナ化アプリケーションにNetApp Astra Control Centerを使用する場合の、アプリケーション対応データ管理機能（バックアップとリカバリ、ビジネス継続性など）の利点についても説明します。

次の図に、解決策 の概要を示します。



対象者

このドキュメントは、CTO（最高技術責任者）、アプリケーション開発者、クラウド解決策 アーキテクト、サイト信頼性エンジニア（SRE）、DevOpsエンジニア、ITOps、コンテナ化されたアプリケーションの設計、ホスティング、管理に重点を置いたプロフェッショナルサービスチームなど、読者を想定しています。

NetApp Astra Control–主なユースケース

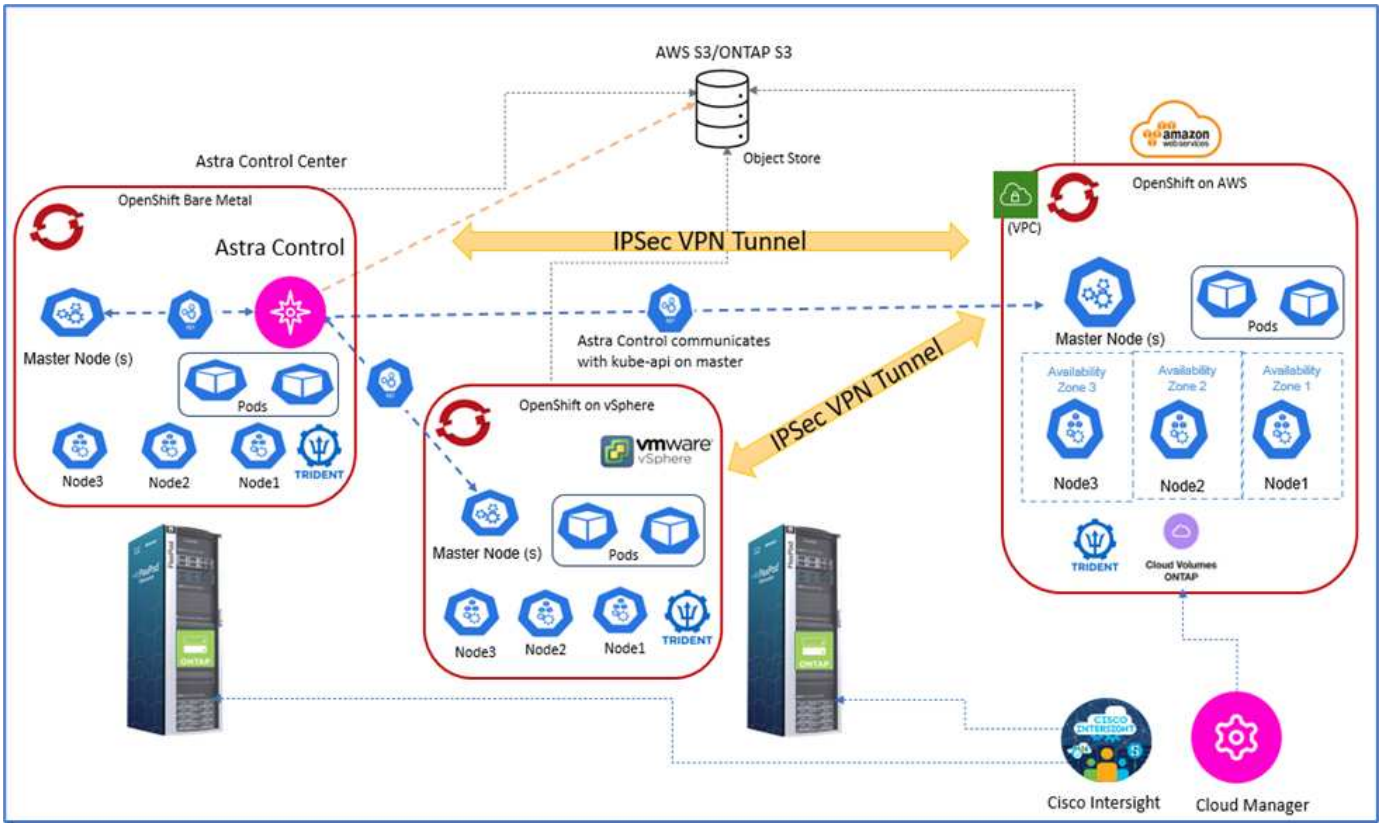
ネットアップのAstra Controlは、クラウドネイティブなマイクロサービスを利用するお客様にアプリケーション保護を簡易化することを目的としています。

- スナップショットを使用したポイントインタイム（**PiT**）アプリケーションリプレゼンテーション。 Astra Controlを使用すると、Kubernetesで実行されているアプリケーションの構成の詳細や、関連付けられた永続的ストレージを含む、コンテナ化されたアプリケーションのエンドツーエンドのスナップショットを作成できます。インシデントが発生した場合は、ボタンクリックでアプリケーションを正常な状態に復元できます。
- フルコピー・アプリケーション・バックアップ Astra Controlを使用すると'事前に定義されたスケジュールでフル・アプリケーション・バックアップを実行できますこのスケジュールを使用すると'アプリケーションを同じKubernetesクラスタにリストアしたり'別のKubernetesクラスタにオンデマンドで自動化された方法でリストアしたりできます
- クローンを使用したアプリケーションの移植と移行 Astra Controlを使用すると、アプリケーション全体をKubernetesクラスタ間または同じKubernetesクラスタ内のデータとともにクローニングできます。この機能は、クラスタがどこにあるかに関係なく、Kubernetesクラスタ間でアプリケーションを移植または移行する場合にも役立ちます（クローニング後にソースアプリケーションインスタンスを削除するだけです）。
- アプリケーションの一貫性をカスタマイズできます。 Astra Controlを使用すると、実行フックを活用してアプリケーションの休止状態を定義できます。「実行前」と「実行後」のフックをスナップショットおよびバックアップのワークフローにドロップすると、スナップショットまたはバックアップが作成される前に、アプリケーションが独自の方法で休止されます。
- アプリケーションレベルのディザスタリカバリ（**DR**）を自動化。 Astra Controlを使用すると、コンテナ化されたアプリケーション用にBCDR（ビジネス継続性ディザスタリカバリ）計画を設定できます。NetApp SnapMirrorはバックエンドで使用されるため、DRワークフローの実装はすべて自動化されます。

解決策 トポロジ

このセクションでは、解決策 の論理トポロジについて説明します。

次の図は、OpenShift Container Platformクラスタを実行するFlexPod オンプレミス環境と、NetApp Cloud Volumes ONTAP 、Cisco Intersight、NetApp Cloud Manager SaaSプラットフォームを使用するAWS上の自己管理型OpenShift Container Platformクラスタからなる解決策 トポロジを示しています。



最初のOpenShift Container PlatformクラスタはFlexPod 上にベアメタルインストールされ、2番目のOpenShift Container PlatformクラスタはFlexPod 上で実行されるVMware vSphereに導入され、3番目のOpenShift Container Platformクラスタはとして導入されます "プライベートクラスタ" 自社で管理するインフラとして、AWS上の既存の仮想プライベートクラウド（VPC）に導入できます。

この解決策 では、FlexPod はサイト間VPNを介してAWSに接続されますが、直接接続の実装を使用してハイブリッドクラウドに拡張することもできます。Cisco Intersightは、FlexPod インフラストラクチャコンポーネントの管理に使用されます。

この解決策 では、Astra Control Centerが、FlexPod およびAWSで実行されているOpenShift Container Platformクラスタでホストされているコンテナ化アプリケーションを管理します。FlexPod で実行されているOpenShiftベアメタルインスタンスにAstraコントロールセンターをインストールします。Astra Controlは、マスターノードのkube-APIと通信し、Kubernetesクラスタの変更を継続的に監視します。Kubernetesクラスタに追加した新しいアプリケーションは自動的に検出され、管理用に使用できるようになります。

コンテナ化されたアプリケーションのPiT表現は、Astra Control Centerを使用してスナップショットとしてキャプチャできます。アプリケーションスナップショットは、スケジュールされた保護ポリシーまたはオンデマンドで開始できます。Astraがサポートしているアプリケーションの場合、スナップショットはクラッシュ整合性があります。アプリケーションスナップショットは、永続ボリューム内のアプリケーションデータのスナップショットと、そのアプリケーションに関連付けられているさまざまなKubernetesリソースのアプリケーションメタデータを構成します。

アプリケーションのフルコピーバックアップは、事前定義されたバックアップスケジュールまたはオンデマンドを使用して、Astra Controlを使用して作成できます。オブジェクトストレージは、アプリケーションデータのバックアップを格納するために使用されます。NetApp ONTAP S3、NetApp StorageGRID 、および汎用のS3実装をオブジェクトストアとして使用できます。

"次の例は、解決策 コンポーネントです。"

解決策コンポーネント

"Previous ：解決策の概要を示します。"

FlexPod

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフトウェアの定義済みセットです。FlexPod には、NetApp ONTAP ストレージ、Cisco Nexusネットワーク、Cisco MDSストレージネットワーク、Cisco Unified Computing System（Cisco UCS）が含まれています。この設計は、ネットワーク、コンピューティング、ストレージを1つのデータセンターラックに収容できる柔軟性を備えています。また、お客様のデータセンター設計に従って導入することもできます。ポート密度を使用すると、ネットワークコンポーネントは複数の構成に対応できます。

Astra Control の略

Astra Controlは、パブリッククラウドとオンプレミスの両方でホストされるクラウドネイティブアプリケーションに対して、アプリケーション対応のデータ保護サービスを提供します。Astra Controlは、Kubernetesで実行されるコンテナ化されたアプリケーションに、データ保護、ディザスタリカバリ、移行の機能を提供します。

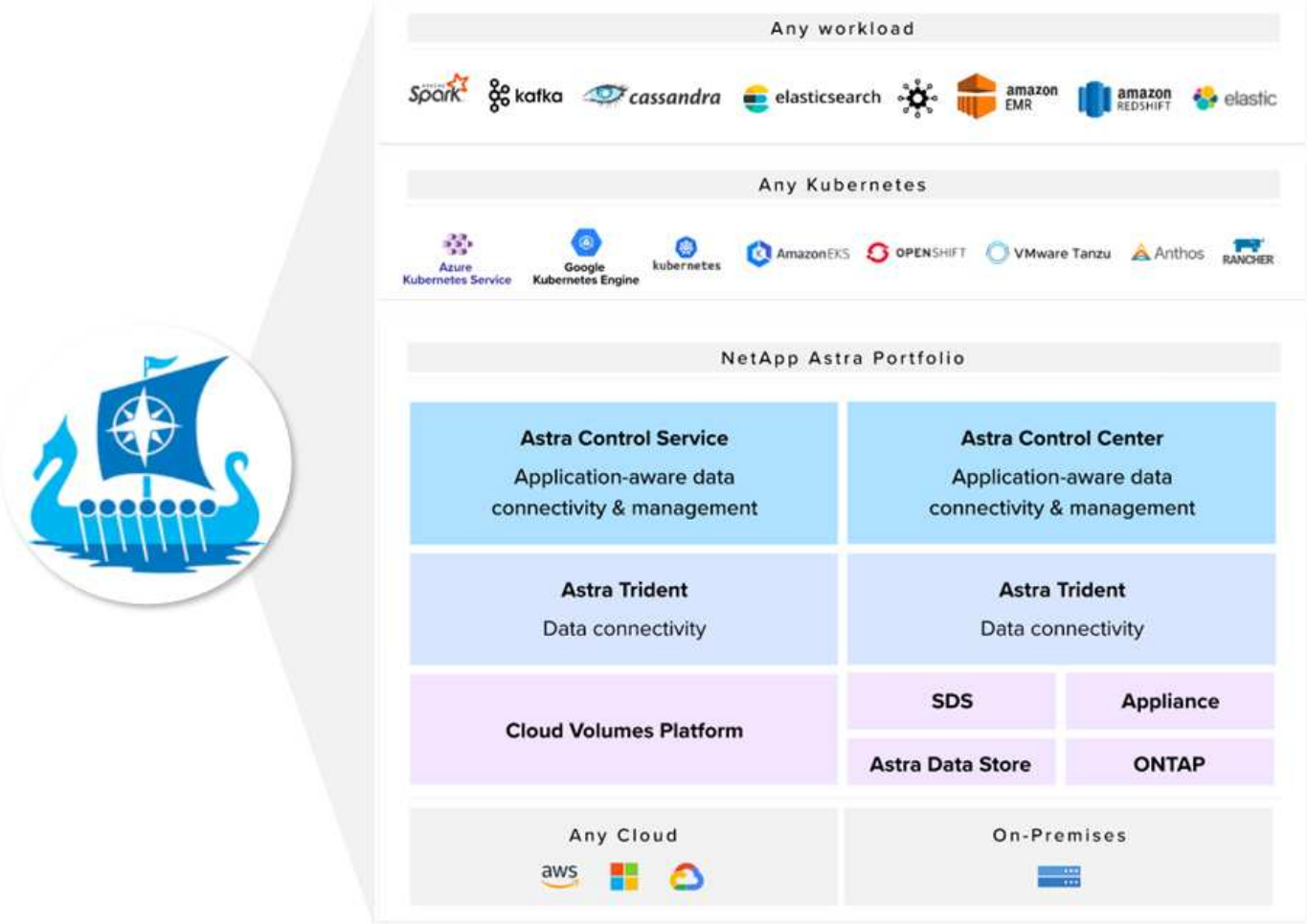
の機能

Astra Control は、 Kubernetes アプリケーションデータのライフサイクル管理に不可欠な機能を提供

- 永続的ストレージを自動的に管理
- アプリケーションと整合性のあるオンデマンドのSnapshotとバックアップを作成
- ポリシーベースのスナップショット処理とバックアップ処理を自動化
- ハイブリッドクラウド環境で、アプリケーションと関連データをKubernetesクラスタから別のクラスタに移行する
- 同じKubernetesクラスタまたは別のKubernetesクラスタにアプリケーションをクローニングする
- アプリケーション保護ステータスを視覚化します
- グラフィカルユーザインターフェイスとすべての保護ワークフローを社内ツールから実装するためのREST APIの完全なリストを提供します。

Astra Controlを使用すると、Kubernetesクラスタで作成された関連リソースの情報を含む、コンテナ化されたアプリケーションを一元的に可視化できます。すべてのクラスタ、すべてのアプリケーション、すべてのクラウド、またはすべてのデータセンターを1つのポータルで表示できます。オンプレミスまたはパブリッククラウドのすべての環境でAstra Control APIを使用して、データ管理ワークフローを実装できます。

次の図は、Astra Controlの機能を示しています。



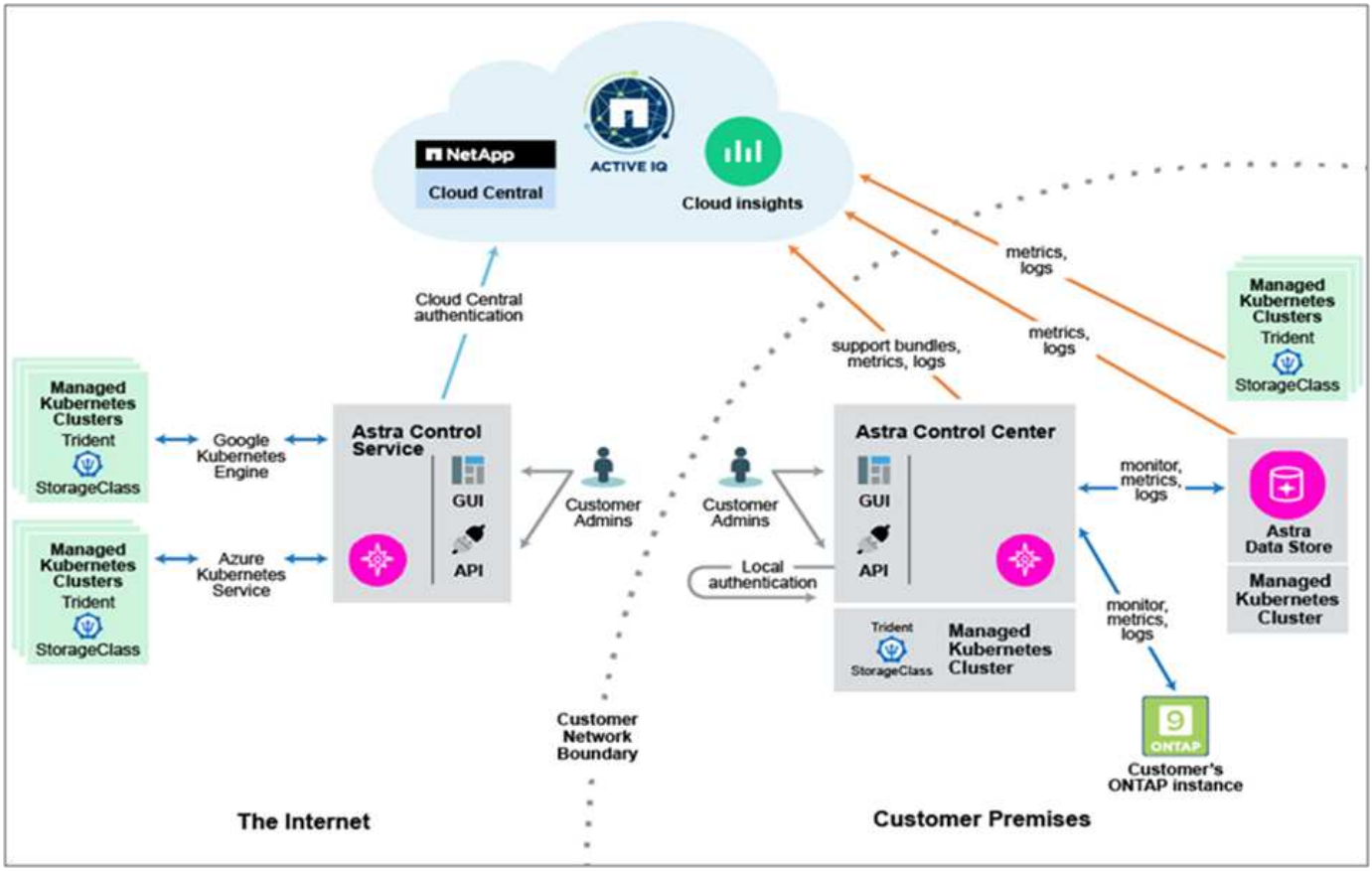
Astra Control消費モデル

Astra Controlには、次の2つの消費モデルがあります。

- * Astra Control Service。ネットアップがホストするフルマネージドサービス。Google Kubernetes Engine（GKE）、Azure Kubernetes Service（AKS）でKubernetesクラスタのアプリケーション対応データ管理を実現します。
- * Astra Control Center。*オンプレミスおよびハイブリッドクラウド環境で実行されるKubernetesクラスタのアプリケーション対応データ管理を提供する、自己管理ソフトウェアです。

このテクニカルレポートでは、Kubernetesで実行されるクラウドネイティブアプリケーションを管理するために、Astra Control Centerを活用しています。

次の図は、Astra Controlアーキテクチャを示しています。



Astra Trident

Astra Tridentは、コンテナやKubernetesディストリビューション向けの、完全にサポートされているオープンソースのストレージオーケストレーションツールです。コンテナ化されたアプリケーションの永続性に対する要求を、業界標準のインターフェイス（など）を使用して満たすことができるように、最初から設計されています "CSI（Container Storage Interface）"。Astra Tridentを使用すると、マイクロサービスやコンテナ化されたアプリケーションを利用して、ネットアップのストレージシステムポートフォリオが提供するエンタープライズクラスのストレージサービスを活用できます。

Kubernetesクラスタにポッドとして導入されるAstra Tridentは、Kubernetesワークロードに動的なストレージオーケストレーションサービスを提供します。コンテナ化されたアプリケーションは、NetApp ONTAP（NetApp AFF 、NetApp FAS 、NetApp ONTAP Select 、Cloudなど）を含むネットアップの幅広いポートフォリオから、永続的ストレージをすばやく簡単に消費できます。 さらに、Amazon FSX for NetApp ONTAP ）、NetApp Element ソフトウェア（NetApp SolidFire ）、Azure NetApp Files サービス、Google Cloud上のクラウドボリュームサービス、AWS上のクラウドボリュームサービスも利用できます。FlexPod 環境では、Astra Tridentを使用して、ネットアップのFlexVol ボリュームをベースとするコンテナや、ONTAP AFF やFAS システム、Cloud Volumes ONTAP などのストレージプラットフォームでホストされるLUNに対応するコンテナの永続的ボリュームを動的にプロビジョニングおよび管理できます。Tridentは、Astra Controlが提供するアプリケーション保護スキームの実装においても重要な役割を果たします。Astra Tridentの詳細については、を参照してください "Astra Tridentのドキュメント"

ストレージバックエンド

Astra Tridentを使用するには、サポートされているストレージバックエンドが必要です。Tridentバックエンドは、Tridentとストレージシステムの関係を定義します。Tridentは、そのストレージシステムとの通信方法や、Tridentがそのシステムからボリュームをプロビジョニングする方法を解説します。Tridentは、あるストレージクラスが定義した要件を満たしたストレージプールをバックエンドから自動的に提供します。

- ONTAP AFF と FAS のストレージバックエンド。ONTAP は、ストレージソフトウェアおよびハードウェアプラットフォームとして、コアストレージサービス、複数のストレージアクセスプロトコルのサポート、およびネットアップのSnapshotコピーやミラーリングなどのストレージ管理機能を提供します。
- Cloud Volumes ONTAP ストレージバックエンド
- "Astra データストア" ストレージバックエンド

NetApp Cloud Volumes ONTAP の略

NetApp Cloud Volumes ONTAP は、ファイルワークロードとブロックワークロードに高度なデータ管理機能を提供するSoftware-Defined Storageです。Cloud Volumes ONTAP を使用すると、データ保護、セキュリティ、コンプライアンスを強化しながら、クラウドストレージのコストを最適化し、アプリケーションのパフォーマンスを向上させることができます。

主なメリットは次のとおりです。

- 組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、クローニングを活用して、ストレージコストを最小限に抑えます。
- クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を確保できます。
- Cloud Volumes ONTAP は、業界をリードするネットアップのレプリケーションテクノロジであるSnapMirrorを活用して、オンプレミスのデータをクラウドにレプリケートします。これにより、複数のユースケースでセカンダリコピーを簡単に利用できます。
- また、 Cloud Volumes ONTAP は Cloud Backup Service との統合により、保護のためのバックアップとリストア機能、およびクラウドデータの長期アーカイブ機能を提供します。
- アプリケーションをオフラインにすることなく、ハイパフォーマンスとローパフォーマンスのストレージプールをオンデマンドで切り替えます。
- NetApp SnapCenter を使用してSnapshotコピーの整合性を確保します。
- Cloud Volumes ONTAP は、データ暗号化をサポートし、ウィルスやランサムウェアからの保護を提供します。
- クラウドデータセンスとの統合により、データコンテキストを把握し、機密データを識別できます。

Cloud Central にアクセスできます

Cloud Centralは、ネットアップのクラウドデータサービスにアクセスして管理するための一元的な場所を提供します。これらのサービスにより、重要なアプリケーションのクラウドでの実行、自動化されたDRサイトの作成、データのバックアップ、複数のクラウド間でのデータの効果的な移行と制御が可能になります。詳細については、を参照してください "Cloud Centralにアクセスできます。"

クラウドマネージャ

Cloud Managerは、エンタープライズクラスのSaaSベースの管理プラットフォームです。ITエキスパートとクラウドアーキテクトは、ネットアップのクラウドソリューションを使用して、ハイブリッドマルチクラウドインフラを一元管理できます。オンプレミスとクラウドのストレージを表示および管理する一元化されたシステムを提供し、ハイブリッドクラウド、複数のクラウドプロバイダ、アカウントをサポートします。詳細については、を参照してください "クラウドマネージャ"。

コネクタ

Connectorは、Cloud Managerがパブリッククラウド環境内のリソースとプロセスを管理できるようにするインスタンスです。Cloud Managerのさまざまな機能を使用するには、コネクタが必要です。コネクタは、クラウドまたはオンプレミスネットワークに導入できます。

Connectorは次の場所でサポートされます。

- AWS
- Microsoft Azure
- Google Cloud
- オンプレミス

コネクタの詳細については、を参照してください "リンクをクリックしてください"

NetApp Cloud Insights の略

ネットアップのクラウドインフラ監視ツールであるCloud Insights を使用すると、Astra Control Centerで管理されるKubernetesクラスタのパフォーマンスと利用率を監視できます。Cloud Insights ：ストレージ使用率とワークロードの相関関係を示します。Cloud Insights 接続を Astra コントロールセンターで有効にすると、テレメータの情報が Astra コントロールセンターの UI ページに表示されます。

NetApp Active IQ Unified Manager の略

NetApp Active IQ Unified Manager では、デザインが一新され、直感的に操作できるインターフェイスからONTAP ストレージクラスタを監視できます。コミュニティの情報やAI分析から得た情報を活用できます。運用、パフォーマンス、プロアクティブな分析情報を提供し、ストレージ環境と仮想マシン（VM）で実行される環境を包括的に分析します。ストレージインフラで問題 が発生すると、Unified Managerから問題 の詳細情報を通知して、ルート原因 の特定に役立てることができます。VMダッシュボードにはVMのパフォーマンス統計が表示されるため、VMware vSphereホストからネットワーク経由で最後にストレージへのI/Oパス全体を調査できます。一部のイベントには、問題 を修正するための対応策も用意されています。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントにカスタムアラートを設定できます。Active IQ Unified Manager を使用すると、容量や使用状況の傾向を予測して問題が発生する前にプロアクティブに対処することができるため、長期的な問題につながる短期的な事後対処策を実施する必要がなくなり、ユーザのストレージ要件に合わせて計画を立てることができます。

Cisco Intersightの

Cisco Intersightは、従来のアプリケーションやクラウドネイティブなインフラに向けて、インテリジェントな自動化、オブザーバビリティ、最適化を実現するSaaSプラットフォームです。このプラットフォームは、ITチームの変化を促進し、ハイブリッドクラウド向けに設計された運用モデルを提供します。

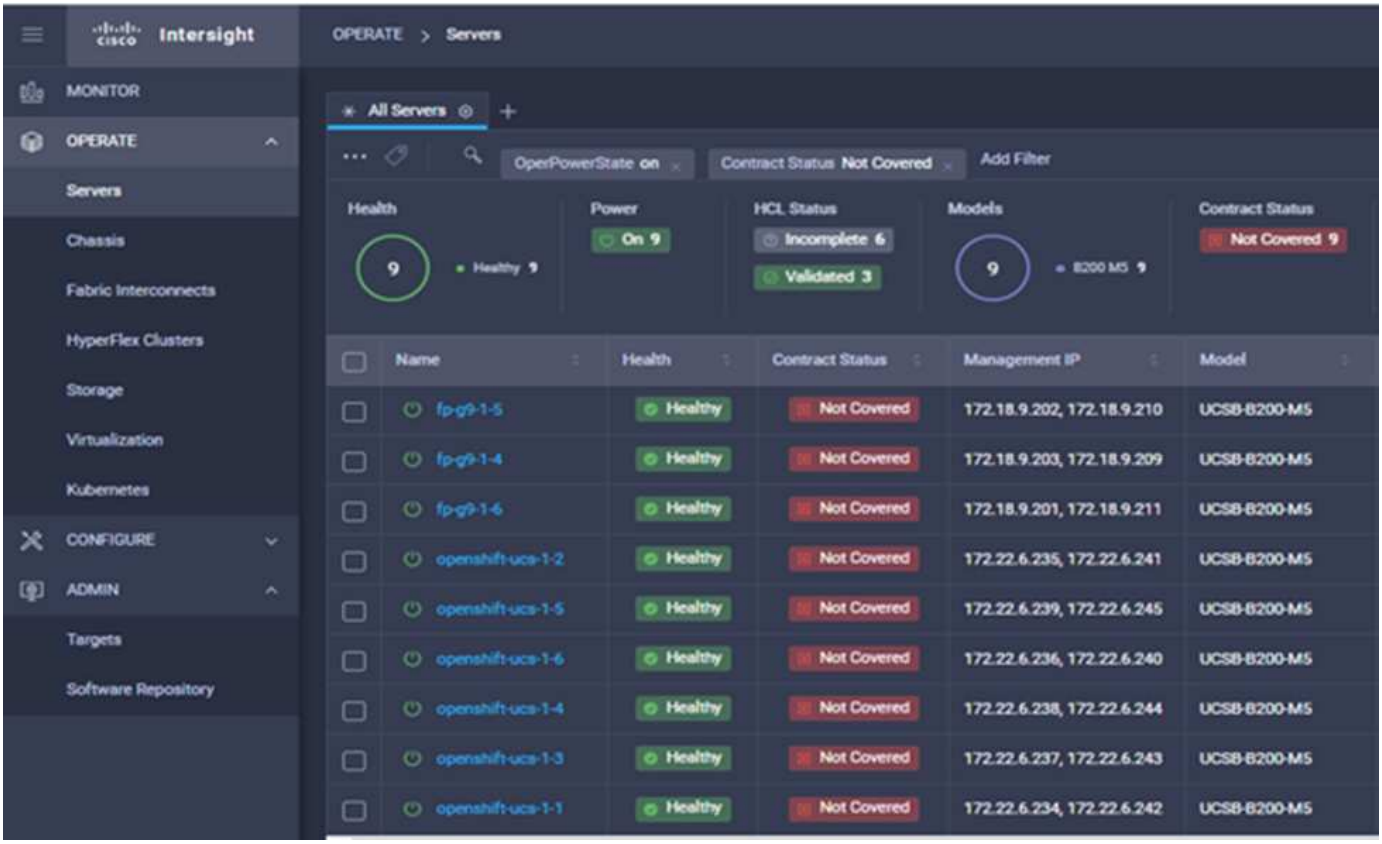
Cisco Intersightには、次のようなメリットがあります。

- *迅速な提供。*俊敏性に優れたソフトウェア開発モデルにより、クラウドまたはお客様のデータセンターからサービスとして提供され、頻繁な更新と継続的な技術革新を実現します。このようにして、お客様は基幹業務の提供を加速することに集中できます。
- *運用の簡素化。*共通のインベントリ、認証、APIを備えた単一のセキュアなSaaS提供ツールを使用して、スタック全体とすべての場所で作業し、チーム間のサイロを排除し、運用を簡素化します。オンプレミスの物理サーバやハイパーバイザーの管理からVM、Kubernetes、サーバレス、自動化、 オンプレミスとパブリッククラウドの両方にわたって最適化とコスト管理を実現

- 継続的な最適化。 Cisco Intersightが提供するインテリジェンスを、Cisco TACだけでなくすべてのレイヤで使用して、環境を継続的に最適化します。このインテリジェンスは、推奨される自動化可能なアクションに変換されるため、ワークロードの移動や物理サーバの稼働状態の監視からKubernetesクラスタの自動サイジングまで、あらゆる変更にリアルタイムで対応できます。また、コスト削減のために、作業中のパブリッククラウドが推奨されます。

Cisco Intersightには、UCSM Managed Mode（UMM）とIntersight Managed Mode（IMM）という2つの管理操作モードがあります。ファブリックインターコネクトの初期セットアップ中に、ファブリック接続Cisco UCSシステムのネイティブUmmまたはIMMを選択できます。この解決策 では、ネイティブUmmが使用されます。

次の図は、Cisco Intersightのダッシュボードを示しています。



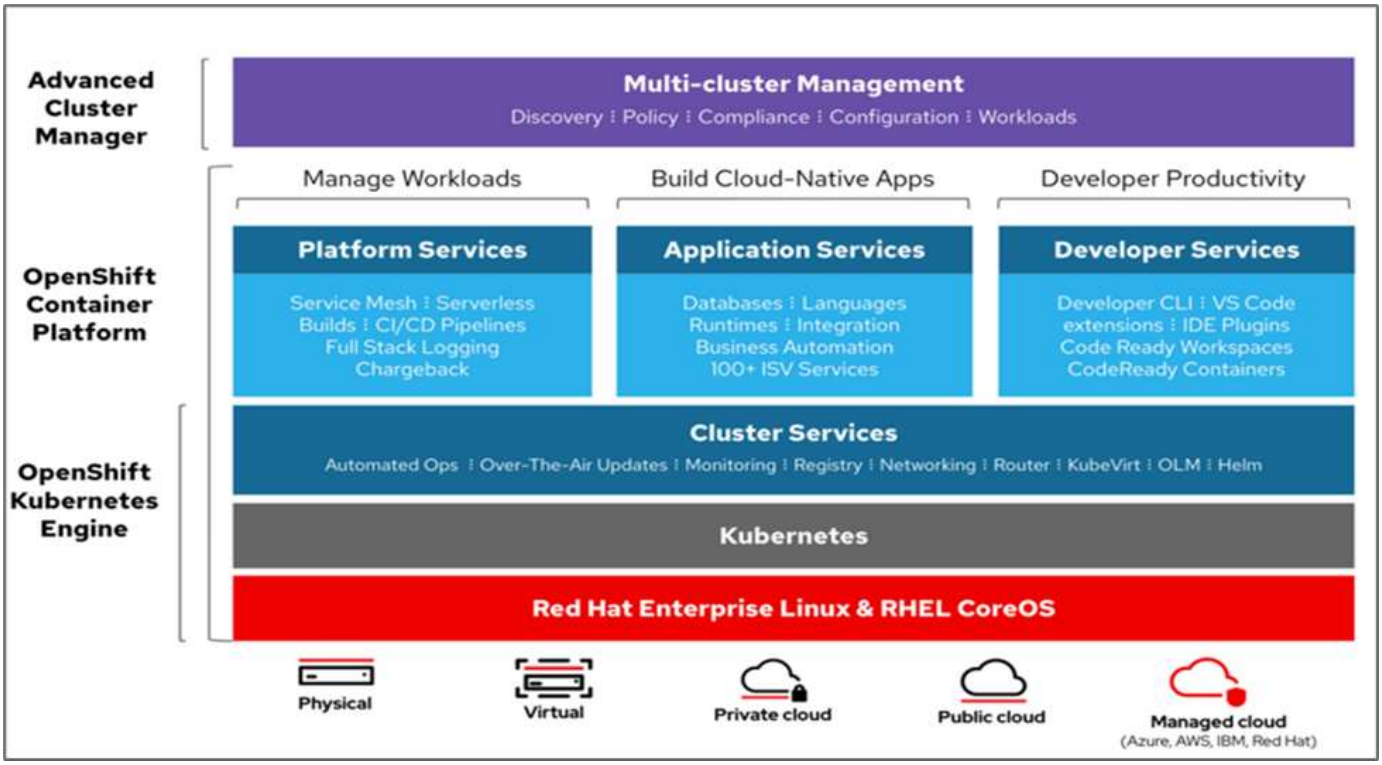
Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platformは、CRI-OとKubernetesを統合し、これらのサービスを管理するためのAPIとWebインターフェイスを提供するコンテナアプリケーションプラットフォームです。CRI-Oは、Kubernetes Container Runtime Interface（CRI）を実装したもので、Open Container Initiative（OCI）互換のランタイムを使用した実行を可能にします。Kubernetesの実行時にDockerを使用する代わりに、軽量なソリューションです。

OpenShift Container Platformにより、お客様はコンテナを作成および管理できます。コンテナは、オペレーティングシステムや基盤のインフラとは無関係に、それぞれの環境で実行されるスタンドアロンプロセスです。OpenShift Container Platformは、コンテナベースのアプリケーションの開発、導入、管理を支援します。アプリケーションをオンデマンドで作成、変更、および導入できるセルフサービスプラットフォームを提供し、開発とリリースのライフサイクルを短縮します。OpenShift Container Platformには、より小規模で分離されたユニットで構成されるマイクロサービスベースのアーキテクチャがあり、連携して機能します。Kubernetesクラスタ上で実行され、信頼性の高いクラスタキーバリュー型データストアであるetcdに格納

されているオブジェクトに関するデータが含まれます。

次の図は、Red Hat OpenShift Containerプラットフォームの概要を示しています。



Kubernetesインフラ

Kubernetesは、OpenShift Container Platform内で、コンテナ化されたアプリケーションを一連のCRI-Oランタイムホスト全体で管理し、導入、メンテナンス、アプリケーション拡張のためのメカニズムを提供します。CRI-Oサービスは、コンテナ化されたアプリケーションをインスタンス化し、実行します。

Kubernetesクラスタは、1つ以上のマスターノードと一連のワーカーノードで構成されます。この解決策 設計には、ハードウェアのハイアベイラビリティ（HA）機能とソフトウェアスタックが含まれています。Kubernetesクラスタは、3つのマスターノードと最低2つのワーカーノードでHAモードで実行されるように設計されており、クラスタに単一点障害がないようにします。

Red Hatコア**OS**

OpenShift Container Platformは、Red Hat Enterprise Linux CoreOS（RHCOS）を使用します。RHCOSは、CoreOSとRed Hat Atomic Host OSの優れた機能を組み合わせたコンテナ指向のオペレーティングシステムです。RHCOSは、コンテナ化されたアプリケーションをOpenShift Container Platformから実行できるように特別に設計されており、新しいツールと連携して、迅速なインストール、オペレータベースの管理、簡単なアップグレードを実現します。

RHCOSには次の機能があります。

- イグニションは、最初にマシンを起動して構成する際に、OpenShift Container Platformが最初のブートシステム構成として使用するものです。
- Kubernetesネイティブのコンテナランタイム実装であるCRI-Oは、オペレーティングシステムと緊密に統合して、Kubernetes環境を効率的かつ最適化します。CRI-Oには、コンテナの実行、停止、再起動を行う機能があります。これは、OpenShift Container Platform 3で使用されていたDocker Container Engineに完

全に代わるものです。

- Kubernetesの主要ノードエージェントであるKubeletはコンテナの起動と監視を担当しています。

VMware vSphere 7.0

VMware vSphereは、大量のインフラ（CPU、ストレージ、ネットワークなどのリソース）をシームレスで汎用性に優れた動的な運用環境として包括的に管理する仮想化プラットフォームです。個々のマシンを管理する従来のオペレーティングシステムとは異なり、VMware vSphereはデータセンター全体のインフラストラクチャを集約して、必要なアプリケーションに迅速かつ動的に割り当てられるリソースを備えた単一の強力なサーバを作成します。

詳細については、を参照してください "VMware vSphere の場合"。

VMware vSphere vCenterの場合

VMware vCenter Serverでは、1つのコンソールからすべてのホストとVMを統合的に管理でき、クラスタ、ホスト、およびVMのパフォーマンス監視を集約できます。VMware vCenter Serverを使用すると、管理者は、コンピューティングクラスタ、ホスト、VM、ストレージ、ゲストOS、 仮想インフラストラクチャのその他の重要なコンポーネントVMware vCenterは、VMware vSphere環境で使用できる豊富な機能を管理します。

ハードウェアおよびソフトウェアのリビジョン

この解決策 は、で定義されている、サポートされているバージョンのソフトウェア、ファームウェア、およびハードウェアを実行している任意のFlexPod 環境に拡張できます "NetApp Interoperability Matrix Tool で確認できます" および "Cisco UCSハードウェア互換性リスト。" OpenShiftクラスタは、VMware vSphereだけでなくベアメタル方式でFlexPod にインストールされます。

複数のOpenShift（k8s）クラスタを管理するために必要なのはAstra Control Centerの1つのインスタンスだけです。各OpenShiftクラスタにはTrident CSIがインストールされています。Astra Control Centerは、このようなOpenShiftクラスタのいずれにもインストールできます。この解決策 では、OpenShiftベアメタルクラスタにAstraコントロールセンターをインストールします。

次の表に、OpenShift用のFlexPod ハードウェアおよびソフトウェアのリビジョンを示します。

コンポーネント	プロダクト	バージョン
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	4.1（3c）
	Cisco UCS B200 M5サーバ	4.1（3c）
ネットワーク	Cisco Nexus 9336C-FX2 NX-OS	9.3（8）
ストレージ	NetApp AFF A700	9.11.1
	ネットアップアストラコントロールセンター	22.04.0
	NetApp Astra Trident CSIプラグイン	22.04.0
	NetApp Active IQ Unified Manager の略	9.11
ソフトウェア	VMware ESXi nenic イーサネットドライバ	1.0.35.0

コンポーネント	プロダクト	バージョン
	vSphere ESXiの場合	7.0（U2）
	VMware vCenter Applianceの略	7.0 U2b
	Cisco Intersight Assist仮想アプライアンス	1.0.9-342
	OpenShift Container Platform	4.9
	OpenShift Container Platformマスターノード	RHCOS 4.9
	OpenShift Container Platform Workerノード	RHCOS 4.9

次の表に、AWS上のOpenShift用のソフトウェアバージョンを示します。

コンポーネント	プロダクト	バージョン
コンピューティング	マスターインスタンスタイプ：m5.xlarge	該当なし
	ワーカーインスタンスタイプ：m5.large	該当なし
ネットワーク	Virtual Private Cloud Transit Gatewayの略	該当なし
ストレージ	NetApp Cloud Volumes ONTAP の略	9.11.1
	NetApp Astra Trident CSIプラグイン	22.04.0
ソフトウェア	OpenShift Container Platform	4.9
	OpenShift Container Platformマスターノード	RHCOS 4.9
	OpenShift Container Platform Workerノード	RHCOS 4.9

"次の例：FlexPod for OpenShift Container Platform 4ベアメタルインストール"

インストールと設定

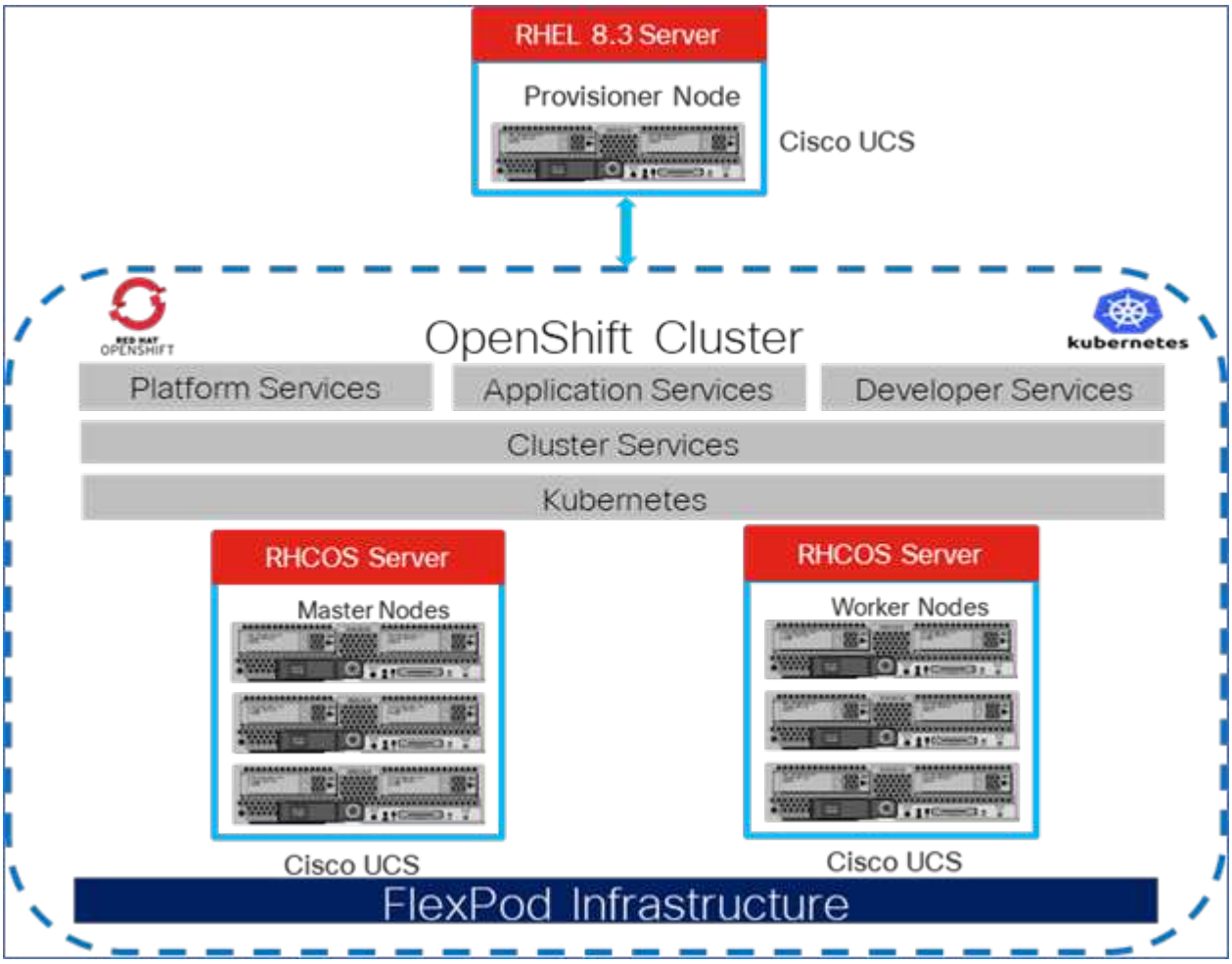
FlexPod for OpenShift Container Platform 4ベアメタルインストール

"前の図：解決策 コンポーネント。"

FlexPod for OpenShift Container Platform 4のベアメタル設計、導入の詳細、およびNetApp Astra Tridentのインストールと設定については、を参照してください "FlexPod with OpenShift Cisco Validated Design and Deploymentガイド（CVD）"。このCVDでは、Ansibleを使用したFlexPod およびOpenShift Container Platformの導入について説明します。CVDには、ワーカーノード、Astra Tridentインストール、ストレージバックエンド、ストレージクラス構成の準備に関する詳細も記載されています。この構成

は、Astra Control Centerの導入と構成を行うためのいくつかの前提条件です。

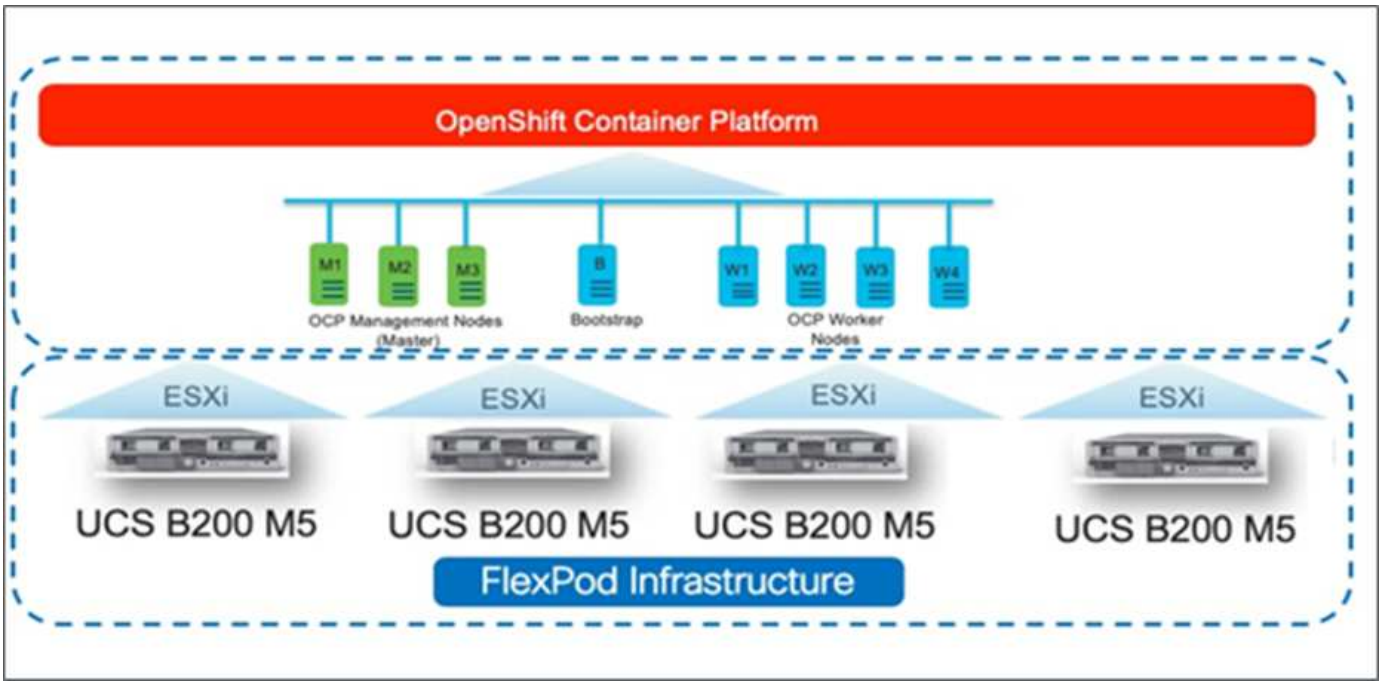
次の図は、FlexPod 上のOpenShift Container Platform 4ベアメタルを示しています。



VMware環境に実装された**OpenShift Container Platform 4**用**FlexPod**

VMware vSphereを実行しているFlexPod にRed Hat OpenShift Container Platform 4を導入する方法については、を参照してください "OpenShift Container Platform 4のFlexPod データセンター"。

次の図は、vSphere上のOpenShift Container Platform 4のFlexPod を示しています。

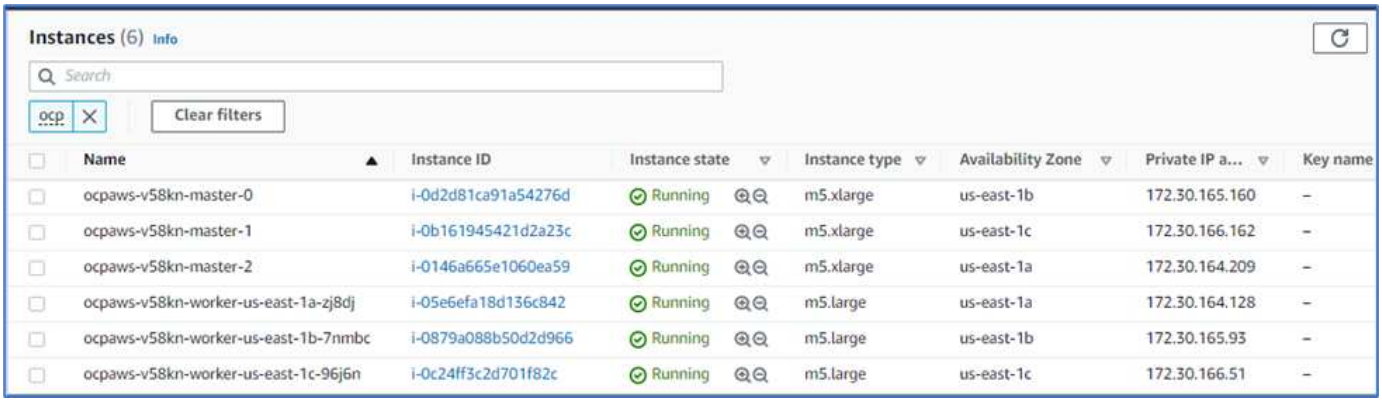


"次の例は、AWSでRed Hat OpenShiftを実装したものです。"

AWSに**Red Hat OpenShift**を実装しました

"従来：FlexPod for OpenShift Container Platform 4ベアメタルインストール"

DRサイトとしてAWSに実装された、独立した自己管理OpenShift Container Platform 4クラスタです。マスターノードとワーカーノードは、3つのアベイラビリティゾーンにまたがって配置されるため、高可用性が実現します。



Instances (6) Info

Search

ocp ✕ Clear filters

Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name
ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	–
ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	–
ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	–
ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	–
ocpaws-v58kn-worker-us-east-1b-7nmbc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	–
ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	–

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal      Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal      Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal      Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal       Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal      Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal       Ready    worker   28m   v1.22.8+f34b40c
```

OpenShiftはとして導入されます "プライベートクラスタ" AWS上の既存のVPCに接続できます。プライベートOpenShift Container Platformクラスタは外部エンドポイントを公開しないため、内部ネットワークからのみアクセスでき、インターネットには表示されません。シングルノードのNetApp Cloud Volumes ONTAPは、NetApp Cloud Managerを使用して導入されます。これにより、TridentからAstraにバックエンドとしてストレージが提供されます。

AWSへのOpenShiftのインストールの詳細については、を参照してください "OpenShiftのドキュメント"。

"次のステップ：NetApp Cloud Volumes ONTAP"

NetApp Cloud Volumes ONTAP の略

"以前は、AWSでRed Hat OpenShiftを利用していました。"

NetApp Cloud Volumes ONTAP インスタンスはAWSに導入され、Astra Tridentのバックエンドストレージとして機能します。Cloud Volumes ONTAP 作業環境を追加する前に、コネクタを配置する必要があります。コネクタを配置せずにCloud Volumes ONTAP の最初の作業環境を作成するかどうかを確認するメッセージが表示されます。AWSにコネクタを導入するには、を参照してください "コネクタを作成します"。

AWSにCloud Volumes ONTAP を導入する手順については、を参照してください "AWSでのクイックスタート"。

Cloud Volumes ONTAP を導入したら、Astra Tridentをインストールし、OpenShift Container Platformクラスタでストレージバックエンドとスナップショットクラスを設定できます。

"次は、OpenShift Container PlatformにAstra Control Centerをインストールする方法です。"

OpenShift Container Platformに**Astra Control Center**をインストールします

"Previous：NetApp Cloud Volumes ONTAP の略。"

FlexPod で実行されているOpenShiftクラスタ、またはCloud Volumes ONTAP ストレージバックエンドを使用するAWSにAstraコントロールセンターをインストールできます。この解決策 では、OpenShiftベアメタルクラスタにAstraコントロールセンターを導入します。

Astra Control Centerは、説明されている標準的なプロセスを使用してインストールできます "こちらをご覧ください" または、Red Hat OpenShift OperatorHubから入手してください。Astra Control Operatorは、Red Hat

認定オペレータです。この解決策 では、AstraコントロールセンターはRed Hat OperatorHubを使用してインストールされます。

環境要件

- Astra Control Centerは複数のKubernetesディストリビューションをサポートします。Red Hat OpenShiftでは、Red Hat OpenShift Container Platform 4.8または4.9がサポートされます。
- Astra Control Centerでは、環境およびエンドユーザーのアプリケーションリソース要件に加えて、次のリソースが必要です。

コンポーネント	要件
ストレージバックエンドの容量	500GB以上の容量があります
ワーカーノード	少なくとも3つのワーカーノードがあり、それぞれ4つのCPUコアと12GBのRAMが搭載されています
Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）アドレス	Astra Control Center の FQDN アドレス
Astra Trident	Astra Trident 21.04 以降がインストールおよび設定されている
入力コントローラまたはロードバランサ	入力コントローラでURLまたはロードバランサを使用してAstra Control Centerを公開し、FQDNに解決されるIPアドレスを提供するように設定します

- 既存のプライベートイメージレジストリが必要です。このレジストリには、Astra Control Centerビルドイメージをプッシュできます。イメージをアップロードするイメージレジストリのURLを指定する必要があります。

> 一部のイメージは特定のワークフローの実行中にプルされ、必要に応じてコンテナが作成および破棄されます。

- Astra Control Center を使用するには、ストレージクラスを作成してデフォルトのストレージクラスとして設定する必要があります。Astra Control Center は、 Astra Trident が提供する次の ONTAP ドライバをサポートしています。
  - ONTAP - NAS
  - ONTAP-NAS-flexgroup
  - ONTAP - SAN
  - ONTAP - SAN - 経済性

> 導入したOpenShiftクラスタにAstra Tridentがインストールされ、ONTAP バックエンドで設定されているとします。また、デフォルトのストレージクラスも定義されています。

- OpenShift環境でアプリケーションクローニングを行う場合、Astra Control CenterはOpenShiftでボリュームをマウントし、ファイルの所有権を変更できるようにする必要があります。これらの処理を許可するようにONTAP エクスポートポリシーを変更するには、次のコマンドを実行します。

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

管理対象のコンピューティングリソースとして2つ目のOpenShift運用環境を追加するには、Astra Tridentボリュームスナップショット機能が有効になっていることを確認します。Tridentを使用してボリュームSnapshotを有効にし、テストする方法については、を参照してください "Astra Tridentの手順"。

- A "VolumeSnapClass" アプリケーションの管理元であるすべてのKubernetesクラスタで設定する必要があります。Astra Control Centerがインストールされているkubernetesクラスタも含めることができます。Astra Control Centerでは、実行中のKubernetesクラスタ上のアプリケーションを管理できます。

アプリケーション管理の要件

- ライセンス。 Astra Control Centerを使用してアプリケーションを管理するには、Astra Control Centerライセンスが必要です。
- *名前空間。*名前空間は、Astra Control Centerによってアプリケーションとして管理できる最大のエンティティです。既存のネームスペース内のアプリケーションラベルとカスタムラベルに基づいてコンポーネントを除外し、リソースのサブセットをアプリケーションとして管理できます。
- * StorageClass.* StorageClassが明示的に設定されたアプリケーションをインストールし、アプリケーションのクローンを作成する必要がある場合、クローン処理のターゲットクラスタに最初に指定されたStorageClassが必要です。明示的にStorageClassを設定したアプリケーションを、同じストレージクラスを持たないクラスタにクローニングすると失敗します。
- * Kubernetesのリソース。* Astra ControlではキャプチャされないKubernetesリソースを使用するアプリケーションには、アプリケーションデータの完全な管理機能が備わっていない可能性があります。Astra Controlでは、次のKubernetesリソースをキャプチャできます。

Kubernetesのリソース		
クラスタロール	ClusterRoleBinding	ConfigMap
CustomResourceDefinition の場合	CustomResource の場合	cronjob
デモンセット（ DemonSet ）	HorizontalPodAutoscaler のように表示されます	入力
DeploymentConfig	MutingWebhook	PersistentVolumeClaim のように表示され
ポッド	PodDisruptionBudget （予算の廃止）	PodTemplate
ネットワークポリシー	ReplicaSet	ロール
RoleBinding です	ルート	秘密
検証 Webhook		

OpenShift OperatorHub を使用して **Astra Control Center** をインストールします

次の手順 は、Red Hat OperatorHubを使用してAstraコントロールセンターをインストールします。この解決策 では、FlexPod 上で動作するベアメタルOpenShiftクラスタにAstraコントロールセンターをインストールします。

1. から Astra Control Center バンドル（「Astra - control-ccenter-[version].tar.gz`）をダウンロードします "NetApp Support Site"。
2. からAstra Control Centerの証明書とキーの.zipファイルをダウンロードします "NetApp Support Site"。
3. バンドルの署名を確認します。

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Astraの画像を抽出します。

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Astra ディレクトリに移動します。

```
cd astra-control-center-[version]
```

6. イメージをローカルレジストリに追加します。

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. 適切なスクリプトを使用して、イメージをロードし、イメージにタグを付け、ローカルレジストリにプッシュします。

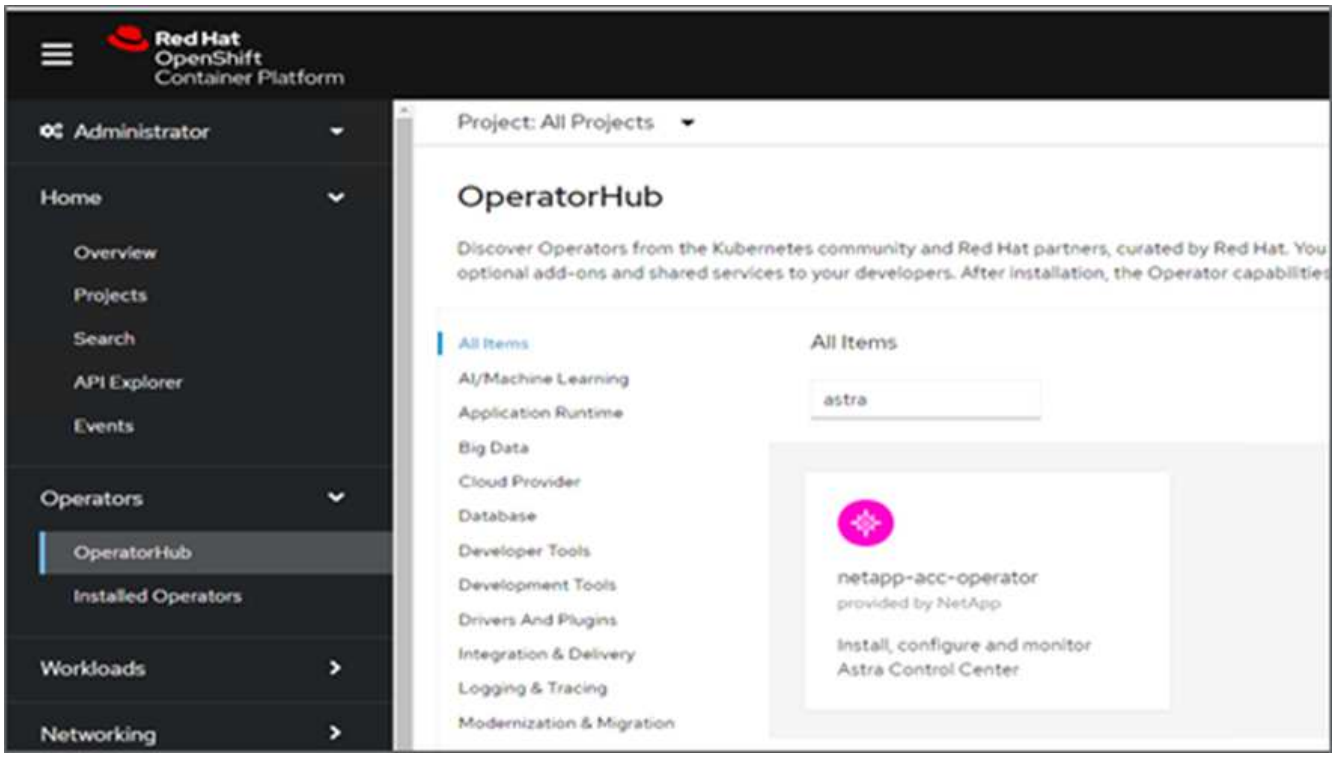
   Docker の場合：

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

Podman の場合：

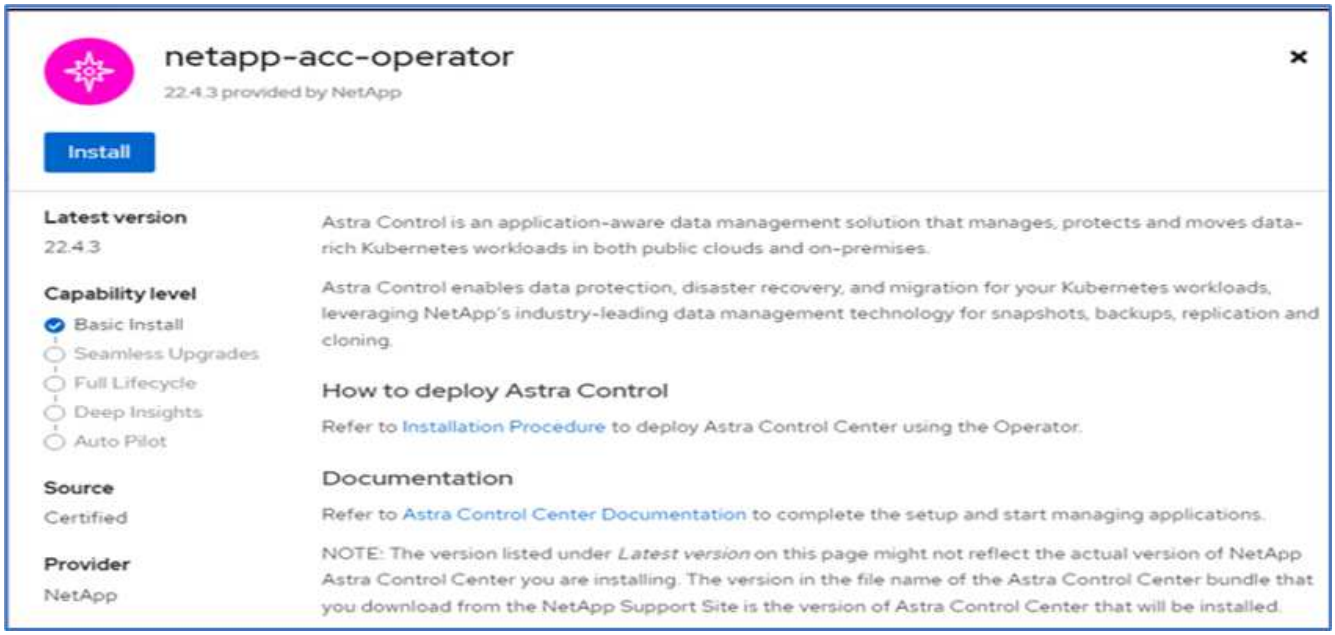
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. ベアメタルOpenShiftクラスタのWebコンソールにログインします。サイドメニューから、[演算子]>[演算子ハブ]を選択します。「stra」と入力して、「NetApp-acc-operator」のリストを表示します。

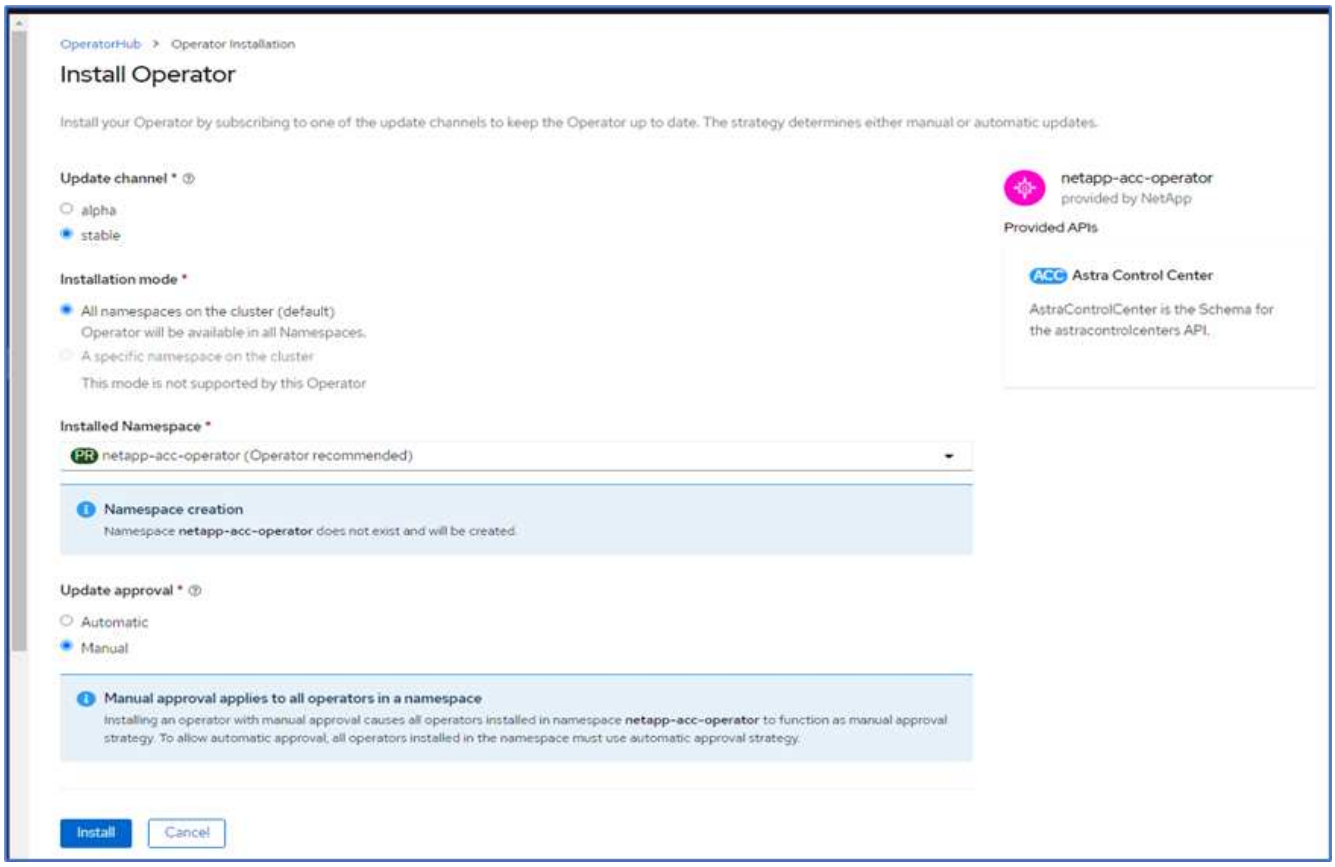


「NetApp-acc-operator」は、Red Hat OpenShift Operatorの認定を受けたもので、OperatorHubカタログの下にリストされています。

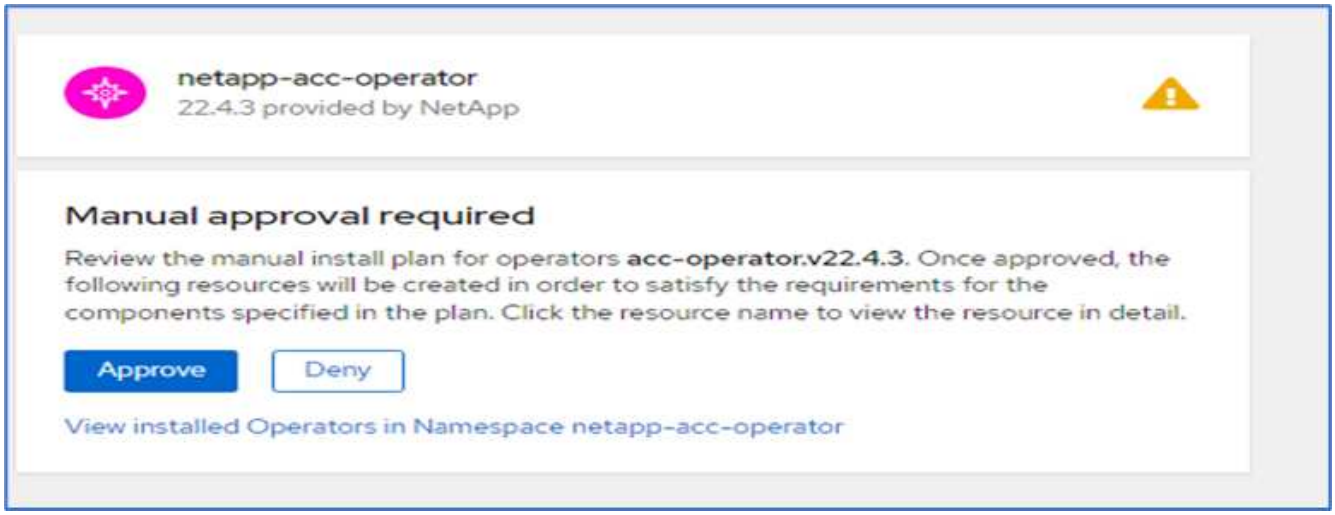
9. 「NetApp-acc-operator」を選択し、「Install」をクリックします。



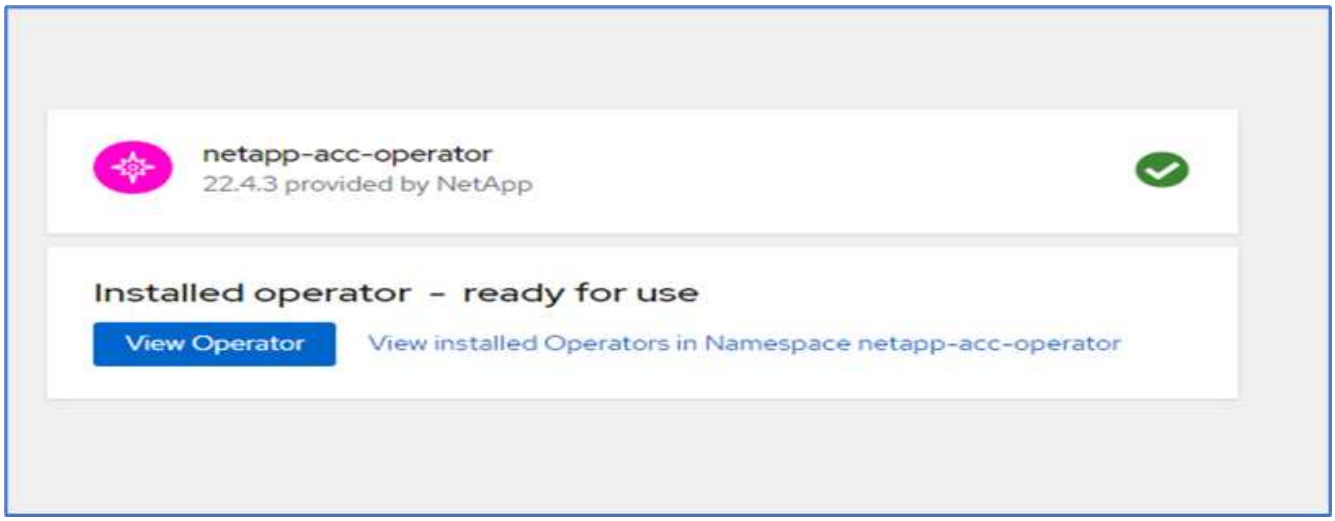
10. 適切なオプションを選択し、[インストール]をクリックします。



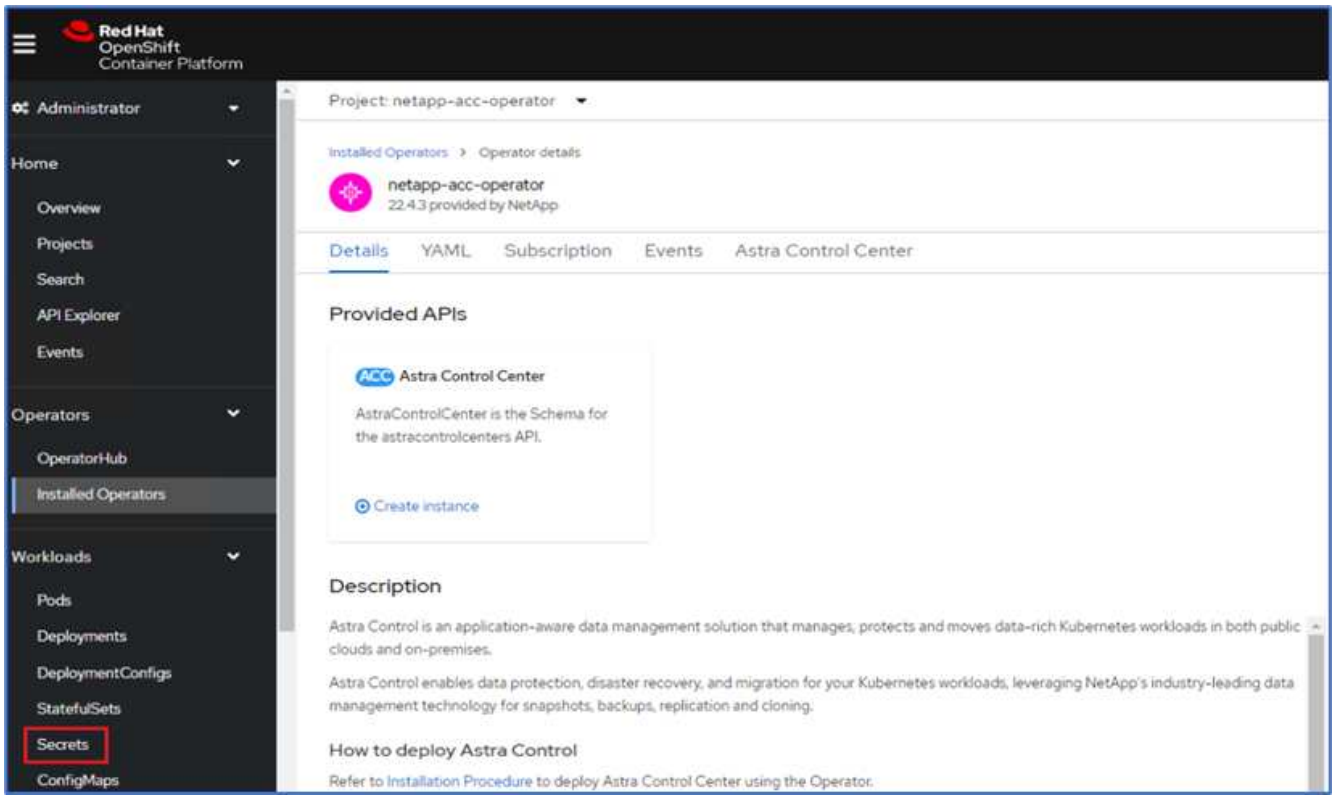
11. インストールを承認し、オペレータがインストールされるまで待ちます。



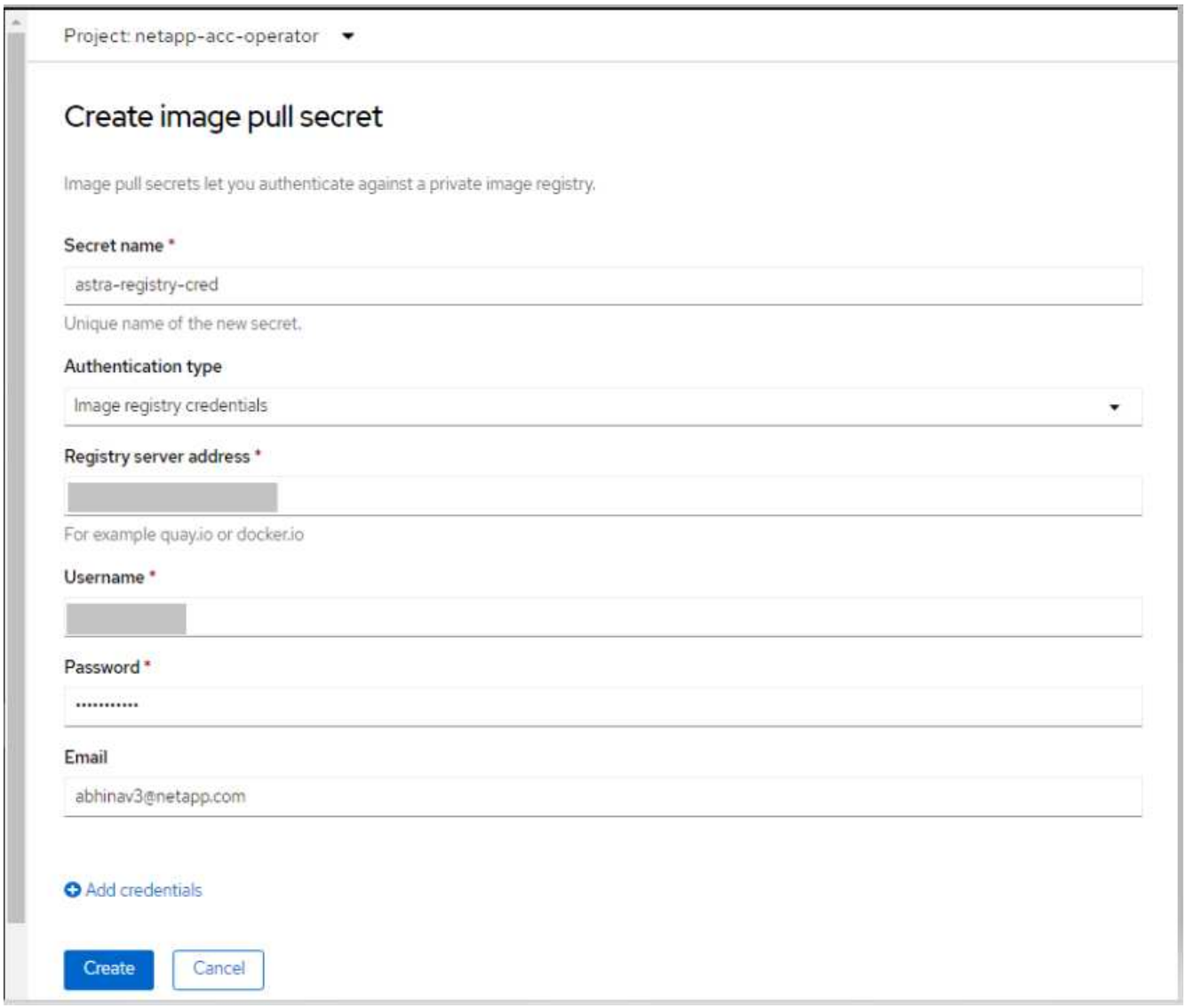
12. この段階で、オペレータは正常にインストールされ、使用可能な状態になります。View Operator（オペレーターの表示）をクリックして、Astra Control Centerのインストールを開始します。



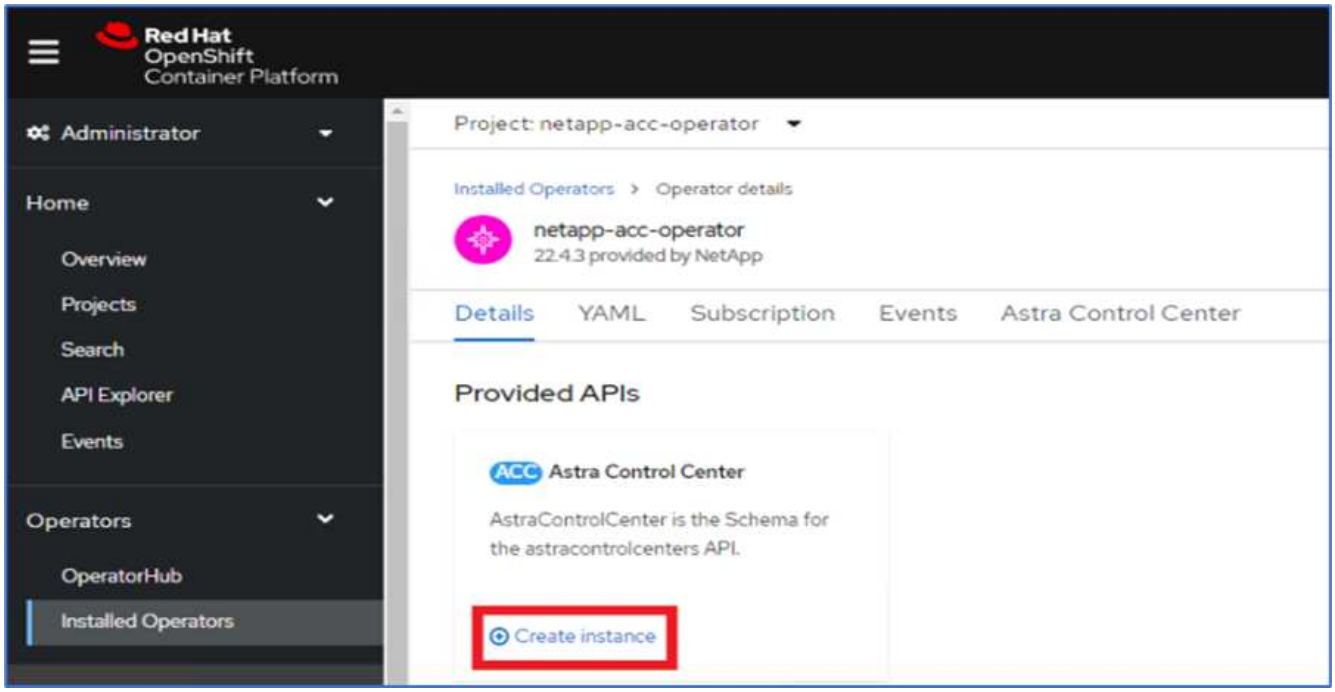
13. Astra Control Centerをインストールする前に、事前にプッシュしたDockerレジストリからAstraイメージをダウンロードするプルシークレットを作成します。



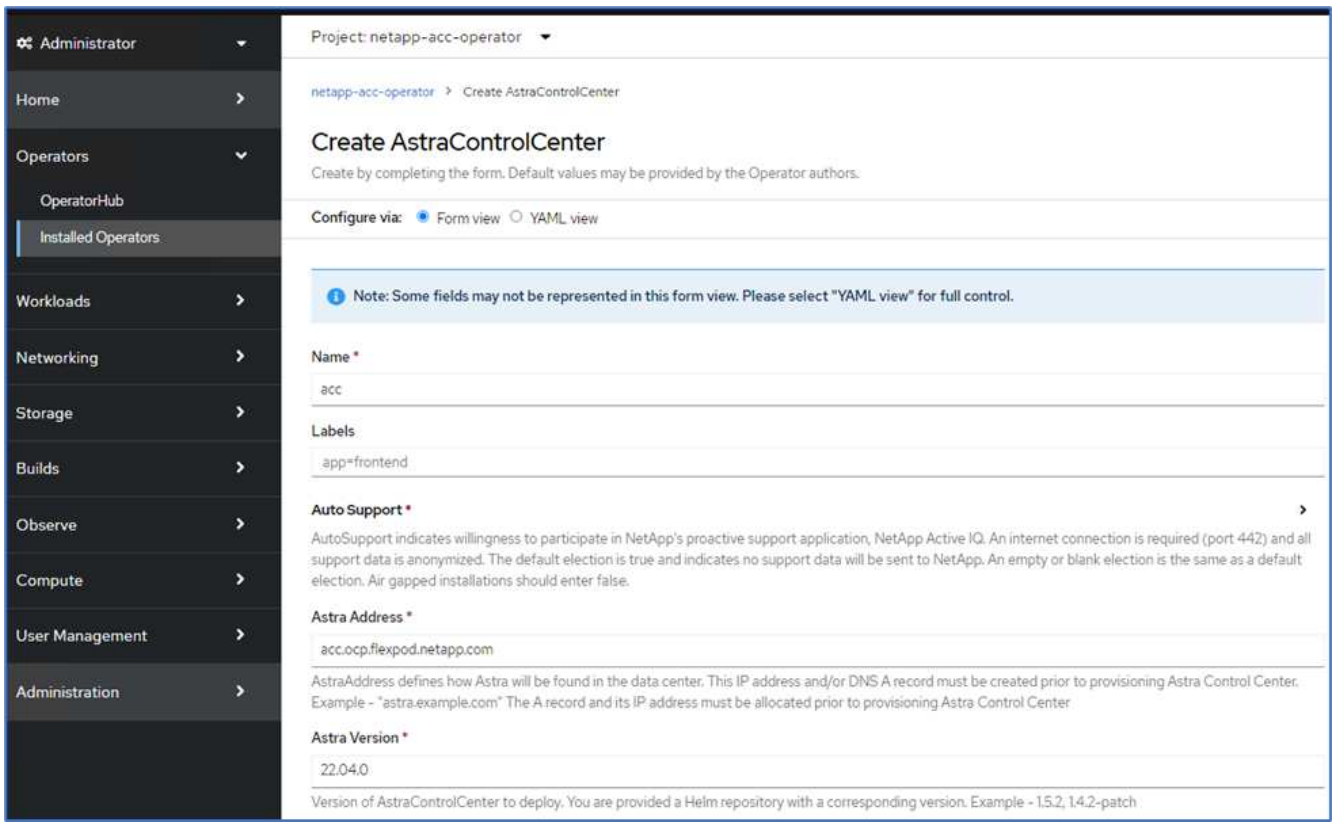
14. Astra Control CenterのイメージをDocker private repoから取得するには、NetApp-acc-operator'ネームスペースにシークレットを作成します。このシークレット名は、後の手順でAstra Control Center YAMLマニフェストに表示されます。



15. サイドメニューから、[演算子]>[インストールされた演算子]を選択し、[提供されたAPI]セクションの下にある[インスタンスの作成]をクリックします。



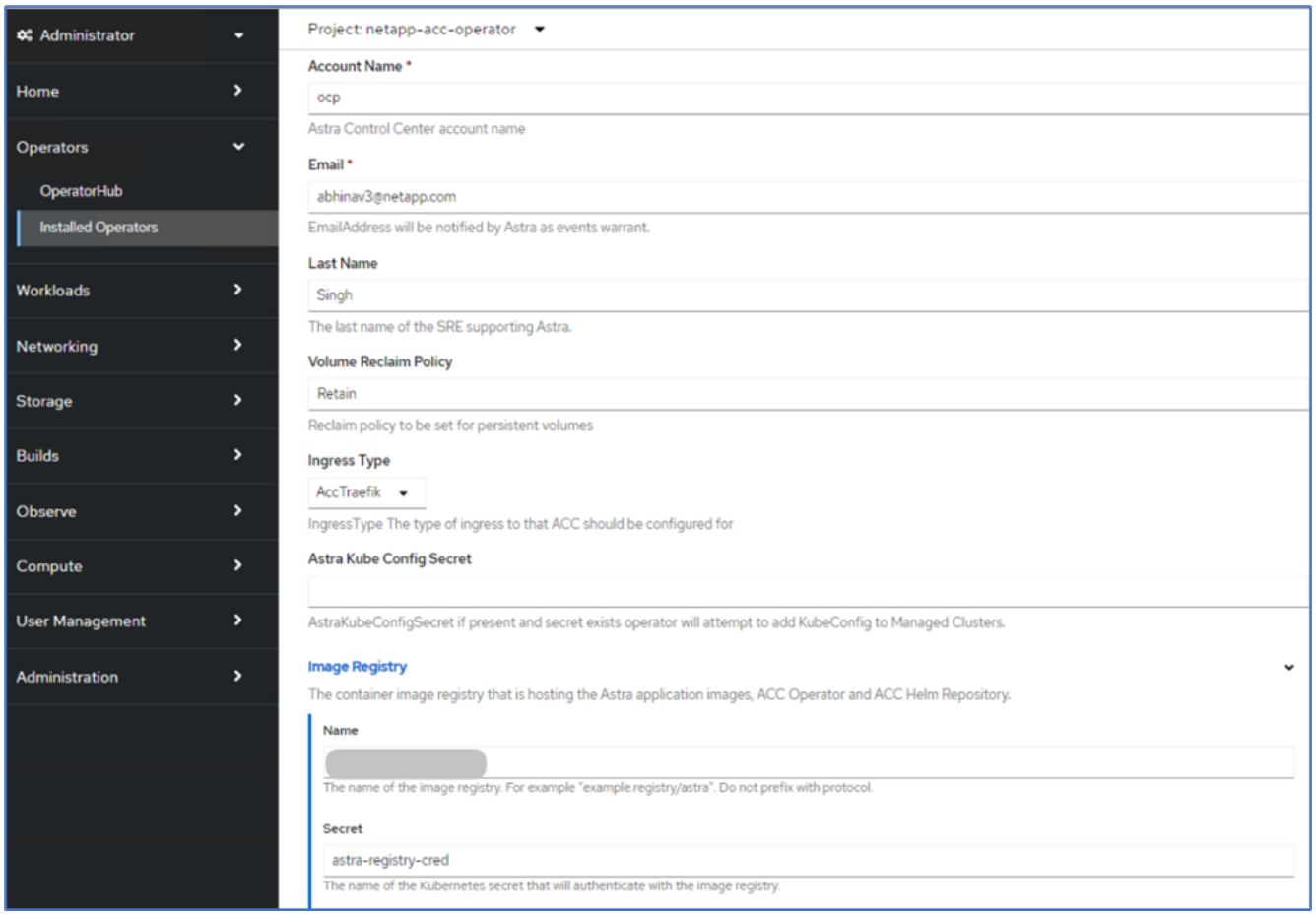
16. Create AstraControlCenterフォームに入力します名前、Astraアドレス、Astraバージョンを入力します。



> [Astra Address]で、Astra Control CenterのFQDNアドレスを入力します。このアドレスは、Astra Control CenterのWebコンソールにアクセスするために使用されます。FQDNは、到達可能なIPネットワークにも解決される必要があり、DNSで設定する必要があります。

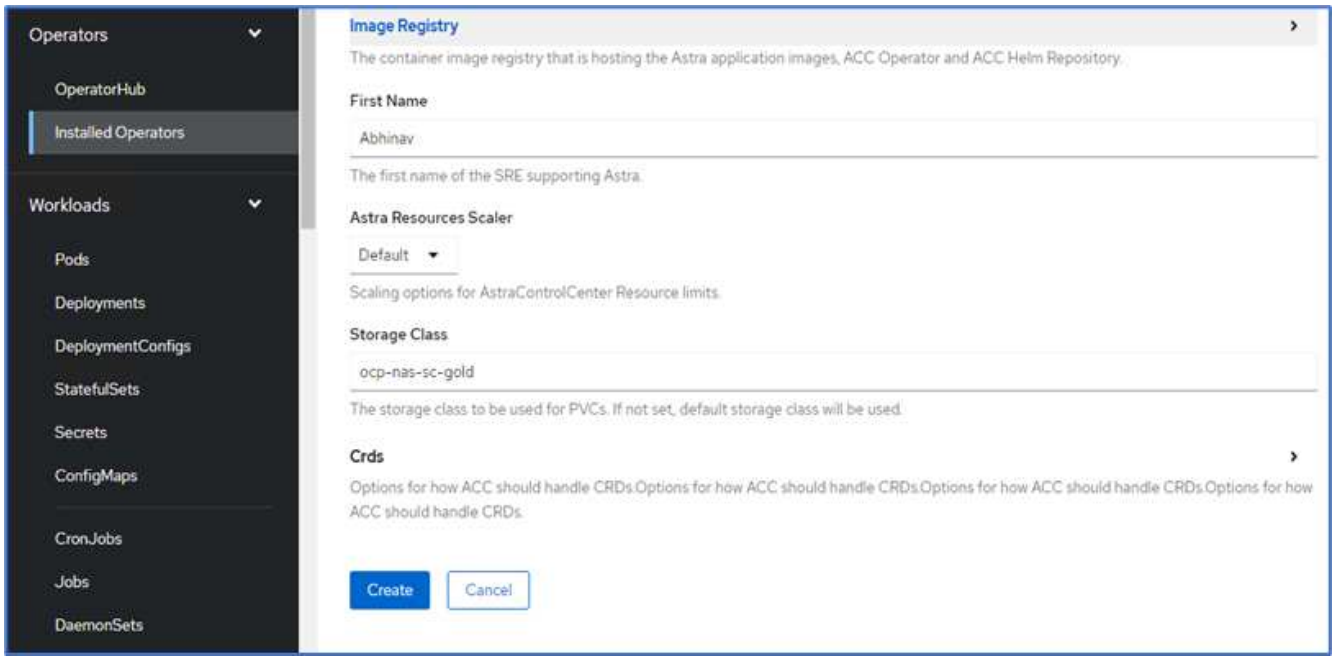
17. アカウント名、Eメールアドレス、管理者の姓を入力し、デフォルトのボリューム再利用ポリシーをその

まま使用します。ロードバランサを使用している場合は、入力タイプを「AccTraefik」に設定します。それ以外の場合は、「Ingress .Controller」で「Generic」を選択します。イメージレジストリで、コンテナイメージのレジストリパスとシークレットを入力します。

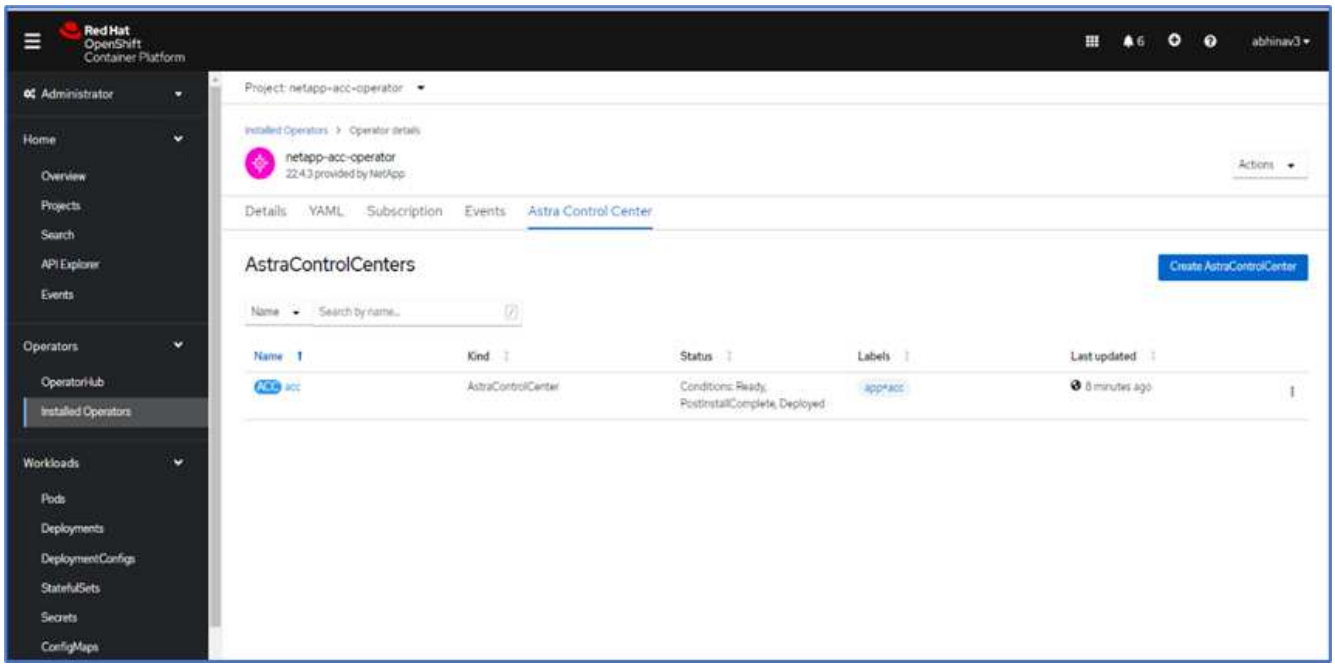


この解決策 では、Metallbロードバランサが使用されます。したがって、入力タイプはAccTraefikです。これにより、Astra Control Center traefikゲートウェイが、LoadBalancerタイプのKubernetesサービスとして公開されます。

18. 管理者の名を入力し、リソースの拡張を設定して、ストレージクラスを指定します。Create をクリックします。 .



Astra Control Centerインスタンスのステータスは、[Deploying]から[Ready]に変わります。



19. すべてのシステムコンポーネントが正常にインストールされ、すべてのポッドが実行されていることを確認します。

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                                READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                      1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn    2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

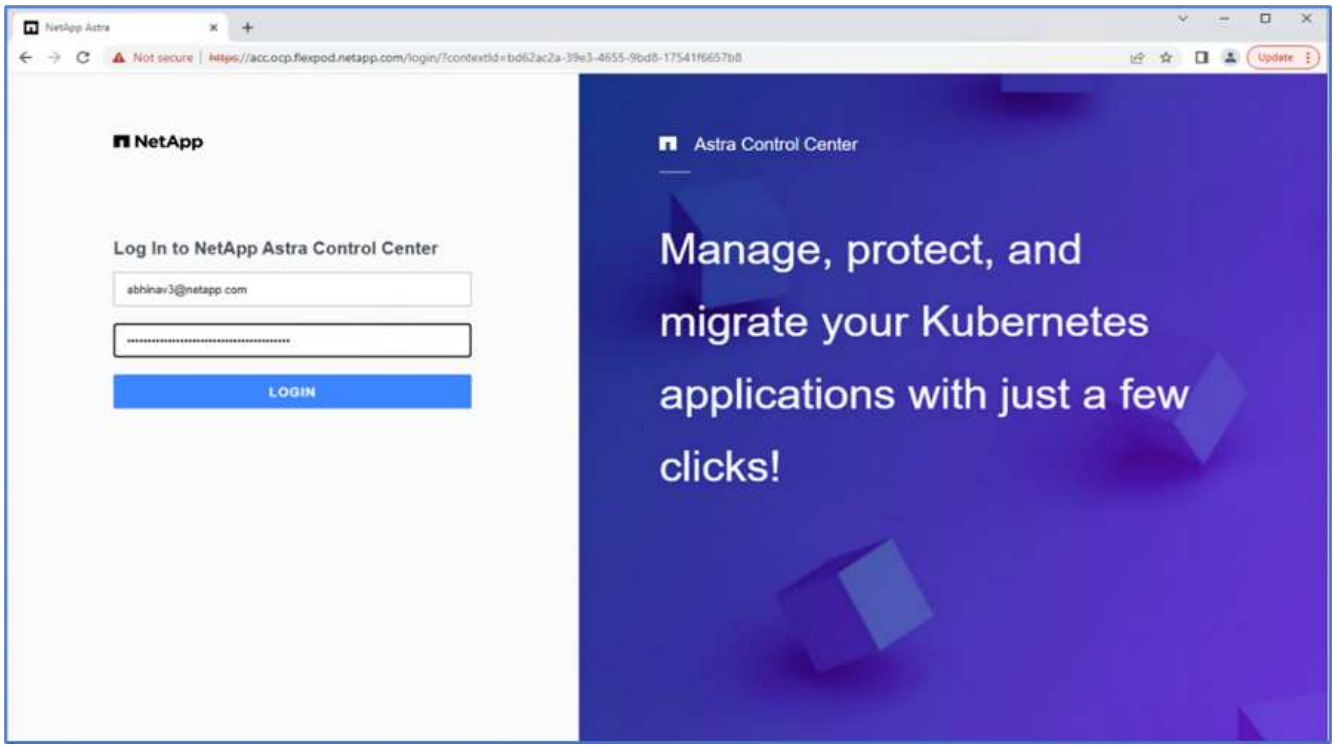
```
polaris-vault-0                                     1/1     Running   0
9m18s
polaris-vault-1                                     1/1     Running   0
9m18s
polaris-vault-2                                     1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                     1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j            1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                    1/1     Running   0
5m25s
telegraf-ds-4zqgz                                   1/1     Running   0
3m36s
telegraf-ds-cp9x4                                   1/1     Running   0
3m36s
telegraf-ds-h4n59                                   1/1     Running   0
3m36s
telegraf-ds-jnp2q                                   1/1     Running   0
3m36s
telegraf-ds-pdz5j                                   1/1     Running   0
3m36s
telegraf-ds-znqtp                                   1/1     Running   0
3m36s
telegraf-rs-rt64j                                   1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                  1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                             1/1     Running   0
6m37s
traefik-6548496576-5v2g6                            1/1     Running   0
98s
traefik-6548496576-g82pq                            1/1     Running   0
3m8s
traefik-6548496576-psn49                            1/1     Running   0
38s
traefik-6548496576-qrkfd                            1/1     Running   0
2m53s
traefik-6548496576-srs6r                            1/1     Running   0
98s
trident-svc-679856c67-78kbt                         1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                   1/1     Running   0
7m37s
```

各ポッドのステータスが「Running」である必要があります。システムのポッドが導入されるまでに数分かかることがあります。

20. すべてのポッドが実行中の場合は、次のコマンドを実行して1回限りのパスワードを取得します。出力のYAMLバージョンで、「status.deploymentState`」フィールドで展開された値を確認し、「status.uuid」値をコピーします。パスワードは「ACC-」で、その後にUUID値が続きます。（ACC -[UUID]）。

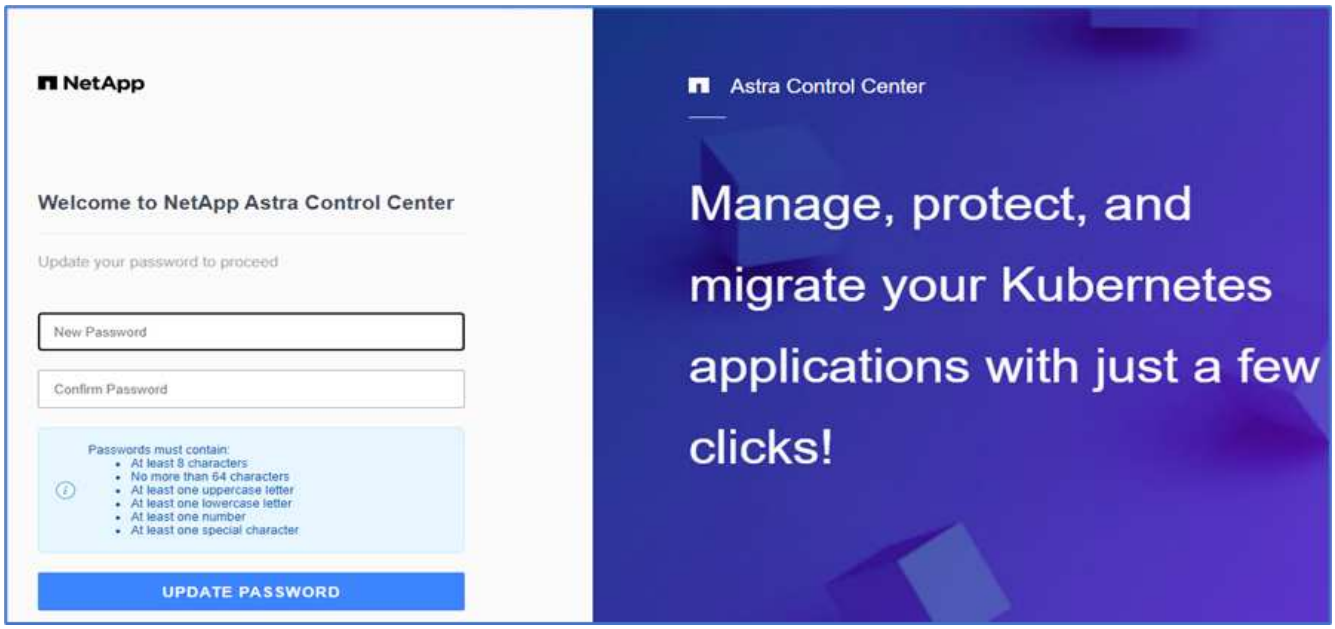
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. ブラウザで、指定したFQDNを使用してURLに移動します。
22. デフォルトのユーザ名（インストール時に指定したEメールアドレス）とワンタイムパスワードACC-[UUID]を使用してログインします。



誤ったパスワードを3回入力すると、管理者アカウントは15分間ロックされます。

23. パスワードを変更して次に進みます。

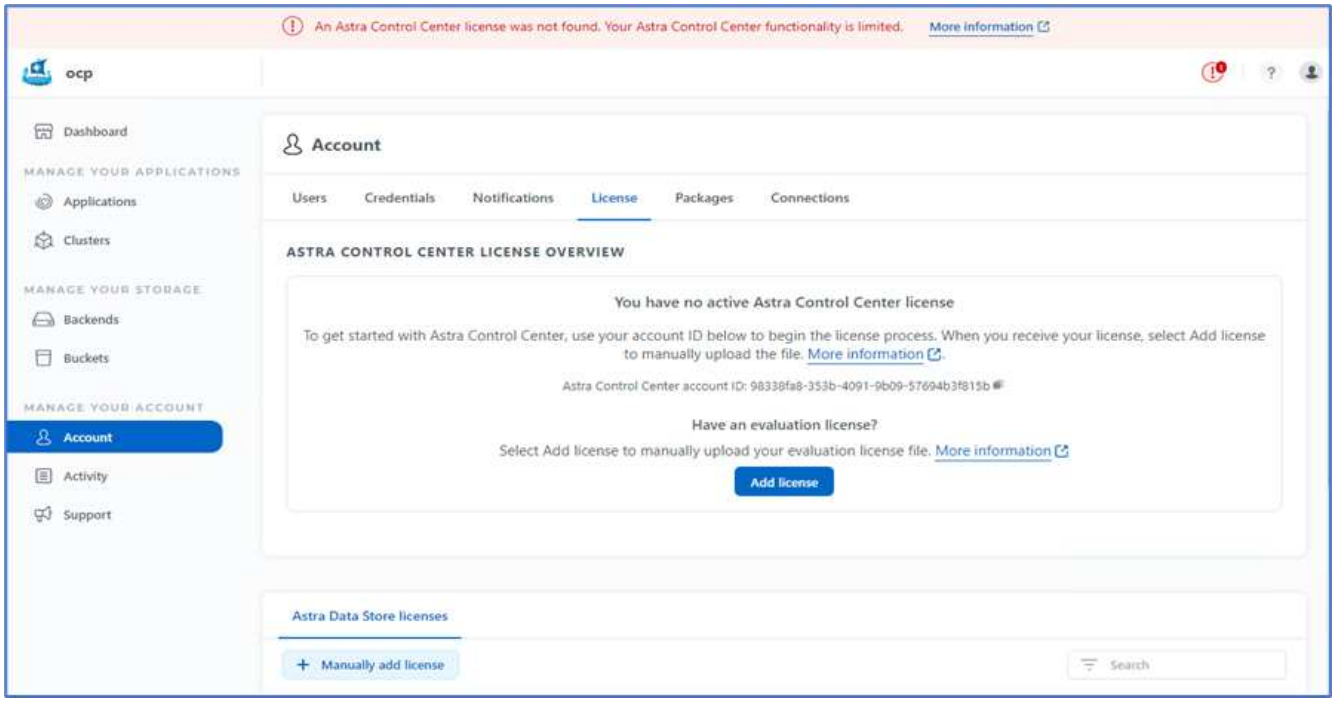


Astra Control Centerのインストールの詳細については、を参照してください "Astra Control Centerのインストールの概要" ページ

Astra Control Center をセットアップします

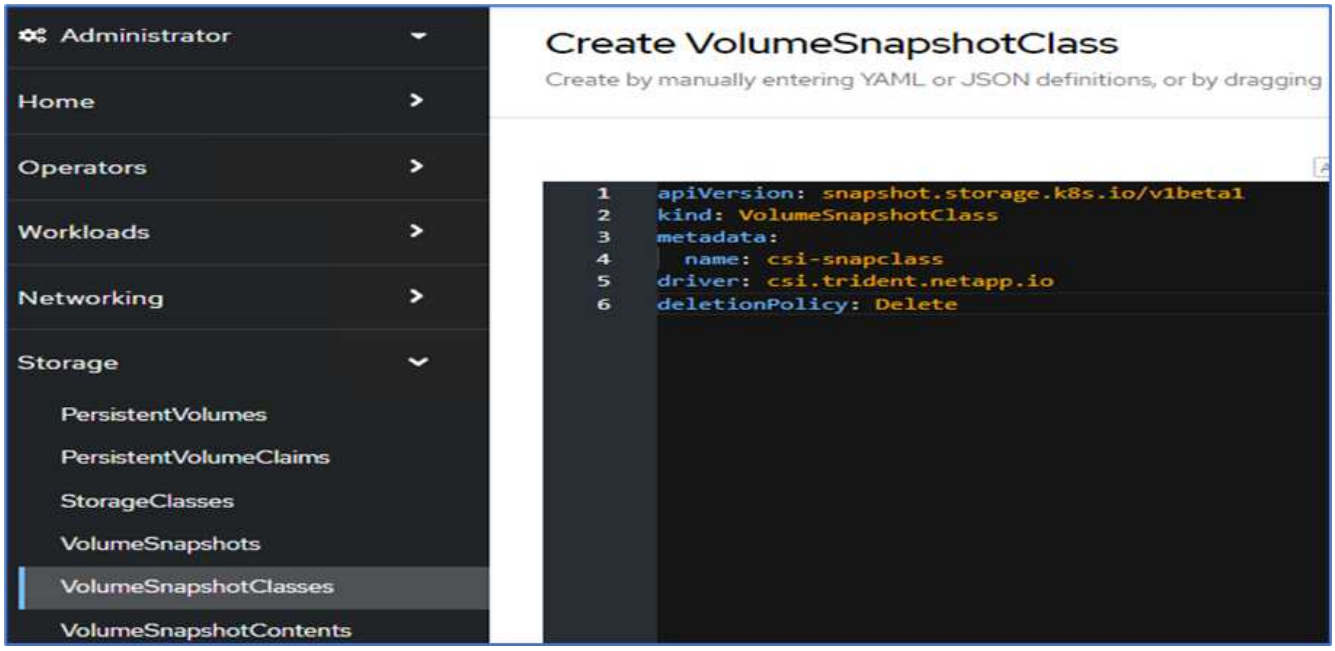
Astra Control Centerをインストールしたら、UIにログインし、ライセンスのアップロード、クラスタの追加、ストレージの管理、バケットの追加を行います。

1. [アカウント]の下のホームページで、[ライセンス]タブに移動し、[ライセンスの追加]を選択してAstraライセンスをアップロードします。

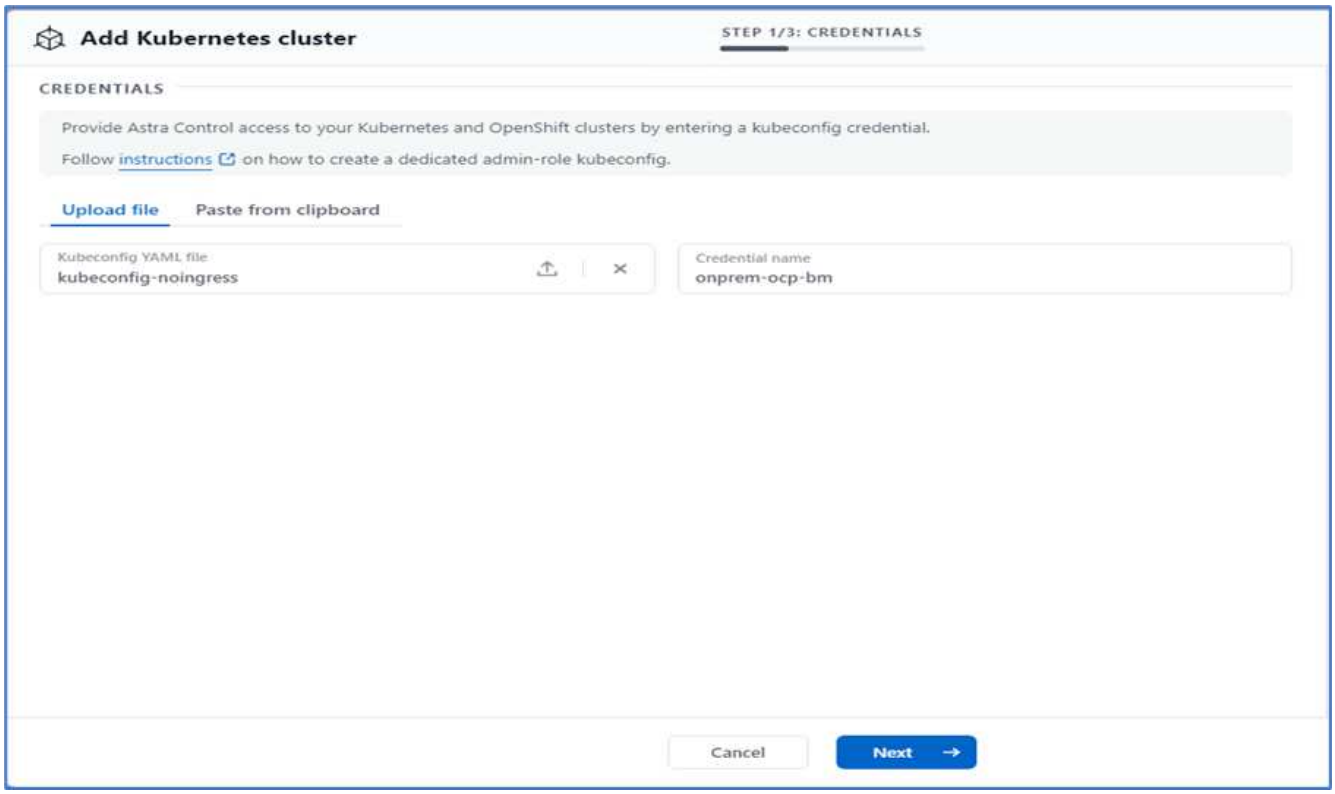


2. OpenShiftクラスタを追加する前に、OpenShift WebコンソールからAstra Tridentボリュームスナップショットクラスを作成します。Volumeスナップショット・クラスには'csi.trident.netapp.io`ドライバが設定さ

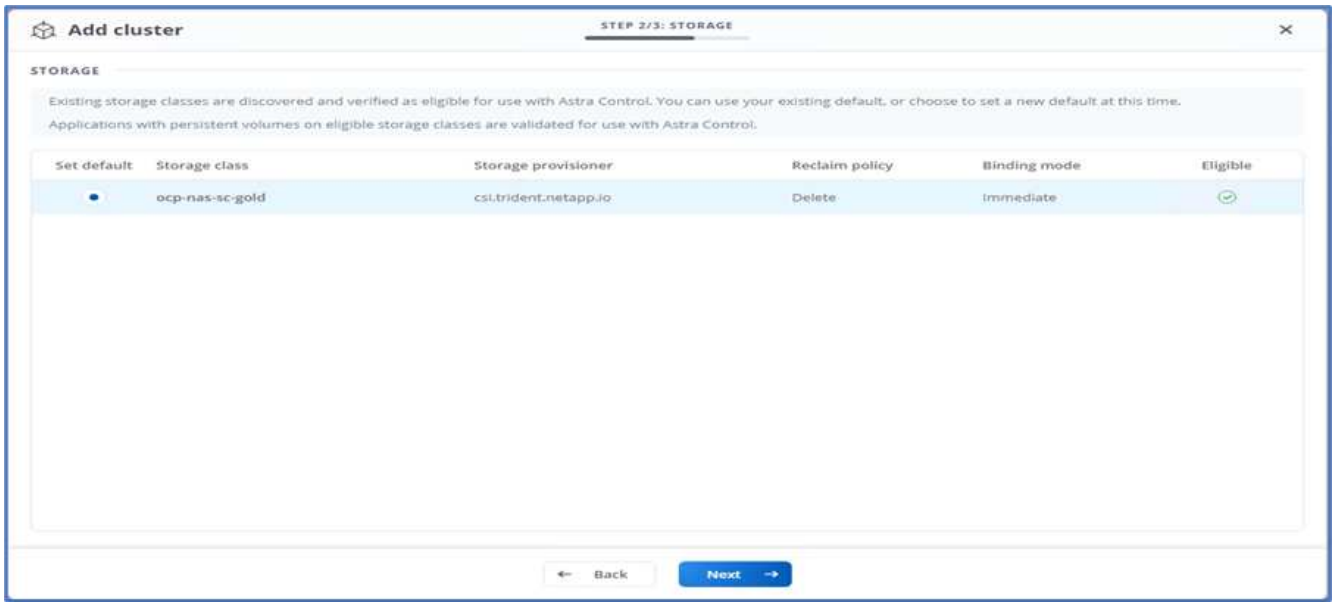
れています



3. Kubernetesクラスタを追加するには、ホームページでクラスタに移動し、Kubernetesクラスタを追加をクリックします。次に、クラスタの「kubeconfig」ファイルをアップロードし、クレデンシャル名を指定します。次へをクリックします。



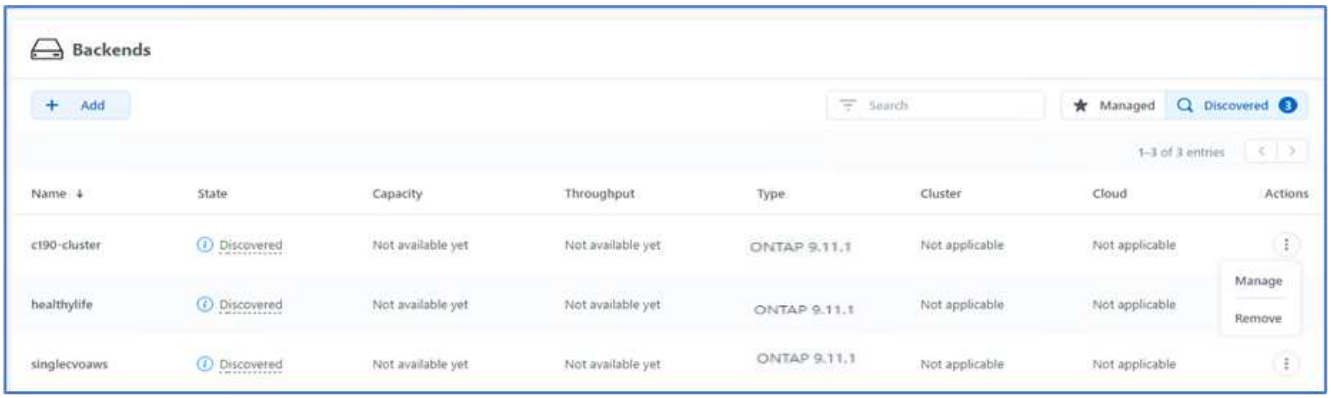
4. 既存のストレージクラスは自動的に検出されます。デフォルトのストレージクラスを選択し、Next（次へ）をクリックし、Add cluster（クラスタの追加）をクリックします。



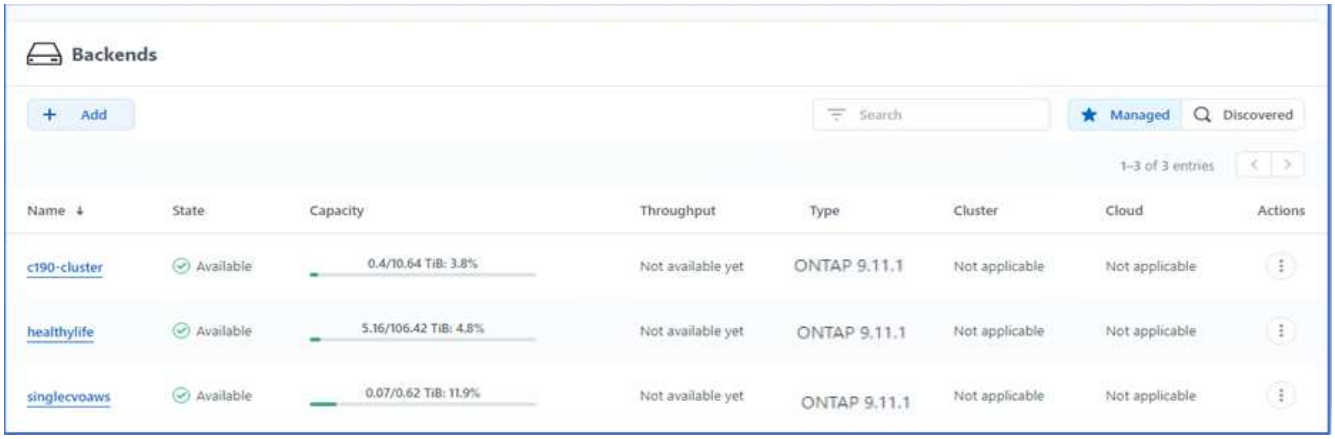
5. クラスタは数分で追加されます。OpenShift Container Platformクラスタを追加するには、手順1~4を繰り返します。

> 管理対象のコンピューティングリソースとしてOpenShift運用環境を追加するには、Astra Tridentを実行してください "VolumeSnapshotClassオブジェクト" が定義されている。

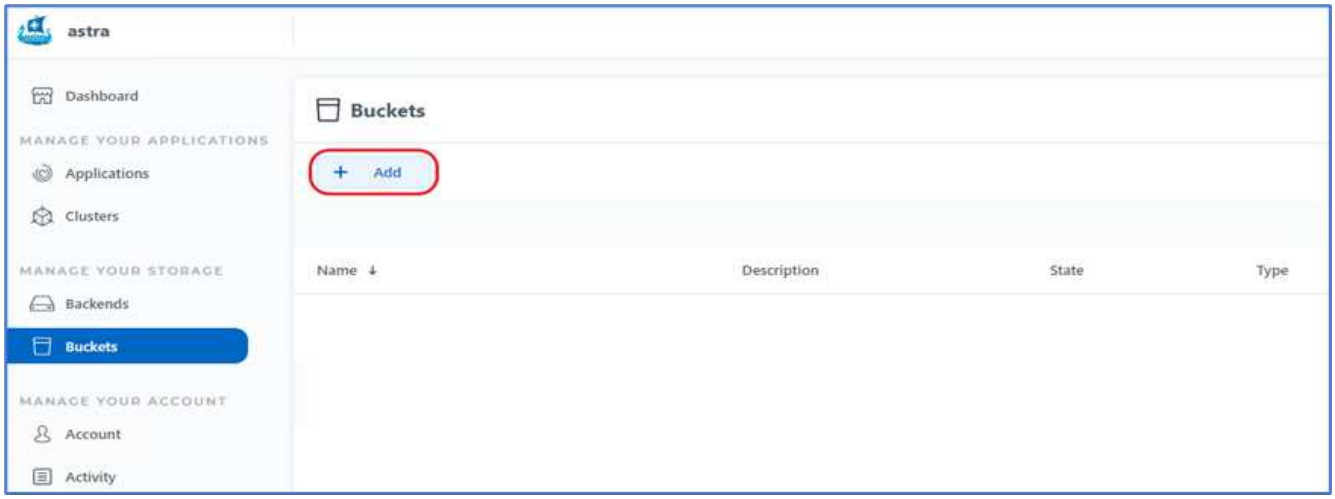
6. ストレージを管理するには、バックエンドに移動し、管理するバックエンドに対する処理の下にある3つのドットをクリックします。[管理]をクリックします



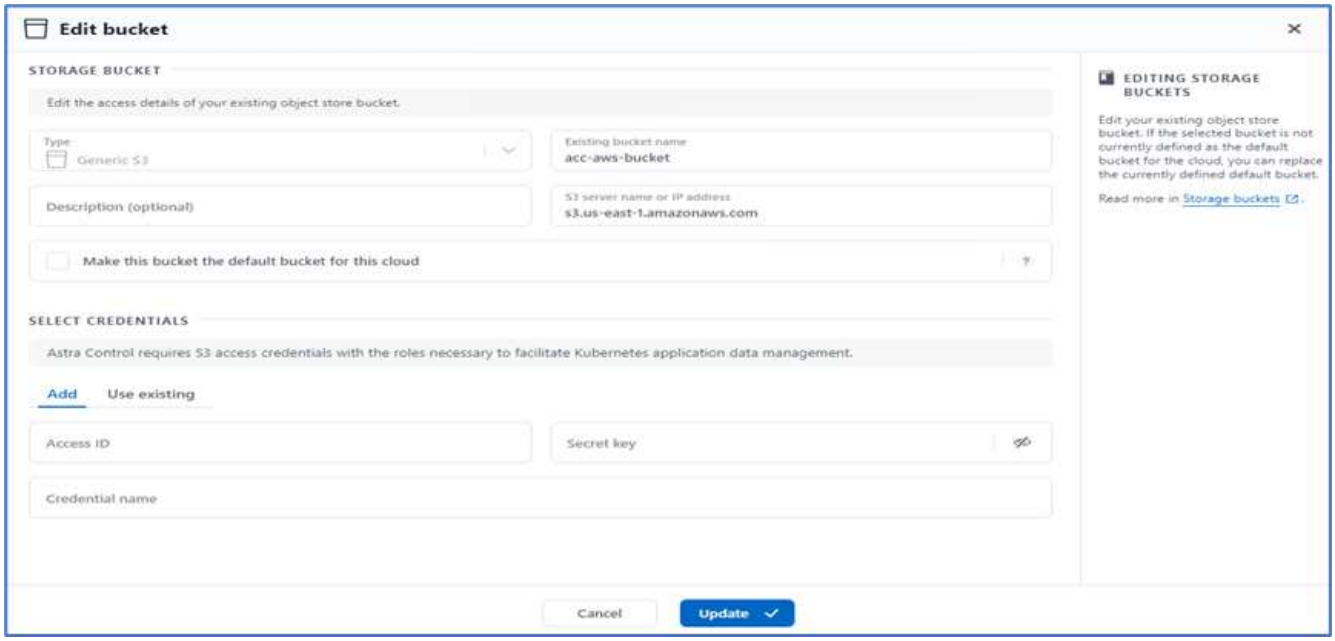
7. ONTAP の資格情報を入力し、[次へ]をクリックします。情報を確認し、[管理]をクリックします。バックエンドは次の例のようになります。



8. Astra Controlにバケットを追加するには、バケットを選択して追加をクリックします。

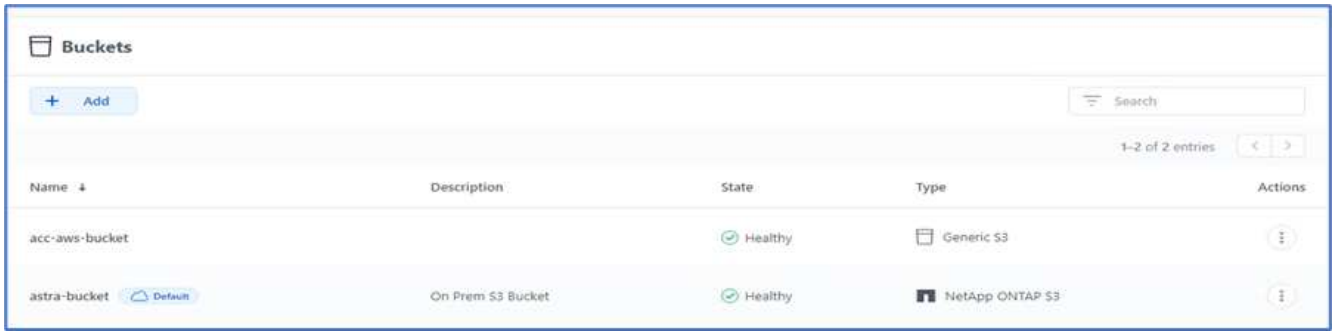


9. バケットタイプを選択し、バケット名、S3サーバ名、またはIPアドレスとS3クレデンシャルを指定します。更新をクリックします。



この解決策 では、AWS S3バケットとONTAP S3バケットの両方が使用されます。StorageGRID を使用することもできます。

バケットは正常な状態である必要があります。



アプリケーション対応データ管理用のAstra Control CenterへのKubernetesクラスタ登録の一部として、Astra Controlは、ロールバインドとネットアップ監視ネームスペースを自動的に作成し、アプリケーションポッドとワーカーノードから指標とログを収集します。サポートされているONTAPベースのストレージクラスのいずれかをデフォルトにします。

お先にどうぞ "Astra Control 管理にクラスタを追加"では、クラスターにアプリケーションをインストールし（Astra Controlの外部）、Astra Controlの[アプリ]ページに移動して、アプリケーションとそのリソースを管理できます。Astraを使用したアプリケーションの管理の詳細については、を参照してください "アプリケーション管理の要件"。

"次：解決策 の検証の概要"

解決策の検証

概要

"前のレポート：OpenShift Container PlatformにAstra Control Centerをインストールしました。"

このセクションでは、いくつかのユースケースで解決策 を復習します。

- リモートバックアップから、クラウドで実行されている別のOpenShiftクラスタへのステートフルアプリケーションのリストア。
- OpenShiftクラスタ内の同じネームスペースへのステートフルアプリケーションのリストア。
- あるFlexPod システム（OpenShift Container Platformベアメタル）から別のFlexPod システム（VMware上のOpenShift Container Platform）にクローニングすることでアプリケーションを移動できます。

特に、この解決策 で検証されるのはユースケースが少ないことがわかります。この検証は、Astra Control Centerの全機能を表しているわけではありません。

"Next：リモートバックアップを使用したアプリケーションのリカバリ。"

リモートバックアップによるアプリケーションのリカバリ

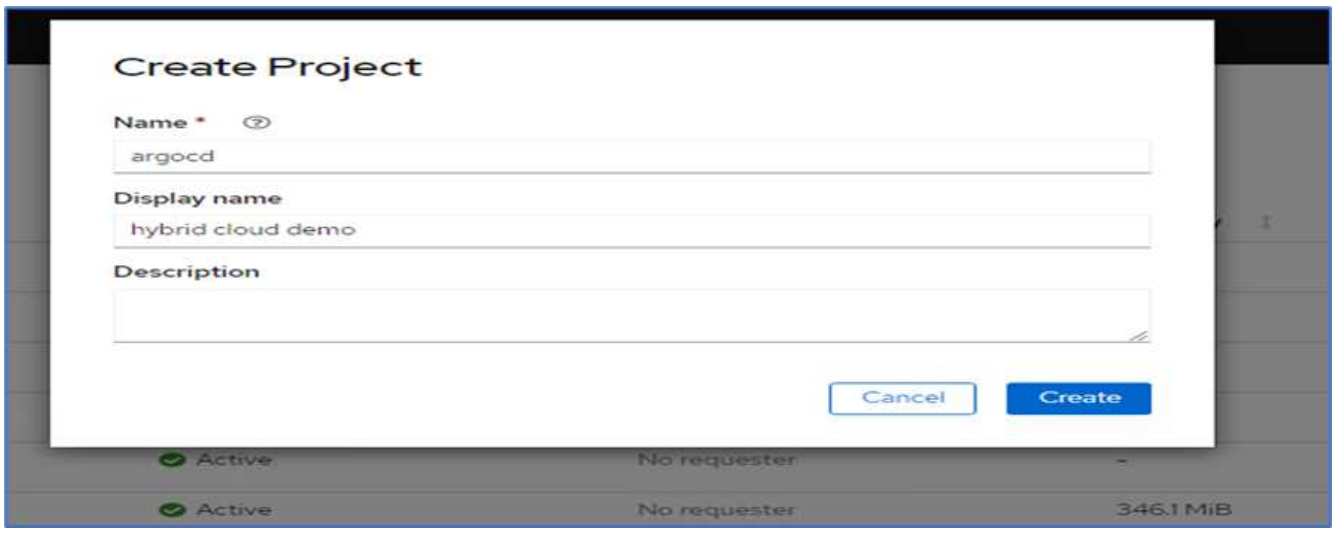
"Previous：解決策 の検証の概要を示します。"

Astraでは、アプリケーションと整合性のあるフルバックアップを作成できます。このバックアップを使用すると、アプリケーションのデータを使用して、オンプレミスのデータセンターやパブリッククラウドで実行されている別のKubernetesクラスタにリストアできます。

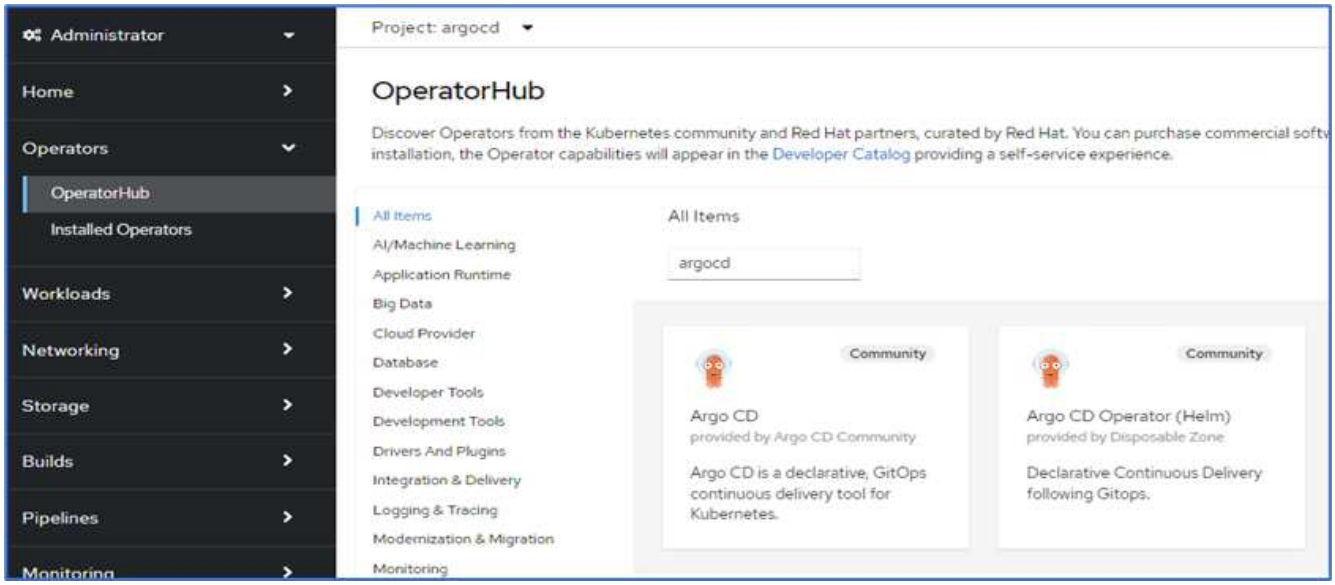
アプリケーションのリカバリが正常に行われるかどうかを検証するには、FlexPod システムで実行されているアプリケーションのオンプレミス障害をシミュレートし、リモートバックアップを使用してクラウドで実行されているKubernetesクラスタにアプリケーションをリストアします。

サンプルアプリケーションは、データベースにMySQLを使用する価格表アプリケーションです。導入を自動化するために、を使用しました "Argo CD" ツール。Argo CDは、Kubernetes向けの宣言型、GitOps、継続的デリバリーツールです。

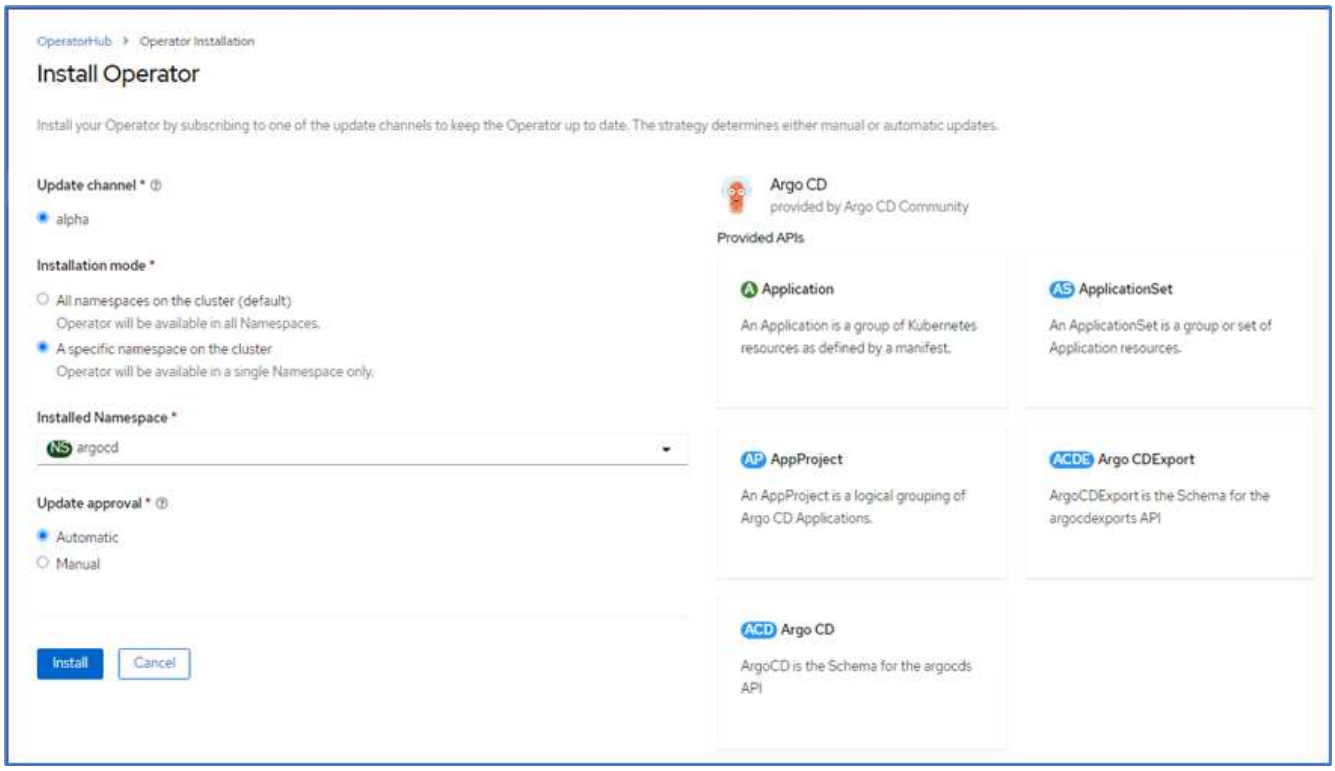
1. オンプレミスOpenShiftクラスタにログインし、「argocd」という名前の新しいプロジェクトを作成します。



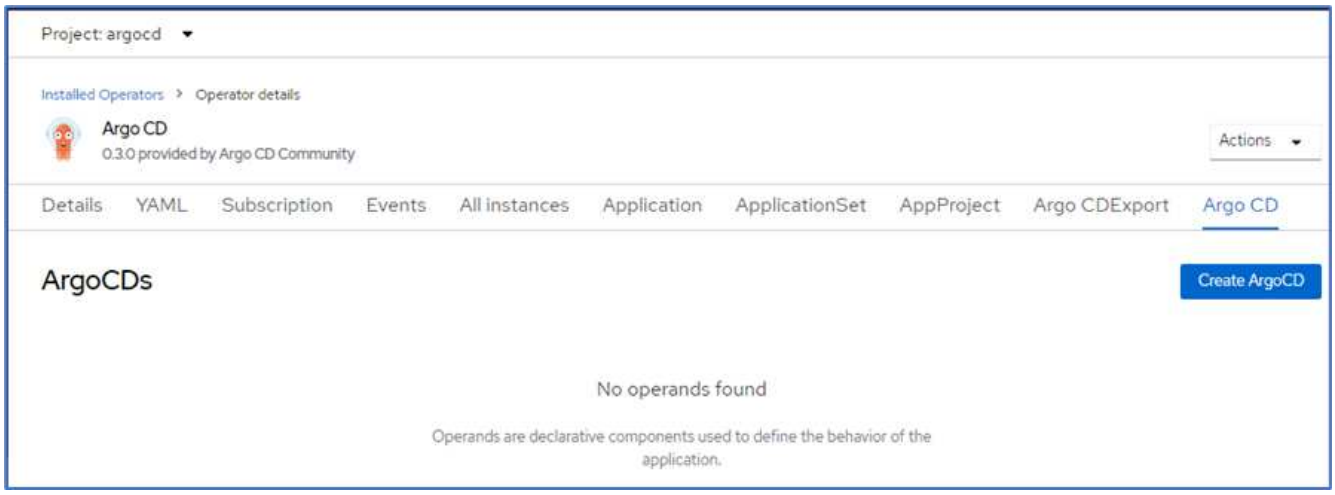
2. OperatorHubで'argocd'を検索し'Argo CD operatorを選択します



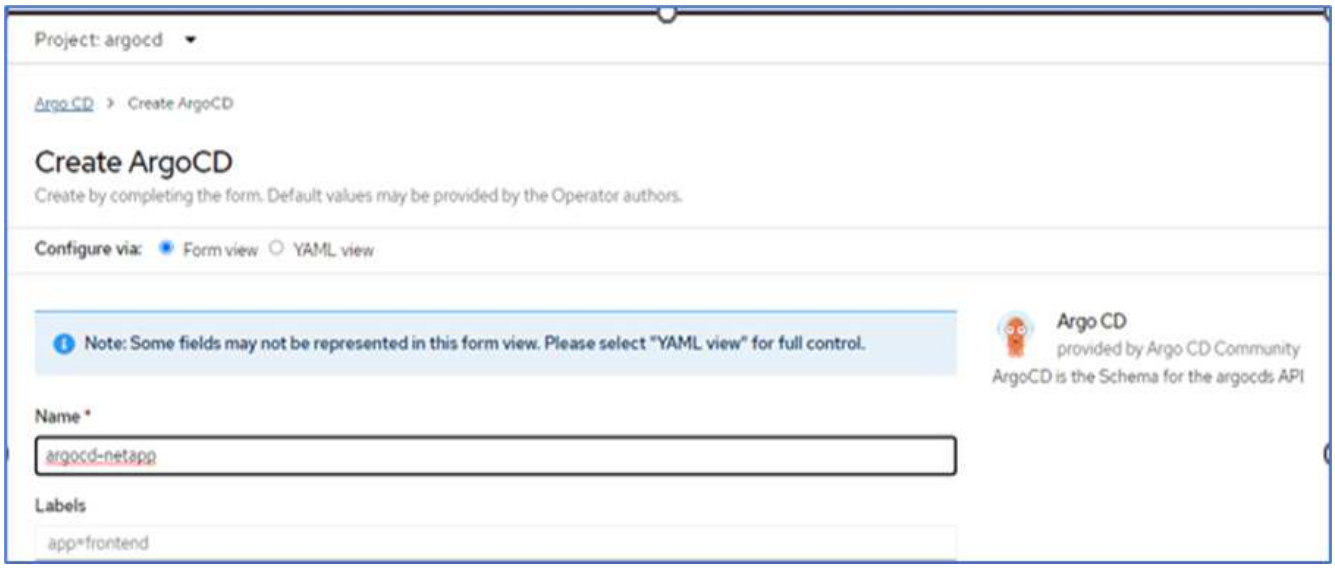
3. 「argocd」名前空間に演算子をインストールします。



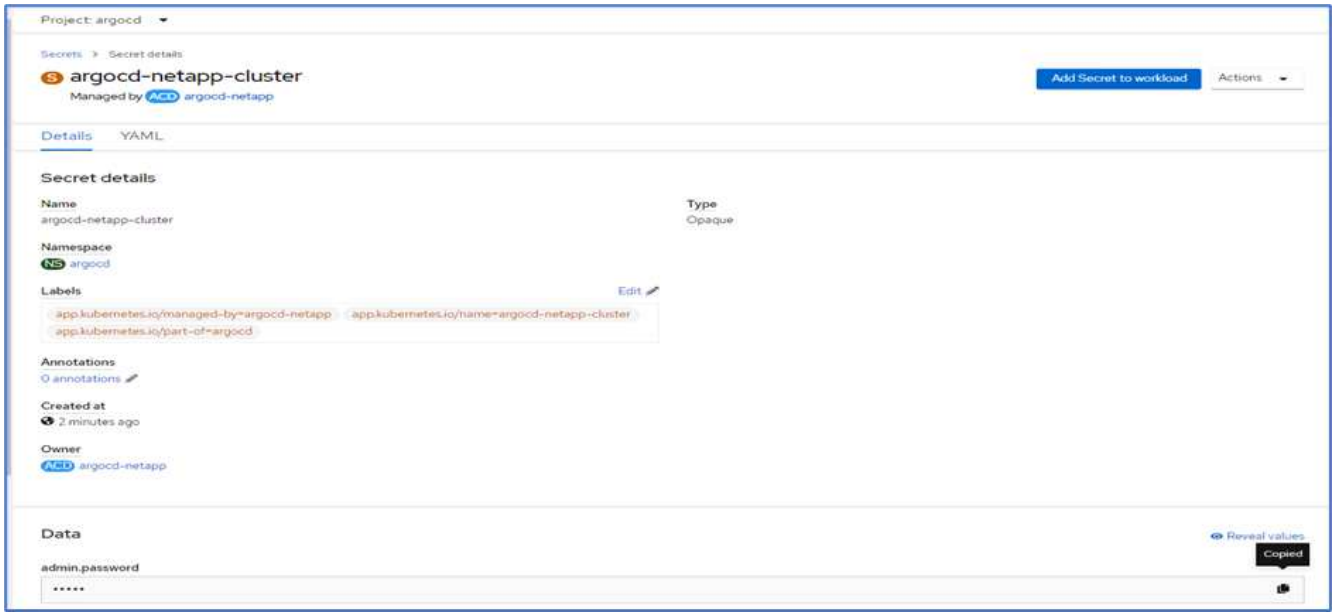
4. オペレータに移動し、Create ArgCDをクリックします。



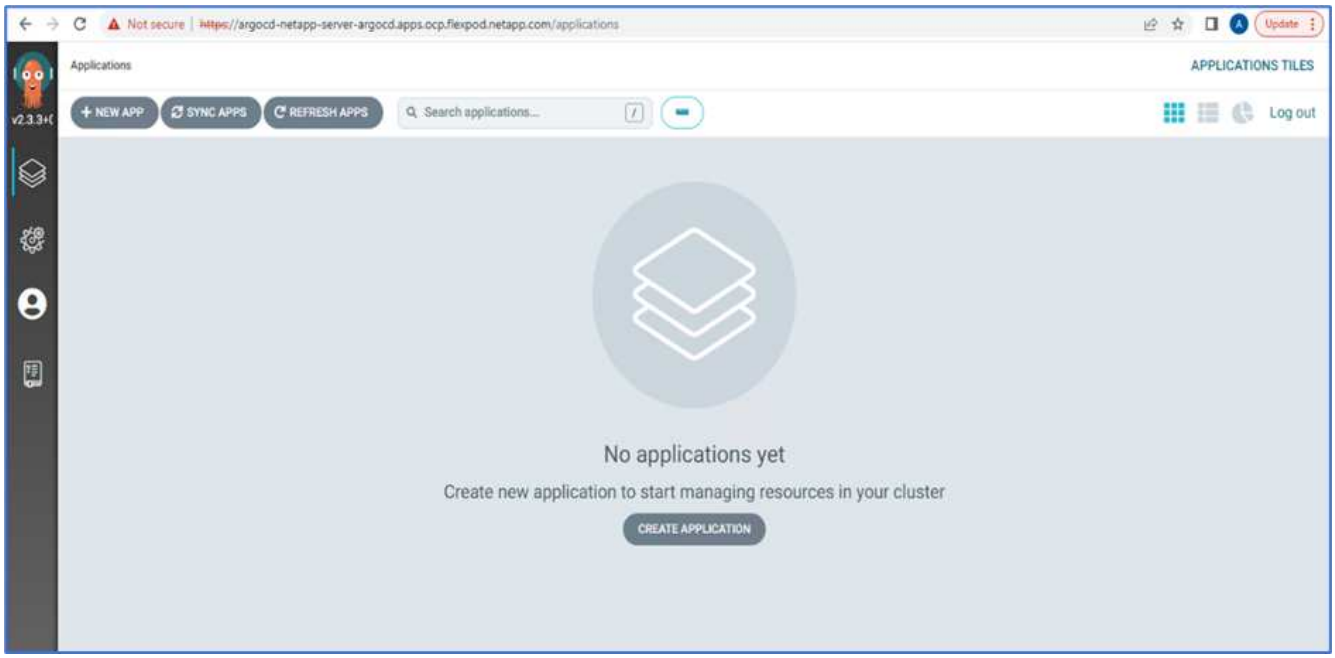
5. Argo CDインスタンスを'argocd'プロジェクトに配備するには'名前を指定してCreateをクリックします



6. Argo CDにログインするには、デフォルトのユーザはadminで、パスワードは「argocd -NetApp-cluster」という名前のシークレットファイルに含まれています。



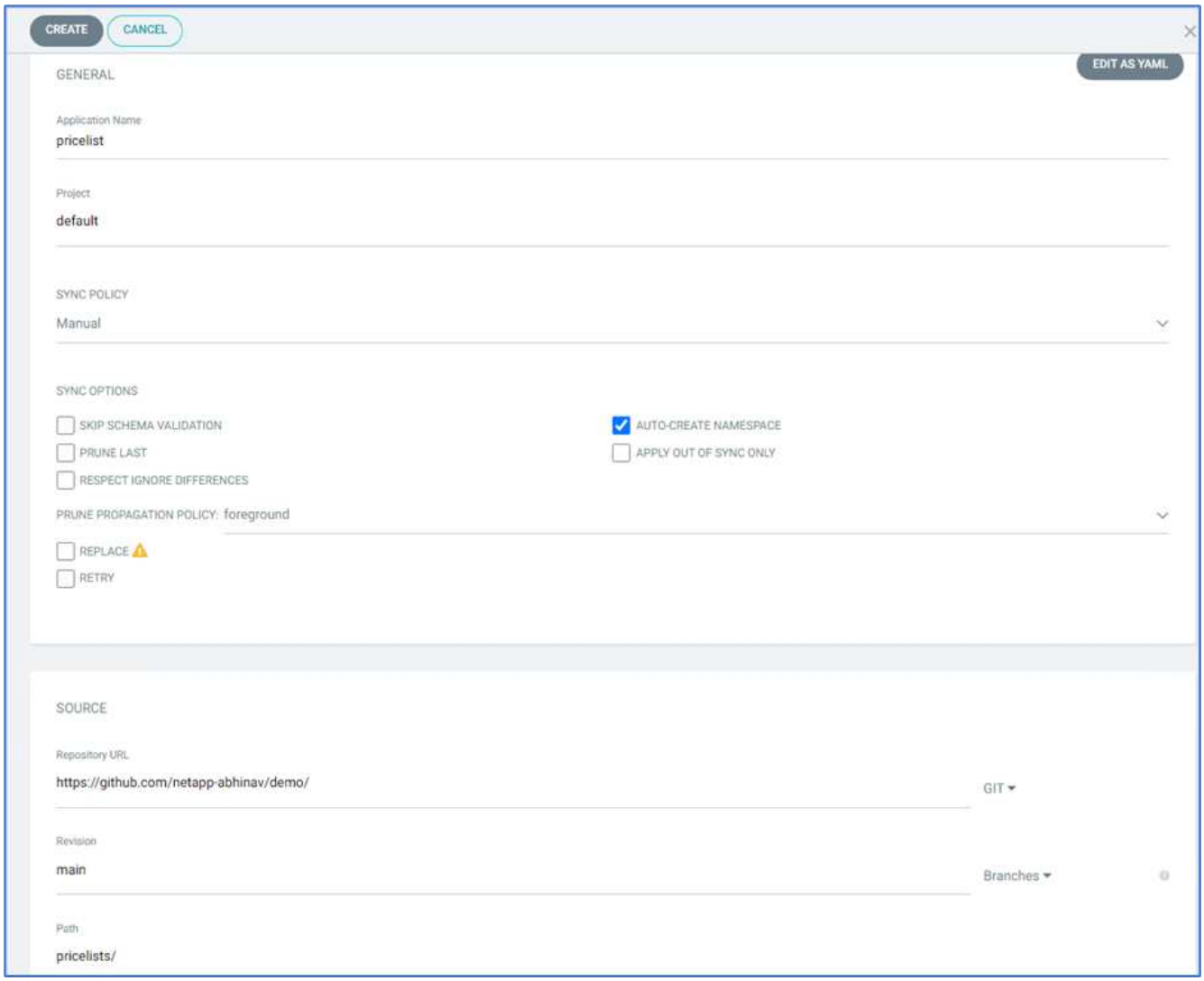
7. サイド・メニューから'ルート>ロケーションを選択し'argocd'ルートのURLをクリックしますユーザ名とパスワードを入力します。



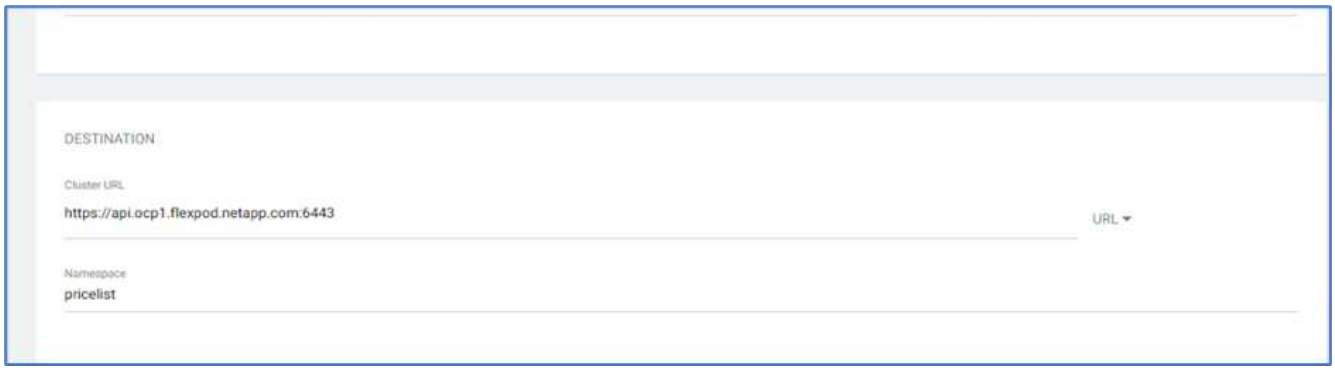
8. CLIを使用して、Argo CDにオンプレミスOpenShiftクラスタを追加します。

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

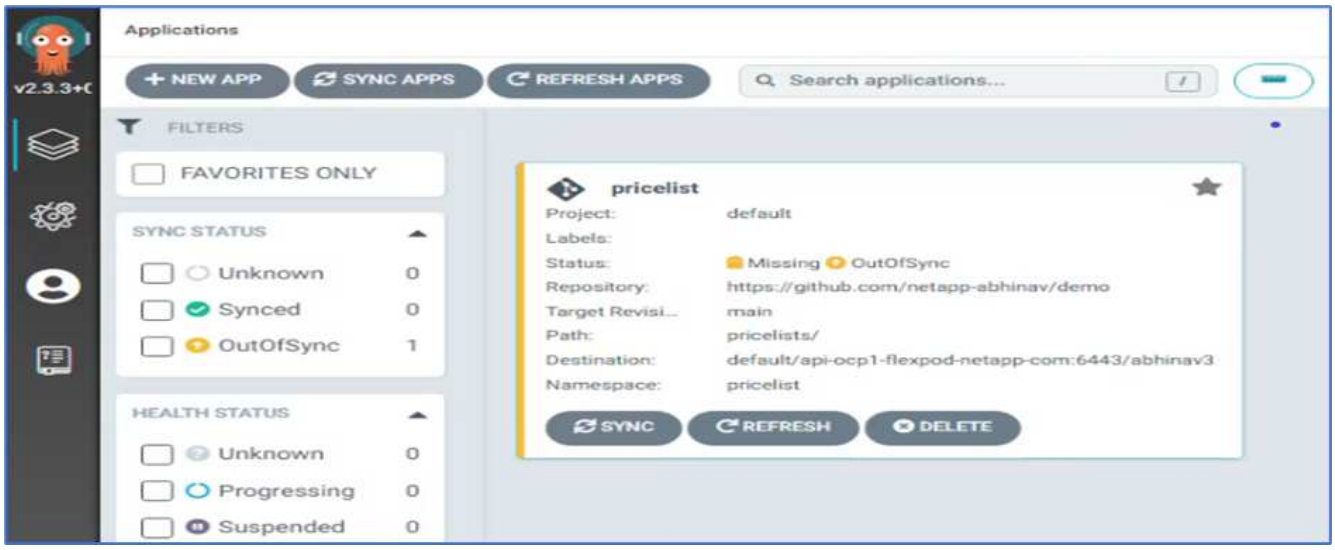
9. ArgodCD UIで、[新しいアプリ]をクリックし、アプリ名とコードリポジトリの詳細を入力します。



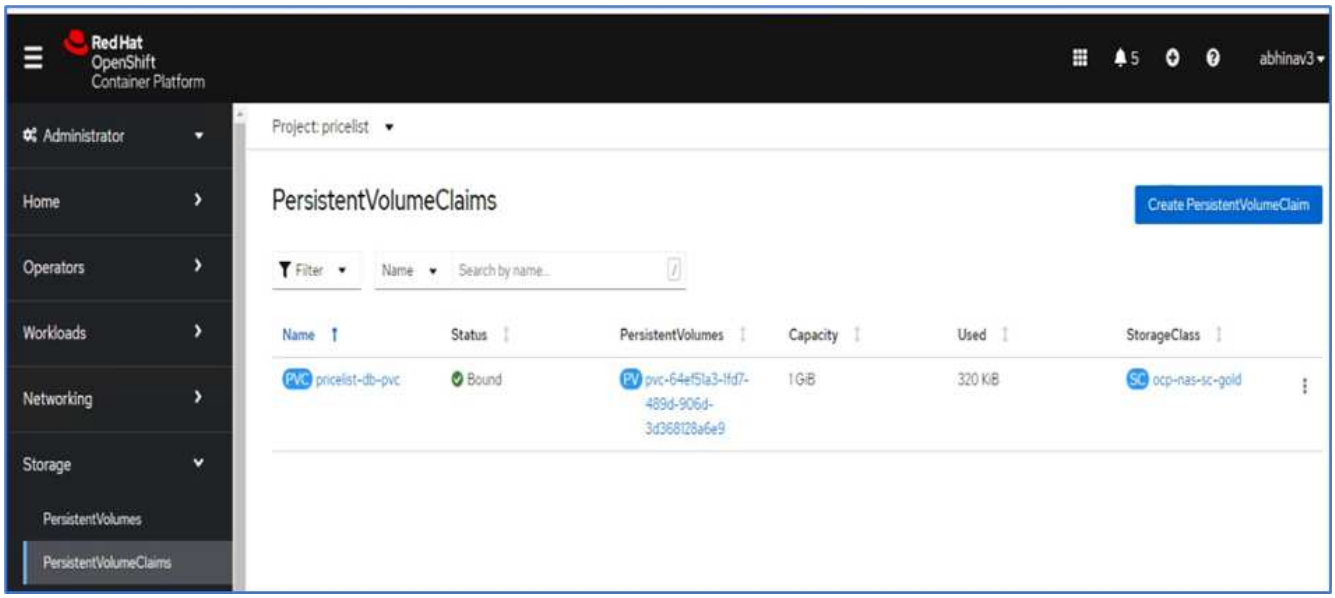
10. ネームスペースとともにアプリケーションを導入するOpenShiftクラスタを入力します。



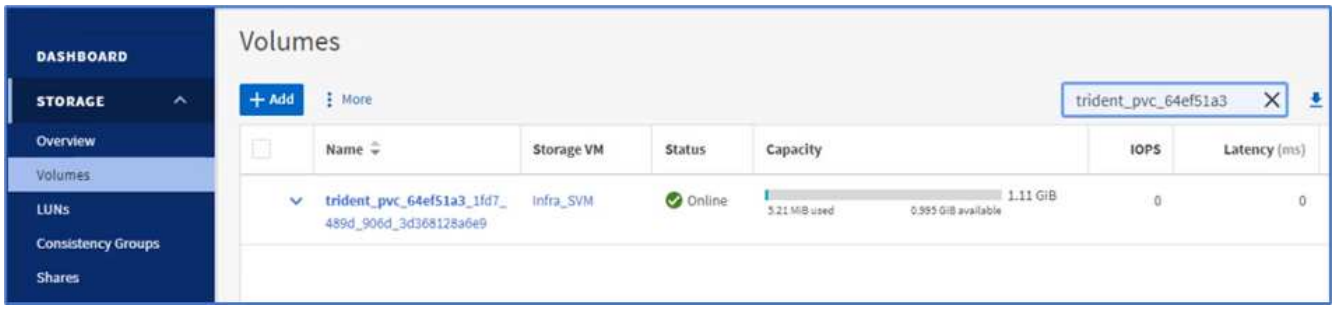
11. オンプレミスOpenShiftクラスタにアプリを導入するには、[同期]をクリックします。



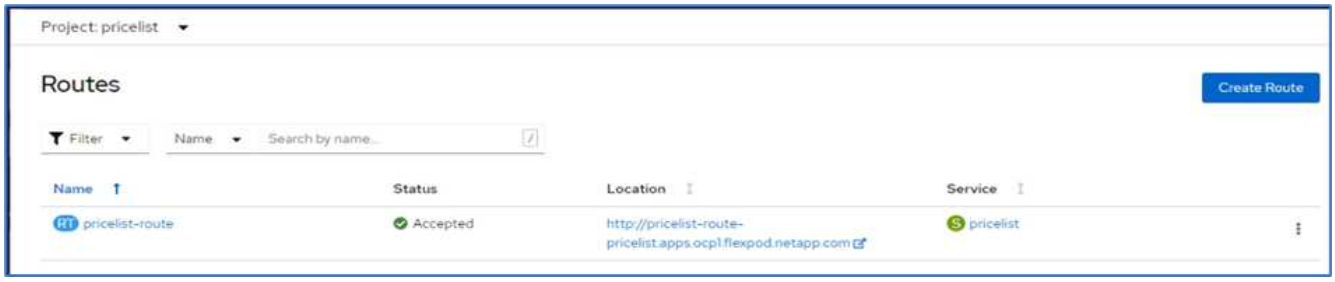
12. OpenShift Container Platformコンソールで、プロジェクト価格表に移動し、ストレージでPVCの名前とサイズを確認します。



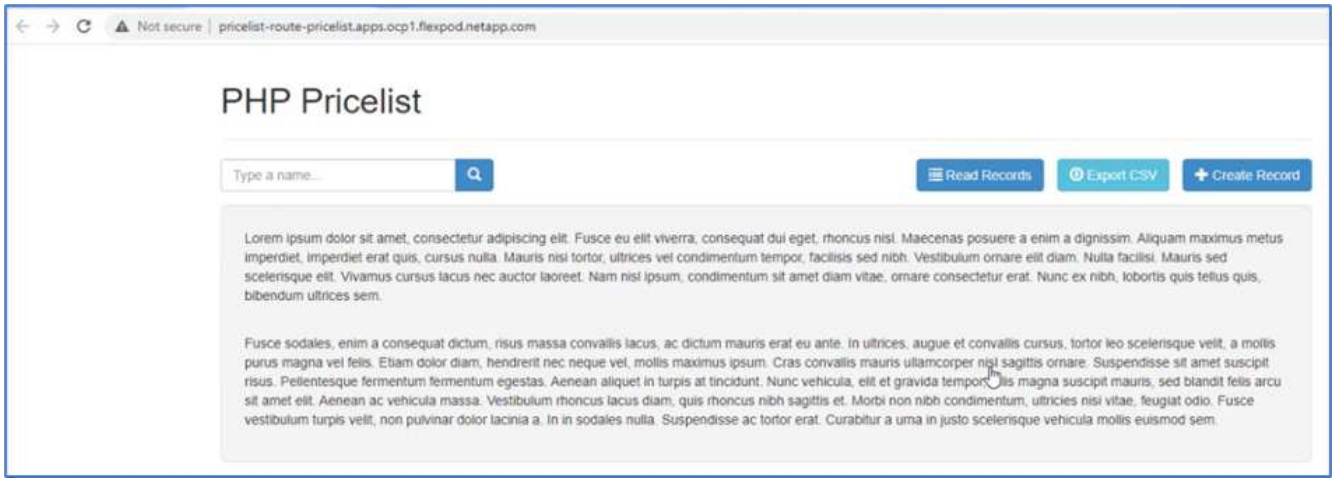
13. System Managerにログインし、PVCを確認します。



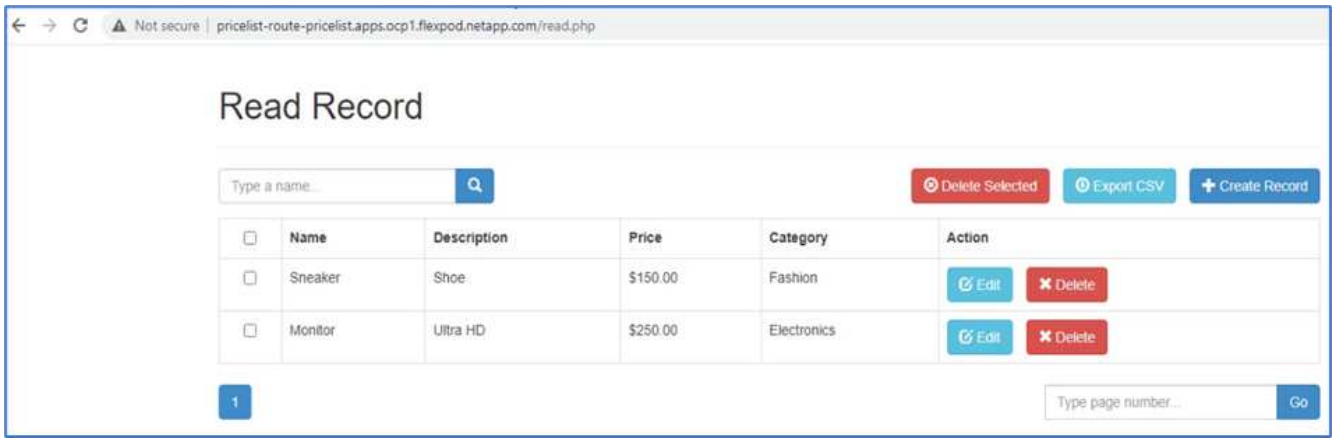
14. ポッドが実行されたら、サイドメニューからネットワーキング／ルートを選択し、「場所」の下のURLをクリックします。



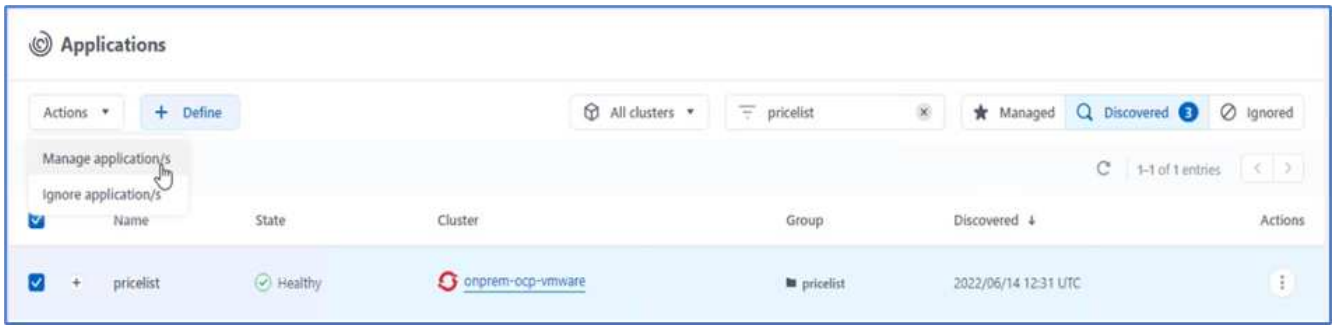
15. 価格表アプリのホームページが表示されます。



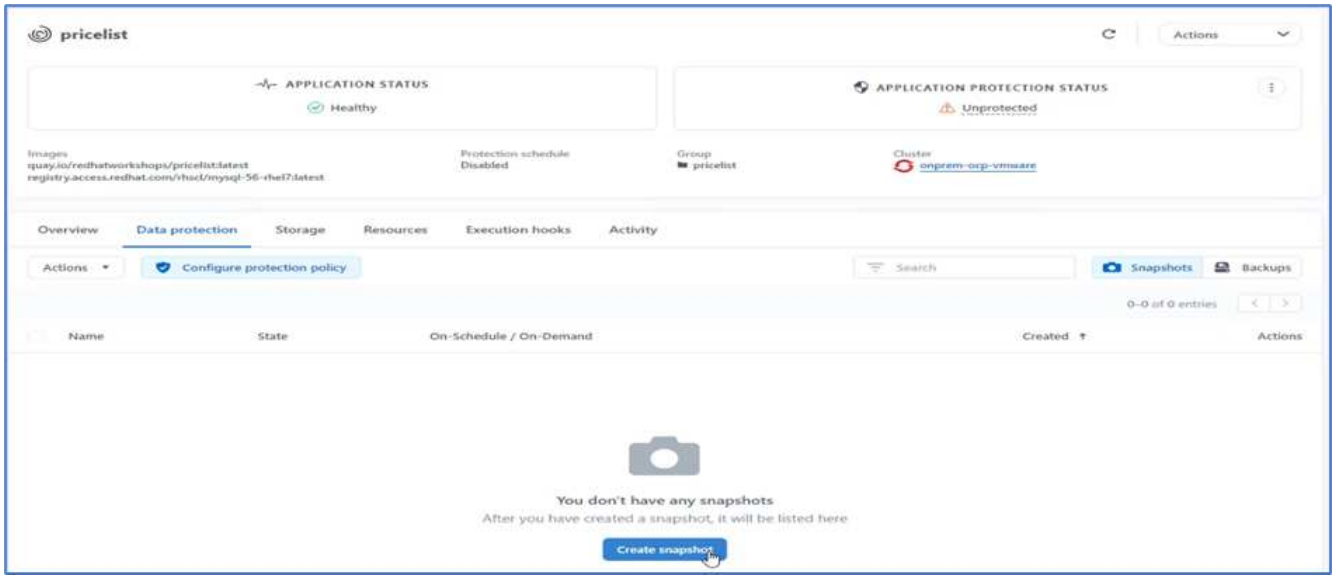
16. Webページにレコードをいくつか作成します。



17. アプリケーションはAstra Control Centerで検出されます。アプリを管理するには、[アプリケーション]>[検出済み]に移動し、価格表アプリを選択して、[アクション]の[アプリケーションの管理]をクリックします。

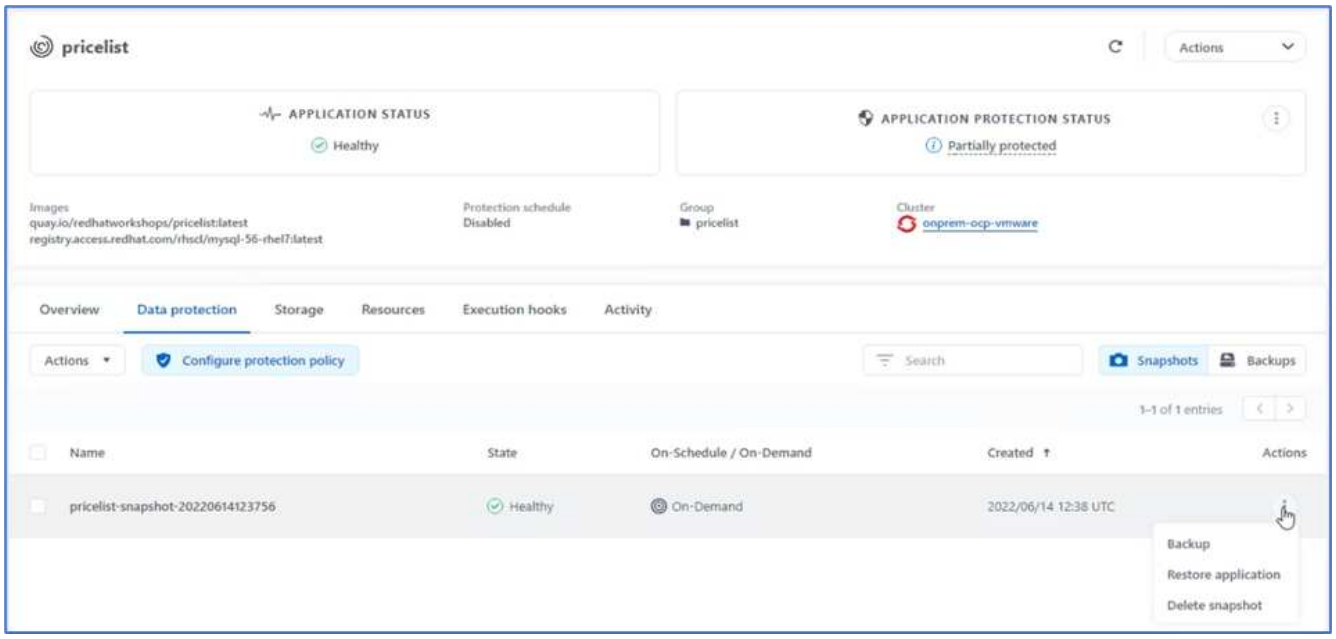


18. 価格表アプリをクリックし、[データ保護]を選択します。この時点では、Snapshotやバックアップは作成されていません。スナップショットの作成をクリックして、オンデマンドスナップショットを作成します。

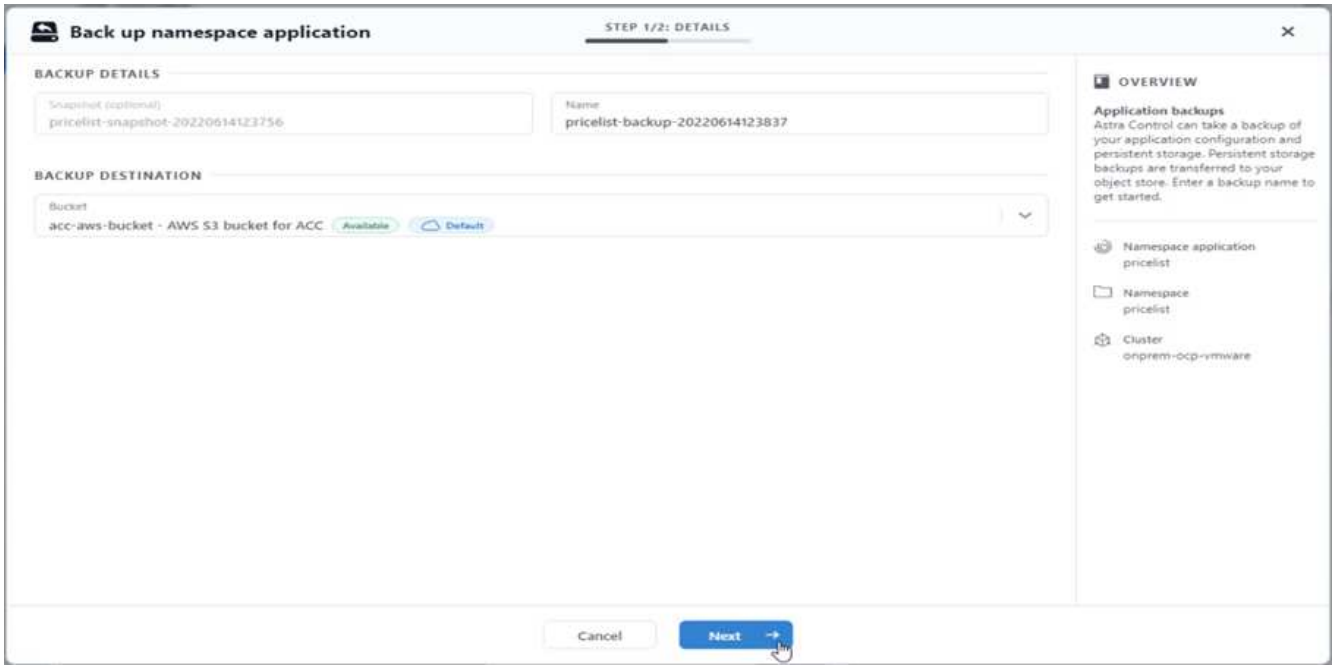


NetApp Astra Control Centerは、オンデマンドおよびスケジュールされたスナップショットとバックアップの両方をサポートします。

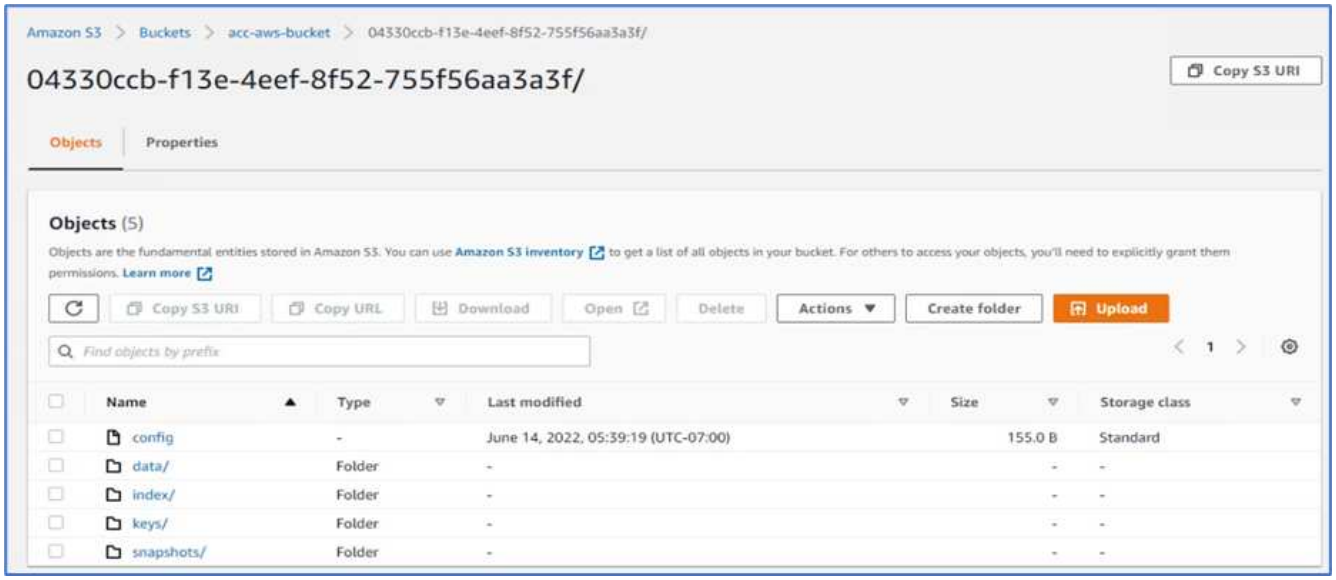
19. スナップショットが作成され、状態が正常になったら、そのスナップショットを使用してリモートバックアップを作成します。このバックアップはS3バケットに格納されます。



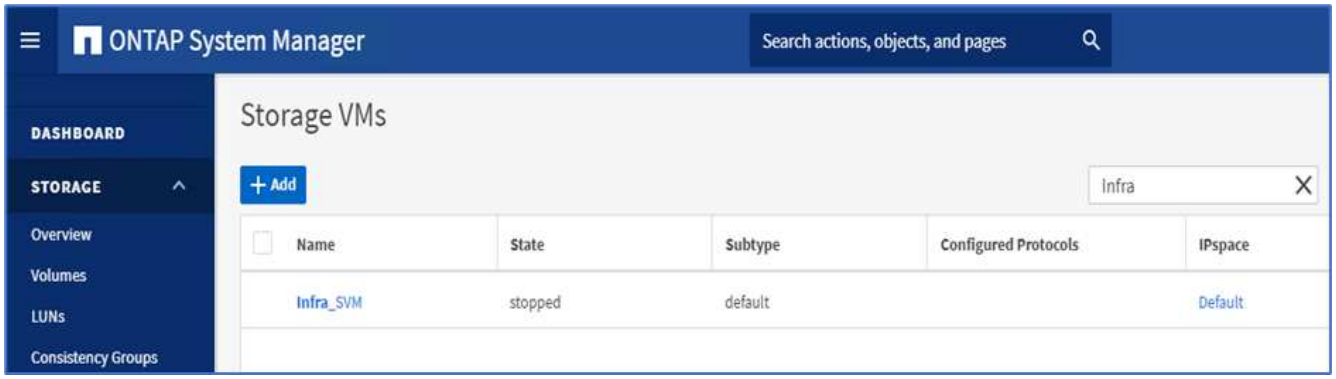
20. AWS S3バケットを選択してバックアップ処理を開始します。



21. バックアップ処理では、AWS S3バケットに複数のオブジェクトを含むフォルダを作成する必要があります。



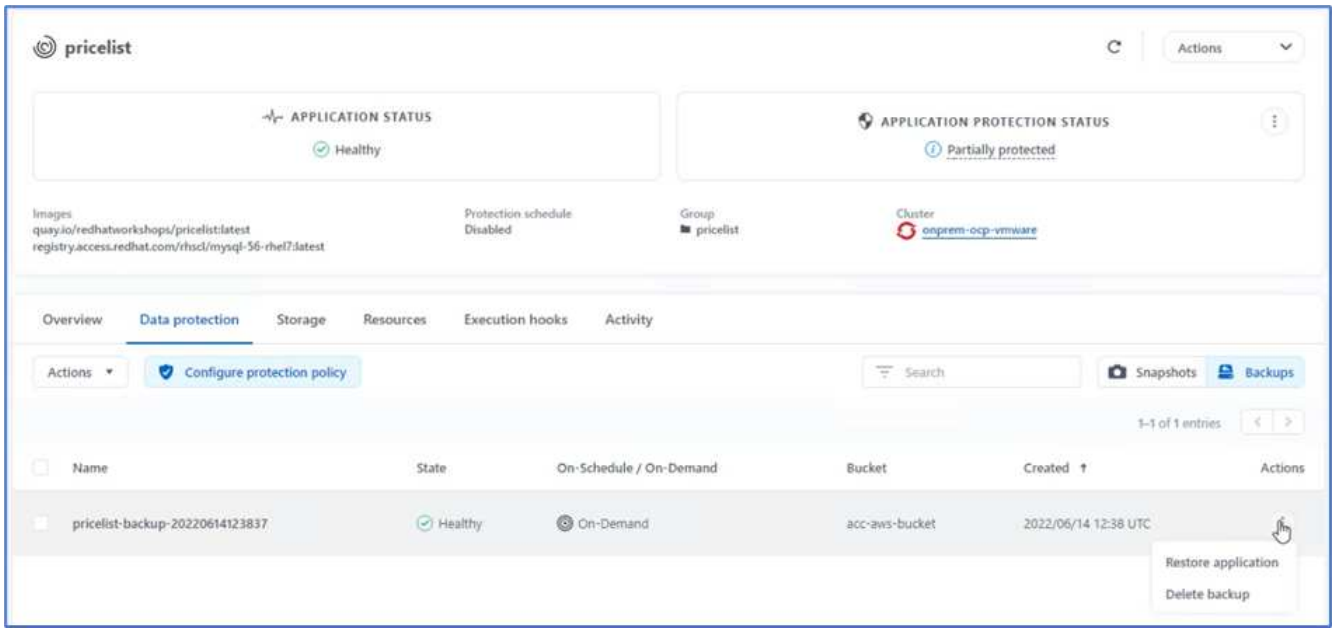
22. リモートバックアップが完了したら、PVの元のボリュームをホストするStorage Virtual Machine（SVM）を停止して、オンプレミスでの災害をシミュレートします。



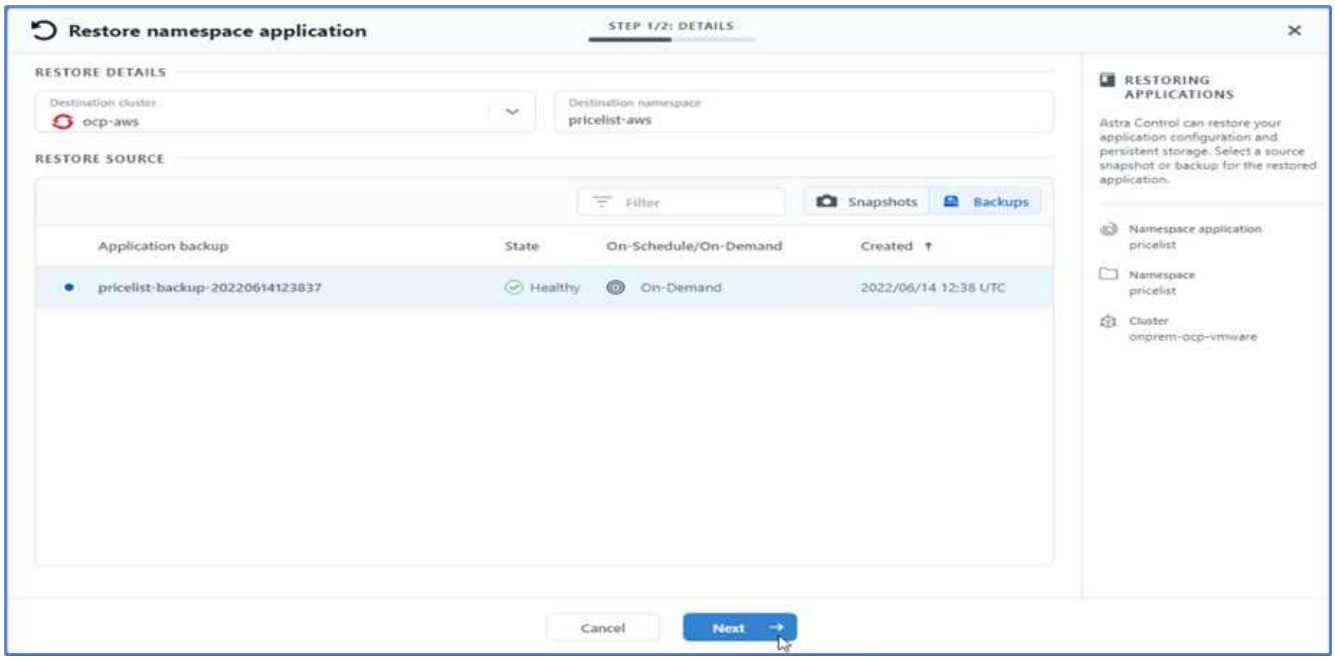
23. Webページを更新してシステム停止を確認します。Webページは使用できません。

ウェブサイトは予想どおりに停止しているので、AWSで実行されているOpenShiftクラスタにAstraを使用して、リモートバックアップからアプリケーションを迅速にリカバリしてみましょう。

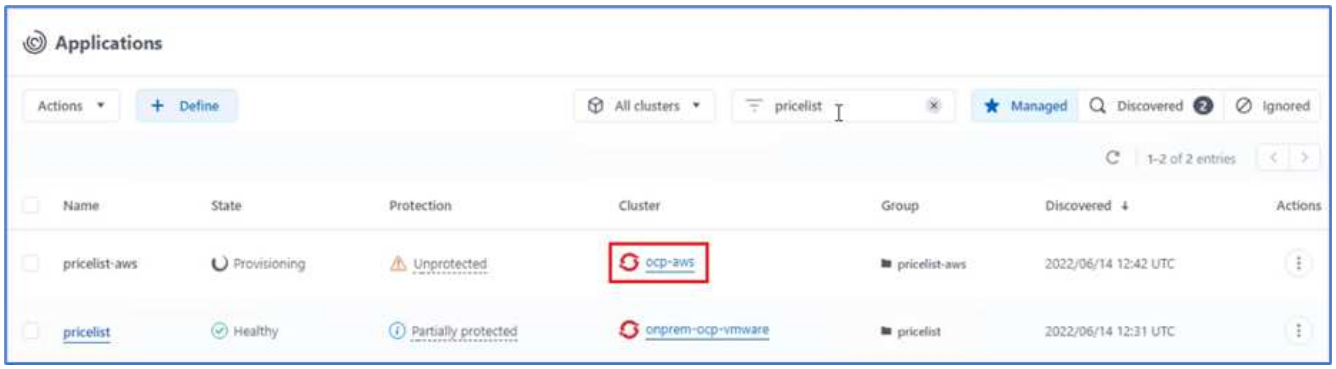
24. Astra Control Centerで、価格表アプリをクリックし、[データ保護]>[バックアップ]を選択します。バックアップを選択し、[操作]の下の[アプリケーションの復元]をクリックします。



25. デスティネーションクラスタとして「OCP-AWS」を選択し、ネームスペースに名前を付けます。[オンデマンドバックアップ]、[次へ]、[復元]の順にクリックします。

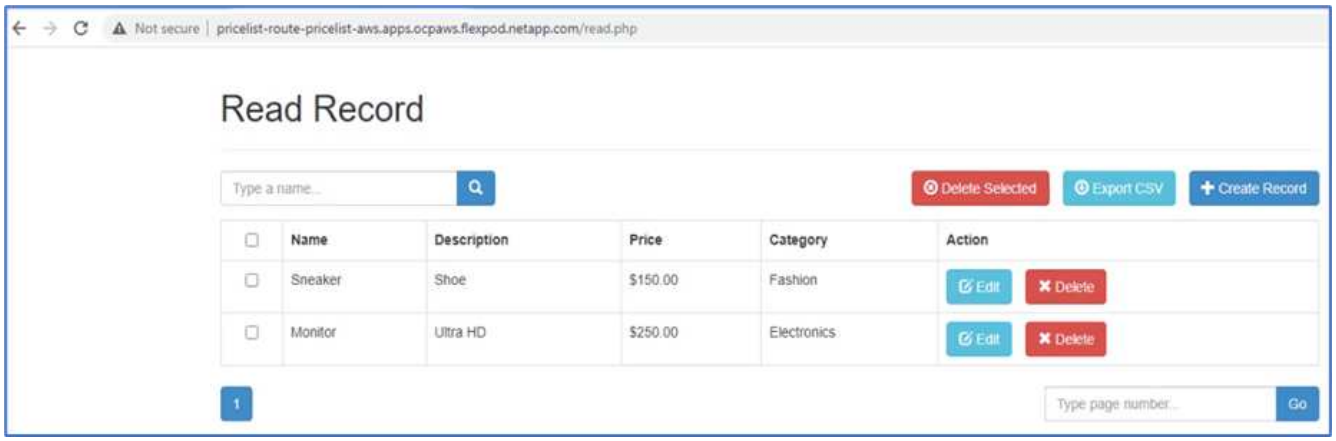


26. 「pricelist-app」という名前の新しいアプリケーションは、AWSで実行されるOpenShiftクラスタでプロビジョニングされます。



27. OpenShift Webコンソールで同じことを確認します。

28. 「pricelist -aws」プロジェクトの下のポッドがすべて実行されたら、「Routes」に移動し、URLをクリックしてWebページを起動します。



このプロセスでは、貴重なアプリケーションが正常に復元され、Astra Control Centerを利用してAWS上でシームレスに実行されるOpenShiftクラスタでデータの整合性が維持されていることを検証します。

Snapshotコピーと**DevTest**のアプリケーション移動によるデータ保護

この使用事例は、次のセクションで説明する2つの部分で構成されています。

パート**1**

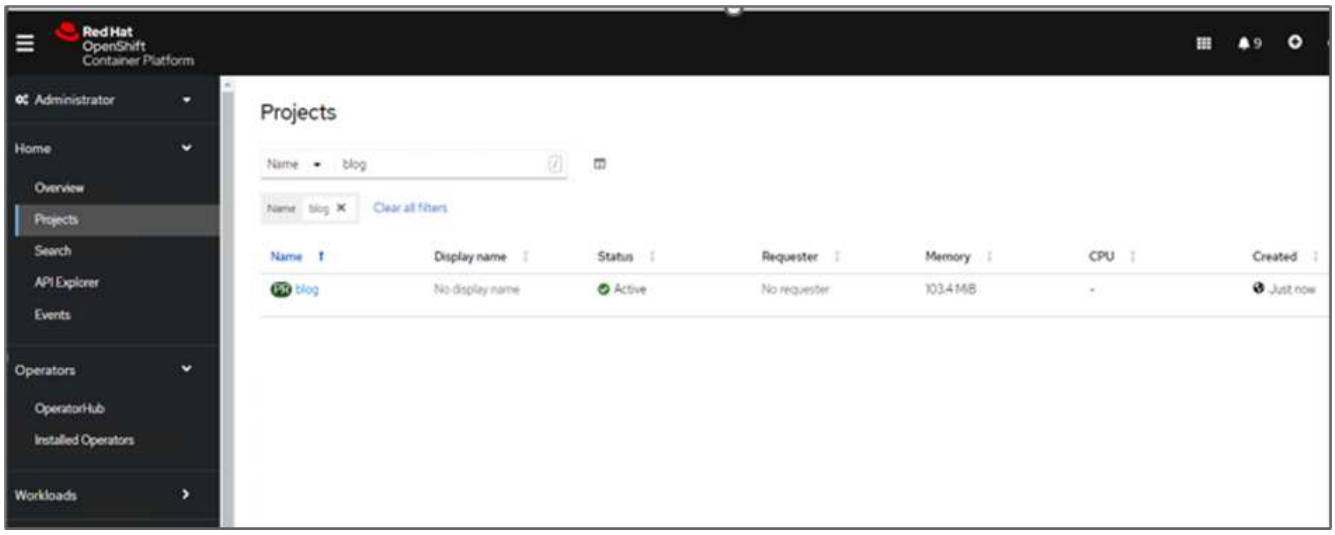
Astra Control Centerを使用すると、アプリケーション対応のスナップショットを作成してローカルデータを

保護できます。データを誤って削除したり破損したりした場合は、以前に記録したスナップショットを使用して、アプリケーションおよび関連データを既知の正常な状態に戻すことができます。

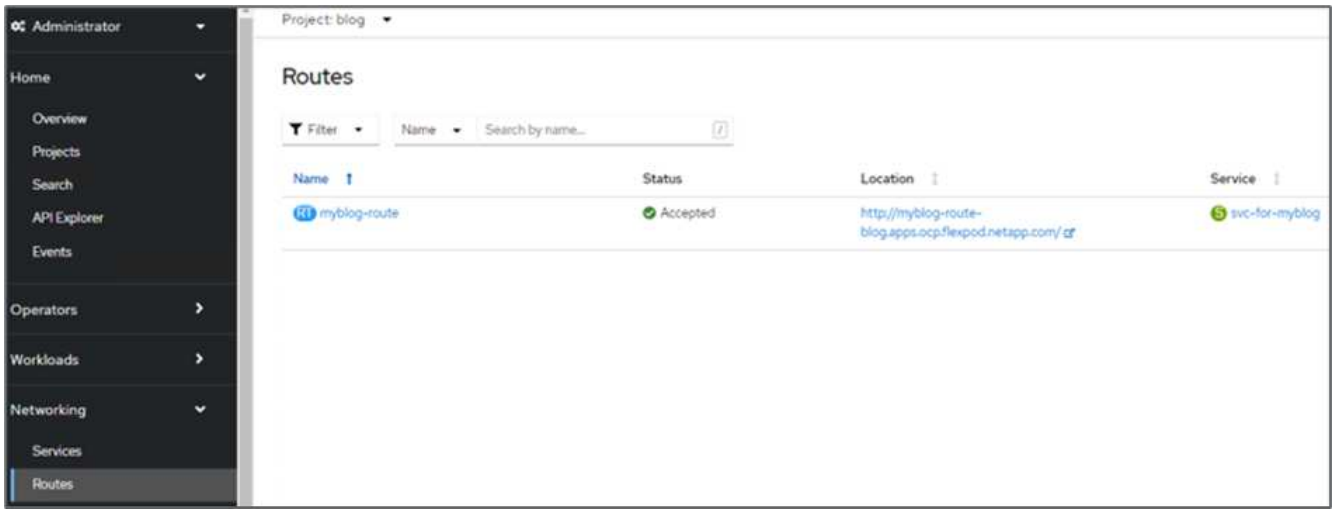
このシナリオでは、開発とテスト（DevTest）チームが、Ghostブログアプリケーションであるサンプルのステートフルアプリケーション（ブログサイト）を導入し、コンテンツを追加し、アプリケーションを最新バージョンにアップグレードします。Ghostアプリケーションでは、データベースにSQLiteを使用します。アプリケーションをアップグレードする前に、Astra Control Centerを使用してスナップショット（オンデマンド）を作成し、データを保護します。詳細な手順は次のとおりです。

1. サンプルブログアプリをデプロイし、ArgoCDから同期します。

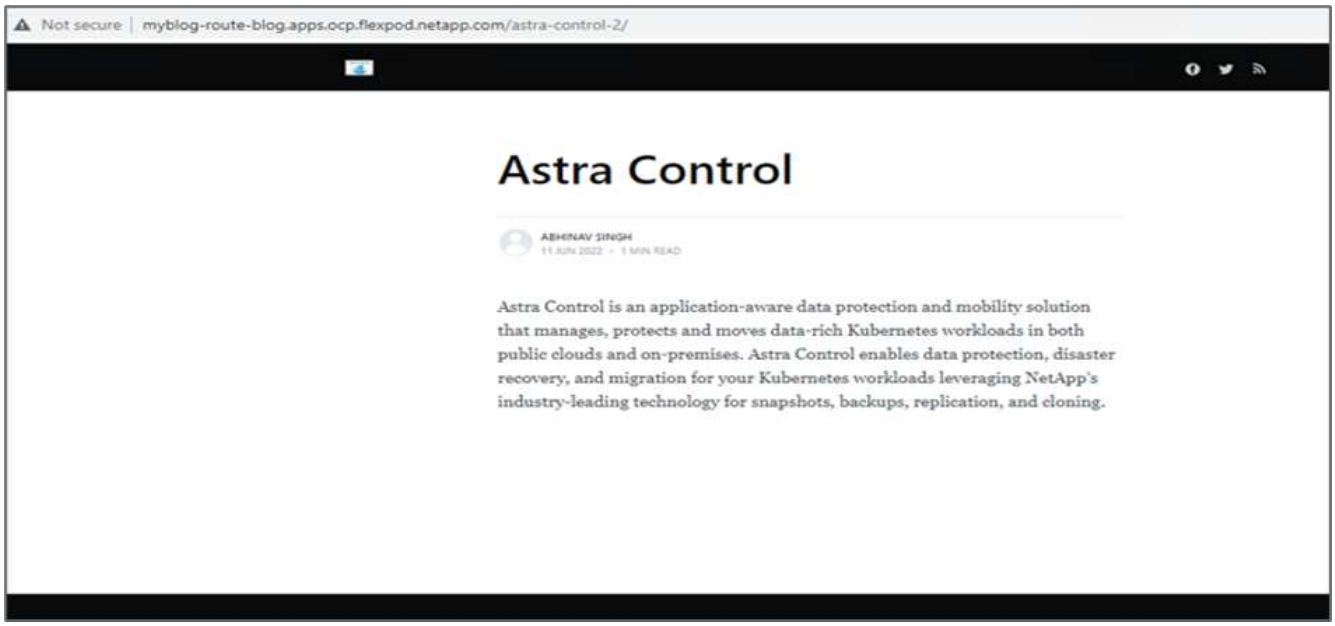
2. 最初のOpenShiftクラスタにログインし、Projectに移動して、検索バーにBlogと入力します。



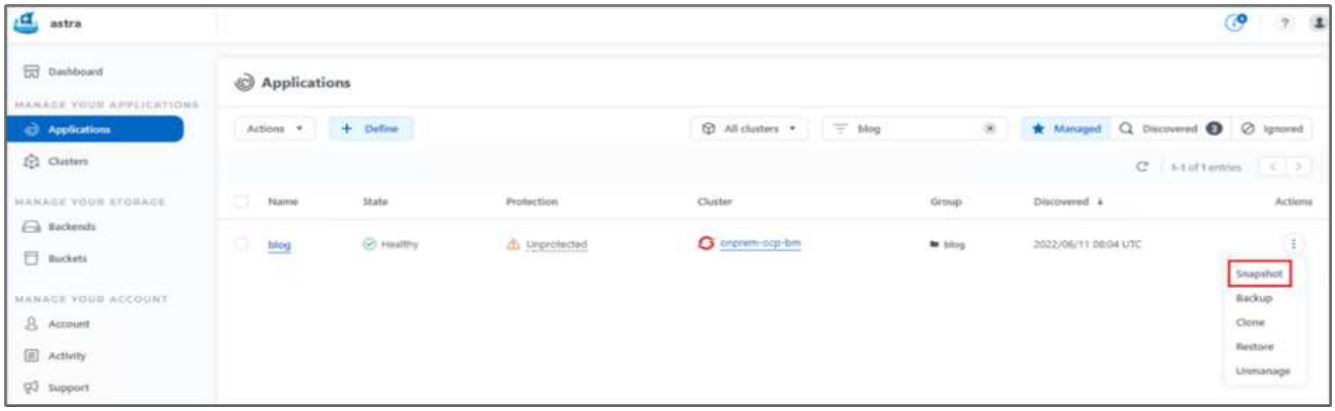
3. サイドメニューから、[Networking]>[Routes]の順に選択し、URLをクリックします。



4. ブログのホームページが表示されます。ブログサイトにコンテンツを追加して公開します。



5. Astra Control Centerにアクセスします。最初に検出タブからアプリケーションを管理してから、Snapshotコピーを作成します。



定義したスケジュールでスナップショット、バックアップ、またはその両方を作成することで、アプリケーションを保護することもできます。詳細については、を参照してください "Snapshot とバックアップでアプリケーションを保護"。

6. オンデマンドスナップショットが正常に作成されたら、アプリケーションを最新バージョンにアップグレードします。現在のイメージのバージョンは「ghost:3.6 -アルパイン」で、ターゲットのバージョンは「ghost:latest」です。アプリをアップグレードするには、Gitリポジトリに直接変更を加え、Argo CDに同期します。

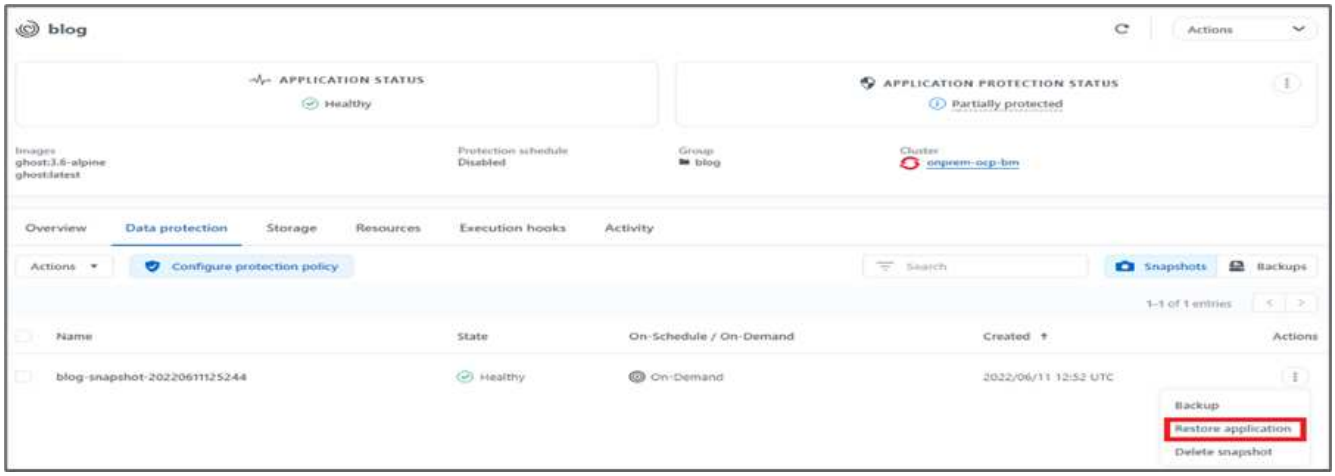
```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

7. ブログサイトがダウンし、アプリケーション全体が破損しているために、最新バージョンへの直接アップグレードがサポートされていないことがわかります。

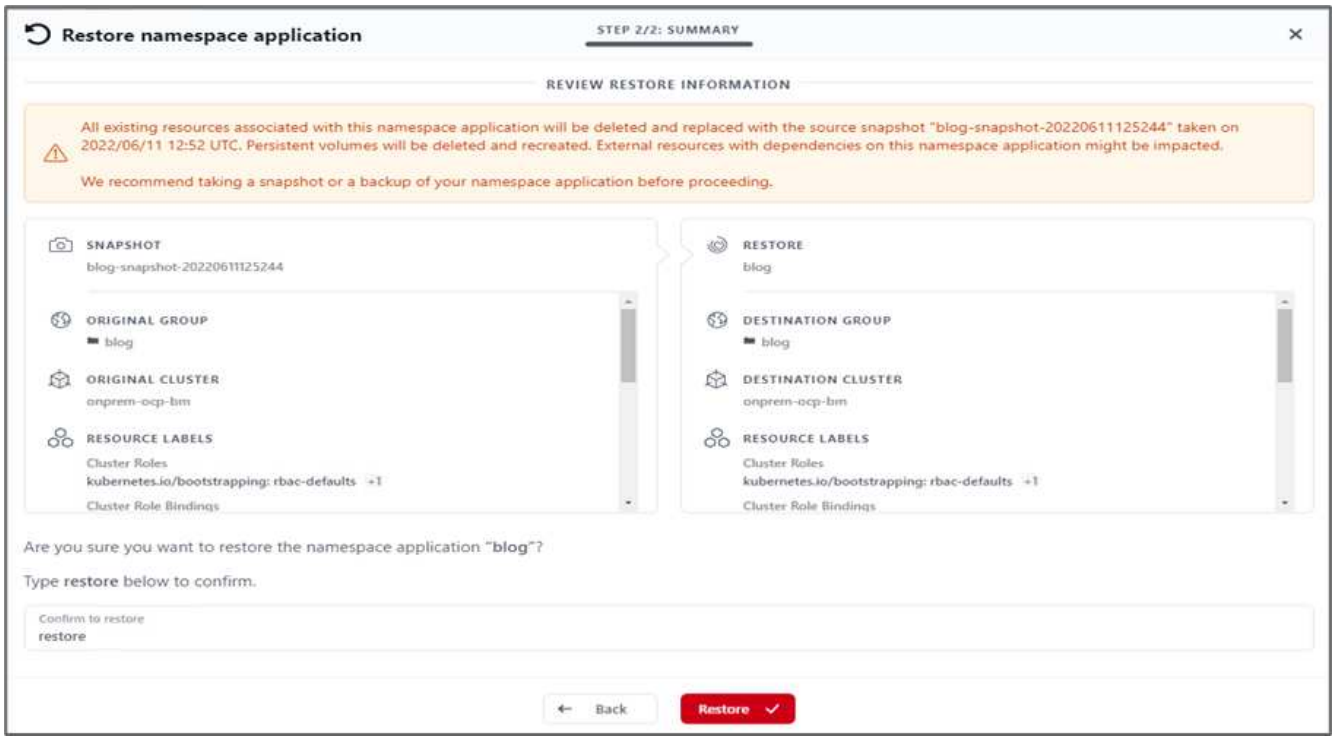
```
Project: blog
Pods > Pod details
myblog-5f899f7b76-zv7rq  CrashLoopBackOff
Details  Metrics  YAML  Environment  Logs  Events  Terminal
Log stream ended.  myblog  Current log
34 lines
[2022-06-11 12:54:05] ←[36mINFO←[39m Creating database backup
[2022-06-11 12:54:05] ←[36mINFO←[39m Database backup written to: /var/lib/ghost/content/data/astra.ghost.2022-06-11-12-54-05.json
[2022-06-11 12:54:05] ←[36mINFO←[39m Running migrations.
[2022-06-11 12:54:06] ←[36mINFO←[39m Rolling back: Unable to run migrations.
[2022-06-11 12:54:06] ←[36mINFO←[39m Rollback was successful.
[2022-06-11 12:54:06] ←[31mERROR←[39m Unable to run migrations
←[31m
←[31mUnable to run migrations←[39m

←[37m"You must be on the latest v3.x to update across major versions - https://ghost.org/docs/update/"←[39m
←[33m"Run 'ghost update v3' to get the latest v3.x version, then run 'ghost update' to get to the latest."←[39m

←[1m←[37mError ID:←[39m←[22m
    ←[90m93b99ce0-e985-11ec-9301-7d29b2c73999←[39m

←[90m------------------------------------------←[39m

←[90mInternalServerError: Unable to run migrations
    at /var/lib/ghost/versions/5.2.2/node_modules/knex-migrator/lib/index.js:1032:19
    at up (/var/lib/ghost/versions/5.2.2/core/server/data/migrations/utils/migrations.js:118:19)
    at Object.up (/var/lib/ghost/versions/5.2.2/core/server/data/migrations/utils/migrations.js:54:19)
    at /var/lib/ghost/versions/5.2.2/node_modules/knex-migrator/lib/index.js:982:33
    at /var/lib/ghost/versions/5.2.2/node_modules/knex/lib/execution/transaction.js:221:22←[39m
←[39m
[2022-06-11 12:54:06] ←[35mWARN←[39m Ghost is shutting down
[2022-06-11 12:54:06] ←[35mWARN←[39m Ghost has shut down
[2022-06-11 12:54:06] ←[35mWARN←[39m Your site is now offline
[2022-06-11 12:54:06] ←[35mWARN←[39m Ghost was running for a few seconds
```

8. ブログサイトが利用できないことを確認するには、URLを更新します。

9. スナップショットからアプリケーションを復元します。

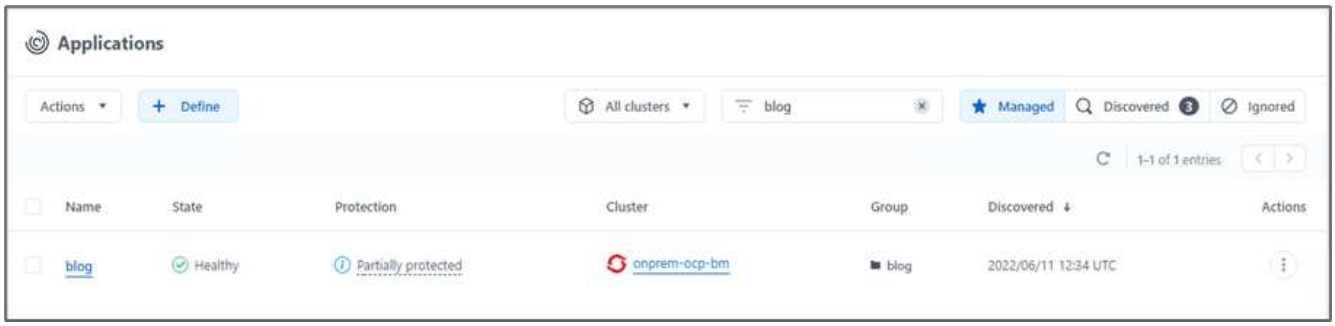


10. アプリケーションは同じOpenShiftクラスタにリストアされます。

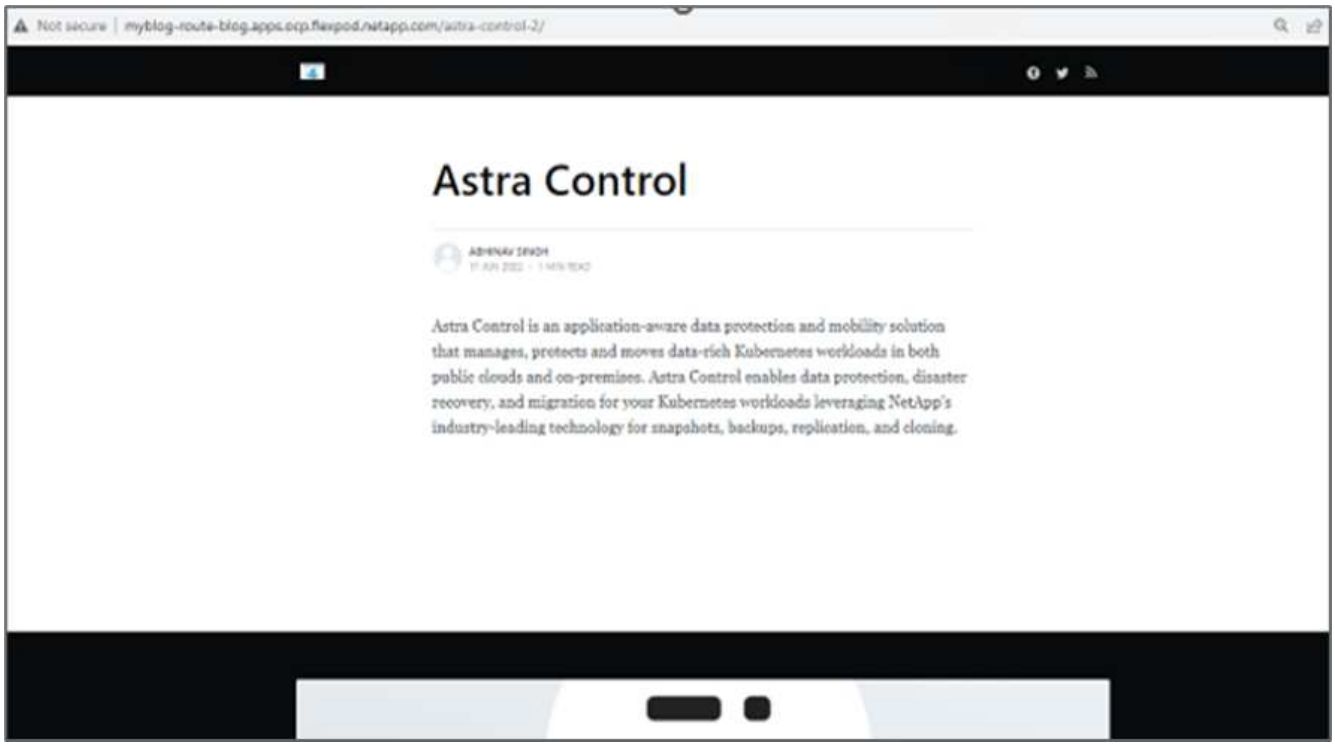


11. アプリケーションのリストアプロセスがただちに開始されます。

12. 数分後に、使用可能なスナップショットからアプリケーションが正常にリストアされます。



13. Webページが表示されるかどうかを確認するには、URLを更新します。

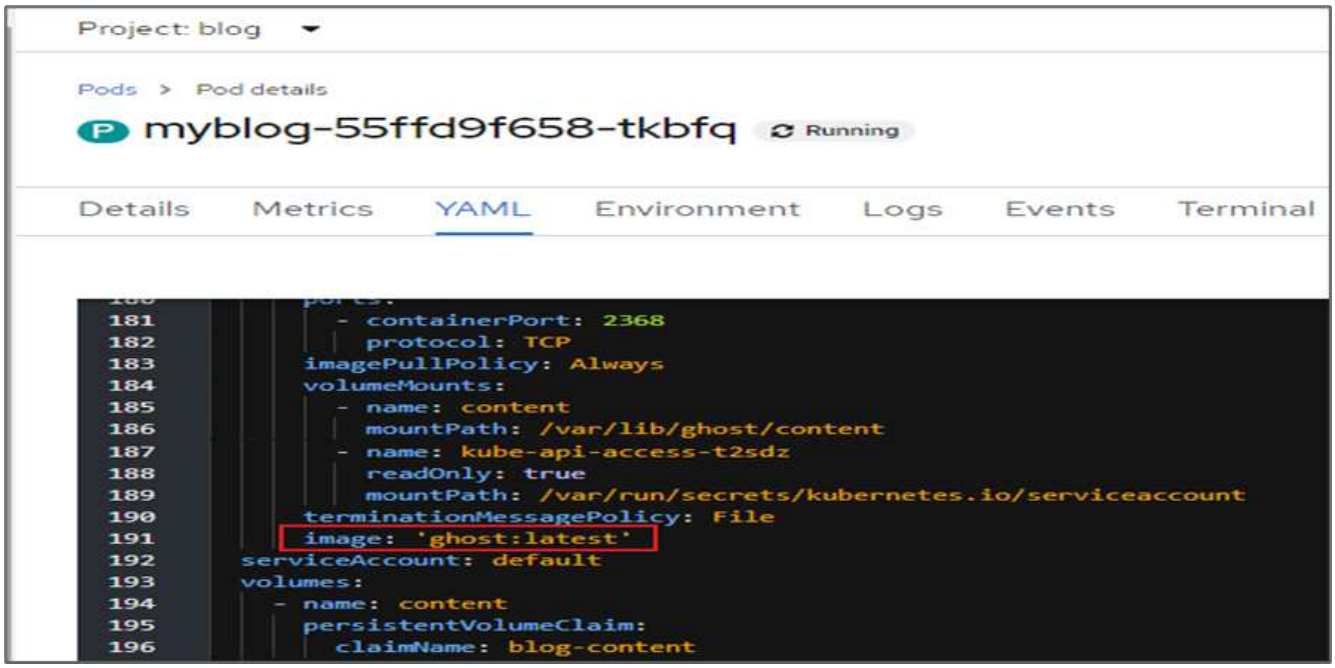


DevTestチームは、Astra Control Centerを活用して、ブログサイトアプリとその関連データをスナップショットを使用して正常にリカバリできます。

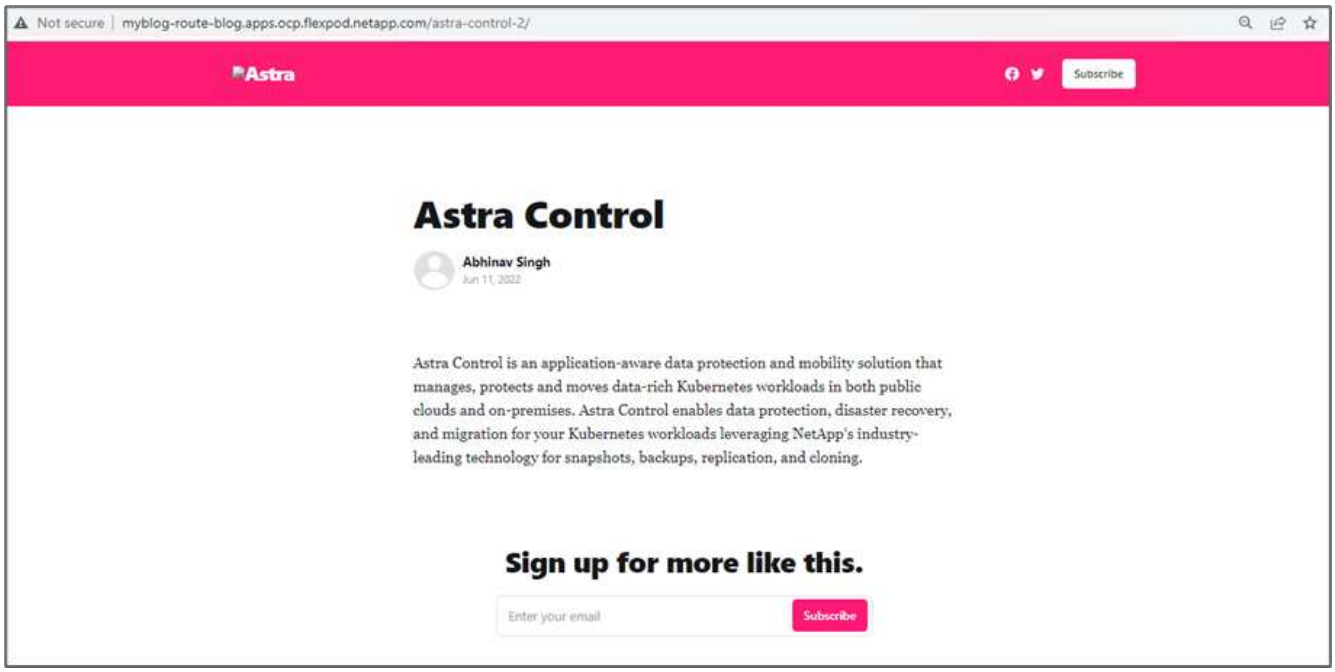
パート**2**

Astra Control Centerを使用すると、クラウド上またはオンプレミスで、クラウド上のどの場所にあるかに関係なく、アプリケーション全体をKubernetesクラスタ間でデータとともに移動できます。

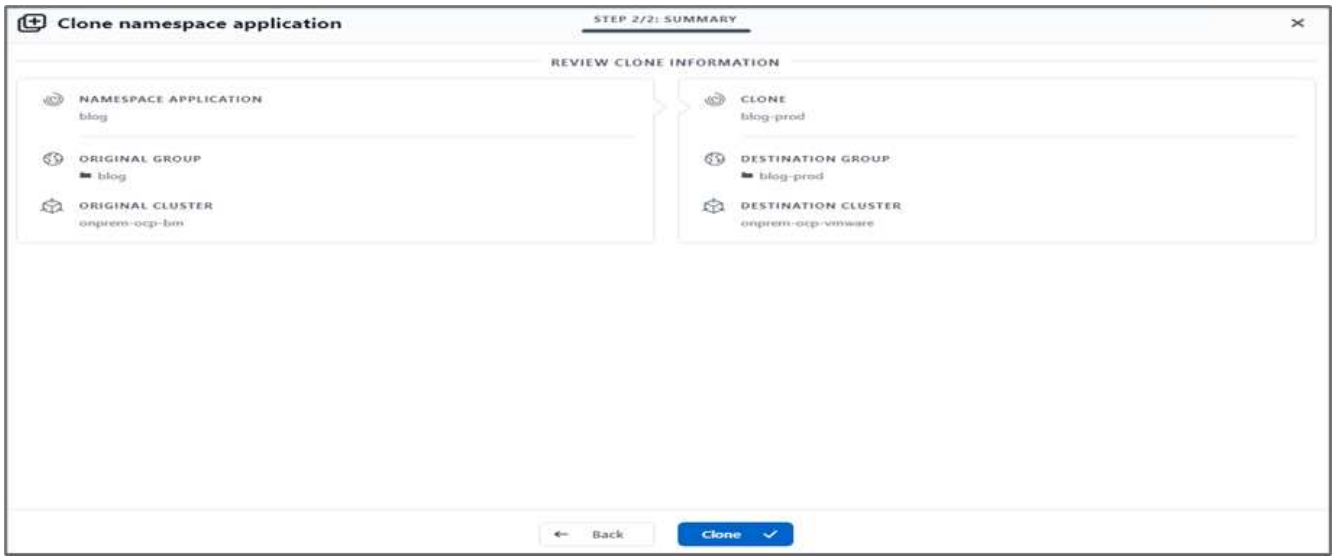
1. DevTestチームは、アプリケーションを最初にサポートされているバージョン（「ゴースト- 4.6 -アルプス」）にアップグレードしてから、最終バージョン（「ゴースト-最新」）にアップグレードして、本番環境を準備します。その後、別のFlexPod システムで実行されている本番環境のOpenShiftクラスタにクローニングされているアプリケーションをアップグレードします。
2. この時点で、アプリケーションが最新バージョンにアップグレードされ、本番環境のクラスタにクローニングできる状態になります。



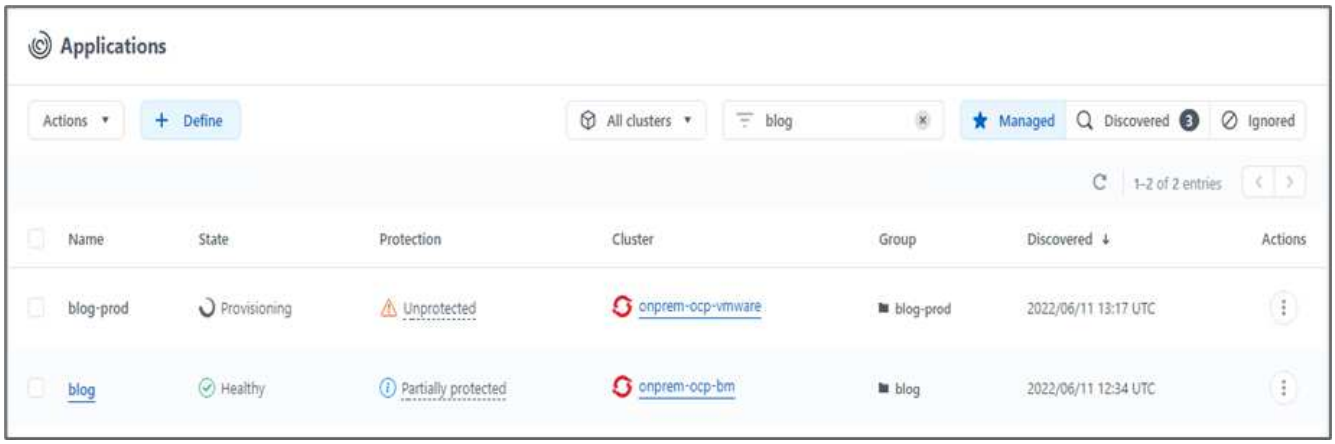
3. 新しいテーマを確認するには、ブログサイトを更新します。



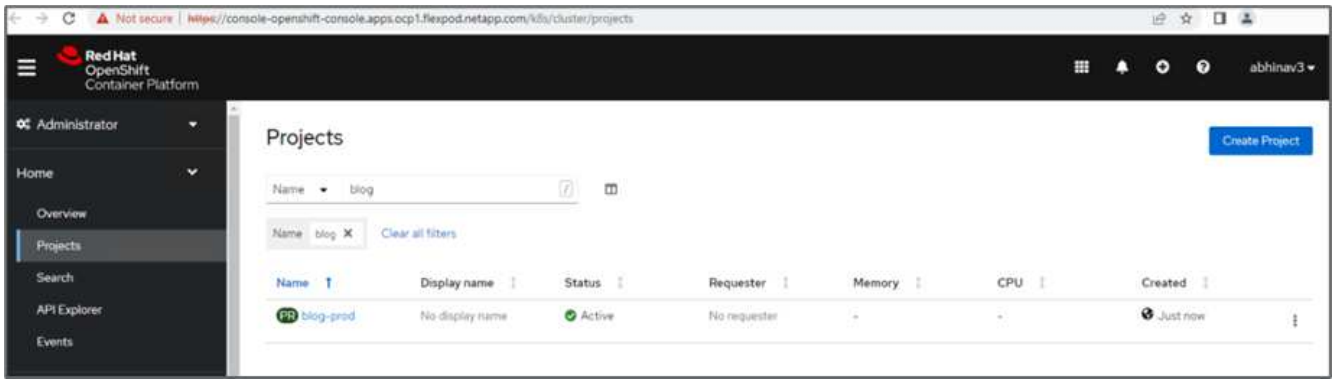
4. Astra Control Centerから、VMware vSphereで実行されている他の本番環境OpenShiftクラスタにアプリケーションをクローニングします。



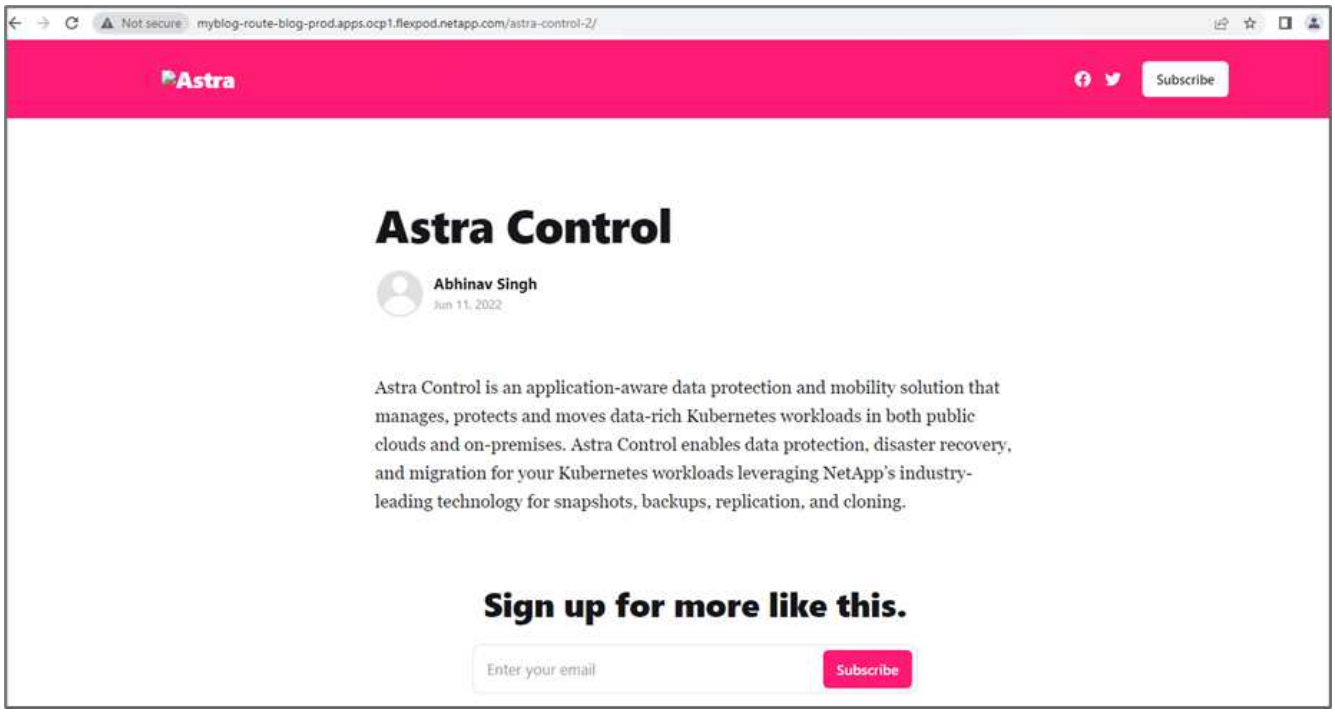
これで、本番環境のOpenShiftクラスタで新しいアプリケーションクローンがプロビジョニングされます。



5. 本番環境のOpenShiftクラスタにログインし、プロジェクトブログを検索します。



6. サイドメニューから、Networking > Routesを選択し、Locationの下のURLをクリックします。同じホームページとコンテンツが表示されます。



これでAstra Control Center解決策 の検証は終了です。Kubernetesクラスタが配置されている場所に関係なく、アプリケーション全体とそのデータを1つのKubernetesクラスタから別のクラスタにクローニングできるようになりました。

"次は終わりです"

まとめ

"Previous：リモートバックアップを使用したアプリケーションのリカバリ。"

この解決策 では、ネットアップのAstraポートフォリオを使用して、FlexPod とAWSで実行されるコンテナ化アプリケーション向けの保護計画を実装しました。ネットアップのAstra Control CenterとAstra Tridentは、Cloud Volumes ONTAP 、Red Hat OpenShift、FlexPod インフラとともに、この解決策 のコアコンポーネントを形成しました。

Snapshotをキャプチャしてアプリケーションの保護を実証し、クラウド環境とオンプレミス環境で実行されているKubernetesクラスタ間でアプリケーションをリストアするフルコピーバックアップを実行しました。

また、Kubernetesクラスタ間でアプリケーションのクローニングを実演し、お客様が希望する場所で選択したKubernetesクラスタにアプリケーションを移行できるようにする方法についても説明しました。

FlexPod は絶えず進化しているため、お客様はアプリケーションやビジネス提供プロセスを最新化できます。この解決策 を使用することで、FlexPod のお客様は、解決策 のコストを低く抑えながら、短期またはフルタイムのDRプランを作成できる場所としてパブリッククラウドを使用して、クラウドネイティブアプリケーション向けのBCDRプランを自信を持って構築できます。

Astra Controlを使用すると、クラスタの配置場所に関係なく、アプリケーション全体をKubernetesクラスタ間でデータとともに移動できます。また、クラウドネイティブアプリケーションの導入、運用、保護を高速化するのにも役立ちます。

トラブルシューティング

トラブルシューティングのガイダンスについては、を参照してください "オンラインドキュメント"。

追加情報の参照先

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 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"

- Ansibleを使用して、VMwareのコードとしてInfrastructureを使用したFlexPod の導入

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

- Ansibleを使用したRed Hat OpenShift Bare Metalのコードとしてのインフラを使用したFlexPod 導入

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

- 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.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Cisco Intersightのデータシート

  "https://intersight.com/help/saas/home"

- ネットアップAstraのドキュメント

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- ネットアップアストラコントロールセンター

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- ネットアップアストラト Trident

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

- NetApp Cloud Manager の略

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP の略

"https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift のサービスです

  "https://www.openshift.com/"

- NetApp Interoperability Matrix Tool で確認できます

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

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7月	ACC 22.04.0用リリース。

NetApp Cloud Insights for FlexPod の略

TR-4868 ：『 NetApp Cloud Insights for FlexPod 』

ネットアップ、 Alan Cowles 氏

協力：

このテクニカルレポートで詳述されている解決策は、 ONTAP データセンター解決策の一部として導入されている NetApp AFF を実行している NetApp Cloud Insights A800 ストレージシステムを監視するために、 NetApp FlexPod サービスを設定する方法を示しています。

お客様にもたらされる価値

ここで詳述する解決策は、フル機能を備えたハイブリッドクラウド環境向けの監視解決策に関心があり、ONTAP をプライマリストレージシステムとして導入するお客様に価値を提供します。これには、ネットアップの AFF および FAS ストレージシステムを使用する FlexPod 環境が含まれます。

ユースケース

この解決策環境のユースケースは次のとおりです。

- FlexPod 解決策の一部として導入された ONTAP ストレージシステムのさまざまなリソースと使用率を監視する必要がある組織。
- AFF または FAS システムを使用して FlexPod 解決策で発生したインシデントのトラブルシューティングを行い、解決時間を短縮したいと考えている組織。
- コストの最適化を検討している組織では、無駄なリソースに関する詳細な情報を提供するカスタマイズされたダッシュボードや、 ONTAP などの FlexPod 環境でコスト削減を実現できる場所などが挙げられます。

対象読者

解決策の対象となるグループは次のとおりです。

- コストの最適化とビジネス継続性に関心を持つ IT エグゼクティブとその関係者。
- データセンターやハイブリッドクラウドの設計と管理に関心のあるソリューションアーキテクト。
- トラブルシューティングとインシデント解決を担当するテクニカルサポートエンジニア。

Cloud Insights は、計画、トラブルシューティング、メンテナンス、およびビジネス継続性の確保に役立ついくつかの有用なデータタイプを提供するように設定できます。FlexPod Datacenter 解決策 with Cloud Insights を監視し、集計データをわかりやすいカスタマイズされたダッシュボードに表示することで、 ニーズに応じて環境内のリソースをいつ拡張する必要があるかを予測できるだけでなく、システム内で問題の原因となっている特定のアプリケーションやストレージボリュームを特定することもできます。これにより、監視対象のインフラストラクチャが予測可能で、期待どおりに動作することが保証されます。これにより、組織は定義済みの SLA を提供し、必要に応じてインフラストラクチャを拡張できるようになり、無駄と追加コストを削減できます。

アーキテクチャ

このセクションでは、 Cloud Insights で監視される NetApp AFF A800 システムを含む、FlexPod データセンター統合インフラのアーキテクチャについて説明します。

解決策テクノロジ

FlexPod Datacenter 解決策には、次に示す最小コンポーネントが含まれており、可用性が高く、拡張性に優れ、検証済みで、サポートされている統合インフラ環境を構築できます。

- NetApp ONTAP ストレージノード × 2 （ HA ペア × 1 ）
- Cisco Nexus データセンターネットワークスイッチ × 2
- Cisco MDS ファブリックスイッチ × 2 （ FC 環境ではオプション）
- Cisco UCS ファブリックインターコネクト × 2
- 1 台の Cisco UCS ブレードシャーシに 2 台の Cisco UCS B シリーズブレードサーバを搭載

または

- Cisco UCS C シリーズラックマウントサーバ × 2

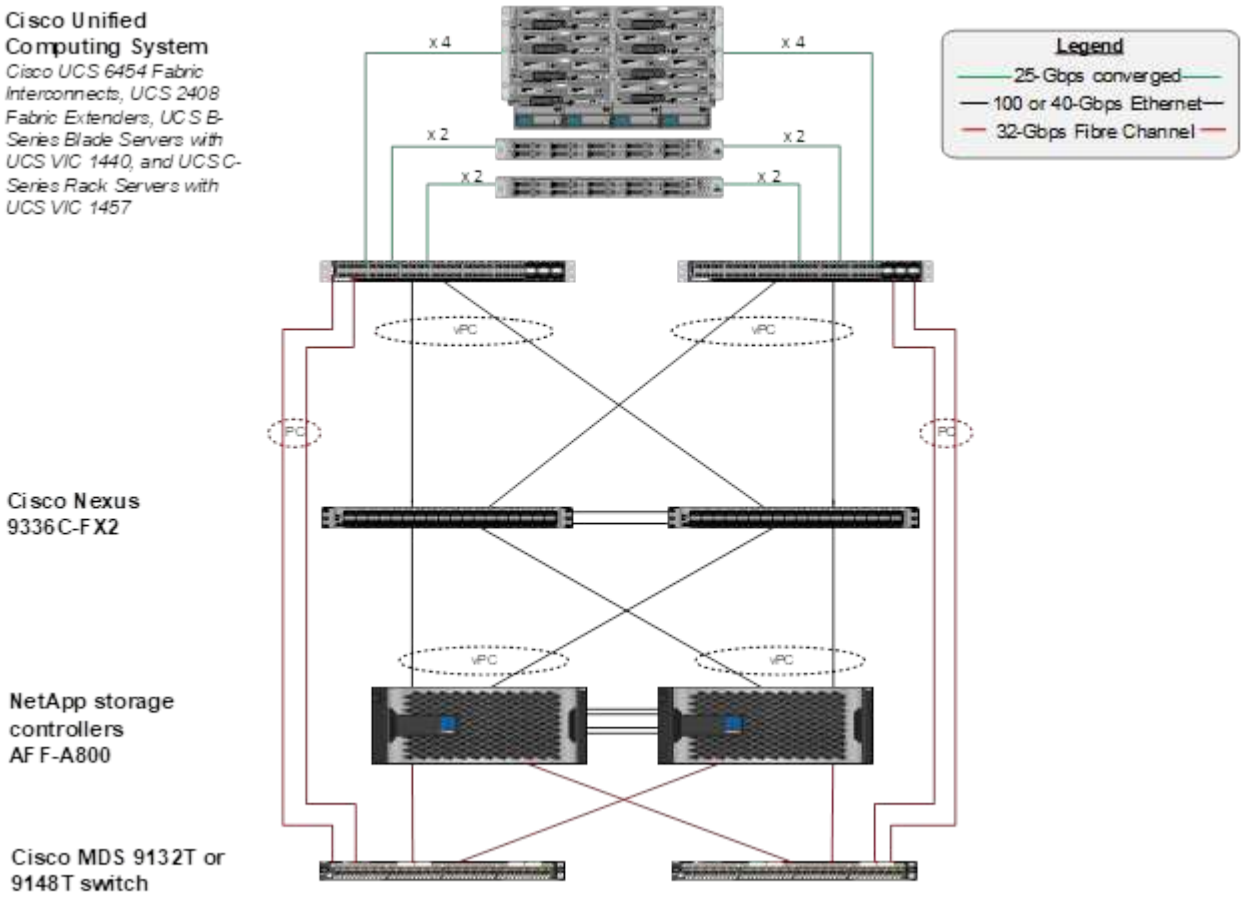
Cloud Insights でデータを収集するには、 FlexPod データセンター環境内、またはデータを収集するコンポーネントにアクセスできる場所に、仮想マシンまたは物理マシンとして Acquisition Unit を導入する必要があります。Acquisition Unit ソフトウェアは、サポートされている複数の Windows または Linux オペレーティングシステムを実行するシステムにインストールできます。次の表に、このソフトウェアの解決策コンポーネントを示します。

オペレーティングシステム	バージョン
Microsoft Windows の場合	10.
Microsoft Windows Server の場合	2012 、 2012 R2 、 2016 、 2019
Red Hat Enterprise Linux の場合	7.2 – 7.6

オペレーティングシステム	バージョン
CentOS の場合	7.2 – 7.6
Oracle Enterprise Linux の場合	7.5
Debian	9.
Ubuntu	18.04 LTS

アーキテクチャ図

次の図に、解決策のアーキテクチャを示します。



ハードウェア要件

次の表に、解決策の実装に必要なハードウェアコンポーネントを示します。解決策の特定の実装で使用されるハードウェアコンポーネントは、お客様の要件に応じて異なる場合があります。

ハードウェア	数量
Cisco Nexus 9336C-FX2	2.
Cisco UCS 6454 ファブリックインターコネクト	2.
Cisco UCS 5108 ブレードシャーシ	1.
Cisco UCS 2408 ファブリックエクステンダ	2.

ハードウェア	数量
Cisco UCS B200 M5 ブレード	2.
NetApp AFF A800	2.

ソフトウェア要件

次の表に、解決策の実装に必要なソフトウェアコンポーネントを示します。解決策の特定の実装で使用されるソフトウェアコンポーネントは、お客様の要件に応じて異なる場合があります。

ソフトウェア	バージョン
Cisco Nexus ファームウェア	9.3 （ 5 ）
Cisco UCS のバージョン	4.1 （ 2a ）
NetApp ONTAP のバージョン	9.7
NetApp Cloud Insights のバージョン	2020 年 9 月、基本
Red Hat Enterprise Linux の場合	7.6
VMware vSphere の場合	6.7U3

ユースケースの詳細

この解決策環境のユースケースは次のとおりです。

- NetApp Active IQ デジタルアドバイザに提供されたデータを基に環境を分析し、ストレージシステムのリスクとストレージ最適化に関する推奨事項を評価します。
- FlexPod Datacenter 解決策に導入された ONTAP ストレージ・システムの問題をトラブルシューティングするには、システム統計情報をリアルタイムで調べます。
- ONTAP データセンター統合インフラに導入された FlexPod ストレージシステムの特定の関心ポイントを簡単に監視できるように、カスタマイズしたダッシュボードを生成できます。

設計上の考慮事項

FlexPod Datacenter 解決策は、シスコとネットアップが設計した統合インフラです。エンタープライズワークロードを実行するための、動的で可用性が高く、拡張性に優れたデータセンター環境を提供します。解決策のコンピューティングリソースとネットワークリソースは Cisco UCS および Nexus 製品から提供され、ストレージリソースは ONTAP ストレージシステムから提供されます。解決策設計は、更新されたハードウェアモデルまたはソフトウェアとファームウェアのバージョンが利用可能になったときに、定期的に拡張されます。これらの詳細情報に加え、解決策の設計と導入に関するベストプラクティスも、 Cisco Validated Design （ CVD ）または NetApp Verified Architecture （ NVA ）ドキュメントにキャプチャされ、定期的に公開されています。

FlexPod Datacenter 解決策の設計に関する最新の CVD ドキュメントを参照できます "こちらをご覧ください"。

Cloud Insights for FlexPod を導入します

解決策を導入するには、次のタスクを実行する必要があります。

1. Cloud Insights サービスに登録します
2. Acquisition Unit として設定する VMware 仮想マシン（ VM ）を作成します
3. Red Hat Enterprise Linux （ RHEL ）ホストをインストールします
4. Cloud Insights ポータルで Acquisition Unit インスタンスを作成し、ソフトウェアをインストールします
5. FlexPod データセンターから Cloud Insights に監視対象のストレージシステムを追加します。

NetApp Cloud Insights サービスに登録します

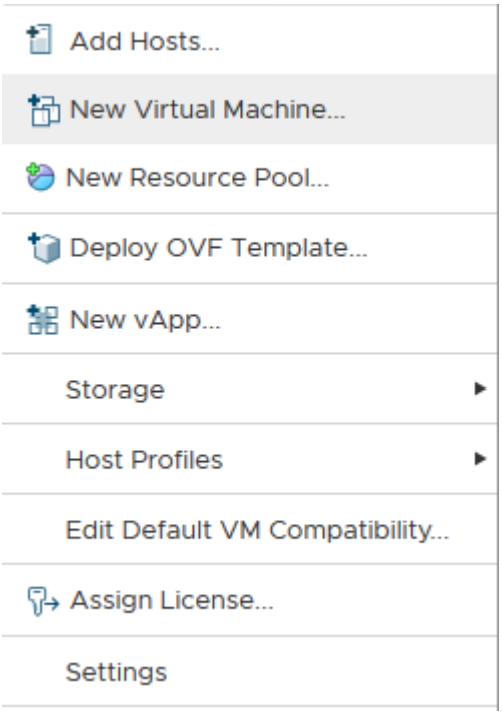
NetApp Cloud Insights サービスに登録するには、次の手順を実行します。

1. に進みます "https://cloud.netapp.com/cloud-insights"
2. 画面の中央にあるボタンをクリックして 14 日間の無償トライアルを開始するか、右上にあるリンクをクリックして、既存の NetApp Cloud Central アカウントに登録またはログインします。

Acquisition Unit として設定する VMware 仮想マシンを作成する

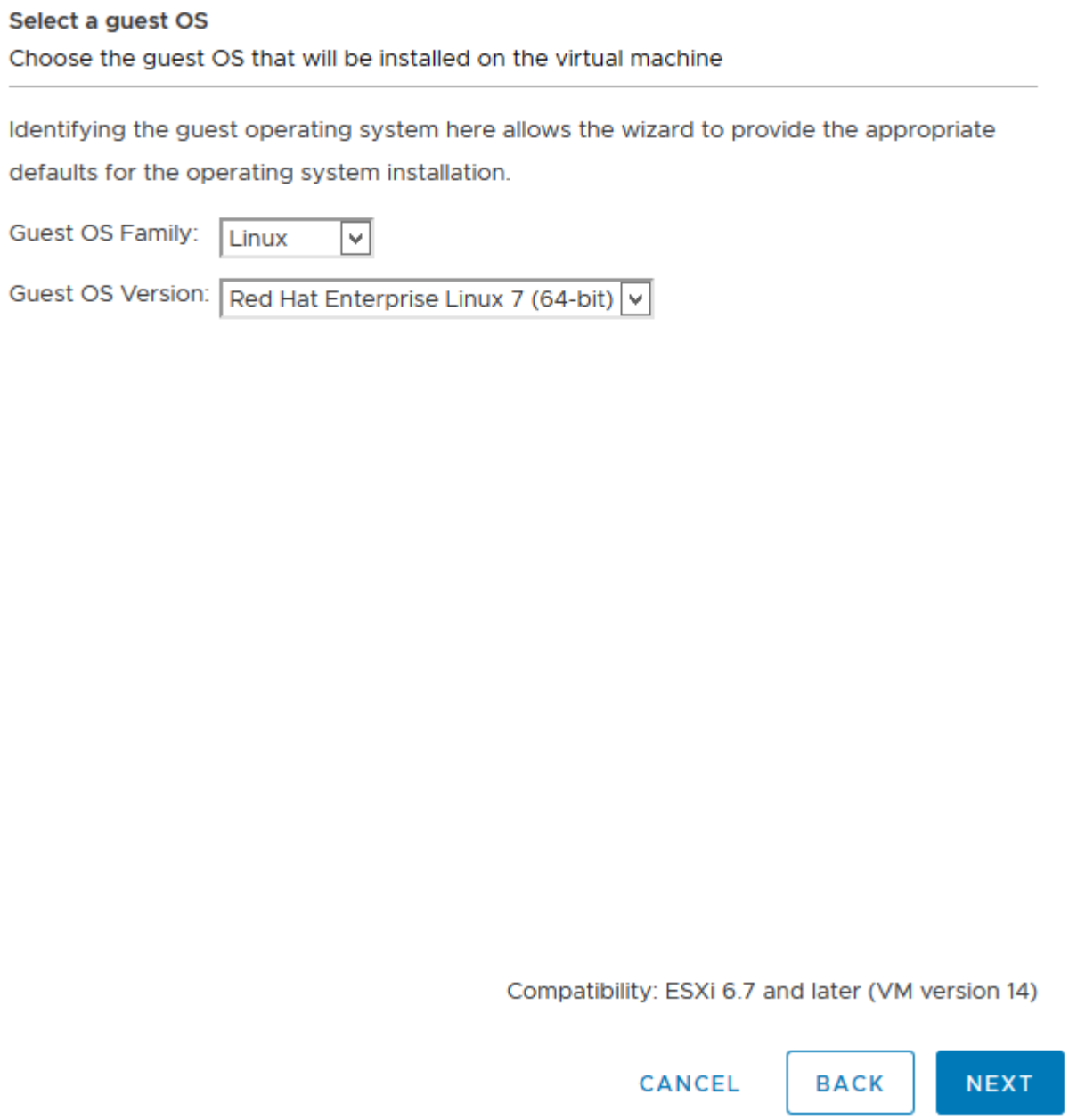
VMware VM を作成して Acquisition Unit として設定するには、次の手順を実行します。

1. Web ブラウザを起動して VMware vSphere にログインし、 VM をホストするクラスタを選択します。
2. そのクラスタを右クリックし、メニューから [仮想マシンの作成] を選択します。



3. 新規仮想マシンウィザードで、次へをクリックします。
4. VM の名前を指定し、インストール先のデータセンターを選択して、 Next （次へ）をクリックします。

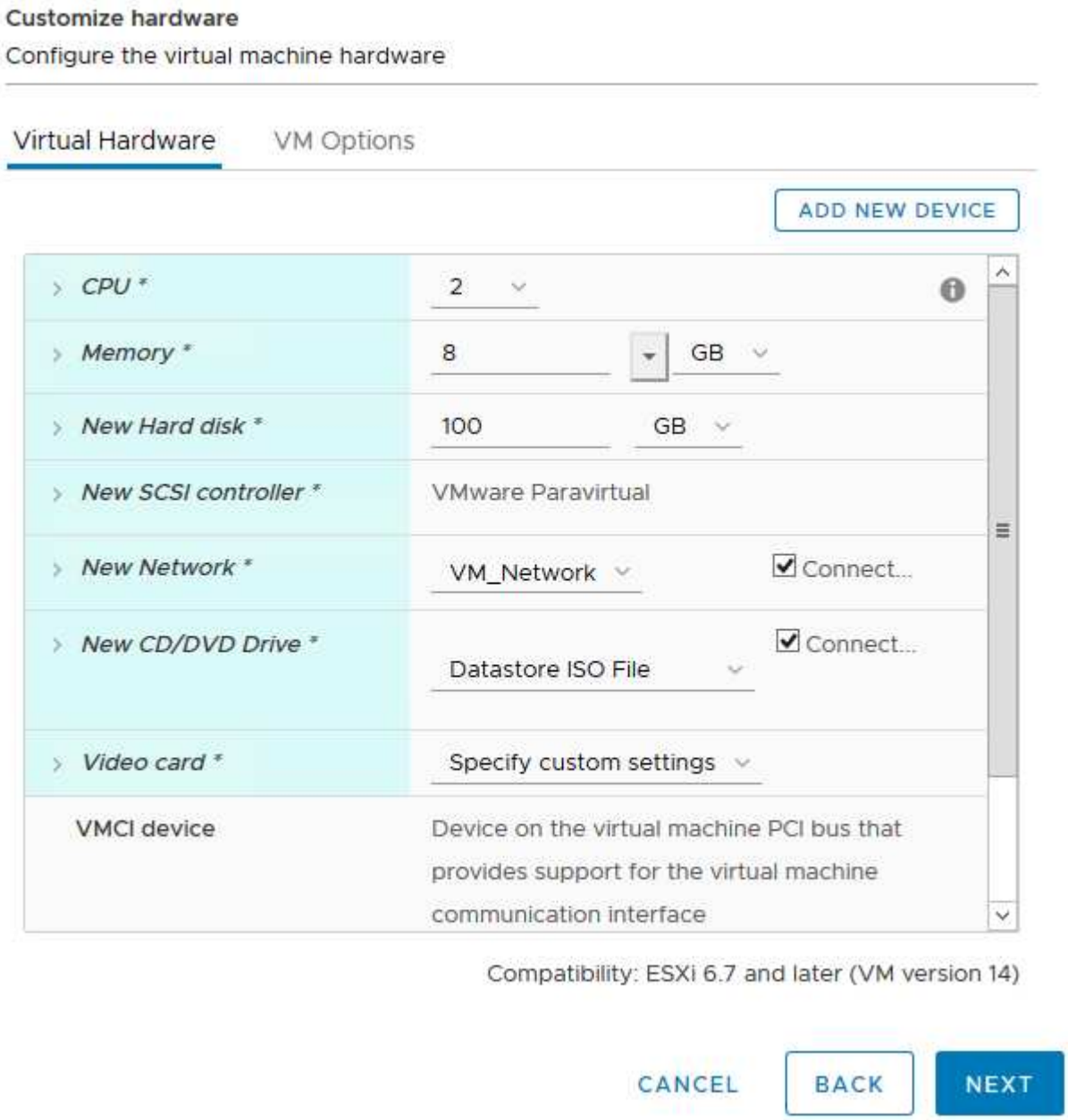
5. 次のページで、 VM のインストール先となるクラスタ、ノード、またはリソースグループを選択し、 [次へ] をクリックします。
6. VM をホストする共有データストアを選択し、 Next （次へ）をクリックします。
7. VM の互換性モードが ESXi 6.7 以降に設定されていることを確認し '[次へ] をクリックします
8. [Guest OS Family Linux, Guest OS Version: Red Hat Enterprise Linux 7 (64 bit)] を選択します。



9. 次のページでは、 VM のハードウェアリソースをカスタマイズできます。Cloud Insights Acquisition Unit には、次のリソースが必要です。リソースを選択したら、 [次へ] をクリックします。
   a. CPU × 2
   b. 8GB の RAM
   c. 100GB のハードディスクスペースが必要です

d. ポート 443 で SSL 接続を介して FlexPod データセンターおよび Cloud Insights サーバのリソースにアクセスできるネットワーク。

e. 選択した Linux ディストリビューション（ Red Hat Enterprise Linux ）の ISO イメージをブート元として指定します。

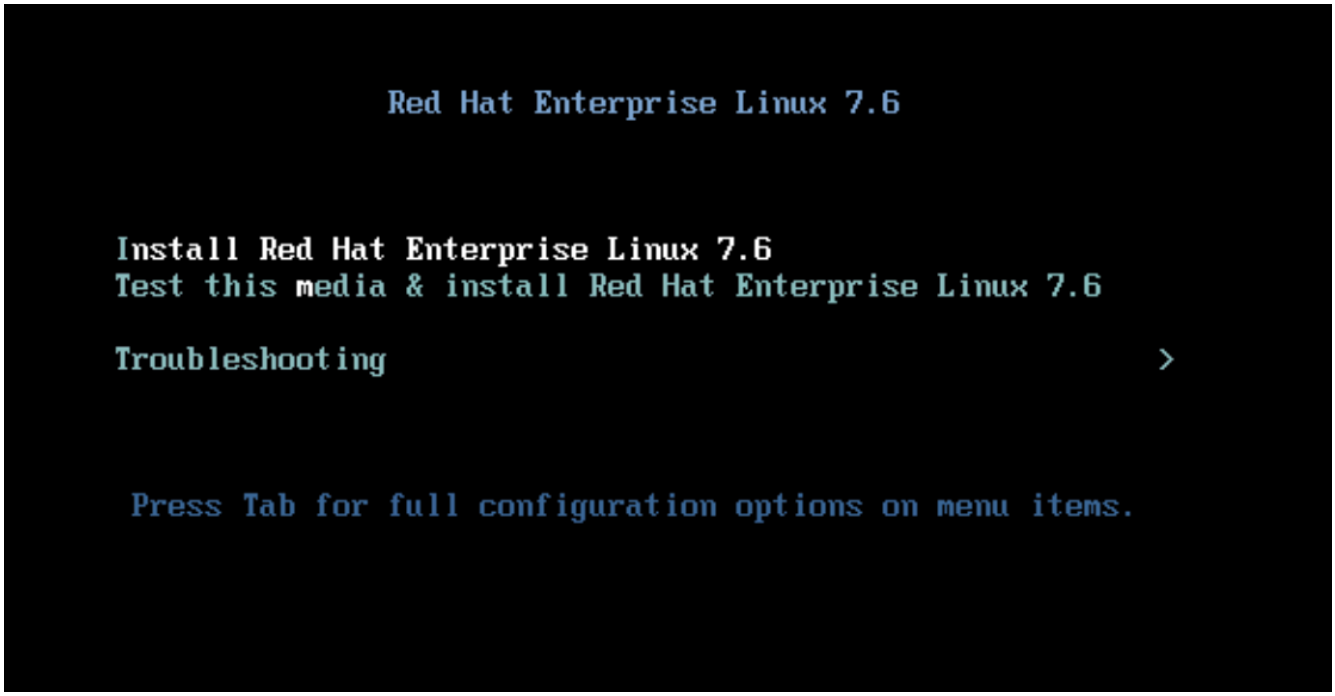


10. VM を作成するには、 [Ready to Complete] ページで設定を確認し、 [Finish] をクリックします。

Red Hat Enterprise Linux をインストールします

Red Hat Enterprise Linux をインストールするには、次の手順を実行します。

1. VM の電源をオンにし、ウィンドウをクリックして仮想コンソールを起動し、 Red Hat Enterprise Linux 7.6 をインストールするオプションを選択します。



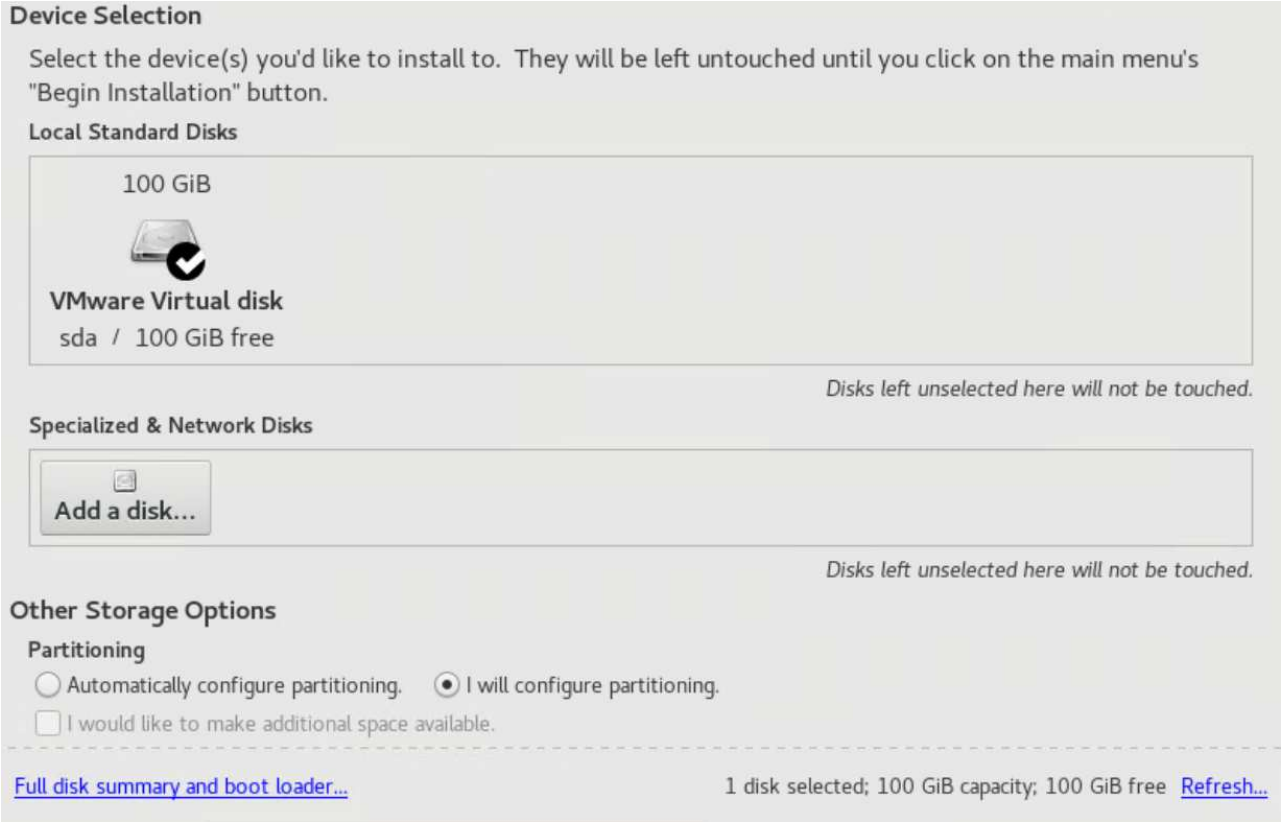
2. 使用する言語を選択し、 [続行] をクリックします。

   次のページはインストールの概要です。これらのオプションのほとんどはデフォルト設定のままでかまいません。

3. 次のオプションを実行して、ストレージレイアウトをカスタマイズする必要があります。

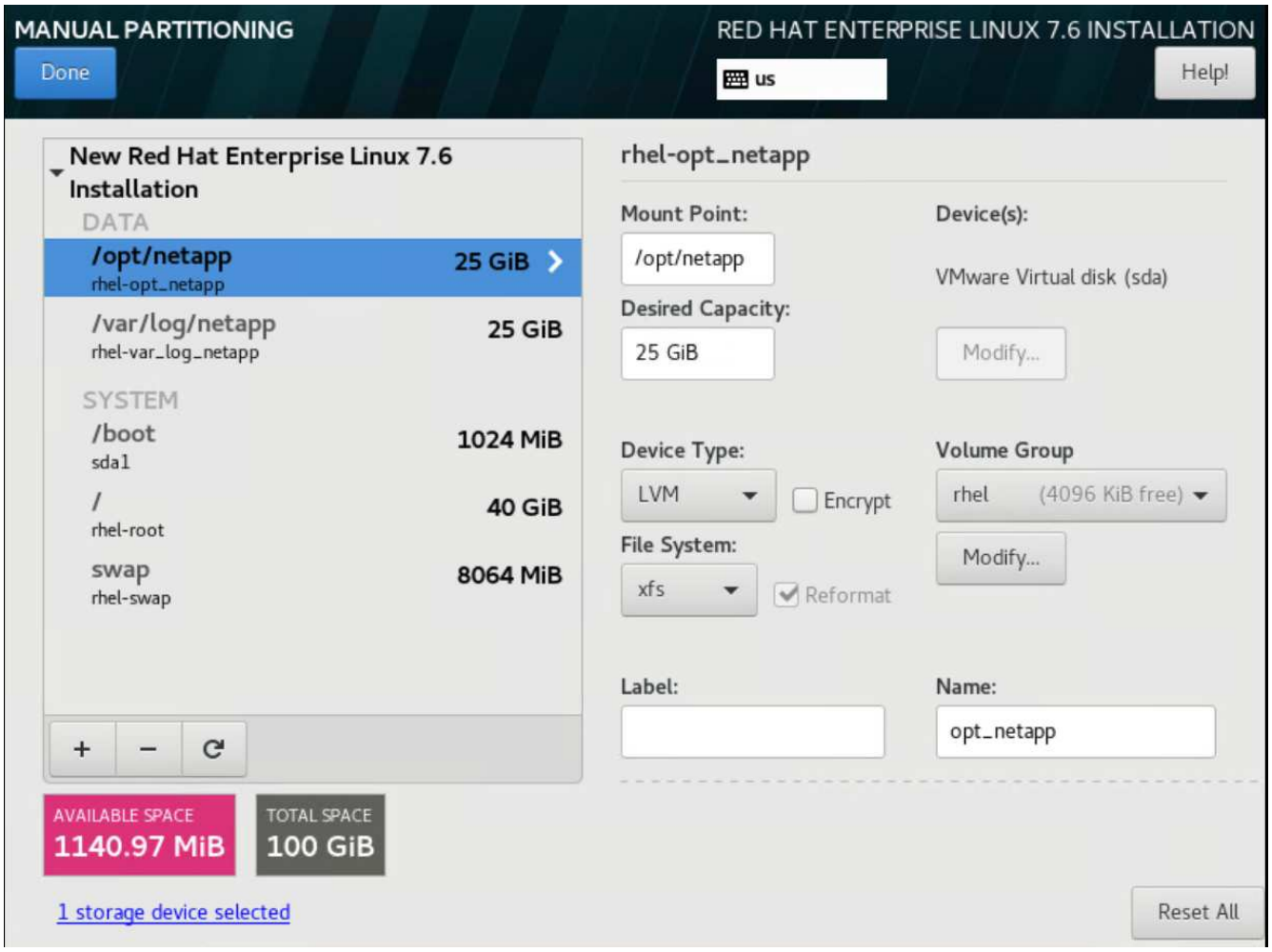
   a. サーバのパーティションをカスタマイズするには、インストール先をクリックします。

   b. VMware 仮想ディスク 100GiB がブラックチェックマークで選択されていることを確認し、 [I will Configure Partitioning （パーティションの設定）] オプションボタンを選択します。



c. 完了をクリックします。

新しいメニューが表示され、パーティションテーブルをカスタマイズできます。それぞれ 25 GB を '/opt/NetApp' と '/var/log/netapp' 専用にします残りのストレージをシステムに自動的に割り当てることができます。

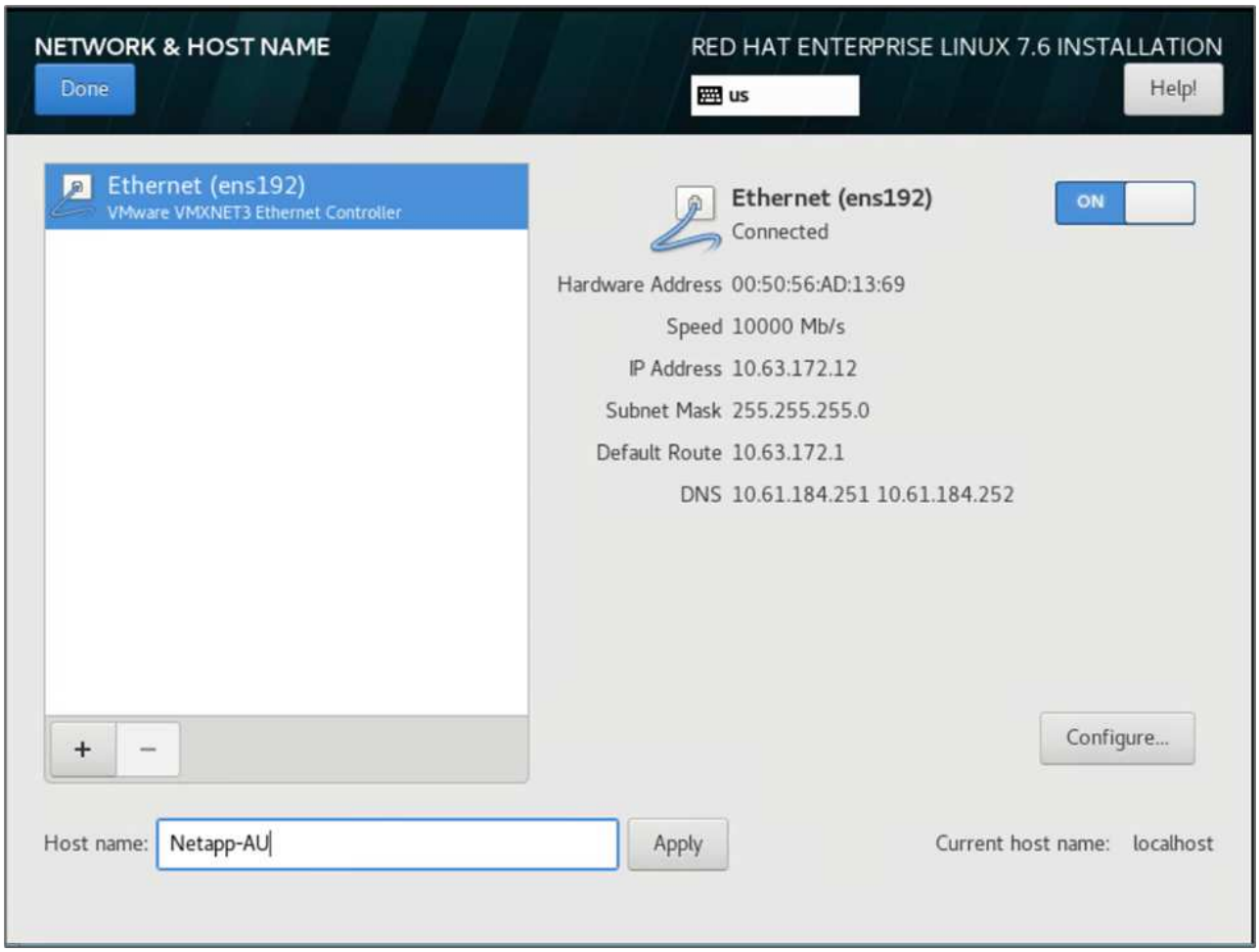


a. [インストールの概要] に戻るには、 [完了] をクリックします。

4. [ネットワークとホスト名] をクリックします。

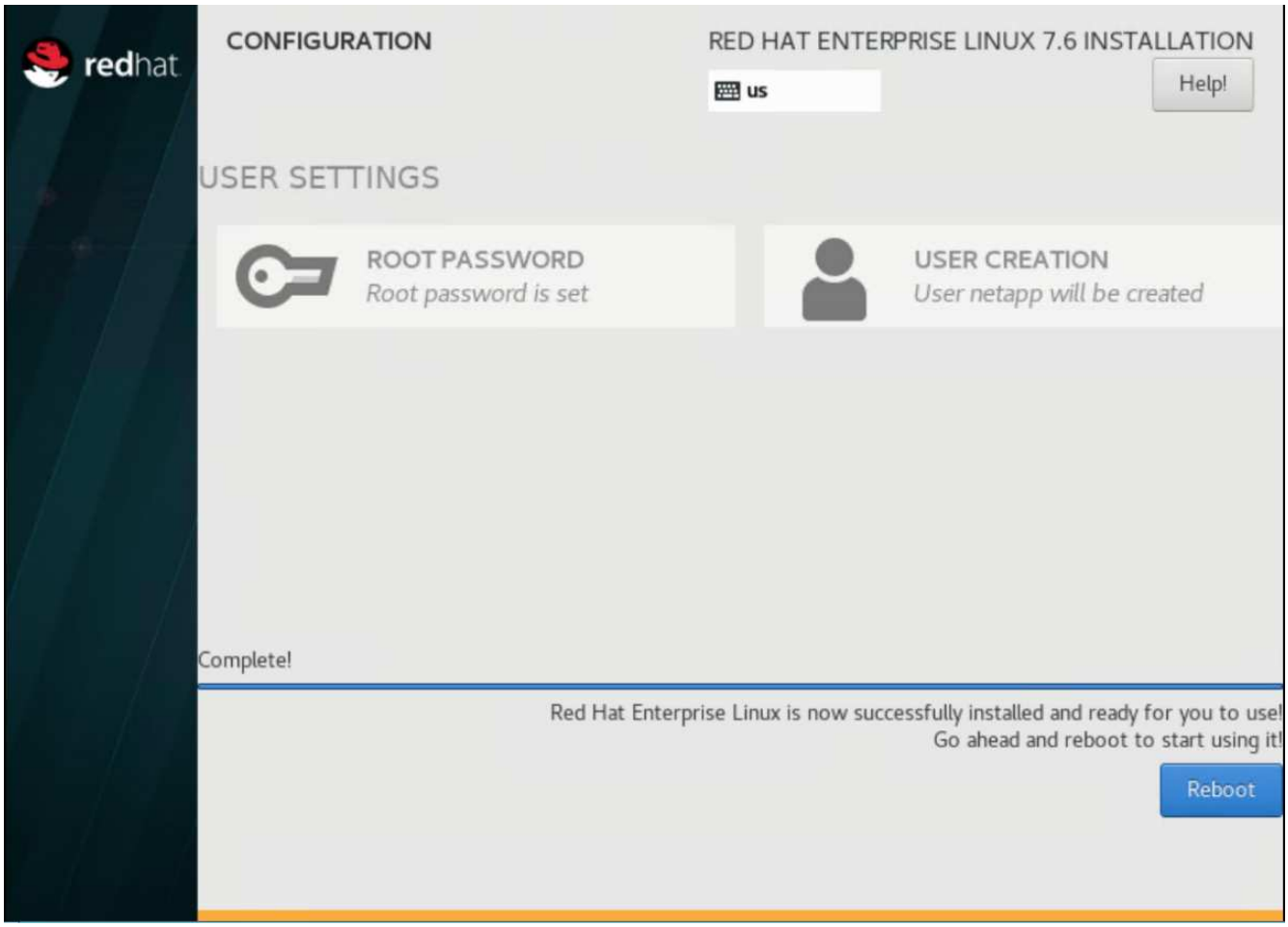
   a. サーバのホスト名を入力します。

   b. スライダボタンをクリックして、ネットワークアダプタの電源をオンにします。ネットワークに Dynamic Host Configuration Protocol （ DHCP ；動的ホスト構成プロトコル）が設定されている場合は、 IP アドレスが割り当てられます。表示されない場合は、 Configure （設定）をクリックし、アドレスを手動で割り当てます。



c. 。[完了] をクリックして、 [インストールの概要] に戻ります。

5. [インストールの概要] ページで、 [インストールの開始] をクリックします。
6. インストールの進行状況ページで、 root パスワードを設定するか、ローカルユーザーアカウントを作成できます。インストールが完了したら、 Reboot （再起動）をクリックしてサーバを再起動します。



7. システムが再起動したら、サーバにログインし、 Red Hat Subscription Manager に登録します。

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

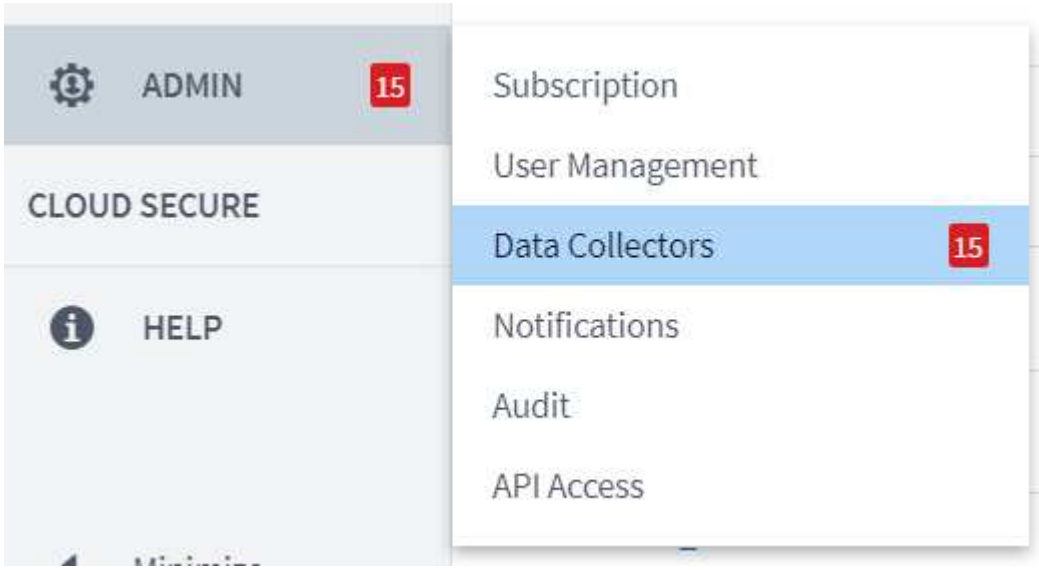
8. Red Hat Enterprise Linux のサブスクリプションを追加します。

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Cloud Insights ポータルで **Acquisition Unit** インスタンスを作成し、ソフトウェアをインストールする

Cloud Insights ポータルで Acquisition Unit インスタンスを作成してソフトウェアをインストールするには、次の手順を実行します。

1. Cloud Insights のホームページで、左側のメインメニューの Admin エントリにカーソルを合わせ、メニューから Data Collectors を選択します。

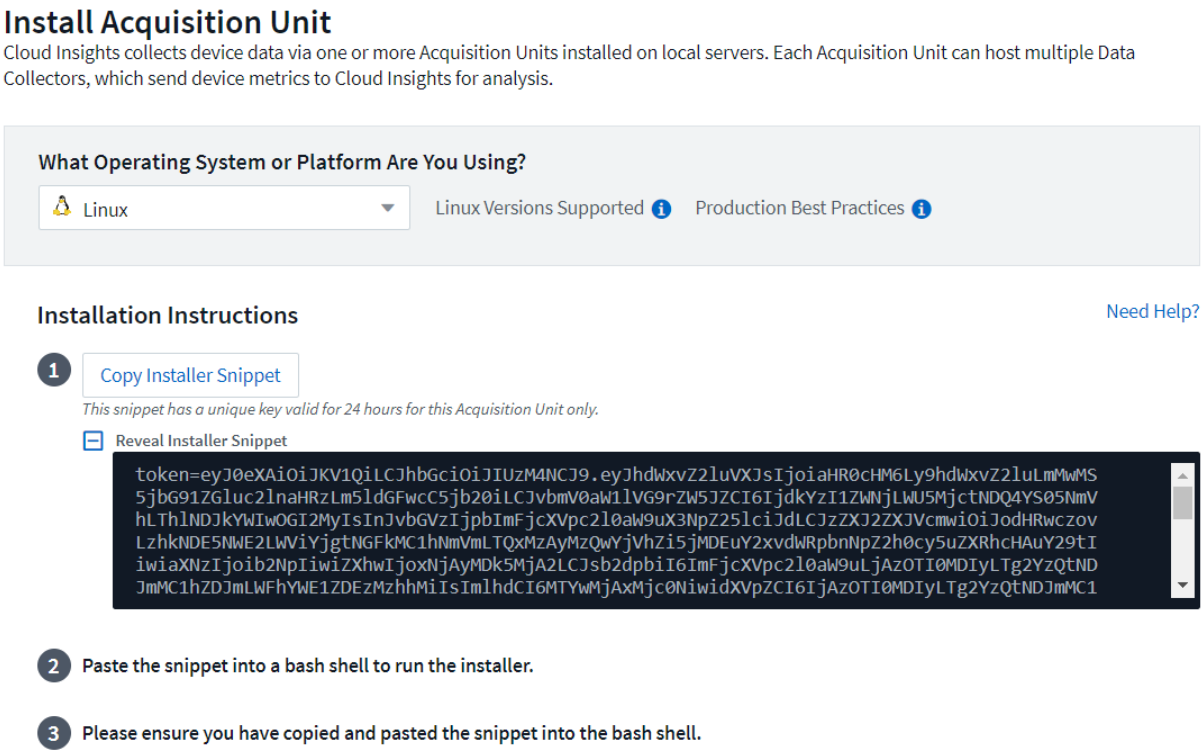


2. データコレクタページの上部中央で、 Acquisition Unit のリンクをクリックします。

3. 新しい Acquisition Unit を作成するには、右側のボタンをクリックします。

4. Acquisition Unit のホストとして使用するオペレーティングシステムを選択し、 Web ページからインストールスクリプトをコピーする手順に従います。

   この例では、 Linux サーバを使用しています。これは、スニペットとトークンを提供し、ホストの CLI に貼り付けます。Web ページは Acquisition Unit への接続を待機します。



5. プロビジョニングされた Red Hat Enterprise Linux マシンの CLI にスニペットを貼り付け、 Enter キーを押します。

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

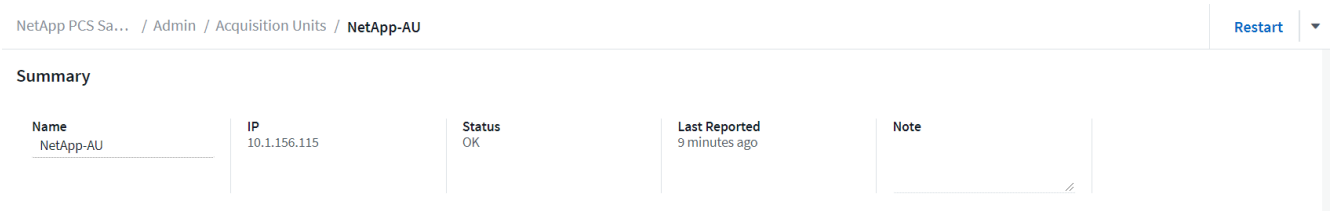
インストールプログラムは、圧縮パッケージをダウンロードしてインストールを開始します。インストールが完了すると、 Acquisition Unit が NetApp Cloud Insights に登録されたことを示すメッセージが表示されます。

```
Welcome to CloudInsights (R) ..
Acquisition Unit

NetApp (R)
Installation: /opt/netapp/cloudinsights
Logs:         /opt/netapp/cloudinsights/logs -> /var/log/netapp/cloudinsights

To control the CloudInsights service:
  sudo cloudinsights-service.sh --help
To uninstall:
  sudo cloudinsights-uninstall.sh --help

1/8 Acquisition Unit Starting
2/8 Connecting to Cloud Insights
3/8 Sending Certificate-Signing Request..
4/8 Logging in to Cloud Insights
5/8 Updating Security Settings..
6/8 Downloading Data Collection Modules
7/8 Registering to Cloud Insights
8/8 Acquisition Unit Ready

Acquisition Unit has been installed successfully.
[root@Netapp-AU ~]#
```

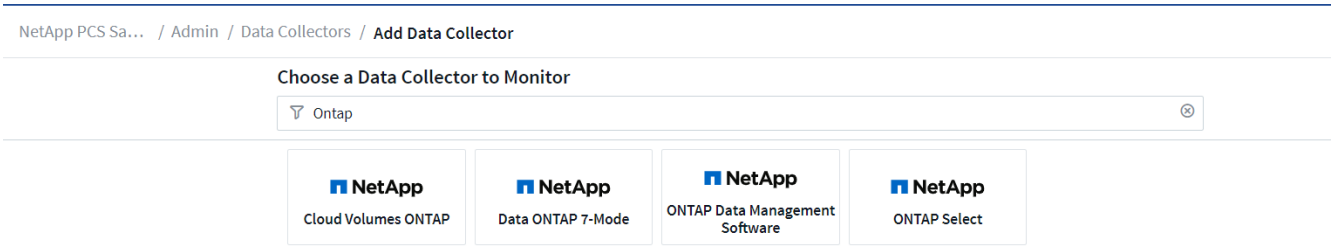
FlexPod データセンターから **Cloud Insights** に監視対象のストレージシステムを追加します

FlexPod 環境から ONTAP ストレージシステムを追加するには、次の手順を実行します。

1. Cloud Insights ポータルの Acquisition Unit ページに戻り、新たに登録されたユニットを探します。ユニットのサマリーを表示するには、ユニットをクリックします。

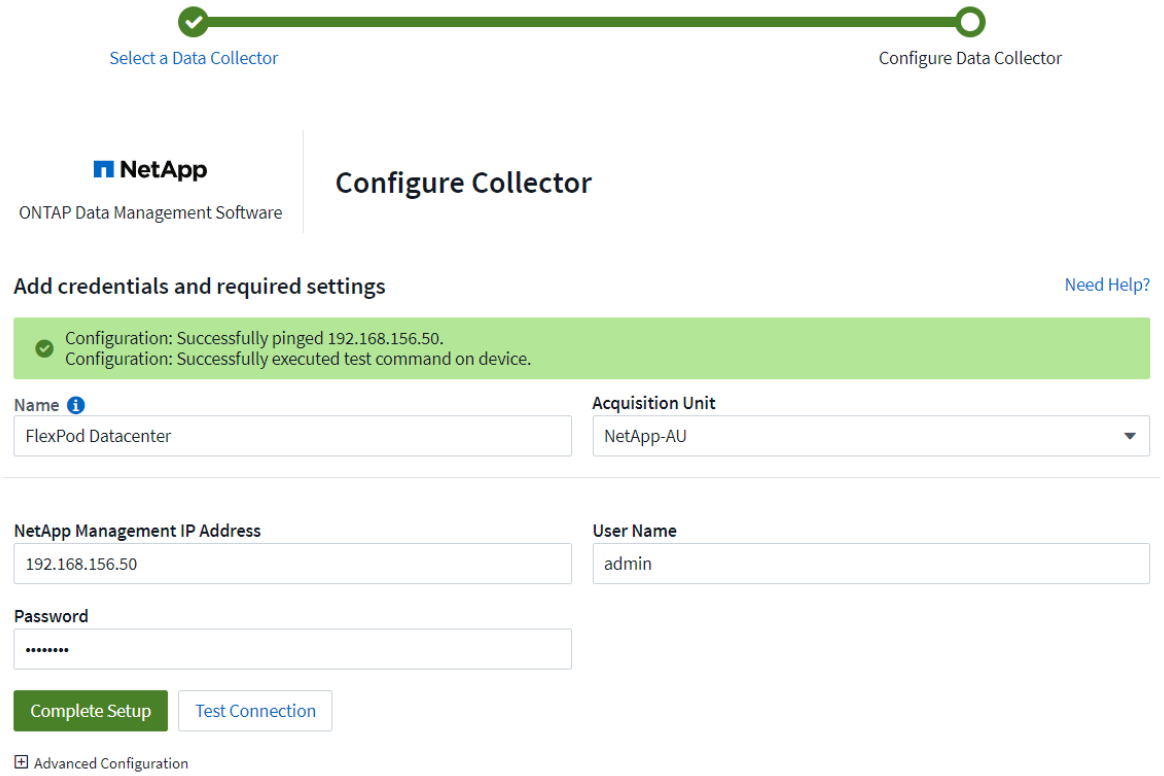


2. ストレージシステムを追加するウィザードを開始するには、概要ページでデータコレクタを作成するボタンをクリックします。最初のページには、データの収集元となるすべてのシステムが表示されます。検索バーを使用して ONTAP を検索します。



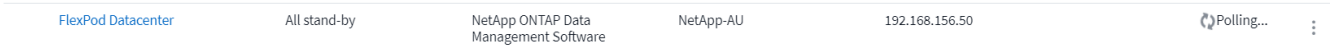
3. ONTAP データ管理ソフトウェアを選択します。

   導入環境の名前を指定し、使用する Acquisition Unit を選択するためのページが表示されます。ONTAP システムの接続情報とクレデンシャルを指定し、接続をテストして確認できます。



4. [セットアップの完了] をクリックします

   ポータルが Data Collectors ページに戻り、 Data Collector は最初のポーリングを開始して、 FlexPod データセンターの ONTAP ストレージシステムからデータを収集します。



ユースケース

FlexPod をセットアップし、解決策 Datacenter Cloud Insights を監視するように設定す

ると、ダッシュボードで実行できるいくつかのタスクを確認して、環境を評価および監視することができます。このセクションでは、 Cloud Insights の主なユースケースを 5 つ紹介します。

- Active IQ 統合
- リアルタイムダッシュボードの表示
- カスタムダッシュボードの作成
- 高度なトラブルシューティング
- ストレージの最適化

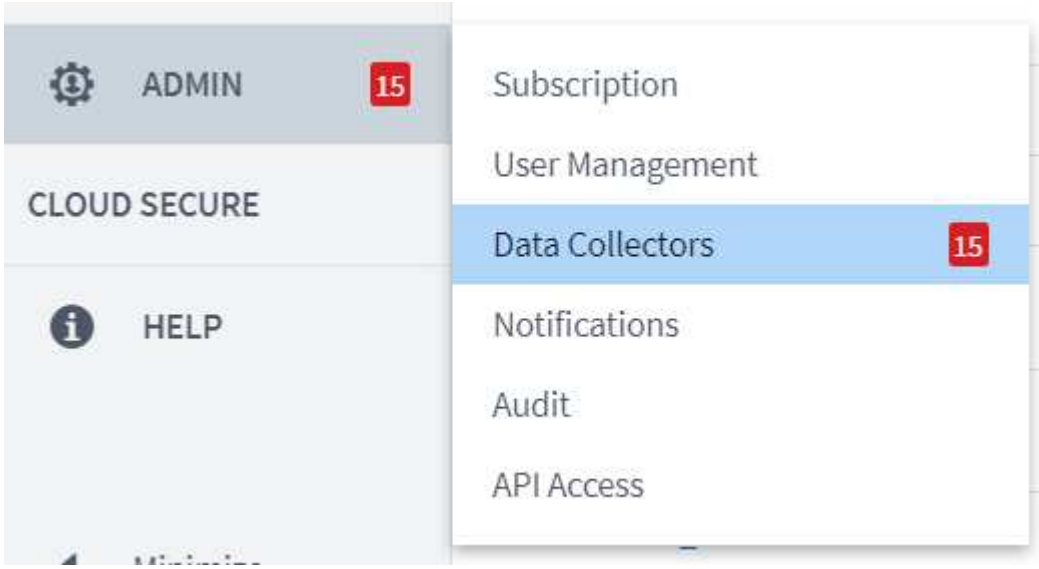
Active IQ 統合

Cloud Insights は、 Active IQ ストレージ監視プラットフォームに完全に統合されています。FlexPod Datacenter 解決策の一部として導入された ONTAP システムは、各システムに組み込まれている AutoSupport 機能を通じてネットアップに情報を送信するように、自動的に設定されます。これらのレポートは、スケジュールに基づいて生成されるか、システムで障害が検出されると動的に生成されます。AutoSupport 経由で送信されたデータは、 Cloud Insights の Active IQ メニューにある簡単にアクセスできるダッシュボードに集約されて表示されます。

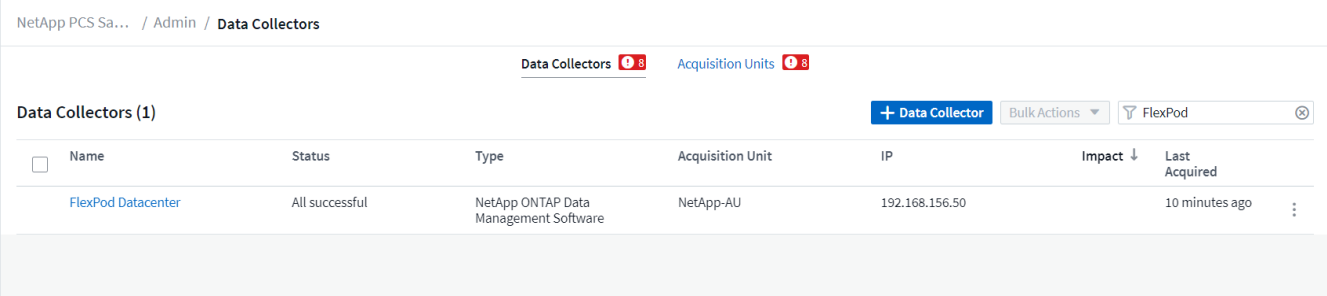
Active IQ ダッシュボードから Cloud Insights 情報にアクセスします

Cloud Insights ダッシュボードから Active IQ 情報にアクセスするには、次の手順を実行します。

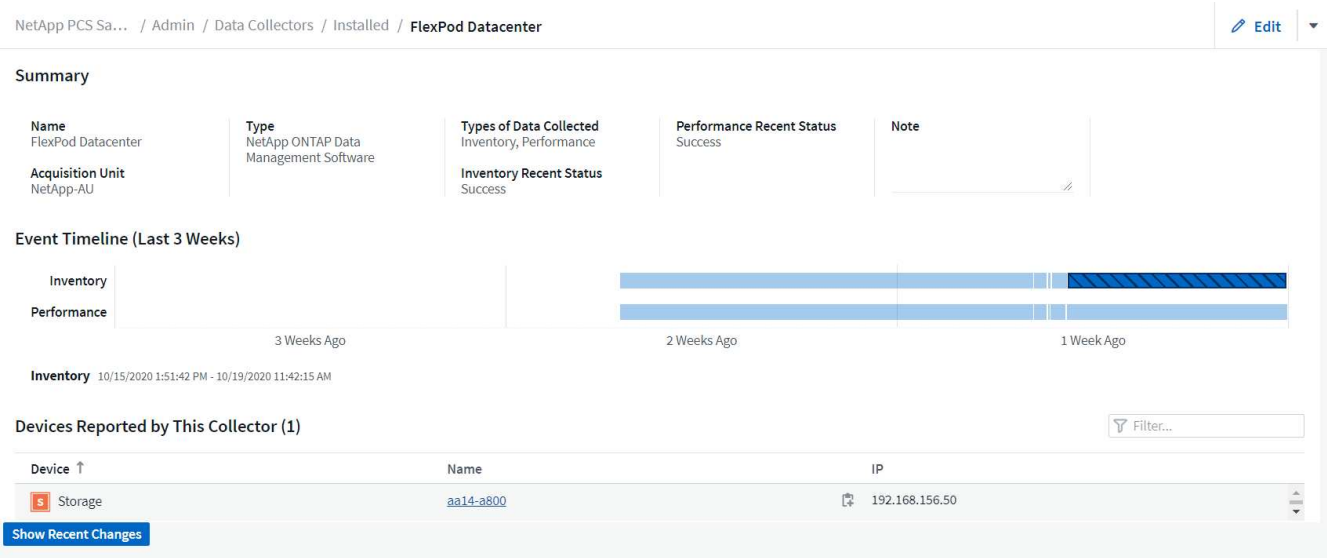
1. 左側の Admin メニューの下にある Data Collector オプションをクリックします。



2. 環境内の特定の Data Collector にフィルタを適用します。この例では、 FlexPod でフィルタリングしています。

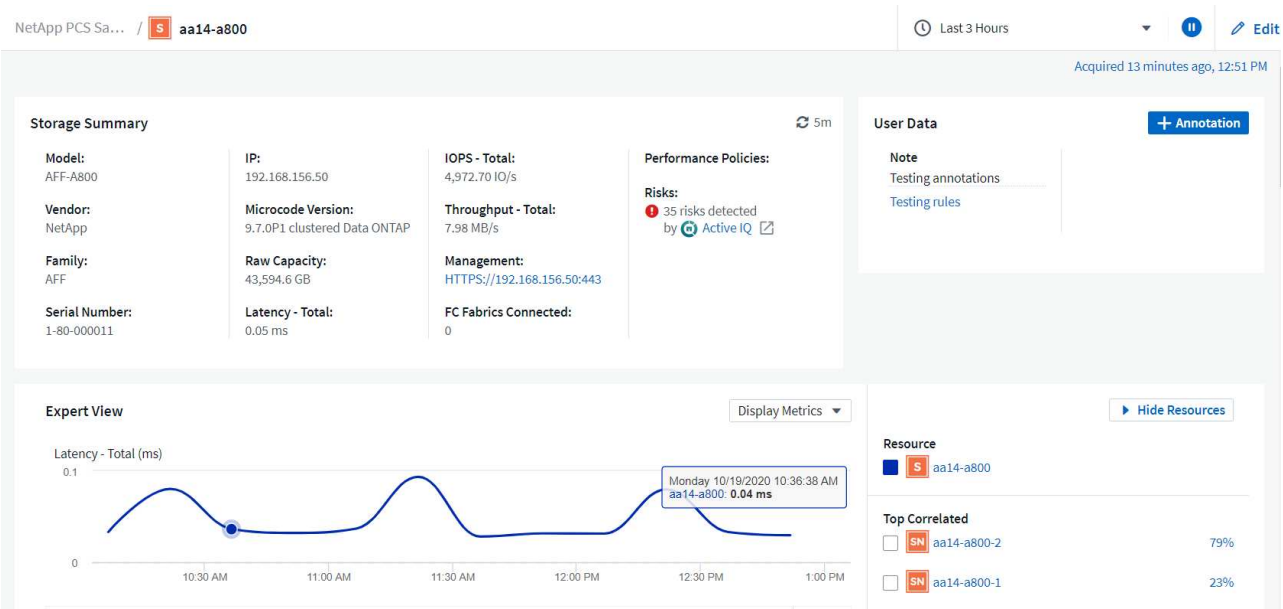


3. Data Collector をクリックして、その Collector によって監視されている環境とデバイスの概要を取得します。

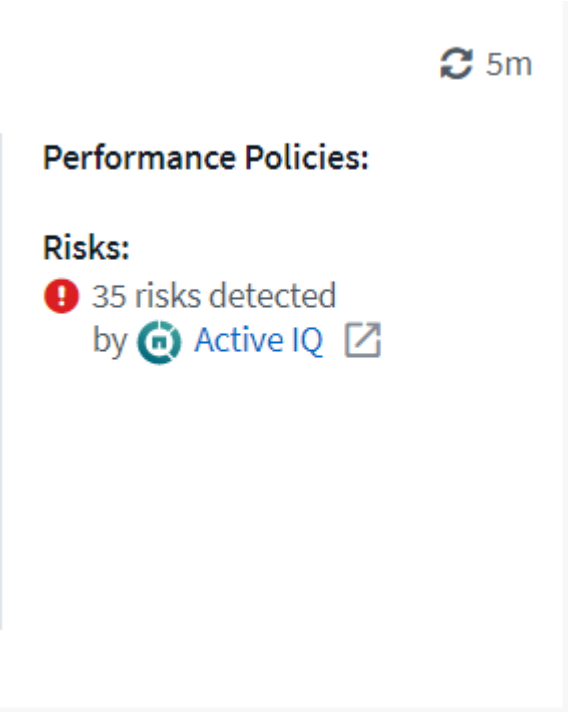


下部のデバイスリストで、監視対象の ONTAP ストレージシステムの名前をクリックします。システムに関して収集された情報を示すダッシュボードが表示されます。これには次の情報が含まれます。

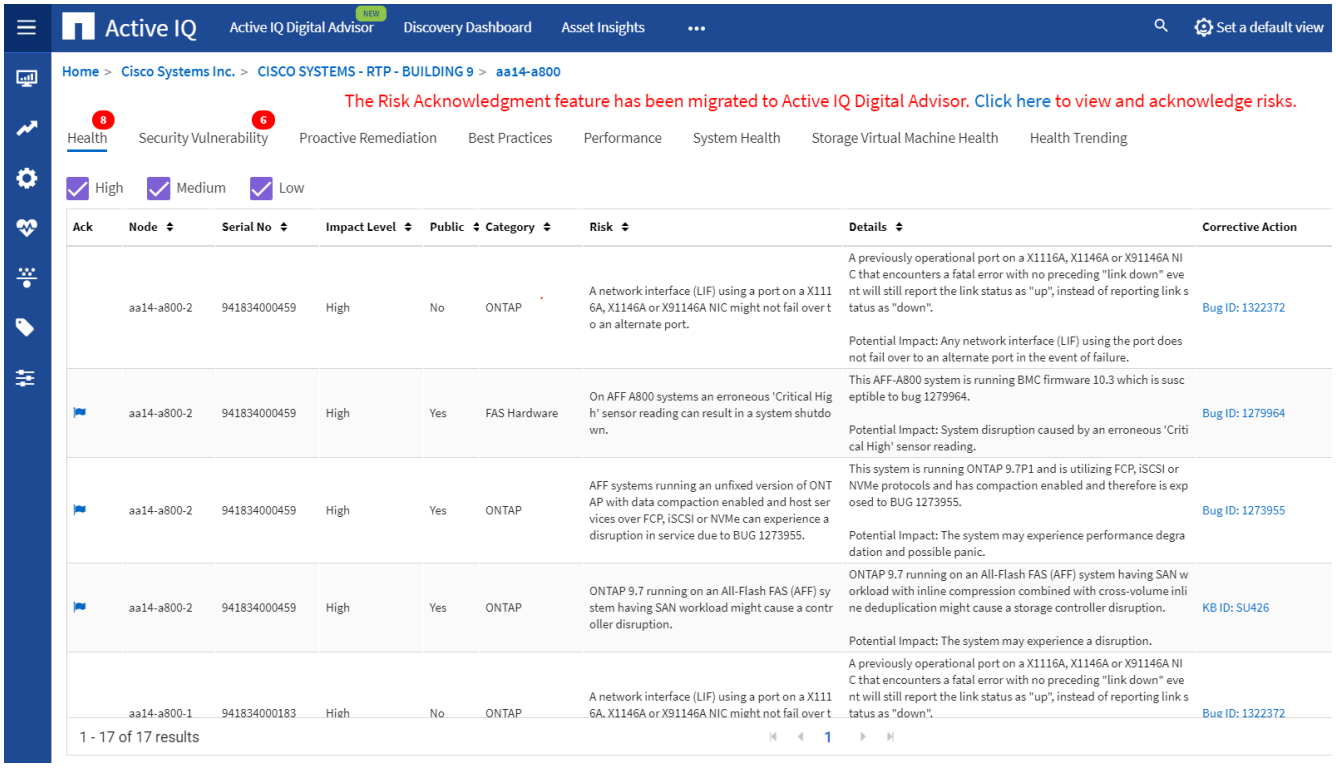
- モデル
- ファミリー
- ONTAP バージョン
- 物理容量
- 平均 IOPS
- 平均レイテンシ
- 平均スループット



また、このページのパフォーマンスポリシーのセクションで、 NetApp Active IQ へのリンクを確認できます。



4. ブラウザの新しいタブを開き、リスク軽減ページに移動します。このページには、影響を受けるノード、リスクがどの程度重要か、特定された問題を修正するために実行する必要がある適切なアクションが表示されます。 Active IQ のリンクをクリックします。

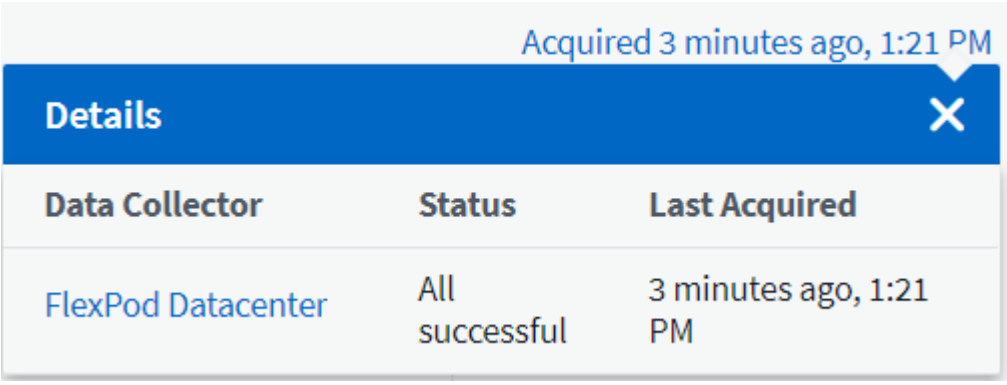


リアルタイムダッシュボードを確認する

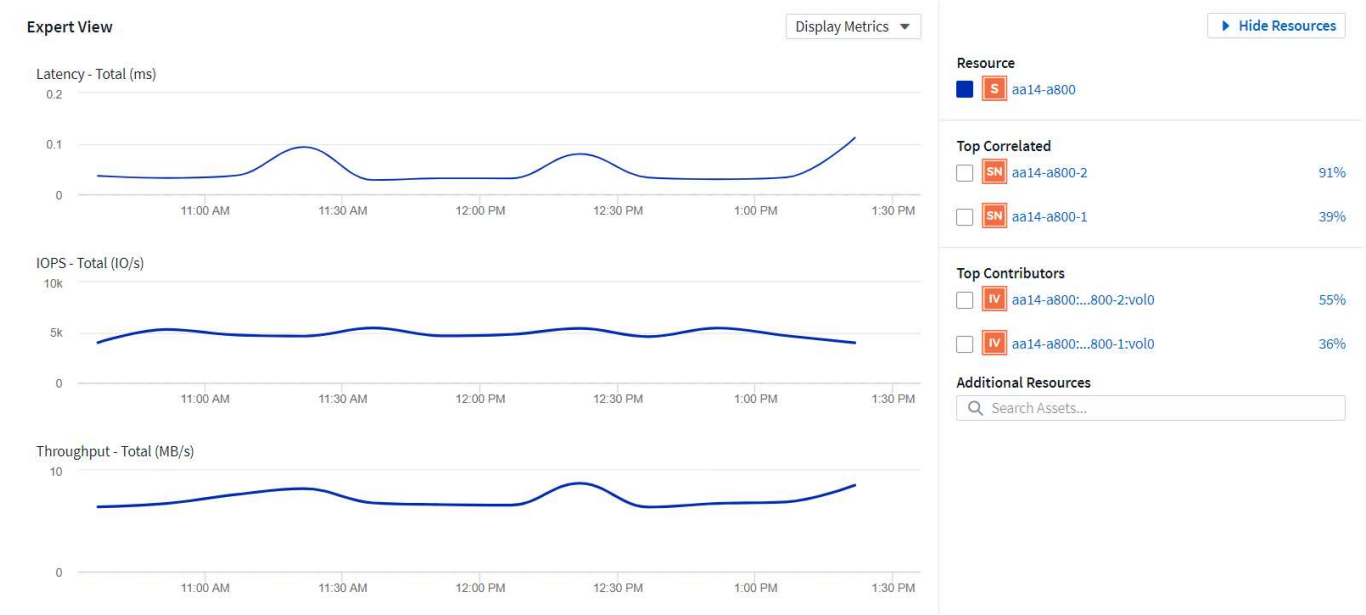
Cloud Insights では、 FlexPod データセンター解決策に導入された ONTAP ストレージシステムでポーリングされた情報のダッシュボードをリアルタイムで表示できます。Cloud Insights Acquisition Unit では、定期的にデータが収集され、デフォルトのストレージシステムダッシュボードに収集された情報が読み込まれます。

Cloud Insights ダッシュボードからリアルタイムグラフにアクセスできます

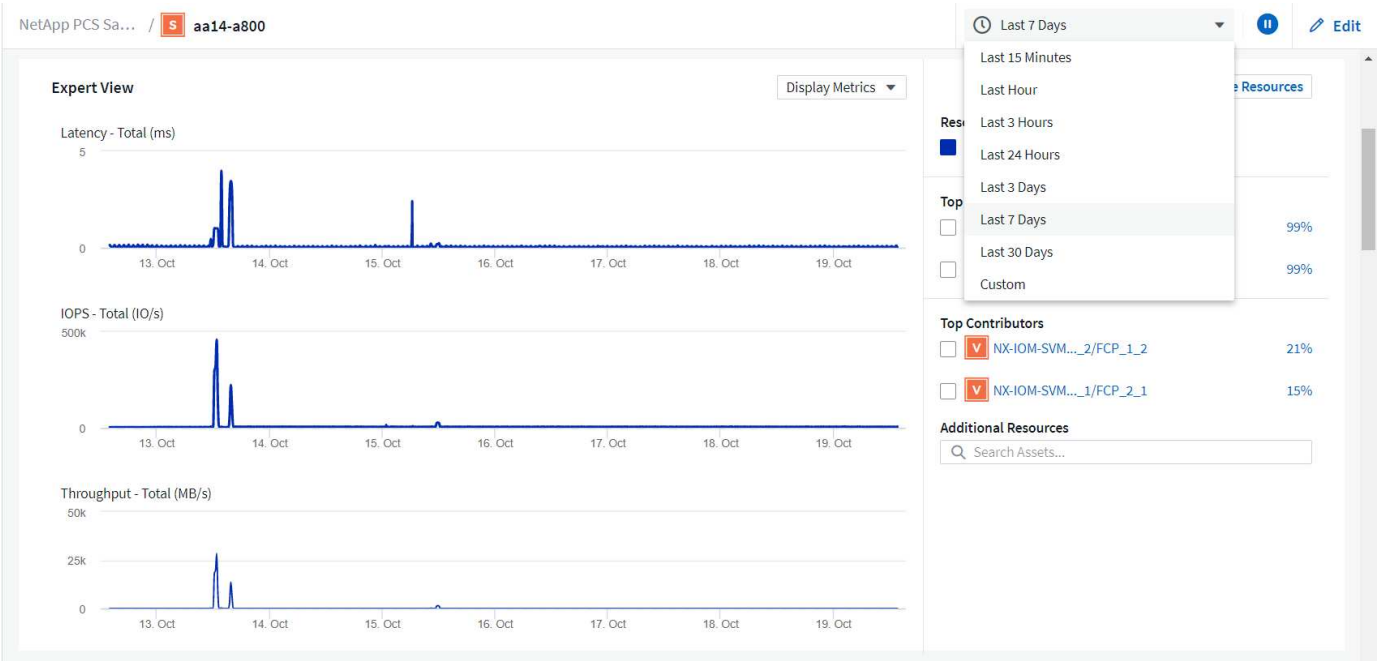
ストレージ・システムのダッシュボードから 'Data Collector が情報を最後に更新した時刻を確認できますこの例を次の図に示します。



デフォルトでは、ストレージシステムダッシュボードのエキスパートビューセクションに、ポーリング対象のストレージシステム、または個々のノードからのシステム全体の指標（レイテンシ、 IOPS 、スループットなど）を示す対話型グラフがいくつか表示されます。これらのデフォルトのグラフの例を次の図に示します。



デフォルトでは、過去 3 時間の情報がグラフに表示されますが、ストレージシステムダッシュボードの右上にあるドロップダウンリストからさまざまな値またはカスタム値に設定できます。これを次の図に示します。



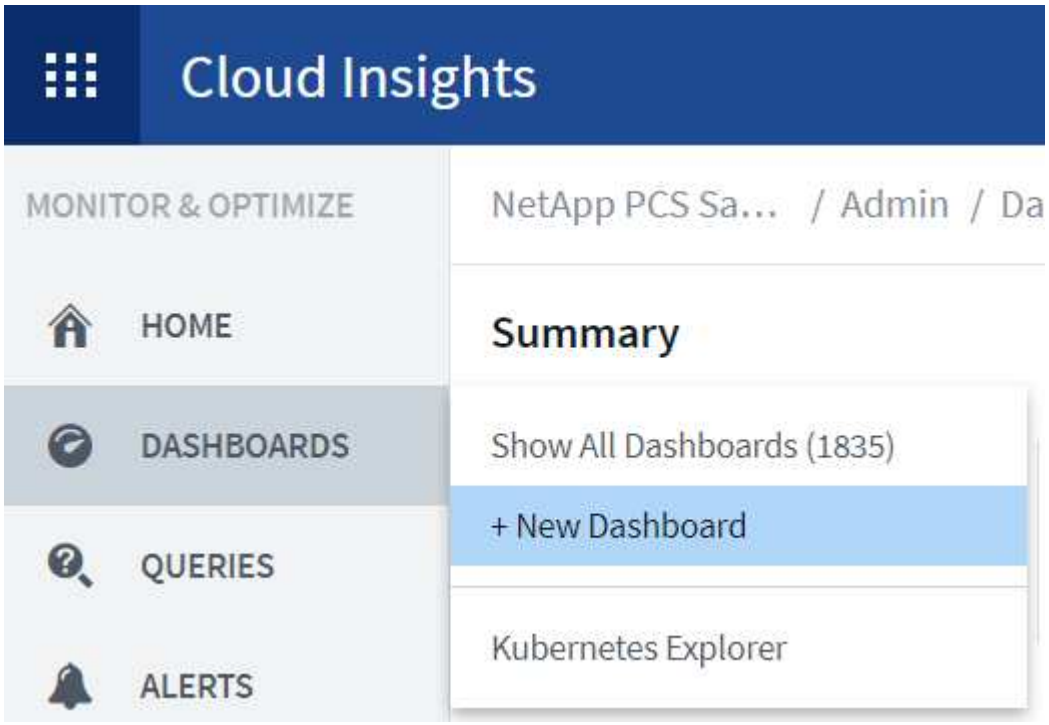
カスタムダッシュボードを作成する

システム全体の情報を表示するデフォルトのダッシュボードを利用する以外に、 Cloud Insights を使用して完全にカスタマイズされたダッシュボードを作成し、 FlexPod Datacenter 解決策の特定のストレージボリュームを対象としたリソースの使用に専念できるようにすることができます。 また、コンバージドインフラに導入されているアプリケーションは、それらのボリュームに依存して効果的に実行されます。これにより、特定のアプリケーションと、データセンター環境で消費されるリソースを視覚的に確認することができます。

カスタマイズしたダッシュボードを作成して、ストレージリソースを評価できます

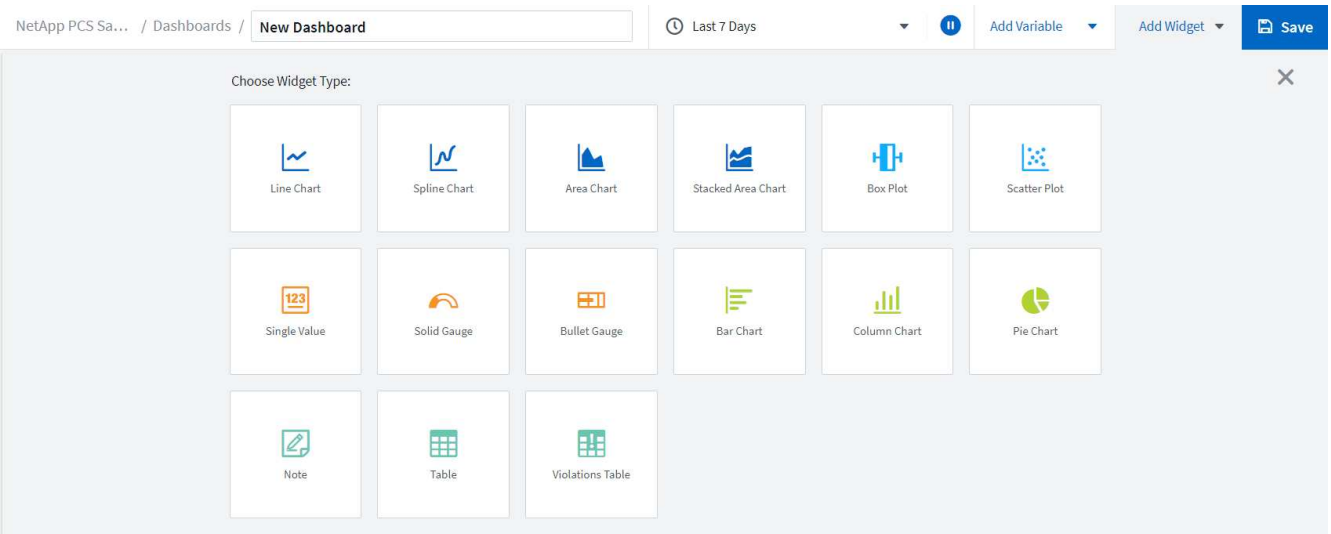
ストレージリソースを評価するためにカスタマイズしたダッシュボードを作成するには、次の手順を実行します。

1. カスタマイズされたダッシュボードを作成するには、 Cloud Insights のメインメニューの [Dashboards] にカーソルを合わせ、ドロップダウンリストで [+] [New Dashboard] をクリックします。



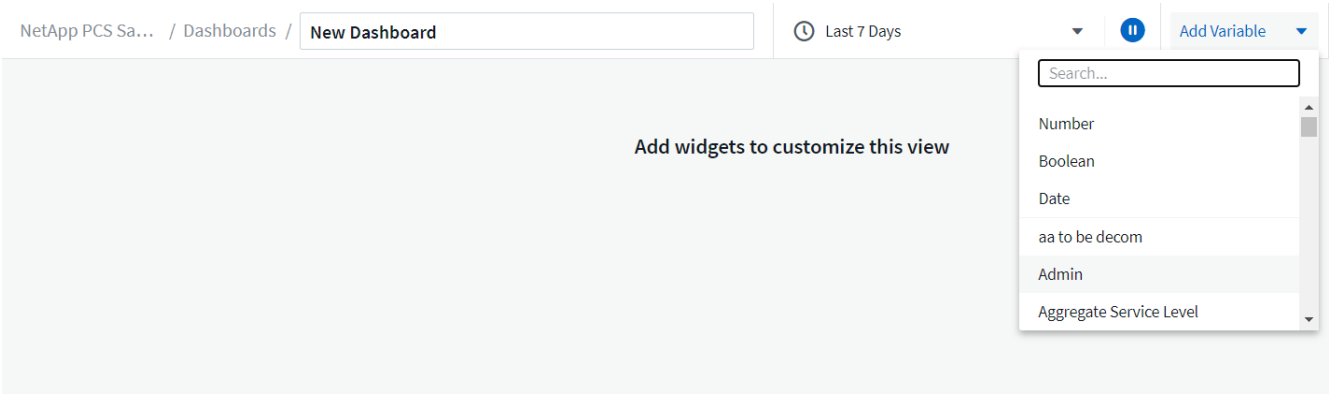
[新しいダッシュボード] ウィンドウが開きます。

2. ダッシュボードに名前を付け、データの表示に使用するウィジェットのタイプを選択します。収集したデータを表示するグラフの種類を選択することも、メモやテーブルの種類を選択することもできます。



3. [変数の追加] メニューから [カスタマイズされた変数] を選択します。

これにより、提示されるデータに集中して、より具体的な、または特殊な要因を表示できます。



4. カスタムダッシュボードを作成するには、使用するウィジェットタイプを選択します。たとえば、円グラフでボリューム別のストレージ利用率を表示します。

   a. [ウィジェットの追加] ドロップダウンリストから [円グラフ] ウィジェットを選択します。

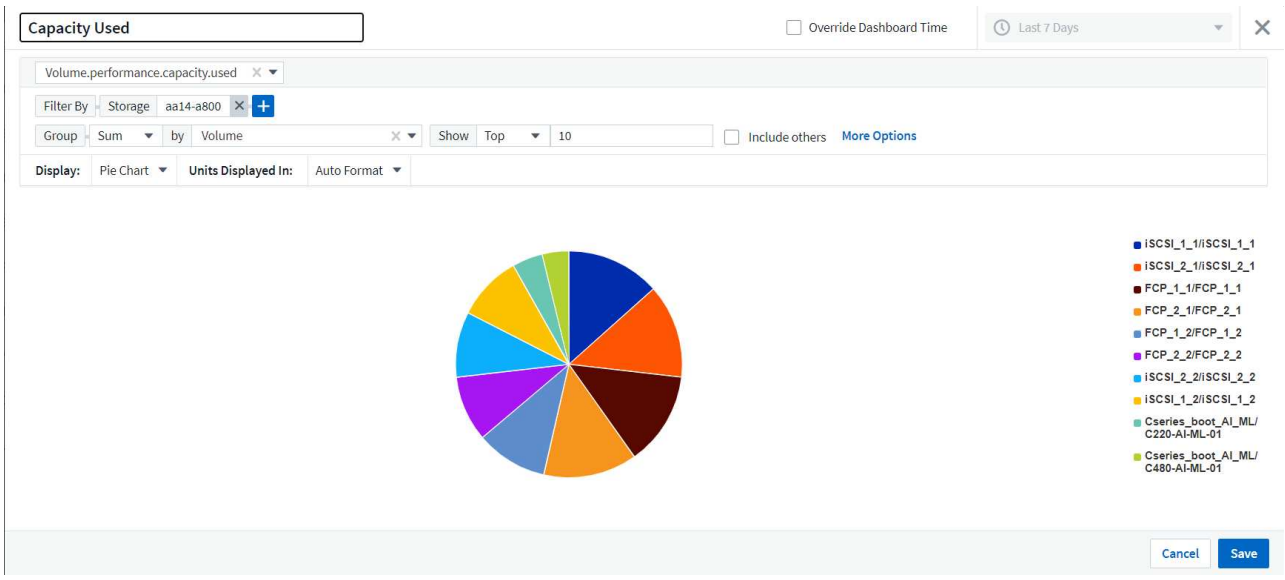
   b. ウィジェットに「 Capacity Used 」などのわかりやすい識別子を付けます。

   c. 表示するオブジェクトを選択します。たとえば、キーワード volume で検索し、「 volume.performance.capacity.used` 」を選択できます。

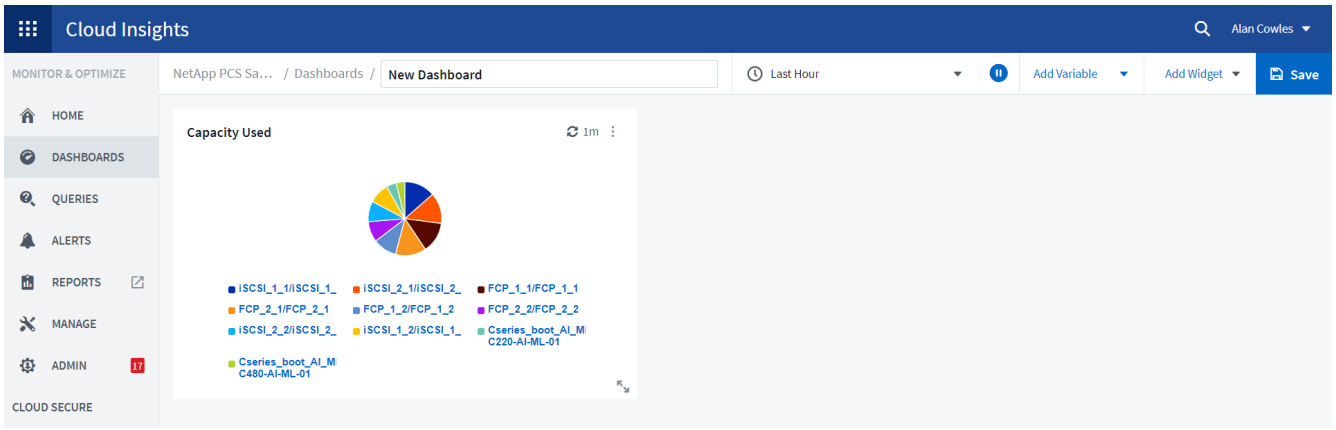
   d. ストレージシステムでフィルタリングするには、 FlexPod Datacenter 解決策で、フィルタを使用してストレージシステムの名前を入力します。

   e. 表示する情報をカスタマイズします。デフォルトでは、 ONTAP データボリュームが表示され、上位 10 個のが表示されます。

   f. カスタマイズしたダッシュボードを保存するには、 [保存] をクリックします。



カスタムウィジェットを保存すると、ブラウザは新しいダッシュボードページに戻ります。このページには、新しく作成したウィジェットが表示され、データポーリング期間の変更などの対話型アクションを実行できます。



高度なトラブルシューティング

Cloud Insights を使用すると、 FlexPod データセンターコンバージドインフラのどのストレージ環境にも高度なトラブルシューティング方法を適用できます。前述した各機能のコンポーネントを使用： Active IQ 統合、リアルタイム統計を表示するデフォルトダッシュボード、カスタマイズされたダッシュボードなど、発生する可能性のある問題は早期に検出されて迅速に解決されます。Active IQ のリスクリストを使用すると、問題につながる可能性のある報告済みの構成エラーを発見したり、報告済みのコードバージョンやパッチが適用されたコードのバージョンを発見したりできます。Cloud Insights ホームページ上のリアルタイムダッシュボードを観察することで、システムパフォーマンスのパターンを発見し、問題の早期発見や早期解決に役立てることができます。最後に、カスタマイズしたダッシュボードを作成することで、お客様はインフラ内の最も重要な資産に集中し、それらを直接監視して、ビジネス継続性の目標を達成できるようになります。

ストレージの最適化

トラブルシューティングに加えて、 Cloud Insights で収集されたデータを使用することで、 FlexPod データセンターコンバージドインフラ解決策に導入されている ONTAP ストレージシステムを最適化することができます。高レイテンシが発生しているボリュームについては、たとえば、高パフォーマンスが求められる複数の VM が同じデータストアを共有している場合など、 Cloud Insights ダッシュボードにその情報が表示されます。ストレージ管理者は、この情報を使用して、 1 つ以上の VM を別のボリュームに移行したり、アグリゲート間や ONTAP ストレージシステムのノード間で移行したりできます。その結果、パフォーマンスが最適化された環境になります。Cloud Insights と Active IQ の統合から収集された情報は、想定よりもパフォーマンスが低下する構成の問題を明らかにし、問題を解決して最適に調整されたストレージシステムを確保するための推奨される対処方法を提供します。

ビデオとデモ

ビデオでは、 NetApp Cloud Insights を使用してオンプレミス環境内のリソースを評価する方法を紹介しています "こちらをご覧ください"。

NetApp Cloud Insights を使用してインフラを監視し、インフラのアラートしきい値を設定する方法を紹介するビデオをご覧ください "こちらをご覧ください"。

環境内の個々のアプリケーションの評価には、 NetApp Cloud Insights の使用方法を示すビデオが視聴できます "こちらをご覧ください"。

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、次の Web サイトを参照して

ください。

- シスコ製品マニュアル

  "https://www.cisco.com/c/en/us/support/index.html"

- FlexPod データセンター

  "https://www.flexpod.com"

- NetApp Cloud Insights の略

  "https://cloud.netapp.com/cloud-insights"

- ネットアップの製品マニュアル

  "https://docs.netapp.com"

FabricPool with FlexPod - Amazon AWS S3 への非アクティブなデータ階層化

TR-4801 ：『 FlexPod with FabricPool - Inactive Data Tiering to Amazon AWS S3 』

ネットアップ、 Scott Kovacs 氏

フラッシュストレージの価格は下落し続けているため、これまでフラッシュストレージの候補とみなされていなかったワークロードやアプリケーションで利用できます。しかし、 IT 管理者にとっては、ストレージへの投資を最も効率的に活用することが非常に重要です。IT 部門は、予算をほとんど増やすことなく、パフォーマンスの高いサービスを提供し続ける必要があります。このようなニーズに対応するために、 NetApp FabricPool では、使用頻度の低いデータをオンプレミスの高価なフラッシュストレージからパブリッククラウドの対費用効果の高いストレージ階層に移動することで、クラウドの経済性を活用できます。アクセス頻度の低いデータをクラウドに移動することで、AFF システムや FAS システム上の貴重なフラッシュストレージスペースが解放され、ビジネスクリティカルなワークロードに対応できる容量がハイパフォーマンスのフラッシュ階層に追加されます。

このテクニカルレポートでは、ネットアップと Cisco が提供する FlexPod コンバージドインフラアーキテクチャに関連して、 ONTAP FabricPool のデータ階層化機能について説明します。このテクニカルレポートで説明する概念を最大限に活用するには、 FlexPod データセンター統合インフラアーキテクチャと ONTAP ストレージソフトウェアについて理解しておく必要があります。FlexPod と ONTAP に精通していることを前提に、 FabricPool とその仕組み、オンプレミスのフラッシュストレージをより効率的に使用するための の使用方法について説明します。このレポートの内容の大部分については、で詳しく説明します "TR-4598 ：『 FabricPool Best Practices 』" およびその他の ONTAP 製品ドキュメントを参照してください。このコンテンツは FlexPod インフラのために集約されており、 FabricPool のすべてのユースケースを網羅しているわけではありません。ONTAP 9.6 では、すべての機能と概念が使用可能です。

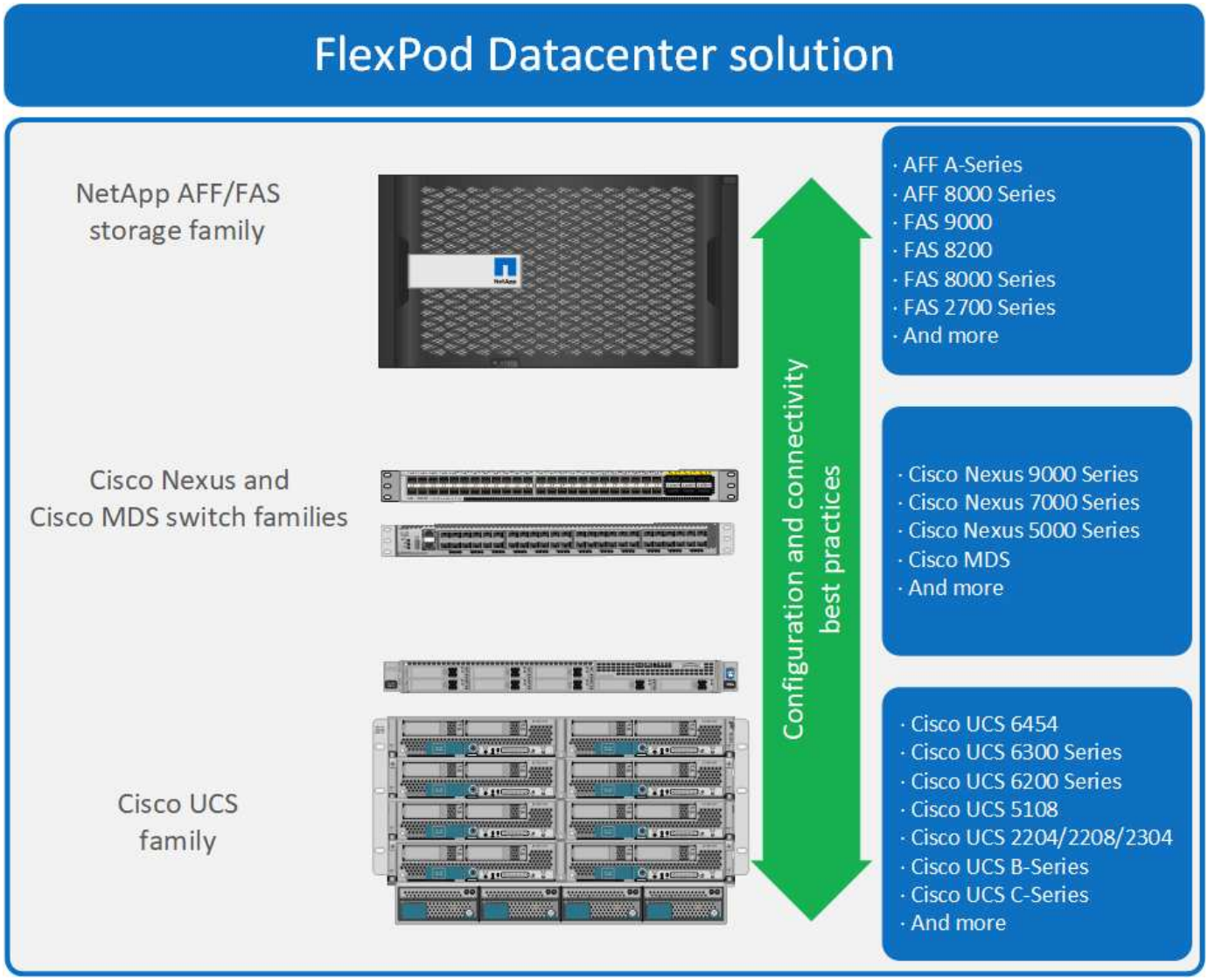
追加情報 About FlexPod をに示します "TR-4036 『 FlexPod データセンター技術仕様』"。

FlexPod の概要とアーキテクチャ

FlexPod の概要

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフトウェアの定義済みセットです。FlexPod には、 NetApp AFF ストレージ、 Cisco Nexus ネットワーク、 Cisco MDS ストレージネットワーク、 Cisco Unified Computing System （ Cisco UCS ）、 VMware vSphere ソフトウェアが 1 つのパッケージに含まれています。この設計は柔軟性に優れており、ネットワーク、コンピューティング、ストレージを 1 つのデータセンターラックに収容することも、お客様のデータセンター設計に従って導入することもできます。ポート密度を使用すると、ネットワークコンポーネントは複数の構成に対応できます。

FlexPod アーキテクチャのメリットの 1 つは、お客様の要件に合わせて環境をカスタマイズしたり柔軟に設定したりできることです。FlexPod ユニットは、要件や需要の変化に応じて簡単に拡張できます。ユニットは、スケールアップ（ FlexPod ユニットにリソースを追加）とスケールアウト（ FlexPod ユニットを追加）の両方に対応しています。FlexPod リファレンスアーキテクチャでは、ファイバチャネルおよび IP ベースのストレージ解決策の耐障害性、コスト上のメリット、および導入の容易さを強調しています。単一のインターフェイスから複数のプロトコルに対応できるストレージシステムなら、選択肢が広がり、投資が無駄にならずに保護されます。これは、まさに Wire-Once アーキテクチャだからです。次の図に、 FlexPod の多くのハードウェアコンポーネントを示します。

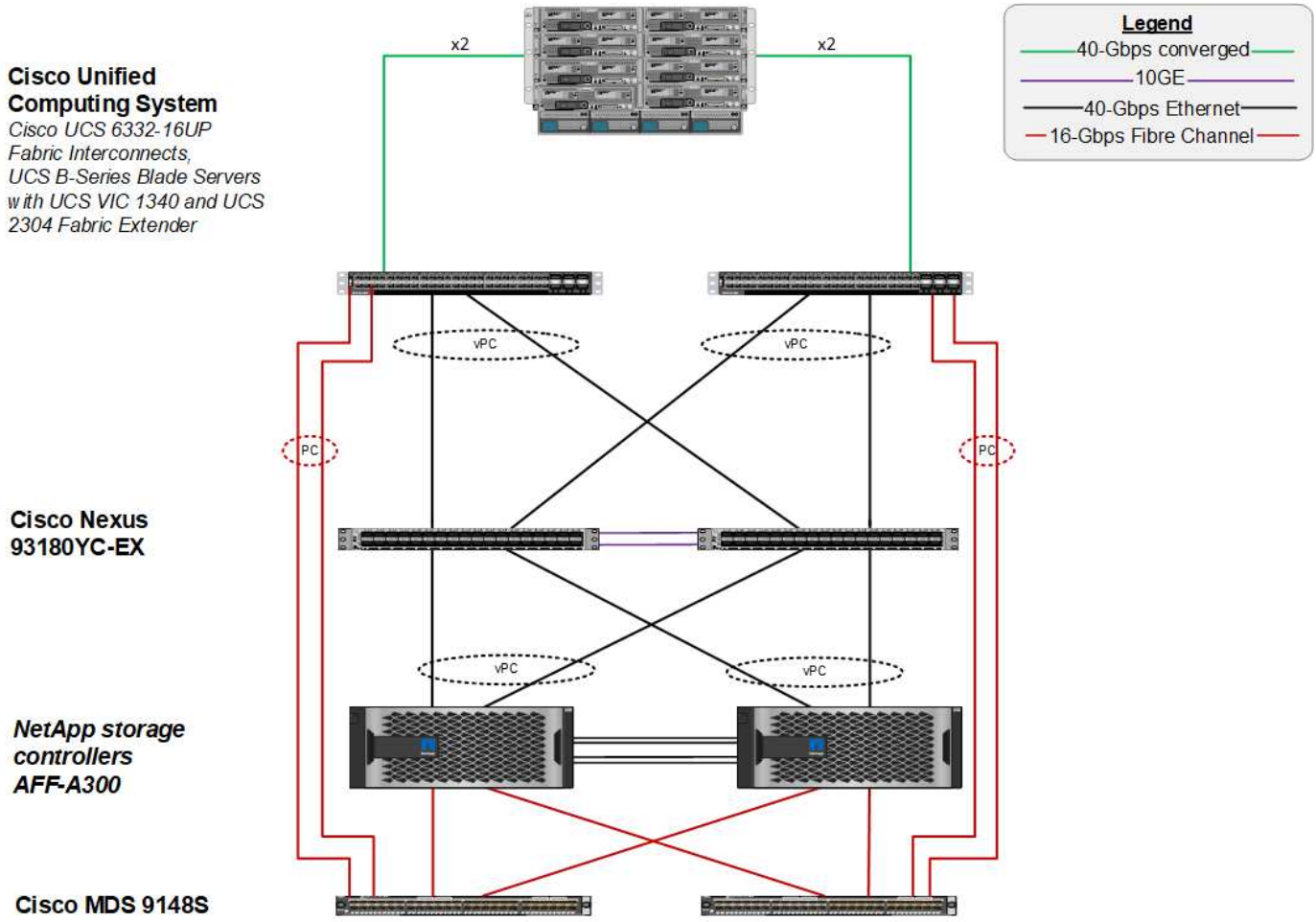


FlexPod アーキテクチャ

次の図に、 VMware vSphere と FlexPod 解決策のコンポーネントと、 Cisco UCS 6454 ファブリックインターコネクトに必要なネットワーク接続を示します。この設計には、次のコンポーネントがあります。

- Cisco UCS 5108 ブレードシャーシと Cisco UCS ファブリックインターコネクト間のポートチャネル 40GB イーサネット接続
- Cisco UCS ファブリックインターコネクトと Cisco Nexus 9000 間の 40GB イーサネット接続
- Cisco Nesxus 9000 と NetApp AFF A300 ストレージアレイ間に 40GB イーサネット接続

これらのインフラオプションは、 Cisco UCS ファブリックインターコネクトと NetApp AFF A300 の間に Cisco MDS スイッチが配置されたことで拡張されました。この構成では、 16Gb FC ブートホストに、共有ストレージへのブロックレベルのアクセスを提供します。これは、アーキテクチャにストレージを追加する場合に、ホストから Cisco UCS ファブリックインターコネクトへのケーブルの再接続が不要になるため、リファレンスアーキテクチャによって wire-once 戦略が強化されることを意味します。



FabricPool

FabricPool の概要

FabricPool は、オールフラッシュ（ SSD ）アグリゲートをパフォーマンス階層として使用し、オブジェクトストアをパブリッククラウドサービスにクラウド階層として使用する、 ONTAP のハイブリッドストレージ解決策です。この構成では、アクセス頻度に応じてポリシーベースのデータ移動が可能です。FabricPool は、

FAS プラットフォームの AFF アグリゲートとオール SSD アグリゲートの両方で ONTAP でサポートされています。データ処理はブロックレベルで実行され、アクセス頻度が高いデータブロックがオールフラッシュのパフォーマンス階層にあり、コールドとしてタグ付けされ、アクセス頻度が低いブロックとホットタグ付けされます。

FabricPool を使用すると、パフォーマンス、効率、セキュリティ、保護を犠牲にすることなくストレージコストを削減できます。FabricPool は、エンタープライズアプリケーションに対して透過的であり、アプリケーションインフラを再設計することなくストレージの TCO を削減することで、クラウドの効率性を活用します。

FlexPod は、 FabricPool のストレージ階層化機能を活用して、 ONTAP フラッシュストレージをより効率的に使用できます。NetApp SnapCenter for vSphere からアクセス頻度の低い仮想マシン（ VM ）、使用頻度の低い VM テンプレート、および VM のバックアップを取得すると、データストアボリュームのスペースを貴重に使用することができます。コールドデータをクラウド階層に移動することで、 FlexPod インフラにホストされているミッションクリティカルなハイパフォーマンスアプリケーションのスペースとリソースを解放できます。

> 一般に、 Fibre Channel および iSCSI プロトコルは、タイムアウト（ 60 ～ 120 秒）が発生するまでに時間がかかりますが、 NAS プロトコルと同じ方法で接続の確立を再試行することはありません。SAN プロトコルがタイムアウトした場合は、アプリケーションを再起動する必要があります。パブリッククラウドへの接続を保証する方法がないため、 SAN プロトコルを使用した本番アプリケーションの停止は、短時間であっても非常に深刻な事態になる可能性があります。この問題を回避するには、 SAN プロトコルがアクセスするデータを階層化するときにプライベートクラウドを使用することを推奨します。

ONTAP 9.6 で FabricPool は、 Alibaba Cloud Object Storage Service 、 Amazon AWS S3 、 Google Cloud Storage 、 IBM Cloud Object Storage 、 Microsoft Azure Blob Storage など、主要なすべてのパブリッククラウドプロバイダと統合されます。本レポートでは、選択するクラウドオブジェクト階層として Amazon AWS S3 ストレージを中心に説明します。

複合アグリゲート

ONTAP インスタンスを作成するには、 FabricPool フラッシュアグリゲートを AWS S3 バケットなどのクラウドオブジェクトストアに関連付けて複合アグリゲートを作成します。ボリュームを複数のアグリゲート内に作成すると、 FabricPool の階層化機能を利用できます。データがボリュームに書き込まれると、 ONTAP は各データブロックに温度を割り当てます。最初に書き込まれたブロックには、ホットの温度が割り当てられます。時間が経過すると、データにアクセスできない場合は、最後にコールドステータスが割り当てられるまでクーリングプロセスが実行されます。アクセス頻度の低いデータブロックは、パフォーマンス SSD アグリゲートからクラウドオブジェクトストアに階層化されます。

ブロックがコールドとして指定され、クラウドオブジェクトストレージに移動されるまでの期間は、 ONTAP のボリューム階層化ポリシーによって変更されます。さらにきめ細かい設定は、ブロックがコールドになるまでに必要な日数を制御する ONTAP 設定を変更することで実現します。データ階層化の対象となるのは、従来のボリューム Snapshot 、 vSphere VM バックアップ用の SnapCenter 、およびその他の NetApp Snapshot ベースのバックアップです。また、 VM テンプレートやアクセス頻度の低い VM データなど、 vSphere データストア内の使用頻度の低いブロックも対象となります。

Inactive Data Reporting の実行

ONTAP では、アグリゲートから階層化できるコールドデータの量を評価するのに役立つ Inactive Data Reporting （ IDR ）を利用できます。ONTAP 9.6 では、 IDR がデフォルトで有効になっており、 31 日間のデフォルトのクーリングポリシーを使用してアクセス頻度の低いデータが特定されます。

階層化されるコールドデータの量は、ボリュームに設定されている階層化ポリシーによって異なります。この量は、デフォルトの 31 日間のクーリング期間を使用して、 IDR によって検出されたコールドデータの量とは異なる場合があります。

オブジェクトの作成とデータの移動

FabricPool は、 NetApp WAFL のブロックレベルで動作し、ブロックを冷却し、ストレージオブジェクトに連結し、それらのオブジェクトをクラウド階層に移行します。各 FabricPool オブジェクトは 4MB で、 1 、 024 個の 4KB ブロックで構成されています。オブジェクトサイズは、主要なクラウドプロバイダからの推奨パフォーマンスに基づいて、 4MB に固定されており、変更できません。コールドブロックが読み取られてホットにされると、 4MB オブジェクト内の要求されたブロックのみが取得され、パフォーマンス階層に戻されます。オブジェクト全体もファイル全体も移行されません。必要なブロックのみが移行されます。

ONTAP は、シーケンシャルな先読みの機会を検出すると、パフォーマンスを向上させるために、読み取り前にブロックをクラウド階層に要求します。

デフォルトでは、パフォーマンスアグリゲートの使用率が 50% を超えている場合にのみ、データがクラウド階層に移動されます。このしきい値を低い割合に設定すると、パフォーマンスフラッシュ階層のデータストレージの量を少なくしてクラウドに移動できます。これは、アグリゲートの容量が上限に近づいている場合にのみコールドデータを移動する階層化戦略がある場合に役立ちます。

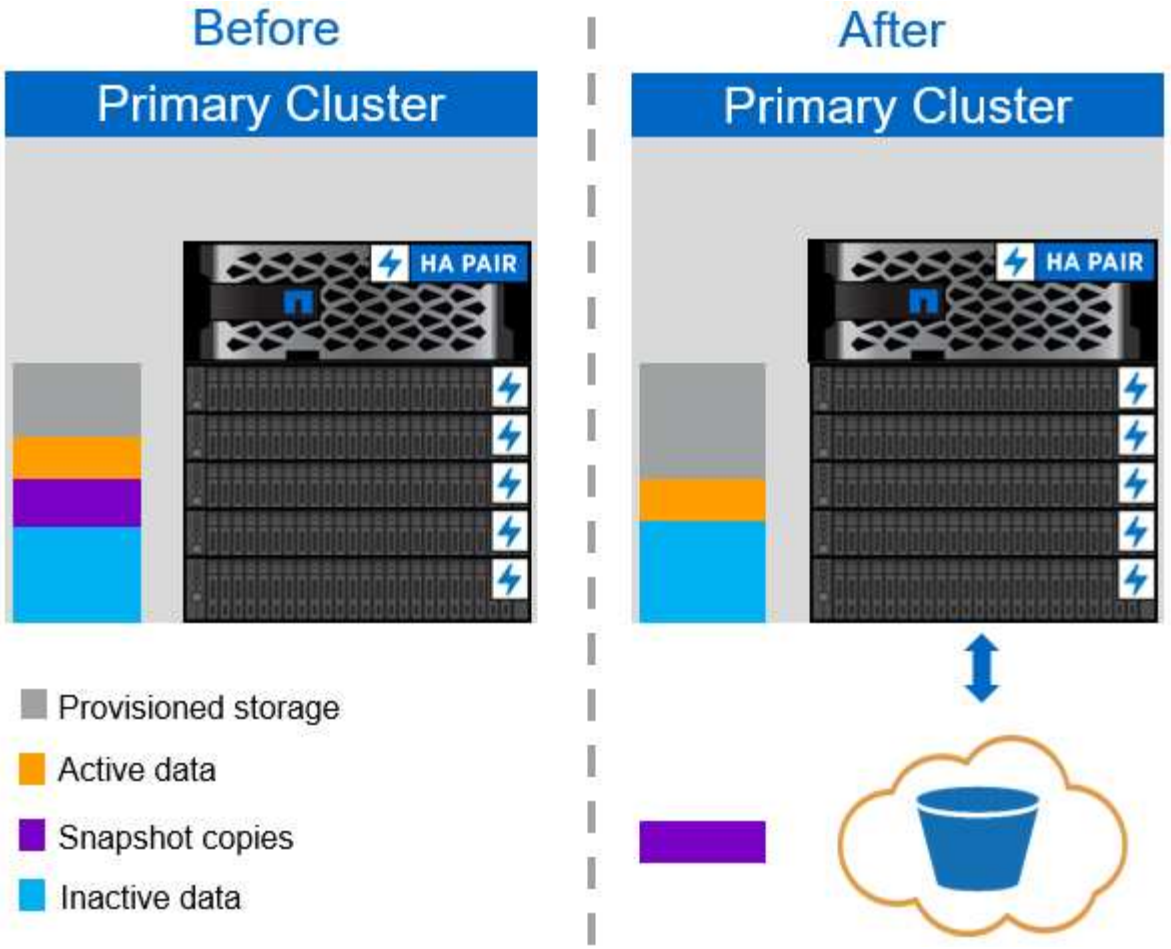
パフォーマンス階層の使用率が 70% を超える場合、コールドデータはパフォーマンス階層に書き戻されることなく、クラウド階層から直接読み取られます。FabricPool では、使用頻度の高いアグリゲートでのコールドデータの書き戻しを防止することで、アクティブデータのアグリゲートが保持されます。

パフォーマンス階層のスペースを再生します

前述したように、 FabricPool の主なユースケースは、ハイパフォーマンスのオンプレミスフラッシュストレージを最も効率的に使用できるようにすることです。FlexPod 仮想インフラのボリューム Snapshot および VM バックアップという形で作成されたコールドデータは、高価なフラッシュストレージを大量に消費している可能性があります。Snapshot のみまたは自動の 2 つの階層化ポリシーのいずれかを実装すると、重要なパフォーマンス階層のストレージを解放できます。

snapshot-only 階層化ポリシー

次の図に示す「 Snapshot のみ」の階層化ポリシーは、ボリュームのコールドスナップショットデータと、スペースを占有しているがアクティブなファイルシステムとブロックを共有していない VM の SnapCenter for vSphere バックアップをクラウドオブジェクトストアに移動します。「 Snapshot のみ」の階層化ポリシーは、コールドデータブロックをクラウド階層に移動します。リストアが必要な場合、クラウド内のコールドブロックがホットになり、オンプレミスのパフォーマンスフラッシュ階層に戻ります。

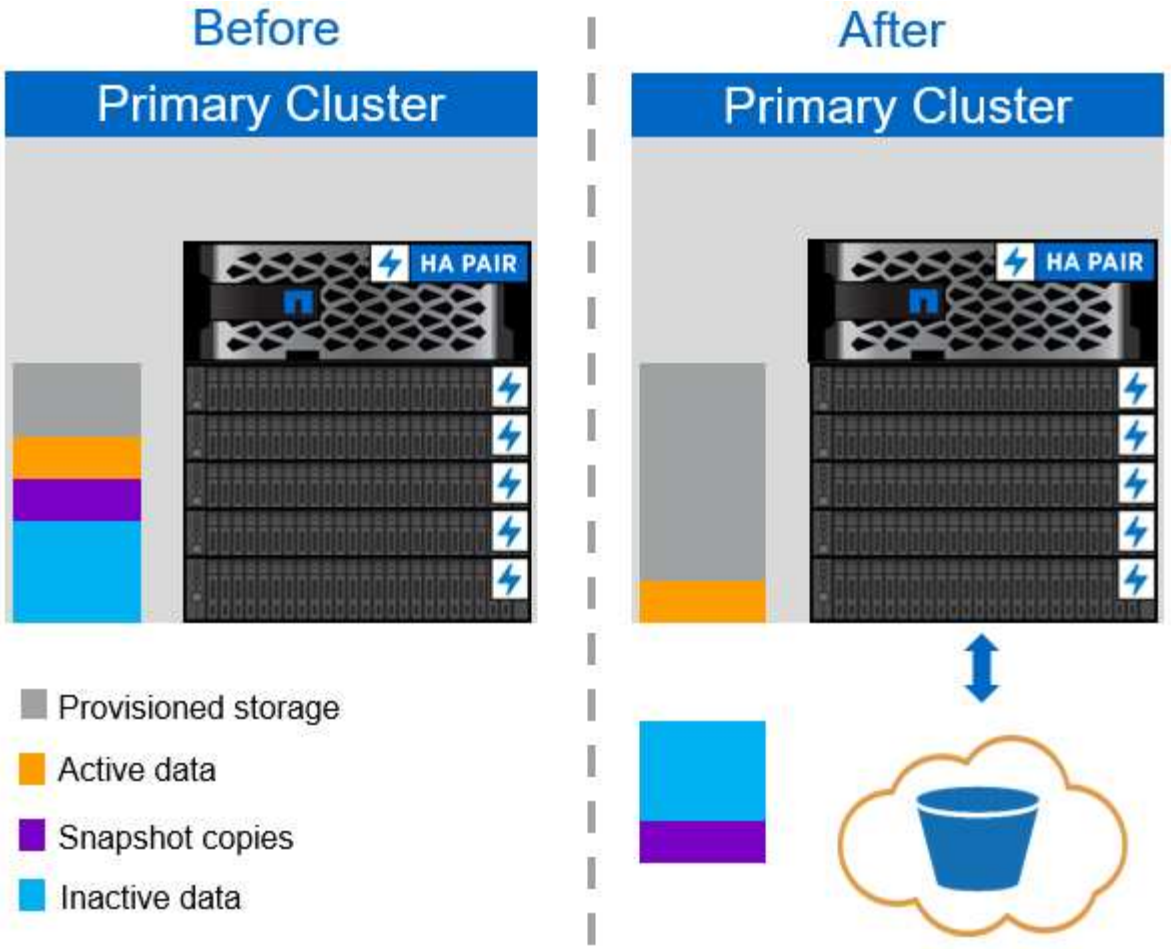


auto 階層化ポリシー

次の図に示す FabricPool の自動階層化ポリシーは、コールドスナップショットのデータブロックをクラウドに移動するだけでなく、アクティブファイルシステムのコールドブロックも移動します。これには、 VM テンプレートと、データストアボリューム内の未使用の VM データが含まれることがあります。どのコールドブロックを移動するかは ' ボリュームの階層化最小冷却日数設定によって制御されますクラウド階層のコールドブロックがアプリケーションによってランダムに読み取られると、それらのブロックがホットになり、パフォーマンス階層に戻ります。ただし、ウィルス対策スキャナなどのプロセスによってコールドブロックが読み取られた場合、ブロックはコールドのままクラウドオブジェクトストアに残り、パフォーマンス階層に戻されることはありません。

auto 階層化ポリシーを使用している場合、ホットに設定されたアクセス頻度の低いブロックは、クラウド接続の速度でクラウド階層から戻されます。これは、レイテンシの影響を受けやすいアプリケーションの場合、VM のパフォーマンスに影響を及ぼす可能性があります。レイテンシが影響を受ける場合は、データストアで自動階層化ポリシーを使用する前に考慮する必要があります。十分なパフォーマンスを確保するために、インタークラスタ LIF は 10GbE の速度のポートに配置することを推奨します。

> オブジェクトストレージプロファイラは、オブジェクトストアを FabricPool アグリゲートに接続する前に、オブジェクトストアに対するレイテンシとスループットをテストするために使用します。



all 階層化ポリシー

「自動」および「 Snapshot のみ」のポリシーとは異なり、「すべて」の階層化ポリシーは、データボリューム全体をただちにクラウド階層に移動します。このポリシーは、セカンダリデータ保護ボリュームまたはアーカイブボリュームに適しています。アーカイブボリュームのデータは、履歴データや規制上の目的で保持する必要があり、ほとんどアクセスされません。VMware データストアボリュームに書き込まれたデータはすぐにクラウド階層に移動されるため、「すべて」のポリシーは推奨されません。以降の読み取り処理はクラウドから実行されるため、データストアボリュームに配置されている VM やアプリケーションでパフォーマンスの問題が発生する可能性があります。

セキュリティ

クラウドと FabricPool では、セキュリティが一元的に懸念されます。ONTAP に標準で搭載されているセキュリティ機能はすべて高パフォーマンス階層でサポートされており、データの移動はクラウド階層に転送される際にセキュリティで保護されます。FabricPool では、を使用します "AES-256-GCM" パフォーマンス階層で暗号化アルゴリズムを使用して、この暗号化をエンドツーエンドでクラウド階層に維持します。クラウドオブジェクトストアに移動されるデータブロックは、ストレージ階層間のデータの機密性と整合性を維持するために、 Transport Layer Security （ TLS ） v1.2 で保護されます。

> 暗号化されていない接続を介したクラウドオブジェクトストアとの通信はサポートされていますが、ネットアップでは推奨していません

データ暗号化

データ暗号化は、知的財産、取引情報、個人を特定できる顧客情報の保護に不可欠です。FabricPool は、既存のデータ保護戦略を維持するために、 NetApp Volume Encryption （ NVE ）と NetApp Storage Encryption （ NSE ）の両方を完全にサポートしています。クラウド階層に移動した場合、パフォーマンス階層で暗号化されたすべてのデータは暗号化されたままになります。クライアント側の暗号化キーは ONTAP によって所有され、サーバ側のオブジェクトストアの暗号化キーはそれぞれのクラウドオブジェクトストアによって所有されます。NVE で暗号化されていないデータは、 AES-256-GCM アルゴリズムで暗号化されます。それ以外の AES-256 暗号はサポートされません。

NSE または NVE の使用はオプションで、 FabricPool を使用する必要はありません。

FabricPool の要件

FabricPool を使用するには、 ONTAP 9.2 以降と、このセクションに記載されたプラットフォームのいずれかで SSD アグリゲートを使用する必要があります。追加の FabricPool 要件は、接続するクラウド階層によって異なります。NetApp AFF C190 など、容量が比較的小さい、固定レベルの AFF プラットフォームでは、アクセス頻度の低いデータをクラウド階層に移動する場合に FabricPool を使用すると効果的です。

プラットフォーム

FabricPool は、次のプラットフォームでサポートされます。

- NetApp AFF
  - A800
  - A700S 、 A700
  - A320 、 A300
  - A220 、 A200
  - C190
  - AFF8080 、 AFF8060 、および AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080 、 FAS8060 、および FAS8040
  - FAS2750 、 FAS2720
  - FAS2650 、 FAS2620

FabricPool を使用できるのは、 FAS プラットフォーム上の SSD アグリゲートのみです。

- クラウド階層
  - Alibaba Cloud Object Storage Service （標準、低頻度アクセス）
  - Amazon S3 （標準、標準 -IA 、 1 ゾーン -IA 、インテリジェント階層化）

- Amazon Commercial クラウドサービス（ C2S ）
- Google Cloud Storage （マルチリージョン、リージョナル、ニアライン、コールドライン）
- IBM Cloud Object Storage （ Standard 、 Vault 、 Cold Vault 、 Flex ）
- Microsoft Azure Blob Storage （ホットおよびクール）

クラスタ間 **LIFs**

FabricPool を使用するクラスタのハイアベイラビリティ（ HA ）ペアでは、クラウド階層と通信するために 2 つのクラスタ間 LIF が必要です。ネットアップでは、追加の HA ペアでクラスタ間 LIF を作成して、これらのノードのアグリゲートにもクラウド階層をシームレスに接続することを推奨しています。

ONTAP が AWS S3 オブジェクトストアとの接続に使用する LIF は、 10Gbps ポート上に配置する必要があります。

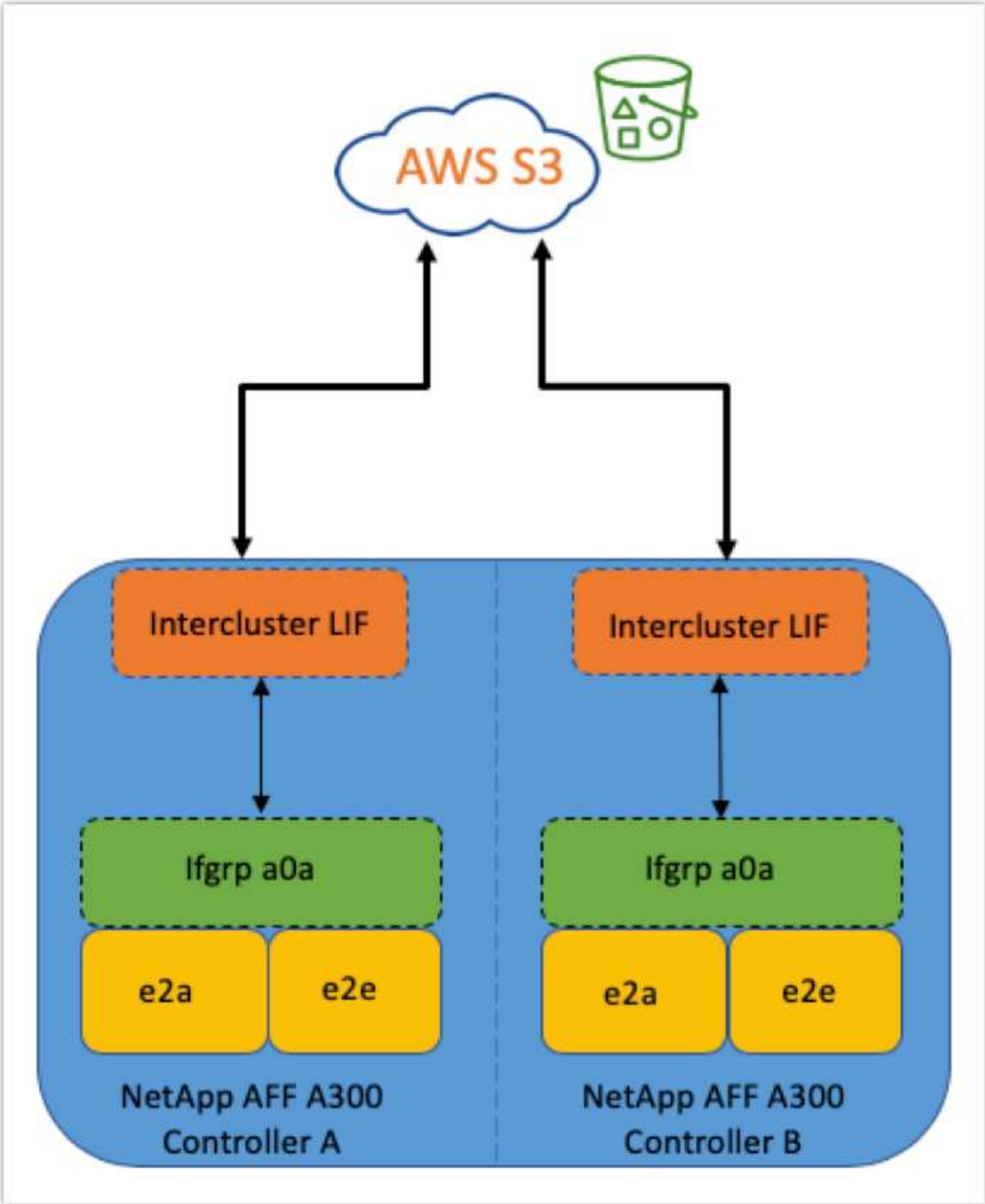
ルーティングが異なるノードで複数の Intercluser LIF を使用する場合は、異なる IPspace に配置することを推奨します。FabricPool では設定時に複数の IPspace から選択できますが、 IPspace 内の特定のクラスタ間 LIF を選択することはできません。

クラスタ間 LIF を無効化または削除すると、クラウド階層への通信が中断されます。

接続性

FabricPool 読み取りレイテンシは、クラウド階層への接続機能です。次の図に示すように、 10Gbps ポートを使用するクラスタ間 LIF は、十分なパフォーマンスを提供します。特定のネットワーク環境のレイテンシとスループットを検証して、 FabricPool のパフォーマンスに与える影響を判断することを推奨します。

低パフォーマンスの環境で FabricPool を使用する場合は、クライアントアプリケーションの最小パフォーマンス要件を引き続き満たし、それに応じてリカバリ時間の目標を調整する必要があります。



オブジェクトストアプロファイラ

次に示すオブジェクトストアプロファイラの例は ONTAP の CLI から実行でき、 FabricPool アグリゲートに接続する前にオブジェクトストアのレイテンシとスループットのパフォーマンスをテストします。

クラウド階層は、オブジェクトストレージプロファイラで使用する前に ONTAP に追加する必要があります。

次のコマンドを使用して、 ONTAP の advanced 権限モードからオブジェクトストアプロファイラを開始します。

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

結果を表示するには、次のコマンドを実行します。

```
storage aggregate object-store profiler show
```

クラウド階層では、パフォーマンス階層のようなパフォーマンスは提供されません（通常は毎秒 GB ）。FabricPool アグリゲートは、 SATA のようなパフォーマンスを簡単に提供できますが、 SATA のようなパフォーマンスを必要としない階層化ソリューションでは、 10 秒という高いレイテンシと低いスループットも許容できます。

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                        min       max       avg
-----------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817      69.55MB
GET     4KB        158636    0         27        1132      41        32.22MB
GET     8KB        0         0         0         0         0         0B
GET     32KB       0         0         0         0         0         0B
GET     256KB      0         0         0         0         0         0B
5 entries were displayed.
```

個のボリューム

ストレージシンプロビジョニングは、 FlexPod 仮想インフラ管理者向けの標準的な手法です。NetApp Virtual Storage Console （ VSC ）では、 VMware データストアのストレージボリュームを、スペースギャランティ（シンプロビジョニング）なしでプロビジョニングできます。また、ネットアップのベストプラクティスに従って、ストレージ効率の設定が最適化されます。VSC を使用して VMware データストアを作成する場合は、データストアボリュームにスペースギャランティを割り当てる必要がないため追加の操作は必要ありません。

FabricPool は、「なし」以外のスペースギャランティを使用するボリュームを含むアグリゲート（「ボリューム」など）にクラウド階層を接続できません。

```
volume modify -space-guarantee none
```

'pace guarantee none' パラメータを設定すると ' ボリュームのシン・プロビジョニングが行われますこのギャランティタイプのボリュームで使用されるスペースの量は、初期ボリュームサイズで決定されるのではなく、データが追加されるにつれて増加します。このアプローチは FabricPool にとって不可欠です。ボリュームがホットになりパフォーマンス階層に戻されるクラウド階層データをサポートする必要があるためです。

ライセンス

FabricPool では、サードパーティのオブジェクトストレージプロバイダ（ Amazon S3 など）を AFF および FAS ハイブリッドフラッシュシステムのクラウド階層として接続する場合、容量ベースのライセンスが必要です。

FabricPool ライセンスには恒久ライセンスとタームベースライセンス（ 1 年または 3 年）があります。

クラウド階層に格納されているデータの量（使用容量）がライセンス容量に達すると、クラウド階層への階層化が停止します。「すべて」の階層化ポリシーを使用したボリュームへの SnapMirror コピーを含む追加データは、ライセンス容量が増加するまで階層化できません。階層化は停止しますが、クラウド階層のデータには引き続きアクセスできます。ライセンスされた容量が増えるまで、追加のコールドデータは SSD に残ります。

新しい ONTAP 9.5 以降のクラスタを購入すると、無料の 10TB 容量のタームベースの FabricPool ライセンスが付属しますが、追加のサポートコストが適用される場合があります。FabricPool ライセンス（既存のライセンスの追加容量を含む）は、 1TB 単位で購入できます。

FabricPool ライセンスは、 FabricPool アグリゲートを含まないクラスタからのみ削除できます。

> FabricPool ライセンスはクラスタ全体に適用されます。ライセンスの購入時にUUIDを用意しておく必要があります (`cluster identify show`）。追加のライセンス情報については、を参照してください "ネットアップナレッジベース"。

設定

ソフトウェアのリビジョン

次の表に、検証済みのハードウェアとソフトウェアのバージョンを示します。

レイヤー（ **Layer** ）	デバイス	イメージ（ **Image** ）	コメント
ストレージ	NetApp AFF A300	ONTAP 9.6P2	
コンピューティング	Cisco UCS B200 M5 ブレードサーバ、 Cisco UCS VIC 1340	リリース 4.0 （ 4b ）	
ネットワーク	Cisco Nexus 6332-16UP ファブリックインターコネクト	リリース 4.0 （ 4b ）	
	NX-OS スタンドアロンモードの Cisco Nexus 93180YC-EX スイッチ	リリース 7.0(3) i7(6)	
ストレージネットワーク	Cisco MDS 9148S	リリース 8.3(2)	

レイヤー（ **Layer** ）	デバイス	イメージ（ **Image** ）	コメント
ハイパーバイザー		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603.
		VMware vCenter Server の各機能を使用し	vCenter サーバ 6.7.0.30000 ビルド 13639309
クラウドプロバイダ		Amazon AWS S3	デフォルトオプションを使用する標準の S3 バケット

FabricPool の基本要件については、を参照してください "FabricPool の要件"。基本的な要件をすべて満たしたら、次の手順を実行して FabricPool を設定します。

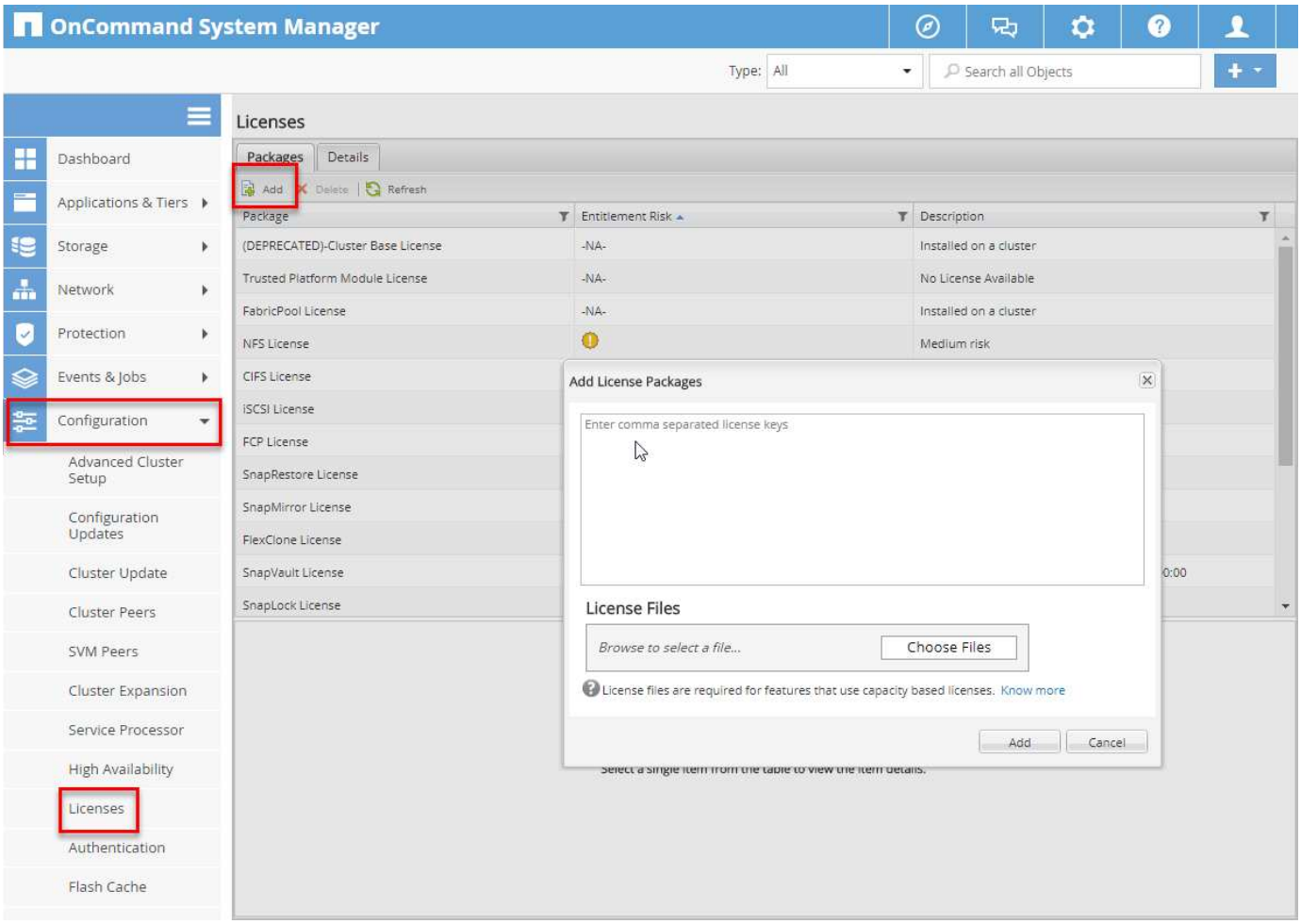
1. FabricPool ライセンスをインストールする。
2. AWS S3 オブジェクトストアバケットを作成する。
3. ONTAP にクラウド階層を追加します。
4. クラウド階層をアグリゲートに接続する。
5. ボリューム階層化ポリシーを設定

"次の手順： FabricPool ライセンスをインストールします。"

FabricPool ライセンスをインストールする

ネットアップライセンスファイルを取得したら、 OnCommand System Manager でインストールできます。ライセンスファイルをインストールするには、次の手順を実行します。

1. 構成をクリックします
2. クラスタをクリックします。
3. [ライセンス] をクリックします
4. 追加をクリックします。
5. [ファイルの選択] をクリックして、ファイルを参照して選択します。
6. 追加をクリックします。



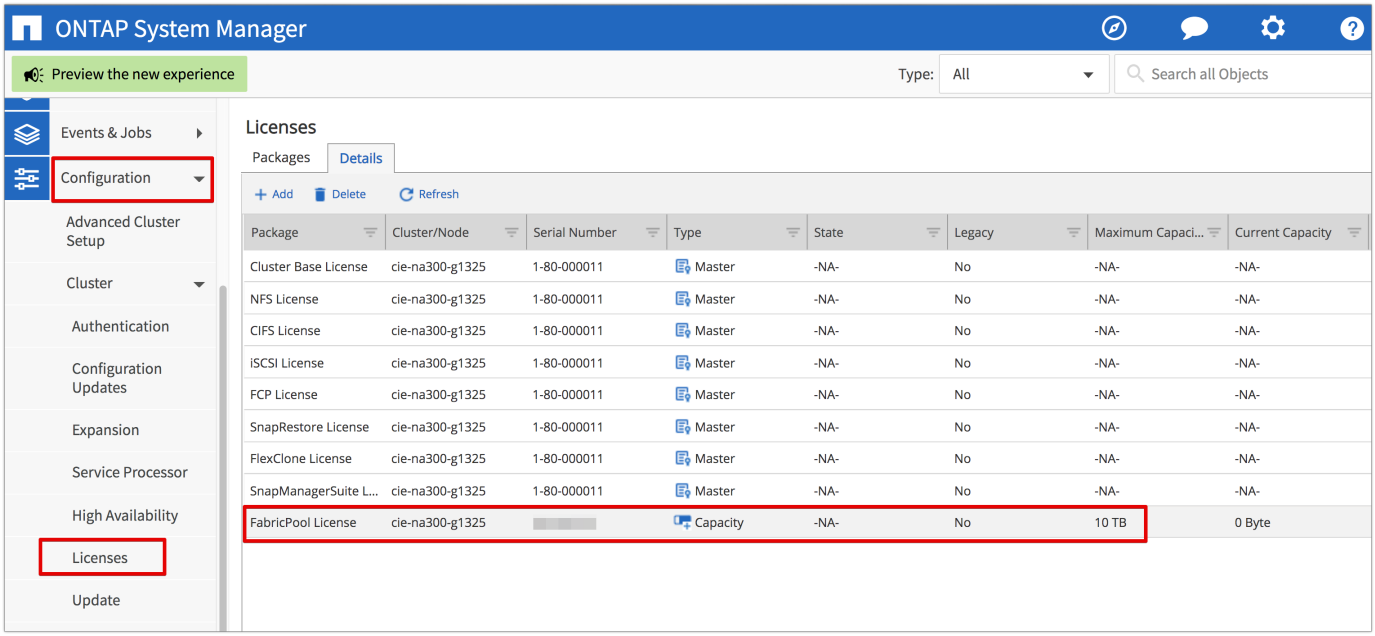
ライセンス容量

ライセンス容量を表示するには、 ONTAP CLI または OnCommand System Manager を使用します。ライセンス容量を確認するには、 ONTAP CLI で次のコマンドを実行します。

```
system license show-status
```

OnCommand システムマネージャで、次の手順を実行します。

1. 構成をクリックします
2. [ライセンス] をクリックします
3. [詳細] タブをクリックします。



FabricPool ライセンスの行には、最大容量と現在の容量が表示されます。

"次： AWS S3 バケットを作成します。"

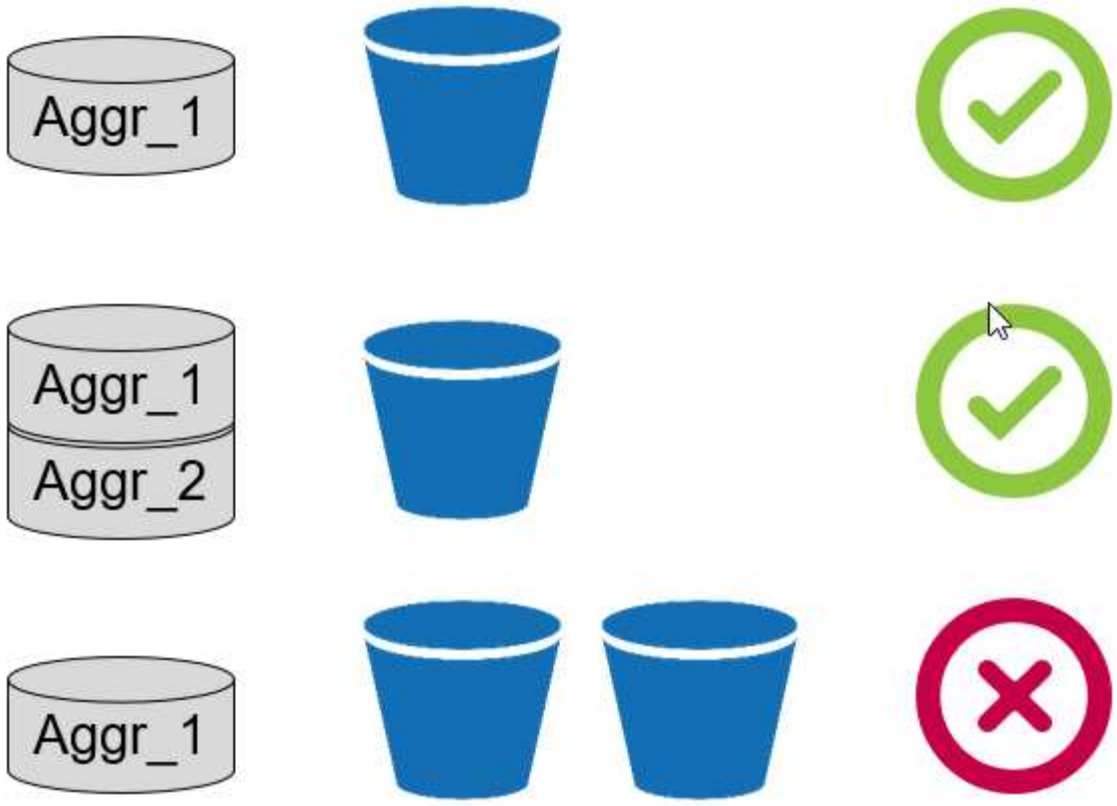
AWS S3 バケットを作成する

バケットは、データを保持するオブジェクトストレージコンテナです。データをクラウド階層としてアグリゲートに追加する前に、データが格納されているバケットの名前と場所を指定する必要があります。

> バケットは、 OnCommand システムマネージャ、 OnCommand Unified Manager 、または ONTAP を使用して作成することはできません。

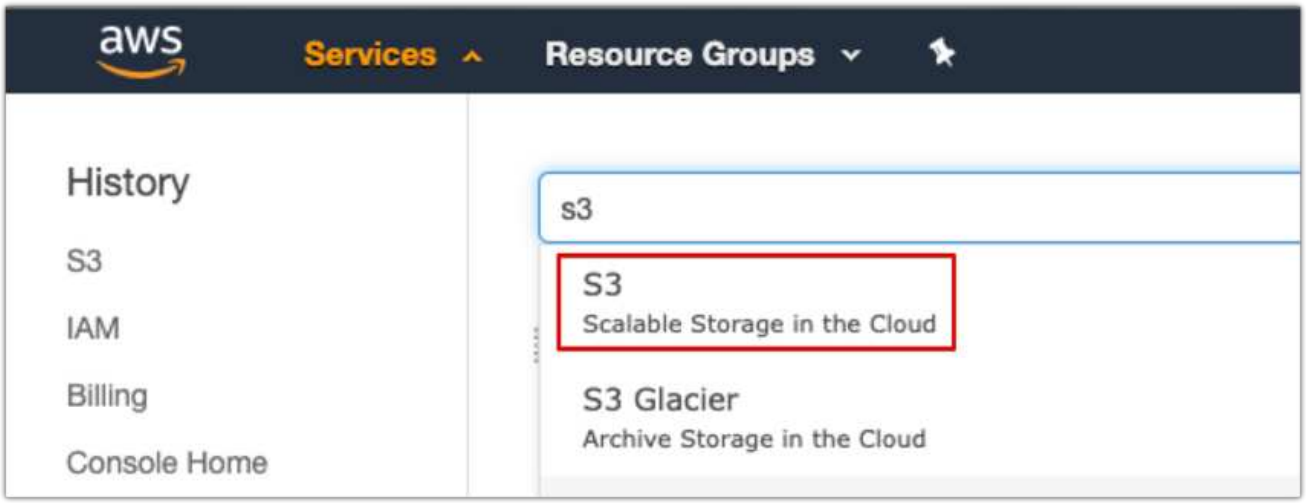
次の図に示すように、 FabricPool ではアグリゲートごとに 1 つのバケットの接続がサポートされます。1 つのバケットを 1 つのアグリゲートに接続し、 1 つのバケットを複数のアグリゲートに接続できます。ただし、 1 つのアグリゲートを複数のバケットに接続することはできません。1 つのバケットをクラスタ内の複数のアグリゲートに接続することはできますが、複数のクラスタ内のアグリゲートに 1 つのバケットを接続することは推奨されません。

ストレージアーキテクチャを計画する際は、バケットとアグリゲートの関係がパフォーマンスにどのように影響するかを検討してください。多くのオブジェクトストレージプロバイダは、サポートされる IOPS の最大数をバケットレベルまたはコンテナレベルで設定しています。最大のパフォーマンスを必要とする環境では、複数のバケットを使用して、オブジェクトストレージの IOPS 制限が複数の FabricPool アグリゲートのパフォーマンスに影響する可能性を軽減する必要があります。クラスタ内のすべての FabricPool アグリゲートに単一のバケットまたはコンテナを接続すると、クラウド階層のパフォーマンスよりも管理性の高い環境が有利になることがあります。

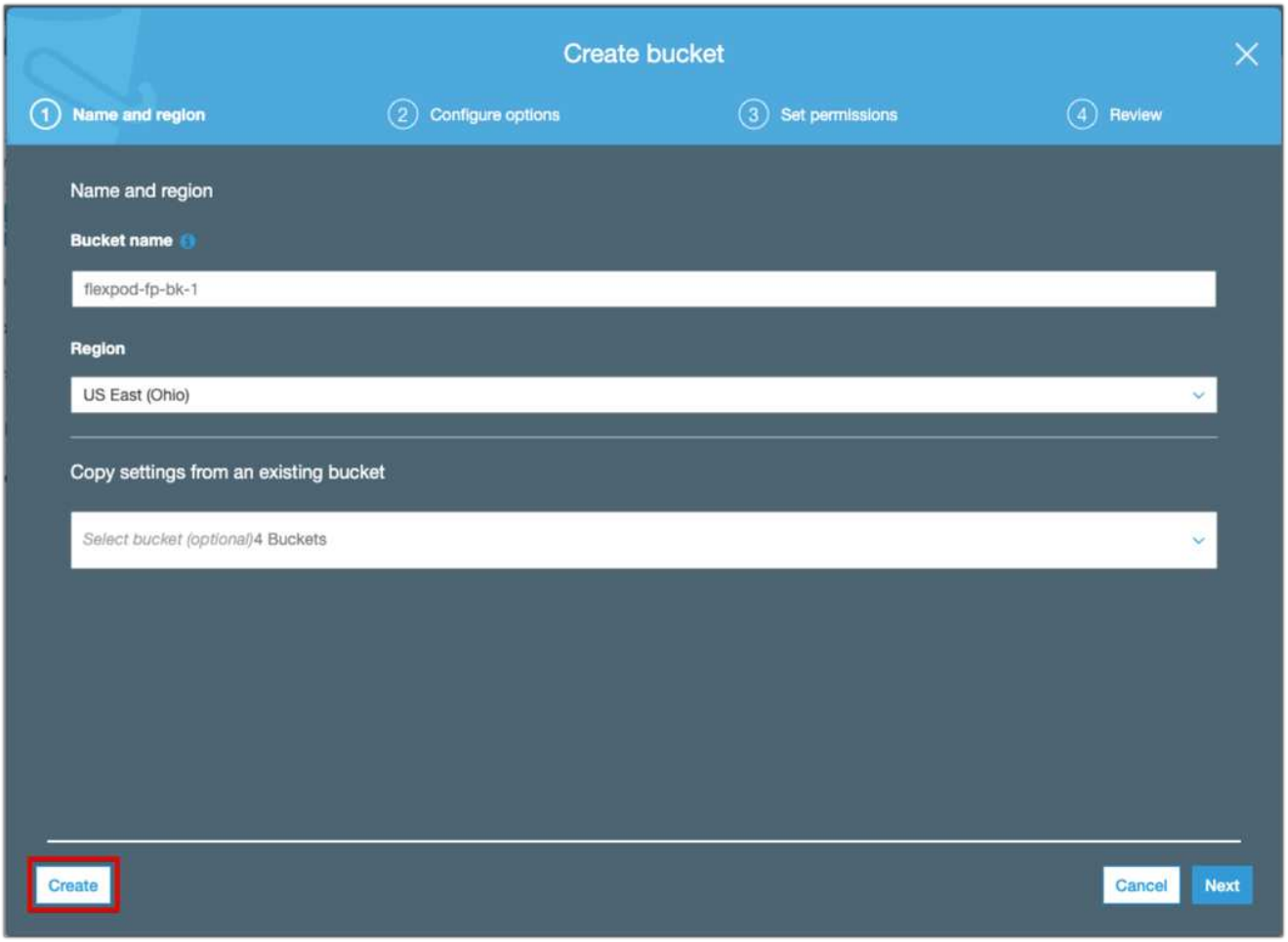


S3 バケットを作成します。

1. ホームページから AWS 管理コンソールの検索バーに「 S3 」と入力します。
2. クラウドで S3 Scalable Storage を選択します。



3. S3 ホームページで、バケットの作成を選択します。
4. DNS 準拠の名前を入力し、バケットを作成するリージョンを選択します。



5. Create をクリックしてオブジェクトストアバケットを作成します。

"次： ONTAP にクラウド階層を追加します"

ONTAP にクラウド階層を追加します

オブジェクトストレージをアグリゲートに接続する前に、オブジェクトストレージを追加し、 ONTAP で識別する必要があります。このタスクは、 OnCommand システムマネージャまたは ONTAP CLI のどちらかで実行できます。

FabricPool は、クラウド階層として Amazon S3 、 IBM Object Cloud Storage 、および Microsoft Azure Blob Storage オブジェクトストアをサポートしています。

次の情報が必要です。

- サーバ名（ FQDN ）。例：「 3.amazonaws.com 」
- アクセスキー ID
- シークレットキー
- コンテナ名（バケット名）

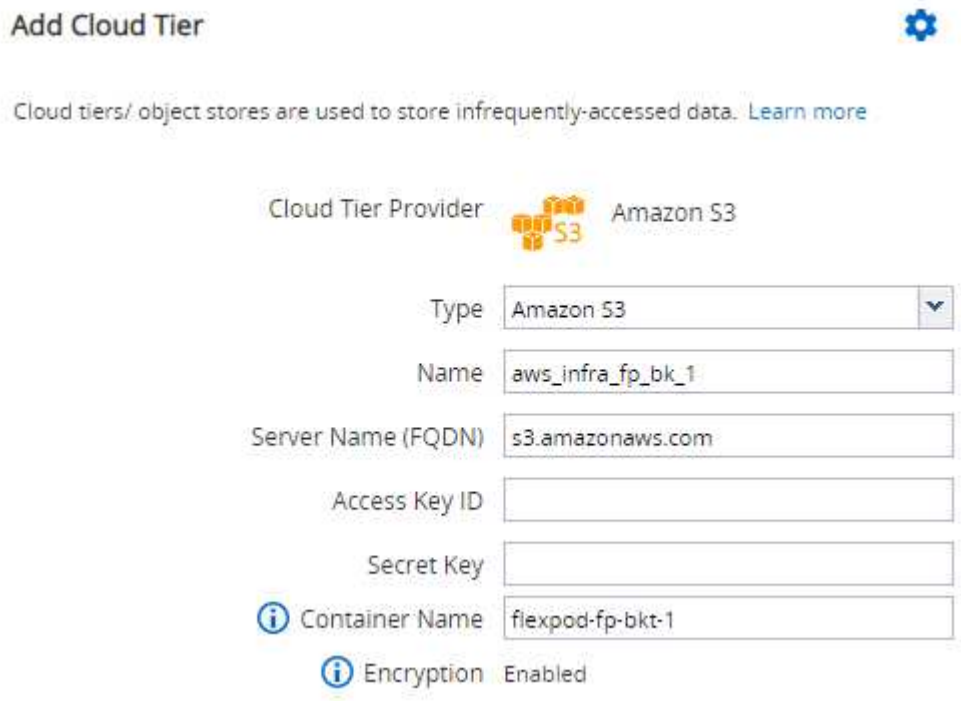
OnCommand システムマネージャ

OnCommand System Manager を使用してクラウド階層を追加するには、次の手順を実行します。

1. OnCommand System Manager を起動します。
2. [ストレージ] をクリックします
3. アグリゲートとディスクをクリックします。
4. クラウド階層をクリックします。
5. オブジェクトストアプロバイダを選択します。
6. オブジェクトストアプロバイダの必要に応じてテキストフィールドを入力します。

   Container Name フィールドに、オブジェクトストアのバケット名またはコンテナ名を入力します。

7. アグリゲートを保存して接続をクリックします。



ONTAP CLI

ONTAP CLI を使用してクラウド階層を追加するには、次のコマンドを入力します。

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"次：クラウド階層を ONTAP アグリゲートに接続します。"

ONTAP アグリゲートにクラウド階層を接続する

ONTAP でオブジェクトストアを追加して識別したら、そのオブジェクトストアをアグリゲートに接続して FabricPool を作成する必要があります。このタスクは、 OnCommand システムマネージャまたは ONTAP CLI を使用して実行できます。

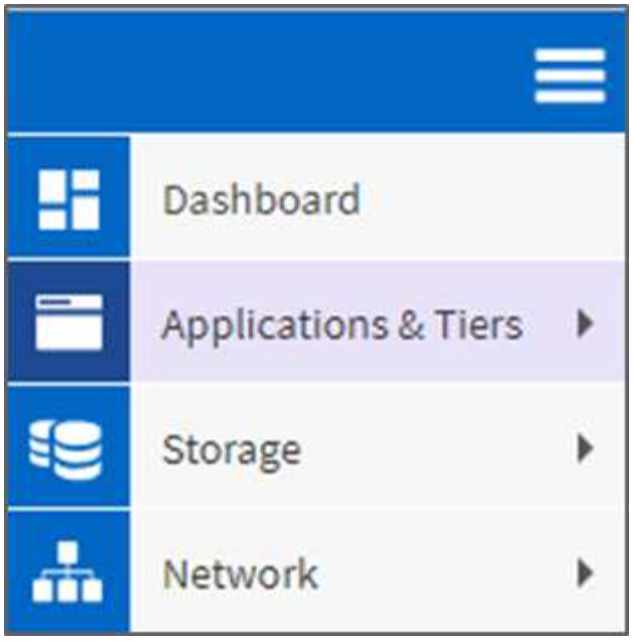
1 つのクラスタに複数のタイプのオブジェクトストアを接続できますが、各アグリゲートに接続できるオブジェクトストアのタイプは 1 つだけです。たとえば、 1 つのアグリゲートで Google Cloud を使用でき、別のアグリゲートで Amazon S3 を使用できますが、 1 つのアグリゲートを両方に接続することはできません。

> クラウド階層をアグリゲートに接続することは、永続的なアクションです。クラウド階層は、接続されているアグリゲートから接続を解除することはできません。

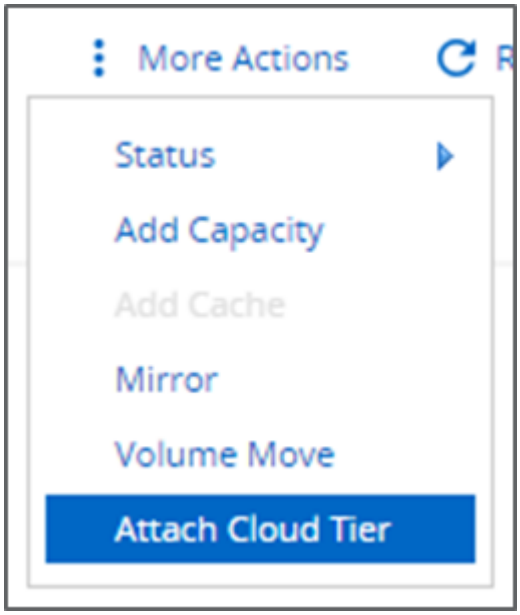
OnCommand システムマネージャ

OnCommand System Manager を使用してクラウド階層をアグリゲートに接続するには、次の手順を実行します。

1. OnCommand System Manager を起動します。
2. [アプリケーションと階層] をクリックします。



3. [ストレージ階層] をクリックします。
4. アグリゲートをクリックします。
5. アクションをクリックし、クラウド階層の接続を選択します。



6. クラウド階層を選択します。
7. アグリゲート上のボリュームの階層化ポリシーを表示および更新します（オプション）。デフォルトでは、ボリューム階層化ポリシーは「 Snapshot のみ」に設定されています。
8. [保存] をクリックします .

ONTAP CLI

ONTAP CLI を使用してアグリゲートにクラウド階層を接続するには、次のコマンドを実行します。

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

例

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"次：ボリューム階層化ポリシーを設定します。"

ボリューム階層化ポリシーを設定します

デフォルトでは、ボリュームは「なし」ボリューム階層化ポリシーを使用します。ボリュームの作成後、 OnCommand システムマネージャまたは ONTAP CLI を使用してボリューム階層化ポリシーを変更できます。

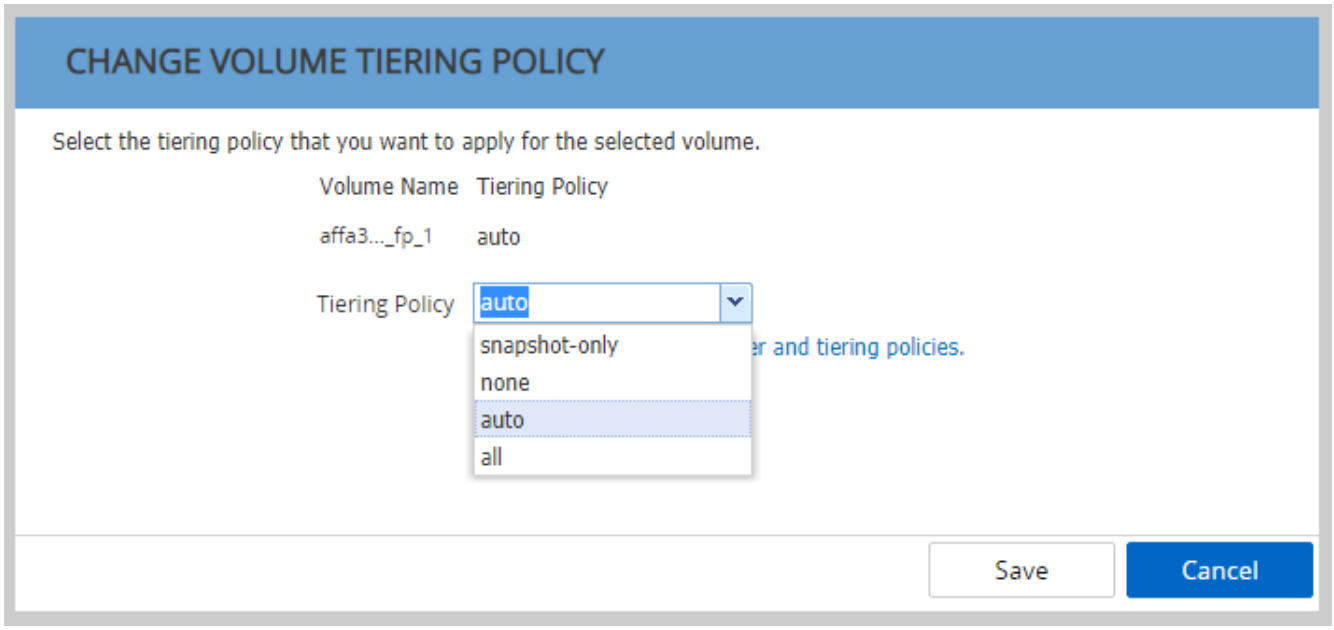
FlexPod で使用する場合、 FabricPool には、「自動」、「 Snapshot のみ」、「なし」の 3 つのボリューム階層化ポリシーが用意されています。

- * 自動 *
  - ボリューム内のすべてのコールドブロックがクラウド階層に移動されます。アグリゲートの使用率が 50% を超えている場合、非アクティブなブロックがコールドになるまでに約 31 日かかります。自動クーリング期間は、「 tiering-minimum-cooling-days 」設定を使用して、 2 日から 63 日の間で調整できます。
  - 階層化ポリシーが「自動」に設定されているボリューム内のコールドブロックがランダムに読み取られると、ブロックがホットになり、パフォーマンス階層に書き込まれます。
  - 階層化ポリシーが「自動」に設定されているボリューム内のコールドブロックが順番に読み取られると、コールドブロックのままクラウド階層に残ります。パフォーマンス階層には書き込まれません。
- * Snapshot のみ *
  - アクティブなファイルシステムと共有されていないボリューム内のコールドスナップショットブロックはクラウド階層に移動されます。アグリゲートの使用率が 50% を超えている場合、非アクティブな Snapshot ブロックがコールドになるまでに約 2 日かかります。「 tiering-minimum-cooling-days 」設定を使用すると、 Snapshot のみのクーリング期間を 2 日から 63 日に調整できます。
  - 階層化ポリシーが「 Snapshot のみ」に設定されているボリューム内のコールドブロックが読み取られるとホットになり、パフォーマンス階層に書き込まれます。
- * なし（デフォルト） *
  - 階層化ポリシーで「なし」を使用するように設定されたボリュームは、コールドデータをクラウド階層に階層化しません。
  - 階層化ポリシーを「なし」に設定すると、新しい階層化が防止されます。
  - 以前にクラウド階層に移動したボリュームデータは、ホットになるまでクラウド階層に残り、パフォーマンス階層に自動的に戻ります。

OnCommand システムマネージャ

OnCommand システムマネージャを使用してボリュームの階層化ポリシーを変更するには、次の手順を実行します。

1. OnCommand System Manager を起動します。
2. ボリュームを選択します。
3. その他の操作をクリックし、階層化ポリシーの変更を選択します。
4. ボリュームに適用する階層化ポリシーを選択します。
5. [保存] をクリックします .



ONTAP CLI

ONTAP CLI を使用してボリュームの階層化ポリシーを変更するには、次のコマンドを実行します。

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"次の手順：ボリューム階層化の最小クーリング日数を設定します。"

ボリューム階層化の最小クーリング日数を設定します

「 tiering-minimum-cooling-days 」設定では、ボリューム内のアクセス頻度の低いデータがコールドとみなされて階層化の対象になるまでの日数を指定します。

自動

Auto 階層化ポリシーのデフォルトの「 tiering-minimum-cooling-days 」設定は 31 日です。

読み取りではブロック温度がホットになるため、この値を大きくすると、階層化の対象となるデータ量が減り、パフォーマンス階層に保持されるデータ量が増加する可能性があります。

この値をデフォルトの 31 日間から減らす場合は、コールドとしてマークされる前にデータをアクティブにしないようにしてください。たとえば ' 複数日のワークロードが 7 日目にかなりの数の書き込みを実行すると予想される場合 ' ボリュームの「 tiering-minimum-cooling-days 」設定は 8 日以上に設定する必要があります

> オブジェクトストレージは、ファイルやブロックストレージのようにトランザクション可能ではありません。ボリュームにオブジェクトとして保存されているファイルを変更してクーリング日数を最小限に抑えると、新しいオブジェクトの作成、既存のオブジェクトの断片化、およびストレージの非効率性の追加につながる可能性があります。

Snapshot のみ

スナップショット専用階層化ポリシーのデフォルトの「 tiering-minimum-cooling-days 」設定は 2 日です。最小値を 2 日間に設定すると、バックグラウンドプロセスの時間が長くなり、ストレージ効率が最大限に向上します。また、日々のデータ保護プロセスがクラウド階層からデータを読み取る必要がなくなります。

ONTAP CLI

ONTAP CLI を使用してボリュームの「 tiering-minimum-cooling-days 」設定を変更するには、次のコマンドを実行します。

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

advanced 権限レベルが必要です。

> 階層化ポリシーを「自動」と「 Snapshot のみ」（またはその逆）の間で変更すると、パフォーマンス階層のブロックの非アクティブ期間がリセットされます。たとえば、「自動」ボリューム階層化ポリシーを使用し、 20 日間非アクティブだったパフォーマンス階層のデータを含むボリュームでは、階層化ポリシーが「 Snapshot のみ」に設定されている場合、パフォーマンス階層のデータが非アクティブになる日数は 0 日にリセットされます。

パフォーマンスに関する考慮事項

高パフォーマンス階層のサイズを設定します

サイジングを検討する場合は、パフォーマンス階層で次のタスクを実行できる必要があります。

- ホットデータのサポート
- 階層化スキャンによってデータがクラウド階層に移動されるまでコールドデータのサポート
- ホットになりパフォーマンス階層に書き戻されるクラウド階層データのサポート
- 接続されたクラウド階層に関連付けられた WAFL メタデータをサポートしています

ほとんどの環境では、 FabricPool アグリゲートのパフォーマンスと容量の比率は 1 ： 10 で、非常に控えめであるため、ストレージを大幅に節約できます。たとえば、 200TB をクラウド階層に階層化する場合、パフォーマンス階層アグリゲートは少なくとも 20TB にする必要があります。

パフォーマンス階層の容量が 70% を超える場合、クラウド階層からパフォーマンス階層への書き込みは無効になります。この場合、ブロックはクラウド階層から直接読み取られます。

クラウド階層のサイズを設定する

サイジングを検討する場合、クラウド階層として機能するオブジェクトストアは次のタスクを実行できる必要があります。

- 既存のコールドデータの読み取りをサポートします
- 新しいコールドデータの書き込みをサポートします
- オブジェクトの削除とデフラグをサポートしています

所有コスト

。 "FabricPool 経済計算ツール" 独立した IT アナリスト企業の Evaluator Group が、オンプレミスとクラウドの間でコールドデータストレージのコスト削減を予測できるよう支援します。この計算ツールは、アクセス頻度の低いデータをパフォーマンス階層に格納するコストと、残りのデータライフサイクルについてクラウド階層に送信するコストを算出するシンプルなインターフェイスです。5 年間の計算に基づいて、ソース容量、データ増加率、スナップショット容量、コールドデータの割合の 4 つの主要な要素を使用して、その期間におけるストレージコストを決定します。

まとめ

クラウドへの移行は、組織ごと、ビジネスユニットごと、組織内のビジネスユニット間で異なります。一部は急速な導入を選択し、その他はより控えめなアプローチを採用しています。FabricPool は、組織の規模やクラウドの導入速度に関係なく、組織のクラウド戦略に適合し、 FlexPod インフラの効率性と拡張性のメリットをさらに実証します。

追加情報の参照先

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。

- FabricPool のベストプラクティス

  "www.netapp.com/us/media/tr-4598.pdf"

- ネットアップの製品マニュアル

  "https://docs.netapp.com"

- TR-4036 ：『 FlexPod データセンター技術仕様』

  "https://www.netapp.com/us/media/tr-4036.pdf"

IBMクラウドプライベートを使用するFlexPod データセンター

Sreenivasa Edula、Cisco Thanachit Wichianchai、IBM Jacky Ben-Bassat、IBM Global Alliance、ネットアップ

IBM Cloud Private（ICP）は、クラウドネイティブやアプリケーション最新化のユースケース向けにコンテナ化されたアプリケーションを開発、管理するためのオンプレミスプラットフォームです。コンテナオーケストレーションとしてKubernetes上に構築された統合環境で、Dockerコンテナ用のプライベートイメージリポジトリ、管理コンソール、監視フレームワーク、多くのオープンソースベースおよびIBMコンテナ化アプリケーションなどが含まれます。Ciscoとネットアップが提供する統合インフラであるFlexPod とICPを組み合わせることで、インフラの導入と管理が簡易化されます。また、ストレージ効率の向上、データ保護の強化、リスクの軽減、この可用性に優れたエンタープライズクラスのインフラスタックを柔軟に拡張できるというメリットも得られ、新しいビジネス要件や長期的なその他の変化に対応できます。

"IBMクラウドプライベートを使用するFlexPod データセンター"

FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage -設計

ネットアップ、Haseeb Niazi、Cisco David Arnette

Cisco Validated Design（CVD）は、お客様の導入を促進および改善するために設計、テスト、文書化されたシステムとソリューションを提供します。これらの設計では、お客様のビジネスニーズに対応し、設計から導入までを支援するために開発されたソリューションポートフォリオに、幅広いテクノロジと製品が組み込まれています。

"FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage -設計"

Cisco CloudCenterとネットアップデータファブリックを使用したマルチクラウド対応のFlexPod データセンター

ネットアップ、Haseeb Niazi、Cisco David Arnette

本ドキュメントでは、FlexPod Datacenter for Hybrid Cloudをセットアップするための設定と実装の詳細なガイドラインを提供します。次の設計要素は、このバージョンのFlexPod を以前のモデルと区別します。

- Cisco CloudCenterとFlexPod データセンターの統合（ACIをプライベートクラウドとして使用
- Cisco CloudCenterとAmazon Web Services（AWS）およびMicrosoft Azure Resource Manager（MS Azure RM）パブリッククラウドの統合
- FlexPod データセンターとパブリッククラウドの間にセキュアな接続を提供し、仮想マシン（VM）間のトラフィックをセキュアに保護
- データレプリケーショントラフィック用に、FlexPod データセンターとNetApp Private Storage（NPS）

の間にセキュアな接続を提供します

- パブリッククラウドまたはプライベートクラウドにアプリケーションインスタンスを導入し、Cisco CloudCenterによるオーケストレーションを通じて最新のアプリケーションデータをこれらのインスタンスで利用できるようにする機能
- この新しいハイブリッドクラウドモードで、開発およびテスト環境の運用面をセットアップ、検証、強調します。

"Cisco CloudCenterとネットアップデータファブリックを使用したマルチクラウド対応のFlexPod データセンター"

エンタープライズデータベース

SAP

FlexPod での SAP の紹介

FlexPod プラットフォームは、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus ファミリースイッチ、およびネットアップストレージコントローラを基盤として構築された、事前設計されたベストプラクティスのデータセンターアーキテクチャです。

FlexPod は、 SAP アプリケーションの実行に適したプラットフォームです。本ソリューションを使用することで、お客様は、カスタマイズされたデータセンター統合モデルを使用して、 SAP HANA を迅速かつ確実に導入できます。FlexPod は、ベースライン構成だけでなく、さまざまなユースケースや要件に対応できるよう、サイズ設定と最適化が可能な柔軟性も備えています。

<xmt-block0>FlexPod</xmt-block> Datacenter for SAP<xmt-block1>解決策</xmt-block> Using FibreChannel SAN with Cisco UCS Manager 4.0 and NetApp<xmt-block2> ONTAP</xmt-block> 9.7

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

本ドキュメントでは、特にSAP HANA対応の第2世代Intel Xeonスケーラブルプロセッサを搭載した、NetApp AFF A400ストレージおよびCisco UCS Managerユニファイドソフトウェアリリース4.1(1)上で稼働するNetApp ONTAP 9.7を搭載したCiscoとNetApp FlexPod データセンターについて説明します。

FlexPod データセンターとNetApp ONTAP 9.7およびCisco UCSユニファイドソフトウェアリリース4.1(1)は、Cisco Unified Computing System（Cisco UCS）、Cisco Nexus 9000スイッチファミリー、MDS 9000マルチレイヤファブリックスイッチ、 およびONTAP 9.7ストレージOSを実行するNetApp AFF Aシリーズストレージアレイ。

"FlexPod Datacenter for SAP解決策 Using FibreChannel SAN with Cisco UCS Manager 4.0 and NetApp ONTAP 9.7"

ホワイトペーパー『SAP Non-HANA with SQL』-『Design』

現在のIT業界は、データセンターソリューションの劇的な変革を目の当たりにしています。近年、検証済みで設計されたデータセンターソリューションに大きな関心が寄せられています。重要な領域での仮想化テクノロジーの導入は、これらのソリューションの設計原則とアーキテクチャに大きな影響を与えました。これにより、ベアメタルシステム上で実行されている多くのアプリケーションを、新しい仮想化統合ソリューションに移行できるようになりました。FlexPod は、IT部門の急速に変化するニーズに対応するように設計された、事前検証済みで設計されたデータセンター解決策 の1つです。Ciscoとネットアップは提携してFlexPod を提供しています。このソリューションでは、データベース、エンタープライズリソースプランニング（ERP）、顧客関係管理（CRM）、Webアプリケーションなど、さまざまなエンタープライズワークロードの基盤として、業界最高クラスのコンピューティング、ネットワーク、ストレージコンポーネント

を使用します。

近年、ITアプリケーション、特にデータベースの統合に大きな関心が寄せられています。過去数年間で最も広く採用され、導入されているデータベースプラットフォームは、Microsoft SQL Serverです。SQL Serverデータベースは、データベーススプロールの影響を受けることが多く、サーバの利用率の低さ、ライセンスの不正確さ、セキュリティ上の懸念、管理上の懸念、膨大な運用コストなど、ITの課題につながっています。そのため、SQL Serverデータベースは、堅牢性、柔軟性、耐障害性に優れたプラットフォーム上での統合に適しています。このドキュメントでは、SQL Serverデータベースを導入および統合するためのFlexPod リファレンスアーキテクチャについて説明します。

"ホワイトペーパー『SAP Non-HANA with SQL』-『Design』"

FlexPod Datacenter for SAP解決策 with Cisco UCS Third-generation fabric and NetApp AFF A–Series

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

本ドキュメントでは、第2世代Intel Xeonスケーラブルプロセッサでサポートされる Cisco UCSコンピューティングシステム（Cisco UCS）をベースにした、CiscoとNetApp FlexPod Datacenter for SAP HANAの導入方法について説明します。

Cisco UCS Manager（UCSM）4.0(4)は、現在のすべてのCisco UCSファブリックインターコネクトモデル（6200、6300、6324、6454）、2200/2300シリーズIOM、Cisco UCS Bシリーズブレード、およびCisco UCS Cシリーズラックフォームファクタサーバの統合サポートを提供します。Cisco UCSユニファイドソフトウェアリリース4.0（4D）とNetApp ONTAP 9.6を搭載したFlexPod データセンターは、Cisco UCS、Cisco Nexus 9000スイッチファミリー、NetApp AFF Aシリーズストレージアレイを基盤に構築された、事前設計されたベストプラクティスに基づくデータセンターアーキテクチャです。

"FlexPod Datacenter for SAP解決策 with Cisco UCS Third-generation Fabric and NetApp AFF A–Series"

『FlexPod Datacenter for SAP解決策 Using FibreChannel SAN with Cisco UCS Manager 4.0 and NetApp ONTAP 9.7-Design』

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

Ciscoとネットアップは提携して、戦略的なデータセンタープラットフォームを実現する一連のFlexPod ソリューションを提供しています。FlexPod 解決策 は、コンピューティング、ストレージ、ネットワーク設計のベストプラクティスを組み込んだ統合アーキテクチャを提供します。そのため、統合アーキテクチャを検証してさまざまなコンポーネント間の互換性を確保することで、ITリスクを最小限に抑えることができます。また、解決策 は、導入のさまざまな段階（計画、設計、実装）で使用できる文書化された設計ガイダンス、導入ガイダンス、およびサポートを提供することで、ITの課題にも対処します。

"『FlexPod Datacenter for SAP解決策 Using FibreChannel SAN with Cisco UCS Manager 4.0 and NetApp ONTAP 9.7-Design』"

FlexPod Datacenter for SAP解決策 with Cisco ACI、Cisco UCS Manager 4.0、and NetApp AFF A–Series-Design

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

このドキュメントでは、SAP HANAテーラードデータセンター統合（TDI）環境を導入するための検証済みアプローチとして、Cisco ACI統合FlexPod 解決策 について説明します。この検証済みの設計では、SAP HANAを実装するためのガイドラインとフレームワークを、Ciscoとネットアップのベストプラクティスとともに提供します。

推奨される解決策 アーキテクチャは、Cisco Unified Computing System（Cisco UCS）上に構築され、ユニファイドソフトウェアリリースを使用して、次のコンポーネントを含むCisco UCSハードウェアプラットフォームをサポートします。

- Cisco UCS BシリーズブレードサーバおよびCisco UCS Cシリーズラックサーバは、Intel Optane Data Center Persistent Memory Module（DCPMM）オプションで構成できます
- Cisco UCS 6400シリーズファブリックインターコネクト
- Cisco Nexus 9000シリーズリーフ/スパインスイッチ
- ネットアップオールフラッシュシリーズストレージアレイ

また、このドキュメントでは、Red Hat Enterprise LinuxとSUSE Linux Enterprise Server for SAP HANAの両方について検証を行います。

"FlexPod Datacenter for SAP解決策 with Cisco ACI、Cisco UCS Manager 4.0、and NetApp AFF A–Series-Design"

<xmt-block0>FlexPod</xmt-block> Datacenter for SAP with Cisco ACI、Cisco UCS Manager 4.0、and NetApp<xmt-block1> AFF</xmt-block> A–Series- Deployment

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

本ドキュメントでは、FlexPod インフラにおけるSAP HANAテーラードデータセンター統合オプションのアーキテクチャと導入手順について説明します。このオプションは次の要素で構成されます。

- Cisco UCS Computing System（Cisco UCS）は、第2世代Intel Xeonスケーラブルプロセッサによってサポートされます。
- Cisco Application Centric Infrastructure（ACI）を活用したスイッチング製品。
- ネットアップAシリーズAFF アレイ：

本ドキュメントでは、SAP HANAを導入するための詳細な設定手順を説明します

"FlexPod Datacenter for SAP with Cisco ACI、Cisco UCS Manager 4.0、and NetApp AFF A–Series-Deployment"

FlexPod Datacenter for SAP解決策 with Cisco UCS Manager 4.0 and NetApp AFF A–Series-Design

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

本ドキュメントでは、CiscoとNetApp FlexPod 解決策 について説明します。これは、SAP HANAテーラードデータセンター統合（TDI）環境を導入するための検証済みアプローチです。この検証済みの設計では、SAP HANAを実装するためのガイドラインとフレームワークを、Ciscoとネットアップのベストプラクティスとともに提供します。

FlexPod は業界をリードする統合インフラで、幅広いエンタープライズワークロードとユースケースに対応しています。この解決策 を使用すると、カスタマイズされたデータセンター統合モードのモデルを使用して、SAP HANAを迅速かつ確実に導入できます。

"FlexPod Datacenter for SAP解決策 with Cisco UCS Manager 4.0 and NetApp AFF A–Series-Design"

SLES 12 SP3およびRHEL 7.4を搭載したCisco UCS M5サーバ上のCisco ACIを搭載したFlexPod Datacenter for SAP解決策

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

このドキュメントでは、FlexPod 業界をリードするSoftware-Defined Networking解決策（SDN）であるCisco Application Centric Infrastructure（ACI）とネットアップAシリーズAFF アレイを活用した、シスコのコンピューティング製品とスイッチング製品で構成される、SAP HANAテーラードデータセンター統合オプションのアーキテクチャと導入手順について説明します。本ドキュメントでは、設計原則と、SAP HANAを導入するための詳細な設定手順について説明します。

"SLES 12 SP3およびRHEL 7.4を搭載したCisco UCS M5サーバ上のCisco ACIを搭載したFlexPod Datacenter for SAP解決策"

FlexPod AFF AシリーズとCisco UCS Manager 3.2を使用した、IPベースのストレージを備えたSAP解決策 用のDatacenter

ネットアップShailendra Mruthunjaya、Cisco Ralf Klahr、Cisco Marco Schoen

このドキュメントで詳述するリファレンスアーキテクチャでは、IPベースのストレージ解決策 の耐障害性、コスト上のメリット、導入のしやすさを強調しています。1つのインターフェイスで複数のプロトコルを処理できるストレージシステムは、真に配線が不要なアーキテクチャであるため、お客様が選択して投資を保護できます。解決策 は、拡張性に優れたSAP HANAワークロードをホストするよう設計されています。

"FlexPod AFF AシリーズとCisco UCS Manager 3.2を使用した、IPベースのストレージを備えたSAP解決策 用のDatacenter"

<xmt-block0>FlexPod</xmt-block> Datacenter for SAP<xmt-block1>解決策</xmt-block> Using FibreChannel SAN with Cisco UCS Manager 4.0 and NetApp<xmt-block2> ONTAP</xmt-block> 9.7

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

本ドキュメントでは、特にSAP HANA対応の第2世代Intel Xeonスケーラブルプロセッサを搭載した、NetApp AFF A400ストレージおよびCisco UCS Managerユニファイドソフトウェアリリース4.1(1)上で稼働するNetApp ONTAP 9.7を搭載したCiscoとNetApp FlexPod データセンターについて説明します。

FlexPod データセンターとNetApp ONTAP 9.7およびCisco UCSユニファイドソフトウェアリリース4.1(1)は、Cisco Unified Computing System（Cisco UCS）、Cisco Nexus 9000スイッチファミリー、MDS 9000マルチレイヤファブリックスイッチ、 およびONTAP 9.7ストレージOSを実行するNetApp AFF Aシリーズストレージアレイ。

"FlexPod Datacenter for SAP解決策 Using FibreChannel SAN with Cisco UCS Manager 4.0 and NetApp ONTAP 9.7"

FlexPod with SQLにSAPアプリケーションサーバを導入します

FlexPod は、IT部門の急速に変化するニーズに対応するように設計された、事前に検証および設計されたデータセンター解決策 です。Ciscoとネットアップは提携して、業界最高のコンピューティング、ネットワーク、ストレージコンポーネントを、データベース、エンタープライズリソースプランニング（ERP）、顧客関係管理（CRM）、Webアプリケーションなど、さまざまなエンタープライズワークロードの基盤として使用するFlexPod を提供しています。近年、ITアプリケーション、特にデータベースの統合に大きな関心が寄せられています。過去数年間で最も広く採用され、導入されているデータベースプラットフォームは、Microsoft SQL Serverです。SQL Serverデータベースは、データベーススプロールの影響を受けることが多く、サーバの利用率の低さ、ライセンスの不正確さ、セキュリティ上の懸念、管理上の懸念、膨大な運用コストなど、ITの課題につながっています。そのため、SQL Serverデータベースは、堅牢性、柔軟性、耐障害性に優れたプラットフォーム上での統合に適しています。このドキュメントでは、SQL Serverデータベースを導入および統合するためのFlexPod リファレンスアーキテクチャについて説明します。

"FlexPod with SQLにSAPアプリケーションサーバを導入します"

FlexPod Datacenter for SAP with Cisco ACI、Cisco UCS Manager 4.0、and NetApp AFF A–Series

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

本ドキュメントでは、FlexPod インフラにおけるSAP HANAテーラードデータセンター統合オプションのアーキテクチャと導入手順について説明します。このオプションは次の要素で構成されます。

- Cisco UCS Computing System（Cisco UCS）は、第2世代Intel Xeonスケーラブルプロセッサによってサポートされます。
- Cisco Application Centric Infrastructure（ACI）を活用したスイッチング製品。
- ネットアップAシリーズAFF アレイ：

"FlexPod Datacenter for SAP with Cisco ACI、Cisco UCS Manager 4.0、and NetApp AFF A–Series"

FlexPod Datacenter for SAP解決策 with Cisco ACI、Cisco UCS Manager 4.0、and NetApp AFF A–Series-Design

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

このドキュメントでは、SAP HANAテーラードデータセンター統合（TDI）環境を導入するための検証済みアプローチとして、Cisco ACI統合FlexPod 解決策 について説明します。この検証済みの設計では、SAP HANAを実装するためのガイドラインとフレームワークを、Ciscoとネットアップのベストプラクティスとともに提供します。

推奨される解決策 アーキテクチャは、Cisco Unified Computing System（Cisco UCS）上に構築され、ユニファイドソフトウェアリリースを使用して、次のコンポーネントを含むCisco UCSハードウェアプラットフォームをサポートします。

- Cisco UCS Bシリーズブレードサーバおよび Cisco UCS Cシリーズラックサーバは、Intel Optane Data Center Persistent Memory Module（DCPMM）オプションで構成できます
- Cisco UCS 6400シリーズファブリックインターコネクト
- Cisco Nexus 9000シリーズリーフ/スパインスイッチ
- ネットアップオールフラッシュシリーズストレージアレイ

また、このドキュメントでは、Red Hat Enterprise LinuxとSUSE Linux Enterprise Server for SAP HANAの両方について検証を行います。

"FlexPod Datacenter for SAP解決策 with Cisco ACI、Cisco UCS Manager 4.0、and NetApp AFF A–Series-Design"

FlexPod Datacenter for SAP解決策 with Cisco UCS Third-generation fabric and NetApp AFF A–Series

ネットアップShailendra Mruthunjaya、Cisco Ralf Klahr、Cisco Marco Schoen

本ドキュメントでは、第2世代Intel Xeonスケーラブルプロセッサでサポートされる Cisco UCSコンピューティングシステム（Cisco UCS）をベースにした、CiscoとNetApp FlexPod Datacenter for SAP HANAの導入方法について説明します。

Cisco UCS Manager（UCSM）4.0(4)は、現在のすべてのCisco UCSファブリックインターコネクトモデル（6200、6300、6324、6454）、2200/2300シリーズIOM、Cisco UCS Bシリーズブレード、およびCisco UCS Cシリーズラックフォームファクタサーバの統合サポートを提供します。Cisco UCSユニファイドソフトウェアリリース4.0（4D）とNetApp ONTAP 9.6を搭載したFlexPod データセンターは、Cisco UCS、Cisco Nexus 9000スイッチファミリー、NetApp AFF Aシリーズストレージアレイを基盤に構築された、設計済みのベストプラクティスに基づくデータセンターアーキテクチャです。

"FlexPod Datacenter for SAP解決策 with Cisco UCS Third-generation fabric and NetApp AFF A–Series"

FlexPod Datacenter for SAP解決策 with Cisco UCS Manager 4.0 and NetApp AFF A–Series-Design

Pramod Ramamurthy、Cisco Marco Schoen、ネットアップ

本ドキュメントでは、CiscoとNetApp FlexPod 解決策 について説明します。これは、SAP HANAテーラードデータセンター統合（TDI）環境を導入するための検証済みアプローチです。この検証済みの設計では、SAP HANAを実装するためのガイドラインとフレームワークを、Ciscoとネットアップのベストプラクティスとともに提供します。

FlexPod は業界をリードする統合インフラで、幅広いエンタープライズワークロードとユースケースに対応しています。この解決策 を使用すると、カスタマイズされたデータセンター統合モードのモデルを使用して、SAP HANAを迅速かつ確実に導入できます。

推奨される解決策 アーキテクチャは、Cisco Unified Computing System（Cisco UCS）上に構築され、ユニファイドソフトウェアリリースを使用して、次のコンポーネントを含むCisco UCSハードウェアプラットフォームをサポートします。

- Cisco UCS Bシリーズブレードサーバ、およびIntel Optane Data Center Persistent Memory Module（DCPMM）オプションで構成可能なCisco UCS Cシリーズラックサーバ
- Cisco UCS 6300シリーズファブリックインターコネクト
- Cisco Nexus 9000 シリーズスイッチ
- ネットアップオールフラッシュシリーズストレージアレイ

また、このドキュメントでは、Red Hat Enterprise LinuxとSUSE Linux Enterprise Server for SAP HANAの両方について検証を行います。

"FlexPod Datacenter for SAP解決策 with Cisco UCS Manager 4.0 and NetApp AFF A–Series-Design"

Oracle の場合

FlexPod Datacenter with Oracle 19C RAC Databases on Cisco UCS and NetApp AFF with NVMe over FiberChannel

Tushar Patel、Cisco Hardikkumar Vyas、Cisco

Cisco Validated Design（CVD）は、お客様の導入を促進および改善するために設計、テスト、文書化されたシステムとソリューションで構成されています。このCVDドキュメントでは、可用性の高いOracle RACデータベース環境を導入するための検証済みのアプローチであるCiscoとNetApp FlexPod 解決策 について説明します。Ciscoとネットアップは、Cisco UCS DatacenterラボのOLTP（Online Transactional Processing）やData Warehouseなど、さまざまなデータベースワークロードでリファレンスアーキテクチャを検証しました。このドキュメントでは、関連するコンポーネントのハードウェアとソフトウェアの構成と、さまざまなテストの結果を示します。また、Cisco UCSとネットアップストレージシステムを使用してNVMe/FC上にOracle RACデータベースを実装す

るためのフレームワークも提供しています。

"FlexPod Datacenter with Oracle 19C RAC Databases on Cisco UCS and NetApp AFF with NVMe over FiberChannel"

Cisco UCS および NetApp AFF A シリーズ上の FlexPod データセンターと Oracle RAC データベース

Tushar Patel、Cisco Hardikkumar Vyas、Cisco

Cisco Validated Designには、お客様の導入を促進および改善するために設計、テスト、文書化されたシステムとソリューションが含まれます。これらの設計には、お客様のビジネスニーズに対応するために開発されたソリューションポートフォリオに、幅広いテクノロジと製品が組み込まれています。Ciscoとネットアップは提携してFlexPod を提供しています。は、さまざまなワークロードの基盤として機能し、お客様の要件に基づいて効率的なアーキテクチャ設計を実現します。FlexPod 解決策 は、Ciscoとネットアップのテクノロジを共有クラウドインフラとして導入するための検証済みのアプローチです。

FlexPod Datacenter with NetApp All Flash AFF システムは、Ciscoとネットアップの優れたテクノロジを組み合わせた、エンタープライズアプリケーション向けの強力な統合プラットフォームを構築した統合インフラプラットフォームです。CiscoとネットアップはOracleと緊密に連携し、今日のビジネスで必要とされる、きわめて要件の厳しいトランザクションデータベースや応答時間重視のデータベースをサポートしています。

このCisco Validated Design（CVD）では、可用性の高いOracle RACデータベース環境を導入するための、Cisco UCSとNetApp All Flash AFF Storageを使用したFlexPod データセンターアーキテクチャのリファレンスについて説明します。このドキュメントでは、関連するコンポーネントのハードウェアとソフトウェアの構成と、さまざまなテストの結果を示します。また、Cisco UCSコンピューティングサーバ、Ciscoファブリックインターコネクトスイッチ、Cisco MDSスイッチ、Cisco Nexusスイッチ、NetApp AFF ストレージ、Oracle RACデータベースを使用した実装とベストプラクティスのガイダンスも提供します。

"Cisco UCS および NetApp AFF A シリーズ上の FlexPod データセンターと Oracle RAC データベース"

Oracle Linux 上の Oracle RAC を使用する FlexPod データセンター

ネットアップ、Tushar Patel、Cisco Niranjan Mohapatra、Cisco John Elliott

Cisco Unified Computing System（Cisco UCS）は、コンピューティング、ネットワーク、ストレージアクセス、仮想化を1つの統合システムに統合する次世代データセンタープラットフォームです。Cisco UCSは、ミッションクリティカルなデータベースワークロードのアーキテクチャに最適なプラットフォームです。Cisco UCSプラットフォーム、ネットアップストレージ、Oracle Real Application Cluster（RAC）アーキテクチャを組み合わせることで、導入時間の短縮、選択の柔軟性の向上、効率性の向上、リスクの軽減を実現し、ITの変革を加速できます。このCisco Validated Design（CVD）は、Oracle 12c RACデータベースを使用した、柔軟性、マルチテナント、ハイパフォーマンス、耐障害性に優れたFlexPod リファレンスアーキテクチャを強調しています。

ネットアップとCiscoが開発したFlexPod プラットフォームは、ストレージ、ネットワーク、サーバの各テクノロジを事前検証済みで提供する、柔軟性に優れた統合インフラ解決策 です。コンピューティングの全体的

なコストを削減しながら、ビジネスニーズへのITの即応性を高めるように設計されています。アップタイムを最大化し、リスクを最小限に抑えます。FlexPod コンポーネントは統合および標準化されているため、タイムリーで反復可能な一貫した導入を実現できます。各FlexPod 環境の電力、設置面積、使用可能な容量、パフォーマンス、コストを正確に計画できます。

FlexPod は最新のテクノロジを採用し、データセンターのワークロードを効率的に簡易化して、価値の提供方法を再定義します。

- NetApp FAS ハイブリッドアレイとFlash Poolフラッシュを組み合わせることで、特定のアプリケーションや環境に合わせて、回転式メディアにフラッシュを正確に割り当てることができます。
- 事前検証済みのプラットフォームを活用することで、業務の中断を最小限に抑え、ITの即応性を向上させ、導入時間を数カ月から数週間に短縮できます。
- 管理時間と総所有コスト（TCO）を50%削減
- データセンターのワークロードに対する、絶えず拡大するハードウェアパフォーマンスのニーズに対応、またはそれ以上のパフォーマンスを提供します。

"Oracle Linux 上の Oracle RAC を使用する FlexPod データセンター"

Cisco UCS および NetApp AFF A シリーズ上の FlexPod データセンターと Oracle RAC データベース

Tushar Patel、Cisco Hardikkumar Vyas、Cisco

FlexPod Datacenter with NetApp All Flash AFF システムは、Ciscoとネットアップの優れたテクノロジを組み合わせた、エンタープライズアプリケーション向けの強力な統合プラットフォームを構築した統合インフラプラットフォームです。CiscoとネットアップはOracleと緊密に連携し、今日のビジネスで必要とされる、きわめて要件の厳しいトランザクションデータベースや応答時間重視のデータベースをサポートしています。

このCisco Validated Design（CVD）では、可用性の高いOracle RACデータベース環境を導入するための、Cisco UCSとNetApp All Flash AFF Storageを使用したFlexPod データセンターアーキテクチャのリファレンスについて説明します。このドキュメントでは、関連するコンポーネントのハードウェアとソフトウェアの構成と、さまざまなテストの結果を示します。また、Cisco UCSコンピューティングサーバ、Ciscoファブリックインターコネクトスイッチ、Cisco MDSスイッチ、Cisco Nexusスイッチ、NetApp AFF ストレージ、Oracle RACデータベースを使用した実装とベストプラクティスのガイダンスも提供します。

"Cisco UCS および NetApp AFF A シリーズ上の FlexPod データセンターと Oracle RAC データベース"

Microsoft SQL Server の場合

FlexPod Datacenter for Microsoft SQL Server 2019 および VMware vSphere 6.7

ネットアップGopu Narasimha Reddy、Cisco Sanjeev Naldurgkar、Cisco Atul Bhalodia

このドキュメントでは、最新のハードウェアおよびソフトウェア製品を使用したFlexPod リファレンスアーキテクチャについて説明し、VMware ESXi仮想環境でMicrosoft SQL Server 2019データベースをホストする場合の導入に関する推奨事項を示します。また、この解決策 では、Cisco Workload Optimization Manager（CWOM）も

使用されています。CWOMは、SQLワークロードとインフラストラクチャの両方でリソースを最適かつ効率的に使用するための推奨事項を自動で提供します。

解決策 は、Cisco UCS Bシリーズブレードサーバ、Cisco UCS 6400ファブリックインターコネクト、Cisco Nexus 9000シリーズスイッチ、NetApp AFF シリーズストレージアレイなどのCisco UCSハードウェアプラットフォームをサポートするために、Cisco Unified Computing System（Cisco UCS）上に構築されています。

"FlexPod Datacenter for Microsoft SQL Server 2019 および VMware vSphere 6.7"

FlexPod Datacenter with Microsoft SQL Server 2016 and VMware vSphere 6.5 」を参照してください

ネットアップGopu Narasimha Reddy、Cisco Sanjeev Naldurgkar、Cisco David Arnette

このドキュメントでは、最新のハードウェア製品とソフトウェア製品を使用したFlexPod リファレンスアーキテクチャについて説明し、仮想環境にMicrosoft SQL Serverデータベースを導入する際の推奨構成について説明します。

推奨される解決策 アーキテクチャは、Cisco UCS Bシリーズブレードサーバ、Cisco UCS 6300ファブリックインターコネクト、Cisco Nexus 9000シリーズスイッチ、ネットアップオールフラッシュシリーズストレージアレイなど、Cisco UCSハードウェアプラットフォームをサポートするCisco Unified Computing System（Cisco UCS）上に構築されています。さらに、この解決策 にはVMware vSphere 6.5とvSphere 6.5が含まれており、ストレージ利用率を最適化し、プライベートクラウドを促進するための多くの新機能を提供します。

"FlexPod Datacenter with Microsoft SQL Server 2016 and VMware vSphere 6.5 」を参照してください"

VMwareおよびHyper-Vで実行されているLinux VM上のMicrosoft SQL Server 2017を搭載したFlexPod データセンター

ネットアップGopu Narasimha Reddy、Cisco Sanjeev Naldurgkar、Cisco Atul Bhalodia

このドキュメントでは、最新のハードウェアおよびソフトウェア製品を使用したFlexPod リファレンスアーキテクチャについて説明し、VMware ESXiおよびMicrosoft Windows Hyper-V仮想環境でMicrosoft SQL Serverデータベースをホストする場合の導入に関する推奨事項について説明します。また、MicrosoftによるSQL Server導入のサポートが有効になっています。

推奨される解決策 アーキテクチャは、Cisco Unified Computing System（Cisco UCS）上に構築され、ユニファイドソフトウェアリリース4.0.1cを使用して、Cisco UCS Bシリーズブレードサーバ、Cisco UCS 6300ファブリックインターコネクト、Cisco Nexus 9000シリーズスイッチ、NetApp AFF シリーズストレージアレイなどのCisco UCSハードウェアプラットフォームをサポートします。

"VMwareおよびHyper-Vで実行されているLinux VM上のMicrosoft SQL Server 2017を搭載したFlexPod データセンター"

VMwareおよびHyper-Vで実行されているLinux VM上のMicrosoft SQL Server 2017を搭載したFlexPod データセンター

ネットアップGopu Narasimha Reddy、Cisco Sanjeev Naldurgkar、Cisco Atul Bhalodia

このドキュメントでは、最新のハードウェアおよびソフトウェア製品を使用したFlexPod リファレンスアーキテクチャについて説明し、VMware ESXiおよびMicrosoft Windows Hyper-V仮想環境でMicrosoft SQL Serverデータベースをホストする場合の導入に関する推奨事項について説明します。また、MicrosoftによるSQL Server導入のサポートが有効になっています。

推奨される解決策 アーキテクチャは、Cisco UCS Bシリーズブレードサーバ、Cisco UCS 6300ファブリックインターコネクト、Cisco Nexus 9000シリーズスイッチ、NetApp AFF シリーズストレージアレイなど、Cisco UCSハードウェアプラットフォームをサポートするために、ユニファイドソフトウェアリリース4.0.1cを使用してCisco Unified Computing System（Cisco UCS）上に構築されています。

"VMwareおよびHyper-Vで実行されているLinux VM上のMicrosoft SQL Server 2017を搭載したFlexPod データセンター"

医療機関

ゲノム解析のための FlexPod

TR-4911 ：『 FlexPod Genomics 』

ネットアップ、 JayaKishore Esankula

医療や生命科学のゲノムよりも重要な医療分野がいくつかあり、ゲノム研究は医師や看護師にとって重要な臨床ツールとなりつつあります。ゲノムと医療画像およびデジタル病理学を組み合わせることで、患者の遺伝子が治療プロトコルによってどのように影響を受けるかを理解できます。医療におけるゲノム研究の成功は、データの大規模な相互運用性にますます左右されています。最終的な目標は、膨大な量の遺伝子データを理解し、臨床的に関連性のある相関と変異を特定して診断を改善し、精密医療を現実にすることです。ゲノム研究では、病気の発生源、疾患の進化、どの治療法や戦略が効果的かを理解することができます。明らかに、ゲノムには、予防、診断、治療にまたがる多くのメリットがあります。医療機関は、次のようないくつかの課題に取り組んでいます。

- ケア品質の向上
- 価値に基づく治療
- データの急増
- 精密医学
- パンダ
- ウェアラブル機器、リモートモニタリング、ケア
- サイバーセキュリティ

標準化された臨床経路と臨床プロトコルは、現代医学の重要な要素の 1 つです。標準化の重要な側面の 1 つは、医療記録だけでなくゲノムデータに対しても、医療提供者間の相互運用性です。医療機関は、個人のゲノムデータや関連する医療記録を患者が所有するのではなく、ゲノムデータの所有権を放棄するのでしょうか？

相互運用可能な患者データは、データの急増に対応する原動力の 1 つである精密医療を実現するための鍵となります。精密医療の目的は、健康維持、疾病予防、診断、治療ソリューションをより効果的かつ正確に行うことです。

データの増加率は急激に上昇しています。2021 年 2 月上旬に、米国の研究所では、 1 週間に約 8 、 000 系統の新型コロナウイルス感染症のシーケンスが確認されましたゲノム配列の数は 2021 年 4 月までに週 29,000 に増加しました。完全に配列されたヒトゲノムのサイズは約 125GB です。したがって、 1 週間に 29,000 個のゲノム配列を持つゲノムの保管データは、 1 年間で 180 ペタバイトを超えることになります。さまざまな国がゲノム疫学にリソースを投入し、ゲノム監視を改善し、世界的な健康問題の次の波に備えるよう取り組んでいます。

ゲノム研究のコスト削減により、遺伝子検査や研究はかつてないほどのスピードで進められています。3 つの PS は、コンピュータのパワー、データのプライバシー、医療のパーソナライズというターニングポイントにあります。2025 年には、研究者らは、ヒトゲノムの配列が 1 億～ 200 億個になると予測している。ゲノム研究を効果的かつ価値ある提案にするには、ゲノム機能が医療ワークフローのシームレスな一部である必要があります。患者の訪問時に、簡単にアクセスして実行可能である必要があります。患者の電子カルテデータを患

者のゲノムデータと統合することも同様に重要です。FlexPod のような最先端の統合インフラの出現により、組織はゲノム機能を医師、看護師、診療所のマネージャーの日常的なワークフローに導入できるようになりました。FlexPod プラットフォームの最新情報については、こちらを参照してください "FlexPod Datacenter with Cisco UCS X Series White Paper 』を参照してください"。

ゲノム研究の真の価値は、患者のゲノムデータに基づく精密な医療と個別化された治療計画です。過去に臨床医とデータサイエンティストの相乗効果が生まれたことはありません。ゲノム研究は、これまでの最新技術革新の恩恵を受けています。また、医療機関と業界の技術リーダーとの真のパートナーシップも享受しています。

学術医療センターやその他の医療および生命科学機関は、ゲノム科学の中心的な研究拠点（ COE ）を確立するために十分に活用されています。博士によるCharlie Gersbach 、 Dr.グレッグ・クローフォード博士Duke University の Tim E Reddy 氏は、「単純なバイナリスイッチでは遺伝子のオン / オフが行われていないことはわかっていますが、複数の遺伝子規制切り替えが連携して機能する結果です。また、「これらのゲノムの部分は、いずれも独立して機能しないと判断しました。ゲノムは非常に複雑なウェブで、進化してきました」（ "参照（ Ref ）"）。

ネットアップと Cisco は、 10 年以上にわたって FlexPod プラットフォームをさらに強化してきました。すべてのお客様からのフィードバックは、 FlexPod のバリューストリームと機能セットに耳を傾け、評価し、結び付けられます。この継続的なフィードバック、コラボレーション、改善、お祝いのループは、 FlexPod を信頼できる統合インフラストラクチャプラットフォームとして世界中で差別化します。シンプル化され、一から設計されたこのプラットフォームは、医療機関にとって最も信頼性が高く、堅牢で汎用性が高く、即応性に優れたプラットフォームです。

適用範囲

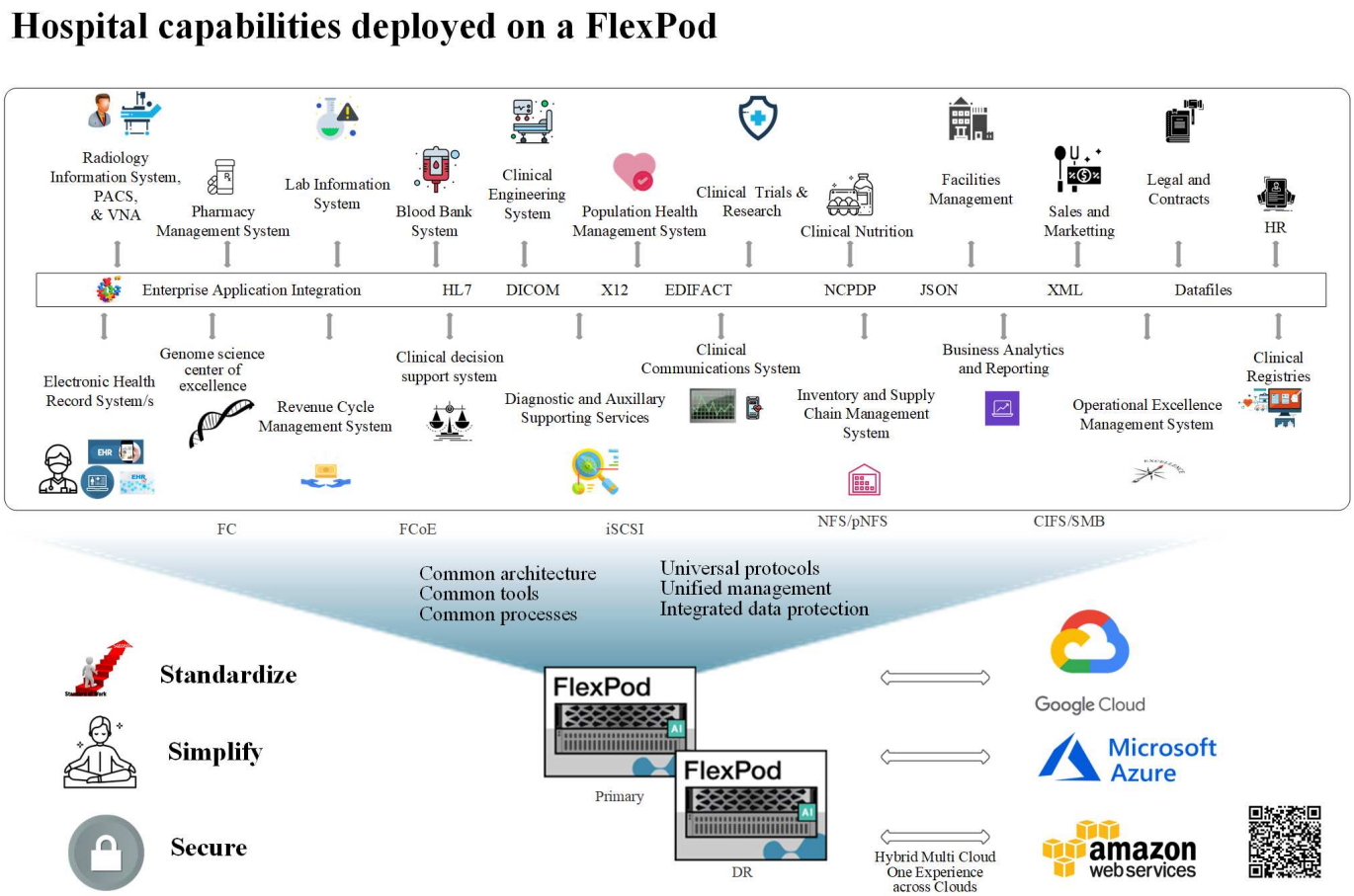
FlexPod コンバージドインフラプラットフォームを使用すると、医療機関は 1 つ以上のゲノム関連ワークロードと、他の臨床 / 非臨床的な医療アプリケーションをホストできます。このテクニカルレポートでは、FlexPod プラットフォームの検証時に GATK と呼ばれる、オープンソースの業界標準ゲノムツールを使用しています。ただし、ゲノム解析や GATK について詳しくは、このドキュメントでは扱いません。

対象者

本ドキュメントは、医療業界の技術リーダー、 Cisco とネットアップのパートナーソリューションエンジニア、およびプロフェッショナルサービス担当者を対象としています。本ドキュメントは、コンピューティングとストレージのサイジングの概念に加え、医療の脅威、医療セキュリティ、医療 IT システム、 Cisco UCS 、ネットアップストレージシステムに関する技術的な知識があることを前提としています。

FlexPod に導入された病院機能

一般的な病院には IT システムが多様化しています。このようなシステムの大半はベンダーから購入されますが、社内の病院システムによって構築されるものはほとんどありません。そのため、病院システムはデータセンターの多様なインフラ環境を管理する必要があります。病院がシステムを FlexPod などの統合インフラプラットフォームに統合すれば、データセンターの運用を標準化できます。FlexPod を使用すると、医療機関は臨床システムと非臨床システムを同じプラットフォームに実装できるため、データセンターの運用を統合できます。



"次は、ゲノムワークロードを FlexPod に導入するメリットです。"

ゲノムワークロードを **FlexPod** に導入するメリット

"前へ：はじめに。"

このセクションでは、 FlexPod コンバージドインフラプラットフォームでゲノミクスワークロードを実行する利点の概要を説明します。では、病院の機能について簡単に説明しましょう。次のビジネスアーキテクチャビューは、ハイブリッドクラウド対応の FlexPod コンバージドインフラストラクチャプラットフォームに導入された病院の機能を示しています。

- * 医療でサイロ化を避ける。 * 医療のサイロ化は非常に大きな懸念事項です。多くの場合、部門は選択したものではなく、進化によって組織的に孤立した独自のハードウェアとソフトウェアのセットにサイロ化しています。放射線科、心臓病、 EHR 、ゲノム解析など 分析、収益サイクル、その他の部門は、個々の専用ソフトウェアとハードウェアで構成されます。医療機関では、ハードウェアとソフトウェアの資産を管理するための IT プロフェッショナルが限られています。このような転換点は、非常に多様なハードウェアとソフトウェアを管理することが求められている場合に生じます。ベンダーによって医療機関にもたらされた矛盾する一連のプロセスによって、不均質性が悪化します。
- * 小さい始め、育つ。 * GATK の用具キットは CPU の実行のために調整される FlexPod のような最もよいスイートルームのプラットホーム。FlexPod を使用すると、ネットワーク、コンピューティング、ストレージの拡張性を個別に拡張できます。ゲノム機能と環境の拡大に合わせて小規模な構成から始め、拡張できます。医療機関は、ゲノムワークロードを実行するために特化したプラットフォームに投資する必要がありません。代わりに、 FlexPod のような汎用性の高いプラットフォームを活用して、同じプラットフ

ォーム上でゲノミクスとゲノム以外のワークロードを実行できます。たとえば、小児部門がゲノム機能の実装を検討している場合、 IT リーダーは既存の FlexPod インスタンスでコンピューティング、ストレージ、ネットワークをプロビジョニングできます。ゲノムビジネスユニットの成長に伴い、医療機関は必要に応じて FlexPod プラットフォームを拡張できます。

- * 単一のコントロールパネルと比類のない柔軟性。 * Cisco Intersight は、アプリケーションとインフラストラクチャをブリッジすることで、 IT 運用を大幅に簡易化し、ベアメタルサーバやハイパーバイザからサーバレスアプリケーションまでの可視化と管理を実現し、コストを削減し、リスクを軽減します。このユニファイド SaaS プラットフォームは、オープン API 設計を採用しており、サードパーティのプラットフォームやツールとネイティブに統合されています。さらに、モバイルアプリを使用して、データセンター運用チームからオンサイトまたは場所を問わず管理を行うことができます。

  ユーザは、 Intersight を管理プラットフォームとして活用することで、目に見える形での価値をすばやく引き出すことができます。多くの日常的な手作業の自動化を可能にする Intersight は、エラーを解消し、日常業務を簡易化します。さらに、 Intersight の高度なサポート機能により、導入者は問題に先手を打つことができ、問題の解決を加速できます。企業がアプリケーションインフラに費やす時間とコストを大幅に削減し、コアビジネスの開発にかける時間を増やしています。

  Intersight の管理と FlexPod の拡張性に優れたアーキテクチャを活用することで、複数のゲノムワークロードを単一の FlexPod プラットフォームで実行できるようになり、利用率が向上し、総所有コスト（ TCO ）が削減されます。FlexPod では、ネットアップの小規模な FlexPod Express から始めて、大規模な FlexPod データセンター実装まで拡張できるため、柔軟なサイジングが可能です。Cisco Intersight に組み込まれているロールベースのアクセス制御機能により、医療機関は堅牢なアクセス制御メカニズムを実装して、個別のインフラスタックを必要としないようにすることができます。医療機関内の複数のビジネスユニットが、ゲノム研究を主要な中核コンピテンシーとして活用できます。

  最終的に FlexPod は、 IT 運用を簡易化し、運用コストを削減します。 IT インフラストラクチャ管理者は、臨床医の革新を支援するタスクに集中できるため、常に最新の状態に維持することはできません。

- * 検証済みの設計と保証された成果。 * FlexPod の設計および導入ガイドは、再現可能であることが検証されており、 FlexPod を確実に導入するために必要な包括的な構成の詳細と業界のベストプラクティスが記載されています。Cisco とネットアップの検証済み設計ガイド、導入ガイド、アーキテクチャを活用すれば、医療機関やライフサイエンス部門が、検証済みで信頼性の高いプラットフォームを最初から導入する際に推測に頼ることがなくなります。FlexPod を使用すると、導入時間を短縮し、コスト、複雑さ、リスクを軽減できます。FlexPod 検証済みの設計と導入ガイドでは、さまざまなゲノムワークロードに最適なプラットフォームとして FlexPod を確立しています。

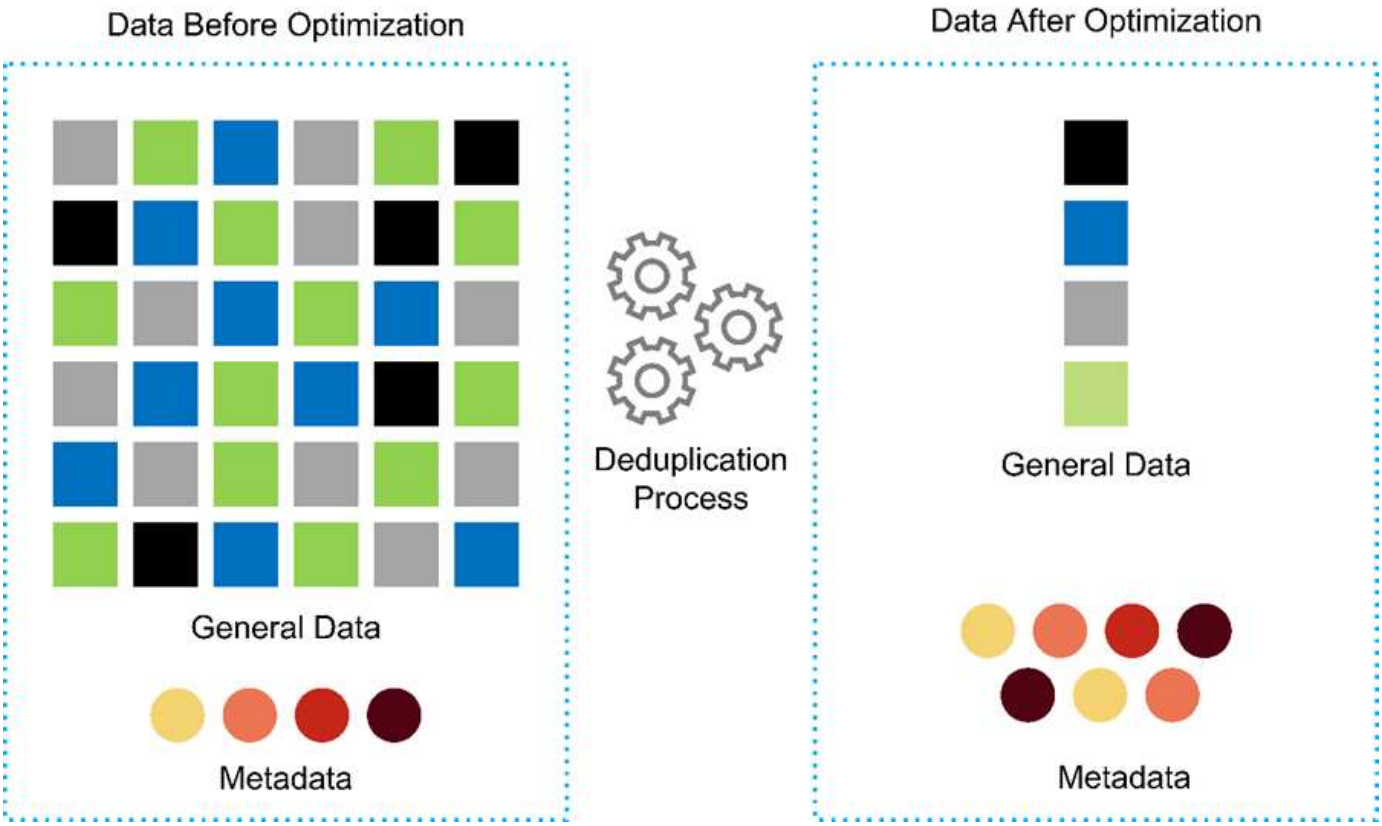
- * 革新性と俊敏性。 * FlexPod は Epic 、 Cerner 、 Meditech 、 Agfa 、 GE 、 Philips などの画像処理システムなどの EHR によって理想的なプラットフォームとして推奨されています。詳細については、を参照してください "EPIC 名誉の転がる" ターゲットとなるプラットフォームアーキテクチャについては、 Epic userweb を参照してください。ゲノム解析の実行 "FlexPod" 医療機関は、即応性を備えた革新的なビジネスを継続できます。FlexPod を導入することで、組織の変化を自然に実現できます。医療機関が FlexPod プラットフォームを標準化すると、 IT エキスパートは時間、労力、リソースをプロビジョニングしてイノベーションを推進できるようになり、エコシステムのニーズに合わせた即応性が実現します。

- * データの制約を解放。 * ONTAP コンバージドインフラプラットフォームと NetApp FlexPod ストレージシステムを使用すると、ゲノムデータを 1 つのプラットフォームから幅広いプロトコルで大規模に利用およびアクセスできます。FlexPod と NetApp ONTAP は、シンプルでわかりやすく、強力なハイブリッドクラウドプラットフォームです。NetApp ONTAP を基盤とするデータファブリックは、サイト間、物理的な境界を超え、アプリケーション間でデータを結び付けます。データファブリックは、 Data-Centric の世界におけるデータ主体の企業向けに構築されています。データは複数の場所に作成されて使用されるため、多くの場合、他の場所、アプリケーション、インフラとの利用や共有が必要になります。そのため、一貫性のある統合された管理方法が必要です。FlexPod を導入することで、 IT チームの管理が容易になり、増え続ける IT の複雑さが軽減されます。

- * セキュアマルチテナンシー。 * FlexPod は FIPS 140-2 準拠の暗号モジュールを使用しているため、セキ

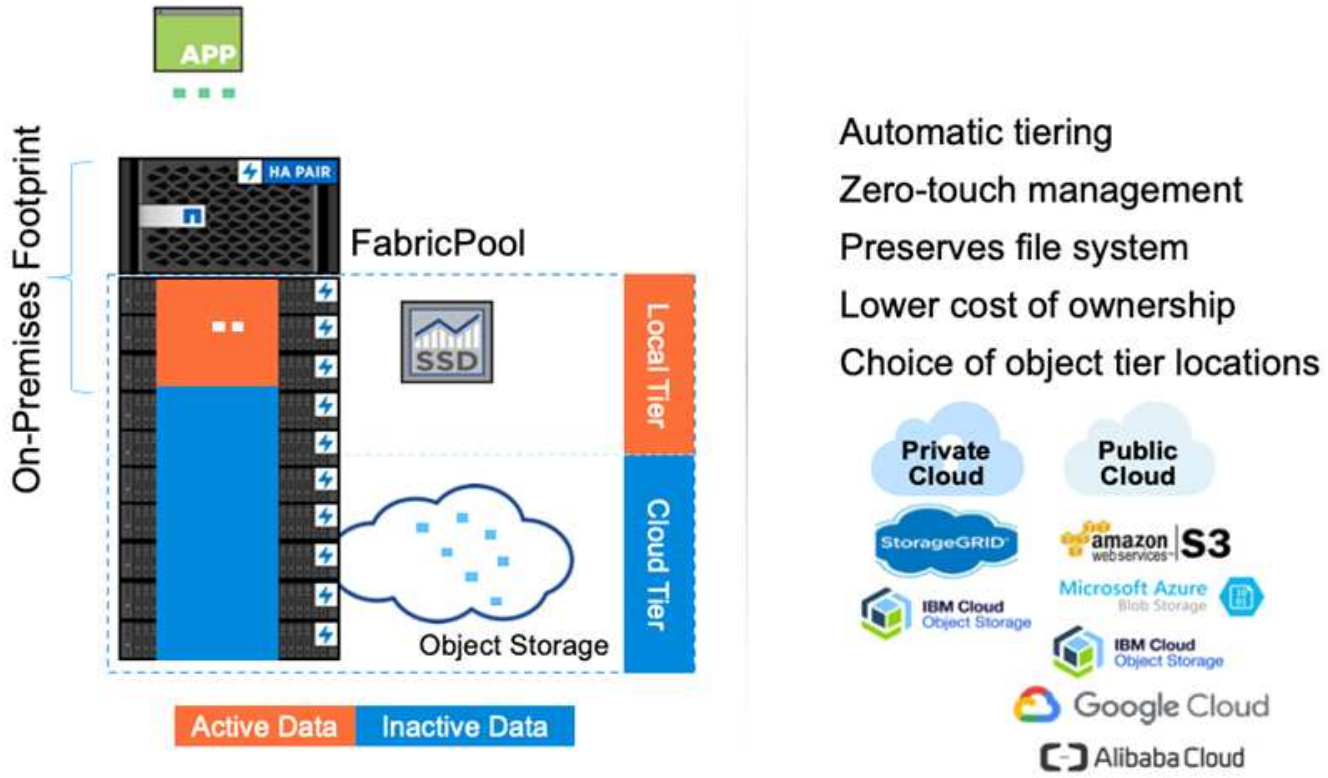
ュリティを後からではなく基本要素として実装できます。FlexPod を使用すると、プラットフォームの規模に関係なく、単一のコンバージドインフラプラットフォームからセキュアマルチテナンシーを実装できます。マルチテナンシーと QoS で FlexPod を保護することで、ワークロードの分離と利用率の最大化を実現します。これにより、使用率の低い可能性のある特殊なプラットフォームに設備が固定され、管理に特殊なスキルセットが必要になるのを回避できます。

- * ストレージ効率化 * ゲノミクスには、基盤となるストレージに業界をリードするストレージ効率化機能が必要です。重複排除（インラインおよびオンデマンド）、データ圧縮、データコンパクション（など）などのネットアップの Storage Efficiency 機能を使用すると、ストレージコストを削減できます "参照（ Ref ）"）。ネットアップの重複排除機能は、 FlexVol ボリューム内でブロックレベルの重複排除を実行します。重複排除機能は、基本的に、重複ブロックを削除して、 FlexVol ボリューム内で一意のブロックのみを保存します。重複排除は非常にきめ細かな方法で機能し、 FlexVol ボリュームのアクティブファイルシステムで機能します。次の図に、ネットアップの重複排除機能の概要を示します。重複排除機能はアプリケーションに対して透過的です。したがって、ネットアップシステムを使用するすべてのアプリケーションのデータに対して重複排除を実行できます。ボリューム重複排除はインラインプロセスおよびバックグラウンドプロセスとして実行できます。CLI 、 NetApp ONTAP System Manager 、または NetApp Active IQ Unified Manager から自動で実行、スケジュール設定、または手動で実行するように設定することができます。



- * ゲノムの相互運用性を実現。 * ONTAP FlexCache は、ファイル配信を簡素化し、 WAN のレイテンシを低減し、 WAN 帯域幅コスト（ "参照（ Ref ）"）。ゲノム変異の同定およびアノテーションにおける重要な活動の 1 つに、臨床医間のコラボレーションがあります。ONTAP FlexCache テクノロジーは、コラボレーションする臨床医が異なる地域にいる場合でも、データのスループットを向上させます。一般的な * 。 BAM ファイルのサイズ（ 1 GB ～ 100 GB ）を考えると、基盤となるプラットフォームが異なる地域の臨床医がファイルを使用できるようにすることが重要です。FlexPod と ONTAP FlexCache を併用することで、ゲノムデータとアプリケーションをマルチサイトに対応できます。その結果、世界中に分散している研究者が、低レイテンシと高スループットを実現しながらシームレスに連携できるようになります。ゲノム研究アプリケーションをマルチサイト環境で実行している医療機関は、データファブリックを使用してスケールアウトを実施し、管理性とコスト、スピードのバランスを取ることができます。

- * ストレージ・プラットフォームをインテリジェントに使用。 * FlexPod と ONTAP の自動階層化機能とネットアップのファブリック・プール・テクノロジーにより、データ管理を簡素化します。FabricPool は、パフォーマンス、効率、セキュリティ、保護を犠牲にすることなくストレージコストを削減します。FabricPool は、エンタープライズアプリケーションに対して透過的であり、アプリケーションインフラを再構築することなくストレージの TCO を削減することで、クラウドの効率性を活用します。FlexPod は、 FabricPool のストレージ階層化機能を活用して、 ONTAP フラッシュストレージをより効率的に使用できます。詳細については、を参照してください "FlexPod with FabricPool の略"。次の図は、 FabricPool とその利点の概要を示しています。



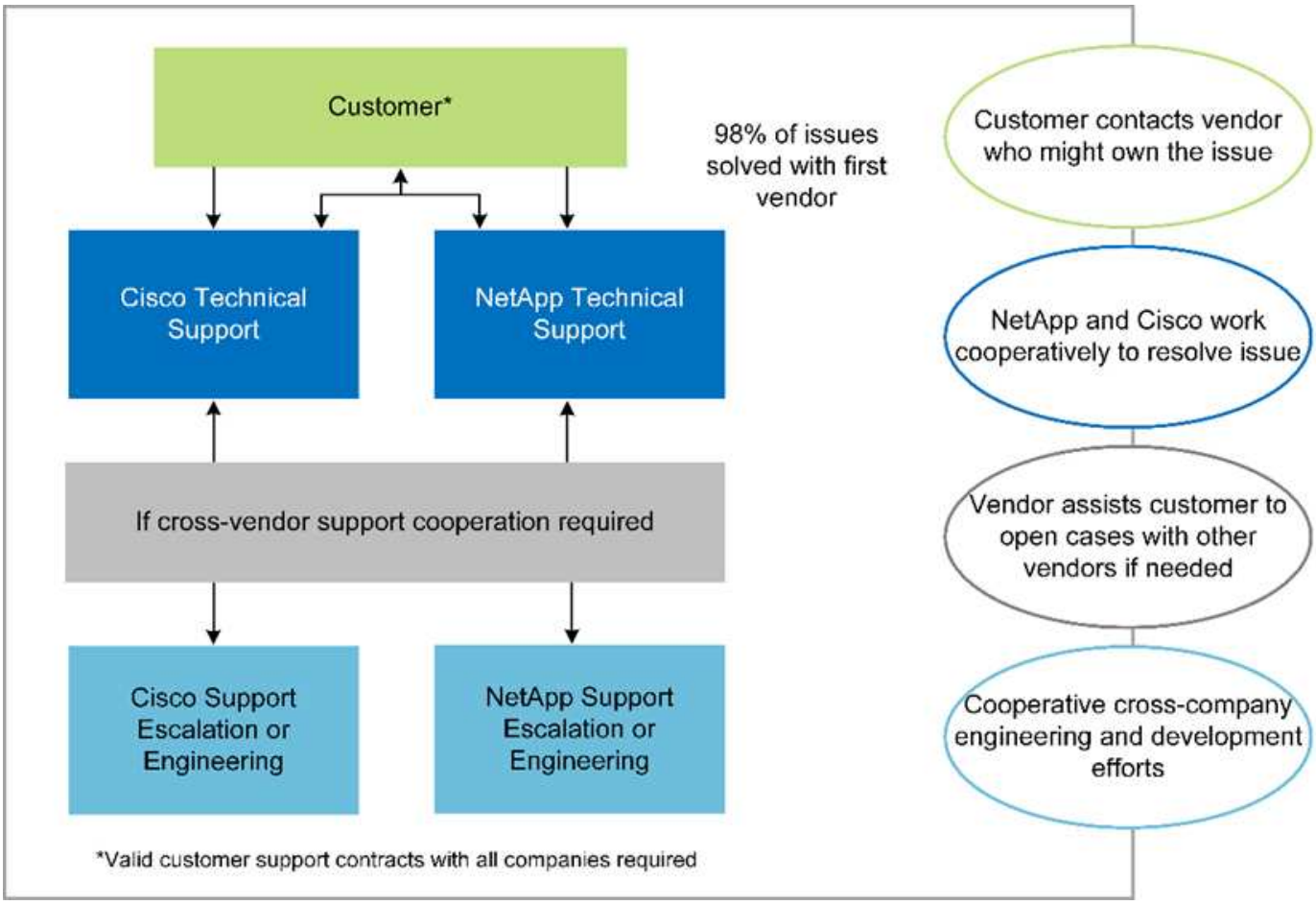
- * バリアント分析とアノテーションの高速化。 * FlexPod プラットフォームの導入と運用開始にかかる時間が短縮されます。FlexPod プラットフォームでは、データを低レイテンシとスループットで大規模に利用できるようにすることで、医療従事者によるコラボレーションが可能になります。相互運用性が向上することで、イノベーションが医療機関は、ゲノムワークロードと非ゲノムワークロードを並行して実行できるため、ゲノム解析の開始に特化したプラットフォームを必要としません。

  FlexPod ONTAP では、ストレージプラットフォームに最新の機能を定期的に追加しています。FlexPod データセンターは、 FC-NVMe を導入するための最適な共有インフラ基盤であり、必要なアプリケーションにハイパフォーマンスなストレージアクセスを提供します。FC-NVMe は進化し、高可用性、マルチパス、およびオペレーティングシステムの追加サポートが組み込まれています。 FlexPod は、このような機能をサポートするために必要な拡張性と信頼性を備えたプラットフォームに最適です。エンドツーエンド NVMe で I/O を高速化した ONTAP により、ゲノム解析を高速化（ "参照（ Ref ）"）。

  ゲノム配列データは大きなファイルサイズを生成します。これらのファイルをバリアント分析装置で使用できるようにすることで、サンプルの収集からバリアントの注釈までにかかる総時間を短縮することが重要です。ストレージアクセスおよびデータ転送プロトコルとして使用される NVMe （ Non-Volatile Memory Express ）は、かつてないレベルのスループットと最速の応答時間を実現します。FlexPod は、PCI Express Bus （ PCIe ； PCI Express バス）を介してフラッシュストレージにアクセスしながら、NVMe プロトコルを導入します。PCIe により、数万のコマンドキューの実装が可能になり、並列化とス

ループットが向上します。ストレージからメモリまで 1 つのプロトコルでデータアクセスが高速化されます。

- * 臨床研究の俊敏性を徹底的に高めています。 * 柔軟で拡張可能なストレージ容量とパフォーマンスにより、医療研究機関は柔軟でジャストインタイム（ JIT ）方式で環境を最適化できます。コンピューティングインフラとネットワークインフラのストレージを分離 FlexPod することで、システムを停止することなくスケールアップとスケールアウトが可能です。Cisco Intersight を使用すると、 FlexPod プラットフォームの管理に組み込みの自動ワークフローとカスタムの自動ワークフローの両方を利用できます。Cisco Intersight のワークフローにより、医療機関はアプリケーションのライフサイクル管理時間を短縮できます。学術医療センターでは、患者データを匿名化して研究インフォマティクスやセンターで高品質な情報を提供する必要がある場合、 IT 部門は Cisco Intersight FlexPod のワークフローを活用して、セキュアなデータバックアップ、クローニング、リストアを数時間ではなく数秒で実行できます。NetApp Trident と Kubernetes を使用すると、 IT 部門は新しいデータサイエンティストをプロビジョニングし、臨床データをわずか数分でモデル開発に利用できます。しかも数秒で完了することもあります。
- * ゲノムデータを保護。 * NetApp SnapLock は、消去や書き換えが不可能な状態でファイルを保存し、コミットできる特殊な用途に対応しています。FlexVol ボリュームに保存されているユーザーの本番データは、 NetApp SnapMirror または SnapVault テクノロジを使用して、 SnapLock ボリュームにミラーリングまたは保存できます。SnapLock ボリューム内のファイル、ボリューム自体、およびホストアグリゲートは、保持期間が終了するまで削除できません。ONTAP FPolicy ソフトウェアを使用している組織では、特定の拡張子のファイルに対する処理を禁止することで、ランサムウェア攻撃を防止できます。FPolicy イベントは、特定のファイル操作に対してトリガーできます。イベントはポリシーに関連付けられており、ポリシーは使用する必要があるエンジンを呼び出します。ポリシーにはランサムウェアを含む可能性のある一連のファイル拡張子を設定できます。拡張子が許可されていないファイルで許可されていない操作を実行しようとすると、 FPolicy によりその操作が実行されなくなります。 ("参照（ Ref ）")。
- * FlexPod 共同サポート * ネットアップと Cisco は、 FlexPod コンバージドインフラに固有のサポート要件を満たす、拡張性と柔軟性に優れた強力なサポートモデルである FlexPod 共同サポートを確立しました。このモデルでは、ネットアップと Cisco が提供する経験、リソース、およびテクニカルサポートの専門知識を組み合わせて、問題の発生場所に関係なく、 FlexPod のサポート問題を特定して解決するための合理的なプロセスを提供します。次の図に、 FlexPod 共同サポートモデルの概要を示します。お客様は、問題を所有する可能性のあるベンダーに連絡し、 Cisco とネットアップは協力して解決するように依頼します。Cisco とネットアップには、複数の企業にわたるエンジニアリングチームと開発チームがあり、これらのチームが協力して問題を解決します。このサポートモデルにより、翻訳中の情報の損失を削減し、信頼性を高め、ダウンタイムを削減できます。

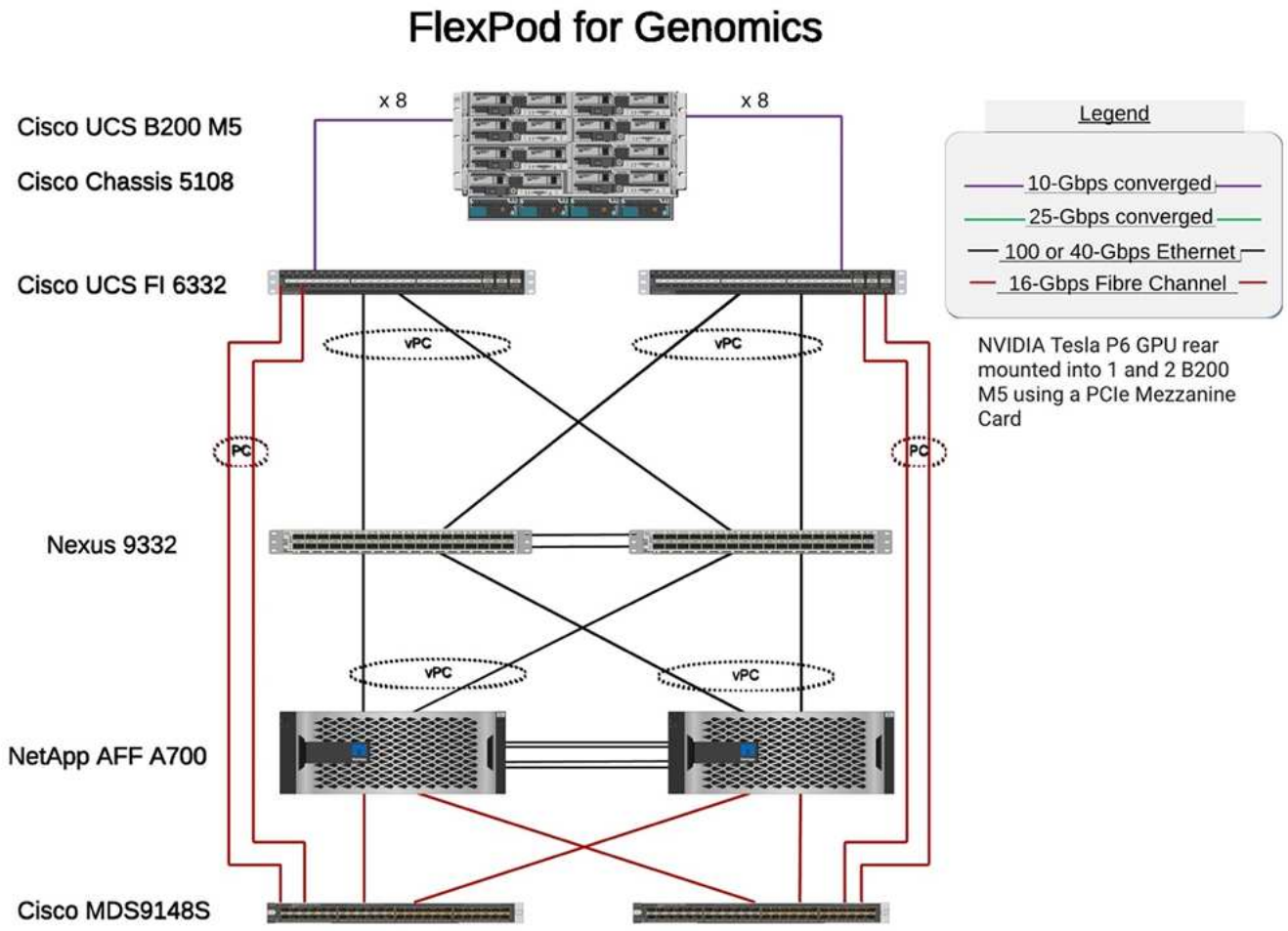


"次の例は、解決策インフラのハードウェアとソフトウェアのコンポーネントです。"

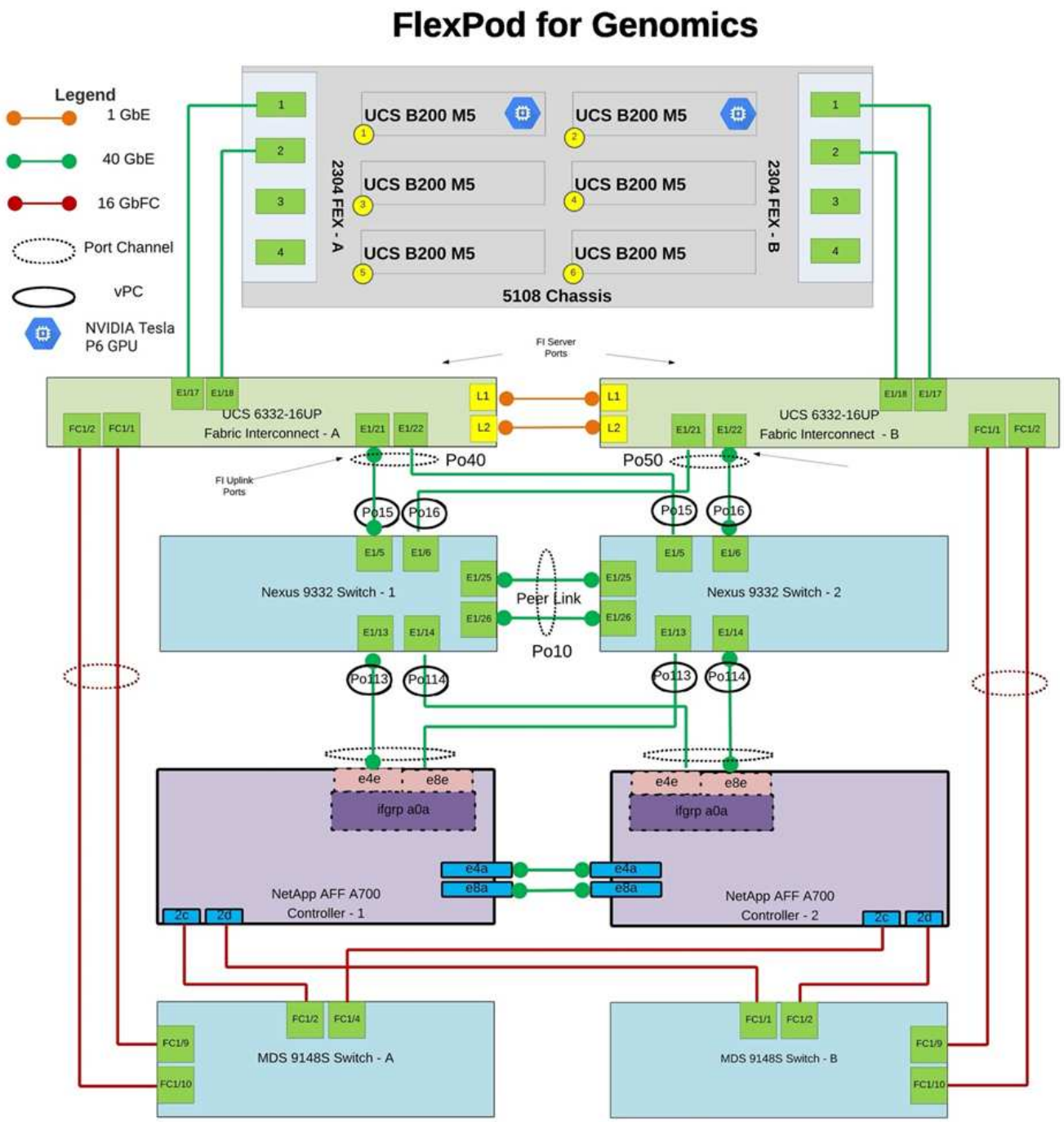
解決策インフラのハードウェアコンポーネントとソフトウェアコンポーネント

"従来：ゲノムワークロードを FlexPod に導入するメリット"

次の図に、 GATK の設定と検証に使用される FlexPod システムを示します。使用しました "FlexPod データセンターと VMware vSphere 7.0 および NetApp ONTAP 9.7 Cisco Validated Design （ CVD ）" セットアッププロセスの実行中です。



次の図は、 FlexPod のケーブル配線の詳細を示しています。



次の表に、 FlexPod で有効にする GATK テスト中に使用されるハードウェアコンポーネントを示します。はこちらです "NetApp Interoperability Matrix Tool で確認できます" （ IMT ）および "シスコハードウェア互換性リスト（ HCL ）"。

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
コンピューティング	Cisco UCS 5108 シャーシ	1 または 2	
	Cisco UCS ブレードサーバ	B200 M5 × 6	それぞれに、 20 コア以上、 2.7GHz 、および 128-384GB RAM を 2 個搭載しています

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
	Cisco UCS 仮想インターフェイスカード（ VIC ）	Cisco UCS 1440	を参照してください
	Cisco UCS ファブリックインターコネクト × 2	6332	-
ネットワーク	Cisco Nexus スイッチ	Cisco Nexus 9332 × 2	-
ストレージネットワーク	SMB / CIFS 、 NFS 、または iSCSI プロトコル経由のストレージアクセス用の IP ネットワーク	上記と同じネットワークスイッチ	-
	FC 経由のストレージアクセス	Cisco MDS 9148S × 2	-
ストレージ	NetApp AFF A700 オールフラッシュストレージシステム	1 クラスタ	2 ノードクラスタ
	ディスクシェルフ	DS224C または NS224 ディスクシェルフ × 1	24 本のドライブをフル装備
	SSD の場合	容量が 24 、 2TB 以上	-

この表は、インフラストラクチャソフトウェアを示しています。

ソフトウェア	製品ファミリー	バージョンまたはリリース	詳細
様々	Linux の場合	RHEL 8.3	-
	Windows の場合	Windows Server 2012 R2（ 64 ビット）	-
	NetApp ONTAP	ONTAP 9.8 以降	-
	Cisco UCS ファブリックインターコネクト	Cisco UCS Manager 4.1 以降	-
	Cisco Ethernet 3000 または 9000 シリーズスイッチ	9000 シリーズの場合、7.0(3) i7(7) 以降（ 3000 シリーズ用）、 9.2(4) 以降	-
	Cisco FC ： Cisco MDS 9132T	8.4(1a) 以降	-
	ハイパーバイザー	VMware vSphere ESXi 7.0	-
ストレージ	ハイパーバイザー管理システム	VMware vCenter Server 7.0 （ vCSA ）以降	-
ネットワーク	NetApp Virtual Storage Console （ VSC ）	VSC 9.7 以降	-
	NetApp SnapCenter	SnapCenter 4.3 以降	-

ソフトウェア	製品ファミリー	バージョンまたはリリース	詳細
	Cisco UCS Manager の略	4.1 （ 3c ）以降	
ハイパーバイザー	ESXi		
管理	ハイパーバイザー管理システム VMware vCenter Server 7.0 （ vCSA ）以降		
	NetApp Virtual Storage Console （ VSC ）	VSC 9.7 以降	
	NetApp SnapCenter	SnapCenter 4.3 以降	
	Cisco UCS Manager の略	4.1 （ 3c ）以降	

"次は、 Genomics - GATK のセットアップと実行です。"

ゲノム - GATK のセットアップと実行

"以前：解決策インフラのハードウェアコンポーネントとソフトウェアコンポーネント。"

国立ヒトゲノム研究所によると "NHGRI") 、「ゲノムとは、人の遺伝子 (ゲノム) のすべての研究であり、これらの遺伝子相互作用や人の環境との相互作用を含みます。」

に従って "NHGRI"「デオキシリボヌクリク酸（ DNA ）は、ほぼすべての生物の活動を開発し、誘導するために必要な指示を含む化学化合物です。DNA 分子は、二重らせんと呼ばれる 2 つのツイスト、ペアストランドで構成されています。」 「生物の DNA の完全なセットは、ゲノムと呼ばれています。」

配列決定は DNA の鎖の塩基の正確な順序を決定するプロセスである。現在使用されている最も一般的なシーケンスタイプの 1 つは、合成による順序付けと呼ばれます。この技術では、蛍光信号の放射を使用して塩基を並べます。研究者は DNA シーケンシングを使用して、遺伝子変異や、人がまだ初期段階にある間に疾患の発症または進行に関与する可能性のある突然変異を検索することができる。

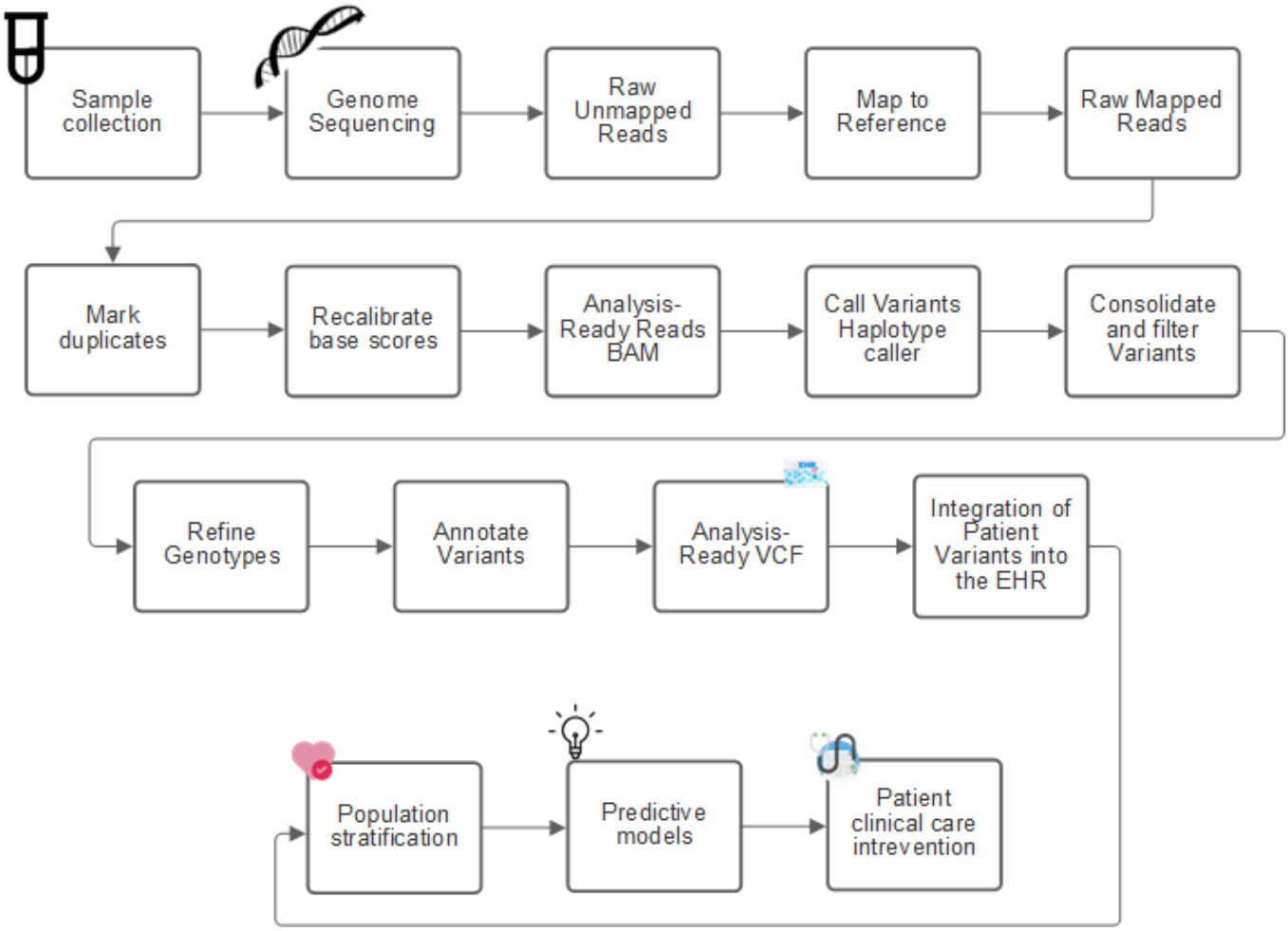
サンプルからバリアントの識別、注釈、および予測まで

ゲノム解析の概要は、以下のステップに分類できます。これは完全なリストではありません。

1. サンプル収集。
2. "ゲノム配列決定" シーケンサーを使用して、 raw データを生成します。
3. 前処理中です例： "重複排除" を使用します "Picard"。
4. ゲノム解析：
   a. 参照ゲノムへのマッピング。
   b. "バリアント" GATK などのツールを使用して、一般的に識別とアノテーションを実行します。
5. 電子カルテ（ EHR ）システムへの統合
6. "人口階層化" 地理的位置と民族的背景を越えた遺伝的変動の同定。
7. "予測モデル" 有意なシングルヌクレオチド多形症を用いている。

8. "検証"。

次の図に、サンプリングからバリアントの識別、注釈、および予測までのプロセスを示します。



ヒトゲノム計画は 2003 年 4 月に完成し、このプロジェクトは、パブリックドメインで利用可能なヒトゲノム配列を非常に高品質でシミュレーションしました。このリファレンスゲノムは、ゲノム機能の研究開発で爆発的に増加しました。事実上すべての人間の病気にその人間の遺伝子の署名がある。最近まで、医師は、単一遺伝子の変化によって発生した特定の相続パターンによって引き起こされる、鎌状赤血球貧血などの出生異常を予測し、判定するために遺伝子を利用していた。ヒトゲノムプロジェクトで収集された膨大なデータがゲノム機能の最新状態に登場しました。

ゲノミクスには幅広いメリットがあります。ヘルスケアおよびライフサイエンス分野のメリットを以下に示します。

- 治療時点でのより良い診断
- 予後が良好である
- 精密医学
- パーソナライズされた治療計画
- 疾患モニタリングの向上
- 有害事象の減少

- 治療へのアクセスが向上しました
- 疾患モニタリングの改善
- 有効な臨床試験への参加と、遺伝子型に基づく臨床試験の患者の選択の向上。

ゲノミクスは a "4 つのヘッドを持つ獣、" 取得、ストレージ、分散、分析という、データセットのライフサイクル全体にわたるコンピューティングのニーズがあるためです。

ゲノム解析ツールキット（ **GATK** ）

GATK は、でデータサイエンスプラットフォームとして開発されました "ブロードインスティテュート" 。GATK は、ゲノム解析を可能にする一連のオープンソース・ツールで、特に変異検出、同定、アノテーション、ジェノタイピングなどを行います。GATK の利点の 1 つは、ツールやコマンドのセットを連鎖させて、完全なワークフローを形成できることです。ブロード研究所が取り組む主な課題は、次のとおりです。

- 病気の根本原因と生物学的メカニズムを理解する。
- 疾患の基礎原因で作用する治療的介入を特定する。
- 変異体から人間の生理学的な機能まで、視線を理解します。
- 標準とポリシーを作成します "フレームワーク" ゲノムデータの表示、保存、分析、セキュリティなどを行います。
- 相互運用可能なゲノム集約データベース（ gnomad ）を標準化し、社会化します。
- ゲノムを用いたモニタリング、診断、および患者の治療をより正確に行うことができます。
- 症状が現れる前に疾患を適切に予測するツールの導入を支援します。
- 生物医学における最も困難で最も重要な問題に対処するために、学際的な協力者のコミュニティを作成し、強化します。

GATK と The Broad Institute によると、ゲノム配列決定は病理学ラボでプロトコルとして扱われるべきです。どのような作業でも、サンプルや実験全体でよく文書化され、最適化され、再現性があり、一貫性が保たれます。以下は、ブロード研究所が推奨する一連の手順です。詳細については、を参照してください "GATK の Web サイト"。

FlexPod セットアップ

ゲノミクスワークロードの検証には、 FlexPod インフラプラットフォームのスクラッチからのセットアップが含まれています。FlexPod プラットフォームは高可用性を備えており、個別に拡張できます。たとえば、ネットワーク、ストレージ、コンピューティングを個別に拡張できます。FlexPod 環境をセットアップするためのリファレンスアーキテクチャドキュメントとして、次のシスコ検証済み設計ガイドを使用しました。 "FlexPod Datacenter with VMware vSphere 7.0 and NetApp ONTAP 9.7 』を参照してください"。次の FlexPod プラットフォームのセットアップのハイライトを参照してください。

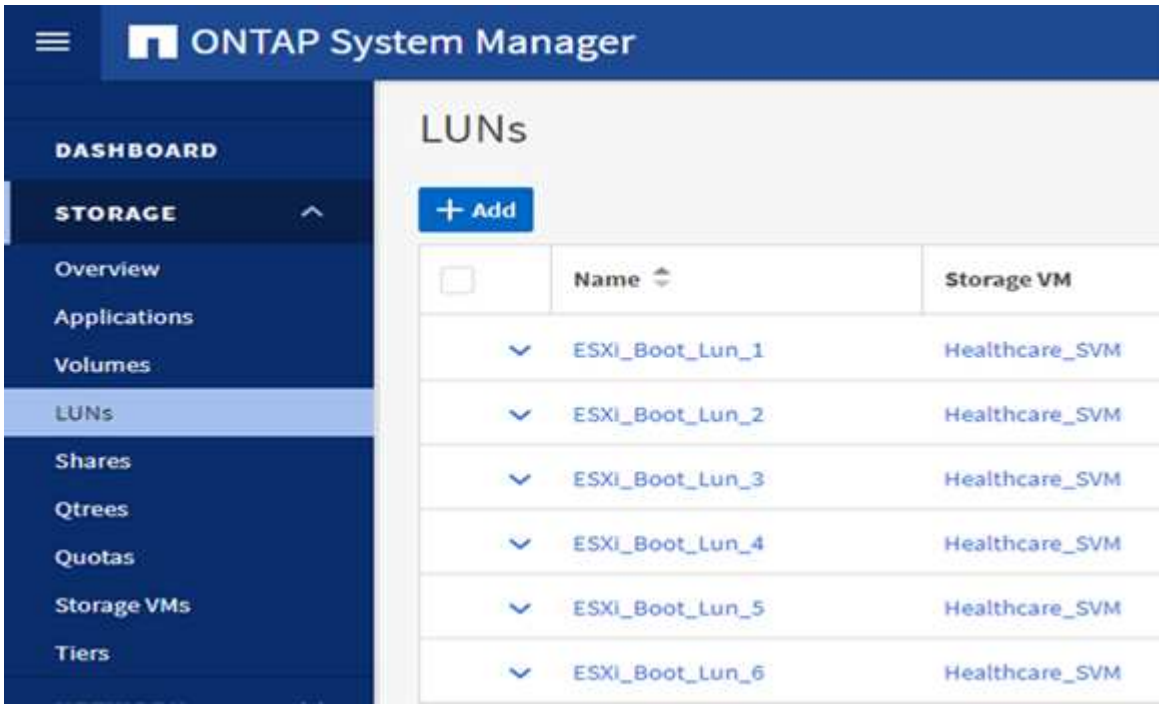
FlexPod のラボセットアップを実行するには、次の手順を実行します。

1. FlexPod ラボのセットアップと検証では、次の IP4 予約と VLAN を使用します。

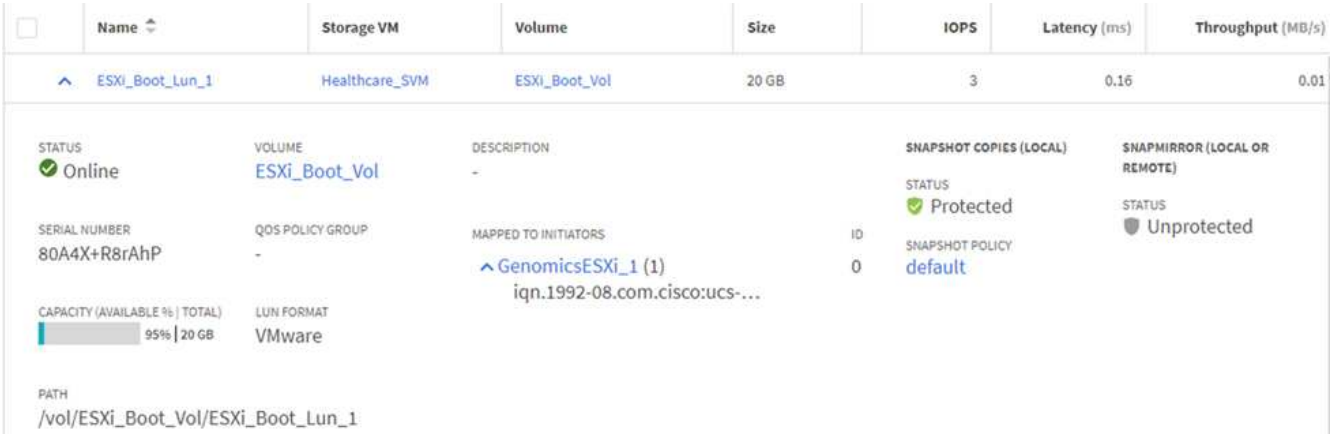
IP Reservations

VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. ONTAP SVM で iSCSI ベースのブート LUN を設定

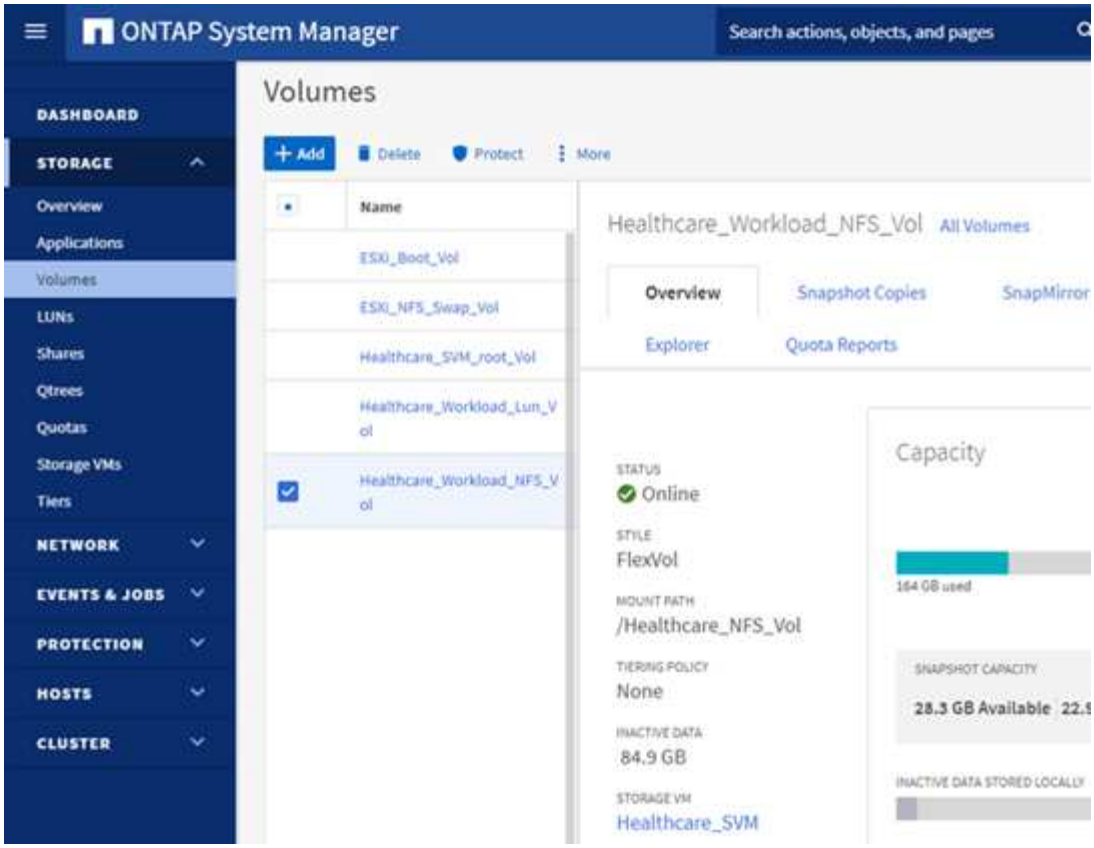


3. LUN を iSCSI イニシエータグループにマッピングします。

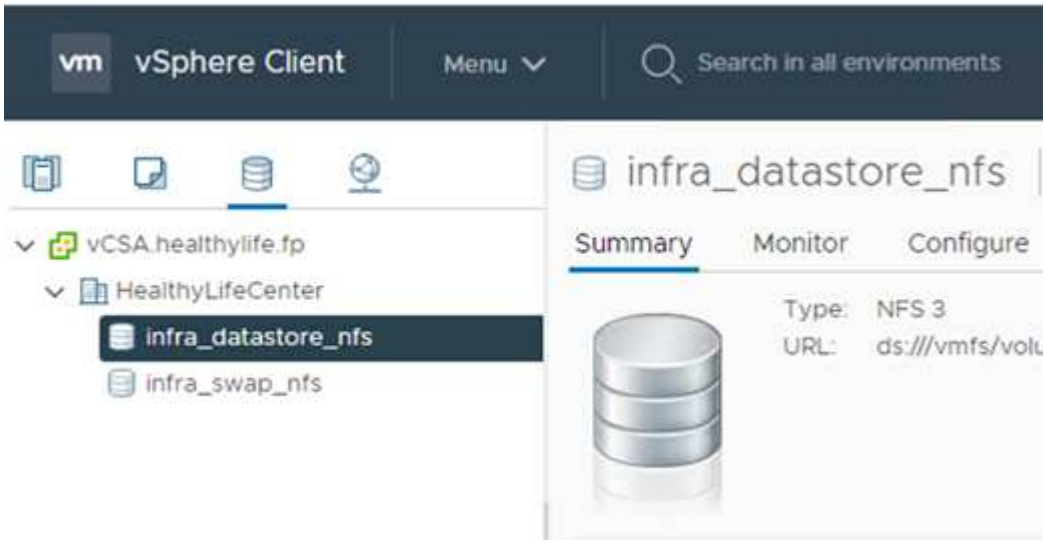


4. iSCSI ブートを使用して vSphere 7.0 をインストールします。
5. ESXi ホストを vCenter に登録します。

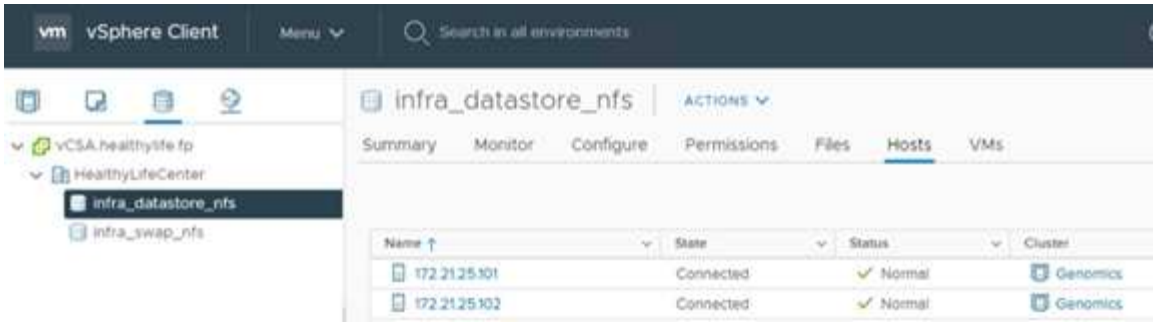
6. ONTAP ストレージ上で NFS データストア「 infra_datastore_nfs 」をプロビジョニングします。



7. vCenter にデータストアを追加します。



8. vCenter を使用して、 ESXi ホストに NFS データストアを追加します。



9. vCenter を使用して、 GATK を実行する Red Hat Enterprise Linux （ RHEL ） 8.3 VM を作成します。
10. NFS データストアが VM に提供され、「 /mnt/ゲノミクス 」でマウントされます。これは、 GATK 実行可能ファイル、スクリプト、 BAM （バイナリ・アライメント・マップ）ファイル、参照ファイル、インデックスファイル、辞書ファイル、およびバリアント呼び出し用の出力ファイルを格納するために使用されます。

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb                308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

GATK のセットアップと実行

Red Hat Enterprise 8.3 Linux VM に次の前提条件をインストールします。

- Java 8 または SDK 1.8 以降
- Broad Institute から GATK 4.2.0.0 をダウンロードしてください "GitHub サイト"。一般に、ゲノム配列データは、タブ区切りの一連の ASCII カラムの形で保存されます。ただし、 ASCII の保存に必要なスペースが多すぎます。したがって、新しい標準は BAM (*.bAM) ファイルと呼ばれて進化しました。BAM ファイルは、シーケンスデータを圧縮、インデックス化、およびバイナリ形式で格納します。私たち "ダウンロードしました" から GATK を実行するために公開されている BAM ファイルのセット "パブリックドメイン"。インデックスファイル（*.bai ）、辞書ファイル（* ）もダウンロードしました。dict ）、および参照データファイル（ * 。FASTA ）を参照してください。

ダウンロード後、 GATK ツールキットには jar ファイルと一連のサポートスクリプトがあります。

- GATK-PACKPACK-4.2.0.0 -local.jar 実行可能ファイル
- 「 GATK 」スクリプトファイル。

父、母、息子 * 。 BAM ファイルで構成された家族の BAM ファイルと対応する索引、辞書、参照ゲノムファイルをダウンロードしました。

クロムウェルエンジン

Cromwell は、ワークフロー管理を可能にする科学的なワークフローを対象としたオープンソースエンジンです。クロムウェルエンジンは 2 つの方法で作動できます "モード"、サーバーモード、または単一ワークフローの実行モード。クロムウェルエンジンの動作は、を使用して制御できます "クロムウェルエンジンコンフィギュレーションファイル"。

- * サーバーモード。 * 有効にします "RESTful なホテル" クロムウェルエンジンでのワークフローの実行。
- * 実行モード。 * 実行モードはクロムウェルで単一のワークフローを実行する場合に最適です。 "参照（

Ref ）" 実行モードで使用可能なすべてのオプションを表示します。

当社では、 Cromwell エンジンを使用してワークフローとパイプラインを大規模に実行しています。クロムウェルエンジンは使いやすいエンジンです "Workflow 概要の言語" (WDL) ベースのスクリプト言語。また、 Cromwell は、 Common Workflow Language （ CWL ）と呼ばれる 2 つ目のワークフロースクリプト標準もサポートしています。このテクニカルレポートでは、 WDL を使用しました。WDL は、もともと、広範なゲノム解析パイプライン研究所によって開発されたものです。WDL ワークフローを使用するには、次のようないくつかの戦略を使用します。

- * リニアチェーン。 * 名前が示すように、タスク #1 からの出力がタスク #2 に入力として送信されます。
- * マルチイン / アウト。 * これは、各タスクで複数の出力を後続のタスクに入力として送信できる点で、リニアチェーンと似ています。
- * Scatter-Gather * これは、特にイベント駆動型アーキテクチャで使用される場合に、最も強力なエンタープライズ・アプリケーション・インテグレーション（ EAI ）戦略の 1 つです。各タスクは分離された方法で実行され、各タスクの出力が最終出力に統合されます。

WDL を使用してスタンドアロンモードで GATK を実行するには、次の 3 つの手順があります。

1. 「 womtool.jar 」を使用して構文を検証します。

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. JSON の生成

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. Cromwell エンジンと Cromwell.jar を使用してワークフローを実行します

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

GATK は、いくつかのメソッドを使用して実行できます。このドキュメントでは、これらの方法のうちの 3 つについて説明します。

jar ファイルを使用した GATK の実行

では、 hplotype バリアントの呼び出し側を使用した単一バリアントのコールパイプラインの実行について見てみましょう。

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

この実行方法では、 GATK ローカル実行 jar ファイルを使用し、 1 つの Java コマンドを使用して jar ファイルを呼び出します。このコマンドには、いくつかのパラメータが渡されます。

1. このパラメータは 'HaplotypeCaller バリアントの呼び出し側パイプラインを呼び出していることを示します
2. --input' は、入力 BAM ファイルを指定します。
3. --output' は、 variant 呼び出し形式（ *.VCF ）でバリアント出力ファイルを指定します。 ("参照（ Ref ）" ）。
4. 「 --reference 」パラメータを使用して、参照ゲノムを渡しています。

実行すると、出力の詳細がセクションに表示されます "jar ファイルを使用して GATK を実行するための出力。"

./GATK スクリプトを使用した GATK の実行

GATK ツール・キットは './GATK' スクリプトを使用して実行できます次のコマンドを見てみましょう。

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

コマンドにはいくつかのパラメータを渡します。

- このパラメータは 'HaplotypeCaller バリアントの呼び出し側パイプラインを呼び出していることを示します
- 「 -i 」は、入力 BAM ファイルを指定します。
- 「 -O 」は、バリアント・コール・フォーマット（ *.VCF ）でバリアント出力ファイルを指定します。 ("参照（ Ref ）"）。

- R パラメータを使用して、参照ゲノムを渡しています。

実行すると、出力の詳細がセクションに表示されます "016e203cf9beada735f224ab14d0b3af"

クロムウェルエンジンを使用した GATK の実行

当社では、クルムウェルエンジンを使用して GATK の実行を管理しています。コマンドラインとパラメータを見てみましょう。

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

ここでは '-car' パラメータを渡して java コマンドを呼び出しますこれは 'Cromwell-65.jar などの jar ファイルを実行することを示します次に渡されるパラメータ (`run') は、クロムウェルエンジンが実行モードで実行されていることを示します。もう 1 つのオプションはサーバーモードです。次のパラメータは '*.wdl ですこれは ' 実行モードがパイプラインを実行するために使用する必要があります次のパラメータは、実行するワークフローへの入力パラメータのセットです。

「 ghplo.wdl 」ファイルの内容は次のようになります。

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

ここでは、 Cromwell エンジンへの入力を持つ、対応する JSON ファイルを示します。

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

Cromwell は実行にインメモリデータベースを使用していることに注意してください。実行すると、出力ログがセクションに表示されます "クロムウェルエンジンを使用した GATK 実行用出力。"

GATK を実行するための包括的な手順については、を参照してください "GATK のドキュメント"。

"次の例： jar ファイルを使用して GATK を実行するための出力。"

jar ファイルを使用して GATK を実行するための出力

"以前のゲノム - GATK のセットアップと実行。"

jar ファイルを使用して GATK を実行すると、次のような出力が得られます。

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
```

```
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
```

```
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

出力ファイルは、実行後に指定された場所にあります。

"fb08e15744e912200b45cf04b5fce2ad"

./GATK スクリプトを使用して GATK を実行するための出力

"Previous ： jar ファイルを使用して GATK を実行するための出力。"

「 ./GATK` 」スクリプトを使用して GATK を実行すると、次の出力例が得られます。

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller -
```

```
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
```

```
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

出力ファイルは、実行後に指定された場所にあります。

"次に、クロムウェルエンジンを使用した GATK の実行出力を示します。"

クロムウェルエンジンを使用した **GATK** 実行用出力

"11fffe01d469840980d9b9a5f45bf9ed"

Cromwell エンジンを使用して GATK を実行すると、次の出力例が得られます。

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
```

```
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
  "cromwellId" : "cromid-41b7e30",
  "heartbeatInterval" : "2 minutes",
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
```

```
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
helloHaplotypeCaller.haplotypeCaller
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
```

```
{
  "outputs": {
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
```

```
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"次は GPU のセットアップです。"

GPU セットアップ

"以前：クロムウェルエンジンを使用した GATK の実行出力。"

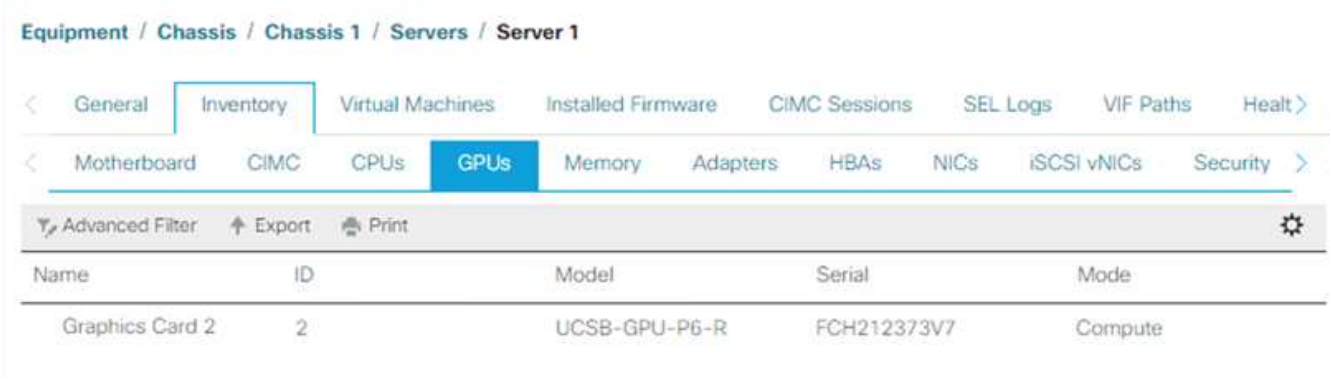
GATK ツールは、公開時点で、オンプレミスでの GPU ベースの実行をネイティブでサポートしていません。以下のセットアップとガイダンスは、 GATK 用の PCIe メザニンカードを使用して、背面取り付けの NVIDIA Tesla P6 GPU で FlexPod を使用する場合の簡単な方法を読者が理解できるようにします。

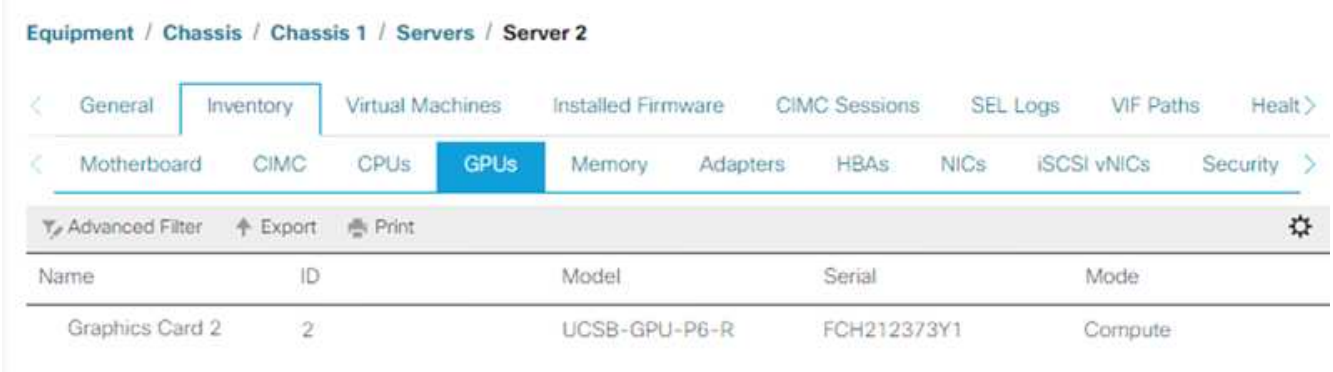
次の Cisco Validated Design （ CVD ）をリファレンスアーキテクチャとして使用し、 FlexPod 環境をセットアップして GPU を使用するアプリケーションを実行できるようにしました。

- "FlexPod Datacenter for AI / ML with Cisco UCS 480 ML for Deep Learning 』を参照してください"

このセットアップの重要なポイントを次に示します。

1. UCS B200 M5 サーバのメザニンスロットに PCIe NVIDIA Tesla P6 GPU を使用しました。





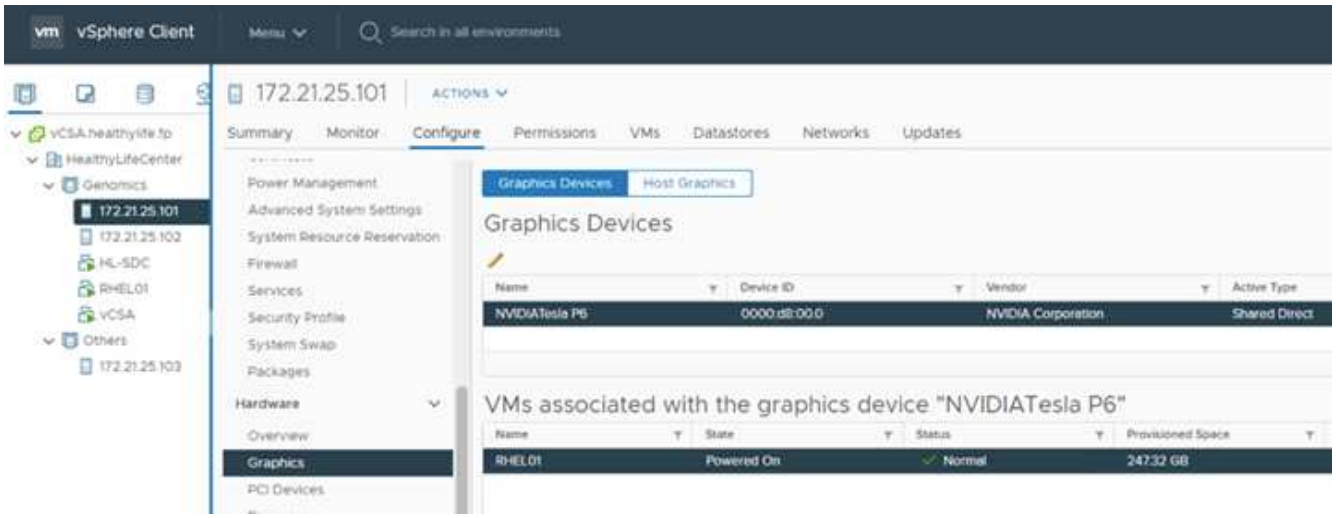
2. このセットアップでは、 NVIDIA パートナーポータルに登録し、コンピューティングモードで GPU を使用できる評価用ライセンス（使用権）を取得しました。
3. NVIDIA パートナーの Web サイトから、必要な NVIDIA vGPU ソフトウェアをダウンロードしました。
4. エンタイトルメント「 *.bin 」ファイルを NVIDIA パートナーの Web サイトからダウンロードしました。
5. NVIDIA vGPU ライセンスサーバをインストールし、 NVIDIA パートナーサイトからダウンロードした「 *.bin 」ファイルを使用してライセンスサーバに使用権を追加しました。
6. NVIDIA パートナーポータルで、導入環境に適した NVIDIA vGPU ソフトウェアのバージョンを選択してください。このセットアップでは、ドライバのバージョン 460.73.02 を使用しました。
7. このコマンドは、をインストールします "NVIDIA vGPU Manager の略" ESXi で。

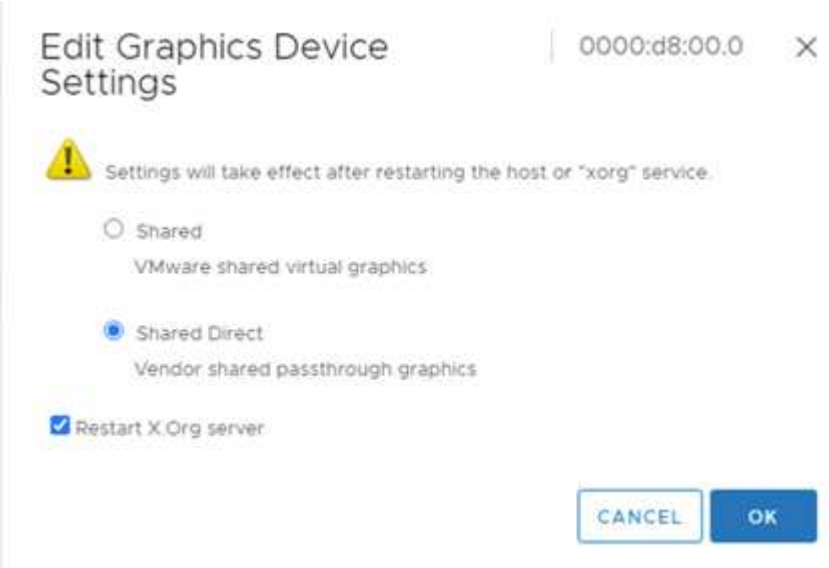
```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

8. ESXi サーバのリブート後、次のコマンドを実行してインストールを検証し、 GPU の健全性を確認します。

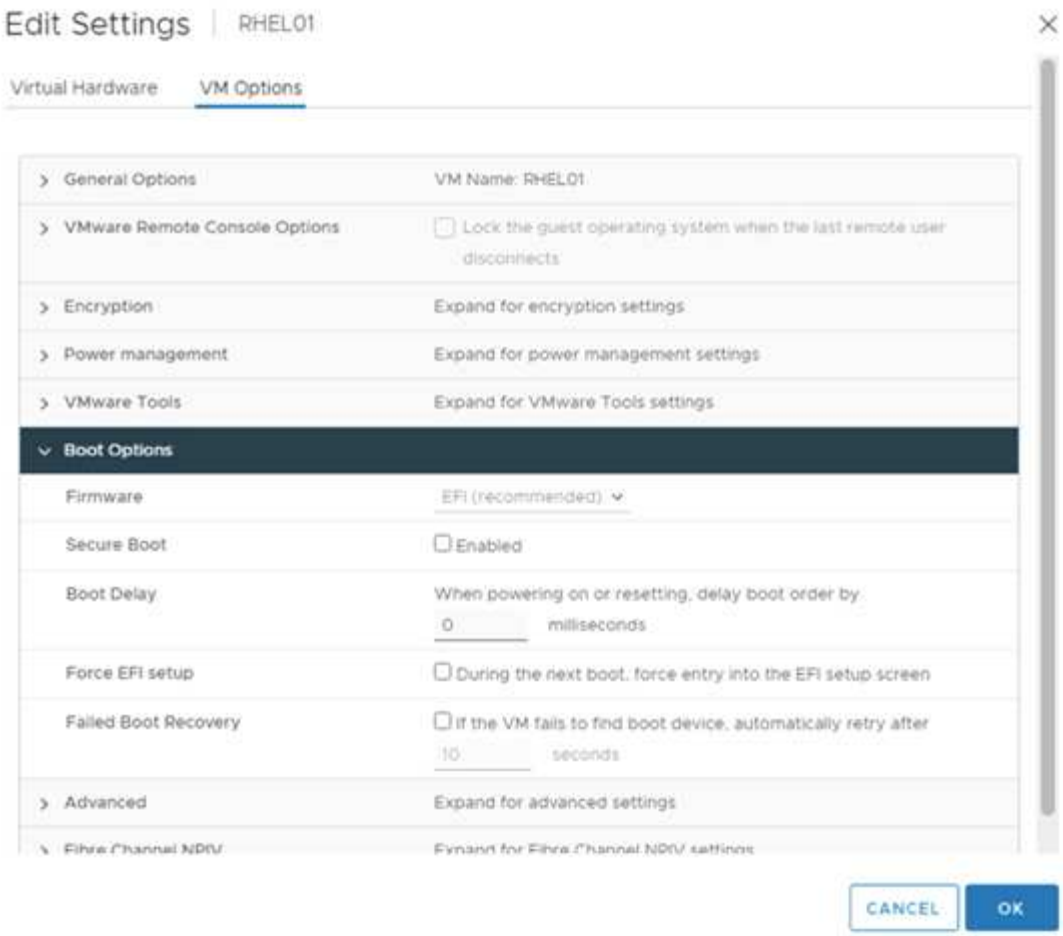
```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+================
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. vCenter を使用 "設定" グラフィックデバイスの設定は「 Shared Direct 」になります。





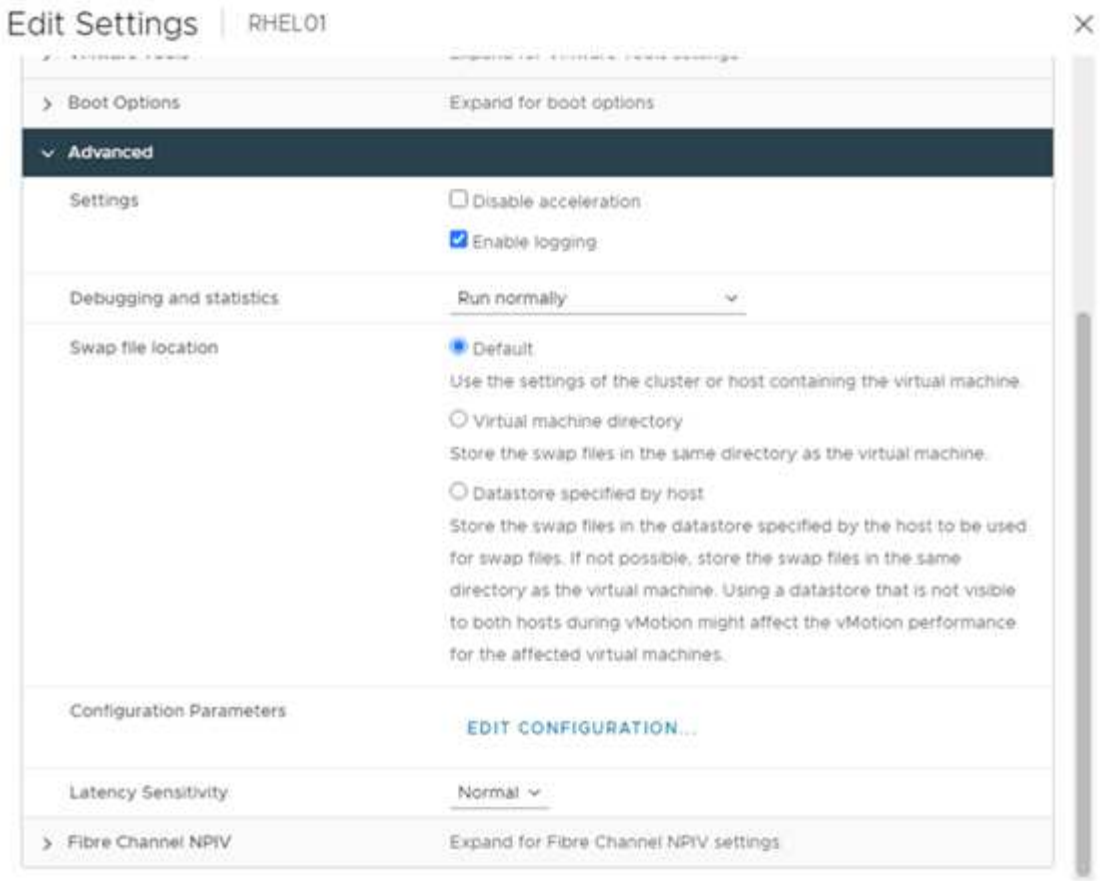
10. RedHat VM のセキュアブートが無効になっていることを確認します。
11. VM 起動オプションファームウェアが EFI （"参照（Ref）"）。

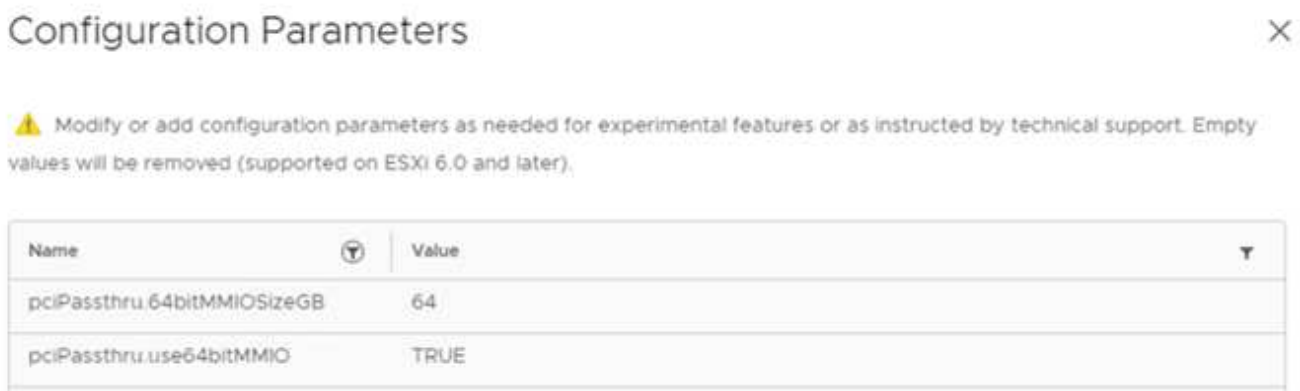


12. 次のパラメータが VM オプションの詳細編集設定に追加されていることを確認します。「pciPassthru.64bitMMIOSizeGB 」パラメータの値は、 VM に割り当てられた GPU のメモリと数によって異なります。例：

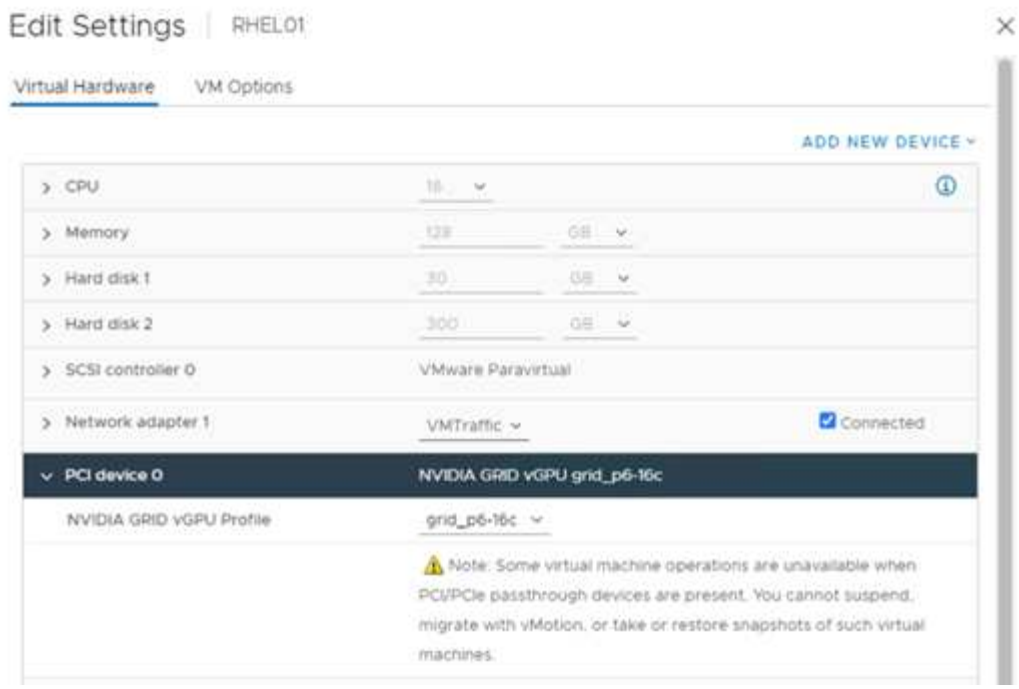
    a. VM に 32GB V100 GPU が 4 つ割り当てられている場合は、この値を 128 にします。

    b. VM に 16GB P6 GPU が 4 つ割り当てられている場合、この値は 64 である必要があります。





13. vCenter で新しい PCI デバイスとして vGPU を仮想マシンに追加する場合は、 PCI デバイスタイプとして NVIDIA GRID vGPU を選択してください。
14. 使用している GPU 、 GPU メモリ、および使用目的を調整する適切な GPU プロファイルを選択します。たとえば、グラフィックスとコンピューティングです。



15. Red Hat Linux VM で、次のコマンドを実行して NVIDIA ドライバをインストールできます。

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. 次のコマンドを実行して、正しい vGPU プロファイルが報告されていることを確認します。

```
[root@genomics1 genomics]# nvidia-smi -query-gpu=gpu_name
-format=csv,noheader -id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. リブート後は、正しい NVIDIA vGPU がドライバのバージョンと一緒に報告されていることを確認します。

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+================
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. vGPU グリッド構成ファイルの VM にライセンスサーバの IP が設定されていることを確認してください。
    a. テンプレートをコピーします。

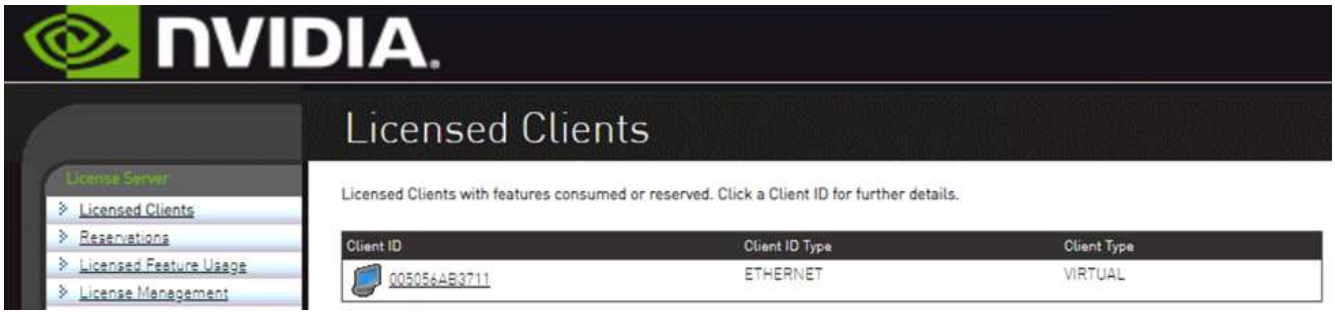
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. /etc/nvidia /rid ファイルを編集し、ライセンス・サーバの IP アドレスを追加して、機能タイプを 1 に設定します。

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. VM を再起動すると、次のように、ライセンスサーバーのライセンスクライアントの下にエントリが表示されます。



20. GATK および Cromwell ソフトウェアのダウンロードの詳細については、「 Solutions Setup 」セクションを参照してください。

21. GATK がオンプレミスで GPU を使用できるようになると、ワークフロー概要言語は「 * 」になります。wdl には、次に示すランタイム属性があります。

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"次は終わりです"

まとめ

"前のバージョン： GPU セットアップ。"

世界中の多くの医療機関が、 FlexPod を共通のプラットフォームとして標準化しています。FlexPod を使用すれば、医療機能を確実に導入できます。FlexPod と NetApp ONTAP には、業界をリードする一連のプロトコルを標準で実装できる機能が標準で搭載されています。特定の患者のゲノム研究の依頼の元にかかわらず、相互運用性、アクセシビリティ、可用性、およびスケーラビリティは、 FlexPod プラットフォームに標準で

備わっています。FlexPod プラットフォーム上で標準化されると、イノベーションの文化は伝染しなくなります。

追加情報の参照先

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 Datacenter for AI / ML with Cisco UCS 480 ML for Deep Learning 』を参照してください

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- FlexPod Datacenter with VMware vSphere 7.0 and NetApp ONTAP 9.7 』を参照してください

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- ONTAP 9 ドキュメンテーション・センター

  "http://docs.netapp.com"

- 即応性と効率性— FlexPod がデータセンターの最新化をどのように推進するか

  "https://www.flexpod.com/idc-white-paper/"

- 医療業界の AI

  "https://www.netapp.com/us/media/na-369.pdf"

- ヘルスケア向けの FlexPod で変革を促進

  "https://flexpod.com/solutions/verticals/healthcare/"

- Cisco とネットアップが提供する FlexPod

  "https://flexpod.com/"

- ヘルスケア向けの AI と分析（ネットアップ）

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- 医療機関における AI スマートインフラの選択が成功を促進します

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- FlexPod 9.8 を備えた ONTAP データセンター、 Cisco Intersight 用の ONTAP ストレージコネクタ、および Cisco Intersight 管理モード。

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- Red Hat Enterprise Linux OpenStack プラットフォームを搭載した FlexPod データセンター

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

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	2021年11月	初版リリース

FlexPod for MEDITECH の指向性サイジングガイド

TR-4774 ：『 FlexPod for MEDITECH Directional Sizing 』

Brandon AGEE 、 John Duignan 、 NetApp Mike Brennan 、 Cisco 、 Jon Ebmeir

協力：

本レポートは、 MEDITECH EHR アプリケーションソフトウェア環境向け FlexPod のサイジングに関するガイダンスを提供します。

目的

FlexPod システムは、 MEDITECH 拡張機能、 6.x 、 5.x 、および Magic サービスをホストすることができます。MEDITECH アプリケーション層をホストする FlexPod サーバは、信頼性の高いハイパフォーマンスインフラストラクチャを実現する統合プラットフォームを提供します。FlexPod 統合プラットフォームは、高度なスキルを持つ FlexPod チャネルパートナーによって迅速に導入され、 Cisco とネットアップのテクニカルアシスタンスセンターによってサポートされます。

サイジングは、 MEDITECH のハードウェア構成提案書と MEDITECH タスクドキュメントの情報に基づいています。コンピューティング、ネットワーク、ストレージのインフラコンポーネントに最適なサイズを判断することがその目的です。

。 "MEDITECH ワークロードの概要" MEDITECH 環境に用意されているコンピューティングワークロードとストレージワークロードの種類については、セクションを参照してください。

。 "小規模、中規模、大規模アーキテクチャの技術仕様" セクションでは、の項で説明した各種ストレージアーキテクチャのコンポーネント一覧の例を示します。ここで示す設定は、一般的なガイドラインにすぎません。ワークロードに基づいてサイジングを行い、それに応じて構成を調整してください。

解決策の全体的なメリット

MEDITECH 環境を FlexPod アーキテクチャ基盤で運用すると、医療機関の生産性が向上し、設備投資と運用コストが削減されます。FlexPod は、 Cisco とネットアップの戦略的パートナーシップにより、検証済みで厳格にテストされた統合インフラを提供します。予測可能な低レイテンシのシステムパフォーマンスと高可用性を実現するように特別に設計されています。その結果、 MEDITECH EHR システムのユーザの応答時間が短縮されます。

Cisco とネットアップが提供する FlexPod 解決策は、パフォーマンスに優れたモジュラ型の検証済み統合型仮想化ソリューションで、 MEDITECH のシステム要件を満たしています。 効率性、拡張性、コスト効率に優れたプラットフォーム。MEDITECH を備えた FlexPod データセンターには、医療業界に固有のいくつかのメリットがあります。

- * モジュラアーキテクチャ * 。FlexPod は、特定のワークロードごとにカスタマイズされた FlexPod システムを使用して、 MEDITECH のモジュラアーキテクチャのさまざまなニーズに対応します。すべてのコンポーネントは、クラスタ化されたサーバおよびストレージ管理ファブリックを通じて接続され、統合された管理ツールセットを使用します。
- * 運用の簡素化とコストの削減 * 。従来のプラットフォームをより効率的で拡張性の高い共有リソースに置き換えることで、どこにいても臨床医をサポートできるようにすることで、コストと複雑さを排除できます。この解決策は、リソースの使用率を向上させて、投資回収率（ ROI ）を向上させます。
- * インフラストラクチャの迅速な導入 * 。FlexPod Datacenter と MEDITECH の統合設計により、お客様は新しいインフラを迅速かつ容易に稼働させることができ、オンサイトとリモートの両方のデータセンターに対応できます。
- * スケールアウトアーキテクチャ * 。SAN と NAS は、実行中のアプリケーションを再構成することなく、数テラバイトから数十ペタバイトまで拡張できます。
- * ノンストップオペレーション * 。ストレージの保守、ハードウェアのライフサイクル処理、ソフトウェアのアップグレードを、ビジネスを中断することなく実行できます。
- * セキュアマルチテナンシー * 。このメリットにより、仮想サーバと共有ストレージインフラのニーズが増大し、施設固有の情報をセキュアマルチテナンシーで利用できるようになります。このメリットは、データベースとソフトウェアの複数のインスタンスをホストする場合に重要です。
- * プールされたリソースの最適化 * 。このメリットは、物理サーバとストレージコントローラの台数の削減、ワークロードの負荷分散、利用率の向上、同時にパフォーマンスの向上にも役立ちます。
- * サービス品質（ QoS ）。 * FlexPod は、スタック全体でサービス品質（ QoS ）を提供します。業界をリードする QoS ストレージポリシーにより、共有環境で差別化されたサービスレベルを実現します。これらのポリシーを使用することで、ワークロードに最適なパフォーマンスを提供し、過負荷のアプリケーションを分離および制御できます。
- * ストレージ効率 *NetApp 7 ： 1 のストレージ効率化機能により、ストレージコストを削減できます。
- * 機敏性 * 。FlexPod システムが提供する、業界をリードするワークフローの自動化、オーケストレーション、管理のためのツールにより、 IT 部門はビジネス要求への即応性を大幅に高めることができます。これらのビジネス・リクエストは 'MEDITECH のバックアップ / プロビジョニング環境や ' テスト / トレーニング環境の追加から ' 人口健全性管理イニシアティブの分析データベース・レプリケーションまで多岐にわたります
- * 生産性 * 。この解決策をすばやく導入して拡張することで、臨床家のエンドユーザー体験を最適化できます。
- * データファブリック * 。ネットアップデータファブリックアーキテクチャは、サイト間、物理的な境界を超え、アプリケーション間でデータを結び付けます。ネットアップデータファブリックは、 Data-Centric の世界におけるデータ主体の企業向けに構築されています。データは複数の場所で作成、使用され、多くの場合、アプリケーションやインフラと共有されます。データファブリックでは、一貫性のある統合データを管理できます。また、 IT 部門がデータをより細かく制御し、増え続ける IT の複雑さを軽減します。

適用範囲

このドキュメントでは、 Cisco UCS および NetApp ONTAP ベースのストレージを使用する環境について説明します。MEDITECH をホストするためのサンプル・リファレンス・アーキテクチャを提供します。

次の内容は含まれません。

- NetApp System Performance Modeler （ SPM ）またはネットアップのその他のサイジングツールを使用し、サイジングに関する詳細なガイダンスを提供します。

- 非本番ワークロード向けのサイジング

対象者

本ドキュメントは、ネットアップおよびパートナーのシステムエンジニアと、ネットアップのプロフェッショナルサービス担当者を対象としています。このドキュメントは、コンピューティングとストレージのサイジングの概念について十分に理解していること、および Cisco UCS とネットアップストレージシステムに関する技術的な知識があることを前提としています。

関連ドキュメント

本テクニカルレポートに関連する次のテクニカルレポートやその他のドキュメントを参照して、 MEDITECH を FlexPod インフラにサイジング、設計、導入するために必要なドキュメントをすべてまとめてください。

- "TR-4753 ：『 FlexPod Datacenter for MEDITECH Deployment Guide 』"
- "TR-4190 ：『 NetApp Sizing Guidelines for MEDITECH Environments 』"
- "TR-4219 ：『 NetApp Deployment Guidelines for MEDITECH Environments 』"

これらのレポートの一部にアクセスするには、 NetApp Field Portal のログインクレデンシャルが必要です。

MEDITECH ワークロードの概要

このセクションでは、 MEDITECH 環境に当てはまるコンピューティングワークロードとストレージワークロードの種類について説明します。

MEDITECH とバックアップのワークロード

MEDITECH 環境向けのネットアップストレージシステムをサイジングする場合は、 MEDITECH の本番用ワークロードとバックアップワークロードの両方を考慮する必要があります。

MEDITECH ホスト
MEDITECH ホストはデータベース・サーバですこのホストは MEDITECH ファイル・サーバ（拡張機能用 '6.x または C/S 5.x プラットフォーム用）または Magic マシン（ Magic プラットフォーム用）とも呼ばれます本ドキュメントでは、 MEDITECH ホストという用語を MEDITECH ファイルサーバと Magic マシンのことに使用しています。

以降のセクションでは、この 2 つのワークロードの I/O 特性とパフォーマンス要件について説明します。

MEDITECH のワークロード

MEDITECH 環境では 'MEDITECH ソフトウェアを実行する複数のサーバが 'MEDITECH システムと呼ばれる統合システムとしてさまざまなタスクを実行しますMEDITECH システムの詳細については、 MEDITECH のドキュメントを参照してください。

- 本番環境の MEDITECH 環境については、該当する MEDITECH のドキュメントを参照して、ネットアップストレージシステムのサイジングに含める必要がある MEDITECH ホストの数とストレージ容量を確認してください。

- 新しい MEDITECH 環境については、ハードウェア構成の提案書を参照してください。既存の MEDITECH 環境については、ハードウェア評価タスクのドキュメントを参照してください。ハードウェア評価タスクは MEDITECH チケットに関連付けられています。お客様は、 MEDITECH からこれらのドキュメントのいずれかをリクエストできます。

MEDITECH システムを拡張して、ホストを追加することで容量とパフォーマンスを向上させることができます。各ホストには、そのデータベースファイルとアプリケーションファイル用のストレージ容量が必要です。各 MEDITECH ホストが使用できるストレージも、ホストが生成した I/O に対応している必要があります。MEDITECH 環境では ' 各ホストがそのホストのデータベースおよびアプリケーション・ストレージ要件をサポートするために 'LUN を使用できますMEDITECH カテゴリのタイプと導入するプラットフォームのタイプによって、各 MEDITECH ホストのワークロード特性とシステム全体のワークロード特性が決まります。

MEDITECH カテゴリ

MEDITECH では、導入規模とカテゴリ番号を 1 〜 6 の範囲で関連付けています。カテゴリ 1 は MEDITECH の導入規模が最小で、カテゴリ 6 は最大です。各カテゴリに関連付けられている MEDITECH アプリケーション仕様には、次のようなメトリックが含まれます。

- 病院ベッドの数
- 1 年あたりの入院患者数
- 1 年あたりの外来患者数
- 緊急の客室訪問回数（年間）
- 1 年あたりの試験数
- 1 日あたりの入院処方
- 1 日あたりの外来処方

MEDITECH カテゴリの詳細については、 MEDITECH カテゴリのリファレンス・シートを参照してください。このシートは、 MEDITECH からお客様経由で入手するか、 MEDITECH システムのインストーラを使用して入手できます。

MEDITECH プラットフォーム

MEDITECH には 4 つのプラットフォームがあります。

- 拡張
- MEDITECH 6.x
- クライアント / サーバ 5.x （ C/S 5.x ）
- マジック

MEDITECH 拡張プラットフォーム '6.x プラットフォーム ' および C/S 5.x プラットフォームの場合 ' 各ホストの I/O 特性は 100% ランダムで ' 要求サイズは 4,000 ですMEDITECH Magic プラットフォームでは、各ホストの I/O 特性は 100% ランダムで、リクエストサイズは 8,000 または 16,000 です。MEDITECH によると、一般的な Magic Production Deployment の要求サイズは 8 、 000 または 1 、 000 です。

読み取りと書き込みの比率は、導入するプラットフォームによって異なります。MEDITECH では ' 読み取りと書き込みの平均の比率を予測してから ' それらを割合として表現していますMEDITECH では、特定の MEDITECH プラットフォーム上の MEDITECH ホストごとに必要な平均持続 IOPS 値も算出しています。次の表は、 MEDITECH が提供するプラットフォーム固有の I/O 特性をまとめたものです。

MEDITECH カテゴリ	**MEDITECH** プラットフォーム	平均ランダムリード率	平均ランダムライト率	**MEDITECH** ホストあたりの平均持続 **IOPS**
1.	拡張、 6.x	20	80	750
2-6	拡張	20	80	750
	6.x	20	80	750
	C/S 5.x	40	60	600
	マジック	90	10.	400

MEDITECH システムの場合、各ホストの平均 IOPS レベルは上記の表に定義された IOPS 値と同じである必要があります。各プラットフォームに基づいて正しいストレージサイジングを決定するために、上記の表に記載されている IOPS 値が、に記載されているサイジング方法の一部として使用されます "小規模、中規模、大規模アーキテクチャの技術仕様" セクション。

MEDITECH では、各ホストのランダムライトの平均レイテンシを 1 ミリ秒未満に抑える必要があります。ただし、バックアップジョブおよび再配置ジョブでは、書き込みレイテンシが一時的に 2 ミリ秒まで上昇することは許容されると考えられます。MEDITECH では ' カテゴリ 1 のホストで平均ランダム・リード・レイテンシーを 7ms 未満に ' カテゴリ 2 のホストでは 5ms 未満に抑える必要もありますこれらのレイテンシ要件は、 MEDITECH プラットフォームが使用されているかどうかに関係なく、すべてのホストに適用されます。

次の表に、 MEDITECH ワークロード用のネットアップストレージをサイジングする際に考慮する必要がある I/O 特性をまとめます。

パラメータ	**MEDITECH** カテゴリ	拡張	**MEDITECH 6.x**	**C/S 5.x**	マジック
リクエストのサイズ	1 ～ 6	4K	4K	4K	8K または 16K
ランダム / シーケンシャル		100% ランダム	100% ランダム	100% ランダム	100% ランダム
平均持続 IOPS	1.	750	750	該当なし	該当なし
	2-6	750	750	600	400
読み取り / 書き込み比率	1 ～ 6	読み取り 20% 、書き込み 80%	読み取り 20% 、書き込み 80%	読み取り 40% 、書き込み 60%	読み取り 90% 、書き込み 10%
書き込みレイテンシ		1 ミリ秒未満	1 ミリ秒未満	1 ミリ秒未満	1 ミリ秒未満
ピーク時の書き込みレイテンシ	1 ～ 6	2 ミリ秒未満	2 ミリ秒未満	2 ミリ秒未満	2 ミリ秒未満
読み取りレイテンシ	1.	7 ミリ秒未満	7 ミリ秒未満	該当なし	該当なし
	2-6	5 ミリ秒未満	5 ミリ秒未満	5 ミリ秒未満	5 ミリ秒未満

カテゴリ 3 ～ 6 の MEDITECH ホストの I/O 特性は ' カテゴリ 2 と同じですMEDITECH カテゴリ 2 ～ 6 の場合 ' 各カテゴリに導入されるホストの数は異なります

ネットアップストレージシステムは、前のセクションで説明したパフォーマンス要件を満たすようにサイジングする必要があります。MEDITECH の本番用ワークロードに加えて、ネットアップのストレージシステム

は、バックアップ処理中にこれらの MEDITECH のパフォーマンスターゲットを保持できる必要があります。詳細については、次のセクションを参照してください。

バックアップワークロードの概要

MEDITECH 認定バックアップ・ソフトウェアは 'MEDITECH システムの各 MEDITECH ホストで使用されている LUN をバックアップしますバックアップをアプリケーションと整合性のある状態にするには、バックアップソフトウェアが MEDITECH システムを休止し、ディスクへの I/O 要求を一時停止します。システムが休止状態になると、バックアップソフトウェアはネットアップストレージシステムにコマンドを発行して、LUN を含むボリュームの NetApp Snapshot コピーを作成します。バックアップ・ソフトウェアはあとで MEDITECH システムの休止を解除し ' 本番 I/O 要求がデータベースに継続できるようにしますSnapshot コピーに基づいて、 NetApp FlexClone ボリュームが作成されます。このボリュームはバックアップソースによって使用され、 LUN をホストする親ボリュームで本番環境の I/O 要求が継続されます。

バックアップソフトウェアによって生成されるワークロードは、 FlexClone ボリューム内に存在する LUN のシーケンシャルリードから発生します。このワークロードは、 100% のシーケンシャルリードワークロードと定義されており、要求サイズは 64,000 です。MEDITECH の本番ワークロードについては、必要な IOPS と関連する読み取り / 書き込みレイテンシレベルを維持することがパフォーマンス基準となります。ただし、バックアップ・ワークロードでは、バックアップ処理中に生成されたデータの総スループット（ MBps ）に注意がシフトされます。MEDITECH LUN のバックアップは 8 時間以内に完了する必要がありますが、すべての MEDITECH LUN のバックアップは 6 時間以内に完了することを推奨します。バックアップを 6 時間以内に完了することを目標にすると、 MEDITECH のワークロードが計画外に増加した場合や、 NetApp ONTAP のバックグラウンド処理が増えた場合など、一定の期間にわたってデータが増加した場合にもその数を軽減できます。これらのいずれかのイベントによって、追加のバックアップ時間が発生する可能性があります。保存されているアプリケーション・データの量にかかわらず ' バックアップ・ソフトウェアは 'MEDITECH ホストごとに LUN 全体のブロック・レベルのフル・バックアップを実行します

このウィンドウ内でバックアップを完了するために必要なシーケンシャルリードのスループットを、次の要因に応じて計算します。

- 必要なバックアップ期間
- LUN の数
- バックアップする各 LUN のサイズ

たとえば、 50 ホストの MEDITECH 環境で、各ホストの LUN サイズが 200GB の場合、バックアップする LUN の合計容量は 10TB になります。

8 時間で 10TB のデータをバックアップするには、次のスループットが必要です。

- = （ 10 x 10^6 ） MB （ 8 x 3 、 600 ）
- = 347.2MBps

ただし、計画外のイベントを考慮して、控えめなバックアップ期間として 5.5 時間を選択し、推奨される 6 時間を超えるヘッドルームを確保します。

8 時間で 10TB のデータをバックアップするには、次のスループットが必要です。

- = （ 10 x 10^6 ） MB （ 5.5 x 3 、 600 ）
- = 500Mbps

500Mbps のスループットレートでは、バックアップは 5.5 時間以内に完了し、 8 時間のバックアップ要件内で快適に完了できます。

次の表に、ストレージシステムのサイズ設定時に使用するバックアップワークロードの I/O 特性をまとめます。

パラメータ	すべてのプラットフォーム
リクエストのサイズ	64K
ランダム / シーケンシャル	100% シーケンシャル
読み取り / 書き込み比率	100% 読み取り
平均スループット	MEDITECH ホストの数と各 LUN のサイズによって異なる：バックアップは 8 時間以内に完了する必要があります
必要なバックアップ期間	8 時間

MEDITECH 向け **Cisco UCS** リファレンスアーキテクチャ

MEDITECH on FlexPod のアーキテクチャは、 MEDITECH 、 Cisco 、 NetApp のガイダンスと、 MEDITECH をご利用のお客様とあらゆる規模のお客様との連携に関するパートナー様の経験に基づいています。このアーキテクチャは柔軟性が高く、お客様のデータセンター戦略に応じて、 MEDITECH のベストプラクティスを適用します。つまり、小規模でも大規模でも、一元化されたものでも、分散型でも、マルチテナント型でも同様です。

MEDITECH を導入する際、シスコは MEDITECH のベストプラクティスに直接適合する Cisco UCS リファレンスアーキテクチャを設計しました。Cisco UCS は、高性能、高可用性、信頼性、拡張性を備えた緊密に統合された解決策を提供し、医師の診療や病院のシステムに数千台のベッドを使用しています。

小規模、中規模、大規模のアーキテクチャ向けの技術仕様

このセクションでは、さまざまなサイズのストレージアーキテクチャに対応するサンプル部品表について説明します。

小規模、中規模、大規模のアーキテクチャ向けの部品表。

FlexPod の設計は、多数の異なるコンポーネントとソフトウェアバージョンを含む柔軟なインフラです。使用 "TR-4036 ：『 FlexPod Technical Specifications 』" 有効な FlexPod 構成を組み立てるためのガイドとして使用してください。次の表に、 FlexPod の最小要件を示します。設定例はそのままです。構成は、環境やユースケースに応じて製品ファミリーごとに拡張できます。

このサイジング演習では、カテゴリ 3 の MEDITECH 環境、カテゴリ 5 のメディア、カテゴリ 6 の大規模環境に対応します。

	小規模	中	大規模
プラットフォーム	NetApp AFF A220 オールフラッシュストレージシステム HA ペア × 1	NetApp AFF A220 HA ペア × 1	NetApp AFF A300 オールフラッシュストレージシステム HA ペア × 1
ディスクシェルフ	3.8TB × 9	3.8TB × 13TB	3.8TB × 19TB
MEDITECH データベースのサイズ	3TB - 12TB	17TB	30TB を超えています
MEDITECH の IOPS	22 、 000 IOPS 超	25 、 000 IOPS 超	32 、 000 IOPS 超

	小規模	中	大規模
合計 IOPS	22000 年	27000	35000
生データ	34.2TB	49.4TB	68.4TB
使用可能容量	18.53TiB	27.96TiB の場合	33.82TiB
実効容量（2 ： 1 のストレージ効率）	55.6TiB	83.89TiB	101.47TiB

お客様の環境によっては、複数の MEDITECH 本番ワークロードを同時に実行している場合や、 IOPS 要件が高い場合があります。その場合は、ネットアップアカウントチームと協力して、必要な IOPS と容量に基づいてストレージシステムのサイジングを行ってください。ワークロードに適したプラットフォームを特定できる必要があります。たとえば、 NetApp AFF A700 オールフラッシュストレージシステム HA ペアで複数の MEDITECH 環境を正常に実行しているお客様がいます。

次の表に、 MEDITECH 構成に必要な標準ソフトウェアを示します。

ソフトウェア	製品ファミリー	バージョンまたはリリース	詳細
ストレージ	ONTAP	ONTAP 9.4 の一般提供（GA）	
ネットワーク	Cisco UCS ファブリックインターコネクト	Cisco UCSM 4.x の場合	現在推奨されているリリース
	Cisco Nexus イーサネットスイッチ	7.0 （3） I7 （6）	現在推奨されているリリース
	Cisco FC ： Cisco MDS 9132T	8.3 （2）	現在推奨されているリリース
ハイパーバイザー	ハイパーバイザー	VMware vSphere ESXi 6.7	
	仮想マシン（VM）	Windows * 2016	
管理	ハイパーバイザー管理システム	VMware vCenter Server 6.7 U1 （vCSA）	
	NetApp Virtual Storage Console （VSC）	VSC 7.0P1	
	NetApp SnapCenter	SnapCenter 4.0	
	Cisco UCS Manager の略	4.x	

次の表は、小規模（カテゴリ 3 ）の構成例 - インフラコンポーネントを示しています。

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
コンピューティング	Cisco UCS 5108 シャーシ	1.	ハーフ幅ブレードを 8 台まで、またはフル幅ブレードを 4 台までサポートします。サーバ要件の増大に合わせてシャーシを追加します。
	Cisco シャーシ I/O モジュール	2 x 2208	8GB x 10GB アップリンクポート
	Cisco UCS ブレードサーバ	B200 M5 × 4	それぞれ 2 x 14 コア、2.6GHz 以上のクロック速度、 384GB BIOS 3.2 （ 3# ）
	Cisco UCS 仮想インターフェイスカード	UCS 1440 × 4	VMware ESXi fnic FC ドライバ： 1.0.47 VMware ESXi eNIC イーサネットドライバ： 1.0.27.0 （ Interoperability Matrix を参照：
	Cisco UCS ファブリックインターコネクト（ FI ） × 2	UCS 6454 FI × 2	10 / 25 / 100Gb イーサネットおよび 32Gb FC をサポートする第 4 世代のファブリックインターコネクト
ネットワーク	Cisco イーサネットスイッチ	Nexus 9336c-FX2 × 2	1Gb 、 10GB 、 25GB 、 40GB 、 100GB
ストレージネットワーク	BLOB ストレージ用の IP Network Nexus 9K		FI および UCS シャーシ
	FC ： Cisco MDS 9132T		Cisco 9132T スイッチ × 2
ストレージ	NetApp AFF A300 オールフラッシュストレージシステム	1 つの HA ペア	すべての MEDITECH ワークロード（ファイルサーバ、イメージサーバ、SQL Server 、 VMware など）に対応する 2 ノードクラスタ
	DS224C ディスクシェルフ	DS224C ディスクシェルフ 1 台	
	ソリッドステートドライブ（ SSD ）	3.8TB × 9	

次の表は、中規模（カテゴリ 5 ）構成の例、インフラストラクチャコンポーネントを示しています

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
コンピューティング	Cisco UCS 5108 シャーシ	1.	ハーフ幅ブレードを 8 台まで、またはフル幅ブレードを 4 台までサポートします。サーバ要件の増大に合わせてシャーシを追加します。
	Cisco シャーシ I/O モジュール	2 x 2208	8GB x 10GB アップリンクポート
	Cisco UCS ブレードサーバ	B200 M5 × 6	それぞれ 2 つの 16 コア、2.5GHz/ 以上のクロック速度、 384GB 以上のメモリ BIOS 3.2 （ 3# ）を備えています。
	Cisco UCS 仮想インターフェイスカード（ VIC ）	UCS 1440 VIC × 6	VMware ESXi fnic FC ドライバ： 1.0.47 VMware ESXi eNIC イーサネットドライバ： 1.0.27.0 （ Interoperability Matrix を参照）
	Cisco UCS ファブリックインターコネクト（ FI ） × 2	UCS 6454 FI × 2	10GB / 25Gb / 100Gb イーサネットおよび 32Gb FC をサポートする第 4 世代ファブリックインターコネクト
ネットワーク	Cisco イーサネットスイッチ	Nexus 9336c-FX2 × 2	1Gb 、 10GB 、 25GB 、 40GB 、 100GB
ストレージネットワーク	BLOB ストレージ用の IP Network Nexus 9K		
	FC ： Cisco MDS 9132T		Cisco 9132T スイッチ × 2
ストレージ	NetApp AFF A220 オールフラッシュストレージシステム	2 つの HA ペア	すべての MEDITECH ワークロード（ファイルサーバ、イメージサーバ、SQL Server 、 VMware など）に対応する 2 ノードクラスタ
	DS224C ディスクシェルフ	DS224C ディスクシェルフ × 1	
	SSD の場合	3.8TB × 13	

次の表は、大規模な（カテゴリ 6 の）構成例 - インフラコンポーネントを示しています。

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
コンピューティング	Cisco UCS 5108 シャーシ	1.	
	Cisco シャーシ I/O モジュール	2 x 2208	10 GB アップリンクポート x 8
	Cisco UCS ブレードサーバ	B200 M5 × 8	各構成には、 2 x 24 コア、 2.7GHz および 768GB BIOS 3.2 （ 3# ）が搭載されています。
	Cisco UCS 仮想インターフェイスカード（ VIC ）	UCS 1440 VIC × 8	VMware ESXi fnic FC ドライバ： 1.0.47 VMware ESXi eNIC イーサネットドライバ： 1.0.27.0 （ Interoperability Matrix を確認してください）
	Cisco UCS ファブリックインターコネクト（ FI ） × 2	UCS 6454 FI × 2	10GB / 25Gb / 100Gb イーサネットおよび 32Gb FC をサポートする第 4 世代ファブリックインターコネクト
ネットワーク	Cisco イーサネットスイッチ	Nexus 9336c-FX2 × 2	Cisco Nexus 9332PQ1 、 10GB 、 25GB 、 40GB 、 100GB × 2
ストレージネットワーク	BLOB ストレージ用の IP ネットワーク N9k		
	FC ： Cisco MDS 9132T		Cisco 9132T スイッチ × 2
ストレージ	AFF A300	1 つの HA ペア	すべての MEDITECH ワークロード（ファイルサーバ、イメージサーバ、 SQL Server 、 VMware など）に対応する 2 ノードクラスタ
	DS224C ディスクシェルフ	DS224C ディスクシェルフ × 1	
	SSD の場合	3.8TB × 19	

これらの構成は、サイジングのガイダンスの開始点となります。一部のお客様の環境で、 MEDITECH の本番ワークロードと MEDITECH 以外のワークロードが同時に実行されている場合や、 IOP 要件が高い場合があります。ネットアップアカウントチームと協力して、必要な IOPS 、ワークロード、容量に基づいてストレージシステムのサイジングを行い、ワークロードに対応するプラットフォームを決定する必要があります。

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、次のドキュメントまたは Web サイトを参照してください。

- FlexPod データセンターと FC の Cisco Validated Design の 2 つの機能があります

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- MEDITECH 環境向けのネットアップ導入ガイドライン

  "https://fieldportal.netapp.com/content/248456" （ネットアップログインが必要）

- MEDITECH 環境向けのネットアップサイジングガイドライン

  "www.netapp.com/us/media/tr-4190.pdf"

- Epic EHR 導入向け FlexPod データセンター

  "www.netapp.com/us/media/tr-4693.pdf"

- FlexPod 設計ゾーン

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

- AFF DC と FC ストレージ（ MDS スイッチ）では、 NetApp FlexPod 、 vSphere 6.5U1 、および Cisco UCS Manager を使用します

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- シスコの医療機関

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

謝辞

本ガイドの執筆および作成には、以下の方々が協力していただきました。

- Brandon AGEE 、テクニカルマーケティングエンジニア、ネットアップ
- ネットアップ、ヘルスケア、ソリューションアーキテクト、 John Duignan 氏
- ネットアップ、プロダクトマネージャー、 Ketan Mota
- Cisco Systems, Inc 、テクニカルソリューションアーキテクト、 Jon Ebmeier 氏
- シスコシステムズ、プロダクトマネージャ、 Mike Brennan 氏

FlexPod Datacenter for MEDITECH 導入ガイド

TR-4753 ：『 FlexPod Datacenter for MEDITECH Deployment Guide 』

Brandon AGEE と John Duignan 氏、 NetApp Mike Brennan 氏、 Cisco の Jon Ebmeier 氏

協力：

解決策の全体的なメリット

FlexPod アーキテクチャ基盤で MEDITECH 環境を運用することで、医療機関はスタッフの生産性向上と設備投資と運用コストの削減を期待できます。FlexPod Datacenter for MEDITECH には、医療業界に特化した次のようなメリットがあります。

- * 運用の簡素化とコストの削減 * レガシー・プラットフォームのコストと複雑さを解消するには、より効率的でスケーラブルな共有リソースを使用します。この共有リソースは、どこにいても臨床医をサポートできます。この解決策は、リソースの使用率を高め、投資回収率（ ROI ）を向上させます。
- * インフラストラクチャの迅速な導入。 * 既存のデータセンターでも、リモートサイトでも、 FlexPod データセンターの統合されたテスト済みの設計により、新しいインフラストラクチャを短時間で稼働させることができ、手間を減らすことができます。
- * 認定ストレージ。 NetApp ONTAP 認定データ管理ソフトウェアと MEDITECH を組み合わせることで、テスト済みの認定済みストレージベンダーの優れた信頼性を実現できます。MEDITECH では他のインフラコンポーネントを認定していません。
- * スケールアウトアーキテクチャ。 * 実行中のアプリケーションを再構成することなく、 SAN と NAS をテラバイト（ TB ）から数十ペタバイト（ PB ）に拡張できます。
- * ノンストップオペレーション。 * ストレージの保守、ハードウェアのライフサイクル処理、 FlexPod のアップグレードを、ビジネスを中断することなく実行できます。
- * セキュアマルチテナンシー。 * 仮想化されたサーバおよびストレージ共有インフラストラクチャのニーズの増大をサポートし、特にシステムが複数のデータベースおよびソフトウェアのインスタンスをホストしている場合に、施設固有の情報のセキュアマルチテナンシーを実現します。
- * プールされたリソースの最適化。 * パフォーマンスを向上させながら、物理サーバとストレージコントローラの数を削減し、ワークロードの負荷を分散し、使用率を向上させます。
- * サービス品質（ QoS ）。 * FlexPod は、スタック全体で QoS を提供します。業界をリードする QoS ネットワーク、コンピューティング、ストレージのポリシーにより、共有環境で差別化されたサービスレベルを実現できます。これらのポリシーを使用することで、ワークロードに最適なパフォーマンスを提供し、過負荷のアプリケーションを分離および制御できます。
- * ストレージ効率。 * でストレージコストを削減 "ネットアップは 7 分の 1 のストレージ容量削減を保証します"。
- * 俊敏性。 * FlexPod システムが提供する業界をリードするワークフロー自動化、オーケストレーション、管理ツールにより、 IT チームはビジネス要求への対応力を大幅に高めることができます。これらのビジネス・リクエストは 'MEDITECH のバックアップ / プロビジョニング環境や ' テスト / トレーニング環境のプロビジョニングから ' 人口健康管理イニシアティブの分析データベースのレプリケーションまで多岐にわたります
- * 生産性の向上。 * この解決策を迅速に導入して拡張し、臨床家のエンドユーザー体験を最適化します。
- * ネットアップデータファブリック：ネットアップデータファブリックアーキテクチャは、サイト間、物理的な境界を越えてアプリケーション間でデータを結び付けます。ネットアップデータファブリックは、Data-Centric の世界におけるデータ主体の企業向けに構築されています。データは作成され、複数の場所で使用されます。多くの場合、データを利用して他の場所、アプリケーション、インフラと共有する必要があります。整合性があり統合されたデータを管理する方法が必要です。データファブリックでは、 IT を管理し、増え続ける IT の複雑さを軽減するデータ管理の方法が提供されます。

FlexPod

MEDITECH EHR 向けの新しいインフラアプローチ

医療機関では、業界をリードする MEDITECH 電子カルテ（ EHR ）への多額の投資からメリットを最大限に引き出す必要があります。ミッションクリティカルなアプリケーションの場合、お客様が MEDITECH ソリューション用のデータセンターを設計する際に、データセンターアーキテクチャに関する次の目標を特定することがよくあります。

- MEDITECH アプリケーションの高可用性
- ハイパフォーマンス
- MEDITECH をデータセンターに容易に導入できます
- MEDITECH の新しいリリースやアプリケーションでビジネスの成長を可能にする即応性と拡張性
- コスト効率
- MEDITECH のガイダンスとターゲット・プラットフォームに対応
- 管理性、安定性、および容易なサポート
- 堅牢なデータ保護、バックアップ、リカバリ、ビジネス継続性

MEDITECH のユーザが組織を変革して担当責任ある医療機関になり、条件が厳しく、バンドルされた償還モデルに適応するようにすると、より効率的で即応性に優れた IT デリバリモデルで必要な MEDITECH インフラを提供するという課題が生じます。

検証済みの統合インフラがもたらす価値

MEDITECH は、予測可能な低レイテンシのシステムパフォーマンスと高可用性を実現するための包括的な要件を備えているため、お客様のハードウェア要件に対応するように規定されています。

FlexPod は、 Cisco とネットアップの戦略的パートナーシップにより、検証済みで厳格にテストされた統合インフラです。予測可能な低レイテンシのシステムパフォーマンスと高可用性を実現するように特別に設計されています。このアプローチにより、 MEDITECH へのコンプライアンスが実現し、最終的に MEDITECH システムのユーザに最適な応答時間が提供されます。

Cisco とネットアップが提供する FlexPod 解決策は、高性能でモジュラ型の検証済み統合型仮想化ソリューションで、 MEDITECH のシステム要件を満たしています。 効率性、拡張性、コスト効率に優れたプラットフォーム。次の機能を提供します

- * モジュラーアーキテクチャ * FlexPod は、特定のワークロードごとに専用構成された FlexPod プラットフォームを使用して、 MEDITECH モジュラーアーキテクチャのさまざまなニーズに対応します。すべてのコンポーネントは、クラスタ化されたサーバ、ストレージ管理ファブリック、統合された管理ツールセットを通じて接続されます。
- * 統合スタックの各レベルで業界をリードするテクノロジ。 * Cisco 、ネットワーキング、ストレージ、オペレーティングシステムの各カテゴリにおいて、業界アナリストは、 Cisco 、 NetApp 、 VMware 、 Microsoft Windows のいずれも第 1 位または第 2 位にランクされています。
- * 標準化された柔軟な IT による投資保護 * FlexPod リファレンス・アーキテクチャでは、新しい製品バージョンとアップデートを予測し、今後のテクノロジーが利用可能になったときに対応できるよう、継続的な厳格な相互運用性テストを実施します。
- * 幅広い環境に導入されていることが実証されています。 * 広く普及しているハイパーバイザ、オペレーティング・システム、アプリケーション、インフラストラクチャ・ソフトウェアとの事前テストと共同検

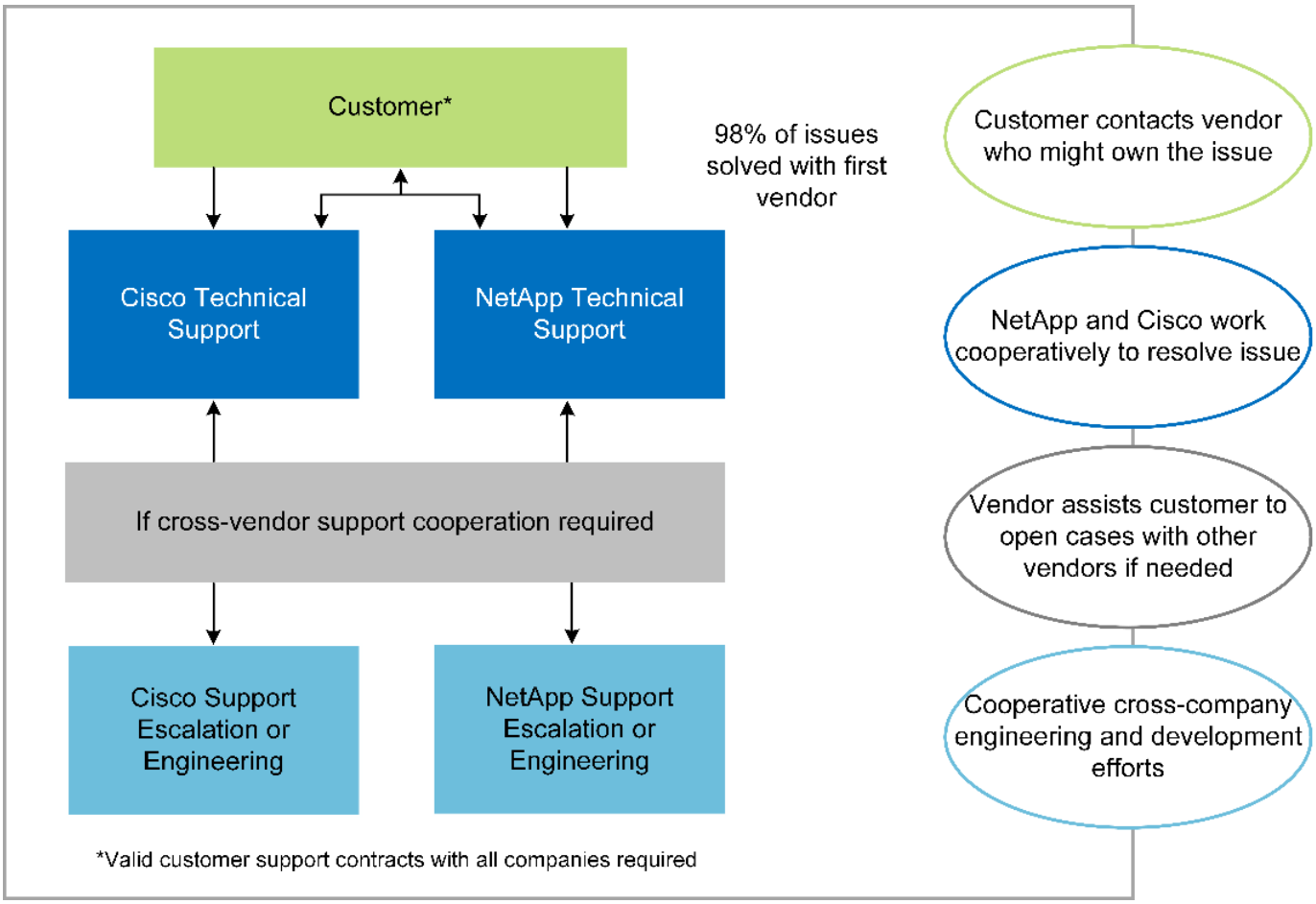
証が行われており、 FlexPod は複数の MEDITECH のお客様組織にインストールされています。

実証済みの **FlexPod** アーキテクチャと共同サポート

FlexPod は、実績のあるデータセンター解決策です。柔軟性に優れた共有インフラを提供します。パフォーマンスに悪影響を及ぼすことなく、増大するワークロードのニーズに容易に対応できるように拡張できます。この解決策は、 FlexPod アーキテクチャを活用することで、次のような FlexPod のメリットをフルに活用できます。

- * MEDITECH のワークロード要件に対応するパフォーマンス。 * MEDITECH ハードウェア構成提案の要件に応じて、必要な I/O およびレイテンシの要件に合わせて異なる ONTAP プラットフォームを導入できます。
- * 臨床データの増加に容易に対応できる拡張性。 * 従来の制限なしに、仮想マシン（ VM ）、サーバ、ストレージ容量をオンデマンドで動的に拡張できます。
- * 効率性の向上。 * 統合仮想化インフラストラクチャにより、管理時間と TCO の両方を削減できます。これにより、管理が容易になり、データをより効率的に保存できるようになり、 MEDITECH ソフトウェアのパフォーマンスが向上します。
- * リスクを軽減。 * 導入による憶測による導入を排除し、継続的なワークロードの最適化に対応する、定義済みのアーキテクチャを基盤とした検証済みプラットフォームにより、ビジネスの中断を最小限に抑えます。
- * FlexPod 共同サポート * ネットアップと Cisco は共同サポートを設立しました。共同サポートは、 FlexPod コンバージドインフラに固有のサポート要件を満たす、拡張性と柔軟性に優れた強力なサポートモデルです。このモデルでは、ネットアップと Cisco が提供する経験、リソース、およびテクニカルサポートの専門知識を組み合わせて、問題の発生場所に関係なく、 FlexPod サポート問題を特定して解決するための合理的なプロセスを提供します。FlexPod 共同サポートモデルを使用すると、お客様の FlexPod システムは効率的に動作し、最新のテクノロジを活用できます。また、経験豊富なチームと協力して、統合に関する問題の解決を支援します。

  FlexPod 共同サポートは、 FlexPod コンバージドインフラ上で MEDITECH などのビジネスクリティカルなアプリケーションを実行している医療機関にとって特に有効です。次の図に、 FlexPod 共同サポートモデルを示します。



これらのメリットに加えて、 MEDITECH 解決策を備えた FlexPod データセンタースタックの各コンポーネントは、 MEDITECH EHR ワークフローに特定のメリットをもたらします。

Cisco Unified Computing System の略

自己統合型の自己認識システムである Cisco Unified Computing System （ Cisco UCS ）は、統合 I/O インフラストラクチャと相互接続された単一の管理ドメインで構成されています。インフラで重要な患者情報を最大限に利用できるように、 MEDITECH 環境向け Cisco UCS は MEDITECH インフラに関する推奨事項とベストプラクティスに適合しています。

Cisco UCS アーキテクチャ上の MEDITECH の基盤となるのは Cisco UCS テクノロジで、統合システム管理、 Intel Xeon プロセッサ、サーバ仮想化が含まれています。これらの統合テクノロジは、データセンターの課題を解決し、 MEDITECH 向けデータセンター設計の目標達成に役立ちます。Cisco UCS は、 LAN 、 SAN 、およびシステム管理を 1 つのシンプルなリンクに統合して、ラックサーバ、ブレードサーバ、 VM に対応します。Cisco UCS は、シスコユニファイドファブリックおよび Cisco Fabric Extender Technology （ FEX テクノロジー）を組み込んだエンドツーエンドの I/O アーキテクチャで、 Cisco UCS のすべてのコンポーネントを単一のネットワークファブリックおよび単一のネットワークレイヤで接続します。

システムは、複数のブレードシャーシ、ラックサーバ、ラック、およびデータセンターに統合して拡張できる単一または複数の論理ユニットとして導入できます。このシステムは徹底的に簡素化されたアーキテクチャを実装しており、従来のブレードサーバシャーシとラックサーバに搭載された複数の冗長デバイスを排除します。従来のシステムでは、イーサネットアダプタや FC アダプタ、シャーシ管理モジュールなどの冗長デバイスは、レイヤを複雑にします。Cisco UCS は、単一の管理ポイントを提供する Cisco UCS Fabric Interconnect （ FI ）の冗長ペアで構成され、すべての I/O トラフィックを単一の制御ポイントで制御します。

Cisco UCS では、サービスプロファイルを使用して、 Cisco UCS インフラストラクチャ内の仮想サーバが正しく設定されるようにします。サービスプロファイルは、各分野の専門家によって一度作成されたネットワーク、ストレージ、およびコンピューティングポリシーで構成されます。サービスプロファイルには、 LAN および SAN アドレッシング、 I/O 設定、ファームウェアバージョン、ブート順、ネットワーク仮想 LAN （ VLAN ）、物理ポート、 QoS ポリシーなど、サーバ ID に関する重要なサーバ情報が含まれます。サービスプロファイルは、数時間や数日単位ではなく、システム内の任意の物理サーバに動的に作成して関連付けることができます。サービスプロファイルと物理サーバの関連付けは、シンプルな単一の操作として実行され、物理的な設定変更を必要とせずに、環境内のサーバ間でアイデンティティを移行できます。撤去したサーバの代わりに、ベアメタルプロビジョニングを迅速に実行できます。

サービスプロファイルを使用することで、企業全体で一貫したサーバ構成が可能になります。複数の Cisco UCS 管理ドメインが使用されている場合、 Cisco UCS Central はグローバルサービスプロファイルを使用して、ドメイン間で設定およびポリシー情報を同期できます。1 つのドメインでメンテナンスを実行する必要がある場合は、仮想インフラストラクチャを別のドメインに移行できます。このアプローチにより、単一ドメインがオフラインの場合でも、アプリケーションは高可用性で実行され続けます。

Cisco UCS がサーバ設定要件を満たしていることを実証するために、 MEDITECH では複数年にわたって広範なテストを実施しています。Cisco UCS は、 MEDITECH 製品リソースシステムサポートサイトに掲載されているサポート対象のサーバプラットフォームです。

シスコのネットワーク

Cisco Nexus スイッチと Cisco MDS マルチレイヤディレクタは、エンタープライズクラスの接続と SAN 統合を実現します。シスコのマルチプロトコルストレージネットワーキングは、 FC 、 Fibre Connection （ FICON ）、 FC over Ethernet （ FCoE ）、 SCSI over IP （ iSCSI ）、 FC over IP （ FCIP ）などの柔軟性とオプションを提供することで、ビジネスリスクを軽減します。

Cisco Nexus スイッチは、単一プラットフォームで最も包括的なデータセンターネットワーク機能セットの 1 つです。データセンターとキャンパスコアの両方で高いパフォーマンスと密度を実現します。また、耐障害性に優れたモジュラプラットフォームで、データセンターのアグリゲーション、行の終わり、およびデータセンターのインターコネクト環境に完全な機能セットを提供します。

Cisco UCS はコンピューティングリソースを Cisco Nexus スイッチと統合し、さまざまなタイプのネットワークトラフィックを識別して処理するユニファイド I/O ファブリックを提供します。このトラフィックには、ストレージ I/O 、デスクトップトラフィックのストリーミング、管理、臨床アプリケーションやビジネスアプリケーションへのアクセスが含まれます。次のようになります。

- * インフラストラクチャの拡張性。 * 仮想化、電力と冷却の効率化、自動化によるクラウドの拡張、高密度、およびハイパフォーマンスはすべて、効率的なデータセンターの拡張をサポートします。
- * 運用継続性。 * この設計では、ハードウェア、 NX-OS ソフトウェアの機能、および管理を統合して、ダウンタイムゼロの環境をサポートします。
- * ネットワークとコンピュータの QoS 。 * シスコは、ポリシーベースのサービスクラス（ CoS ）と QoS をネットワーク、ストレージ、およびコンピューティングファブリック全体に提供し、ミッションクリティカルなアプリケーションのパフォーマンスを最適化します。
- * 転送の柔軟性。 * コスト効率の高い解決策を使用して、新しいネットワークテクノロジーを段階的に導入します。

Cisco UCS と Cisco Nexus スイッチおよび Cisco MDS マルチレイヤディレクタを組み合わせることで、 MEDITECH に最適なコンピューティング、ネットワーク、 SAN 接続の解決策を提供できます。

NetApp ONTAP

ONTAP ソフトウェアを実行するネットアップストレージなら、ストレージの総コストを削減できるだけでなく、 MEDITECH のワークロードに必要な低レイテンシの読み取り / 書き込み応答時間と IOPS を実現できます。ONTAP はオールフラッシュストレージとハイブリッドストレージの両方の構成をサポートしているため、 MEDITECH の要件に最適なストレージプラットフォームを構築できます。NetApp のフラッシュ・アクセラレーション対応システムは、 MEDITECH の検証と認定を受けており、 MEDITECH のお客様は、レイテンシの影響を受けやすい MEDITECH の運用にとって重要なパフォーマンスと応答性を得ることができます。ネットアップシステムでは、 1 つのクラスタに複数の障害ドメインを作成することで、本番環境を非本番環境から分離することもできます。ネットアップのシステムでは、 ONTAP の QoS 機能によって、保証された最小パフォーマンスレベルでパフォーマンスの問題も軽減されます。

ONTAP ソフトウェアのスケールアウトアーキテクチャは、さまざまな I/O ワークロードに柔軟に対応できます。臨床アプリケーションで必要とされるスループットと低レイテンシを実現すると同時に、モジュラ型のスケールアウトアーキテクチャを提供するために、通常は ONTAP アーキテクチャで使用されます。NetApp AFF ノードは、ハイブリッド（ HDD およびフラッシュ）ストレージノードと同じスケールアウトクラスタに混在させることができます。このストレージノードは、高スループットで大規模なデータセットを格納するのに適しています。MEDITECH 認定のバックアップ解決策と併用すれば、高価なソリッドステートドライブ（ SSD ）ストレージから他のノード上の HDD ストレージに MEDITECH 環境のクローンを作成し、複製し、バックアップを実行できます。このアプローチは 'SAN ベースのクローン作成および本番プールのバックアップに関する MEDITECH のガイドラインに適合しているか ' それを超えています

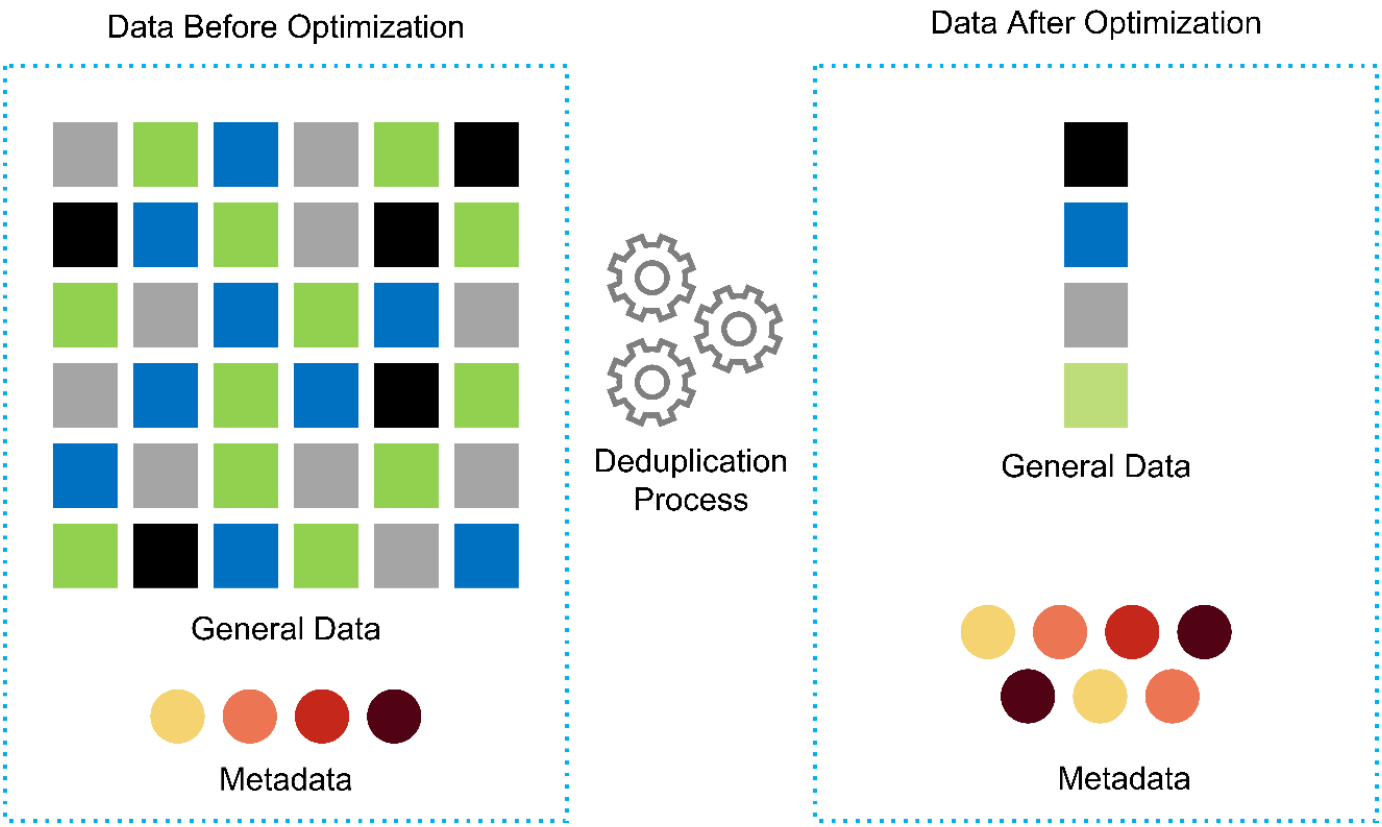
ONTAP 機能の多くは、 MEDITECH 環境で特に役立ちます。管理の簡易化、可用性と自動化の向上、必要なストレージの総容量の削減などです。これらの機能により、次のことが可能になります。

- * 卓越したパフォーマンス。 * NetApp AFF 解決策は、統合ストレージアーキテクチャ、 ONTAP ソフトウェア、管理インターフェイス、充実したデータサービス、その他の NetApp FAS 製品ファミリーに搭載されている高度な機能セットを共有しています。オールフラッシュメディアと ONTAP を組み合わせたこの革新的なソリューションは、業界をリードする ONTAP ソフトウェアの品質を活かして、オールフラッシュストレージの一貫した低レイテンシと高 IOPS を実現します。
- * Storage Efficiency 。 * 重複排除、 NetApp FlexClone データレプリケーションテクノロジ、インライン圧縮、インラインコンパクション、シンレプリケーション、シンプロビジョニング、 アグリゲートの重複排除

  ネットアップの重複排除機能は、 NetApp FlexVol またはデータ構成要素でブロックレベルの重複排除を実行します。重複排除機能は、基本的に、重複ブロックを削除して、 FlexVol またはデータ構成要素内で一意のブロックのみを保存します。

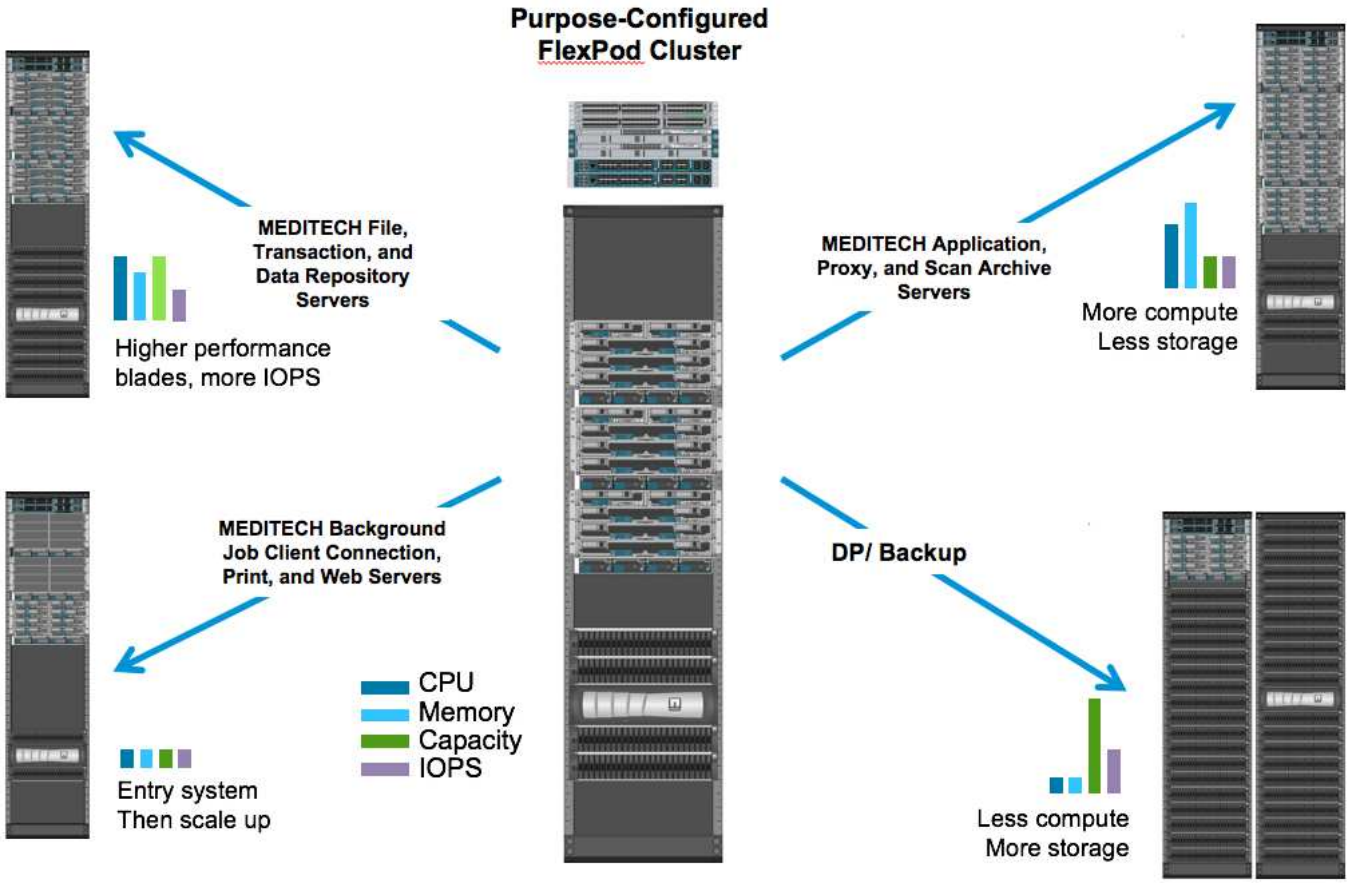
  重複排除は非常にきめ細かな単位で機能し、 FlexVol またはデータ構成要素のアクティブファイルシステムで機能します。透過的なアプリケーションであるため、ネットアップシステムを使用するすべてのアプリケーションのデータに対して重複排除を実行できます。ボリュームの重複排除はインラインプロセスとして実行できます（ ONTAP 8.3.2 以降）。また、自動実行やスケジュール設定による実行、または CLI 、 NetApp ONTAP System Manager 、 NetApp Active IQ Unified Manager を使用した手動実行を設定するバックグラウンドプロセスとして実行することもできます。

  次の図に、ネットアップの重複排除機能の仕組みを示します。



- * スペース効率に優れたクローニング。 * FlexClone 機能により、クローンをほぼ瞬時に作成し、バックアップとテストの環境更新をサポートできます。これらのクローンは、変更が加えられるとストレージのみを消費します。
- * ネットアップの Snapshot テクノロジと SnapMirror テクノロジ。 * ONTAP を使用すると、 MEDITECH ホストで使用されている論理ユニット番号（ LUN ）のスペース効率に優れた Snapshot コピーを作成できます。デュアルサイト環境では、 SnapMirror ソフトウェアを実装して、データレプリケーションと耐障害性を強化できます。
- * 統合されたデータ保護。 * 完全なデータ保護と災害復旧機能により、重要なデータ資産を保護し、災害復旧を実現します。
- * ノンストップオペレーション。 * データをオフラインにすることなく、アップグレードとメンテナンスを実行できます。
- * QoS とアダプティブ QoS （ AQoS ）。 * ストレージ QoS により、潜在的な影響源のワークロードを制限できます。さらに重要なのは、 QoS によって MEDITECH の本番環境などの重要なワークロードに最低限のパフォーマンスを保証できることです。ネットアップの QoS は、競合を制限することでパフォーマンス関連の問題を軽減します。AQoS は、ボリュームに直接適用できる事前定義されたポリシーグループと連携します。これらのポリシーグループを使用すると、スループットの上限や下限をボリュームサイズに自動的に調整し、ボリュームサイズが変わっても容量に対する IOPS とギガバイトの比率を維持できます。
- * ネットアップデータファブリック。 * ネットアップデータファブリックは、クラウド環境とオンプレミス環境全体でデータ管理を簡易化、統合することで、デジタル変革を加速します。データ管理のための一貫した統合的サービスとアプリケーションを提供することで、データの可視性と分析、データのアクセスと制御、データの保護とセキュリティを実現します。ネットアップは Amazon Web Services （ AWS ）、 Azure 、 Google Cloud Platform 、 IBM Cloud クラウドと統合されているため、幅広い選択肢を提供します。

次の図は、 MEDITECH ワークロード向けの FlexPod アーキテクチャを示しています。



MEDITECH の概要

Medical Information Technology, Inc. （別名 MEDITECH ）は、医療機関向けの情報システムを提供するマサチューセッツ州のソフトウェア企業です。MEDITECH は EHR システムを提供しています。このシステムは最新の患者データを保存して整理し、臨床スタッフにデータを提供するように設計されています。患者データには、人口統計、病歴、投薬、検査結果が含まれますが、これらに限定されません。 放射線画像、年齢、身長、体重などの個人情報。

MEDITECH ソフトウェアがサポートする幅広い機能については、このドキュメントでは説明していません。付録 A では ' これらの広範な MEDITECH 機能の詳細について説明していますMEDITECH アプリケーションでは、これらの機能をサポートするために複数の VM が必要です。これらのアプリケーションを導入するには、 MEDITECH の推奨事項を参照してください。

ストレージシステムの観点から見た各導入では、すべての MEDITECH ソフトウェアシステムに、患者主体の分散データベースが必要です。MEDITECH には独自のデータベースがあり、 Windows オペレーティング・システムが使用されています。

bridgehead と Commvault は、ネットアップと MEDITECH の両方の認定を受けた 2 つのバックアップソフトウェアアプリケーションです。本ドキュメントでは、これらのバックアップアプリケーションの導入については説明していません。

本ドキュメントの主な目的は、 FlexPod スタック（サーバとストレージ）が、 EHR 環境の MEDITECH データベースとバックアップ要件に対応できるようにすることです。

特定の MEDITECH ワークロードに特化して設計されています

MEDITECH では、サーバ、ネットワーク、ストレージハードウェア、ハイパーバイザー、オペレーティングシステムは再販できません。 ただし、インフラスタックのコンポーネントごとに固有の要件があります。そのため、 Cisco とネットアップは、お客様の MEDITECH 本番環境の要件に対応できるように、 FlexPod データセンターのテストと構成、導入、サポートを共同で実施しました。

MEDITECH のカテゴリ

MEDITECH では、展開サイズをカテゴリ番号 1 ～ 6 に関連付けます。カテゴリ 1 は MEDITECH の導入規模が最小で、カテゴリ 6 は MEDITECH の導入規模が最大です。

MEDITECH ホストの I/O 特性とパフォーマンス要件については、ネットアップを参照してください "TR-4190 ：『 NetApp Sizing Guidelines for MEDITECH Environments 』"。

MEDITECH プラットフォーム

MEDITECH 拡張プラットフォームは最新バージョンの EHR ソフトウェアです。それよりも前の MEDITECH プラットフォームは、 Client/Server 5.x と Magic です。このセクションでは、 MEDITECH ホストとそのストレージ要件に関連する MEDITECH プラットフォーム（拡張、 6.x 、 C/S 5.x 、 Magic に適用可能）について説明します。

上記のすべての MEDITECH プラットフォームで ' 複数のサーバで MEDITECH ソフトウェアを実行し ' さまざまなタスクを実行します前の図は ' アプリケーション・データベース・サーバやその他の MEDITECH サーバとして動作する MEDITECH ホストなど ' 一般的な MEDITECH システムを示していますその他の MEDITECH サーバには ' データ・リポジトリ・アプリケーション ' スキャン / アーカイブ・アプリケーション ' バックグラウンド・ジョブ・クライアントなどがありますその他の MEDITECH サーバの完全なリストについては、『 Hardware Configuration Proposal 』（新規導入の場合）および『 Hardware Evaluation Task 』（既存の導入の場合）を参照してください。これらのドキュメントは、 MEDITECH システムインテグレータ、または MEDITECH テクニカルアカウントマネージャ（ TAM ）から MEDITECH を介して入手できます。

MEDITECH ホスト

MEDITECH ホストはデータベース・サーバですこのホストは 'MEDITECH ファイル・サーバ（拡張版 '6.x' または C/S 5.x プラットフォーム用）または Magic マシン（ Magic プラットフォーム用）とも呼ばれますこのドキュメントでは MEDITECH ホストという用語を MEDITECH ファイルサーバまたは Magic マシンを指します

MEDITECH ホストには、 Microsoft Windows Server オペレーティング・システム上で稼働している物理サーバまたは VM を使用できます。ほとんどの場合、 MEDITECH ホストは VMware ESXi サーバ上で実行される Windows VM として導入されます。本ドキュメントの執筆時点で、 VMware は MEDITECH がサポートしている唯一のハイパーバイザーです。MEDITECH ホストのプログラム ' 辞書 ' データ・ファイルは 'Windows システム上の Microsoft Windows ドライブ（ドライブ E など）に保存されます

仮想環境では、 Windows E ドライブは、物理互換モードで raw デバイスマッピング（ RDM ）を使用して VM に接続された LUN に配置されます。このシナリオでは、仮想マシンディスク（ VMDK ）ファイルを Windows E ドライブとして使用することは、 MEDITECH ではサポートされていません。

MEDITECH ホスト・ワークロードの I/O 特性

各 MEDITECH ホストとシステム全体の I/O 特性は ' 導入する MEDITECH プラットフォームによって異なりますMEDITECH プラットフォーム（拡張、 6.x 、 C/S 5.x 、および Magic ）はすべて、 100% ランダムワークロードを生成します。

MEDITECH 拡張プラットフォームでは、書き込み処理の割合が最も高く、ホストあたりの総 IOPS が最も高く、その後に 6.x 、 C/S 5.x 、 Magic プラットフォームが続くため、要件が最も厳しいワークロードが生成されます。

MEDITECH ワークロードの説明の詳細については、を参照してください "TR-4190 ：『 NetApp Sizing Guidelines for MEDITECH Environments 』"。

ストレージネットワーク

MEDITECH を使用するには、 NetApp FAS または AFF システムと MEDITECH ホストの全カテゴリのデータトラフィックに FC プロトコルを使用する必要があります。

MEDITECH ホスト用のストレージプレゼンテーション

MEDITECH ホストごとに 2 つの Windows ドライブが使用されている：

- * ドライブ C* このドライブには 'Windows Server オペレーティング・システムと MEDITECH ホスト・アプリケーション・ファイルが格納されています
- * ドライブ E. * MEDITECH ホストは Windows Server オペレーティングシステムのドライブ E にプログラム、辞書、データファイルを保存します。ドライブ E は、ネットアップの FAS または AFF システムから FC プロトコルを使用してマッピングされる LUN です。MEDITECH を使用するには、 MEDITECH ホストの IOPS 要件と読み取り / 書き込みレイテンシ要件が満たされていることが必要です。

ボリュームと **LUN** の命名規則

MEDITECH では ' すべての LUN に特定の命名規則を使用する必要があります

ストレージを導入する前に、 MEDITECH ハードウェア構成提案書で LUN の命名規則を確認してください。MEDITECH のバックアップ・プロセスでは ' ボリュームと LUN の命名規則に基づいて ' バックアップする特定の LUN を適切に識別します

包括的な管理ツールと自動化機能

Cisco UCS と **Cisco UCS Manager**

シスコは、シンプル化、セキュリティ、拡張性という 3 つの主要な要素を重視して、優れたデータセンターインフラストラクチャを提供しています。Cisco UCS Manager ソフトウェアとプラットフォームのモジュール性を組み合わせることで、簡素化され、セキュアでスケーラブルなデスクトップ仮想化プラットフォームを実現できます。

- * シンプル。 * Cisco UCS は、業界標準のコンピューティングに対する抜本的な新しいアプローチを提供し、すべてのワークロードに対応するデータセンターインフラストラクチャのコアを提供します。Cisco UCS には、必要なサーバ数の削減や、サーバごとに使用するケーブル数の削減など、多数の機能とメリットがあります。もう 1 つの重要な機能は、 Cisco UCS サービスプロファイルを使用してサーバを迅速に導入または再プロビジョニングする機能です。サーバやアプリケーションのワークロードのプロビジョニングを合理化することで、管理対象のサーバやケーブルを減らすことができ、運用が簡素化されます。Cisco UCS Manager サービスプロファイルを使用すると、ブレードサーバとラックサーバの数を数分でプロビジョニングできます。Cisco UCS サービスプロファイルにより、サーバ統合のランブックが排除され、設定のずれが解消されます。このアプローチにより、エンドユーザの生産性向上、ビジネスの俊敏性の向上、 IT リソースの他のタスクへの割り当てが可能になります。

  Cisco UCS Manager は、サーバ、ネットワーク、ストレージアクセスインフラの設定やプロビジョニングなど、エラーを発生させやすい多くのデータセンター運用を自動化します。また、 Cisco UCS B シリ

ーズブレードサーバと C シリーズラックサーバには、メモリフットプリントが大きいため、アプリケーションの密度が高くなり、サーバインフラストラクチャ要件の軽減に役立ちます。

これにより、 MEDITECH インフラの導入が高速化され、成功を収められるようになります。

- * セキュア * 仮想マシンは、従来の物理マシンよりも本質的に安全性が高くなっていますが、新たなセキュリティ上の課題が生じています。仮想デスクトップなどの共通インフラストラクチャを使用するミッションクリティカルな Web サーバおよびアプリケーションサーバは、セキュリティの脅威に対するリスクが高くなっています。VM 間トラフィックには、セキュリティに関する重要な考慮事項があります。これは、 VMware vMotion を使用する VM がサーバインフラストラクチャ間で移動する動的な環境では特に、IT 管理者が対処する必要があることを意味します。

  そのため、仮想化は、特に拡張コンピューティングインフラストラクチャ全体で VM モビリティの動的かつ流動的な性質を考慮すると、ポリシーとセキュリティに対する VM レベルの認識の必要性を大幅に高めます。新しい仮想デスクトップを簡単に拡張できることは、仮想化対応のネットワークおよびセキュリティインフラストラクチャの重要性をさらに高めます。デスクトップ仮想化のための Cisco データセンターインフラストラクチャ（ Cisco UCS 、 Cisco MDS 、および Cisco Nexus ファミリソリューション）は、強力なデータセンター、ネットワーク、およびデスクトップセキュリティを提供し、デスクトップからハイパーバイザまで、包括的なセキュリティを提供します。セキュリティは、仮想デスクトップのセグメンテーション、 VM 対応のポリシーと管理、および LAN および WAN インフラストラクチャ全体のネットワークセキュリティによって強化されます。

- * 拡張性。 * 仮想化ソリューションの成長はすべて避けられないため、解決策はその成長に合わせて拡張でき、予測どおりに拡張できる必要があります。シスコの仮想化ソリューションは、高い仮想マシン密度（サーバあたりの VM 数）をサポートし、ほぼリニアなパフォーマンスでより多くのサーバを拡張できます。シスコのデータセンターインフラストラクチャは、成長のための柔軟なプラットフォームを提供し、ビジネスの俊敏性を向上させます。Cisco UCS Manager サービスプロファイルを使用すると、ホストのプロビジョニングをオンデマンドで実行できるため、数十台のホストを導入する場合でも、数百台のホストを簡単に導入できます。

  Cisco UCS サーバは、ほぼリニアなパフォーマンスと拡張性を提供します。Cisco UCS は、特許取得済みの Cisco 拡張メモリテクノロジーを実装して、ソケット数が少ない大容量のメモリを提供します（ 2 ソケットおよび 4 ソケットサーバで最大 1 TB のメモリ拡張性を実現）。ユニファイドファブリックテクノロジーをビルディングブロックとして使用することで、 Cisco UCS サーバの総帯域幅をサーバあたり 80 Gbps まで拡張でき、ノースバウンド Cisco UCS ファブリックインターコネクトはラインレートで 2Tbps を出力できます。この機能により、デスクトップ仮想化の I/O およびメモリのボトルネックを防止できます。高性能で低遅延のユニファイドファブリックベースのネットワーキングアーキテクチャを備えた Cisco UCS は、高解像度のビデオトラフィックや通信トラフィックなど、大量の仮想デスクトップトラフィックをサポートします。また、 FlexPod は、 ONTAP 仮想化ソリューションの一部として、ブートストームおよびログインストーム時にデータの可用性と最適なパフォーマンスを維持します。

  Cisco UCS 、 Cisco MDS 、および Cisco Nexus データセンターインフラストラクチャ設計は、成長に最適なプラットフォームです。サーバ、ネットワーク、ストレージのリソースを透過的に拡張して、デスクトップ仮想化、データセンターアプリケーション、クラウドコンピューティングをサポートできます。

VMware vCenter Server の各機能を使用し

VMware vCenter Server は、 MEDITECH 環境を管理するための一元化されたプラットフォームを提供します。これにより、医療機関は仮想インフラを自動化し、安心して提供できます。

- * シンプルな導入。 * 仮想アプライアンスを使用して、 vCenter Server を迅速かつ簡単に導入できます。
- * 一元管理と可視性。 * VMware vSphere インフラストラクチャ全体を 1 か所から管理します。

- * プロアクティブな最適化。 * リソースを割り当てて最適化し、効率を最大限に高めます。
- * 管理。 * 強力なプラグインとツールを使用して、管理を簡素化し、制御を拡張します。

Virtual Storage Console for VMware vSphere

Virtual Storage Console （ VSC ）、 vSphere API for Storage Awareness （ VASA ） Provider 、および VMware vSphere for VMware vSphere は、ネットアップ製の単一の仮想アプライアンスを構成します。この製品スイートには、 vCenter Server のプラグインとして SRA と VASA Provider が含まれています。これらは、ネットアップストレージシステムを使用する VMware 環境で、 VM のエンドツーエンドのライフサイクル管理を実現します。

VSC 、 VASA Provider 、 SRA 仮想アプライアンスは VMware vSphere Web Client とシームレスに統合されており、 SSO サービスを使用できます。複数の VMware vCenter Server インスタンスがある環境では、管理する各 vCenter Server インスタンスに固有の VSC インスタンスが登録されている必要があります。VSC のダッシュボードページでは、データストアと VM の全体的なステータスを簡単に確認できます。

VSC 、 VASA Provider 、 SRA 仮想アプライアンスを導入すると、次のタスクを実行できます。

- * VSC を使用して、ストレージの導入と管理、 ESXi ホストの構成を行います。 * VSC を使用して、クレデンシャルの追加、削除、クレデンシャルの割り当て、 VMware 環境内のストレージコントローラのアクセス許可の設定を行うことができます。また、ネットアップストレージシステムに接続された ESXi サーバを管理することもできます。数回のクリックで、すべてのホストのホストタイムアウト、 NAS 、マルチパスに関する推奨されるベストプラクティス値を設定できます。ストレージの詳細を表示したり、診断情報を収集したりすることもできます。
- * ストレージ機能プロファイルの作成やアラームの設定には VASA Provider を使用します。 * VASA Provider for ONTAP は、 VASA Provider 拡張機能を有効にすると VSC に登録されます。ストレージ機能プロファイルと仮想データストアを作成して使用できます。また、アラームを設定して、ボリュームやアグリゲートがほぼいっぱいになったときに通知することもできます。仮想データストアに作成された VMDK および VM のパフォーマンスを監視できます。
- * SRA をディザスタリカバリに使用します。 * SRA を使用して、障害時のディザスタリカバリ用に、環境内の保護対象サイトとリカバリサイトを設定できます。

NetApp OnCommand Insight と ONTAP

NetApp OnCommand Insight は、インフラ管理を MEDITECH のサービス提供チェーンに統合します。このアプローチにより、医療機関は、ストレージ、ネットワーク、コンピューティングのインフラの管理、自動化、分析をより効率的に行うことができます。IT 部門は、現在のインフラを最適化して最大限のメリットを得られるようにすると同時に、購入するリソースや購入時期を簡単に判断できるようにします。また、複雑なテクノロジの移行に伴うリスクを軽減することもできます。エージェントが不要なため、インストールは簡単で、システムを停止する必要がありません。インストール済みのストレージデバイスと SAN デバイスは継続的に検出され、ストレージ環境全体を可視化するために詳細情報が収集されます。未使用の資産、ミスアライメント資産、利用率の低い資産、孤立した資産をすばやく特定し、将来の拡張に備えて再利用することができます。OnCommand Insight は、次のようなメリットを

- * 既存のリソースを最適化。 * 活用されていない資産、利用率の低い資産、孤立した資産を特定するために、確立されたベストプラクティスを活用して、問題を回避し、サービスレベルを満たすことができます。
- * より的確な意思決定。 * リアルタイム・データにより、容量の問題をより迅速に解決し、将来の購入を正確に計画し、過剰支出を回避し、設備投資を先送りすることができます。
- * IT イニシアチブを加速 * 仮想環境をよりよく理解し、リスク管理、ダウンタイムの最小化、クラウド導入の高速化を支援します。

設計

MEDITECH 向け FlexPod のアーキテクチャは、 MEDITECH 、 Cisco 、 NetApp のガイダンスや、 MEDITECH をご利用のお客様とあらゆる規模のお客様との連携に関するパートナー様の経験に基づいています。アーキテクチャは柔軟性に優れており、データセンターの戦略、組織の規模、システムの一元化、分散化、マルチテナント環境に応じて、 MEDITECH のベストプラクティスを適用できます。

適切なストレージアーキテクチャは、合計 IOPS を使用した全体的なサイズによって決まります。パフォーマンスだけを重視するわけではなく、お客様の追加の要件に基づいて、より大きなノード数を使用する場合もあります。ネットアップストレージを使用する利点は、要件の変化に応じてクラスタを無停止で簡単にスケールアップできることです。また、機器の転用や機器の更新時に、ノードをクラスタから無停止で削除することもできます。

NetApp ONTAP ストレージアーキテクチャのメリットには、次のようなものがあります。

- * システムを停止することなく簡単にスケールアップ / スケールアウトできます。 * ONTAP のノンストップオペレーション機能を使用して、ディスクとノードをアップグレード、追加、または削除できます。ノードは 4 つから始めて 6 つに移動することも、大容量のコントローラに無停止でアップグレードすることもできます。
- * Storage Efficiency 。 * 重複排除、 NetApp FlexClone 、インライン圧縮、インラインコンパクション、シンレプリケーションにより、必要な総容量を削減 シンプロビジョニング、およびアグリゲートの重複排除：FlexClone 機能を使用すると、バックアップおよびテスト環境の更新に対応するクローンをほぼ瞬時に作成できます。これらのクローンは、変更が加えられるとストレージのみを消費します。
- * 災害復旧シャドウ・データベース・サーバ * 災害復旧シャドウ・データベース・サーバは ' ビジネス継続性戦略の一部です（ストレージの読み取り専用機能をサポートし ' ストレージの読み取り / 書き込みインスタンスとして構成される可能性があります）したがって、 3 つ目のストレージシステムの配置とサイジングは、通常、本番環境のデータベースストレージシステムと同じです。
- * データベースの整合性（多少考慮が必要）。 * NetApp SnapMirror バックアップコピーをビジネス継続性に関連して使用する場合は、を参照してください "TR-3446 ：『非同期 SnapMirror ベストプラクティスガイド』"。

ストレージレイアウト

MEDITECH ホスト専用アグリゲート

MEDITECH の高パフォーマンスおよび高可用性要件を満たすための最初のステップは 'MEDITECH ホストの本番ワークロードを専用の高性能ストレージに分離するために 'MEDITECH 環境のストレージ・レイアウトを適切に設計することです

MEDITECH ホストのプログラムファイル、ディクショナリファイル、データファイルを格納するために、各ストレージコントローラに 1 つの専用アグリゲートをプロビジョニングする必要があります。他のワークロードが同じディスクを使用してパフォーマンスに影響しないように、それらのアグリゲートから他のストレージがプロビジョニングされることはありません。

> 他の MEDITECH サーバ用にプロビジョニングするストレージは、 MEDITECH ホストが使用する LUN 専用のアグリゲートに配置しないでください。他の MEDITECH サーバ用のストレージは別のアグリゲートに配置してください。その他の MEDITECH サーバのストレージ要件については、『 Hardware Configuration Proposal 』（新規導入の場合）および『 Hardware Evaluation Task 』（既存導入の場合）を参照してください。これらのドキュメントは、 MEDITECH システムインテグレータ、または MEDITECH テクニカルアカウントマネージャ（ TAM ）から MEDITECH を介して入手できます。ネットアップのソリューションエンジニアは、 NetApp MEDITECH Independent Software Vendor （ ISV ）チームと相談して、適切で包括的なネットアップストレージのサイジングを実施できます。

MEDITECH ホストのワークロードをすべてのストレージコントローラに均等に分散します

NetApp FAS システムと AFF システムは、 1 つ以上のハイアベイラビリティペアとして導入されます。MEDITECH の拡張機能と 6.x のワークロードを各ストレージコントローラに均等に分散し、各ストレージコントローラにコンピューティング、ネットワーク、キャッシングのリソースを適用することを推奨します。

MEDITECH のワークロードを各ストレージコントローラに均等に分散するには、次のガイドラインに従います。

- 各 MEDITECH ホストの IOPS がわかっている場合は、 MEDITECH の拡張ボリュームと 6.x のワークロードをすべてのストレージコントローラに均等に分散できるので、各コントローラが MEDITECH ホストから同じ数の IOPS を提供していることを確認できます。
- MEDITECH ホストごとに IOPS がわからない場合でも、 MEDITECH の拡張機能と 6.x のワークロードをすべてのストレージコントローラに均等に分散できます。MEDITECH ホストのアグリゲートの容量がすべてのストレージコントローラに均等に分散されていることを確認して、このタスクを完了します。これにより、 MEDITECH ホスト専用のすべてのデータアグリゲート間でディスク数が同じになります。
- 同様のディスクタイプと同一の RAID グループを使用して、両方のコントローラのストレージアグリゲートを作成し、ワークロードを均等に分散します。ストレージアグリゲートを作成する前に、 NetApp Certified Integrator にお問い合わせください。

> MEDITECH によると、 MEDITECH システムの 2 台のホストは他のホストよりも高い IOPS を生成します。この 2 つのホストの LUN は、別々のストレージコントローラに配置します。システムを導入する前に、 MEDITECH チームの支援を受けてこれら 2 つのホストを特定する必要があります。

ストレージ配置

MEDITECH ホスト用のデータベース・ストレージ

MEDITECH ホストのデータベース・ストレージは、 NetApp FAS または AFF システムからブロック・デバイス（ LUN ）として提供されます。通常、 LUN は E ドライブとして Windows オペレーティングシステムにマウントされます。

その他のストレージ

MEDITECH のホストオペレーティングシステムとデータベースアプリケーションは、通常はストレージにかなりの IOPS を生成します。MEDITECH のホスト VM とその VMDK ファイルのストレージプロビジョニングは、必要に応じて、 MEDITECH のパフォーマンスしきい値を満たすために必要なストレージとは別のものとみなされます。

他の MEDITECH サーバ用にプロビジョニングされたストレージは、 MEDITECH ホストが使用する LUN 専用のアグリゲートに配置しないでください。他の MEDITECH サーバ用のストレージを別のアグリゲートに配置します。

ストレージコントローラの構成

高可用性

コントローラ障害の影響を軽減し、ストレージシステムの無停止アップグレードを可能にするには、ハイアベイラビリティモードでコントローラを搭載したストレージシステムを設定する必要があります。

ハイアベイラビリティコントローラペア構成では、ディスクシェルフを複数のパスでコントローラに接続する必要があります。この接続は、シングルパス障害から保護することでストレージの耐障害性を高め、コントローラフェイルオーバーが発生した場合のパフォーマンスの一貫性を向上させます。

ストレージコントローラのフェイルオーバー中のストレージパフォーマンス

ハイアベイラビリティペアのコントローラで構成されたストレージシステムでは、コントローラに障害が発生した場合でも、パートナーコントローラが、障害が発生したコントローラのストレージリソースとワークロードを引き継ぎます。コントローラに障害が発生した場合に満たす必要があるパフォーマンス要件をお客様に確認し、それに応じてシステムのサイズを決定することが重要です。

ハードウェアアシストテイクオーバー

ネットアップでは、両方のストレージコントローラでハードウェアアシストテイクオーバー機能を有効にすることを推奨します。

ハードウェアアシストテイクオーバーは、ストレージコントローラのフェイルオーバーにかかる時間を最小限に抑えるように設計されています。1 台のコントローラの Remote LAN Module またはサービスプロセッサモジュールが、ハートビートタイムアウトトリガーよりも早くコントローラ障害についてパートナーに通知できるため、フェイルオーバーにかかる時間が短縮されます。ハードウェアアシストテイクオーバー機能は、ハイアベイラビリティ構成ではストレージコントローラに対してデフォルトで有効になります。

ハードウェアアシストテイクオーバーの詳細については、を参照してください "ONTAP 9 ドキュメンテーション・センター"。

ディスクタイプ

MEDITECH ワークロードに必要な読み取りレイテンシを抑えるために、 MEDITECH ホスト専用の AFF システムにアグリゲートを配置する場合は高性能の SSD を使用することを推奨します。

NetApp AFF

ネットアップは、高スループットが求められる MEDITECH ワークロードや、ランダムデータアクセスパターンや低レイテンシが求められる MEDITECH ワークロードに対応するハイパフォーマンス AFF アレイを提供しています。MEDITECH ワークロードに対応する AFF アレイは、 HDD ベースのシステムに比べてパフォーマンスに優れています。フラッシュテクノロジとエンタープライズデータ管理を組み合わせることで、パフォーマンス、可用性、ストレージ効率の 3 つの主要領域でメリットが得られます。

ネットアップのサポートツールおよびサービス

ネットアップでは、包括的なサポートツールとサービスを提供しています。NetApp AutoSupport ツールを有効にして、ハードウェア障害やシステム構成ミスが発生した場合にホームコールできるように NetApp AFF /

FAS システムで設定する必要があります。ホームアラートをネットアップサポートチームに連絡することで、問題を迅速に解決できます。NetApp Active IQ は、ネットアップシステムの AutoSupport 情報に基づいた Web ベースのアプリケーションです。予測に基づいてプロアクティブに分析情報を提供することで、可用性、効率性、パフォーマンスの向上を支援します。

導入と設定

概要

本ドキュメントでは、 FlexPod 導入に関するネットアップストレージのガイダンスに以下の内容を記載します。

- ONTAP を使用する環境
- Cisco UCS ブレードサーバとラックマウントサーバを使用する環境

本ドキュメントの内容は以下のとおりです。

- FlexPod データセンター環境の詳細な導入

  詳細については、を参照してください "FlexPod データセンターと FC の Cisco Validated Design の 2 つの機能があります" （ CVD ）。

- MEDITECH ソフトウェア環境、リファレンス・アーキテクチャ、統合に関するベスト・プラクティス・ガイダンスの概要

  詳細については、を参照してください "TR-4300i ：『 NetApp FAS and All-Flash Storage Systems for MEDITECH Environments Best Practices Guide 』" （ネットアップログインが必要です）。

- パフォーマンス要件とサイジングガイダンスを定量化

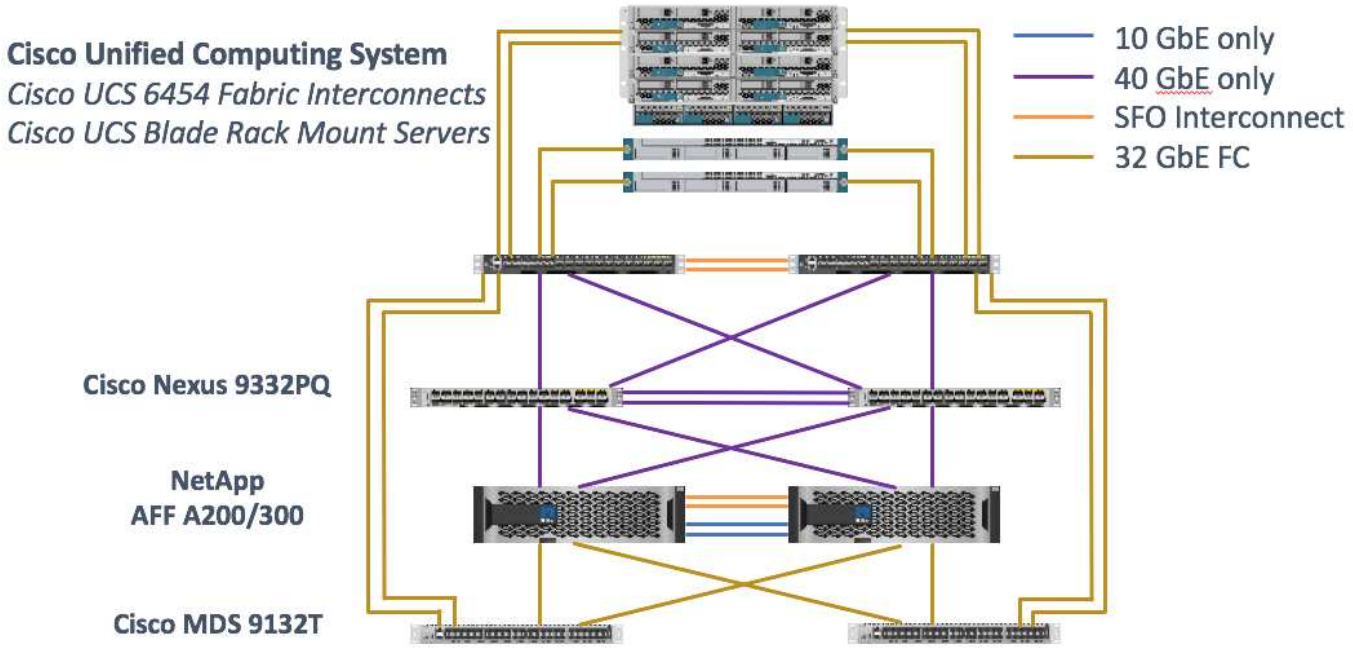
  詳細については、を参照してください "TR-4190 ：『 NetApp Sizing Guidelines for MEDITECH Environments 』"。

- バックアップとディザスタリカバリの要件を満たすためにネットアップの SnapMirror テクノロジを使用する。
- ネットアップストレージの一般的な導入ガイダンス

ここでは、インフラ導入のベストプラクティスを含む構成例を示し、インフラのハードウェア / ソフトウェアのさまざまなコンポーネントと使用可能なバージョンを示します。

ケーブル配線図

次の図は、 MEDITECH 環境の 32Gb FC / 40GbE トポロジを示しています。



必ずを使用してください "Interoperability Matrix Tool （ IMT ）" ソフトウェアとファームウェアのすべてのバージョンがサポートされていることを検証します。セクションの表 "MEDITECH のモジュールとコンポーネント" に、解決策テストで使用したインフラのハードウェアコンポーネントとソフトウェアコンポーネントを示します。

"次のステップ：基本インフラの構成。"

ベースインフラの構成

ネットワーク接続

インフラを設定する前に、次のネットワーク接続を確立しておく必要があります。

- ポートチャネルと仮想ポートチャネル（ vPC ）を使用するリンクアグリゲーションが全体的に使用され、帯域幅と高可用性を向上させる設計が可能になります。
  - vPC は、 Cisco FI スイッチと Cisco Nexus スイッチの間で使用されます。
  - 各サーバには、ユニファイドファブリックへの冗長接続を持つ仮想ネットワークインターフェイスカード（ vNIC ）があります。NIC フェールオーバーは、 FI 間で冗長性を確保するために使用されます。
  - 各サーバには仮想 Host Bus Adapter （ vHBA ）があり、ユニファイドファブリックに冗長接続されます。
- Cisco UCS FI は推奨されるエンドホストモードで設定され、アップリンクスイッチへの vNIC のダイナミックなピン接続を提供します。

ストレージ接続

インフラを設定する前に、次のストレージ接続を確立しておく必要があります。

- ストレージポートインターフェイスグループ（ ifgroups 、 vPC ）
- スイッチ N9K-A への 10Gb リンク

- スイッチ N9K-B への 10Gb リンク
- インバンド管理（アクティブ / パッシブボンド）：
  - 管理スイッチ N9K-A への 1GB リンク
  - 管理スイッチ N9K-B への 1GB リンク
- Cisco MDS スイッチを介した 32Gb FC のエンドツーエンド接続、単一イニシエータのゾーニング構成
- FC SAN は、ステートレスコンピューティングを完全に実現するためにブートします。サーバは、 AFF ストレージクラスタでホストされているブートボリューム内の LUN からブートされます
- MEDITECH のワークロードはすべて FC LUN にホストされており、ストレージコントローラノードに分散されています

ホストソフトウェア

次のソフトウェアをインストールする必要があります。

- Cisco UCS ブレードに ESXi をインストールします
- VMware vCenter がインストールおよび設定されている（すべてのホストが vCenter に登録されている）
- VSC をインストールして VMware vCenter に登録
- ネットアップクラスタが設定されました

"次に、 Cisco UCS ブレードサーバとスイッチの設定を行います。"

Cisco UCS ブレードサーバとスイッチの構成

FlexPod for MEDITECH ソフトウェアは、あらゆるレベルのフォールトトレランスに対応して設計されています。システムに単一点障害がない。最適なパフォーマンスを得るために、ホットスペアブレードサーバの使用をお勧めします。

本ドキュメントでは、 MEDITECH ソフトウェア向け FlexPod 環境の基本構成に関する概要を説明します。このセクションでは、 FlexPod 構成の Cisco UCS コンピューティングプラットフォーム要素を準備するための手順の概要と例をいくつか示します。このガイダンスを開始するには、の手順に従って、 FlexPod 構成がラックに設置され、電源が投入され、ケーブルが接続されている必要があります "VMware vSphere 6.5 Update 1 、 NetApp AFF A シリーズ、および Cisco UCS Manager 3.2 を使用した、ファイバチャネルストレージを備えた FlexPod データセンター"CVD ：

Cisco Nexus スイッチの設定

耐障害性に優れた Cisco Nexus 9300 シリーズイーサネットスイッチペアが解決策用に導入されます。これらのスイッチは、の説明に従ってケーブル接続する必要があります "ケーブル配線図" セクション。Cisco Nexus 構成により、 MEDITECH アプリケーションに合わせてイーサネットトラフィックフローが最適化されます。

1. 初期セットアップとライセンスの設定が完了したら、次のコマンドを実行して両方のスイッチにグローバル設定パラメータを設定します。

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. グローバルコンフィギュレーションモードを使用して、各スイッチに解決策用の VLAN を作成します。

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. トラブルシューティング用のネットワークタイムプロトコル（ NTP ）配信インターフェイス、ポートチャネル、ポートチャネルパラメータ、およびポートの説明をに作成します "VMware vSphere 6.5 Update 1 、 NetApp AFF A シリーズ、および Cisco UCS Manager 3.2 を使用した、ファイバチャネルストレージを備えた FlexPod データセンター"CVD ：

Cisco MDS 9132T 構成

Cisco MDS 9100 シリーズ FC スイッチは、 NetApp AFF A200 または AFF A300 コントローラと Cisco UCS コンピューティングファブリック間で冗長な 32Gb FC 接続を提供します。の説明に従ってケーブルを接続します "ケーブル配線図" セクション。

1. 各 MDS スイッチのコンソールで次のコマンドを実行して、解決策に必要な機能を有効にします。

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. の FlexPod Cisco MDS スイッチの設定セクションに従って、個々のポート、ポートチャネル、および説明を設定します "FlexPod データセンターと FC の Cisco Validated Design の 2 つの機能があります"。
3. 解決策に必要な仮想 SAN （ VSAN ）を作成するには、グローバルコンフィギュレーションモードで次の

手順を実行します。

a. ファブリック A MDS スイッチに対して、次のコマンドを実行します。

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

このコマンドの最後の 2 行のポートチャネル番号は、リファレンスドキュメントを使用して個々のポート、ポートチャネル、および説明をプロビジョニングしたときに作成されました。

b. ファブリック B MDS スイッチに対して、次のコマンドを実行します。

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

このコマンドの最後の 2 行のポートチャネル番号は、リファレンスドキュメントを使用して個々のポート、ポートチャネル、および説明をプロビジョニングしたときに作成されました。

4. 各 FC スイッチについて、リファレンスドキュメントの詳細を使用して、各デバイスをわかりやすい方法で識別するデバイスエイリアス名を作成します。
5. 最後に、各 MDS スイッチについて手順 4 で作成したデバイスエイリアス名を使用して、 FC ゾーンを作成します。

a. ファブリック A MDS スイッチに対して、次のコマンドを実行します。

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

b. ファブリック B MDS スイッチに対して、次のコマンドを実行します。

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

Cisco UCS の設定に関するガイダンス

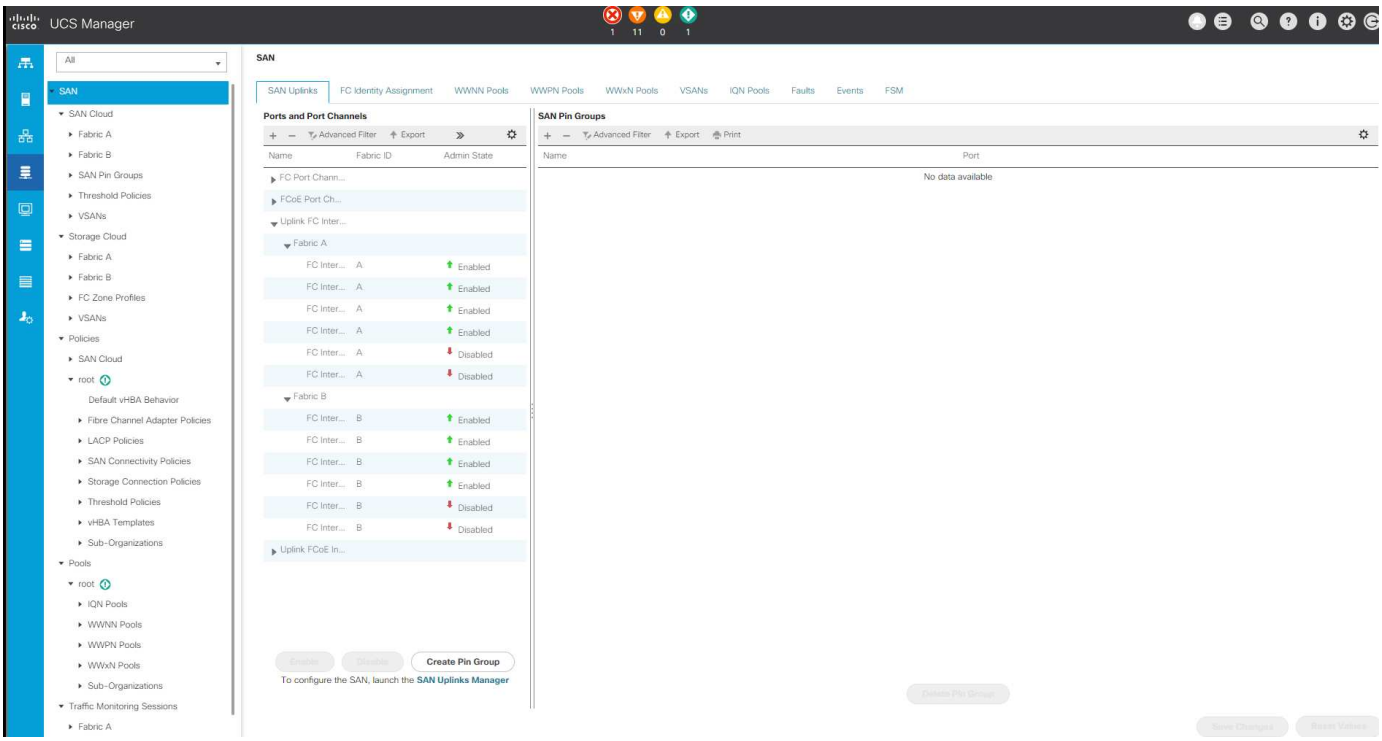
Cisco UCS を使用することで、 MEDITECH のお客様は、ネットワーク、ストレージ、コンピューティングの専門知識を活用して、お客様固有のニーズに合わせて環境をカスタマイズできるポリシーとテンプレートを作

成できます。作成されたポリシーとテンプレートをサービスプロファイルに統合することで、シスコのブレードサーバとラックサーバの一貫した、繰り返し可能で信頼性の高い、迅速な導入を実現できます。

Cisco UCS には、ドメインと呼ばれる Cisco UCS システムを管理するための 3 つの方法があります。

- Cisco UCS Manager HTML5 GUI
- Cisco UCS CLI
- マルチドメイン環境向けの Cisco UCS Central

次の図に、 Cisco UCS Manager の SAN ノードのサンプルスクリーンショットを示します。



大規模な導入では、独立した Cisco UCS ドメインを構築して、 MEDITECH の主要な機能コンポーネントレベルでのフォールトトレランスを強化できます。

2 つ以上のデータセンターを備えた耐障害性の高い設計では、 Cisco UCS Central は、企業全体のホスト間で一貫性を保つために、グローバルポリシーとグローバルサービスプロファイルを設定するうえで重要な役割を果たします。

Cisco UCS コンピューティングプラットフォームをセットアップするには、次の手順を実行します。これらの手順は、 Cisco UCS B200 M5 ブレードサーバを Cisco UCS 5108 AC ブレードシャーシに設置したあとに実行します。また、に記載されているケーブル接続要件についても競合する必要があります "ケーブル配線図" セクション。

1. Cisco UCS Manager ファームウェアをバージョン 3.2(2f) 以降にアップグレードします。
2. ドメインのレポート、 Cisco Call Home 機能、および NTP 設定を行います。
3. 各ファブリックインターコネクトにサーバポートとアップリンクポートを設定します。
4. シャーシ検出ポリシーを編集します。
5. アウトオブバンド管理、 Universal Unique Identifier （ UUID ）、 MAC アドレス、サーバ、 Worldwide

Node Name （ WWNN ；ワールドワイドノード名）、および Worldwide Port Name （ WWPN ；ワールドワイドポート名）用のアドレスプールを作成します。

6. イーサネットおよび FC アップリンクポートチャネルおよび VSAN を作成します。
7. SAN 接続、ネットワーク制御、サーバプールの認定、電源制御、サーバ BIOS 、 デフォルトのメンテナンスに使用できます。
8. vNIC および vHBA テンプレートを作成します。
9. vMedia ブートポリシーと FC ブートポリシーを作成します。
10. MEDITECH プラットフォームの各要素のサービスプロファイルテンプレートとサービスプロファイルを作成します。
11. サービスプロファイルを適切なブレードサーバに関連付けます。

FlexPod の Cisco UCS サービスプロファイルの各主要要素を設定する詳細な手順については、を参照してください "VMware vSphere 6.5 Update 1 、 NetApp AFF A シリーズ、および Cisco UCS Manager 3.2 を使用した、ファイバチャネルストレージを備えた FlexPod データセンター"CVD ドキュメント

"次のセクションでは、 ESXi の構成のベストプラクティスを説明します"

ESXi 構成のベストプラクティス

ESXi ホスト側の構成では、エンタープライズデータベースのワークロードを実行する場合と同様に VMware ホストを構成します。

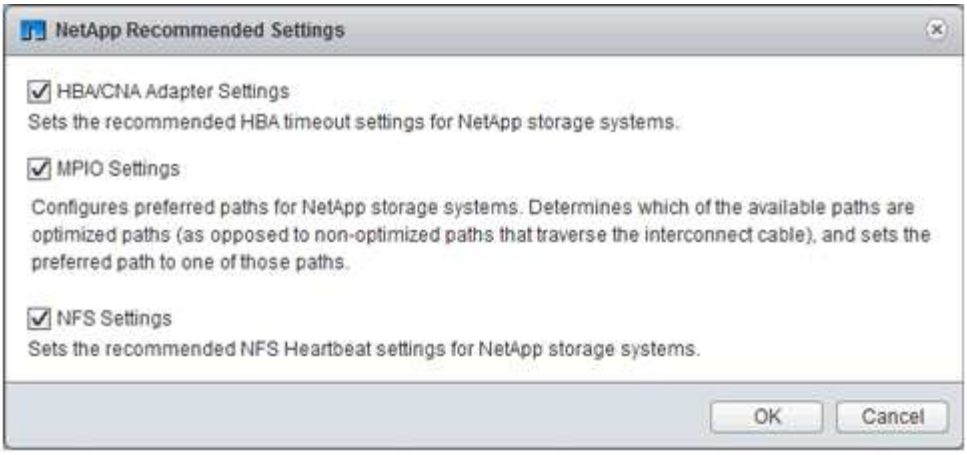
- VSC for VMware vSphere は、 ESXi ホストのマルチパス設定と HBA タイムアウト設定を確認し、ネットアップストレージシステムに最も適した設定を行います。VSC で設定される値は、ネットアップによる厳格な内部テストに基づいています。
- ストレージパフォーマンスを最適化するには、 VMware vStorage APIs for Array Integration （ VAAI ）をサポートしているストレージハードウェアの使用を検討してください。NetApp Plug-in for VAAI は、ESXi ホストにインストールされている VMware の仮想ディスクライブラリを統合するソフトウェアライブラリです。VMware VAAI パッケージを使用すると、特定のタスクを物理ホストからストレージアレイにオフロードできます。

  シンプロビジョニングやハードウェアアクセラレーションなどのタスクをアレイレベルで実行して、ESXi ホスト上のワークロードを削減できます。コピーオフロード機能やスペースリザベーション機能によって、 VSC の処理のパフォーマンスが向上します。ネットアップサポートサイトから、このプラグインのインストールパッケージをダウンロードして、インストール手順を確認できます。

  VSC は、ネットアップストレージコントローラのパフォーマンスの最適化とフェイルオーバーを実現するために、 ESXi ホストのタイムアウト、マルチパス設定、 HBA タイムアウト設定などの値を設定します。次の手順を実行します。

  a. VMware vSphere Web Client のホームページで、 vCenter > Hosts を選択します。
  b. ホストを右クリックし、 Actions > NetApp VSC > Set Recommended Values を選択します。
  c. NetApp Recommended Settings （ネットアップの推奨設定）ダイアログボックスで、システムに最も適した値を選択します。

     標準の推奨値がデフォルトで設定されます。



a. [OK] をクリックします。

"次：ネットアップの構成"

NetApp の設定

MEDITECH ソフトウェア環境に導入されているネットアップストレージでは、ハイアベイラビリティペア構成のストレージコントローラを使用します。ストレージは、両方のコントローラから MEDITECH データベースサーバに FC プロトコル経由で提供する必要があります。この構成では、両方のコントローラのストレージが提供され、通常運用時にアプリケーションの負荷が均等に分散されます。

ONTAP の設定

ここでは、関連する ONTAP コマンドを使用した導入およびプロビジョニング手順の例を示します。特に重視するのは、ハイアベイラビリティコントローラペアを使用するネットアップが推奨するストレージレイアウトを実装するためのストレージのプロビジョニング方法です。ONTAP の大きなメリットの 1 つは、既存の高可用性ペアを中断せずにスケールアウトできることです。

ONTAP ライセンス

ストレージコントローラのセットアップが完了したら、ライセンスを適用して、ネットアップが推奨する ONTAP 機能を有効にします。MEDITECH ワークロードに対応しているライセンスは、 FC 、 CIFS 、 NetApp Snapshot 、 SnapRestore 、 FlexClone 、 および SnapMirror テクノロジ：

ライセンスを設定するには、 NetApp ONTAP System Manager を開き、「設定 - ライセンス」に移動して、該当するライセンスを追加します。

または、 CLI を使用して次のコマンドを実行してライセンスを追加します。

```
license add -license-code <code>
```

AutoSupport の設定

NetApp AutoSupport ツールは、概要のサポート情報を HTTPS 経由でネットアップに送信します。AutoSupport を設定するには、次の ONTAP コマンドを実行します。

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

ハードウェアアシストテイクオーバーの設定

各ノードで、ハードウェアアシストテイクオーバーを有効にして、コントローラで障害が発生した場合にテイクオーバーを開始するまでの時間を最小限に抑えます。ハードウェアアシストテイクオーバーを設定するには、次の手順を実行します。

1. 次の ONTAP コマンドを xxx に実行します。

   パートナー・アドレス・オプションを prod1-01 の管理ポートの IP アドレスに設定します

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
   <prod1-02-mgmt-ip>
   ```

2. 次の ONTAP コマンドを xxx に実行します。

   パートナー・アドレス・オプションを 'cluster1-02 の管理ポートの IP アドレスに設定します

   ```
   MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
   <prod1-01-mgmt-ip>
   ```

3. 次の ONTAP コマンドを実行して ' ハードウェア支援型のテイクオーバーを ' prod1-01 と prod1-02 の両方の HA コントローラ・ペアで有効にします

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist true
   MEDITECH::> storage failover modify -node prod1-02 -hwassist true
   ```

"次の例は、アグリゲートの構成を示し"

アグリゲートの構成

NetApp RAID DP

ネットアップでは、通常のネットアップの Flash Pool アグリゲートを含め、ネットアップ FAS または AFF システム内のすべてのアグリゲートの RAID タイプとして RAID DP テクノロジを推奨しています。MEDITECH のドキュメントで RAID 10 の使用が規定されているかもしれませんが、 MEDITECH では

RAID DP の使用が承認されています。

RAID グループのサイズと数

デフォルトの RAID グループサイズは 16 です。このサイズは、特定のサイトの MEDITECH ホストに対応するアグリゲートに適しているとはかぎりません。ネットアップが RAID グループで使用することを推奨しているディスクの数については、を参照してください "ネットアップ TR-3838 ：『 Storage Subsystem Configuration Guide 』"。

ネットアップでは、 RAID グループサイズと同じ 1 つ以上のディスクグループを含むアグリゲートにディスクを追加することを推奨しているため、 RAID グループのサイズはストレージ拡張にとって重要です。RAID グループの数は、データディスクの数と RAID グループのサイズによって異なります。必要なデータディスクの数を判断するには、 NetApp System Performance Modeler （ SPM ）サイジングツールを使用します。データディスクの数を決定したら、 RAID グループのサイズを調整して、各ディスクタイプの RAID グループサイズの推奨範囲内でパリティディスクの数が最小になるようにします。

MEDITECH 環境向け SPM サイジングツールの使用方法については、を参照してください "NetApp TR-4190 ：『 NetApp Sizing Guidelines for MEDITECH Environments 』"。

ストレージ拡張に関する考慮事項

ディスク数の多いアグリゲートを拡張する場合は、アグリゲート RAID グループサイズと同じグループに含まれるディスクを追加します。このアプローチに従うことで、アグリゲート全体でパフォーマンスの一貫性を確保できます。

たとえば、 RAID グループサイズが 20 で作成されたアグリゲートにストレージを追加する場合、ネットアップでは 20 本以上のディスクグループを追加することを推奨します。そのため、ディスクに 20 、 40 、 60 などを追加します。

アグリゲートを拡張したら、影響を受けるボリュームまたはアグリゲートで再配置タスクを実行して、既存のデータストライプを新しいディスクに分散することで、パフォーマンスを向上できます。この処理は、特に既存のアグリゲートがいっぱいになった場合に役立ちます。

> CPU 負荷の高いタスクとディスク負荷の高いタスクであるため、営業時間外にスケジュールの再割り当てを計画する必要があります。

アグリゲート拡張後の再配置の使用の詳細については、を参照してください "ネットアップの TR-3929 ：『 Reallocate Best Practices Guide 』"。

アグリゲートレベルの Snapshot コピー

アグリゲートレベルの NetApp Snapshot コピーリザーブを 0 に設定し、デフォルトのアグリゲート Snapshot スケジュールを無効にします。可能であれば、既存のアグリゲートレベルの Snapshot コピーを削除します。

"次： Storage Virtual Machine の構成"

Storage Virtual Machine の設定

このセクションでは、 ONTAP 8.3 以降のバージョンへの導入について説明します。

> Storage Virtual Machine （ SVM ）は、 ONTAP API および ONTAP CLI では Vserver とも呼ばれます。

MEDITECH ホスト LUN 用の SVM

ONTAP ストレージクラスタごとに 1 つの専用 SVM を作成して、その SVM に MEDITECH ホスト用の LUN が含まれているアグリゲートを所有して管理する必要があります。

SVM の言語エンコード設定

すべての SVM に言語エンコードを設定することを推奨します。SVM の作成時に言語エンコード設定を指定しなかった場合は、デフォルトの言語エンコード設定が使用されます。ONTAP のデフォルトの言語エンコード設定は C.UTF-8 です。言語エンコードを設定したあとで、 Infinite Volume を備えた SVM の言語を変更することはできません。

SVM に関連付けられたボリュームは、ボリュームの作成時に別の設定を明示的に指定しないかぎり、 SVM の言語エンコード設定を継承します。特定の処理を実行できるようにするには、サイトのすべてのボリュームで一貫した言語エンコード設定を使用する必要があります。たとえば、 SnapMirror では、ソース SVM とデスティネーション SVM の言語エンコード設定が同じである必要があります。

"次の手順：ボリューム構成"

ボリューム構成

ボリュームのプロビジョニング

MEDITECH ホスト専用の MEDITECH ボリュームはシックプロビジョニングでもシンプロビジョニングでもかまいません。

ボリュームレベルのデフォルトの Snapshot コピー

Snapshot コピーはバックアップワークフローの一環として作成されます。各 Snapshot コピーを使用して、MEDITECH LUN に格納されているデータに異なる時間でアクセスできます。MEDITECH 承認のバックアップ解決策は、これらの Snapshot コピーに基づいてシンプロビジョニングされた FlexClone ボリュームを作成し、 MEDITECH LUN のポイントインタイムコピーを提供します。MEDITECH 環境は、認定済みのバックアップソフトウェア解決策と統合されています。そのため、 MEDITECH の本番データベース LUN を構成する NetApp FlexVol ボリュームごとに、デフォルトの Snapshot コピースケジュールを無効にすることを推奨します。

- 重要： FlexClone ボリュームは親データボリュームのスペースを共有するため、バックアップサーバが作成する MEDITECH データ LUN と FlexClone ボリュームに十分なスペースをボリュームに確保しておくことが重要です。FlexClone ボリュームは、データボリュームが占めるスペースの増加は行いません。ただし、 MEDITECH LUN が短時間で大幅に削除された場合は、クローンボリュームが大きくなる可能性があります。

アグリゲートあたりのボリューム数

Flash Pool キャッシュまたは NetApp Flash Cache キャッシュを使用する NetApp FAS システムについては、MEDITECH プログラム、ディクショナリ、およびデータファイルの格納専用のボリュームをアグリゲートごとに 3 つ以上プロビジョニングすることを推奨します。

AFF システムについては、 MEDITECH のプログラム、ディクショナリ、データファイルを格納するボリュームをアグリゲートごとに 4 つ以上確保することを推奨します。

ボリュームレベルの再割り当てスケジュール

特に MEDITECH 拡張プラットフォーム '6.x プラットフォーム 'C/S 5.x プラットフォームなどの書き込み負荷の高いワークロードで使用される場合 ' ストレージのデータ・レイアウトは時間の経過とともに最適化されません時間の経過とともに、シーケンシャルリードのレイテンシが高くなり、バックアップが完了するまでの時間が長くなる可能性があります。データレイアウトが適切でないか、断片化が書き込みレイテンシに影響する可能性もあります。ボリュームレベルの再割り当てを使用してディスク上のデータのレイアウトを最適化することで、書き込みレイテンシの低減とシーケンシャル読み取りアクセスの向上を実現できます。ストレージレイアウトが改善され、割り当てられた時間の 8 時間以内にバックアップが完了するようになりました。

ベストプラクティス
少なくとも、週単位のボリューム再割り当てスケジュールを実装して、割り当てられたメンテナンス時または本番用サイトのピーク時以外の時間帯に再割り当て処理を実行することを推奨します。 ネットアップでは、コントローラごとに一度に 1 つのボリュームで再割り当てタスクを実行することを強く推奨します。

業務用データベース・ストレージに適したボリューム再配置スケジュールの決定の詳細については、のセクション 3.12 を参照してください "ネットアップの TR-3929 ：『 Reallocate Best Practices Guide 』"。また、ビジー状態のサイトに対して週次再配置スケジュールを作成する方法についても説明します。

"次の例は、 LUN の構成を示して"

LUN の設定

環境内の MEDITECH ホストの数によって、 NetApp FAS または AFF システム内に作成される LUN の数が決まります。Hardware Configuration Proposal （ハードウェア構成提案）は、各 LUN のサイズを指定します。

LUN のプロビジョニング

MEDITECH ホスト専用の MEDITECH LUN にはシックプロビジョニングとシンプロビジョニングがあります。

LUN オペレーティングシステムのタイプ

作成した LUN のアライメントを正しく行うには、 LUN のオペレーティングシステムのタイプを正しく設定する必要があります。ミスアライメント状態の LUN では不要な書き込み処理のオーバーヘッドが発生するため、ミスアライメント状態の LUN を修正するとコストがかかります。

MEDITECH ホストサーバは通常、 VMware vSphere ハイパーバイザーを使用して仮想化された Windows Server 環境で実行されます。ホストサーバは、ベアメタルサーバ上の Windows Server 環境でも実行できます。設定するオペレーティング・システム・タイプの値を決定するには ' の LUN Create セクションを参照してください "clustered Data ONTAP 8.3 コマンド：マニュアルページリファレンス"。

LUN サイズ

MEDITECH ホストごとの LUN サイズを確認するには、 MEDITECH の Hardware Configuration Proposal （新規導入）または Hardware Evaluation Task （既存導入）ドキュメントを参照してください。

LUN の提供

MEDITECH を使用するには、プログラム、ディクショナリ、データファイル用のストレージを、 FC プロトコルを使用して MEDITECH ホストに LUN として提供する必要があります。VMware 仮想環境では、MEDITECH ホストをホストしている VMware ESXi サーバに LUN が提供されます。次に、 VMware ESXi サーバに提供される各 LUN は、物理互換モードで RDM を使用して、各 MEDITECH ホスト VM にマッピングされます。

適切な LUN 命名規則を使用して、 MEDITCH ホストに LUN を提供する必要があります。たとえば ' 管理を容易にするには 'MEDITECH ホストの mt-host-01 に LUN 「 M TFS01E 」を提供する必要があります

MEDITECH とバックアップシステムのインストーラを使用して、 MEDITECH ホストで使用する LUN に適した一貫した命名規則を考案する場合は、 MEDITECH ハードウェア構成提案書を参照してください。

MEDITECH LUN 名の例は「 MFS05E 」です。

- 「 TFS 」は MEDITECH ファイルサーバ（ MEDITECH ホスト用）を示します。
- 「 05 」はホスト番号 5 を示します。
- 「 E 」は Windows E ドライブを示します。

"次の例：イニシエータグループの設定"

イニシエータグループの構成

FC をデータネットワークプロトコルとして使用する場合は、各ストレージコントローラに 2 つのイニシエータグループ（ igroup ）を作成します。1 つ目の igroup には、MEDITECH ホスト VM （ MEDITECH 向け igroup ）をホストしている VMware ESXi サーバ上の FC ホストインターフェイスカードの WWPN が含まれています。

MEDITECH igroup オペレーティングシステムのタイプは環境設定に応じて設定する必要があります。例：

- Windows Server 環境のベアメタルサーバ・ハードウェアにインストールされているアプリケーションには、 igroup オペレーティング・システム・タイプ「 windows 」を使用します。
- VMware vSphere ハイパーバイザを使用して仮想化されるアプリケーションには、 igroup オペレーティングシステムタイプ「 vmware 」を使用します。

> igroup のオペレーティングシステムのタイプは、 LUN のオペレーティングシステムのタイプと異なる場合があります。たとえば、仮想化された MEDITECH ホストの場合、 igroup のオペレーティング・システム・タイプを「 vmware 」に設定する必要があります。仮想化された MEDITECH ホストが使用する LUN の場合は ' オペレーティング・システムのタイプを Windows 2008 以降に設定する必要がありますMEDITECH ホストオペレーティングシステムが Windows Server 2008 R2 64 ビット Enterprise Edition であるため、この設定を使用します。

オペレーティング・システム・タイプに適した値については、の「 LUN igroup の作成」および「 LUN の作成」を参照してください "『 clustered Data ONTAP 8.2 コマンド：マニュアルページリファレンス』"。

"次のコマンド： LUN マッピング"

LUN マッピング

MEDITECH ホストの LUN マッピングは、 LUN の作成時に確立されます。

MEDITECH のモジュールとコンポーネント

MEDITECH アプリケーションは複数のモジュールとコンポーネントに対応しています。次の表に、これらのモジュールでカバーされる機能を示します。これらのモジュールの設定と導入については、 MEDITECH のマニュアルを参照してください。追加情報

機能	を入力します
接続性	• Web サーバ • ライブアプリケーションサーバー (Wi-Fi – Web 統合) • アプリケーションサーバーのテスト (WI) • SAML 認証サーバ（ Wi-Fi ） • SAML プロキシサーバ（ Wi-Fi ） • データベースサーバ
インフラ	• ファイルサーバ • バックグラウンドジョブクライアント • 接続サーバ • トランザクションサーバ
スキャンとアーカイブ	• イメージサーバ
データリポジトリ	• SQL サーバ
ビジネス分析と臨床分析	• ライブインテリジェンスサーバ（ BCA ） • Test Intelligence Server （ BCA ；テストインテリジェンスサーバ） • データベースサーバ（ BCA ）

機能	を入力します
家の心配	• リモートサイトの解決策 • 接続性 • インフラ • 印刷 • フィールドデバイス • スキャン中です • ホストされたサイトの要件 • ファイアウォールの設定
サポート	• バックグラウンドジョブクライアント（ CAL - クライアントアクセスライセンス）
ユーザーデバイス	• タブレット • 固定デバイス
印刷	• ライブネットワークプリントサーバー（必須、既に存在する場合があります） • ネットワークプリントサーバーのテスト（必須、既に存在する場合があります）
サードパーティの要件	• First Databank (FDB) MedKnowledge Framework v4.3

謝辞

本ガイドの作成には、以下の方々が関わってきました。

- Brandon AGEE 、テクニカルマーケティングエンジニア、ネットアップ
- ネットアップ、テクニカルマーケティングエンジニア、 Atul Bhalodia 氏
- ネットアップシニアプロダクトマネージャー、 Ketan Mota 氏
- ネットアップ、ヘルスケア、ソリューションアーキテクト、 John Duignan 氏
- シスコ、 Jon Ebmeier 氏
- シスコ、マイク・ブレナン

追加情報の参照先

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または Web サイトを参照してください。

FlexPod デザインゾーン

- "FlexPod 設計ゾーン"
- "AFF FlexPod 、 vSphere 6.5U1 、および Cisco UCS Manager を使用する FC ストレージ（ MDS スイッチ）を備えた データセンターです"

ネットアップテクニカルレポート

- "TR-3929 ：『 Reallocate Best Practices Guide 』"
- "TR-3987 ：『 Snap Creator Framework Plug-in for Intersystems Cach é 』"
- "TR-4300i ：『 NetApp FAS and All-Flash Storage Systems for MEDITECH Environments Best Practices Guide 』"
- "TR-4017 ：『 FC SAN Best Practices 』"
- "TR-3446 ：『非同期 SnapMirror ベストプラクティスガイド』"

ONTAP のドキュメント

- "ネットアップの製品マニュアル"
- "Virtual Storage Console （ VSC ） for vSphere のドキュメント"
- "ONTAP 9 ドキュメンテーション・センター"：
  - "ESXi 向け FC エクスプレスガイド"
- "ONTAP 9.3 のすべてのドキュメント"：
  - "『 Software Setup Guide 』を参照して"
  - "『 Disks and Aggregates Power Guide 』を参照してください"
  - "『 SAN アドミニストレーションガイド』"
  - "『 SAN 構成ガイド』"
  - "『 FC Configuration for Windows Express Guide 』を参照してください"
  - "『 FC SAN 向け AFF セットアップガイド』"
  - "『 High-Availability 構成ガイド』"
  - "論理ストレージ管理ガイド』を参照してください"
  - "パフォーマンス管理パワーガイド"
  - "SMB/CIFS 構成パワーガイド"
  - "SMB/CIFS Reference 』を参照してください"
  - "データ保護パワーガイド"
  - "『データ保護：テープバックアップおよびリカバリガイド』"
  - "NetApp Encryption パワーガイド』を参照してください"
  - "ネットワーク管理ガイド"
  - "『コマンド：マニュアルページリファレンスガイド - ONTAP 9.3 』"

Cisco Nexus 、 MDS 、 Cisco UCS 、および Cisco UCS Manager の各ガイドを参照してください

- "Cisco UCS サーバの概要"
- "Cisco UCS ブレードサーバの概要"
- "Cisco UCS B200 M5 データシート"
- "Cisco UCS Manager の概要"
- "Cisco UCS Manager 3.2 （ 3a ）インフラストラクチャバンドル" （ Cisco.com 認証が必要）
- "Cisco Nexus 9300 プラットフォームスイッチ"
- "Cisco MDS 9132T FC スイッチ"

FlexPod for Medical Imaging の略

TR-4865 ： FlexPod for Medical Imaging

NetApp 、 Jaya Kishore Esanakula 、 Atul Bhalodia

医療画像は、医療機関が生成するすべてのデータの 70% を占めています。デジタルモダリティが進化し続け、新しいモダリティが出現すると、データ量は増加し続けます。たとえば、アナログからデジタルへの移行により、現在のデータ管理戦略に挑戦する速度で画像サイズが大幅に増加します。

新型コロナウイルス感染症がデジタル変革を明確に刷新しました "レポート"新型コロナウイルス感染症は、 5 年前までにデジタルコマースを加速してきました。問題解決者が主導する技術革新は、日常生活の仕方を根本的に変えています。このテクノロジ主導の変革により、ヘルスケアを含む、私たちの生活の多くの重要な側面が全面的に改善されます。

ヘルスケアは、今後数年の間に大きな変化を迫られています。新型コロナウイルス感染症は、医療業界を推進するために、少なくとも数年かかるイノベーションを加速しています。この変化の中核をなすのは、信頼性を損なうことなく、より低コストで可用性が高く、アクセス可能な医療をパンダ処理に柔軟にすることです。

この医療の変化の基盤となるのが、適切に設計されたプラットフォームです。プラットフォームを測定するための重要な指標の 1 つは、プラットフォームの変更を簡単に実装できることです。スピードは新しいスケールであり、データ保護に妥協することはできません。世界で最も重要なデータの一部は、臨床医を支援する臨床システムによって作成され、消費されています。ネットアップは、臨床医が必要とする患者のケアに重要なデータを提供しています。このデータは、オンプレミス、クラウド、ハイブリッド環境のいずれにも存在します。ハイブリッドマルチクラウド環境は、 IT アーキテクチャの最先端のテクノロジです。

医療については、医療機関（医師、看護師、放射線科医、医療機器技術者など）と患者を中心に展開しています。患者とプロバイダーをより近くに配置し、地理的な場所を単なるデータポイントにすることで、プロバイダーや患者が必要になったときに基盤となるプラットフォームを利用できるようにすることがさらに重要になります。このプラットフォームは、効率性とコスト効率の両方を長期間維持する必要があります。患者ケアコストをさらに削減するために、 "責任あるケア組織" (ACOS) は、効率的なプラットフォームによって強化されます。

医療機関が使用する医療情報システムに関しては、構築と購入の問題で回答を 1 つ購入する傾向があります。これは、多くの主観的な理由で発生する可能性があります。購入に関する意思決定は、長年にわたって左右されない情報システムを生み出すことができます。各システムには、導入先のプラットフォームに固有の要件があります。最も重要な問題は ' 情報システムが必要とする ' 大規模で多様なストレージ・プロトコルとパ

フォーマンス・レベルですこれにより ' プラットフォームの標準化と最適な運用効率が大きな課題となります医療機関は、多様なスキルを必要とし、 SME の定着を必要とする大規模なプラットフォームのような、運用上の必要性が小さく、ミッションクリティカルな問題に集中することはできません。

課題は、次のカテゴリに分類できます。

- 異機種混在ストレージのニーズ
- 部門のサイロ
- IT 運用の複雑さ
- クラウドへの接続
- サイバーセキュリティ
- 人工知能とディープラーニング

FlexPod を使用すると、 1 つのプラットフォームで FC 、 FCoE 、 iSCSI 、 NFS / pNFS 、 SMB / CIFS などをサポートできます。人、プロセス、テクノロジーは、 FlexPod が設計および構築する DNA の一部です。FlexPod アダプティブ QoS は、基盤となる同じ FlexPod プラットフォーム上で複数のミッションクリティカルな臨床システムをサポートすることで、部門のサイロを解消します。FlexPod は FedRAMP 認定および FIPS 140-2 認定済みです。さらに、医療機関は人工知能やディープラーニングなどのビジネスチャンスに直面しています。FlexPod とネットアップは、これらの課題を解決し、オンプレミスやハイブリッドマルチクラウド環境で必要とされる場所で、標準化されたプラットフォームでデータを利用できるようにします。詳細および一連のユーザ事例については、を参照してください "FlexPod ヘルスケア"。

一般的な医療画像情報および PACS システムには、次の機能があります。

- 受付と登録
- スケジュール設定
- イメージング
- 文字変換
- 管理
- データ交換
- イメージアーカイブ
- 臨床医のための画像撮影と読み取り、および画像表示用の画像表示

イメージングに関しては、医療分野は以下の臨床的課題を解決しようとしています。

- の普及拡大 "自然言語処理" （ NLP ）ベースの技術者および医師による画像読み取りアシスタント。放射線科では、音声認識を利用してレポートを転記することができます。NLP を使用すると、患者の記録（特に DICOM 画像に埋め込まれた DICOM タグ）の識別と匿名化を行うことができます。NLP 機能を使用するには、イメージ処理の応答時間が短いハイパフォーマンスプラットフォームが必要です。FlexPod の QoS 機能は、パフォーマンスだけでなく、将来の拡張に備えて必要な容量を予測します。
- ACOS や地域の医療機関が標準化された臨床経路とプロトコルを幅広く採用。これまで、臨床的な意思決定をガイドする統合ワークフローではなく、静的なガイドラインセットとして臨床経路が使用されてきました。NLP および画像処理の進歩により、画像内の DICOM タグを臨床的経路に統合して臨床判断を促進することができます。そのため、これらのプロセスには、基盤となるインフラプラットフォームやストレージシステムから、高いパフォーマンス、低いレイテンシ、高いスループットが求められます。
- 畳み込みニューラルネットワークを活用する ML モデルでは、画像処理機能をリアルタイムで自動化でき

るため、 GPU 対応のインフラが必要になります。FlexPod は、 CPU と GPU の両方のコンピューティングコンポーネントを同じシステムに搭載し、 CPU と GPU を個別に拡張できます。

- DICOM タグが臨床ベストプラクティスアドバイザリのファクトとして使用されている場合、システムは低遅延および高スループットの DICOM アーティファクトのより多くの読み取りを実行する必要があります。
- 画像を評価する場合、組織全体の放射線科医間でリアルタイムのコラボレーションを行うには、エンドユーザーコンピューティングデバイスで高性能なグラフィックス処理が必要です。ネットアップは、ハイエンドグラフィックスのユースケースに特化して設計され実証された、業界をリードする VDI ソリューションを提供しています。詳細については、を参照してください "こちらをご覧ください"。
- ACO 医療機関全体で画像およびメディア管理を行う場合は、画像の記録システムに関係なく、 Digital Imaging や Communications in Medicine などのプロトコルを使用して、単一のプラットフォームを使用できます（ "DICOM"）および DICOM 永続オブジェクトへの Web アクセス（ "WADO"）
- ヘルス情報交換（ "HIE") メッセージに埋め込まれた画像を含みます。
- ハンドヘルド、ワイヤレススキャンデバイスなどのモバイルモダリティは、 DoD レベルのセキュリティ、信頼性、遅延を持つ堅牢なネットワークインフラストラクチャを必要とします。このインフラストラクチャは、デバイス、ワイヤレススキャンデバイス（携帯電話に接続されているポケットハンドヘルド超音波スキャナなど）のエッジ、コア、クラウドに必要です。 "ネットアップが実現するデータファブリック" 大規模な組織にこの機能を提供します。
- 新しいモダリティには急激なストレージニーズがあります。たとえば、 CT や MRI ではモダリティごとに数百 MB 必要ですが、デジタル病理画像（スライド全体のイメージングを含む）のサイズは数 GB になります。FlexPod の設計は、です "基本的な特性としてのパフォーマンス、信頼性、拡張性"。

適切に設計された医療画像システムプラットフォームは、イノベーションの中心にあります。FlexPod アーキテクチャは、業界をリードする Storage Efficiency 機能を備えた、柔軟なコンピューティング機能とストレージ機能を提供します。

解決策の全体的なメリット

FlexPod アーキテクチャ基盤でイメージングアプリケーション環境を実行することで、医療機関はスタッフの生産性向上と設備投資と運用コストの削減を期待できます。FlexPod は、予測可能な低レイテンシのシステムパフォーマンスと高可用性を実現するように設計された、厳密にテストされた検証済みの統合ソリューションです。このアプローチにより、高い快適性が得られ、最終的には医療画像システムのユーザーに最適な応答時間が得られます。

イメージングシステムのさまざまなコンポーネントが、 SMB/CIFS 、 NFS 、 ext4 、または NTFS ファイルシステム内のデータの格納を必要とする場合があります。つまり、インフラが、 NFS 、 SMB / CIFS 、 SAN の各プロトコル経由でデータアクセスを提供できる必要があります。1 つのネットアップストレージシステムで NFS 、 SMB / CIFS 、 SAN の各プロトコルをサポートできるため、プロトコル固有のストレージシステムという従来のプラクティスは必要ありません。

FlexPod インフラは、モジュラ型で、統合型で、仮想化と拡張性に優れた、コスト効率の高いプラットフォームです。FlexPod プラットフォームでは、コンピューティング、ネットワーク、ストレージを個別にスケールアウトできるため、アプリケーションの導入時間が短縮されます。また、モジュラアーキテクチャにより、システムのスケールアウトやアップグレード時にもノンストップオペレーションが実現します。

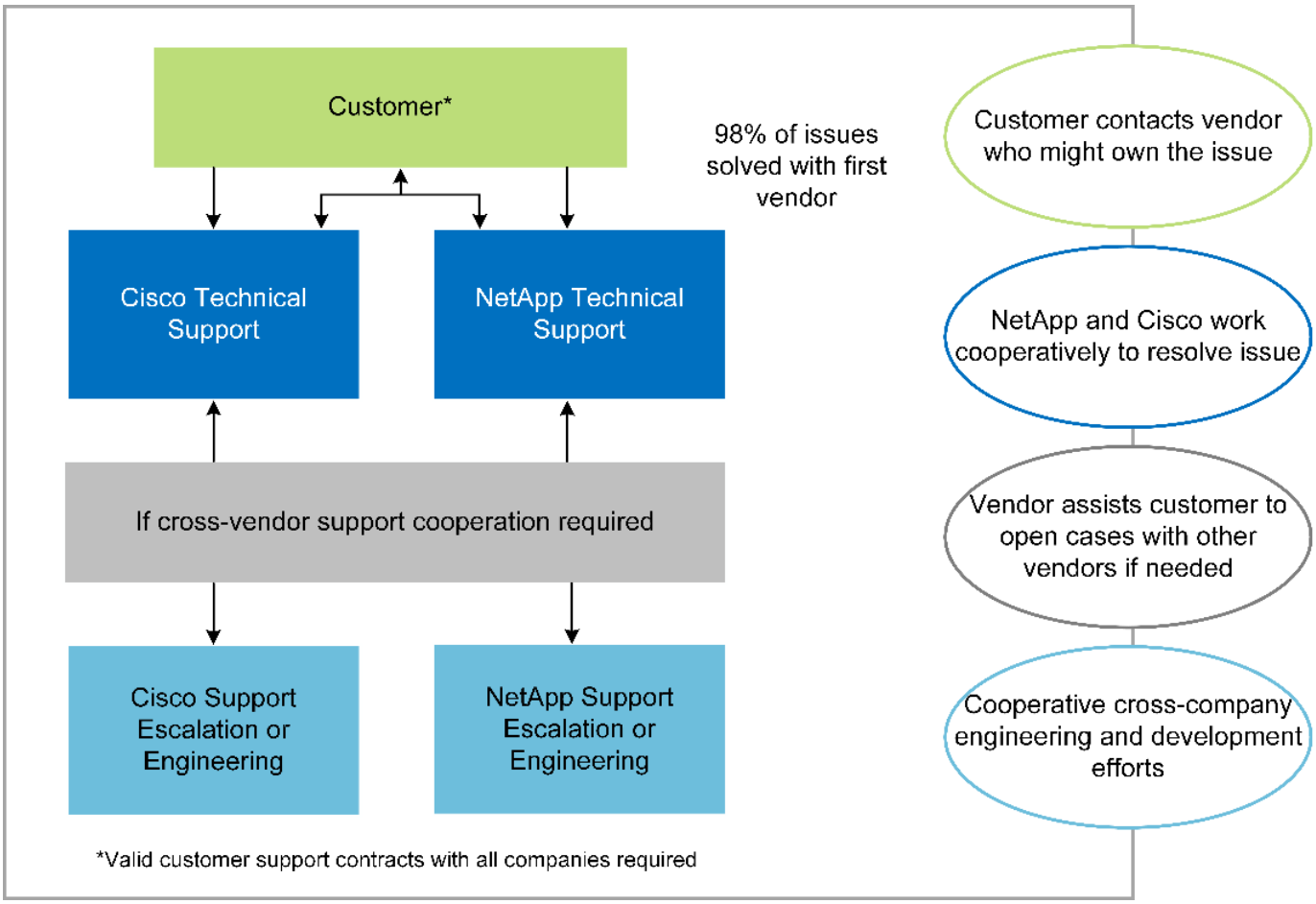
FlexPod には、医療画像業界に特有の利点がいくつかあります。

- * 低遅延のシステム性能。 * 放射線科医の時間は、高価値のリソースであり、放射線科医の時間を効率的に使用することが最重要です。画像やビデオのロードを待つと、臨床医の効率性や患者の安全性に影響を与える可能性があります。

- * モジュラーアーキテクチャ * FlexPod コンポーネントは、クラスタ化されたサーバー、ストレージ管理ファブリック、統合管理ツールセットを通じて接続されます。イメージング設備が年々拡大し、研究の数が増加するにつれて、基盤となるインフラストラクチャもそれに合わせて拡張する必要があります。FlexPod では、コンピューティング、ストレージ、ネットワークを個別に拡張できます。
- * インフラストラクチャの迅速な導入。 * 既存のデータセンターにあるかリモートサイトにあるかに関係なく、 FlexPod データセンターの統合およびテスト済みの設計により、新しいインフラストラクチャをより短時間で導入し、より少ない労力で稼働させることができます。
- * アプリケーションの導入時間を短縮。 * 検証済みのアーキテクチャにより、あらゆるワークロードへの導入時間とリスクが削減され、ネットアップテクノロジによってインフラの導入が自動化されます。解決策を使用して医療画像の初期展開、ハードウェアの更新、拡張を行う場合でも、プロジェクトのビジネス価値にリソースを移行することができます。
- * 運用の簡素化とコストの削減。 * 従来の商用プラットフォームをより効率的でスケーラブルな共有リソースに置き換えることで、ワークロードの動的なニーズに対応することで、コストと複雑さを解消できます。この解決策は、インフラリソースの利用率を高め、投資回収率（ ROI ）を向上させます。
- * スケールアウトアーキテクチャ。 * 実行中のアプリケーションを再構成することなく、 SAN と NAS を数テラバイトから数十ペタバイトまで拡張できます。
- * ノンストップオペレーション。 * ストレージの保守、ハードウェアのライフサイクル処理、ソフトウェアのアップグレードを、ビジネスを中断することなく実行できます。
- * セキュアマルチテナンシー。この利点は、仮想化されたサーバおよびストレージ共有インフラストラクチャのニーズの増大に対応し、特にデータベースとソフトウェアの複数のインスタンスをホストする場合に、施設固有の情報のセキュアマルチテナンシーを可能にします。
- * プールされたリソースの最適化。 * この利点は、物理サーバとストレージコントローラの数を減らし、ワークロードの負荷を分散し、使用率を高めながらパフォーマンスを向上させるのに役立ちます。
- * サービス品質（ QoS ）。 * FlexPod は、スタック全体で QoS を提供します。業界をリードするこれらの QoS ストレージポリシーによって、共有環境で差別化されたサービスレベルを実現できます。これらのポリシーは、ワークロードのパフォーマンスを最適化し、過負荷のアプリケーションを分離して制御するのに役立ちます。
- * QoS を使用したストレージ階層の SLA のサポート。 * 医療画像環境で通常必要とされるストレージ階層ごとに異なるストレージシステムを導入する必要はありません。1 つのストレージクラスタに複数の NetApp FlexVol を配置し、それぞれの階層に対して固有の QoS ポリシーを設定することで、同じクラスタでこの目的を実現できます。この手法では、ストレージインフラを動的に特定のストレージ階層のニーズの変化に対応させることができます。NetApp AFF では、 FlexVol ボリュームのレベルで QoS を許可することで、ストレージ階層ごとに異なる SLA をサポートできます。そのため、アプリケーションごとに異なるストレージシステムを用意する必要はありません。
- * ストレージ効率。 * 医療画像は通常、約 2.5 ： 1 の JPEG2K 圧縮へのイメージング・アプリケーションによって事前圧縮されています。ただし、これはイメージングアプリケーションおよびベンダー固有です。大規模なイメージングアプリケーション環境（ 1PB 超）では、ストレージ容量を 5 〜 10% 削減でき、ネットアップの Storage Efficiency 機能によりストレージコストを削減できます。イメージングアプリケーションベンダーやネットアップの専門知識を持つ担当者と協力して、医療画像システムのストレージ効率を最大限に高めることができます。
- * 俊敏性。 * FlexPod システムが提供する業界をリードするワークフロー自動化、オーケストレーション、管理ツールにより、 IT チームはビジネス要求への対応力を大幅に高めることができます。こうしたビジネス要求は、医療画像のバックアップや追加のテストおよびトレーニング環境のプロビジョニングから、人口健康管理イニシアチブのための分析データベースの複製まで多岐にわたります。
- * 生産性の向上。 * この解決策は迅速に導入および拡張できるため、医療従事者によるエンドユーザエクスペリエンスを最適化できます。

- * データファブリック。 * ネットアップのデータファブリックは、サイト間、物理的な境界を越えて、アプリケーション間でデータを結び付けます。ネットアップのデータファブリックは、 Data-Centric の世界におけるデータ主体の企業向けに構築されています。データは複数の場所に作成されて使用されるため、多くの場合、他の場所、アプリケーション、インフラとの利用や共有が必要になります。そのため、一貫性のある統合された管理方法が必要です。この解決策では、データを管理する方法が提供されます。これにより、 IT チームはこれまで以上に複雑な IT 作業を管理できるようになります。
- * ONTAP FabricPool 。 * NetApp FabricPool は、パフォーマンス、効率、セキュリティ、保護を犠牲にすることなく、ストレージコストを削減します。FabricPool は、エンタープライズアプリケーションに対して透過的であり、アプリケーションインフラを再構築することなくストレージの TCO を削減することで、クラウドの効率性を活用します。FlexPod は、 FabricPool のストレージ階層化機能を活用して、ONTAP フラッシュストレージをより効率的に使用できます。詳細については、を参照してください "FlexPod with FabricPool の略"。
- * FlexPod のセキュリティ。 * セキュリティは FlexPod の非常に基礎にある。ここ数年、ランサムウェアは重大な脅威になり、脅威も増大しています。ランサムウェアは、暗号ウイルスに基づいたマルウェアで、暗号化を使用して悪意のあるソフトウェアを構築します。このマルウェアは、対称キー暗号と非対称キー暗号の両方を使用して、被害者のデータをロックし、データを復号化するための鍵を提供するために身代金を要求できます。FlexPod がランサムウェアなどの脅威を軽減する方法については、を参照してください "解決策によるランサムウェア対策"。FlexPod インフラコンポーネントも連邦情報処理標準です "（ FIPS ） 140-2" 準拠。
- * FlexPod 共同サポート * ネットアップと Cisco は、 FlexPod コンバージドインフラに固有のサポート要件を満たす、拡張性と柔軟性に優れた強力なサポートモデルである FlexPod 共同サポートを確立しました。このモデルでは、ネットアップと Cisco が提供する経験、リソース、およびテクニカルサポートの専門知識を組み合わせて、問題の発生場所に関係なく、 FlexPod サポート問題を特定して解決するための合理的なプロセスを提供します。FlexPod 共同サポートモデルは、お客様の FlexPod システムが効率的に動作し、最新のテクノロジを活用できることを確認すると同時に、経験豊富なチームが統合の問題の解決を支援します。

  FlexPod 共同サポートは、医療機関がビジネスクリティカルなアプリケーションを実行する場合に特に有効です。次の図は、 FlexPod 共同サポートモデルの概要を示しています。



適用範囲

このドキュメントでは、この医用画像処理解決策をホストするための Cisco Unified Computing System （ Cisco UCS ）と NetApp ONTAP ベースの FlexPod インフラの技術概要について説明します。

対象者

本ドキュメントは、医療業界の技術リーダー、 Cisco とネットアップのパートナーソリューションエンジニア、およびプロフェッショナルサービス担当者を対象としています。ネットアップは、読者がコンピューティングとストレージのサイジングの概念を十分に理解していること、および医用画像システム、 Cisco UCS 、ネットアップストレージシステムに関する技術的な知識を持っていることを前提としています。

医療画像アプリケーション

典型的な医療画像処理アプリケーションでは、中小規模、大規模の医療機関向けにエンタープライズクラスの画像処理解決策を作成するアプリケーションスイートを提供しています。

製品スイートの中心には、次の臨床的能力があります。

- エンタープライズイメージングリポジトリ
- 放射線や心臓などの従来の画像ソースをサポートします。また、眼科、皮膚科、結腸内視鏡検査、写真やビデオなどの医療用画像機器など、その他のケア分野もサポートしています。
- "画像のアーカイブと通信システム" （ PACS ）。従来の放射線フィルムの役割をコンピュータ化した方法で置き換えます

- Enterprise Imaging Vendor Neutral Archive （ VNA ）：
  - DICOM ドキュメントおよび非 DICOM ドキュメントの拡張可能な統合
  - 中央集中型医用画像システム
  - 企業内の複数の（ ACS ）間でのドキュメント同期およびデータ整合性のサポート
  - 次のようなドキュメントメタデータを活用するルールベースのエキスパートシステムによるドキュメントライフサイクル管理
  - モダリティタイプ
  - 調査の年齢
  - 患者の年齢（現在および画像取得時）
  - 企業の内部と外部（ HIE) との統合の一元化：
  - コンテキスト認識ドキュメントのリンク
  - Health Level 7 International （ HL7 ）、 DICOM 、および WADO
  - ストレージに依存しないアーカイブ機能
- HL7 および状況認識リンクを使用するその他の医療情報システムとの統合：
  - EHR では、患者チャートや画像ワークフローなどから患者画像への直接リンクを実装できます。
  - 患者の長手治療画像履歴を EHR に埋め込むことができます。
- 放射線技師のワークフロー
- あらゆるデバイスのどこからでも画像を表示できる、ゼロフットプリントの大企業視聴者
- 過去のデータとリアルタイムデータを活用する分析ツール：
  - コンプライアンスレポート
  - 運用レポート
  - 品質管理および品質保証レポート

医療機関の規模とプラットフォームのサイジング

医療機関は、 ACO などのプログラムを支援する標準ベースの手法を使用して、広範囲に分類できます。そのような分類の 1 つは、臨床統合ネットワーク（ CIN ）の概念を使用します。病院のグループは、実績のある標準的な臨床プロトコルや経路に協力して準拠することで、治療の価値を高め、患者のコストを削減する場合に、 CIN と呼ばれます。CIN 内の病院には、 CIN の中核的な価値観に従った医師のオンボード制御と実践が行われています。従来、統合型デリバリネットワーク（ IDN ）は病院および医師グループに限定されていました。CIN は従来の IDN 境界を越えており、 CIN は ACO の一部である場合もあります。CIN の原則に従い、医療機関は小規模、中規模、大規模に分類できます。

小規模な医療機関

医療機関は、外来診療所と入院診療科を持つ病院が 1 つだけの場合は小規模ですが、 CIN の一部ではありません。医師は介護者として働き、ケアの連続性において患者の治療を調整します。これらの小規模な組織には通常、医師が運営する施設が含まれています。患者に対する総合的な治療として、緊急治療や外傷治療を実施する場合とそうでない場合がある。一般的に、小規模な医療機関では年間約 25 万件の臨床画像検査を実施しています。イメージングセンターは小規模な医療機関とみなされ、イメージングサービスを提供します。一部の組織では、放射線ディクテーションサービスも提供しています。

中規模の医療機関

以下のような、焦点を絞った組織を持つ複数の病院システムが含まれている場合、医療機関は中規模と見なされます。

- 成人診療所および成人入院患者の病院
- 労働および配送部門
- 育児医院および小児入院病院
- がん治療センター
- 成人の緊急部門
- 子供の緊急部門
- 家族の薬および主要な心配のオフィス
- 成人の外傷治療センター
- 小児外傷治療センター

中規模の医療機関では、医師は CIN の原則に従い、 1 つのユニットとして運用します。病院には、病院、医師、薬局などの別々の請求機能があります。病院は、学術研究機関に関連付けられ、インターベンションに適した臨床研究や臨床試験を行う場合があります。中規模の医療機関は、年間 50 万件もの臨床画像検査を実施しています。

大規模な医療機関

医療機関は、中規模の医療組織の特性を含めて大規模とみなされ、複数の地域のコミュニティに中規模の臨床機能を提供します。

大規模な医療機関では、通常、次のような機能があります。

- 全体的な機能を管理するセントラルオフィスがある
- 他の病院との合弁事業に参加する
- 支払者組織と年に 1 回料金を交渉します
- 都道府県ごとに支払者率をネゴシエートします
- 有意義な使用 (MU) プログラムに参加する
- 標準ベースの母集団 Health Management （ PHM ）ツールを使用して、母集団の健康コホート全体で高度な臨床研究を行っています
- 年間最大 100 万件の臨床画像検査を実施します

CIN に参加している大規模な医療機関にも、 AI ベースの画像読み取り機能があります。これらの組織は通常、年間 100 万～ 200 万件の臨床画像検査を実施しています。

これらの異なるサイジングの組織が最適なサイズの FlexPod システムにどのように変わるかを確認するには、 FlexPod のさまざまなコンポーネントと FlexPod システムの各種機能について理解しておく必要があります。

Cisco Unified Computing System の略

Cisco UCS は、統合 I/O インフラストラクチャと相互接続された単一の管理ドメインで構成されます。医療画像処理環境向け Cisco UCS は、ネットアップの医療画像処理システムインフラに関する推奨事項とベストプラクティスに沿っています。これにより、インフラで重要な患者情報を最大限に利用できるようになります。

エンタープライズ医用画像処理のコンピューティング基盤は Cisco UCS テクノロジーで、統合システム管理、 Intel Xeon プロセッサ、およびサーバ仮想化を備えています。これらの統合テクノロジーは、データセンターの課題を解決し、一般的な医療画像システムを使用してデータセンター設計の目標を達成します。Cisco UCS は、 LAN 、 SAN 、およびシステム管理を 1 つのシンプルなリンクに統合して、ラックサーバ、ブレードサーバ、および仮想マシン（ VM ）を実現します。Cisco UCS は、冗長ペアの Cisco UCS ファブリックインターコネクトで構成されており、単一の管理ポイントと、すべての I/O トラフィックを一元的に制御できます。

Cisco UCS はサービスプロファイルを使用して、 Cisco UCS インフラストラクチャ内の仮想サーバが正しく一貫して設定されるようにします。サービスプロファイルには、 LAN および SAN アドレッシング、 I/O 設定、ファームウェアバージョン、ブート順、ネットワーク仮想 LAN （ VLAN ）、物理ポート、 QoS ポリシーなど、サーバ ID に関する重要なサーバ情報が含まれます。サービスプロファイルは、数時間や数日単位ではなく、システム内の任意の物理サーバに動的に作成して関連付けることができます。サービスプロファイルと物理サーバの関連付けは、 1 回のシンプルな操作として実行されます。この操作により、物理的な設定変更を必要とせずに、環境内のサーバ間で ID を移行できます。また、障害が発生したサーバの代わりに、ベアメタルプロビジョニングを迅速に実行できます。

サービスプロファイルを使用することで、企業全体で一貫したサーバ構成が行われるようになります。複数の Cisco UCS 管理ドメインを使用する場合、 Cisco UCS Central はグローバルサービスプロファイルを使用して、ドメイン間で設定およびポリシー情報を同期できます。1 つのドメインでメンテナンスを実行する必要がある場合は、仮想インフラストラクチャを別のドメインに移行できます。このアプローチでは、 1 つのドメインがオフラインの場合でも、アプリケーションは高可用性を維持します。

Cisco UCS は、ブレードおよびラックサーバコンピューティング向けの次世代解決策です。このシステムは、低レイテンシでロスレスの 40GbE ユニファイドネットワークファブリックと、エンタープライズクラスの x86 アーキテクチャサーバを統合しています。このシステムは、拡張性に優れた統合型マルチシャーシプラットフォームであり、すべてのリソースが統合された管理ドメインに参加します。Cisco UCS は、エンドツーエンドのプロビジョニングと移行サポートを通じて、仮想化システムと非仮想化システムの両方で、新しいサービスの提供をシンプルかつ確実かつセキュアに高速化します。Cisco UCS には次の機能があります。

- 包括的な管理
- 徹底的な簡素化
- ハイパフォーマンス

Cisco UCS は次のコンポーネントで構成されています。

- * コンピューティング。 * このシステムは、インテル ® Xeon ® スケーラブル・プロセッサー製品ファミリーをベースにしたラックマウント型およびブレードサーバーを組み込んだ、まったく新しいクラスのコンピューティング・システムをベースとしています。
- * ネットワーク。 * このシステムは、低遅延、ロスレス、 40Gbps のユニファイドネットワークファブリックに統合されています。このネットワーク基盤は、 LAN 、 SAN 、ハイパフォーマンスコンピューティングネットワークを統合したもので、現在は別々のネットワークです。ユニファイドファブリックは、ネットワークアダプタ、スイッチ、ケーブルの数を減らし、必要な電力と冷却コストを削減することで、コストを削減します。

- * 仮想化 * 仮想化システムは、仮想環境の拡張性、パフォーマンス、運用管理を強化することで、仮想化の可能性を最大限に引き出します。シスコのセキュリティ、ポリシー適用、診断機能が仮想化環境に拡張され、ビジネス要件と IT 要件の変化をより適切にサポートできるようになりました。
- * ストレージ・アクセス。 * ユニファイド・ファブリックを介した SAN ストレージと NAS への統合アクセスを提供します。Software-Defined Storage にも最適なシステムです。単一のフレームワークのメリットを組み合わせることで、コンピューティングサーバとストレージサーバの両方を 1 つのペインで管理できるので、必要に応じて QoS を実装して、システムに I/O スロットリングを導入できます。また ' サーバ管理者はストレージ・リソースにストレージ・アクセス・ポリシーを事前に割り当てることができるため ' ストレージの接続と管理が容易になり ' 生産性が向上します外部ストレージに加えて、ラックサーバとブレードサーバの両方に内蔵ストレージがあり、組み込みのハードウェア RAID コントローラからアクセスできます。Cisco UCS Manager でストレージプロファイルとディスク構成ポリシーを設定することにより、ホスト OS とアプリケーションデータのストレージニーズは、ユーザ定義の RAID グループによって満たされます。その結果、高可用性と優れたパフォーマンスが実現します。
- * 管理。 * システムはすべてのシステムコンポーネントを一意に統合し、解決策全体を Cisco UCS Manager によって単一のエンティティとして管理できるようにします。すべてのシステム構成と運用を管理するために、 Cisco UCS Manager には、わかりやすい GUI 、 CLI 、強力なスクリプトライブラリモジュールが用意されています。このモジュールは、堅牢な API をベースに構築されています。

Cisco Unified Computing System は、アクセスレイヤネットワーキングとサーバを統合します。この高性能な次世代サーバシステムは、データセンターにワークロードの即応性と拡張性をもたらします。

Cisco UCS Manager の略

Cisco UCS Manager は、 Cisco UCS のすべてのソフトウェアコンポーネントとハードウェアコンポーネントを統合管理します。単一接続テクノロジーを使用することで、 UCS Manager は数千台の VM に対して複数のシャーシを管理、制御、管理します。管理者は、直感的な GUI 、 CLI 、 XML API を使用して、 Cisco UCS 全体を単一の論理エンティティとして管理できます。Cisco UCS Manager は、クラスタ化されたアクティブ / スタンバイ構成を使用してハイアベイラビリティを実現する、 2 つの Cisco UCS 6300 シリーズファブリックインターコネクト上に配置されます。

Cisco UCS Manager は、サーバ、ネットワーク、ストレージを統合した統合管理インターフェイスを提供します。Cisco UCS Manager は自動検出を実行して、追加または変更したシステムコンポーネントのインベントリの検出、管理、およびプロビジョニングを行います。サードパーティとの統合に対応した包括的な XML API セットを提供し、 9 、 000 箇所の統合ポイントを公開します。また、自動化やオーケストレーションのためのカスタム開発を容易にし、システムの可視性と制御を新たなレベルに引き上げます。

サービスプロファイルは、仮想環境と非仮想環境のどちらにも適しています。この機能により、ワークロードをサーバ間で移動したり、サーバをオフラインにしてサービスやアップグレードを行ったりするときなど、非仮想化サーバのモビリティが向上します。また、プロファイルを仮想化クラスタと組み合わせて使用することで、新しいリソースを簡単にオンラインにし、既存の VM のモビリティを補完することもできます。

Cisco UCS Manager の詳細については、を参照してください "Cisco UCS Manager の製品ページ"。

Cisco UCS の差別化要因

Cisco Unified Computing System は、データセンターでのサーバ管理の方法に革命を起こしています。Cisco UCS および Cisco UCS Manager の次の独自の差別化要因について説明します。

- * 組み込み管理。 * Cisco UCS では、サーバはファブリックインターコネクトの組み込みファームウェアによって管理されるため、外部の物理デバイスや仮想デバイスを管理する必要がありません。
- * ユニファイドファブリック。 * Cisco UCS では、ブレードサーバシャーシまたはラックサーバからファブリックインターコネクトまで、 LAN 、 SAN 、および管理トラフィック用に 1 本のイーサネットケーブ

ルを使用します。この I/O 統合により、必要なケーブル、 SFP 、アダプタの数が削減され、解決策全体の設備投資と運用コストが削減されます。

- * 自動検出。 * ブレードサーバをシャーシに挿入するだけで、またはラックサーバをファブリックインターコネクトに接続することで、コンピューティングリソースの検出とインベントリが自動的に実行されます。管理者の介入は必要ありません。ユニファイドファブリックと自動検出機能を組み合わせることで、Cisco UCS の Wire-Once アーキテクチャが実現します。このアーキテクチャでは、コンピューティング機能を簡単に拡張しながら、 LAN 、 SAN 、および管理ネットワークへの既存の外部接続を維持できます。
- * ポリシーベースのリソース分類。 * コンピューティングリソースが Cisco UCS Manager によって検出されると、定義したポリシーに基づいて、自動的に特定のリソースプールに分類されます。この機能は、マルチテナントクラウドコンピューティングで役立ちます。
- * ラックとブレードサーバの管理を統合。 * Cisco UCS Manager は、同じ Cisco UCS ドメイン内で B シリーズブレードサーバと C シリーズラックサーバを管理できます。この機能とステートレスコンピューティングにより、コンピューティングリソースはハードウェアフォームファクタに依存しません。
- * モデルベースの管理アーキテクチャ。 * Cisco UCS Manager のアーキテクチャと管理データベースは、モデルベースおよびデータベースです。管理モデルで動作するオープン XML API により、 Cisco UCS Manager を他の管理システムと容易かつ拡張性の高い方法で統合できます。
- * ポリシー、プール、およびテンプレート。 * Cisco UCS Manager の管理方法は、整理された構成ではなく、ポリシー、プール、およびテンプレートの定義に基づいています。コンピューティング、ネットワーク、ストレージのリソースを管理するためのシンプルで緩やかに結合されたデータ主体のアプローチを実現します。
- * 参照整合性の緩み。 * Cisco UCS Manager では、サービスプロファイル、ポートプロファイル、またはポリシーは、他のポリシーや、参照整合性の緩い他の論理リソースを参照できます。参照ポリシーは参照ポリシーの作成時に存在することはできませんが、参照ポリシーは他のポリシーが参照ポリシーを参照している場合でも削除できます。この機能により、さまざまな分野のエキスパートが互いに独立して作業することができます。ネットワーク、ストレージ、セキュリティ、サーバ、仮想化など、さまざまなドメインのさまざまなエキスパートが連携して複雑なタスクを実行できるため、柔軟性が大幅に向上します。
- * ポリシー解決。 * Cisco UCS Manager では、実際のテナントや組織の関係を模倣する組織単位階層のツリー構造を作成できます。組織階層のさまざまなレベルで、さまざまなポリシー、プール、およびテンプレートを定義できます。別のポリシーを名前で参照するポリシーは、最も近いポリシーに一致する組織階層で解決されます。ルート組織の階層に特定の名前を持つポリシーが見つからない場合は、「 default 」という名前の特別なポリシーが検索されます。このポリシー解決手法により、自動化に対応した管理 API が実現し、さまざまな組織のオーナーに柔軟性がもたらされます。
- * サービス・プロファイルとステートレス・コンピューティング。 * サービス・プロファイルは、サーバを論理的に表現したもので、さまざまなアイデンティティとポリシーを保持します。リソース要件を満たしていれば、この論理サーバを任意の物理コンピューティングリソースに割り当てることができます。ステートレスコンピューティングにより、サーバの調達が数分で完了し、従来のサーバ管理システムでは数日かかっていました。
- * 組み込みのマルチテナンシーサポート。 * ポリシー、プール、テンプレート、参照整合性の緩み、組織階層でのポリシー解決、およびコンピューティングリソースに対するサービスプロファイルベースのアプローチの組み合わせにより、 Cisco UCS Manager は、一般にプライベートクラウドとパブリッククラウドで見られるマルチテナント環境に本質的に適しています。
- * 拡張メモリ。 * エンタープライズクラスの Cisco UCS B200 M5 ブレードサーバは、ハーフ幅のブレードフォームファクタで Cisco Unified Computing System ポートフォリオの機能を拡張します。Cisco UCS B200 M5 は、最新の Intel Xeon スケーラブルプロセッサ CPU のパワーと最大 3TB の RAM を活用します。この機能により、多数の導入環境で必要とされる VM と物理サーバの比率が大幅になります。また、特定のアーキテクチャでビッグデータなどの大規模なメモリ処理をサポートすることもできます。
- * 仮想化対応ネットワーク。 * Cisco Virtual Machine Fabric Extender （ VM-FEX ）テクノロジーは、アク

セスネットワークレイヤにホスト仮想化を認識させます。この認識により、ネットワーク管理者チームによって定義されたポートプロファイルによって仮想ネットワークが管理される場合に、仮想化によるコンピューティングおよびネットワークドメインの汚染を防止できます。VM-FEX は、ハードウェア内でスイッチングを実行することでハイパーバイザ CPU をオフロードし、ハイパーバイザ CPU がより多くの仮想化関連タスクを実行できるようにします。クラウド管理を簡素化するために、 VM-FEX テクノロジーは VMware vCenter 、 Linux Kernel-Based Virtual Machine （ KVM ）、および Microsoft Hyper-V SR-IOV と十分に統合されています。

- * QoS の簡素化。 * FC とイーサネットは Cisco UCS に統合されていますが、 QoS とロスレスイーサネットのサポートが組み込まれているため、シームレスに動作します。Cisco UCS Manager では、すべてのシステムクラスを 1 つの GUI パネルに表示することで、ネットワーク QoS が簡素化されます。

Cisco Nexus IP スイッチおよび **MDS** スイッチ

Cisco Nexus スイッチと Cisco MDS マルチレイヤディレクタを使用すると、エンタープライズクラスの接続と SAN 統合を実現できます。シスコのマルチプロトコルストレージネットワーキングは、 FC 、 Fibre Connection （ FICON ）、 FC over Ethernet （ FCoE ）、 iSCSI 、 FC over IP （ FCIP ）などの柔軟性とオプションを提供することで、ビジネスリスクを軽減します。

Cisco Nexus スイッチは、単一プラットフォームで最も包括的なデータセンターネットワーク機能セットの 1 つです。データセンターとキャンパスコアの両方で、高いパフォーマンスと密度を実現します。また、耐障害性に優れたモジュラプラットフォームで、データセンターのアグリゲーション、行の終わり、およびデータセンターのインターコネクト環境に完全な機能セットを提供します。

Cisco UCS は、コンピューティングリソースを Cisco Nexus スイッチと統合し、さまざまなタイプのネットワークトラフィックを識別して処理するユニファイドファブリックを提供します。このトラフィックには、ストレージ I/O 、デスクトップトラフィックのストリーミング、管理、臨床アプリケーションやビジネスアプリケーションへのアクセスが含まれます。次の機能を利用できます。

- * インフラストラクチャの拡張性。 * 仮想化、電力と冷却の効率化、自動化によるクラウドの拡張、高密度、およびパフォーマンスのすべてが、効率的なデータセンターの拡張をサポートします。
- * 運用の継続性。 * この設計では、ハードウェア、 Cisco NX-OS ソフトウェアの機能、および管理を統合して、ダウンタイムゼロの環境をサポートします。
- * 転送の柔軟性。 * このコスト効率の高い解決策を使用して、新しいネットワークテクノロジを段階的に導入できます。

Cisco UCS と Cisco Nexus スイッチおよび MDS マルチレイヤディレクタを組み合わせることで、エンタープライズ医用画像システム向けのコンピューティング、ネットワーキング、 SAN 接続の解決策が実現します。

ネットアップのオールフラッシュストレージ

ONTAP ソフトウェアを実行するネットアップストレージは、ストレージの総コストを削減すると同時に、医療画像処理システムのワークロードに必要な、読み取り / 書き込みの応答時間を短縮し、高い IOPS を実現します。一般的な医用画像システムの要件を満たす最適なストレージシステムを構築するため、 ONTAP はオールフラッシュとハイブリッドストレージの両方の構成をサポートしています。ネットアップのフラッシュストレージは、医療画像システムのお客様に、高パフォーマンスと応答性の主要コンポーネントを提供し、遅延の影響を受けやすい医療画像システムの運用をサポートします。ネットアップのテクノロジでは、 1 つのクラスタに複数の障害ドメインを作成することで、本番環境と非本番環境を分離することもできます。また、 ONTAP の最小 QoS で、システムのパフォーマンスが特定のレベルを下回ることのないようにすることで、システムのパフォーマンスの問題が軽減されます。

ONTAP ソフトウェアのスケールアウトアーキテクチャは、さまざまな I/O ワークロードに柔軟に対応できま

す。臨床アプリケーションに必要なスループットと低レイテンシを実現し、モジュラ型のスケールアウトアーキテクチャを提供するために必要なスループットを実現するために、通常は ONTAP アーキテクチャで使用されます。NetApp AFF ノードは、ハイブリッド（ HDD およびフラッシュ）ストレージノードと同じスケールアウトクラスタに混在させることができ、スループットの高い大規模データセットの格納に適しています。高価な SSD ストレージから他のノード上のより経済的な HDD ストレージに医用画像システム環境の複製、複製、バックアップを実行できます。ネットアップのクラウド対応ストレージとデータファブリックを使用すれば、オンプレミスまたはクラウドのオブジェクトストレージにバックアップできます。

医療画像処理では、 ONTAP は主要な医療画像システムによって検証されています。つまり、医用画像処理のための高速で信頼性の高い性能を提供するためにテストされています。さらに、次の機能によって、管理が簡易化され、可用性と自動化が向上し、必要なストレージの総容量が削減されます。

- * 卓越したパフォーマンス。 * NetApp AFF 解決策は、他の NetApp FAS 製品ファミリーと同じユニファイドストレージアーキテクチャ、 ONTAP ソフトウェア、管理インターフェイス、充実したデータサービス、高度な機能セットを提供します。オールフラッシュメディアと ONTAP を組み合わせたこの革新的なソリューションは、業界をリードする ONTAP ソフトウェアを使用して、オールフラッシュストレージの一貫した低レイテンシと高 IOPS を実現します。
- * ストレージ効率。 * NetApp SME と連携して、貴社固有の医療画像システムがどのように適用されたかを把握することができます。
- * スペース効率に優れたクローニング。 * FlexClone 機能を使用すると、ほぼ瞬時にクローンを作成し、バックアップとテストの環境更新をサポートできます。これらのクローンは、変更が行われた場合にのみストレージを消費します。
- * 統合されたデータ保護。 * 完全なデータ保護と災害復旧機能により、重要なデータ資産を保護し、災害復旧を実現します。
- * ノンストップオペレーション。 * データをオフラインにすることなく、アップグレードとメンテナンスを実行できます。
- * QoS 。 * ストレージ QoS により、潜在的な Bully ワークロードを制限できます。さらに重要なのは、 QoS によって最小のパフォーマンス保証が作成されることです。これは、医用画像システムの本番環境などの重要なワークロードのシステムパフォーマンスが特定のレベルを下回ることがないことを保証するものです。また、競合を制限することで、ネットアップの QoS によってパフォーマンス関連の問題を軽減できます。
- * データファブリック。 * デジタル変革を加速するため、ネットアップのデータファブリックは、クラウド環境とオンプレミス環境全体でデータ管理を簡易化、統合します。データ管理のための一貫した統合的サービスとアプリケーションを提供することで、優れたデータの可視性と分析、データのアクセスと制御、データの保護とセキュリティを実現します。ネットアップは、 AWS 、 Azure 、 Google Cloud 、 IBM Cloud などの大規模なパブリッククラウドと統合されており、 幅広い選択肢を提供します。

ホストの仮想化： **VMware vSphere**

FlexPod アーキテクチャは、業界をリードする仮想化プラットフォームである VMware vSphere 6.x で検証済みです。VM の導入と実行には VMware ESXi 6.x が使用されます。vCenter Server Appliance 6.x は、 ESXi ホストと VM の管理に使用されます。Cisco UCS B200 M5 ブレードで実行される複数の ESXi ホストを使用して、 VMware ESXi クラスタを形成します。VMware ESXi クラスタは、すべてのクラスタノードのコンピューティング、メモリ、およびネットワークリソースをプールし、クラスタで実行されている VM に耐障害性に優れたプラットフォームを提供します。VMware ESXi クラスタの機能である vSphere High Availability （ vSphere 高可用性）と Distributed Resource Scheduler （ DRS ）は、いずれも vSphere クラスタの障害耐性に貢献し、 VMware ESXi ホスト間でリソースを分散するのに役立ちます。

ネットアップストレージプラグインと Cisco UCS プラグインは VMware vCenter と統合されるため、必要なストレージリソースとコンピューティングリソースの運用ワークフローを実現できます。

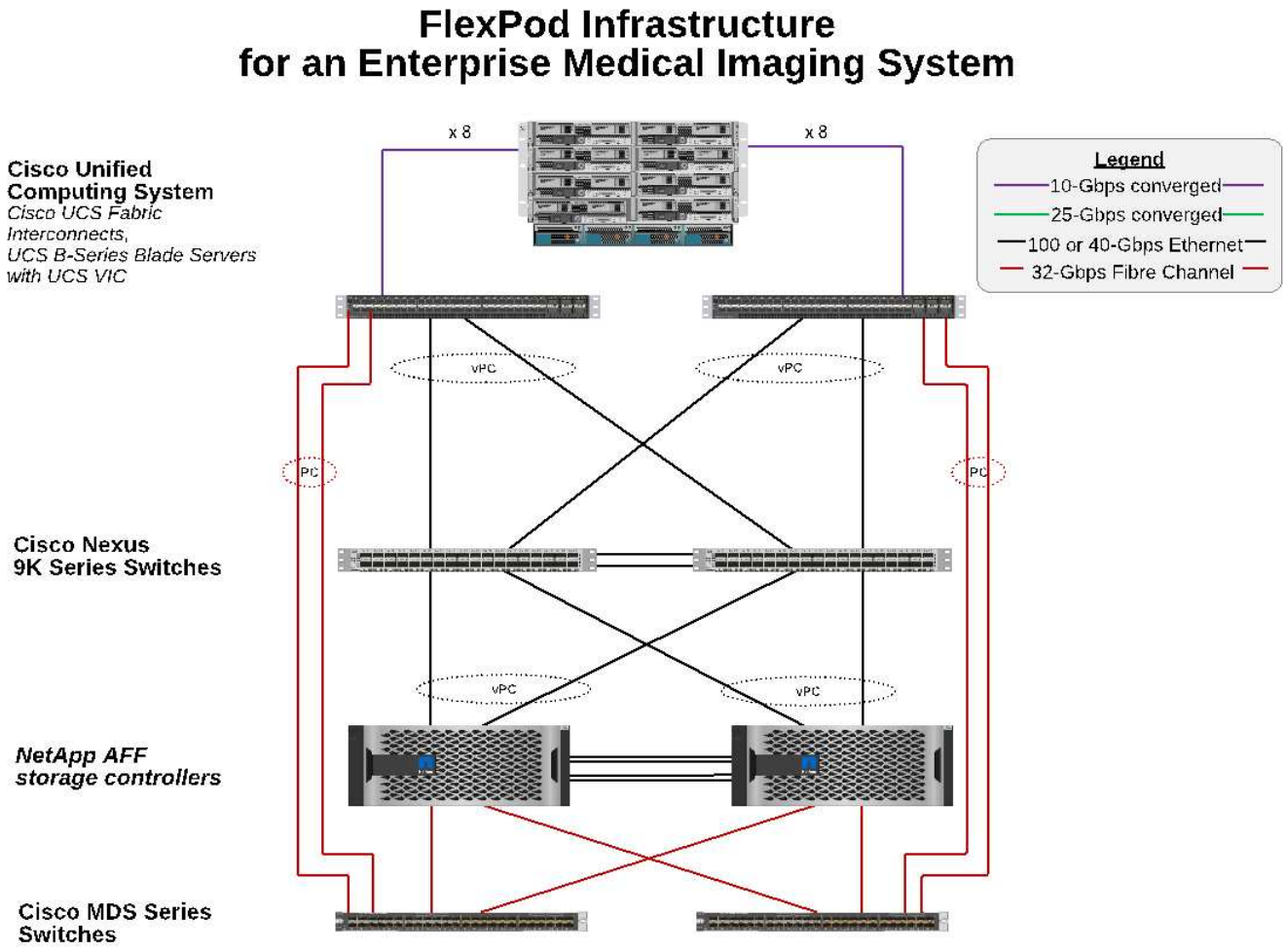
VMware ESXi クラスタと vCenter Server を使用すると、医療画像処理環境を VM に導入するための一元的なプラットフォームが提供されます。医療機関は、以下のような業界をリードする仮想インフラのメリットを確実に実現できます。

- * シンプルな導入。 * 仮想アプライアンスを使用して、 vCenter Server を迅速かつ簡単に導入できます。
- * 一元管理と可視性。 * vSphere インフラストラクチャ全体を 1 箇所から管理します。
- * プロアクティブな最適化。 * リソースの割り当て、最適化、移行を行い、効率を最大限に高めます。
- * 管理。 * 強力なプラグインとツールを使用して、管理を簡素化し、制御を拡張します。

アーキテクチャ

FlexPod アーキテクチャは、コンピューティング、ネットワーク、ストレージスタック全体でコンポーネントやリンクに障害が発生した場合に高可用性を提供するように設計されています。クライアントアクセスとストレージアクセス用に複数のネットワークパスを用意することで、ロードバランシングとリソース利用率の最適化を実現します。

次の図は、医用画像システム解決策環境用の 16Gb FC/40Gb イーサネット（ 40GbE ）トポロジを示しています。



ストレージアーキテクチャ

このセクションのストレージアーキテクチャのガイドラインを使用して、エンタープライズ医用画像システム用のストレージインフラを構成します。

ストレージ階層

一般的なエンタープライズ医用画像環境は、複数の異なるストレージ階層で構成されています。各階層には、パフォーマンスとストレージプロトコルに関する固有の要件があります。ネットアップのストレージはさまざまな RAID テクノロジをサポートしており、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"。以下に、 NetApp AFF ストレージシステムが、イメージングシステムのさまざまなストレージ階層のニーズに対応する仕組みを示します。

- * パフォーマンス・ストレージ（階層 1 ）。 * この階層は、データベース、 OS ドライブ、 VMware VMFS （ Virtual Machine File System ）データストアなどに、高いパフォーマンスと高い冗長性を提供します。ONTAP に設定されているように、ブロック I/O は、ファイバを介して SSD の共有ストレージアレイに移動されます。最小レイテンシは 1 ミリ秒 ~3 ミリ秒で、一時的にピークは 5 ミリ秒に設定されます。このストレージ階層は通常、短期保存キャッシュに使用されます。通常、オンライン DICOM 画像にすばやくアクセスするための 6 〜 12 か月の画像保存に使用されます。この階層は、イメージキャッシュやデータベースバックアップなどに高パフォーマンスと高冗長性を提供します。ネットアップのオールフラッシュアレイは、持続可能な帯域幅で 1 ミリ秒未満のレイテンシを実現します。これは、一般的なエンタープライズ医用画像環境で想定されるサービス時間よりもはるかに短くなります。NetApp ONTAP RAID-TEC は、 3 つのディスク障害に対応するためにトリプルパリティ RAID ）と RAID DP （ 2 つのディスク障害に対応するためにダブルパリティ RAID ）の両方をサポートしています。
- * アーカイブ・ストレージ（階層 2 ）。 * この階層は、一般的なコスト最適化ファイル・アクセス、大容量ボリューム用の RAID 5 または RAID 6 ストレージ、長期的な低コスト / パフォーマンス・アーカイブに使用されます。NetApp ONTAP RAID-TEC は、 3 つのディスク障害に対応するためにトリプルパリティ RAID ）と RAID DP （ 2 つのディスク障害に対応するためにダブルパリティ RAID ）の両方をサポートしています。FlexPod の NetApp FAS を使用すると、 NFS / SMB 経由で SAS ディスクアレイにアプリケーション I/O をイメージングできます。NetApp FAS システムは、持続可能な帯域幅で最大 10 ミリ秒のレイテンシを実現します。エンタープライズ医用画像システム環境のストレージティア 2 では、予想されるサービス時間よりもはるかに短くなります。

ハイブリッドクラウド環境でのクラウドベースのアーカイブは、 S3 などのプロトコルを使用してパブリッククラウドストレージプロバイダにアーカイブする場合に使用できます。NetApp SnapMirror テクノロジを使用すると、オールフラッシュアレイまたは FAS アレイから低速のディスクベースストレージアレイ、または Cloud Volumes ONTAP for AWS 、 Azure 、 Google Cloud にイメージデータをレプリケーションできます。

NetApp SnapMirror は、業界をリードするデータレプリケーション機能を備えており、ユニファイドデータレプリケーションによって医療画像システムを保護します。フラッシュ、ディスク、クラウドにわたるクロスプラットフォームレプリケーションにより、データファブリック全体でデータ保護管理を簡易化できます。

- ネットアップストレージシステム間でデータをシームレスかつ効率的に転送し、同じターゲットボリュームと I/O ストリームを使用してバックアップとディザスタリカバリの両方をサポートします。
- 任意のセカンダリボリュームにフェイルオーバーします。セカンダリストレージ上の任意のポイントインタイム Snapshot からリカバリします。
- データ損失ゼロの同期レプリケーション（ RPO=0 ）により、最も重要なワークロードを保護します。
- ネットワークトラフィックを削減効率的な運用でストレージの設置面積を縮小
- 変更されたデータブロックのみが転送されるため、ネットワークトラフィックが軽減されます。
- 重複排除、圧縮、コンパクションなどのストレージ効率化のメリットを、転送時もプライマリストレージで維持できます。

- ネットワーク圧縮機能によりインライン効率化をさらに向上

詳細については、を参照してください "こちらをご覧ください"。

次の表は、一般的な医用画像システムで特定の遅延およびスループットパフォーマンス特性に必要な各階層を示しています。

ストレージ階層	要件	ネットアップが推奨します
1.	1 ～ 5 ミリ秒の遅延 35 ～ 500 Mbps のスループット	1 ミリ秒未満のレイテンシ AFF が設定された AFF A300 ハイアベイラビリティ（ HA ）ペアで 2 台のディスクシェルフを使用すると、最大 1.6GBps のスループットを処理できます
2.	オンプレミスアーカイブ	FAS で最大 30 ミリ秒のレイテンシを実現
	クラウドへのアーカイブ	Cloud Volumes ONTAP への SnapMirror レプリケーション、または NetApp StorageGRID ソフトウェアによるバックアップのアーカイブ

ストレージネットワーク接続

FC ファブリック

- FC ファブリックは、コンピューティングからストレージへのホスト OS I/O に対応します。
- 2 つの FC ファブリック（ファブリック A とファブリック B ）がそれぞれ Cisco UCS ファブリック A と UCS ファブリック B に接続されています。
- 各コントローラノードには、 2 つの FC 論理インターフェイス（ LIF ）を備えた Storage Virtual Machine （ SVM ）があります。各ノードで、 1 つの LIF をファブリック A に接続し、もう 1 つの LIF をファブリック B に接続します
- 16Gbps FC のエンドツーエンド接続は、 Cisco MDS スイッチ経由で行われます。単一のイニシエータポート、複数のターゲットポート、およびゾーニングがすべて設定されている必要があります。
- FC SAN ブートは、完全なステートレスコンピューティングを作成するために使用されます。サーバは、AFF ストレージクラスタでホストされているブートボリューム内の LUN からブートされます。

iSCSI 、 **NFS** 、 **SMB / CIFS** 経由のストレージアクセス用の **IP** ネットワーク

- 各コントローラノードの SVM に iSCSI LIF が 2 つあります。各ノードで 1 つの LIF をファブリック A に接続し、 2 つ目の LIF をファブリック B に接続します
- NAS データ LIF が各コントローラノードの SVM に 2 つあります。各ノードで 1 つの LIF をファブリック A に接続し、 2 つ目の LIF をファブリック B に接続します
- スイッチ N9k-B への 10Gbps リンク用のストレージポートインターフェイスグループ（仮想ポートチャネル [vPC] ）、スイッチ N9k-B への 10Gbps リンク用
- VM からストレージへの ext4 または NTFS ファイルシステムのワークロード：

- IP 経由の iSCSI プロトコル。
- NFS データストアでホストされている VM ：
  - VM OS I/O は、 Nexus スイッチを介して複数のイーサネットパスを経由します。

インバンド管理（アクティブ / パッシブボンド）

- 管理スイッチ N9k-B に 1Gbps リンク、管理スイッチ N9k-B に 1Gbps リンク

バックアップとリカバリ

FlexPod データセンターは、ネットアップの ONTAP データ管理ソフトウェアで管理されるストレージアレイ上に構築されます。ONTAP ソフトウェアは 20 年以上にわたって進化し、 VM 、 Oracle データベース、 SMB / CIFS ファイル共有、 NFS 向けにさまざまなデータ管理機能を提供してきました。また、 NetApp Snapshot テクノロジ、 SnapMirror テクノロジ、 NetApp FlexClone データレプリケーションテクノロジなどの保護テクノロジも提供します。NetApp SnapCenter ソフトウェアには、 VM 、 SMB / CIFS ファイル共有、 NFS 、 Oracle データベースのバックアップとリカバリに ONTAP の Snapshot 、 SnapRestore 、 FlexClone 機能を使用するためのサーバと GUI クライアントがあります。

NetApp SnapCenter ソフトウェアを採用しています "特許取得済み" Snapshot テクノロジ：ネットアップストレージボリューム上に、 VM または Oracle データベース全体のバックアップを瞬時に作成します。Oracle Recovery Manager （ RMAN ）と比較すると、 Snapshot コピーはブロックの物理コピーとして格納されないため、フルベースラインバックアップコピーは必要ありません。Snapshot コピーは、 Snapshot コピーが作成されたときに ONTAP WAFL ファイルシステムに存在していたストレージブロックへのポインタとして格納されます。このような物理的な緊密な関係により、 Snapshot コピーは元のデータと同じストレージアレイ上に保持されます。Snapshot コピーはファイルレベルで作成することもでき、バックアップをより細かく制御できます。

Snapshot テクノロジは、 Redirect-On-Write 方式に基づいています。最初はメタデータポインタのみを格納し、最初のデータ変更がストレージブロックに送信されるまでスペースをあまり消費しません。既存のブロックが Snapshot コピーによってロックされている場合、新しいブロックは ONTAP WAFL ファイルシステムによってアクティブコピーとして書き込まれます。この方法を用いると、書き込み時の変更手法で発生する二重書き込みを回避できます。

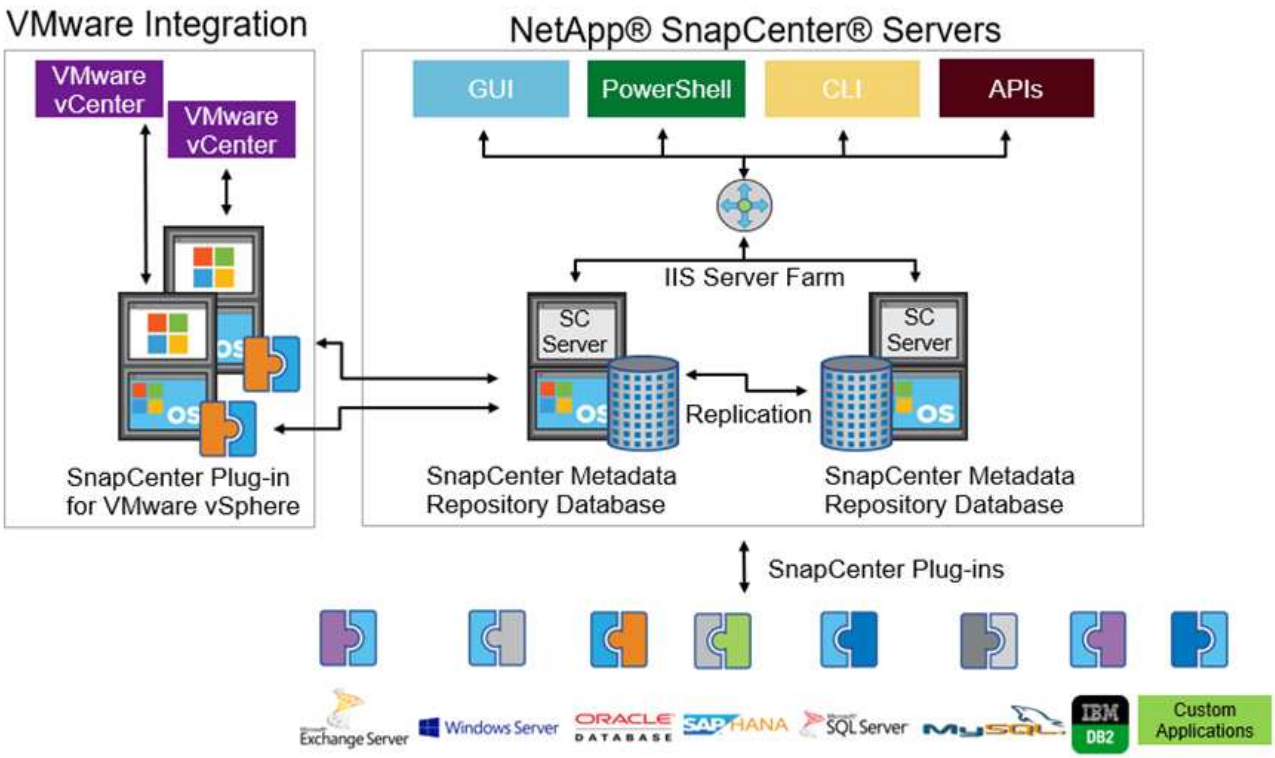
Oracle データベースのバックアップでは、 Snapshot コピーを使用することで時間を大幅に削減できます。たとえば、 RMAN のみを使用したバックアップの完了に 26 時間を要した場合、 SnapCenter ソフトウェアを使用した場合、完了までに 2 分未満かかることがあります。

また、データのリストアではデータブロックはコピーされず、 Snapshot コピーの作成時にアプリケーションと整合性のある Snapshot ブロックイメージへのポインタが反転されるため、 Snapshot バックアップコピーをほぼ瞬時にリストアできます。SnapCenter クローニングでは、既存の Snapshot コピーへのメタデータポインタの独立したコピーが作成され、ターゲットホストに新しいコピーがマウントされます。このプロセスは、高速かつストレージ効率にも優れています。

次の表に、 Oracle RMAN と NetApp SnapCenter ソフトウェアの主な違いをまとめます。

	バックアップ	リストア	クローン	フルバックアップが必要です	スペース使用量	オフサイトへのコピー
RMAN を使用します	遅い	遅い	遅い	はい。	高	はい。
SnapCenter	高速	高速	高速	いいえ	低	はい。

次の図に、 SnapCenter のアーキテクチャを示します。



NetApp MetroCluster の構成は、世界中の数千社の企業で、高可用性（ HA ）、データ損失ゼロ、データセンター内外のノンストップオペレーションに使用されます。MetroCluster は、 ONTAP ソフトウェアのフリー機能で、別々の場所または障害ドメインにある 2 つの ONTAP クラスタ間でデータと設定を同期的にミラーリングします。MetroCluster は、クラスタに書き込まれたデータを同期的にミラーリングすることで、 RPO （ Recovery Point Objective ：目標復旧時点）ゼロという 2 つの目標を自動的に処理することで、アプリケーション用の継続的な可用性を備えたストレージを提供します。ほぼゼロの RTO （ Recovery Time Objective ：目標復旧時間）：2 番目のサイトのデータをミラーリングし、 2 番目のサイトの MetroCluster でデータへのアクセスを自動化することで、 2 つのサイトにある 2 つの独立したクラスタ間でデータと設定を自動的にミラーリングすることができます1 つのクラスタ内でストレージがプロビジョニングされると、 2 つ目のサイトの 2 つ目のクラスタに自動的にミラーリングされます。NetApp SyncMirror テクノロジは、 RPO がゼロのすべてのデータの完全なコピーを提供します。そのため、 1 つのサイトのワークロードをいつでも反対のサイトに切り替えて、データを失うことなくデータの提供を継続できます。詳細については、を参照してください "こちらをご覧ください"。

ネットワーキング

Cisco Nexus スイッチのペアは、コンピューティングからストレージへの IP トラフィックと、医用画像システムイメージビューアの外部クライアントへの冗長パスを提供します。

- ポートチャネルと vPC を使用するリンクアグリゲーションは、全体的に採用されており、より高い帯域幅と高可用性を実現します。
  - vPC は、ネットアップストレージアレイと Cisco Nexus スイッチの間で使用されます。
  - vPC は、 Cisco UCS ファブリックインターコネクトと Cisco Nexus スイッチの間で使用されます。
  - 各サーバには、ユニファイドファブリックへの冗長接続を持つ仮想ネットワークインターフェイスカード（ vNIC ）があります。冗長性を確保するために、ファブリックインターコネクト間で NIC フェ

イルオーバーが使用されます。
    - 各サーバには仮想 Host Bus Adapter （ vHBA ）があり、ユニファイドファブリックに冗長接続されます。
- Cisco UCS ファブリックインターコネクトは、推奨されるようにエンドホストモードで設定され、アップリンクスイッチへの vNIC のダイナミックなピン接続を提供します。
- FC ストレージネットワークは、 Cisco MDS スイッチのペアによって提供されます。

コンピューティング： **Cisco Unified Computing System**

異なるファブリックインターコネクトを介して 2 つの Cisco UCS ファブリックが、 2 つの障害ドメインを提供します。各ファブリックは、 IP ネットワークスイッチと別々の FC ネットワークスイッチの両方に接続されます。

各 Cisco UCS ブレードのサービスプロファイルは、 FlexPod ESXi を実行するためのベストプラクティスに従って作成されます。各サービスプロファイルには、次のコンポーネントが必要です。

- NFS 、 SMB / CIFS 、およびクライアントまたは管理トラフィックを伝送する 2 つの vNIC （各ファブリックに 1 つ）
- NFS 、 SMB / CIFS 、およびクライアントまたは管理トラフィック用の vNIC に追加の必要な VLAN
- iSCSI トラフィックを伝送する 2 つの vNIC （各ファブリックに 1 つ）
- ストレージへの FC トラフィック用に 2 つのストレージ FC HBA （ファブリックごとに 1 つ）
- SAN ブート

仮想化

VMware ESXi ホストクラスタはワークロード VM を実行します。クラスタは、 Cisco UCS ブレードサーバ上で実行される ESXi インスタンスで構成されます。

各 ESXi ホストには、次のネットワークコンポーネントが含まれます。

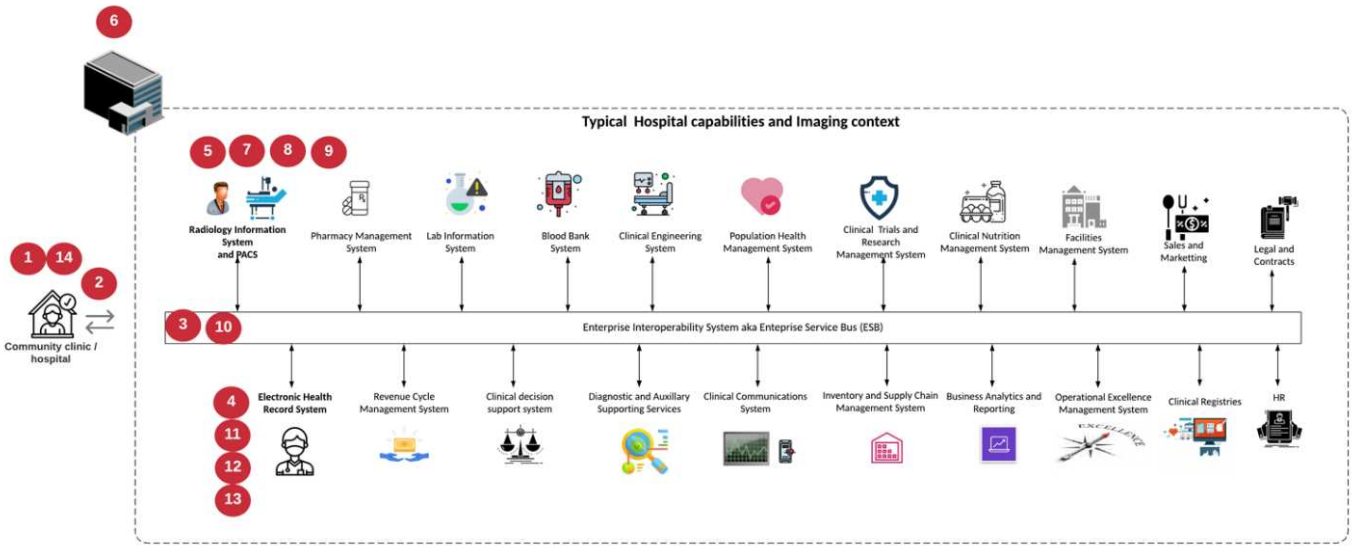
- FC または iSCSI で SAN をブートします
- ネットアップストレージ上のブート LUN （ブート OS 専用 FlexVol 内）
- NFS 、 SMB / CIFS 、または管理トラフィック用の 2 つの VMNIC （ Cisco UCS vNIC ）
- ストレージへの FC トラフィック用に 2 つのストレージ HBA （ Cisco UCS FC vHBA ）
- 標準スイッチまたは分散仮想スイッチ（必要に応じて）
- ワークロード VM 用の NFS データストア
- VM の管理、クライアントトラフィックネットワーク、およびストレージネットワークポートグループ
- 各 VM の管理、クライアントトラフィック、ストレージアクセス（ NFS 、 iSCSI 、または SMB / CIFS ）用のネットワークアダプタ
- VMware DRS が有効になりました
- ストレージへの FC または iSCSI パスに対してネイティブマルチパスが有効化されています
- VM の VMware スナップショットがオフになっています
- VM のバックアップ用に VMware 用に NetApp SnapCenter を導入

医用画像システムのアーキテクチャ

医療機関では、医療画像システムは重要なアプリケーションであり、患者の登録から始まり、収益サイクルで請求関連の活動を終えるまでの臨床ワークフローに統合されています。

次の図は、一般的な大病院におけるさまざまなシステムを示しています。この図は、一般的な医用画像システムのアーキテクチャコンポーネントを拡大する前に、医療画像システムにアーキテクチャのコンテキストを提供することを目的としています。ワークフローは多岐にわたり、病院やユースケースによって異なります。

次の図は、患者、コミュニティクリニック、および大規模な病院のコンテキストにおける医用画像システムを示しています。



1. 患者は、症状があるコミュニティクリニックを訪問します。相談中に、地域の医師は、 HL7 オーダーメッセージの形式で、より大きな病院に送信されるイメージングオーダーを作成します。
2. 地域の医師の EHR システムは、 HL7 オーダー / ORD メッセージを大規模な病院に送信します。
3. エンタープライズ相互運用性システム（ Enterprise Service Bus （ ESB ）とも呼ばれる）は、注文メッセージを処理し、注文メッセージを EHR システムに送信します。
4. EHR は注文メッセージを処理します。患者記録が存在しない場合は、新しい患者記録が作成されます。
5. EHR はイメージングオーダーを医療画像システムに送信します。
6. 患者は、画像検査の予約のために大病院に電話をかけます。
7. イメージング受信およびレジストレーションデスクは、放射線情報または同様のシステムを使用して、イメージング予約のための患者をスケジュールします。
8. 患者が到着して画像取得の予約が行われ、画像またはビデオが作成されて PACS に送信されます。
9. 放射線科医は画像を読み取り、ハイエンド／ GPU グラフィック対応の診断ビューアを使用して PACS 内の画像に注釈を付けます。特定の画像処理システムには、画像処理ワークフローに組み込まれた人工知能（ AI ）対応の効率向上機能があります。
10. 画像オーダーの結果は、 ESB を介して HL7 ORU メッセージがオーダー結果として EHR に送信されます。
11. EHR はオーダー結果を患者の記録に処理し、サムネイル画像をコンテキスト対応のリンクで実際の DICOM 画像に配置します。EHR 内からより高い解像度の画像が必要な場合、医師は診断ビューアを起動できます。

12. 医師が画像をレビューし、患者の記録に医師のメモを入力します。医師は、臨床決定支援システムを使用してレビュープロセスを強化し、患者の適切な診断を支援することができます。
13. EHR システムは、注文結果メッセージの形式で注文結果をコミュニティ病院に送信します。この時点で、コミュニティ病院が完全な画像を受信できる場合、画像は WADO または DICOM 経由で送信されます。
14. 地域の医師が診断を完了し、次の手順を患者に提供します。

典型的な医療画像システムでは、 N 層構造のアーキテクチャが採用されています。医療画像処理システムのコアコンポーネントは、さまざまなアプリケーションコンポーネントをホストするアプリケーションサーバーです。一般的なアプリケーションサーバは、 Java ランタイムベースまたは C# .NET CLR ベースです。ほとんどのエンタープライズ医療画像処理ソリューションでは、 Oracle データベースサーバ、 MS SQL Server 、または Sybase をプライマリデータベースとして使用しています。さらに、一部のエンタープライズ医療画像システムでは、地理的領域でのコンテンツの高速化とキャッシュにデータベースを使用しています。企業の医療画像システムの中には、 MongoDB や Redis などの NoSQL データベースを、 DICOM インターフェイスや API 用のエンタープライズ統合サーバと組み合わせて使用するものもあります。

一般的な医療画像システムでは、診断ユーザー / 放射線医、または画像をオーダーした臨床医または医師の 2 人の異なるユーザーセットの画像にアクセスできます。

放射線科医は一般的に、仮想デスクトップインフラの物理的または一部であるハイエンドのコンピューティングワークステーションおよびグラフィックスワークステーションで実行されている、グラフィック対応の診断ビューアを使用します。仮想デスクトップインフラへの移行を開始する場合は、さらに詳しい情報が記載されています "こちらをご覧ください"。

ハリケーン・カトリナがルイジアナ州の主要な教育病院の 2 つを破壊したとき、リーダーたちは集まって、3000 台以上の仮想デスクトップを含む復元力のある電子カルテ・システムを記録的に構築しました。ユースケースリファレンスアーキテクチャと FlexPod リファレンスバンドルに関する詳細については、を参照してください "こちらをご覧ください"。

臨床医は 2 つの主要な方法で画像にアクセスします。

- * ウェブベースのアクセス。 * PACS 画像を患者の電子医療記録（ EMR ）へのコンテキスト認識リンクとして埋め込み、画像ワークフロー、手順ワークフロー、進捗状況メモワークフローなどに配置できるリンクとして EHR システムで使用されます。Web ベースのリンクは、患者ポータルを介して患者に画像アクセスを提供するためにも使用されます。Web ベースアクセスでは、コンテキスト対応リンクと呼ばれるテクノロジーパターンが使用されます。コンテキスト認識リンクは、 DICOM メディアへの静的リンク /URI 、またはカスタムマクロを使用して動的に生成されたリンク /URI のいずれかです。
- * シッククライアント。 * 一部のエンタープライズ医療システムでは、シッククライアントベースのアプローチを使用して画像を表示することもできます。シッククライアントは、患者の EMR 内から起動することも、スタンドアロンアプリケーションとして起動することもできます。

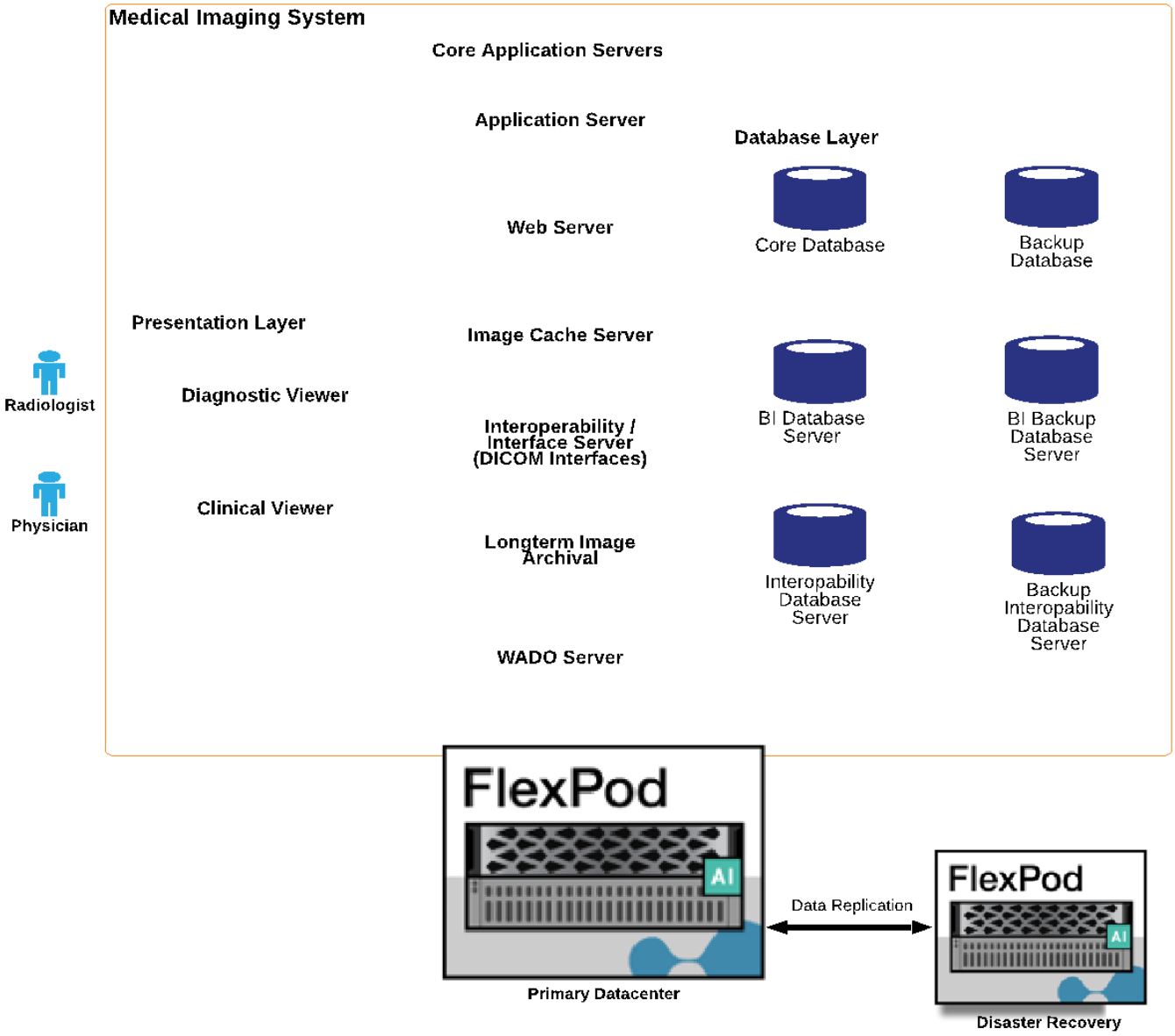
医療画像システムは、医師または CIN 参加医師のコミュニティに画像アクセスを提供します。典型的な医療画像システムには、医療機関内外の他の医療 IT システムと画像の相互運用を可能にするコンポーネントが含まれています。コミュニティの医師は、 Web ベースのアプリケーションを使用して画像にアクセスするか、画像交換プラットフォームを利用して画像の相互運用性を実現できます。画像交換プラットフォームでは、通常、 WADO または DICOM を基盤となる画像交換プロトコルとして使用します。

医療画像システムは、 PACS または画像システムを教室で使用する必要のある学術医療センターもサポートします。学術活動をサポートするために、一般的な医療画像システムでは PACS システムの機能をより小さな設置面積で、または教育のみの画像環境で使用できます。一般的なベンダーに依存しないアーカイブシステムや一部のエンタープライズクラスの医療画像システムでは、 DICOM 画像タグモーフィング機能を使用して、教育目的で使用される画像を匿名化できます。タグモーフィングにより、医療機関はベンダーに依存しな

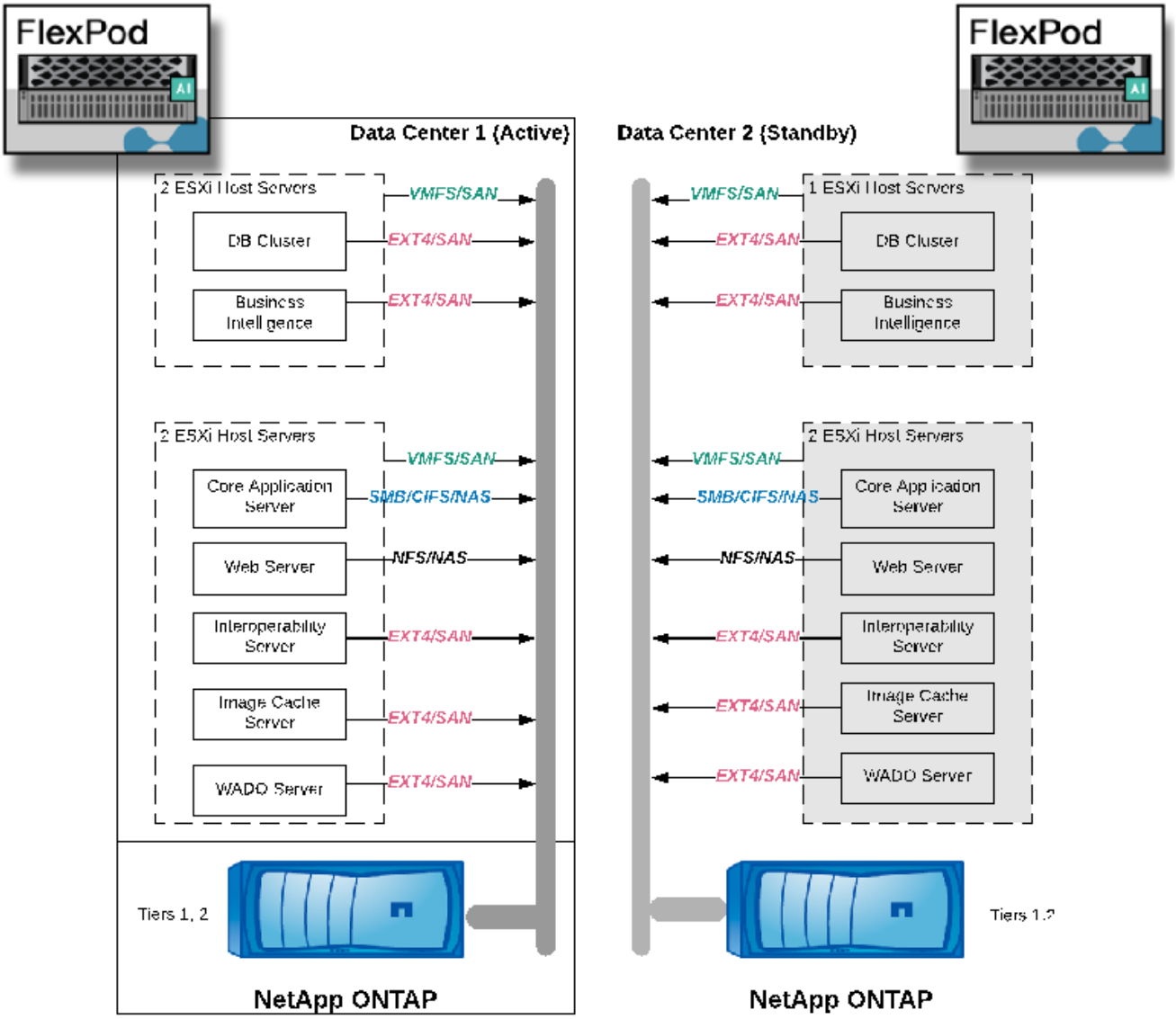
い方法で、異なるベンダーの医療画像システム間で DICOM 画像を交換できます。また、タグモーフィングにより、医療画像システムは医療画像に対して企業全体のベンダーに依存しないアーカイブ機能を実装できます。

医用画像システムの使用が開始されています "GPU ベースのコンピューティング機能" 画像を前処理することでヒューマンワークフローを強化し、効率性を向上させます。一般的なエンタープライズ医用画像システムでは、業界をリードするネットアップの Storage Efficiency 機能を利用しています。企業の医療画像システムでは、通常、バックアップ、リカバリ、リストアのアクティビティに RMAN を使用します。パフォーマンスを向上させ、バックアップの作成にかかる時間を短縮するために、 Snapshot テクノロジをバックアップ処理に使用でき、 SnapMirror テクノロジをレプリケーションに使用できます。

次の図は、階層構造ビュー内の論理アプリケーションコンポーネントを示しています。



次の図は、物理アプリケーションコンポーネントを示しています。



論理アプリケーションコンポーネントを使用するには、インフラが多様なプロトコルとファイルシステムをサポートしている必要があります。NetApp ONTAP ソフトウェアは、業界をリードするプロトコルとファイルシステムをサポートしています。

次の表に、アプリケーションコンポーネント、ストレージプロトコル、およびファイルシステムの要件を示します。

アプリケーションコンポーネント	**SAN/NAS**	ファイルシステムのタイプ	ストレージ階層	レプリケーションの種類
VMware ホスト本番データベース	ローカル	SAN	VMFS	ティア 1
アプリケーション	VMware ホスト本番データベース	担当者	SAN	VMFS
ティア 1	アプリケーション	VMware ホスト本番アプリケーション	ローカル	SAN

アプリケーションコンポーネント	**SAN/NAS**	ファイルシステムのタイプ	ストレージ階層	レプリケーションの種類
VMFS	ティア 1	アプリケーション	VMware ホスト本番アプリケーション	担当者
SAN	VMFS	ティア 1	アプリケーション	コアデータベースサーバ
SAN	ext4	ティア 1	アプリケーション	バックアップデータベースサーバ
SAN	ext4	ティア 1	なし	イメージキャッシュサーバ
NAS	SMB/CIFS	ティア 1	なし	アーカイブサーバー
NAS	SMB/CIFS	ティア 2	アプリケーション	Web サーバ
NAS	SMB/CIFS	ティア 1	なし	WADO サーバ
SAN	NFS	ティア 1	アプリケーション	ビジネスインテリジェンスサーバ
SAN	NTFS	ティア 1	アプリケーション	ビジネスインテリジェンスバックアップ
SAN	NTFS	ティア 1	アプリケーション	相互運用性サーバ
SAN	ext4	ティア 1	アプリケーション	相互運用性データベースサーバ

解決策インフラのハードウェアコンポーネントとソフトウェアコンポーネント

次の表に、医用画像システム用 FlexPod インフラストラクチャのハードウェアコンポーネントとソフトウェアコンポーネントをそれぞれ示します。

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
コンピューティング	Cisco UCS 5108 シャーシ	1 または 2	年間調査数をサポートするために必要なブレード数に基づきます
	Cisco UCS ブレードサーバ	B200 M5	20 コア以上、 2.7GHz 以上、 128-384GB RAM を搭載した各年の調査数に基づくブレードの数
	Cisco UCS 仮想インターフェイスカード（ VIC ）	Cisco UCS 1440	を参照してください
	Cisco UCS ファブリックインターコネクト × 2	6454 以降	–
ネットワーク	Cisco Nexus スイッチ	Cisco Nexus 3000 シリーズまたは 9000 シリーズ × 2	–

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
ストレージネットワーク	SMB / CIFS 、 NFS 、または iSCSI プロトコル経由のストレージアクセス用の IP ネットワーク	上記と同じネットワークスイッチ	–
	FC 経由のストレージアクセス	Cisco MDS 9132T × 2	–
ストレージ	NetApp AFF A400 オールフラッシュストレージシステム	1 つ以上の HA ペア	2 つ以上のノードで構成されるクラスタ
	ディスクシェルフ	1 台以上の DS224C または NS224 ディスクシェルフ	24 本のドライブをフル装備
	SSD の場合	容量が 24 、 2TB 以上	–

ソフトウェア	製品ファミリー	バージョンまたはリリース	詳細
エンタープライズ医療画像システム			
	MS SQL または Oracle データベースサーバ	医療画像システムのベンダーから提案されているとおりです	
	MongoDB サーバのような SQL DB はありません	医療画像システムのベンダーから提案されているとおりです	
	アプリケーションサーバ	医療画像システムのベンダーから提案されているとおりです	
	統合サーバ（ MS BizTalk 、 MuleSoft 、 Rhapsody 、 Tibco ）	医療画像システムのベンダーから提案されているとおりです	
	仮想マシン	Linux （ 64 ビット）	
	仮想マシン	Windows Server （ 64 ビット）	
ストレージ	ONTAP	ONTAP 9.7 以降	
ネットワーク	Cisco UCS ファブリックインターコネクト	Cisco UCS Manager 4.1 以降	
	Cisco イーサネットスイッチ	9.2(3) i7(2) 以降	
	Cisco FC ： Cisco MDS 9132T	8.4(2) 以降	
ハイパーバイザー	ハイパーバイザー	VMware vSphere ESXi 6.7 U2 以降	

ソフトウェア	製品ファミリー	バージョンまたはリリース	詳細
管理	ハイパーバイザー管理システム	VMware vCenter Server 6.7 U1 （ vCSA ）以降	
	NetApp Virtual Storage Console （ VSC ）	VSC 9.7 以降	
	SnapCenter	SnapCenter 4.3 以降	

解決策のサイジング

ストレージのサイジング

このセクションでは、スタディの数と、対応するインフラストラクチャ要件について説明します。

次の表に示すストレージ要件では、既存のデータは、プライマリシステム（第 1 層、第 2 層）で 1 年間の調査で 1 年間の増加に加えて予測されるものであることを前提としています。最初の 2 年間で、 3 年間の成長予測に伴う追加のストレージニーズも個別に記載します。

	小規模	中	大規模
年次研究	< 250K の研究	250K 〜 500K の研究	50 万〜 100 万件の調査
ティア 1 ストレージ			
IOPS （平均）	1.5 、 000 ~ 5 、 000	5k – 15K	15K ~ 40K
IOPS （ピーク）	5k	20K	65K
スループット	50 ~ 100Mbps	50 〜 150Mbps	100 〜 300Mbps
キャパシティデータセンター 1 （ 1 年間の古いデータと 1 年間の新しい調査）	70TB	140TB	260TB
キャパシティデータセンター 1 （新しい調査のために 4 年間必要）	25TB	45TB	80TB
キャパシティデータセンター 2 （ 1 年間の古いデータと 1 年間の新しい調査）	45TB	110TB	165TB
キャパシティデータセンター 2 （新しい調査のために 4 年間必要）	25TB	45TB	80TB
ティア 2 ストレージ			
IOPS （平均）	1 、 000	2 、 000	3 、 000
容量データセンター 1.	320TB	800TB	2 、 000TB

コンピューティングのサイジング

次の表は、小規模、中規模、および大規模の医用画像システムの計算要件を示しています。

	小規模	中	大規模
年次研究	< 250K の研究	250K ～ 500K の研究	50 万～ 100 万件の調査
データセンター 1			
VM の数	21	27	35
仮想 CPU （ vCPU ）の総数	56	124	220
必要な総メモリ容量	225GB	450 GB	900GB
物理サーバ（ブレード）の仕様（ vCPU 1 個 = コア 1 個を想定）	サーバ x 4 、 20 コア、 1 、 192 GB RAM	サーバ × 8 （ 20 コア、各 128GB RAM ）	サーバ × 14 、 20 コア、 128GB の RAM
データセンター 2.			
VM の数	15	17	22
vCPU の合計数	42	72	140
必要な総メモリ容量	179GB	243GB	513GB
物理サーバ（ブレード）の仕様（ vCPU 1 個 = コア 1 個を想定）	サーバ × 3 （各 20 コア、 168GB RAM	サーバ × 6 、各サーバのコア数は 20 、 RAM 容量は 128GB です	サーバ × 8 、 24 コア、 128GB の RAM

ネットワークと **Cisco UCS** インフラのサイジング

次の表は、小規模、中規模、および大規模の医用画像システムのネットワークと Cisco UCS インフラストラクチャの要件を示しています。

	小規模	中	大規模
データセンター 1			
ストレージノードポートの数	Converged Network Adapter （ CNA ；統合ネットワークアダプタ） × 2 、 FCS × 2	CNA × 2 、 FCS × 2	CNA × 2 、 FCS × 2
IP ネットワークスイッチポート（ Cisco Nexus 9000 ）	48 ポートスイッチ	48 ポートスイッチ	48 ポートスイッチ
FC スイッチ（ Cisco MDS ）	32 ポートスイッチ	32 ポートスイッチ	48 ポートスイッチ
Cisco UCS シャーシ数	5108 x 1	5108 x 1	5108 x 2
Cisco UCS ファブリックインターコネクト	2 x 6332	2 x 6332	2 x 6332
データセンター 2.			

	小規模	中	大規模
Cisco UCS シャーシ数	5108 x 1	5108 x 1	5108 x 1
Cisco UCS ファブリックインターコネクト	2 x 6332	2 x 6332	2 x 6332
ストレージノードポートの数	CNA × 2 、 FCS × 2	CNA × 2 、 FCS × 2	CNA × 2 、 FCS × 2
IP ネットワークスイッチポート（ Cisco Nexus 9000 ）	48 ポートスイッチ	48 ポートスイッチ	48 ポートスイッチ
FC スイッチ（ Cisco MDS ）	32 ポートスイッチ	32 ポートスイッチ	48 ポートスイッチ

ベストプラクティス

ストレージのベストプラクティス

高可用性

ネットアップストレージクラスタはあらゆるレベルで高可用性を提供します。

- クラスタノード
- バックエンドストレージの接続
- 3 つのディスク障害に対応できる RAID-TEC
- 2 つのディスクに障害が発生しても運用を継続できる RAID DP
- 各ノードから 2 つの物理ネットワークへの物理接続
- ストレージ LUN およびボリュームへの複数のデータパス

セキュアマルチテナンシー

ネットアップの Storage Virtual Machine （ SVM ）は、セキュリティドメイン、ポリシー、および仮想ネットワークを分離するための仮想ストレージアレイ構造を提供します。ストレージクラスタのデータをホストするテナント組織ごとに専用の SVM を作成することを推奨します。

ネットアップストレージのベストプラクティス

次のネットアップストレージのベストプラクティスを考慮してください。

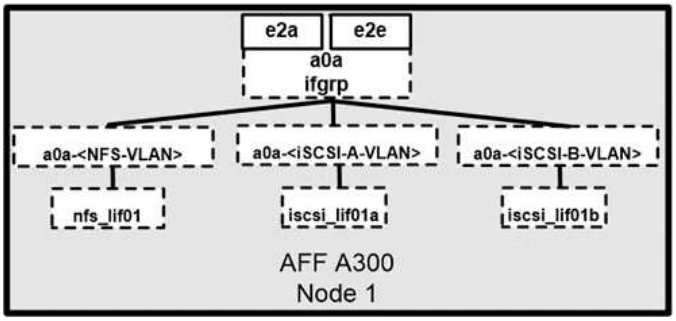
- サポート概要情報を HTTPS 経由でネットアップに送信する NetApp AutoSupport テクノロジは常に有効にしてください。
- 可用性と移動性を最大限に高めるために、 NetApp ONTAP クラスタ内の各ノードに各 SVM 用に LIF が作成されていることを確認してください。Asymmetric Logical Unit Access （ ALUA ；非対称論理ユニットアクセス）は、パスを解析し、アクティブな最適化（直接）パスとアクティブな非最適化パスを識別するために使用されます。ALUA は、 FC 、 FCoE 、 iSCSI の両方に使用されます。
- LUN の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、ジャンクションパスも必要ありません。

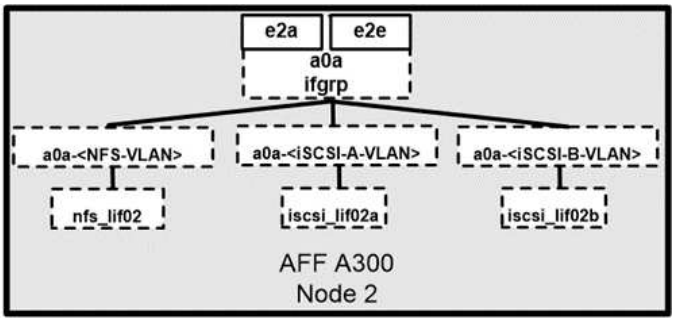
- ESXi でチャレンジハンドシェイク認証プロトコル（ CHAP ）をターゲット認証に使用する場合は、ONTAP でも設定する必要があります。CLI （「 vserver iscsi security create 」）または NetApp ONTAP System Manager （ストレージ > SVM > SVM 設定 > プロトコル > iSCSI でイニシエータセキュリティを編集）を使用します。

SAN ブート

Cisco UCS サーバの SAN ブートは、 FlexPod Datacenter 解決策に実装することを推奨します。この手順により、オペレーティングシステムを NetApp AFF ストレージシステムによって安全に保護し、パフォーマンスを向上させることができます。この解決策で概説している設計では、 iSCSI SAN ブートを使用します。

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、ストレージへのすべての方法で冗長接続が提供されます。この例では、 Cisco Nexus スイッチに接続された e2a と e2a のストレージポートを、インターフェイスグループ（ ifgrp ）と呼ばれる 1 つの論理ポートにグループ化しています（この例では a0a ）。iSCSI VLAN は igroup 上に作成され、 iSCSI ポートグループ（この例では、 a0a -<iscsi-A-vlan> ）上に iSCSI LIF が作成されます。iSCSI ブート LUN は、 igroup を使用して iSCSI LIF を通じてサーバに公開されます。この方法では、許可されたサーバのみがブート LUN にアクセスできます。ポートと LIF のレイアウトについては、次の図を参照してください。





NAS ネットワークインターフェイスとは異なり、 SAN ネットワークインターフェイスは障害発生時にフェイルオーバーするように設定されません。代わりに、ネットワークインターフェイスが使用できなくなった場合は、ホストによって、使用可能なネットワークインターフェイスへの最適パスが新たに選択されます。ネットアップがサポートする標準の ALUA は、 SCSI ターゲットに関する情報を提供します。これにより、ホストはストレージへの最適なパスを識別できます。

ストレージ効率とシンプロビジョニング

ネットアップは、プライマリワークロードに対して初めて重複排除を実行する場合や、圧縮機能を強化して小さなファイルと I/O を効率的に格納するインラインデータコンパクションを使用する場合など、 Storage Efficiency の革新的なテクノロジで業界をリードしてきました。ONTAP は、インライン重複排除とバックグラウンド重複排除のほか、インライン圧縮とバックグラウンド圧縮の両方をサポートしています。

ブロック環境で重複排除のメリットを実現するには、 LUN をシンプロビジョニングする必要があります。VM 管理者からは引き続き LUN がプロビジョニング済み容量として認識されますが、重複排除による削減効果は他のニーズに使用できるようにボリュームに戻されます。これらの LUN は、 LUN の 2 倍の容量でシンプロビジョニングされた FlexVol に導入することを推奨します。この方法で LUN を導入した場合、 FlexVol ボリュームは単なるクォータとして機能し、LUN が消費するストレージは、 FlexVol とその包含アグリゲートでレポートされます。

重複排除による削減効果を最大限に高めるために、バックグラウンド重複排除のスケジュール設定を検討しただし、これらのプロセスは、実行時にシステムリソースを使用します。そのため、あまりアクティブでない時間帯（週末など）にスケジュールを設定するか、頻繁に実行して、処理される変更データの量を減らすことを推奨します。AFF システムでの自動バックグラウンド重複排除は、フォアグラウンドアクティビティに対す

る影響を大幅に軽減します。バックグラウンド圧縮（ハードディスクベースのシステムの場合）でもリソースが消費されるため、パフォーマンス要件が限定されたセカンダリワークロードでのみ使用することを検討してください。

サービス品質

ONTAP ソフトウェアを実行するシステムでは、 ONTAP ストレージ QoS 機能を使用して、スループットをメガビット / 秒（ Mbps ）で制限できます。また、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 IOPS を制限できます。アダプティブ QoS を使用して、 IOPS の下限（ QoS 最小）と上限（ QoS 最大）を設定します。これは、データストアの容量と使用済みスペースに基づいて動的に調整されます。

スループットの制限は、不明なワークロードや、導入前のテストワークロードを制御して、他のワークロードに影響しないことを確認するのに役立ちます。また、これらの制限を使用して、特定された Bully ワークロードを制限することもできます。IOPS に基づく最小サービスレベルもサポートされており、 ONTAP の SAN オブジェクトに一貫したパフォーマンスを提供できます。

NFS データストアでは、 QoS ポリシーを FlexVol ボリューム全体またはボリューム内の個々の仮想マシンディスク（ VMDK ）ファイルに適用できます。ONTAP LUN を使用する VMFS データストア（ Hyper-V の Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）では、 LUN を含む FlexVol または個々の LUN に QoS ポリシーを適用できます。ただし、 ONTAP は VMFS を認識しないため、個々の VMDK ファイルに QoS ポリシーを適用できません。VSC 7.1 以降で VMware 仮想ボリューム（ vVol ）を使用する場合、ストレージ機能プロファイルを使用して個々の VM に最大 QoS を設定できます。

VMFS または CSV を含む LUN に QoS ポリシーを割り当てるには、 VSC ホームページのストレージシステムメニューから ONTAP SVM （「 Vserver 」と表示）、 LUN パス、およびシリアル番号を取得します。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。

オブジェクトの QoS の最大スループット制限を MBps と IOPS 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すると、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ついては、各ファイルに独自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。

ストレージレイアウト

ここでは、ストレージ上の LUN 、ボリューム、およびアグリゲートのレイアウトに関するベストプラクティスを示します。

Storage LUNs

最適なパフォーマンス、管理、バックアップを実現するために、 LUN 設計に関する次のベストプラクティスを推奨します。

- データベースデータとログファイルを格納するための独立した LUN を作成します。
- Oracle データベースログバックアップを格納するために、インスタンスごとに個別の LUN を作成します。LUN は同じボリュームに属することができます。
- データベースファイルとログファイル用にシンプロビジョニングを使用して LUN をプロビジョニング（スペースリザベーションオプションを無効に）します。
- すべてのイメージングデータは FC LUN でホストされます。FlexVol ボリューム内にこれらの LUN を作成

します。これらの LUN は、異なるストレージコントローラノードに所有されているアグリゲート間に分散されています。

ストレージボリューム内での LUN の配置については、次のセクションのガイドラインに従ってください。

ストレージボリューム

最適なパフォーマンスと管理を実現するために、ボリューム設計に関する次のベストプラクティスを推奨します。

- I/O負荷の高いクエリを使用して、別々のストレージボリュームにデータベースを分離します。
- データファイルは1つのLUNまたはボリュームに配置できますが、スループットを高めるためには複数のボリューム/ LUNを使用することを推奨します。
- 複数のLUNを使用する場合は、サポートされている任意のファイルシステムを使用してI/Oの並列処理を実現できます。
- データベースファイルとトランザクションログは別々のボリュームに配置すると、リカバリの精度が向上します。
- 自動サイズ、Snapshotリザーブ、QoSなどのボリューム属性の使用を検討してください。

アグリゲート

アグリゲートは、ネットアップストレージ構成のプライマリストレージコンテナであり、データディスクとパリティディスクの両方で構成される 1 つ以上の RAID グループを含みます。

ネットアップでは、データファイルとトランザクションログファイルが分離された共有アグリゲートと専用アグリゲートを使用して、さまざまな I/O ワークロード特性分析テストを実施しました。このテストでは、複数の RAID グループとドライブ（ HDD または SSD ）を使用する 1 つの大規模なアグリゲートによって、ストレージパフォーマンスが最適化されて向上するとともに、管理者が次の 2 つの理由から管理しやすくなることが実証されています。

- 1 つの大きなアグリゲートで、すべてのドライブの I/O 機能をすべてのファイルで使用できます。
- 1 つの大きなアグリゲートで、最も効率的なディスクスペースを使用できます。

効果的なディザスタリカバリを実現するために、ディザスタリカバリサイトの別のストレージクラスタの一部であるアグリゲートに非同期レプリカを配置し、 SnapMirror テクノロジを使用してコンテンツをレプリケートすることを推奨します。

ストレージのパフォーマンスを最適化するために、アグリゲートには少なくとも 10% の空きスペースを確保することを推奨します。

AFF A300 システム（ 24 ドライブ搭載の 2 台のディスクシェルフ）のストレージアグリゲートのレイアウトガイダンスには、次のものがあります。

- スペアドライブを 2 本用意します。
- アドバンストディスクパーティショニングを使用して、各ドライブにルートとデータの 3 つのパーティションを作成します。
- アグリゲートごとに合計 20 個のデータパーティションと 2 個のパリティパーティションを使用します。

バックアップのベストプラクティス

NetApp SnapCenter は、 VM とデータベースのバックアップに使用されます。バックアップに関する次のベストプラクティスを推奨します。

- バックアップ用の Snapshot コピーを作成するために SnapCenter を導入している場合は、 VM とアプリケーションデータをホストする FlexVol の Snapshot スケジュールを無効にします。
- ホストブート LUN 専用の FlexVol を作成します。
- 同じ目的に使用する VM に、同様のバックアップポリシーまたは単一のバックアップポリシーを使用します。
- ワークロードタイプに応じて同様のバックアップポリシーまたは単一のバックアップポリシーを使用します。たとえば、すべてのデータベースワークロードに同様のポリシーを使用します。データベース、 Web サーバ、エンドユーザ仮想デスクトップなどに異なるポリシーを使用します。
- SnapCenter でバックアップの検証を有効にします。
- バックアップ Snapshot コピーのアーカイブを NetApp SnapVault バックアップ解決策に設定します。
- アーカイブスケジュールに基づいて、プライマリストレージでのバックアップの保持を設定します。

インフラのベストプラクティス

ネットワークのベストプラクティス

ネットアップでは、ネットワークに関する次のベストプラクティスを推奨しています。

- システムに、本番トラフィックとストレージトラフィック用に冗長な物理 NIC が搭載されていることを確認します。
- コンピューティングとストレージの間で iSCSI 、 NFS 、 SMB / CIFS のトラフィック用に VLAN を分離
- システムに、医療画像システムへのクライアントアクセス専用の VLAN が含まれていることを確認してください。

ネットワークに関するその他のベストプラクティスについては、 FlexPod インフラの設計および導入ガイドを参照してください。

コンピューティングのベストプラクティス

推奨されるコンピューティングのベストプラクティスは次のとおりです。

- 指定した各 vCPU が物理コアでサポートされていることを確認してください。

仮想化のベストプラクティス

仮想化に関する次のベストプラクティスを推奨します。

- VMware vSphere 6 以降を使用。
- ESXi ホストサーバの BIOS と OS レイヤを Custom Controlled – High Performance に設定します。
- バックアップはピーク時以外の時間帯に作成してください。

医療画像システムのベストプラクティス

一般的な医用画像システムの次のベストプラクティスといくつかの要件を参照してください。

- 仮想メモリをオーバーコミットしないでください。
- vCPU の総数が物理 CPU の数と同じであることを確認してください。
- 大規模な環境では、専用の VLAN が必要です。
- 専用の HA クラスタを使用してデータベース VM を設定する。
- VM OS の VMDK が高速階層 1 のストレージでホストされていることを確認します。
- 医療画像システムベンダーと協力して、迅速な導入とメンテナンスのために VM テンプレートを準備する最適な方法を特定します。
- 管理、ストレージ、本番環境のネットワークでは、 VMware vMotion 用に独立した VLAN を使用して、データベースを LAN で分離する必要があります。
- と呼ばれるネットアップのストレージアレイベースのレプリケーションテクノロジを使用します "SnapMirror" vSphereベースのレプリケーションではなく、
- VMware API を活用したバックアップテクノロジを使用します。バックアップウィンドウは通常の業務時間外にする必要があります。

まとめ

FlexPod で医療画像処理環境を実行することで、医療機関はスタッフの生産性の向上と設備投資と運用コストの削減を期待できます。FlexPod は、 Cisco とネットアップの戦略的パートナーシップにより、検証済みで厳格にテストされた統合インフラを提供します。予測可能な低レイテンシのシステムパフォーマンスと高可用性を実現するように特別に設計されています。このアプローチにより、医療画像システムのユーザーに優れたユーザー体験と最適な応答時間が実現します。

医用画像処理システムのさまざまなコンポーネントが、 SMB / CIFS 、 NFS 、 ext4 、 NTFS ファイルシステムのデータストレージを必要とします。そのため、インフラで、 NFS 、 SMB / CIFS 、 SAN の各プロトコル経由でデータアクセスを提供する必要があります。ネットアップストレージシステムでは、これらのプロトコルを単一のストレージアレイでサポートしています。

高可用性、ストレージ効率、 Snapshot コピーベースのスケジュールされた高速バックアップ、高速リストア処理、ディザスタリカバリ用のデータレプリケーション、 FlexPod ストレージインフラ機能は、いずれも業界をリードするデータストレージと管理システムを提供します。

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。

- 『 FlexPod Datacenter for AI / ML with Cisco UCS 480 ML for Deep Learning Design Guide 』を参照してください

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- VMware vSphere 6.7 U1 、 Cisco UCS 第 4 世代、および NetApp AFF A シリーズを使用した FlexPod データセンターインフラ

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

- SnapCenter 解決策 Datacenter を使用した FlexPod データベース・バックアップの概要

  "https://www.netapp.com/us/media/sb-3999.pdf"

- Cisco UCS および NetApp AFF A シリーズ上の FlexPod データセンターと Oracle RAC データベース

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.html"

- Oracle Linux 上の Oracle RAC を使用する FlexPod データセンター

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- FlexPod for Microsoft SQL Server の略

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- Cisco とネットアップが提供する FlexPod

  "https://flexpod.com/"

- "MongoDB 向けネットアップソリューション" 解決策 Brief （ネットアップログインが必要）

  "https://fieldportal.netapp.com/content/734702"

- TR-4700 ：『 SnapCenter Plug-in for Oracle Database 』

  "https://www.netapp.com/us/media/tr-4700.pdf"

- ネットアップの製品マニュアル

  "https://www.netapp.com/us/documentation/index.aspx"

- 仮想デスクトップインフラ（ VDI ） for FlexPod ソリューション

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

仮想デスクトップインフラ

FlexPod Datacenter with Citrix Virtual Apps & Desktops 1912 LTSR and VMware vSphere 7（最大6000シート

Jeff Nichols、Cisco Suresh Thoppay、ネットアップDre Jackson

本ドキュメントでは、最大6、000人のエンドユーザコンピューティングユーザを対象とした仮想デスクトップインフラのアーキテクチャと設計について説明します。解決策は、第5世代のCisco UCS B200 M5ブレードサーバ上に仮想化され、AFF A400ストレージアレイからFC SAN経由でVMware vSphere 7.01 Update 1をブートします。仮想デスクトップは、Citrix Provisioning Server 1912 LTSRとCitrix RDS/Citrix Virtual Apps & Desktops 1912 LTSRを使用して、RDSでホストされる共有デスクトップ（6000）、プールまたはノンパーシステントホストの仮想Windows 10デスクトップ（5000）、 また、Citrix Machine Creation Services（5000）でプロビジョニングされたパーシステントホスト型仮想Windows 10デスクトップで、ユーザ数をサポートします。該当する場合は、この解決策 をお客様に導入する際のベストプラクティスの推奨事項とサイジングガイドラインを記載します。

"FlexPod Datacenter with Citrix Virtual Apps Desktops 1912 LTSR and VMware vSphere 7（最大6000シート"

FlexPod Datacenter with VMware Horizon View 7.10、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0、およびNetApp ONTAP 9.6（最大6700シート

Vadim Lebedev、Cisco Suresh Thoppay、ネットアップ

本ドキュメントでは、Cisco UCSとNetApp AFF A300、NetApp ONTAP データ管理ソフトウェアを搭載したFlexPod Datacenter上の5000シートから6000シートのデスクトップワークロード、エンドユーザコンピューティング環境を対象としたリファレンスアーキテクチャと設計ガイドを提供します。解決策 には、VMware Horizonサーバベースのの RDS Windows Server 2019セッション、VMware Horizonパーシステントフルクローン Microsoft Windows 10仮想デスクトップ、VMware vSphere 6.7U2上のVMware Horizonノンパーシステント/インスタントクローンMicrosoft Windows 10仮想デスクトップが含まれます

"FlexPod Datacenter with VMware Horizon View 7.10、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0、およびNetApp ONTAP 9.6（最大6700シート"

CitrixとNVIDIAによる3Dグラフィックスの視覚化-ホワイトペーパー

このドキュメントでは、SPECviewperf 13を搭載したCisco UCS C240 M5およびB200

M5サーバで、NVIDIA Tesla P4、P6、およびP40カードを搭載したCitrix XenServer上のCitrix XenDesktopのパフォーマンスについて説明します。

"CitrixとNVIDIAによる3Dグラフィックスの視覚化-ホワイトペーパー"

Citrix XenDesktop/XenApp 7.15およびVMware vSphere 6.5 Update 1（6000シート）を搭載したFlexPod Datacenter

Vadim Lebedev、Cisco Chris Rodriguez、ネットアップ

このドキュメントでは、NetApp All Flash FAS （AFF ）A300ストレージとVMware vSphere ESXi 6.5ハイパーバイザープラットフォームを搭載したCisco UCS上に構築されたCitrix XenApp/XenDesktop 7.15を使用した仮想デスクトップおよびアプリケーションの設計のリファレンスアーキテクチャについて説明します。

デスクトップとアプリケーションの仮想化の状況は絶えず変化しています。新しいM5高性能Cisco UCSブレードサーバとCisco UCSユニファイドファブリックは、FlexPod の実証済みインフラストラクチャの一部として統合されており、最新世代のNetApp AFF ストレージを使用することで、プラットフォームのコンパクト性、パフォーマンス、信頼性、効率性が向上します。

"Citrix XenDesktop/XenApp 7.15およびVMware vSphere 6.5 Update 1（6000シート）を搭載したFlexPod Datacenter"

FlexPod Datacenter with VMware Horizon View 7.3 and VMware vSphere 6.5 Update 1 with Cisco UCS Manager 3.2 for 5000 seats

ネットアップ、Cisco David Arnette、Ramesh Guduru

本ドキュメントでは、Cisco UCSとNetApp All Flash FAS （AFF ）A300ストレージを搭載したFlexPod Datacenterに、最大5000シートの混在ワークロードエンドユーザコンピューティング環境を導入するためのリファレンスアーキテクチャ、設計ガイド、および導入について説明します。解決策 には、VMware Horizonサーバベースのリモートデスクトップサーバホストセッション、VMware HorizonのパーシステントMicrosoft Windows 10仮想デスクトップ、VMware vSphere 6.5上のVMware Horizonノンパーシステント Microsoft Windows 10インスタントクローン仮想デスクトップが含まれます。

"FlexPod Datacenter with VMware Horizon View 7.3 and VMware vSphere 6.5 Update 1 with Cisco UCS Manager 3.2 for 5000 seats"

FlexPod Datacenter with VMware Horizon View 7.10 、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0、およびNetApp ONTAP 9.6（最大6700シート

Vadim Lebedev、Cisco Suresh Thoppay、ネットアップ

本ドキュメントでは、Cisco UCS、NetApp AFF A300、NetApp ONTAP データ管理ソフトウェアを搭載したFlexPod データセンターで、5000シートから6000シートのデスクトップワークロードのエンドユーザコンピューティング環境を構築するためのリファレンスアーキテクチャと設計ガイドを提供します。解決策 には、VMware Horizonサーバベースの RDS Windows Server 2019セッション、VMware Horizonパーシステント/フルクローンMicrosoft Windows 10仮想デスクトップ、VMware vSphere 6.7 U2上のVMware Horizonノンパーシステント/インスタントクローニングMicrosoft Windows 10仮想デスクトップが含まれます。

"FlexPod Datacenter with VMware Horizon View 7.10、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0、およびNetApp ONTAP 9.6（最大6700シート"

最新のアプリケーション

FlexPod Datacenter for combined AI and ML with Cisco UCS 480 ML for deep learning - Design

ネットアップ、Haseeb Niazi、Cisco Arvind Ramakrishnan

このドキュメントでは、FlexPod データセンター解決策 へのCisco UCS C480 ML M5プラットフォームの統合に関する設計の詳細を説明し、統合インフラ内でAIおよびML機能を提供するための統合アプローチを提供します。従来のFlexPod システムの管理に使用している使い慣れたツールを使用して、AIとMLを組み合わせたサーバを管理できるようにすることで、管理オーバーヘッドとディープラーニングプラットフォームの導入コストを大幅に削減できます。このCVDで提示されている設計には、2つのNVIDIA T4 GPUを搭載したC220 M5サーバや、2つのNVIDIA V100 32GB PCIeカードを搭載したC240 M5サーバなど、他のCisco UCSプラットフォームも含まれています。これは、AIとMLの同時処理ワークロードを処理するための追加オプションです。

"FlexPod Datacenter for Combined AI and ML with Cisco UCS 480 ML for Deep Learning - Design"

FlexPod を使用したCiscoコンテナプラットフォームにNetApp Trident CSIプラグインを導入

このドキュメントでは、FlexPod 解決策 のCisco Container Platform Kubernetesテナントクラスタに NetApp Trident Container Storage Interface（CSI）プラグインを導入する手順を詳しく説明します。

"FlexPod を使用したCiscoコンテナプラットフォームにNetApp Trident CSIプラグインを導入"

FlexPod Datacenter for OpenShift Container Platform 4 -導入

Haseeb Niazi、Cisco Alan Cowles、ネットアップ

Red Hat OpenShiftは、ハイブリッドクラウドやマルチクラウドの環境を管理するための、エンタープライズ対応のKubernetesコンテナプラットフォームです。Red Hat OpenShift Container Platformには、ハイブリッドクラウド、エンタープライズコンテナ、Kubernetesの開発と導入に必要なすべての機能が含まれています。エンタープライズクラスのLinuxオペレーティングシステム、コンテナランタイム、ネットワーク、監視、コンテナレジストリ、 認証および承認ソリューション。

Red Hat OpenShiftとFlexPod Datacenter解決策 を組み合わせることで、コンテナインフラの導入と管理を簡易化できます。お客様は、この可用性に優れたエンタープライズクラスのインフラスタックを柔軟に拡張して、効率性の向上、データ保護の強化、リスクの軽減、新しいビジネス要件に対応できます。事前検証済みの統合解決策 アプローチにより、アプリケーションの最新化やデジタル変革へのあらゆる取り組みに必要なスピード、柔軟性、拡張性を実現できます。

"FlexPod Datacenter for OpenShift Container Platform 4 -導入"

<xmt-block0>FlexPod</xmt-block> Datacenter with Docker Enterprise Edition for Container Managementを参照してください

Muhammad Afzal、Cisco John George、Cisco Amit Borulkar、NetApp Uday Shetty、Docker

Dockerは、開発者やIT運用担当者が分散アプリケーションをどこでも構築、出荷、実行できる、世界をリードするソフトウェアコンテナプラットフォームです。マイクロサービスアーキテクチャが次世代のITを形作る中、モノリシックアプリケーションに多額の投資をしている企業は、アプリケーションアーキテクチャを最新化し、組織の競争力とコスト効率を維持するための戦略としてDockerを採用する方法を模索しています。コンテナ化は、開発者やIT運用者がインフラ全体でアプリケーションを構築、導入するために必要な即応性、制御性、モビリティを提供します。Dockerプラットフォームを使用すると、分散したアプリケーションを軽量なアプリケーションコンテナに簡単に構成できます。このコンテナは、システムを停止することなく動的に変更できます。この機能により、ローカル、データセンター、さまざまなクラウドサービスプロバイダのネットワークを介して、物理マシンまたは仮想マシンで実行されている開発、テスト、本番環境全体でアプリケーションを移植できます。

"FlexPod Datacenter with Docker Enterprise Edition for Container Managementを参照してください"

FlexPod Datacenter for OpenShift Container Platform 4-設計

Haseeb Niazi、Cisco Alan Cowles、ネットアップ

Ciscoとネットアップは提携して、戦略的なデータセンタープラットフォームを実現する一連のFlexPod ソリューションを提供しています。FlexPod 解決策 は、コンピューティング、ストレージ、ネットワーク設計のベストプラクティスを組み込んだ統合アーキテクチャを提供します。そのため、統合アーキテクチャを検証してさまざまなコンポーネント間の互換性を確保することで、ITリスクを最小限に抑えることができます。また、解決策 は、導入のさまざまな段階（計画、設計、実装）で使用できる文書化された設計ガイダンス、導入ガイダンス、およびサポートを提供することで、ITの課題にも対処します。

"FlexPod Datacenter for OpenShift Container Platform 4-設計"

<xmt-block0>FlexPod</xmt-block> Datacenter for combined AI and ML with Cisco UCS 480 ML for deep learning - Deployment

ネットアップ、Haseeb Niazi、Cisco Arvind Ramakrishnan

このドキュメントでは、Cisco UCS C480 ML M5プラットフォームをFlexPod データセンター解決策 に統合して、統合インフラ内でAIとMLの機能を提供するための統合アプローチを提供する方法について、導入の詳細とガイダンスを提供します。また、Cisco UCS C220およびC240プラットフォームでのNVIDIA GPU構成についても説明します。この解決策 で使用されるプラットフォームとテクノロジーの詳細な設計については、を参照してください "FlexPod データセンター：AIとMLを統合し、Cisco UCS 480 MLを活用したディープラーニング設計を実現します"。

"FlexPod Datacenter for combined AI and ML with Cisco UCS 480 ML for deep learning - Deployment"

Cisco UCSでVMwareとNVIDIAを使用した3Dグラフィックスの可視化-ホワイトペーパー

このドキュメントでは、Cisco UCS C240 M5ラックサーバおよびB200 M5ブレードサーバ上で、NVIDIA Tesla P4、P6、P40解決策 を使用したVMware ESXiハイパーバイザとVMware Horizonのパフォーマンスについて説明します。

"Cisco UCSでVMwareとNVIDIAを使用した3Dグラフィックスの可視化-ホワイトペーパー"

CitrixとNVIDIAによる3Dグラフィックスの視覚化-ホワイトペーパー

このドキュメントでは、SPECviewperf 13を搭載したCisco UCS C240 M5およびB200 M5サーバで、NVIDIA Tesla P4、P6、およびP40カードを搭載したCitrix XenServer上のCitrix XenDesktopのパフォーマンスについて説明します。

"CitrixとNVIDIAによる3Dグラフィックスの視覚化-ホワイトペーパー"

FlexPod エクスプレスの略

FlexPod Express with Cisco UCS C シリーズおよび NetApp AFF C190 シリーズ設計ガイド

NVA-1139 - 設計： FlexPod Express with Cisco UCS C シリーズ and NetApp AFF C190 シリーズ

ネットアップ、 Savita Kumari 氏

協力：

業界のトレンドは、共有インフラとクラウドコンピューティングへの大規模なデータセンターの移行を示しています。さらに、データセンターで使い慣れたテクノロジを使用するリモートオフィスやブランチオフィスに、シンプルで効果的な解決策を求めています。

FlexPod Express は、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus ファミリースイッチ、および NetApp AFF システム上に構築された、事前設計されたベストプラクティスのデータセンターアーキテクチャです。FlexPod Express のコンポーネントは、 FlexPod Datacenter と同様に、小規模な IT インフラ環境全体で管理面の相乗効果を実現します。FlexPod Datacenter と FlexPod Express は、仮想化に最適なプラットフォームで、ベアメタルのオペレーティングシステムやエンタープライズワークロードに最適です。

"次のページ：プログラムの概要"

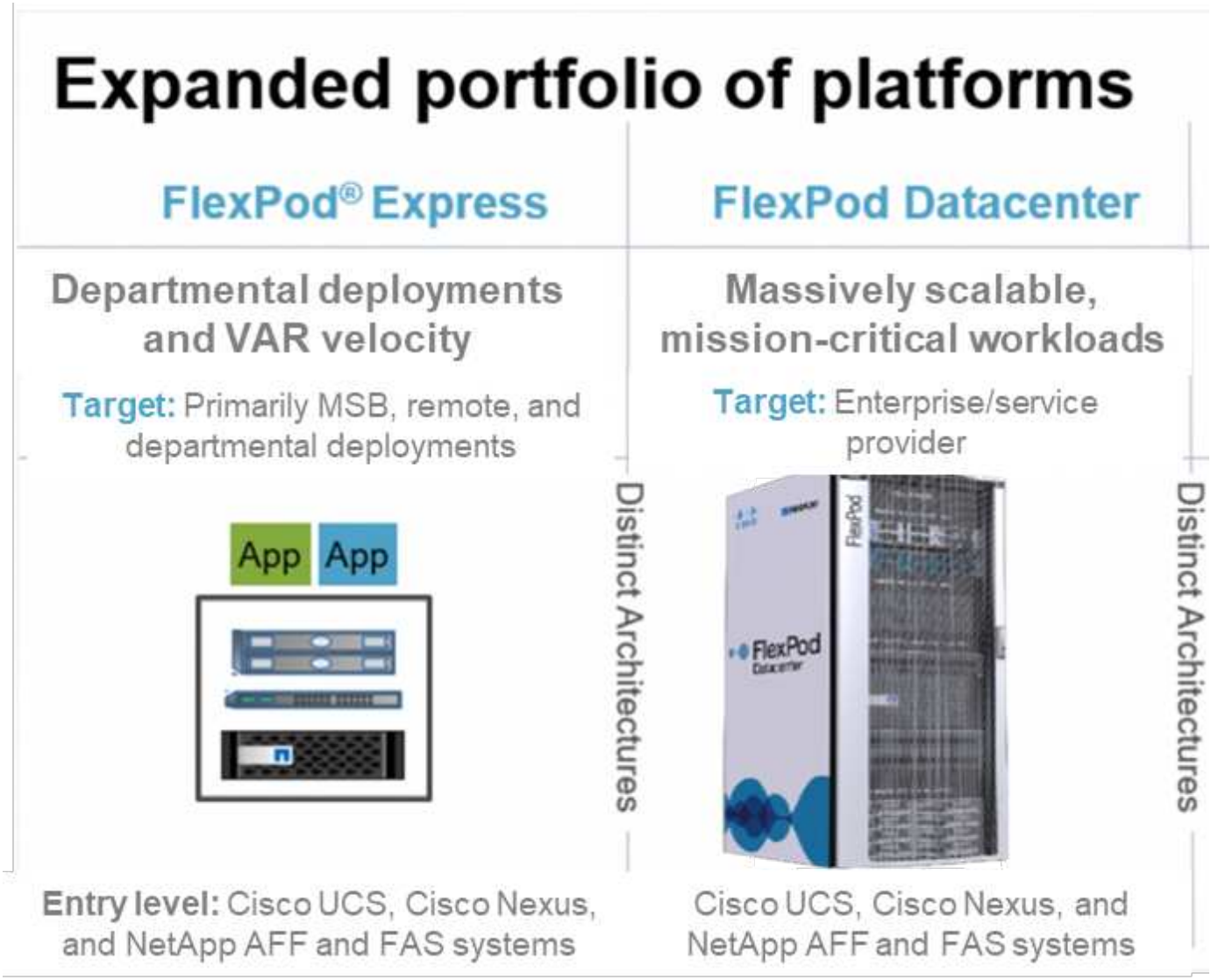
プログラムの概要

FlexPod 統合インフラのポートフォリオ

FlexPod リファレンスアーキテクチャは、 Cisco Validated Design （ CVD ）または NetApp Verified Architectures （ NVA ）として提供されます。該当する CVD または NVA からのお客様の要件に基づく差異は、それらのバリエーションによってサポートされていない構成が導入されない場合に認められます。

次の図に示すように、 FlexPod ポートフォリオには FlexPod Express および FlexPod Datacenter というソリューションが含まれています。

- * FlexPod Express* は、 Cisco とネットアップのテクノロジーを搭載したエントリーレベルの解決策です。
- * FlexPod Datacenter * は、さまざまなワークロードやアプリケーションに最適な多目的基盤を提供します。



NetApp Verified Architecture プログラム

NetApp Verified Architecture プログラムは、ネットアップソリューションの検証済みアーキテクチャを提供するものです。NVA 解決策には、次の特性があります。

- 入念にテストされています
- あらかじめ規定されている
- 導入リスクを最小限に抑えます
- 市場投入までの時間を短縮：このガイドでは、 VMware vSphere を使用した FlexPod Express の設計について詳しく説明します。

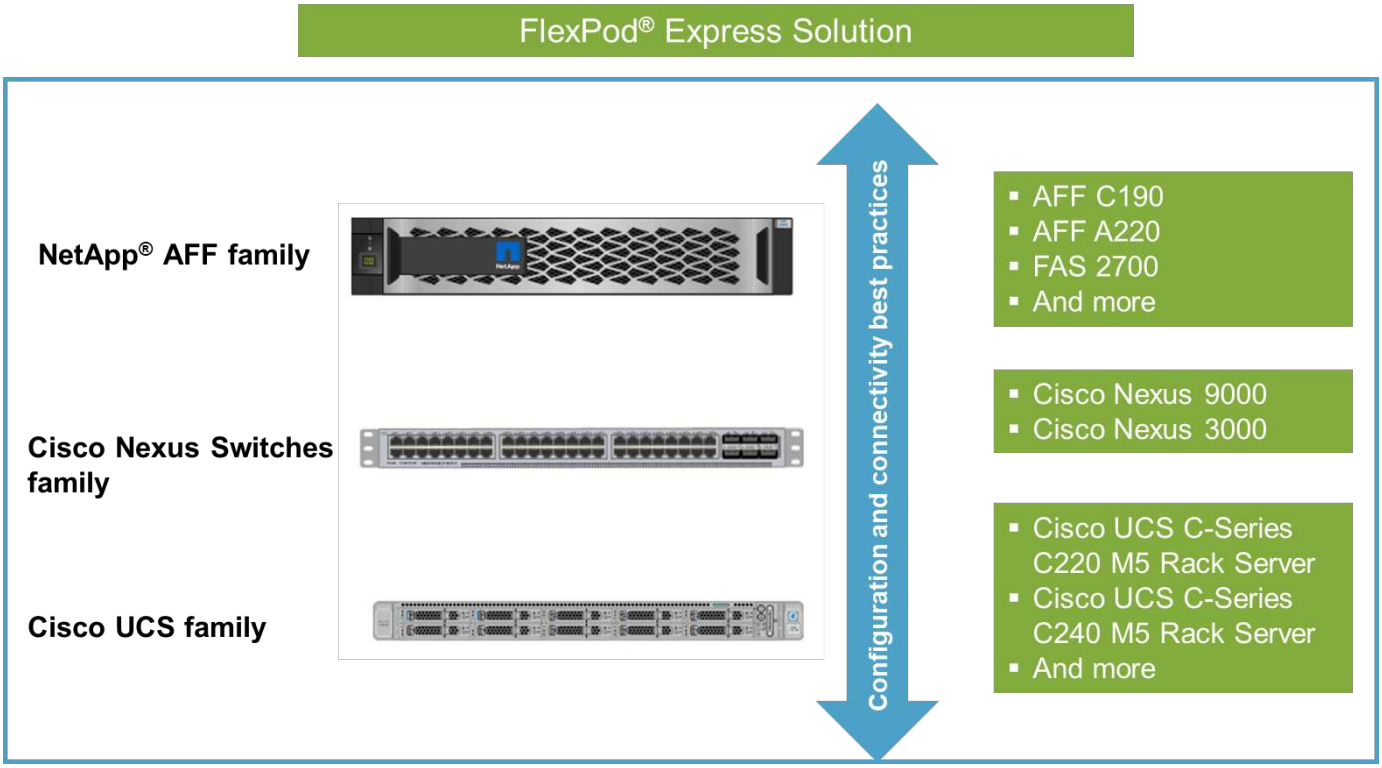
また、この設計では、 NetApp ONTAP 9.6 ソフトウェア、 Cisco Nexus 31108 スイッチ、および Cisco UCS C220 M5 サーバをハイパーバイザーノードとして実行する、新しい AFF C190 システムを利用します。

解決策の概要

FlexPod Express は、混在仮想化ワークロードを実行するように設計されています。リモートオフィス、ブランチオフィス、中堅企業を対象としています。また、特定の目的に専用の解決策を実装したい大規模企業にも

最適です。この新しい解決策 for FlexPod Express には、 NetApp ONTAP 9.6 、 NetApp AFF C190 システム、 VMware vSphere 6.7U2 などの新しいテクノロジが追加されています。

次の図に、 FlexPod Express 解決策に含まれるハードウェアコンポーネントを示します。

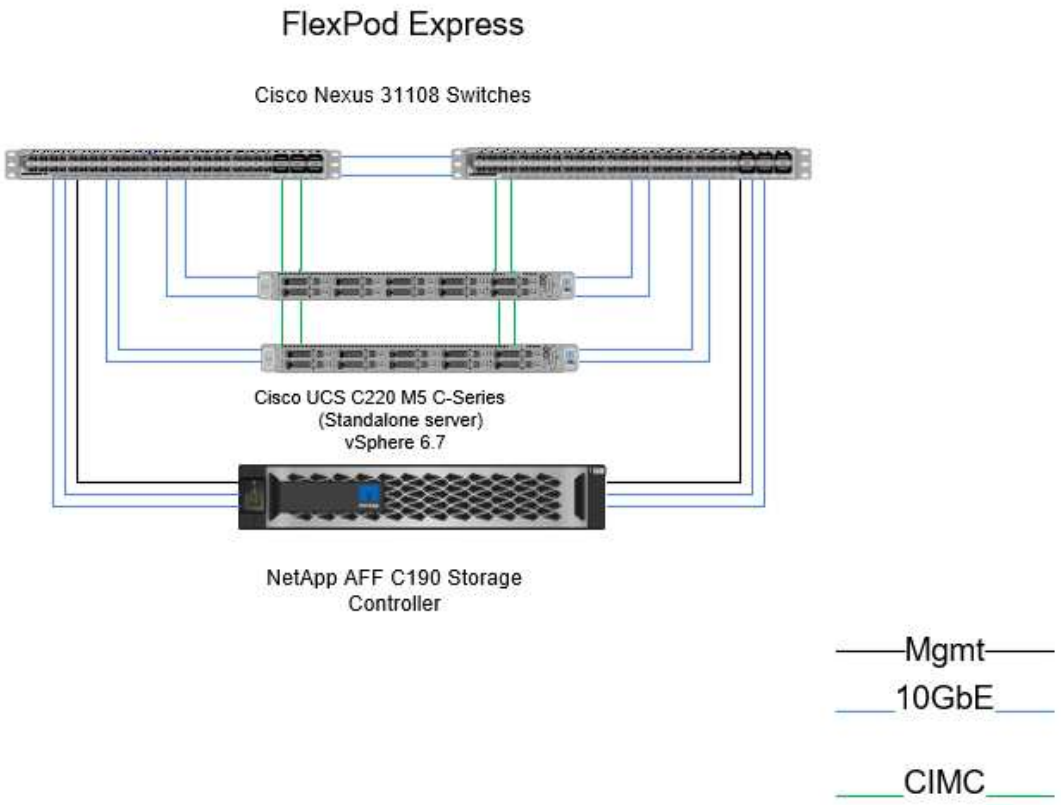


対象読者

本ドキュメントは、 IT の効率性を高め、 IT のイノベーションを実現するために構築されたインフラを活用したい方を対象としています。本ドキュメントが対象とする主な読者は、セールスエンジニア、フィールドコンサルタント、プロフェッショナルサービス担当者、 IT マネージャーなどです。 パートナー様のエンジニア、お客様

解決策テクノロジ

この解決策は、ネットアップ、 Cisco 、 VMware の最新テクノロジを活用しています。このシステムには、 ONTAP 9.6 ソフトウェア、 Cisco Nexus 31108 デュアルスイッチ、および VMware vSphere 6.7U2 を実行する Cisco UCS C220 M5 ラックサーバを実行する、新しい NetApp AFF C190 システムが搭載されています。この検証済み解決策は、次の図に示すように、 10 ギガビットイーサネット（ 10GbE ）テクノロジを使用しています。また、 FlexPod Express アーキテクチャが組織の進化するビジネスニーズに適応できるように、 2 つのハイパーバイザーノードを一度に追加して拡張する方法についても説明します。



"次のステップ：テクノロジの要件"

テクノロジ要件

FlexPod Express では、選択したハイパーバイザーとネットワークの速度に応じて、ハードウェアコンポーネントとソフトウェアコンポーネントを組み合わせる必要があります。また FlexPod 、ハイパーバイザーノードをシステムに追加するために必要なハードウェアコンポーネントが 2 つのユニットに配置されます。

ハードウェア要件

選択したハイパーバイザーに関係なく、すべての FlexPod Express 構成で同じハードウェアが使用されます。したがって、ビジネス要件が変わっても、同じ FlexPod Express ハードウェア上で別のハイパーバイザーを使用できます。

次の表に、この FlexPod 構成に必要なハードウェアコンポーネントと、この解決策の実装に必要なハードウェアコンポーネントを示します。解決策の実装で使用されるハードウェアコンポーネントは、お客様の要件に応じて異なる場合があります。

ハードウェア	数量
AFF C190 は 2 ノードクラスタです	1.
Cisco UCS C220 M5 サーバ	2.

ハードウェア	数量
Cisco Nexus 31108 スイッチ	2.
Cisco UCS C220 M5 ラックサーバ用 Cisco UCS Virtual Interface Card （ VIC ；仮想インターフェイスカード） 1457	2.

ソフトウェア要件

次の表に、 FlexPod Express 解決策のアーキテクチャを実装するために必要なソフトウェアコンポーネントを示します。

ソフトウェア	バージョン	詳細
Cisco Integrated Management Controller （ CIMC ）	4.0.4	C220 M5 ラックサーバ用
Cisco NX-OS	7.0 （ 3 ） I7 （ 6 ）	Cisco Nexus 31108 スイッチの場合
NetApp ONTAP	9.6	NetApp AFF C190 コントローラの場合

次の表に、 FlexPod Express のすべての VMware vSphere 環境に必要なソフトウェアを示します。

ソフトウェア	バージョン
VMware vCenter Server Appliance の略	6.7U2
VMware vSphere ESXi の場合	6.7U2
NetApp VAAI Plug-in for ESXi	1.1.2
NetApp Virtual Storage Console の略	9.6

"次のステップ：設計の選択肢。"

設計の選択肢

このセクションに記載されているテクノロジは、アーキテクチャ設計フェーズで採用されました。各テクノロジは、 FlexPod Express Infrastructure 解決策の特定の目的に使用されます。

NetApp AFF ONTAP 9.6 搭載 C190 シリーズ

この解決策は、 NetApp AFF C190 システムと ONTAP 9.6 ソフトウェアの 2 つの最新ネットアップ製品を活用しています。

AFF C190 システム

ターゲットグループとは、リーズナブルな価格でオールフラッシュテクノロジを導入し、 IT インフラを最新化したいと考えているお客様です。AFF C190 システムには、 ONTAP 9.6 とフラッシュバンドルの新しいライセンスが付属しています。つまり、次の機能が搭載されています。

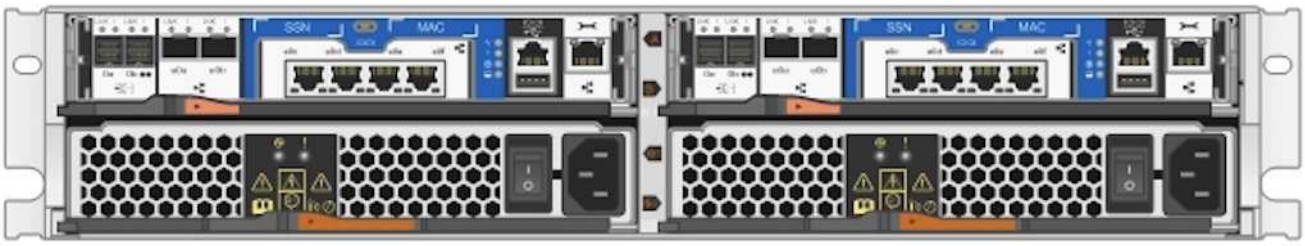
- CIFS 、 NFS 、 iSCSI 、および FCP

- NetApp SnapMirror データレプリケーションソフトウェア、 NetApp SnapVault バックアップソフトウェア、 NetApp SnapRestore データリカバリソフトウェア、 NetApp SnapManager ストレージ管理ソフトウェア製品スイート、 NetApp SnapCenter ソフトウェア
- FlexVol テクノロジ
- 重複排除、圧縮、コンパクション
- シンプロビジョニング
- Storage QoS
- NetApp RAID DP テクノロジ
- NetApp Snapshot テクノロジ
- FabricPool

次の図に、ホスト接続の 2 つのオプションを示します。

次の図は、 SFP+ モジュールを挿入できる UTA 2 ポートを示しています。

次の図に、従来の RJ-45 イーサネットケーブルを介した接続用の 10GBASE-T ポートを示します。



10GBASE-T ポートオプションの場合、 10GBASE-T ベースのアップリンクスイッチが必要です。

AFF C190 システムは、 960GB SSD のみで構成されます。拡張には 4 つの段階があり、その中から選択できます。

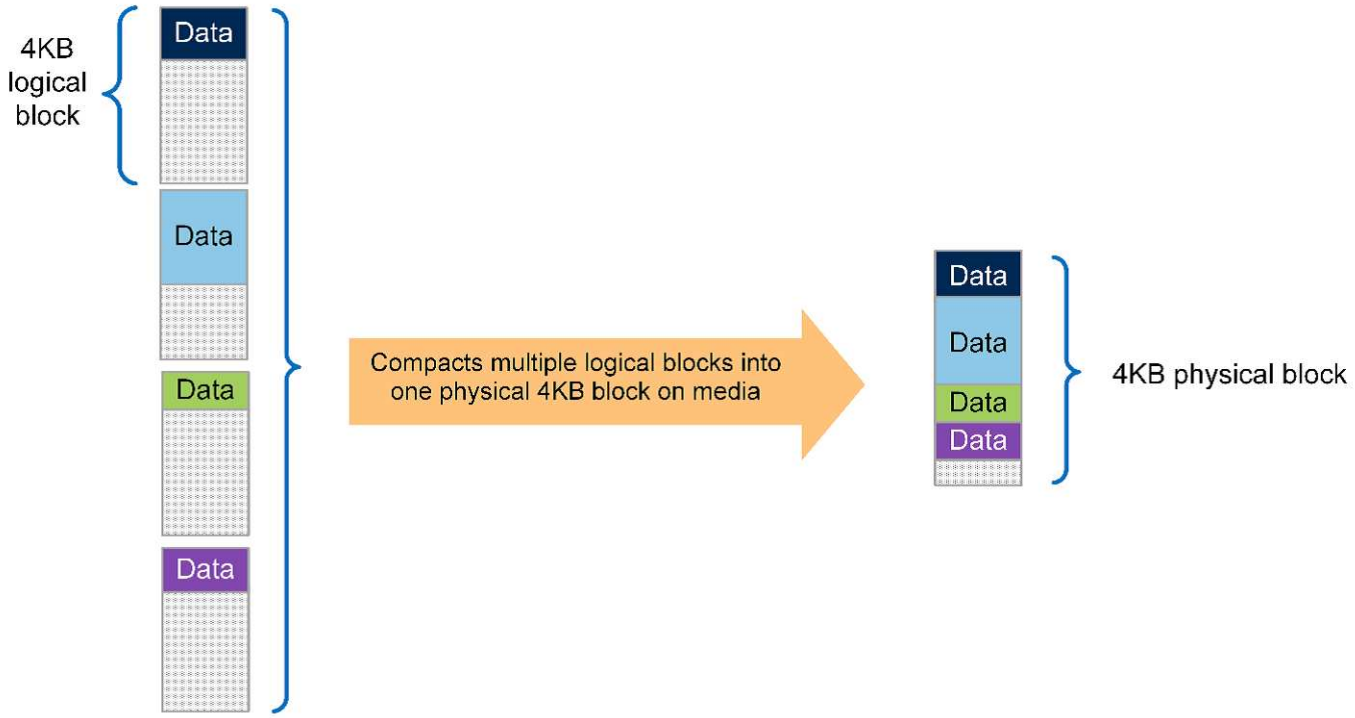
- 960GB × 8
- 960GB ： 12 倍
- 960GB × 18
- 24X 960GB

AFF C190 ハードウェアシステムの詳細については、を参照してください "NetApp AFF C190 オールフラッシュアレイのページ"。

ONTAP 9.6 ソフトウェア

NetApp AFF C190 システムでは、新しい ONTAP 9.6 データ管理ソフトウェアを使用します。ONTAP 9.6 は、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す。新しいレベルのシンプルさと柔軟性、強力なデータ管理機能、ストレージ効率化機能、業界をリードするクラウド統合機能を兼ね備えています。

ONTAP 9.6 には、 FlexPod Express 解決策に最適ないくつかの機能があります。最も重要なのは、ストレージ効率化に対するネットアップの取り組みです。これは、小規模環境で最も重要な機能の 1 つです。ONTAP 9.6 では、重複排除、圧縮、コンパクション、シンプロビジョニングなどのネットアップの Storage Efficiency 機能が特徴です。NetApp WAFL システムは、常に 4KB ブロックを書き込みます。したがって、コンパクションでは、ブロックが割り当てられた 4KB のスペースを使用していない場合、複数のブロックが 4KB ブロックにまとめられます。次の図に、このプロセスを示します。



ONTAP 9.6 では、 NVMe ボリューム用のオプションの 512 バイトブロックサイズがサポートされるようになりました。この機能は、 512 バイトのブロックをネイティブで使用する VMware Virtual Machine File System （ VMFS ）と連携します。デフォルトの 4K サイズをそのまま使用することも、必要に応じて 512 バイトのブロックサイズを設定することもできます。

ONTAP 9.6 のその他の機能拡張には、次のものがあります。

- * NetApp Aggregate Encryption （ NAE ）。 * NAE はアグリゲートレベルでキーを割り当て、アグリゲート内のすべてのボリュームを暗号化します。この機能では、アグリゲートレベルでボリュームを暗号化および重複排除できます。
- * NetApp ONTAP FlexGroup のボリューム機能強化 * 。ONTAP 9.6 では、 FlexGroup ボリュームの名前を簡単に変更できます。データをに移行するために新しいボリュームを作成する必要はありません。ボリュームサイズは、 ONTAP システムマネージャまたは CLI を使用して縮小することもできます。
- * FabricPool の機能強化 * ONTAP 9.6 では、クラウド階層としてのオブジェクトストアのサポートが追加

されています。Google Cloud と Alibaba Cloud Object Storage Service （ OSS ）のサポートもリストに追加されました。FabricPool は、 AWS S3 、 Azure Blob 、 IBM Cloud オブジェクトストレージ、 NetApp StorageGRID オブジェクトベースストレージソフトウェアなど、複数のオブジェクトストアをサポートしています。

- * SnapMirror の機能拡張。 * ONTAP 9.6 では、新しいボリュームレプリケーション関係はデフォルトで暗号化されたあとにソースアレイから削除され、 SnapMirror デスティネーションで復号化されます。

Cisco Nexus 3000 シリーズ

Cisco Nexus 31108PC-V は、 10Gbps SFP + ベースのトップオブラック（ ToR ）スイッチで、 48 個の SFP+ ポートと 6 個の QSFP28 ポートを備えています。各 SFP+ ポートは 100Mbps 、 10Gbps 、各 QSFP28 ポートはネイティブの 100Gbps モードまたは 40Gbps モードまたは 4x 10Gbps モードで動作し、柔軟な移行オプションを提供します。このスイッチは、低レイテンシと低消費電力に最適化された、真の PHY レス・スイッチです。

Cisco Nexus 31108PC-V 仕様には、次のコンポーネントが含まれています。

- 最大 1.2Tbps のスイッチング容量および転送速度（ 31108PC-V
- SFP ポート × 48 で 1 / 10 ギガビットイーサネット（ 10GbE ）をサポート。 QSFP28 ポート × 6 では、それぞれ 4 個の 10GbE または 40GbE 、 100GbE をサポートします

次の図に、 Cisco Nexus 31108PC-V スイッチを示します。

Cisco Nexus 31108PC-V スイッチの詳細については、を参照してください "Cisco Nexus 3172PQ 、 3172TQ 、 3172TQ-32T 、 3172PQ-XL 、および 3172TQ-XL スイッチのデータシート"。

Cisco UCS C-Series

Cisco UCS C シリーズラックサーバは FlexPod Express 用に選択されました。多くの設定オプションを使用することで、 FlexPod Express 環境の特定の要件に合わせて調整できます。

Cisco UCS C シリーズラックサーバは、業界標準のフォームファクタでユニファイドコンピューティングを提供し、 TCO の削減と即応性の向上を実現します。

Cisco UCS C シリーズラックサーバには、次のようなメリットがあります。

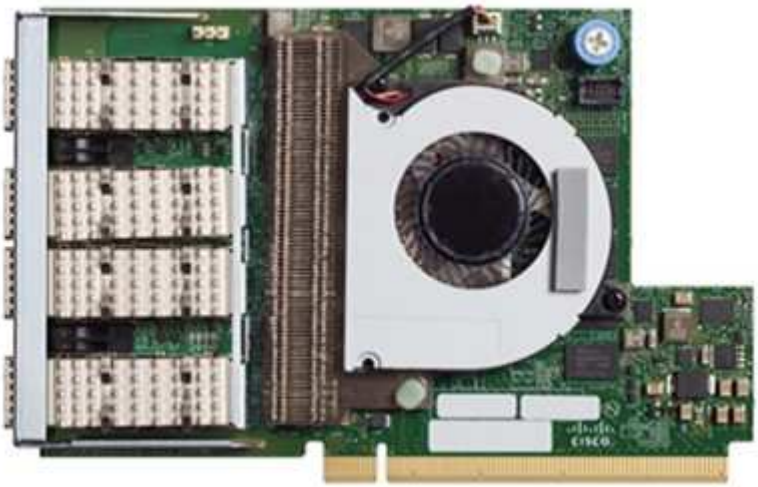
- フォームファクタに依存しない Cisco UCS へのエントリポイント
- アプリケーションを簡単かつ迅速に導入
- ユニファイドコンピューティングの革新性と利点をラックサーバに拡張
- 使い慣れたラックパッケージに独自のメリットをもたらし、お客様の選択肢を拡大

Cisco UCS C220 M5 ラックサーバは、この図のように、業界で最も汎用性の高い汎用エンタープライズインフラおよびアプリケーションサーバの 1 つです。高密度の 2 ソケットラックサーバで、仮想化、コラボレーション、ベアメタルなど、さまざまなワークロードに業界最高レベルのパフォーマンスと効率性を提供します。Cisco UCS C シリーズラックサーバは、スタンドアロンサーバとして導入することも、 Cisco UCS の一部として導入することもできます。これにより、シスコの標準ベースのユニファイドコンピューティングの革新的な技術を活用して、お客様の TCO を削減し、ビジネスの俊敏性を高めることができます。

C220 M5 サーバの詳細については、を参照してください "Cisco UCS C220 M5 ラックサーバデータシート"。

C220 M5 ラックサーバ用 Cisco UCS VIC 1457 接続

次の図に示す Cisco UCS VIC 1457 アダプタは、 M5 世代の Cisco UCS C シリーズサーバ用に設計された、クアッドポート Small Form-Factor Pluggable （ SFP28 ） Modular LAN on Motherboard （ mLOM ）カードです。このカードは 10/25Gbps のイーサネットまたは FCoE をサポートしています。このカードは、 PCIe 標準準拠のインタフェースをホストに提供でき、 NIC または HBA として動的に構成できます。



Cisco UCS VIC 1457 アダプタの詳細については、を参照してください "Cisco UCS 仮想インターフェイスカード 1400 シリーズデータシート"。

VMware vSphere 6.7U2

VMware vSphere 6.7U2 は、 FlexPod Express で使用するハイパーバイザーオプションの 1 つです。VMware vSphere を使用すると、購入したコンピューティング容量が十分に使用されていることを確認しながら、組織の電力および冷却のフットプリントを削減できます。また、 VMware vSphere を使用すると、ハードウェア障害からの保護（ VMware High Availability 、 VMware HA ）が可能になり、 vSphere ホストのクラスタ全体（メンテナンスモードの VMware Distributed Resource Scheduler 、または VMware DRS - MM ）でリソースのロードバランシングを計算できます。

カーネルのみが再起動されるため、 VMware vSphere 6.7U2 を使用すると、ハードウェアを再起動せずに vSphere ESXi をロードすることで、迅速なブートが可能になります。vSphere 6.7U2 vSphere クライアント（ HTML5 ベースのクライアント）には、コードキャプチャ機能と API エクスプローラ機能を備えた Developer Center などの新しい機能拡張がいくつかあります。コードキャプチャを使用すると、 vSphere ク

ライアントにアクションを記録して、わかりやすいシンプルなコード出力を提供できます。vSphere 6.7U2 には、メンテナンスモードの DRS （ DRS-MM ）などの新機能も含まれています。

VMware vSphere 6.7U2 には次の機能があります。

- VMware は、外部の VMware Platform Services Controller （ PSC ）導入モデルを廃止しています。

> vSphere の次回のメジャーリリース以降、外部 PSC は利用できません。

- vCenter Server Appliance のバックアップおよびリストアでサポートされる新しいプロトコルが追加されました。サポートされるプロトコルの選択肢として NFS と SMB を導入、合計で最大 7 つ（ HTTP 、 HTTPS 、 FTP 、 FTPS 、 SCP 、 NFS 、および SMB ）：ファイルベースのバックアップまたはリストア処理用に vCenter Server を設定する場合。
- コンテンツライブラリを使用する際の新しい機能。vCenter Server でリンクモードが強化されている場合は、コンテンツライブラリ間でネイティブの VM テンプレートを同期できるようになりました。
- をに更新します "[クライアントプラグイン ページ"^]。
- VMware vSphere Update Manager には、 vSphere Client の機能強化も含まれています。1 つの画面で、準拠状況の確認と修正をすべて実行できます。

VMware vSphere 6.7 U2 の詳細については、を参照してください "VMware vSphere のブログページ"。

VMware vCenter Server 6.7 U2 の更新の詳細については、を参照してください "リリースノート"。

> この解決策は vSphere 6.7U2 で検証されていますが、は他のコンポーネントで認定されている任意の vSphere バージョンをサポートします "ネットアップの Interoperability Matrix Tool （ IMT ）"。ネットアップでは、修正および機能強化のために、次のリリースバージョンの vSphere を導入することを推奨します。

ブートアーキテクチャ

FlexPod Express ブートアーキテクチャでは、次のオプションがサポートされています。

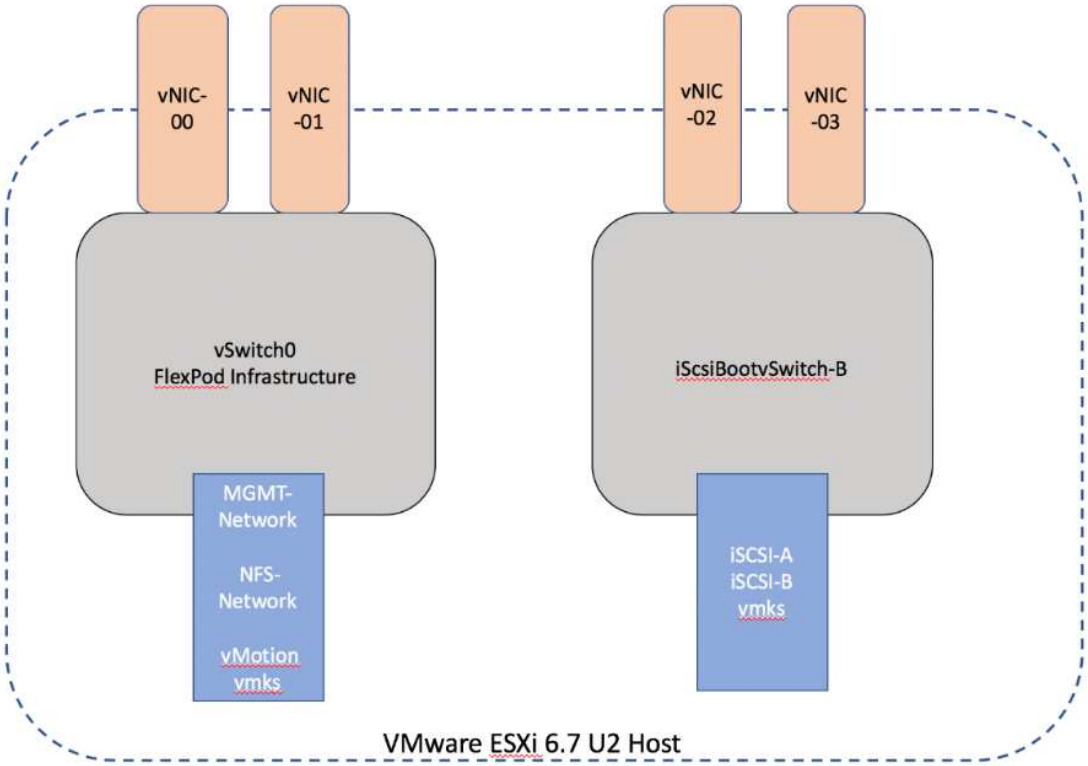
- iSCSI SAN LUN
- Cisco FlexFlash SD カード
- ローカルディスク

FlexPod データセンターは iSCSI LUN からブートされるため、 FlexPod Express でも iSCSI ブートを使用することで解決策の管理性が向上します。

ESXi ホストの仮想ネットワークインターフェイスカードのレイアウト

Cisco UCS VIC 1457 には 4 つの物理ポートがあります。この解決策検証では、 ESXi ホストを使用するのこれら 4 つの物理ポートを確認します。NIC の数が少ないかそれよりも多い場合は、 VMNIC の数が異なる可能性があります。

iSCSI ブート実装では、 iSCSI ブートには個別の Virtual Network Interface Card （ vNIC; 仮想ネットワークインターフェイスカード）が必要です。これらの vNIC は、次の図に示すように、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、 iSCSI ブート vSwitch に接続します。



"次は終わりです"

まとめ

FlexPod Express Validated Design は、業界をリードするコンポーネントを使用したシンプルで効果的な解決策です。拡張性に優れ、ハイパーバイザープラットフォームのオプションを提供する FlexPod Express は、特定のビジネスニーズに合わせてカスタマイズできます。FlexPod Express は、中堅企業、リモートオフィスやブランチオフィスなど、特定用途向けのソリューションを必要とする企業向けに設計されています。

"次へ：追加情報の検索場所。"

追加情報の参照先

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、次のドキュメントおよび Web サイトを参照してください。

- AFF および FAS システムドキュメントセンター

  "https://docs.netapp.com/platstor/index.jsp"

- AFF ドキュメントのリソースページ

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FlexPod Express with VMware vSphere 6.7 and NetApp AFF C190 Deployment Guide （現在のリリース

）

- NetApp のドキュメント

  "https://docs.netapp.com"

FlexPod Express with Cisco UCS C シリーズおよび NetApp AFF C190 シリーズ導入ガイド

NVA-1142-deploy ： FlexPod Express with Cisco UCS C シリーズ and NetApp AFF C190 Series - NVA Deployment （英語

ネットアップ、 Savita Kumari 氏

業界の動向から、共有インフラやクラウドコンピューティングへの大規模なデータセンターの移行が進行していることがわかります。さらに、データセンターで使い慣れたテクノロジを使用しているリモートオフィスやブランチオフィスに、シンプルで効果的な解決策を求めています。

FlexPod ® Express は、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus ファミリースイッチ、およびネットアップストレージテクノロジを基盤とした、事前設計されたベストプラクティスのデータセンターアーキテクチャです。FlexPod Express システムのコンポーネントは、 FlexPod Datacenter と同様に、小規模な IT インフラ環境全体での管理面の相乗効果を実現します。FlexPod Datacenter と FlexPod Express は、仮想化に最適なプラットフォームで、ベアメタルのオペレーティングシステムやエンタープライズワークロードに最適です。

FlexPod Datacenter と FlexPod Express は、ベースライン構成が可能で、多種多様なユースケースや要件に対応できるよう、サイズ設定と最適化が可能な柔軟性を備えています。FlexPod データセンターを利用している既存のお客様は、使い慣れたツールを使用して FlexPod Express システムを管理できます。FlexPod Express をご利用のお客様は、環境の拡大に合わせて、 FlexPod データセンターの管理に容易に移行できます。

FlexPod Express は、リモートオフィス、ブランチオフィス、中堅企業に最適なインフラ基盤です。また、専用のワークロードにインフラを提供したいお客様にも最適な解決策です。

FlexPod Express は、ほぼすべてのワークロードに適した、管理しやすいインフラを提供します。

解決策の概要

この FlexPod Express 解決策は、 FlexPod コンバージドインフラプログラムの一部です。

FlexPod 統合インフラプログラム

FlexPod リファレンスアーキテクチャは、 Cisco Validated Design （ CVD ；シスコ検証済み設計）または NetApp Verified Architectures （ NVA ；ネットアップ検証済みアーキテクチャ）として提供されます。これらのバリエーションでサポートされない構成が作成されない場合、特定の CVD または NVA からのお客様の要件に基づく差異は認められます。

FlexPod プログラムには、 FlexPod Express と FlexPod Datacenter の 2 つのソリューションが含まれていま

す。

- * FlexPod Express. * は、 Cisco とネットアップが提供するテクノロジを搭載したエントリレベルの解決策をお客様に提供します。
- * FlexPod * Datacenter * は、さまざまなワークロードやアプリケーションに最適な多目的基盤を提供します。

NetApp Verified Architecture プログラム

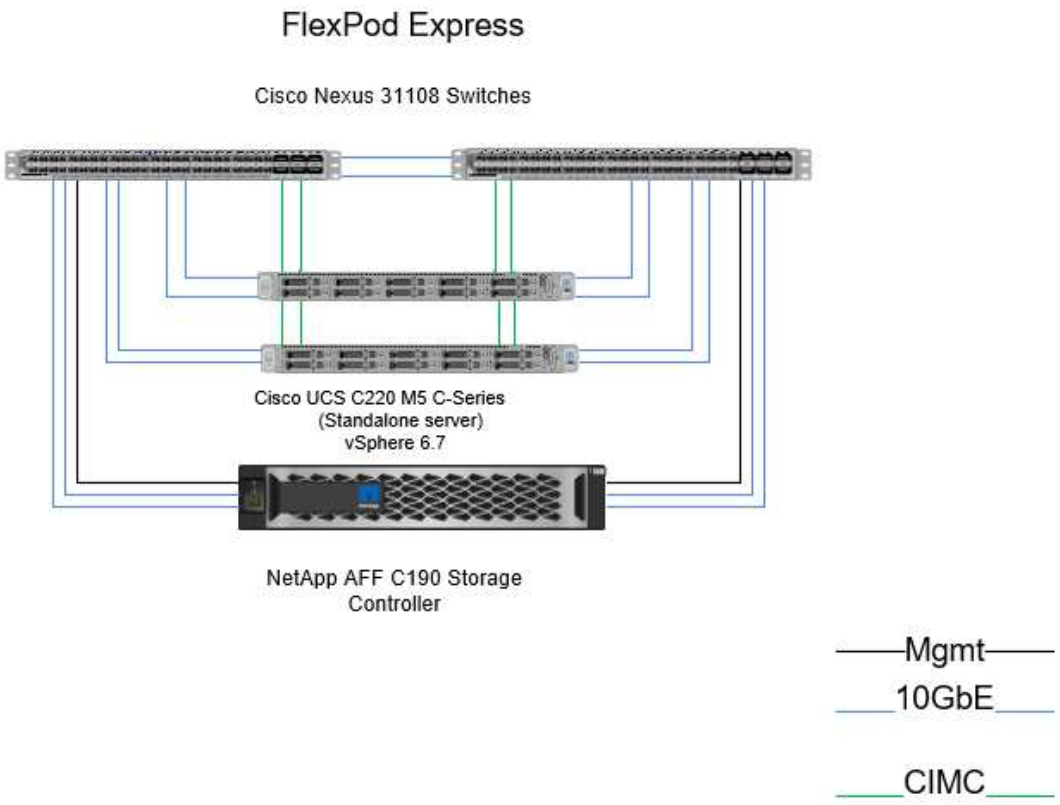
NetApp Verified Architecture プログラムは、ネットアップソリューションの検証済みアーキテクチャを提供するものです。NetApp Verified Architecture は、 NetApp 解決策アーキテクチャに次の品質を提供します。

- 徹底的なテスト
- あらかじめ規定されている
- 導入リスクを最小限に抑制
- 運用開始までの時間を短縮

このガイドでは、 VMware vSphere を使用した FlexPod Express の設計について詳しく説明します。また、この設計では、新しい AFF C190 システム（ NetApp ONTAP ® 9.6 を実行）、 Cisco Nexus 31108 、および Cisco UCS C シリーズ C220 M5 サーバをハイパーバイザーノードとして使用します。

解決策テクノロジ

この解決策は、ネットアップ、 Cisco 、 VMware の最新テクノロジを活用しています。この解決策は、ONTAP 9.6 を実行する新しい NetApp AFF C190 、 Cisco Nexus 31108 スイッチを 2 台使用する Cisco UCS C220 M5 ラックサーバ、 VMware vSphere 6.7U2 を実行する Cisco UCS C220 M5 ラックサーバを特長としています。この検証済み解決策は 10GbE テクノロジを使用しています。また、 FlexPod Express アーキテクチャが組織の進化するビジネスニーズに適応できるように、 2 つのハイパーバイザノードを一度に追加することでコンピューティング容量を拡張する方法についても説明します。



VIC 1457 で 4 つの物理 10GbE ポートを効率的に使用するには、各サーバから上部ラックスイッチへのリンクを 2 つ追加で作成します。

ユースケースの概要

FlexPod Express 解決策は、次のようないくつかのユースケースに適用できます。

- リモートオフィスまたはブランチオフィス
- 中堅・中小企業向け
- コスト効率に優れた専用の解決策が必要な環境

FlexPod Express は、仮想ワークロードと混在ワークロードに最適です。この解決策は vSphere 6.7U2 で検証されていますが、ネットアップ Interoperability Matrix Tool により、他のコンポーネントで認定されている vSphere バージョンもサポートされます。ネットアップでは、次のような修正点と強化された機能のために、vSphere 6.7U2 を導入することを推奨しています。

- HTTP 、 HTTPS 、 FTP 、 FTPS を含む、 vCenter Server Appliance のバックアップとリストアをサポートする新しいプロトコル SCP 、 NFS 、および SMB 。
- コンテンツライブラリを利用する際の新しい機能。vCenter Server でリンクモードが強化されている場合、ネイティブの VM テンプレートをコンテンツライブラリ間で同期できるようになりました。
- 更新されたクライアントプラグインページ。
- vSphere Update Manager （ VUM ）と vSphere Client の機能強化が追加されました。アタッチ、チェックコンプライアンス、修正の各アクションを 1 つの画面で実行できるようになりました。

この問題の詳細については、を参照してください "vSphere 6.7U2 ページ" および "vCenter Server 6.7U2 リリースノート"。

テクノロジ要件

FlexPod Express システムには、ハードウェアコンポーネントとソフトウェアコンポーネントを組み合わせて使用する必要があります。FlexPod Express では、システムにハイパーバイザーノードを追加するために必要なハードウェアコンポーネントについても、 2 つのユニット単位で説明します。

ハードウェア要件

選択したハイパーバイザーに関係なく、すべての FlexPod Express 構成で同じハードウェアが使用されます。したがって、ビジネス要件が変わっても、同じ FlexPod Express ハードウェア上で別のハイパーバイザーを使用できます。

次の表に、 FlexPod 構成および実装に必要なハードウェアコンポーネントを示します。解決策の実装に使用されるハードウェアコンポーネントは、お客様の要件に応じて変更される場合があります。

ハードウェア	数量
AFF C190 は、 2 ノードクラスタです	1.
Cisco C220 M5 サーバ	2.
Cisco Nexus 31108PC-V スイッチ	2.
Cisco UCS C220 M5 ラックサーバ用 Cisco UCS 仮想インターフェイスカード（ VIC ） 1457	2.

次の表に、 10GbE を実装するための基本構成に加えて、必要なハードウェアを示します。

ハードウェア	数量
Cisco UCS C220 M5 サーバ	2.
Cisco VIC 1457	2.

ソフトウェア要件

次の表に、 FlexPod Express ソリューションのアーキテクチャを実装するために必要なソフトウェアコンポーネントを示します。

ソフトウェア	バージョン	詳細
Cisco Integrated Management Controller （ CIMC ）	4.0.4	Cisco UCS C220 M5 ラックサーバの場合
Cisco nenic ドライバ	1.0.0.29	VIC 1457 インターフェイスカード用
Cisco NX-OS	7.0 （ 3 ） I7 （ 6 ）	Cisco Nexus 31108PC-V スイッチ向け
NetApp ONTAP	9.6	AFF C190 コントローラの場合

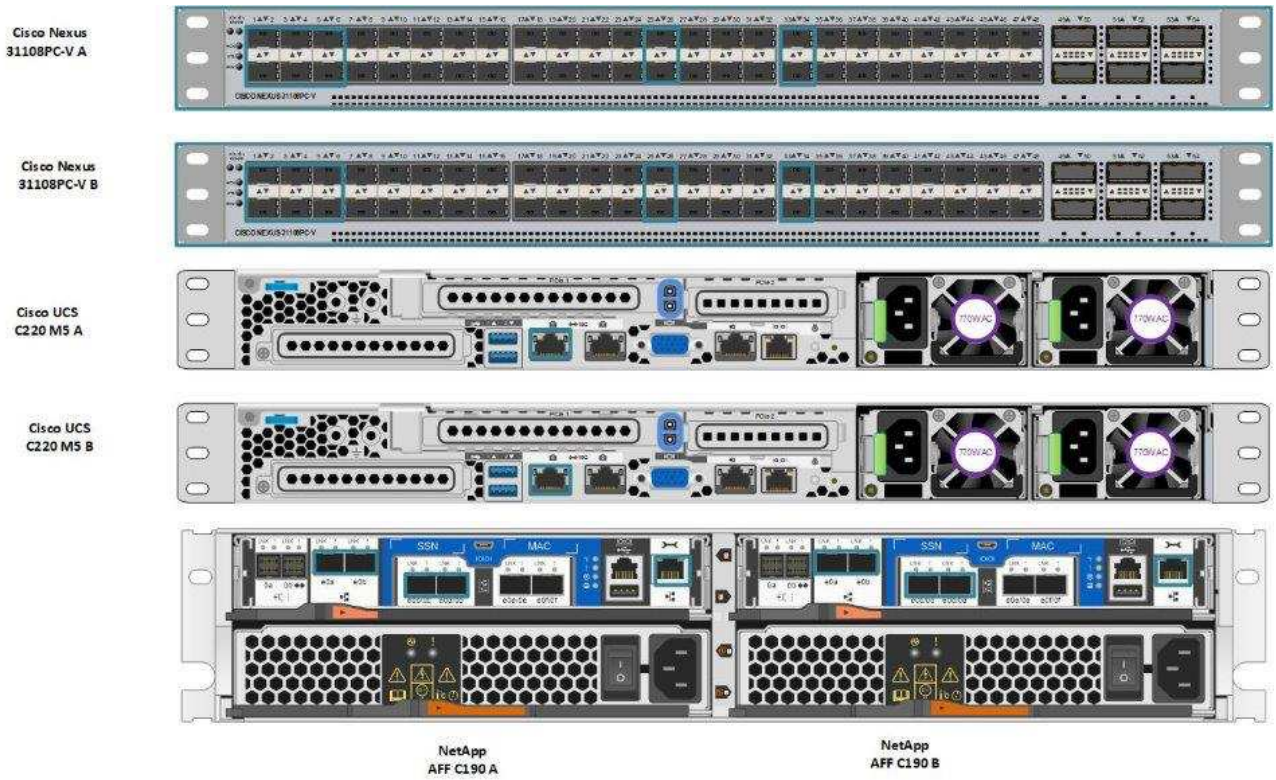
次の表に、 FlexPod Express でのすべての VMware vSphere 環境に必要なソフトウェアを示します。

ソフトウェア	バージョン
VMware vCenter Server Appliance の略	6.7U2
VMware vSphere ESXi ハイパーバイザー	6.7U2
NetApp VAAI Plug-in for ESXi	1.1.2
NetApp VSC	9.6

FlexPod エクスプレスケーブル接続情報

この参照検証は、次の図と表に示すようにケーブル接続されています。

この図は、リファレンス検証のケーブル配線を示しています。



次の表に、 Cisco Nexus スイッチ 31108PCV-A のケーブル接続情報を示します

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
Cisco Nexus スイッチ 31108PC-V A	Eth1/1	NetApp AFF C190 ストレージコントローラ A	e0c
	Eth1/2	NetApp AFF C190 ストレージコントローラ B	e0c
	Eth1/3	Cisco UCS C220 C シリーズスタンドアロンサーバ A	MLOM0
	Eth1/4	Cisco UCS C220 C シリーズスタンドアロンサーバ B	MLOM0
	Eth1/5	Cisco UCS C220 C シリーズスタンドアロンサーバ A	MLOM1
	Eth1/6	Cisco UCS C220 C シリーズスタンドアロンサーバ B	MLOM1
	Eth1/25	Cisco Nexus スイッチ 31108PC-V B	Eth1/25
	Eth1/26	Cisco Nexus スイッチ 31108PC-V B	Eth1/26
	Eth1/33	NetApp AFF C190 ストレージコントローラ A	e0M
	Eth1/34	Cisco UCS C220 C シリーズスタンドアロンサーバ A	CIMC （ FEX135/1/25 ）

この表は、 Cisco Nexus スイッチ 31108PCV-B のケーブル接続情報を示しています

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
Cisco Nexus スイッチ 31108PC-V B	Eth1/1	NetApp AFF C190 ストレージコントローラ A	e0d
	Eth1/2	NetApp AFF C190 ストレージコントローラ B	e0d
	Eth1/3	Cisco UCS C220 C シリーズスタンドアロンサーバ A	MLOM2
	Eth1/4	Cisco UCS C220 C シリーズスタンドアロンサーバ B	MLOM2
	Eth1/5	Cisco UCS C220 C シリーズスタンドアロンサーバ A	MLOM3
	Eth1/6	Cisco UCS C220 C シリーズスタンドアロンサーバ B	MLOM3
	Eth1/25	Cisco Nexus スイッチ 31108 A	Eth1/25
	Eth1/26	Cisco Nexus スイッチ 31108 A	Eth1/26
	Eth1/33	NetApp AFF C190 ストレージコントローラ B	e0M
	Eth1/34	Cisco UCS C220 C シリーズスタンドアロンサーバ B	CIMC （ FEX135/1/26 ）

次の表に、 NetApp AFF C190 ストレージコントローラ A のケーブル接続情報を示します

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
NetApp AFF C190 ストレージコントローラ A	e0a	NetApp AFF C190 ストレージコントローラ B	e0a
	e0b	NetApp AFF C190 ストレージコントローラ B	e0b
	e0c	Cisco Nexus スイッチ 31108PC-V A	Eth1/1
	e0d	Cisco Nexus スイッチ 31108PC-V B	Eth1/1
	e0M	Cisco Nexus スイッチ 31108PC-V A	Eth1/33

この表は、 NetApp AFF C190 ストレージコントローラ B のケーブル接続情報を示しています

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
NetApp AFF C190 ストレージコントローラ B	e0a	NetApp AFF C190 ストレージコントローラ A	e0a
	e0b	NetApp AFF C190 ストレージコントローラ A	e0b
	e0c	Cisco Nexus スイッチ 31108PC-V A	Eth1/2
	e0d	Cisco Nexus スイッチ 31108PC-V B	Eth1/2
	e0M	Cisco Nexus スイッチ 31108PC-V B	Eth1/33

導入手順

概要

このドキュメントでは、完全な冗長性と高可用性を備えた FlexPod Express システムの構成について詳しく説明します。この冗長性を反映するために、各手順で設定するコンポーネントをコンポーネント A またはコンポーネント B と呼びますたとえば、このドキュメントでプロビジョニングされている 2 台のネットアップストレージコントローラは、コントローラ A とコントローラ B で識別されます。スイッチ A とスイッチ B は Cisco Nexus スイッチのペアを表します。

また、このドキュメントでは、複数の Cisco UCS ホストをプロビジョニングする手順についても説明します。これらのホストは、サーバ A 、サーバ B などとして順次識別されます。

環境に関連する情報をステップに含める必要があることを示すために、コマンド構造の一部として「 \ <text>> 」が表示されます。「 vlan create 」コマンドについては、次の例を参照してください。

```
Controller01> network port vlan create –node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

本ドキュメントでは、 FlexPod Express 環境を完全に構成する方法について説明します。このプロセスでは、さまざまな手順で、お客様固有の命名規則、 IP アドレス、および VLAN （仮想 LAN ）スキームを入力する必要があります。次の表に、このガイドで説明するように、導入に必要な VLAN を示します。このテーブルは、特定のサイト変数に基づいて作成し、ドキュメントの設定手順を実装するために使用できます。

> 別々のインバンド管理 VLAN とアウトオブバンド管理 VLAN を使用する場合は、それらの間にレイヤ 3 ルートを作成する必要があります。この検証では、共通の管理 VLAN を使用しました。

VLAN 名	**VLAN** の目的	**VLAN ID**	
管理 VLAN	管理インターフェイス用の VLAN	3437	vSwitch0

VLAN 名	VLAN の目的	VLAN ID	
NFS VLAN	NFS トラフィック用の VLAN	3438	vSwitch0
VMware vMotion VLAN	ある物理ホストから別の物理ホストへの仮想マシン（ VM ）の移動用に指定された VLAN	3441	vSwitch0
VM トラフィック VLAN	VM アプリケーショントラフィック用の VLAN	3442	vSwitch0
iSCSI-A VLAN	ファブリック A の iSCSI トラフィック用 VLAN	3439	iScsiBootvSwitch
iSCSI-B VLAN	ファブリック B の iSCSI トラフィック用 VLAN	3440	iScsiBootvSwitch
ネイティブ VLAN	タグなしフレームが割り当てられている VLAN	2.	

VLAN 番号は、 FlexPod Express の設定全体で必要になります。VLAN は「 <<var_xxxx_vlan>> 」と呼ばれます。「 xxxx 」は VLAN の目的（ iSCSI-A など）です。

この検証で作成される vSwitch は 2 つです。

次の表に、解決策 vSwitch を示します。

vSwitch の名前	アクティブなアダプタ	ポート	MTU	負荷分散
vSwitch0	vmnic2 、 vmnic4	デフォルト（ 120 ）	9 、 000	IP ハッシュに基づいたルート
iScsiBootvSwitch	vmnic3 、 vmnic5	デフォルト（ 120 ）	9 、 000	発信元の仮想ポート ID に基づいたルート。

ロードバランシングの IP ハッシュ方式では、スタティック（モードオン）ポートチャネルで SRC-DST-IP EtherChannel を使用する基盤となる物理スイッチを適切に設定する必要があります。スイッチの設定ミスにより接続が断続的に中断される場合は、ポートチャネル設定のトラブルシューティングを行う間、 Cisco スイッチ上の 2 つの関連するアップリンクポートのいずれかを一時的にシャットダウンして ESXi 管理 vmkernel ポートへの通信をリストアします。

次の表に、作成される VMware VM を示します。

VM 概要の略	ホスト名
VMware vCenter Server の各機能を使用し	FlexPod - VCSA
Virtual Storage Console の略	Flexpo-VSC

Cisco Nexus 31108PC-V の導入

このセクションでは、 FlexPod Express 環境で使用する Cisco Nexus 33108PC-V スイ

ッチの構成について詳しく説明します。

Cisco Nexus 31108PC-V スイッチの初期セットアップ

次の手順では、 FlexPod Express の基本環境で使用するように Cisco Nexus スイッチを設定する方法について説明します。

> この手順は、 NX-OS ソフトウェアリリース 7.0(3) i7(6) を実行する Cisco Nexus 31108PC-V を使用していることを前提としています。

1. スイッチのコンソールポートを最初にブートして接続すると、 Cisco NX-OS セットアップが自動的に開始されます。この初期構成では、スイッチ名、 mgmt0 インターフェイス構成、および Secure Shell （ SSH ）セットアップなどの基本的な設定を行います。
2. FlexPod Express 管理ネットワークは、さまざまな方法で構成できます。31108PC-V スイッチの mgmt0 インターフェイスは既存の管理ネットワークに接続することも、 31108PC-V スイッチの mgmt0 インターフェイスをバックツーバックで接続することもできます。ただし、このリンクは、 SSH トラフィックなどの外部管理アクセスには使用できません。

   > この導入ガイドでは、 FlexPod Express Cisco Nexus 31108PC-V スイッチを既存の管理ネットワークに接続します。

3. Cisco Nexus 31108PC-V スイッチを設定するには、スイッチの電源をオンにし、画面の指示に従います。ここでは、両方のスイッチの初期セットアップを示します。スイッチ固有の情報については、適切な値に置き換えてください。

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 31108PC-V-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

4. 設定の概要が表示され、編集するかどうかの確認を求められます。設定が正しい場合は、「n」と入力します。

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. その後、この設定を使用するかどうかを確認するメッセージが表示され、保存します。その場合は、「y」と入力します。

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus スイッチ B について、この手順を繰り返します

高度な機能を有効にします

追加の設定オプションを提供するには、 Cisco NX-OS で特定の高度な機能をイネーブルにする必要があります。Cisco Nexus スイッチ A およびスイッチ B で適切な機能を有効にするには、コマンド（ config t ）を使用して構成モードに切り替え、次のコマンドを実行します。

```
feature interface-vlan
feature lacp
feature vpc
```

> ポートチャネルのデフォルトのロードバランシングハッシュでは、ソースおよびデスティネーションの IP アドレスを使用して、ポートチャネルのインターフェイス全体のロードバランシングアルゴリズムを決定します。ハッシュアルゴリズムにソースおよびデスティネーションの IP アドレス以外にもデータを提供することで、ポートチャネルのメンバー全体へのより均等なロードバランシングを実現できます。同じ理由から、ソースおよびデスティネーションの TCP ポートをハッシュアルゴリズムに追加することを推奨します。

構成モード（ config t ）から次のコマンドを入力し、 Cisco Nexus スイッチ A とスイッチ B のグローバルポートチャネルロードバランシング設定を行います。

```
port-channel load-balance src-dst ip-l4port
```

グローバルスパニングツリーを設定します

Cisco Nexus プラットフォームでは、ブリッジアシュアランスと呼ばれる新しい保護機能を使用します。ブリッジアシュアランスは、スパニングツリーアルゴリズムを実行していないデバイスでデータトラフィックの転送を継続する単方向リンクやその他のソフトウェア障害から保護するのに役立ちます。ポートは、プラットフォームに応じて、ネットワークやエッジなどのいくつかの状態のいずれかに配置できます。

すべてのポートがデフォルトでネットワークポートとみなされるように、ブリッジアシュアランスを設定することを推奨します。この設定により、ネットワーク管理者は各ポートの設定を確認することになります。また、未識別のエッジポートや、ブリッジアシュアランス機能が有効になっていないネイバーなど、最も一般的な構成エラーも表示されます。また、スパニングツリーでブロックするポートの数が少なすぎない方が、多くのポートをブロックする方が安全で、デフォルトのポートの状態でネットワーク全体の安定性を高めることができます。

サーバ、ストレージ、アップリンクスイッチを追加するときは、スパニングツリーの状態に細心の注意を払ってください。追加する構成がブリッジアシュアランスをサポートしていない場合は特に注意が必要です。このような場合は、ポートをアクティブにするためにポートタイプの変更が必要になることがあります。

Bridge Protocol Data Unit （ BPDU; ブリッジプロトコルデータユニット）ガードは、別の保護レイヤとしてデフォルトでエッジポートでイネーブルになっています。ネットワーク内のループを防止するために、このインターフェイス上で BPDU が別のスイッチから受信された場合、この機能はポートをシャットダウンします。

Cisco Nexus スイッチ A およびスイッチ B で、構成モード（ config t ）から次のコマンドを実行し、デフォルトのポートタイプや BPDU ガードなどのデフォルトのスパニングツリーオプションを設定します。

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

VLAN を定義します

VLAN の異なるポートを個別に設定する前に、レイヤ 2 VLAN をスイッチ上に定義する必要があります。また、 VLAN に名前を付けておくと、今後のトラブルシューティングを簡単に行うことができます。

構成モード（ config t ）から次のコマンドを実行し、 Cisco Nexus スイッチ A とスイッチ B のレイヤ 2 VLAN を定義して説明します。

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

アクセスポートと管理ポートの説明を設定します

レイヤ 2 VLAN に名前を割り当てる場合と同様に、すべてのインターフェイスに説明を設定すると、プロビジョニングとトラブルシューティングの両方に役立ちます。

各スイッチの構成モード（ config t ）から、 FlexPod Express の大規模構成に関する次のポート説明を入力します。

Cisco Nexus スイッチ A

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus スイッチ B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

サーバおよびストレージの管理インターフェイスを設定します

サーバとストレージの管理インターフェイスで使用する VLAN は、通常、どちらも 1 つだけです。そのため、管理インターフェイスポートをアクセスポートとして設定します。各スイッチの管理 VLAN を定義し、スパニングツリーポートタイプをエッジに変更します。

構成モード（ config t ）から次のコマンドを入力し、サーバとストレージの両方の管理インターフェイスのポート設定を行います。

Cisco Nexus スイッチ **A**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus スイッチ **B**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

仮想ポートチャネルのグローバル設定を実行します

仮想ポートチャネル（ vPC ）を使用すると、 2 つの異なる Cisco Nexus スイッチに物理的に接続されたリンクを、 3 番目のデバイスに対する単一のポートチャネルとして認識できます。3 番目のデバイスには、スイッチ、サーバ、またはその他のネットワークデバイスを使用できます。vPC はレイヤ 2 マルチパスを提供します。これにより、帯域幅を増やし、ノード間で複数のパラレルパスを有効にし、代替パスが存在する場合はトラフィックをロードバランシングすることで、冗長性を確保できます。

vPC には次の利点があります。

- 1 つのデバイスが 2 つのアップストリームデバイス間でポートチャネルを使用できるようにする
- スパニングツリープロトコルのブロックポートの排除
- ループフリートポロジを提供する
- 使用可能なすべてのアップリンク帯域幅を使用する
- リンクまたはデバイスのいずれかに障害が発生した場合に、高速コンバージェンスを提供します
- リンクレベルの耐障害性を提供します
- 高可用性の実現を支援します

vPC 機能を正しく機能させるには、 2 つの Cisco Nexus スイッチ間でいくつかの初期セットアップを行う必要があります。バックツーバックの mgmt0 構成を使用する場合は、インターフェイスに定義されたアドレスを使用し、「 ping `\<switch_a/B_mgmt0_ip_addr>vrf ' management コマンドを使用してそれらのアドレスで通信が可能であることを確認します。

構成モード（ config t ）から次のコマンドを実行し、両方のスイッチの vPC グローバル構成を設定します。

Cisco Nexus スイッチ **A**

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf
management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus スイッチ **B**

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

ストレージポートチャネルを設定します

ネットアップストレージコントローラでは、 Link Aggregation Control Protocol （ LACP ）を使用してネットワークにアクティブ / アクティブ接続できます。LACP は、スイッチ間でネゴシエーションとロギングの両方を行うため、 LACP の使用を推奨します。ネットワークは vPC 用に設定されているため、ストレージからのアクティブ / アクティブ接続を可能にして、別々の物理スイッチに接続できます。各コントローラには、各スイッチへのリンクが 2 つあります。ただし、 4 つのリンクはすべて同じ vPC とインターフェイスグループ（ ifgrp ）に属します。

構成モード（ config t ）から各スイッチで次のコマンドを実行し、個々のインターフェイスと、 NetApp AFF コントローラに接続されたポートのポートチャネル構成を設定します。

1. スイッチ A およびスイッチ B で次のコマンドを実行して、ストレージコントローラ A のポートチャネルを設定します。

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. スイッチ A とスイッチ B で次のコマンドを実行して、ストレージコントローラ B のポートチャネルを設定します。

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

サーバ接続を設定します

Cisco UCS サーバには 4 ポートの仮想インターフェイスカード VIC1457 があり、 iSCSI を使用した ESXi オペレーティングシステムのデータトラフィックおよびブートに使用されます。これらのインターフェイスは互いにフェイルオーバーするように設定されているため、単一リンク以上の冗長性が追加されます。これらのリンクを複数のスイッチに分散させることで、あるスイッチが完全に停止した場合でもサーバの運用を継続することができます。

構成モード（ config t ）から次のコマンドを実行し、各サーバに接続されたインターフェイスのポート設定を行います。

Cisco Nexus スイッチ A ： Cisco UCS サーバ A と Cisco UCS サーバ B の構成

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Cisco Nexus スイッチ B ： Cisco UCS サーバ A および Cisco UCS サーバ B の構成

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

サーバポートチャネルを設定します

スイッチ A およびスイッチ B で次のコマンドを実行して、サーバ A のポートチャネルを設定します。

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

スイッチ A およびスイッチ B で次のコマンドを実行して、サーバ B のポートチャネルを設定します。

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

この解決策検証では MTU 9000 が使用されていました。ただし、アプリケーションの要件に応じて、 MTU に別の値を設定することもできます。FlexPod 解決策全体で同じ MTU 値を設定することが重要です。コンポーネント間の MTU 設定が正しくないと、パケットが破棄され、これらのパケットを再送信する必要があり、解決策の全体的なパフォーマンスに影響します。

Cisco UCS サーバを追加して解決策を拡張するには、新しく追加したサーバがスイッチ A および B に接続されているスイッチポートを使用して、上記のコマンドを実行します

既存のネットワークインフラへのアップリンク

使用可能なネットワークインフラに応じて、 FlexPod 環境をアップリンクするためのいくつかの方法や機能があります。既存の Cisco Nexus 環境がある場合は、 vPC を使用して、 FlexPod 環境に含まれる Cisco Nexus 31108 スイッチをインフラにアップリンクすることを推奨します。必要に応じて、 10GbE インフラ解決策の場合は 10GbE アップリンク、 1GbE インフラ解決策の場合は 1GbE アップリンクがサポートされます。前述の手順を使用して、既存の環境へのアップリンク vPC を作成できます。設定が完了したら、 copy

start を実行して各スイッチに設定を保存してください。

"次の記事：ネットアップストレージ導入手順 （パート1）"

ネットアップストレージ導入手順（パート **1** ）

このセクションでは、 NetApp AFF ストレージ導入手順について説明します。

ネットアップストレージコントローラ **AFF C190** シリーズの設置

NetApp Hardware Universe の略

NetApp Hardware Universe （ HWU ）アプリケーションは、特定の ONTAP バージョンでサポートされているハードウェアコンポーネントとソフトウェアコンポーネントを提供します。ONTAP ソフトウェアで現在サポートされているネットアップのすべてのストレージアプライアンスに関する構成情報を提供します。また、コンポーネントの互換性の表も示します。

使用するハードウェアコンポーネントとソフトウェアコンポーネントが、インストールする ONTAP のバージョンでサポートされていることを確認します。

にアクセスします "HWU" システム設定ガイドを表示するアプリケーション。コントローラタブをクリックして、 ONTAP ソフトウェアの異なるバージョンとネットアップストレージアプライアンスの互換性を必要な仕様で確認します。

または、ストレージアプライアンス別にコンポーネントを比較するには、ストレージシステムの比較をクリックします。

コントローラ **AFFC190** シリーズの前提条件
ストレージシステムの物理的な場所を計画するには、 NetApp Hardware Universe を参照してください。次のセクションを参照してください。 • 電力要件 • サポートされている電源コード • オンボードポートとケーブル

ストレージコントローラ

AFF のコントローラの物理的な設置手順に従います "C190" ドキュメント

NetApp ONTAP 9.6

設定ワークシート

セットアップスクリプトを実行する前に、製品マニュアルから構成ワークシートに情報を記入してください。設定ワークシートは、 ONTAP 9.6 ソフトウェアセットアップガイドで入手できます。

> このシステムは、 2 ノードスイッチレスクラスタ構成でセットアップされます。

次の表に、 ONTAP 9.6 のインストールと設定の情報を示します。

クラスタの詳細	クラスタの詳細の値
クラスタノード A の IP アドレス	<<var_nodeA_mgmt_ip>>
クラスタノード A のネットマスク	<<var_nodeA_mgmt_mask>> を使用します
クラスタノード A のゲートウェイ	<<var_nodeA_mgmt_gateway>> を使用します
クラスタノードの名前	<<var_nodeA>> を使用します
クラスタノード B の IP アドレス	<<var_nodeB_mgmt_ip>>
クラスタノード B のネットマスク	<<var_nodeB_mgmt_mask>> を使用します
クラスタノード B のゲートウェイ	<<var_nodeB_mgmt_gateway>> を使用します
クラスタノード B の名前	<<var_nodeB>> を使用します
ONTAP 9.6 URL	<<var_url_boot_software>> を参照してください
クラスタの名前	\<<var_clustername> を使用します
クラスタ管理 IP アドレス	<<var_clustermgmt_ip>>
クラスタ B ゲートウェイ	<<var_clustermgmt_gateway>> を使用します
クラスタ B のネットマスク	<<var_clustermgmt_mask>> を使用します
ドメイン名	<<var_domain_name>> を参照してください
DNS サーバ IP （複数入力できます）	<<var_dns_server_ip を使用します
NTP サーバ IP （複数入力可能）	<<var_ntp_server_ip>>

ノード **A** を設定

ノード A を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   システムをブートできるようにします。

   ```
   autoboot
   ```

2. Ctrl+C キーを押してブートメニューを表示します。

   > ONTAP 9.6 がブートしているソフトウェアのバージョンでない場合は、次の手順に進み、新しいソフトウェアをインストールします。ONTAP 9.6 がブートしているバージョンの場合は、オプション 8 および y を選択してノードをリブートします。その後、手順 14 に進みます。

3. 新しいソフトウェアをインストールするには、オプション 7 を選択します。

4. 「 y 」と入力してアップグレードを実行します。
5. ダウンロードに使用するネットワークポートに e0M を選択します。
6. 「 y 」と入力して今すぐリブートします。
7. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

8. ソフトウェアを検索できる URL を入力します。

> ping 可能な Web サーバを指定する必要があります。

```
<<var_url_boot_software>>
```

9. ユーザ名が入力されていない場合は、 Enter キーを押します。
10. y を入力して、新しくインストールしたソフトウェアを、以降のリブートで使用するデフォルトとして設定します。
11. 「 y 」と入力してノードをリブートします。

> 新しいソフトウェアをインストールするときに、 BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

12. Ctrl+C キーを押してブートメニューを表示します。
13. Clean Configuration および Initialize All Disks のオプション 4 を選択します。
14. ディスクを初期化し、設定をリセットして、新しいファイルシステムをインストールするには、「 y 」と入力します。
15. 「 y 」と入力して、ディスク上のすべてのデータを消去します。

> ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。ノード A のディスクの初期化中も、ノード B の設定を続行できます。

ノード A を初期化している間に、ノード B の設定を開始します

ノード **B** を設定

ノード B を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Ctrl+C キーを押してブートメニューを表示します。

```
autoboot
```

3. プロンプトが表示されたら、 Ctrl-C キーを押します。

> ONTAP 9.6 がブートしているソフトウェアのバージョンでない場合は、次の手順に進み、新しいソフトウェアをインストールします。ONTAP 9.6 がブートしているバージョンの場合は、オプション 8 および y を選択してノードをリブートします。その後、手順 14 に進みます。

4. 新しいソフトウェアをインストールするには、オプション 7.A を選択します
5. 「 y 」と入力してアップグレードを実行します。
6. ダウンロードに使用するネットワークポートに e0M を選択します。
7. 「 y 」と入力して今すぐリブートします。
8. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. ソフトウェアを検索できる URL を入力します。

> ping 可能な Web サーバを指定する必要があります。

```
<<var_url_boot_software>>
```

10. ユーザ名が入力されていない場合は、 Enter キーを押します。
11. y を入力して、新しくインストールしたソフトウェアを、以降のリブートで使用するデフォルトとして設定します。
12. 「 y 」と入力してノードをリブートします。

> 新しいソフトウェアをインストールするときに、 BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

13. Ctrl+C キーを押してブートメニューを表示します。
14. Clean Configuration および Initialize All Disks のオプション 4 を選択します。
15. ディスクを初期化し、設定をリセットして、新しいファイルシステムをインストールするには、「 y 」と

入力します。

16. 「 y 」と入力して、ディスク上のすべてのデータを消去します。

> ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。

ノード **A** の構成とクラスタ構成を継続

ストレージコントローラ A （ノード A ）のコンソールポートに接続されているコンソールポートプログラムから、ノードセットアップスクリプトを実行します。このスクリプトは、 ONTAP 9.6 がノードで初めてブートしたときに表示されます。

> ONTAP 9.6 では、ノードとクラスタのセットアップ手順が少し変更されています。クラスタセットアップウィザードを使用してクラスタの最初のノードを設定できるようになりました。また、 NetApp ONTAP System Manager （旧 OnCommand ® System Manager ）を使用してクラスタを設定します。

1. プロンプトに従ってノード A をセットアップします

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. ノードの管理インターフェイスの IP アドレスに移動します。

> クラスタのセットアップは、 CLI を使用して実行することもできます。このドキュメントでは、 System Manager のセットアップガイドを使用したクラスタのセットアップについて説明します。

3. クラスタを設定するには、セットアップガイドをクリックします。
4. クラスタ名には「 \<<var_clustername>> 」を、設定する各ノードには「 <<var_nodeA>` 」と「 \<<var_nodeB>> 」を入力します。ストレージシステムに使用するパスワードを入力します。クラスタタイプに「スイッチレスクラスタ」を選択します。クラスタベースライセンスを入力します。
5. クラスタ、 NFS 、および iSCSI の機能ライセンスを入力することもできます。
6. クラスタの作成中を示すステータスメッセージが表示されます。このステータスメッセージは、複数のステータスを切り替えます。このプロセスには数分かかります。
7. ネットワークを設定します

a. [IP Address Range] オプションを選択解除します。

b. Cluster Management IP Address フィールドに「 <<var_clustermgmt_ip>> 」、 Netmask フィールドに「 \var_clustermgmt_mask>> 」と入力します。また、 Gateway フィールドに「 <<var_clustermgmt_gateway>> 」と入力します。使用する方法 Port フィールドのを選択し、ノード A の e0M を選択します

c. ノード A のノード管理 IP がすでに入力されています。ノード B には '\<<var_nodeA_mgmt_ip>> を入力します

d. [DNS Domain Name] フィールドに「 <<var_domain_name>` 」と入力します。[DNS Server IP Address] フィールドに「 \<<var_dns_server_ip>> 」と入力します。

> DNS サーバの IP アドレスは複数入力できます。

e. Primary NTP Server フィールドに「 10.63.172.16.2 」と入力します。

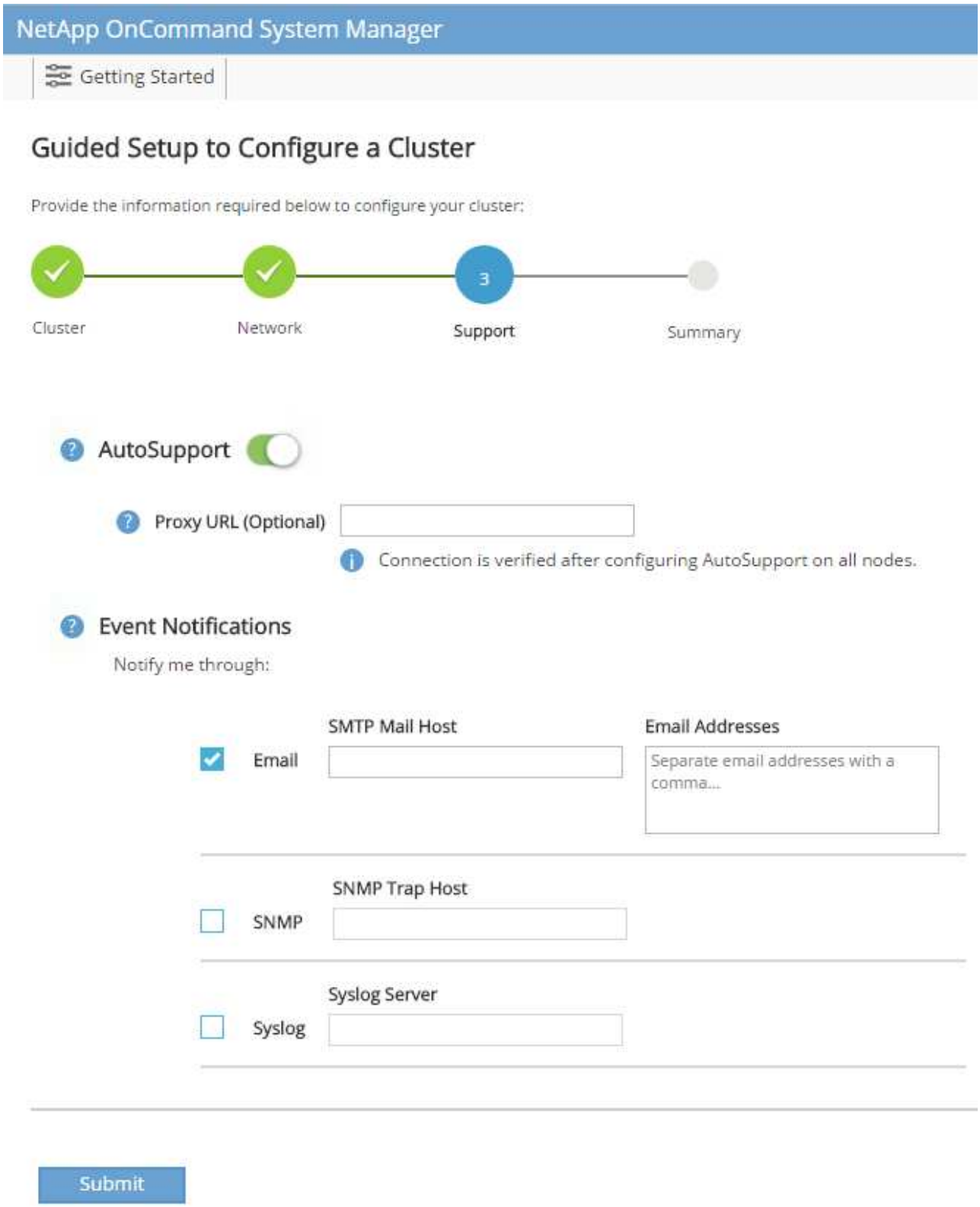
> 代替 NTP サーバを入力することもできます。「 \<<var_ntp_server_ip>> 」の IP アドレス「 10.63.172.16.2 」は、 Nexus Mgmt IP です。

8. サポート情報を設定します。

a. AutoSupport へのアクセスにプロキシが必要な環境の場合は、プロキシの URL をプロキシの URL に入力します。

b. イベント通知に使用する SMTP メールホストと E メールアドレスを入力します。

> 続行するには、少なくともイベント通知方式を設定する必要があります。いずれかの方法を選択できます。



クラスタ構成が完了したことを示すメッセージが表示されたら、 Manage Your Cluster （クラスタの管理）をクリックしてストレージを構成します。

ストレージノードとベースクラスタの設定が完了したら、ストレージクラスタの設定に進むことができます。

すべてのスペアディスクを初期化します

クラスタ内のすべてのスペアディスクを初期化するには、次のコマンドを実行します。

```
disk zerospares
```

オンボード **UTA2** ポートパーソナリティを設定します

1. ucadmin show コマンドを実行して、現在のモードとポートの現在のタイプを確認します。

```
AFF C190::> ucadmin show
                       Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. 使用中のポートの現在のモードが CNA であり、現在のタイプが target に設定されていることを確認します。そうでない場合は、次のコマンドを使用してポートパーソナリティを変更します。

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

> 前のコマンドを実行するには、ポートをオフラインにする必要があります。ポートをオフラインにするには、次のコマンドを実行します。

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

> ポートパーソナリティを変更した場合、変更を有効にするには、各ノードをリブートする必要があります。

管理論理インターフェイスの名前を変更します

管理論理インターフェイス（ LIF ）の名前を変更するには、次の手順を実行します。

1. 現在の管理 LIF の名前を表示します。

```
network interface show -vserver <<clustername>>
```

2. クラスタ管理 LIF の名前を変更します。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. ノード B の管理 LIF の名前を変更します。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

クラスタ管理で自動リバートを設定する

クラスタ管理インターフェイスで auto-revert パラメータを設定します。

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

サービスプロセッサのネットワークインターフェイスをセットアップします

各ノードのサービスプロセッサに静的 IPv4 アドレスを割り当てるには、次のコマンドを実行します。

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

サービスプロセッサの IP アドレスは、ノード管理 IP アドレスと同じサブネット内にある必要があります。

ONTAP でストレージフェイルオーバーを有効にします

ストレージフェイルオーバーが有効になっていることを確認するには、フェイルオーバーペアで次のコマンド

を実行します。

1. ストレージフェイルオーバーのステータスを確認

```
storage failover show
```

> \<<var_nodeA>>` と \<<var_nodeB>> の両方がテイクオーバーを実行できる必要があります。ノードでテイクオーバーを実行できる場合は、ステップ 3 に進みます。

2. 2 つのノードのどちらかでフェイルオーバーを有効にします。

```
storage failover modify -node <<var_nodeA>> -enabled true
```

> フェイルオーバーは、片方のノードで有効にすれば、両方のノードで有効になります。

3. 2 ノードクラスタの HA ステータスを確認

> この手順は、ノードが 3 つ以上のクラスタには適用されません。

```
cluster ha show
```

4. ハイアベイラビリティが構成されている場合は、ステップ 6 に進みます。ハイアベイラビリティが設定されている場合は、コマンドの実行時に次のメッセージが表示されます。

```
High Availability Configured: true
```

5. HA モードは 2 ノードクラスタでのみ有効にします。

> ノードが 3 つ以上のクラスタの場合は、このコマンドを実行しないでください。フェイルオーバーで問題が発生します。

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. ハードウェアアシストが正しく設定されていることを確認し、必要に応じてパートナーの IP アドレスを変更

```
storage failover hwassist show
```

「 Keep Alive Status: Error: 」というメッセージは、いずれかのコントローラがハードウェアアシストが設定されていないことを示すハードウェアアシストのキープアライブアラートをパートナーから受信しなかったことを示します。ハードウェアアシストを設定するには、次のコマンドを実行します。

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP でジャンボフレーム MTU ブロードキャストドメインを作成します

MTU が 9000 のデータブロードキャストドメインを作成するには、次のコマンドを実行します。

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

デフォルトのブロードキャストドメインからデータポートを削除します

10GbE のデータポートは iSCSI / NFS トラフィックに使用されます。これらのポートはデフォルトドメインから削除する必要があります。ポート e0e と e0f は使用されないため、デフォルトのドメインからも削除する必要があります。

ブロードキャストドメインからポートを削除するには、次のコマンドを実行します。

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 ポートではフロー制御を無効にします

ネットアップでは、外部デバイスに接続されているすべての UTA2 ポートでフロー制御を無効にすることをベストプラクティスとして推奨します。フロー制御を無効にするには、次のコマンドを実行します。

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

ONTAP でインターフェイスグループ **LACP** を設定します

このタイプのインターフェイスグループには複数のイーサネットインターフェイスと LACP をサポートするスイッチが必要です。セクション 5.1 のこのガイドの手順に基づいて設定されていることを確認してください。

クラスタのプロンプトで、次の手順を実行します。

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

ONTAP でジャンボフレームを設定します

ジャンボフレーム（通常は MTU が 9 、 000 バイトのフレーム）を使用するように ONTAP ネットワークポートを設定するには、クラスタシェルから次のコマンドを実行します。

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

ONTAP で VLAN を作成します

ONTAP で VLAN を作成するには、次の手順を実行します。

1. NFS VLAN ポートを作成し、データブロードキャストドメインに追加します。

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. iSCSI VLAN ポートを作成し、データブロードキャストドメインに追加します。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN ポートを作成します。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

ONTAP でデータアグリゲートを作成する

ONTAP のセットアッププロセスで、ルートボリュームを含むアグリゲートが作成されます。追加のアグリゲートを作成するには、アグリゲート名、アグリゲートを作成するノード、アグリゲートに含まれるディスク数を確認します。

アグリゲートを作成するには、次のコマンドを実行します。

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

構成内で少なくとも 1 つのディスクをスペアとして保持します（最も大きいディスクを選択してください）。ディスクのタイプとサイズごとに少なくとも 1 つのスペアを用意しておくことを推奨します。

ディスクは 5 本から始めて、追加のストレージが必要になったときにアグリゲートにディスクを追加できます。

ディスクの初期化が完了するまで、アグリゲートを作成することはできません。aggr show コマンドを実行して、アグリゲートの作成ステータスを表示します。次の手順は、aggr1_cluster1_01 がオンラインになるまで実行しないでください。

ONTAP でタイムゾーンを設定します

時刻の同期を設定し、クラスタのタイムゾーンを設定するには、次のコマンドを実行します。

```
timezone <<var_timezone>>
```

たとえば、米国東部では、タイムゾーンは America/New_York になります。タイムゾーン名の入力を開始したら、 Tab キーを押して使用可能なオプションを表示します。

ONTAP で SNMP を設定します

SNMP を設定するには、次の手順を実行します。

1. 場所や連絡先などの SNMP 基本情報を設定します。ポーリング時に ' この情報は 'sysLocation' 変数と SNMP の sysContact' 変数として表示されます

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. リモートホストに送信する SNMP トラップを設定します。

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

ONTAP で SNMPv1 を設定します

SNMPv1 を設定するには、コミュニティと呼ばれる共有シークレットのプレーンテキストパスワードを設定します。

```
snmp community add ro <<var_snmp_community>>
```

「 snmp community delete all 」コマンドは慎重に使用してください。他の監視製品にコミュニティストリングが使用されている場合、このコマンドはそれらを削除します。

ONTAP で SNMPv3 を設定します

SNMPv3 では、認証用のユーザを定義および設定する必要があります。SNMPv3 を設定するには、次の手順を実行します。

1. 「 securitysnmpusers 」コマンドを実行して、エンジン ID を表示します。
2. 「 mpv3user 」という名前のユーザを作成します。

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 信頼できるエンティティのエンジン ID を入力し、認証プロトコルとして MD5 を選択してください。
4. プロンプトが表示されたら、認証プロトコルのパスワードとして最低 8 文字のパスワードを入力します。
5. プライバシープロトコルとして des を選択します。
6. プロンプトが表示されたら、プライバシープロトコルのパスワードとして最低 8 文字のパスワードを入力します。

ONTAP で AutoSupport HTTPS を設定します

NetApp AutoSupport ツールは、サポート概要情報を HTTPS 経由でネットアップに送信します。AutoSupport を設定するには、次のコマンドを実行します。

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Storage Virtual Machine を作成

インフラ Storage Virtual Machine （ SVM ）を作成するには、次の手順を実行します。

1. vserver create コマンドを実行します

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. NetApp VSC のインフラ SVM アグリゲートリストにデータアグリゲートを追加します。

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS と iSCSI を残して、未使用のストレージプロトコルを SVM から削除します。

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. インフラ SVM で NFS プロトコルを有効にして実行します。

```
nfs create -vserver Infra-SVM -udp disabled
```

5. NetApp NFS VAAI プラグインの「 VM vStorage 」パラメータをオンにします。次に、 NFS が設定されていることを確認します。

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

> SVM は以前は Vserver と呼ばれていたため、コマンドラインでは「 vserver 」の前にコマンドが配置されます。

ONTAP で NFSv3 を設定します

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ESXi ホスト A の NFS IP アドレス	<<var_esxi_hostA_nfs_ip>>
ESXi ホスト B の NFS IP アドレス	<<var_esxi_hostB_nfs_ip>> を追加します

SVM に NFS を設定するには、次のコマンドを実行します。

1. デフォルトのエクスポートポリシーに各 ESXi ホスト用のルールを作成します。
2. 作成する各 ESXi ホストにルールを割り当てます。各ホストには独自のルールインデックスがあります。最初の ESXi ホストのルールインデックスは 1 、 2 番目の ESXi ホストのルールインデックスは 2 のようになります。

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. エクスポートポリシーをインフラ SVM ルートボリュームに割り当てます。

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

> エクスポートポリシーは、 vSphere のセットアップ後にインストールするように選択した場合に自動的に処理されます。インストールしない場合は、 Cisco UCS C シリーズサーバを追加するときにエクスポートポリシールールを作成する必要があります。

ONTAP で iSCSI サービスを作成します

SVM に iSCSI サービスを作成するには、次のコマンドを実行します。また、このコマンドでは iSCSI サービスが開始され、 SVM の iSCSI IQN が設定されます。iSCSI が設定されていることを確認します。

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP で SVM ルートボリュームの負荷共有ミラーを作成

ONTAP で SVM ルートボリュームの負荷共有ミラーを作成するには、次の手順を実行します。

1. インフラ SVM ルートボリュームの負荷共有ミラーとなるボリュームを各ノードに作成します。

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate
aggr1_nodeA -size 1GB -type DP
volume create -vserver Infra_Vserver -volume rootvol_m02 -aggregate
aggr1_nodeB -size 1GB -type DP
```

2. ルートボリュームのミラー関係を 15 分ごとに更新するジョブスケジュールを作成します。

```
job schedule interval create -name 15min -minutes 15
```

3. ミラーリング関係を作成

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. ミラーリング関係を初期化し、作成されたことを確認します。

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

ONTAP で HTTPS アクセスを設定する

ストレージコントローラへのセキュアなアクセスを設定するには、次の手順を実行します。

1. 証明書コマンドにアクセスするには、権限レベルを上げてください。

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 通常は、自己署名証明書がすでに存在します。次のコマンドを実行して証明書を確認します。

```
security certificate show
```

3. 表示されている各 SVM の証明書の共通名は、 SVM の DNS FQDN と一致する必要があります。4 つのデフォルト証明書を削除して、認証局の自己署名証明書または証明書に置き換える必要があります。

> 証明書を作成する前に期限切れになった証明書を削除することを推奨します。「 securitycertificate delete 」コマンドを実行して、期限切れの証明書を削除します。次のコマンドでは、タブ補完を使用して、デフォルトの証明書を選択して削除します。

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 自己署名証明書を生成してインストールするには、次のコマンドを 1 回限りのコマンドとして実行します。インフラ SVM とクラスタ SVM のサーバ証明書を生成します。これらのコマンドの実行に役立つように、タブ補完を使用してください。

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 次の手順で必要なパラメータの値を取得するには、 security certificate show コマンドを実行します。
6. 作成した各証明書を ' – server-enabled true' および– client-enabled false' パラメータを使用して有効にしますタブ補完を使用してください。

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL と HTTPS アクセスを設定して有効にし、 HTTP アクセスを無効にします。

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

これらのコマンドの一部で、エントリが存在しないことを示すエラーメッセージが返されますが、これは通常の動作であり問題ありません。

8. admin 権限レベルにリバートしてセットアップを作成し、 SVM を Web で使用できるようにします。

```
set -privilege admin
vserver services web modify -name spi -vserver * -enabled true
```

ONTAP で NetApp FlexVol ボリュームを作成します

NetApp FlexVol ® ボリュームを作成するには、ボリューム名、サイズ、およびボリュームが存在するアグリゲートを入力します。2 つの VMware データストアボリュームと 1 つのサーバブートボリュームを作成します。

```
volume create -vserver Infra-SVM -volume infra_datastore -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP で LUN を作成します

2 つのブート LUN を作成するには、次のコマンドを実行します。

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cisco UCS C シリーズサーバを追加する場合は、追加のブート LUN を作成する必要があります。

ONTAP に **iSCSI LIF** を作成

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ストレージノード A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
ストレージノード A の iSCSI LIF01A ネットワークマスク	<<var_nodeA_iscsi_lif01a _mask>> をクリックします
ストレージノード A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
ストレージノード A の iSCSI LIF01B ネットワークマスク	<<var_nodeA_iscsi_lif01b_mask>> をクリックします
ストレージノード B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
ストレージノード B iSCSI LIF01A ネットワークマスク	<<var_nodeB_iscsi_lif01a_mask>> を選択します
ストレージノード B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
ストレージノード B iSCSI LIF01B ネットワークマスク	<<var_nodeB_iscsi_lif01b_mask>> をクリックします

各ノードに 2 つずつ、 4 つの iSCSI LIF を作成します。

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface show
```

ONTAP に NFS LIF を作成します

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ストレージノード A NFS LIF 01 IP	<<var_nodeA_nfs_lif_01_ip>>
ストレージノード A NFS LIF 01 のネットワークマスク	<<var_nodeA_nfs_lif_01_mask>> を参照してください
ストレージノード B の NFS LIF 02 IP	<<var_nodeB_nfs_lif_02_ip>>
ストレージノード B の NFS LIF 02 ネットワークマスク	<<var_nodeB_nfs_lif_02_mask>> を参照してください

NFS LIF を作成します。

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface show
```

インフラ **SVM** 管理者を追加

次の表に、 SVM 管理者を追加するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
vsmgmt IP	<<var_svm_mgmt_ip>> を追加します
vsmgmt ネットワークマスク	<<var_SVM_mgmt_mask>> を使用します
vsmgmt デフォルトゲートウェイ	<<var_SVM_mgmt_gateway>> を使用します

インフラ SVM 管理者および SVM 管理論理インターフェイスを管理ネットワークに追加するには、次の手順を実行します。

1. 次のコマンドを実行します。

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port  e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true
```

> ここで指定する SVM 管理 IP は、ストレージクラスタ管理 IP と同じサブネット内にある必要があります。

2. SVM 管理インターフェイスの外部へのアクセスを許可するデフォルトルートを作成します。

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. SVM の vsadmin ユーザのパスワードを設定し、ユーザのロックを解除します。

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver Infra-SVM
```

"次の記事：Cisco UCS Cシリーズラックサーバの導入"

Cisco UCS C シリーズラックサーバを導入する

ここでは、手順 Express 構成で使用する Cisco UCS C シリーズスタンドアロンラックサーバを設定するための詳細な FlexPod について説明します。

CIMC の **Cisco UCS C** シリーズスタンドアロンサーバの初期セットアップを実行します

Cisco UCS C シリーズスタンドアロンサーバの CIMC インターフェイスの初期セットアップを行うには、次の手順を実行します。

次の表に、 Cisco UCS C シリーズスタンドアロンサーバごとに CIMC を設定するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
CIMC IP アドレス	\<CIMC_IP>>
CIMC サブネットマスク	\<CIMC_netmask に追加されました
CIMC デフォルトゲートウェイ	\<CIMC_Gateway>> のようになります

この検証で使用されている CIMC のバージョンは CIMC 4.4.0(4) です。

すべてのサーバ

1. Cisco KVM （キーボード、ビデオ、およびマウス）ドングル（サーバに付属）を、サーバ前面の KVM ポートに取り付けます。VGA モニタと USB キーボードを、 KVM ドングルの対応するポートに接続します。

   サーバの電源を入れ、 CIMC 設定を開始するかどうか確認するプロンプトが表示されたら F8 キーを押します。

2. CIMC 設定ユーティリティで、次のオプションを設定します。

   a. ネットワークインターフェイスカード（ NIC ）モード：

      専用の「 [X] 」

   b. IP （ベーシック）：

      IPv4 ：「 [X] 」

      DHCP が有効になっています

      CIMC IP:`\<CIMC_IP>`

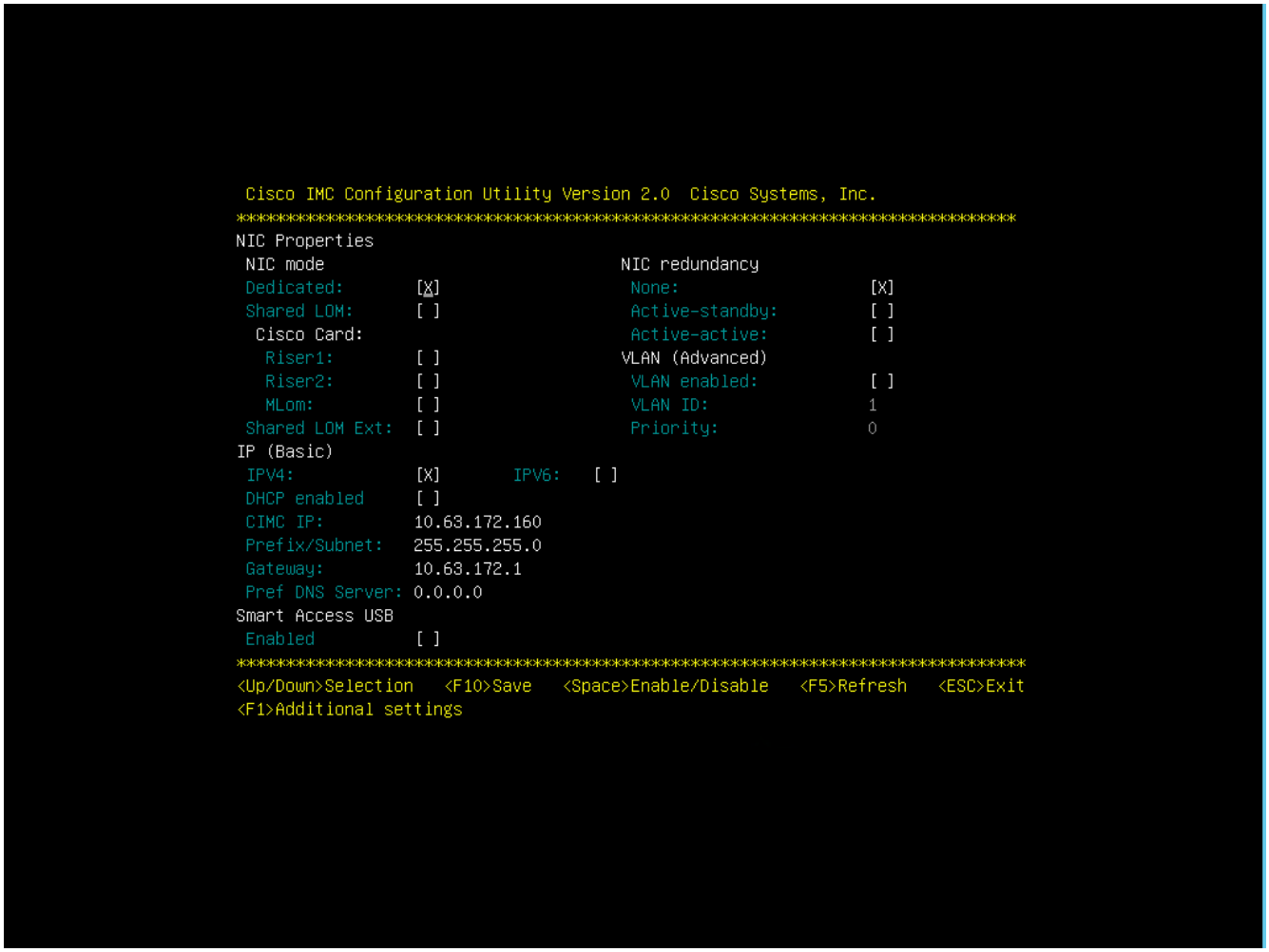
      プレフィックス / サブネット： `\<CIMC_netmask>`

      ゲートウェイ：`\<CIMC_gateway>`

   c. VLAN （ Advanced ）： VLAN タギングを無効にする場合は、オフのままにします。

      NIC の冗長性

      なし :[X]`



3. F1 キーを押して、その他の設定を表示します。

   a. 共通プロパティ：

      ホスト名：`\<ESXi_host_name>`

      ダイナミック DNS:`[]

      工場出荷時のデフォルト：オフのままにします。

   b. デフォルトユーザ（ basic ）：

      デフォルトのパスワード： `\<admin_password>`

      パスワード「 \<admin_password>>` 」を再入力します

      ポートのプロパティ：デフォルト値を使用します。

   ポートプロファイル：クリアしたままにします。

4. F10 キーを押し、 CIMC インターフェイス設定を保存します。
5. 設定を保存したら、 Esc キーを押して終了します。

Cisco UCS C シリーズサーバの **iSCSI** ブートを設定します

この FlexPod Express 構成では、 iSCSI ブートに VIC1457 が使用されます。

次の表に、 iSCSI ブートの設定に必要な情報を示します。

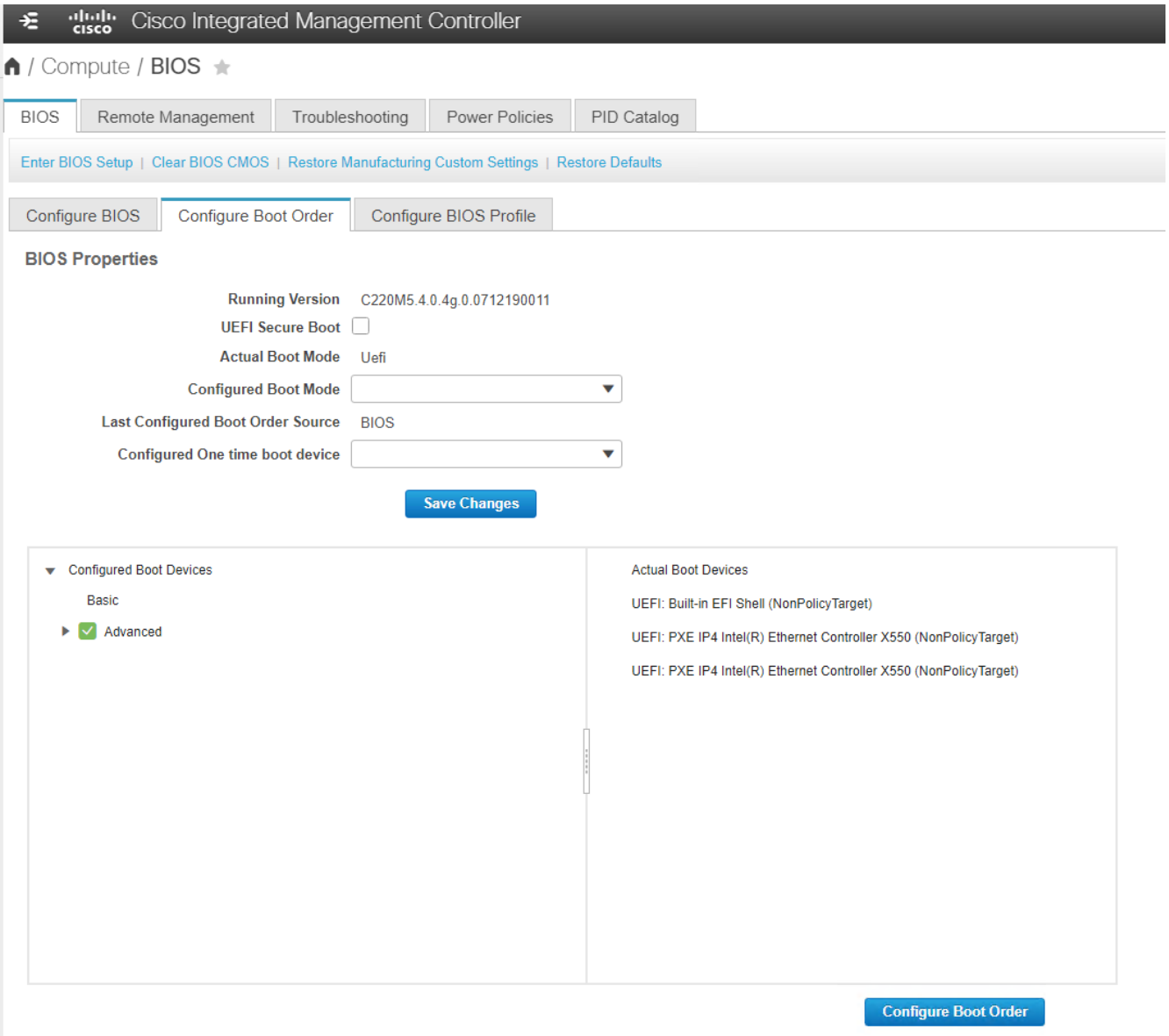
斜体のフォントは、 ESXi ホストごとに一意の変数を示します。

詳細（ **Detail** ）	詳細値
ESXi ホストイニシエータの名前	<<var_UCS_initiator_name_a>> を参照してください
ESXi ホスト iSCSI-A IP	<<var_esxi_host_iscsia_ip>>
ESXi ホスト iSCSI - ネットワークマスク	<<var_esxi_host_iscsia_mask>> を指定します
ESXi ホスト iSCSI A のデフォルトゲートウェイ	<<var_esxi_host_iscsia_gateway>> を指定します
ESXi ホストイニシエータ B の名前	<<var_UCS_initiator_name_b>> を参照してください
ESXi ホスト iSCSI-B IP	<<var_esxi_host_iSCSIb_ip>>
ESXi ホストの iSCSI-B ネットワークマスク	<<var_esxi_host_iSCSIb_mask>> を指定します
ESXi ホスト iSCSI-B ゲートウェイ	<<var_esxi_host_iSCSIb_gateway>> を指定します
IP アドレス iSCSI_lif01a	<<var_iscsi_dlif01a>>
IP アドレス iSCSI_lif02a	<<var_iscsi_dlif02a>>
IP アドレス iSCSI_lif01b	<<var_iscsi_dlif01b>> を参照してください
IP アドレス iSCSI_lif02b	<<var_iscsi_dlif02b>>
インフラ SVM IQN	<<var_svm_iqn>> をクリックします

起動順序の設定

ブート順の設定を行うには、次の手順を実行します。

1. CIMC インターフェイスのブラウザウィンドウで、 [Compute] タブをクリックし、 BIOS を選択します。
2. Configure Boot Order （起動順序の設定）をクリックし、 OK をクリックします。



3. Add Boot Device の下のデバイスをクリックし、 Advanced タブに移動して、次のデバイスを設定します。

   a. 仮想メディアの追加：

      名前： KVM-CD-DVD

      サブタイプ： KVM マップ DVD

      状態：有効

      順序： 1.

   b. iSCSI ブートの追加：

      名前： iSCSI-A

      状態：有効

ご注文： 2.

スロット： mLOM

ポート： 1.

c. Add iSCSI Boot をクリックします。

名前： iSCSI-B

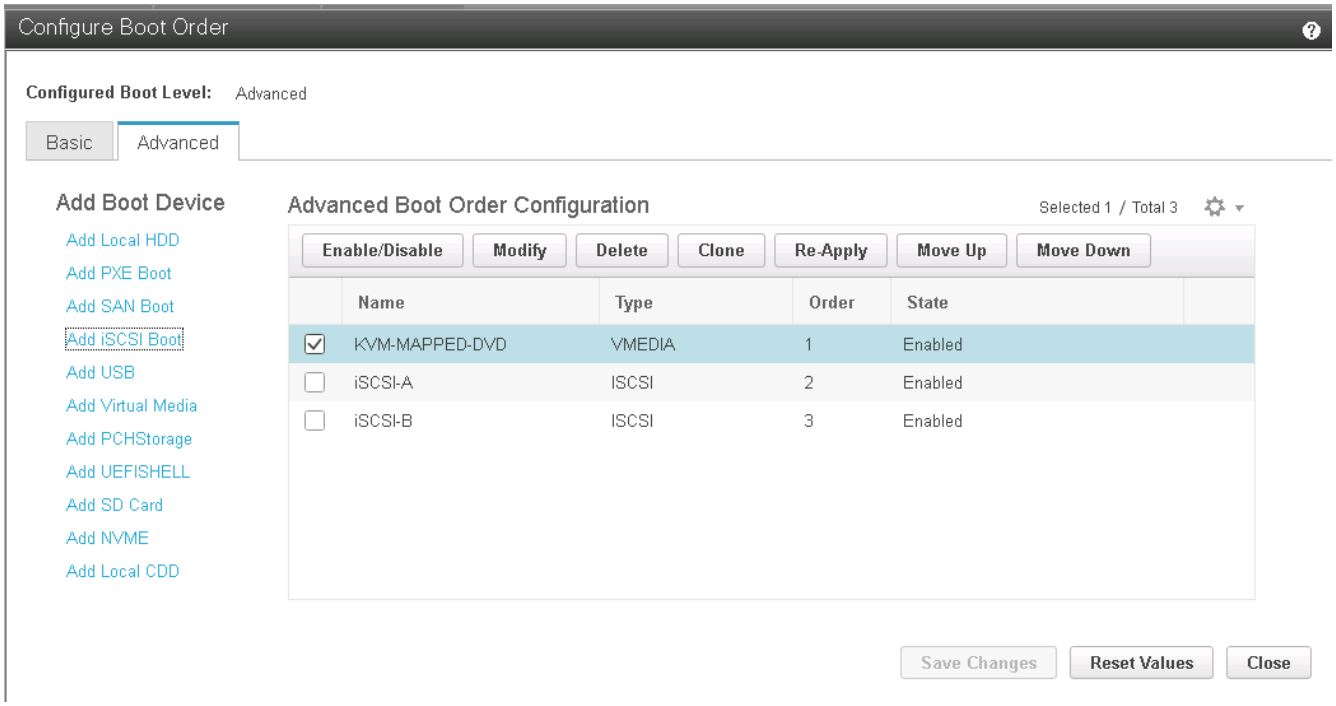
状態：有効

順序： 3.

スロット： mLOM

ポート： 3.

4. Add Device をクリックします。
5. [変更の保存] をクリックし、 [閉じる] をクリックします。



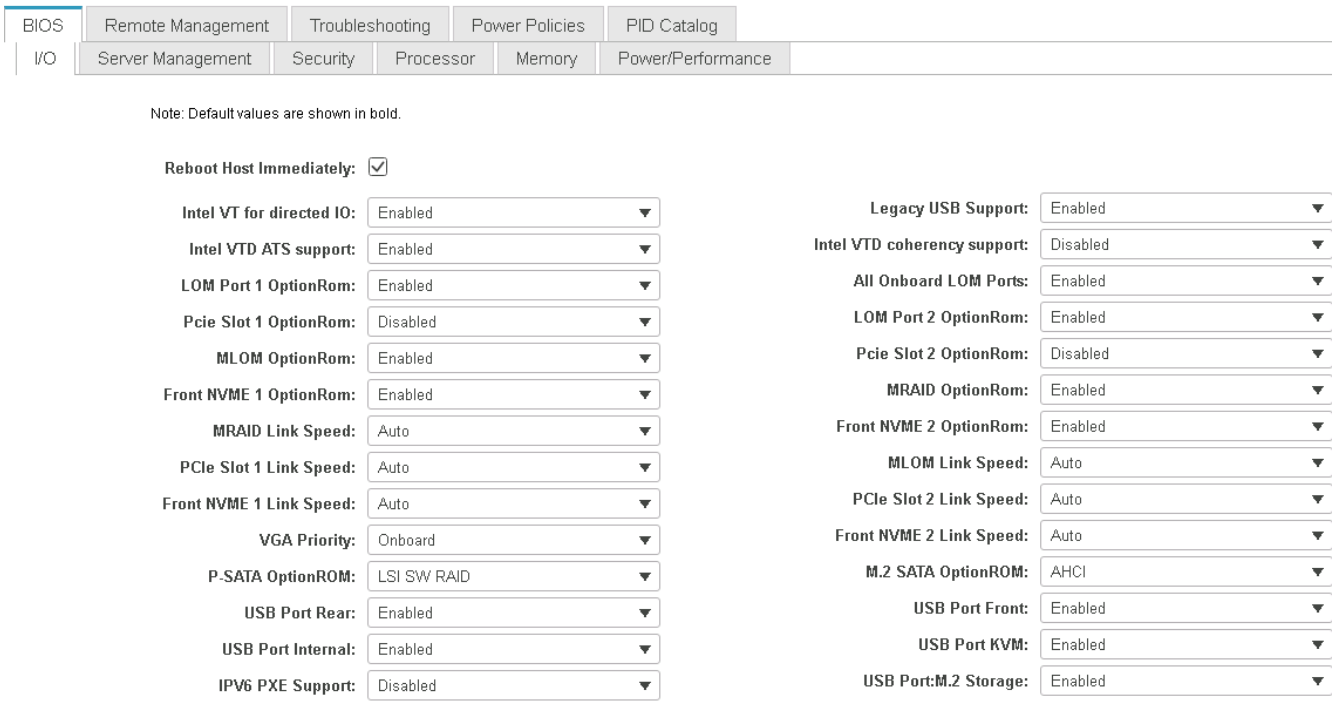
6. サーバをリブートして、新しいブート順序でブートします。

RAID コントローラを無効にする（存在する場合）

C シリーズサーバに RAID コントローラが搭載されている場合は、次の手順を実行します。SAN 構成からのブートでは RAID コントローラは必要ありません。必要に応じて、サーバから RAID コントローラを物理的に取り外すこともできます。

1. Compute タブで、 CIMC の左側のナビゲーションペインで BIOS をクリックします。
2. [Configure BIOS] を選択します。

3. 下にスクロールして [PCIe Slot:HBA Option ROM] を表示します。
4. 値が無効になっていない場合は、 disabled に設定します。

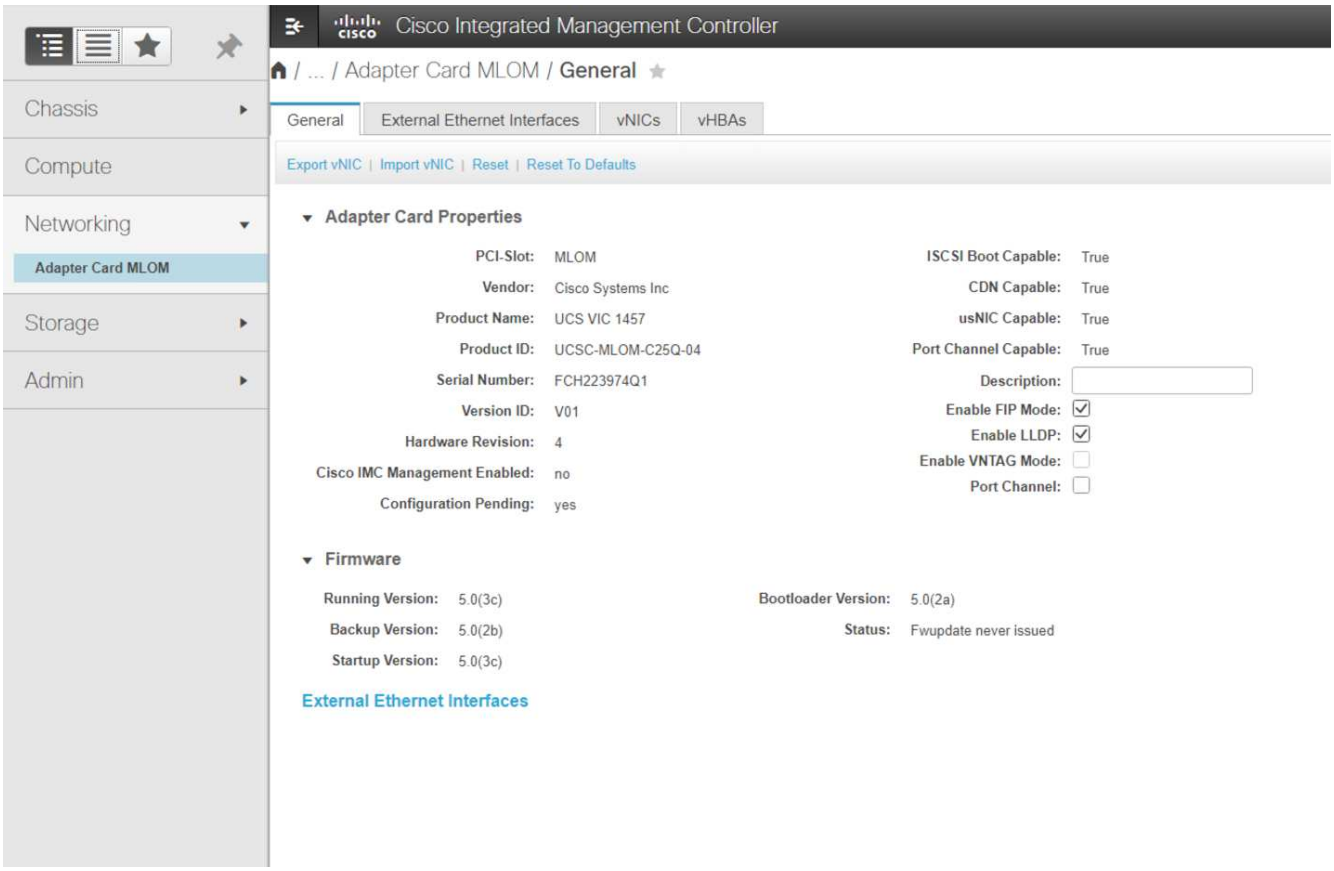


iSCSI ブート用に **Cisco VIC1457** を設定します

次の設定手順は、 Cisco VIC 1457 で iSCSI ブートを使用する場合の手順です。

> ポート 0 、 1 、 2 、および 3 間のデフォルトのポートチャネリングをオフにしてから、 4 つの個別ポートを設定する必要があります。ポートチャネリングがオフになっていない場合、 VIC 1457 には 2 つのポートのみが表示されます。CIMC でポートチャネルを有効にするには、次の手順を実行します。

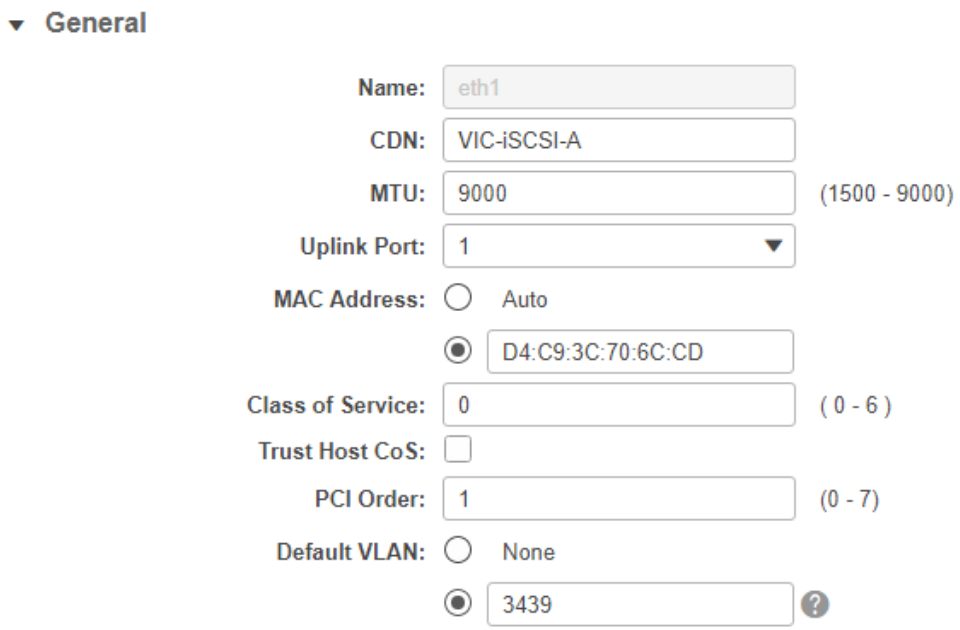
1. [ネットワーク] タブで、 [Adapter Card mLOM] をクリックします。
2. General タブで、ポートチャネルのチェックを外します。
3. 変更を保存し、 CIMC をリブートします。



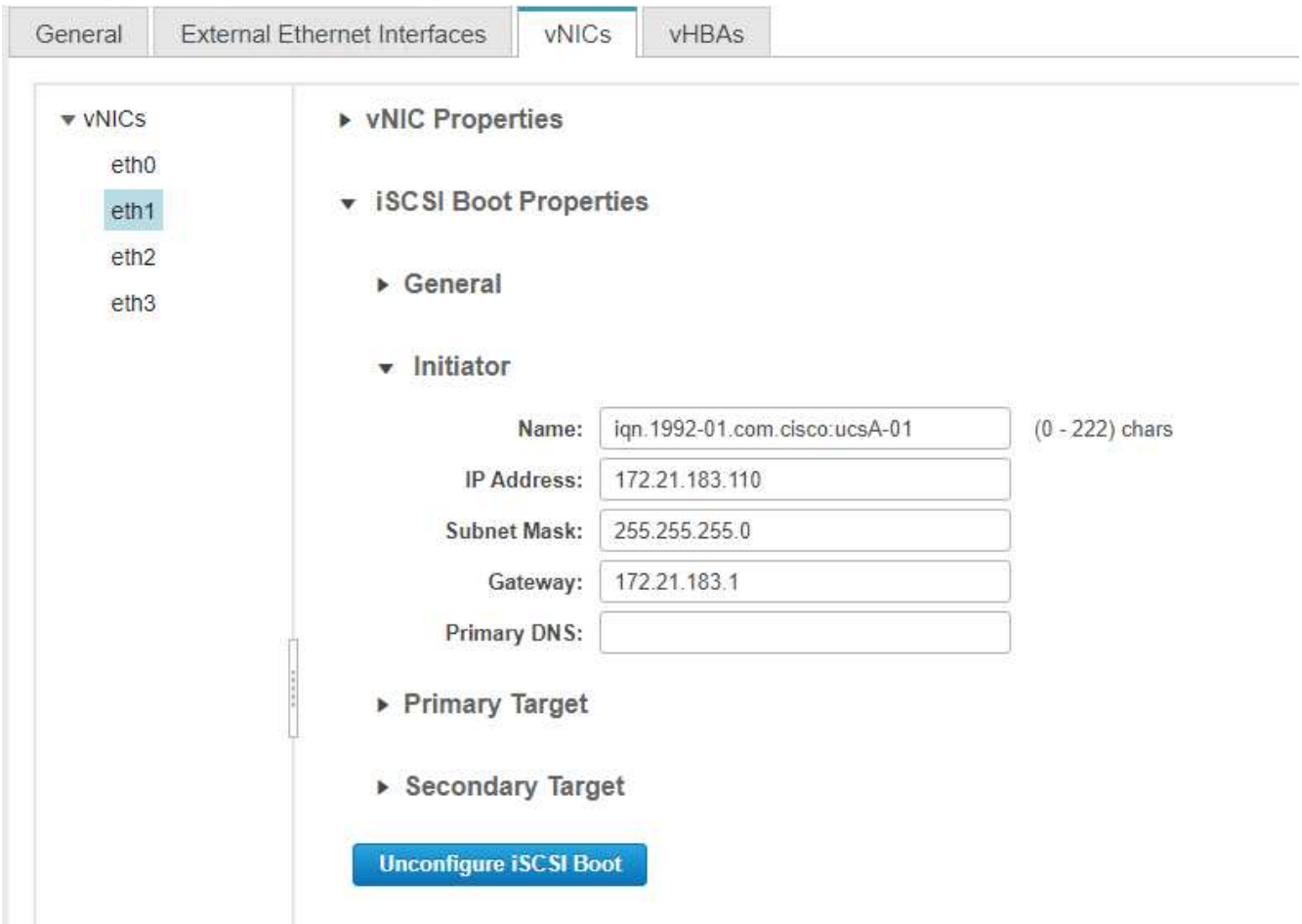
iSCSI vNIC を作成します

iSCSI vNIC を作成するには、次の手順を実行します。

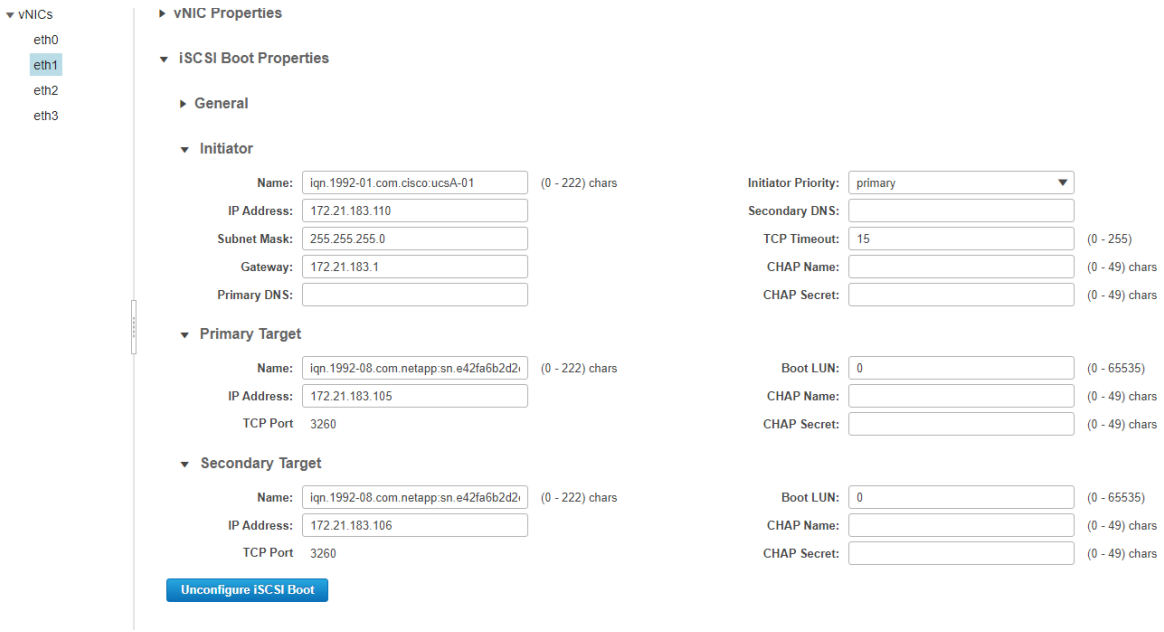
1. [ネットワーク] タブで、 [Adapter Card mLOM] をクリックします。
2. [Add vNIC] をクリックして vNIC を作成します。
3. [Add vNIC] セクションで、次の設定を入力します。
   - 名前： eth1
   - CDN 名： iscsi-vNIC-A
   - MTU ： 9000
   - デフォルト VLAN ： `\<<var_iscsi_vlan_a>`
   - VLAN モード：トランク
   - Enable PXE boot: チェック
4. [Add vNIC] をクリックし、 [OK] をクリックします。
5. このプロセスを繰り返して、 2 番目の vNIC を追加します。
   - vNIC eth3 に名前を付けます。
   - CDN 名： iscsi-vNIC-B
   - VLAN として「 <<var_iscsi_vlan_b>> 」と入力します。
   - アップリンクポートを 3 に設定します。



6. 左側の vNIC eth1 を選択します。



7. iSCSI Boot Properties （ iSCSI 起動プロパティ）で、イニシエータの詳細を入力します。
   - 名前 : \<<var_ucsa_initiator_name_a>
   - IP アドレス :`<<var_esxi_hosta_iscsia_ip>>
   - サブネットマスク : `<<var_esxi_hosta_iscsia_mask>>
   - ゲートウェイ :`<<var_esxi_hosta_iscsia_gateway>>



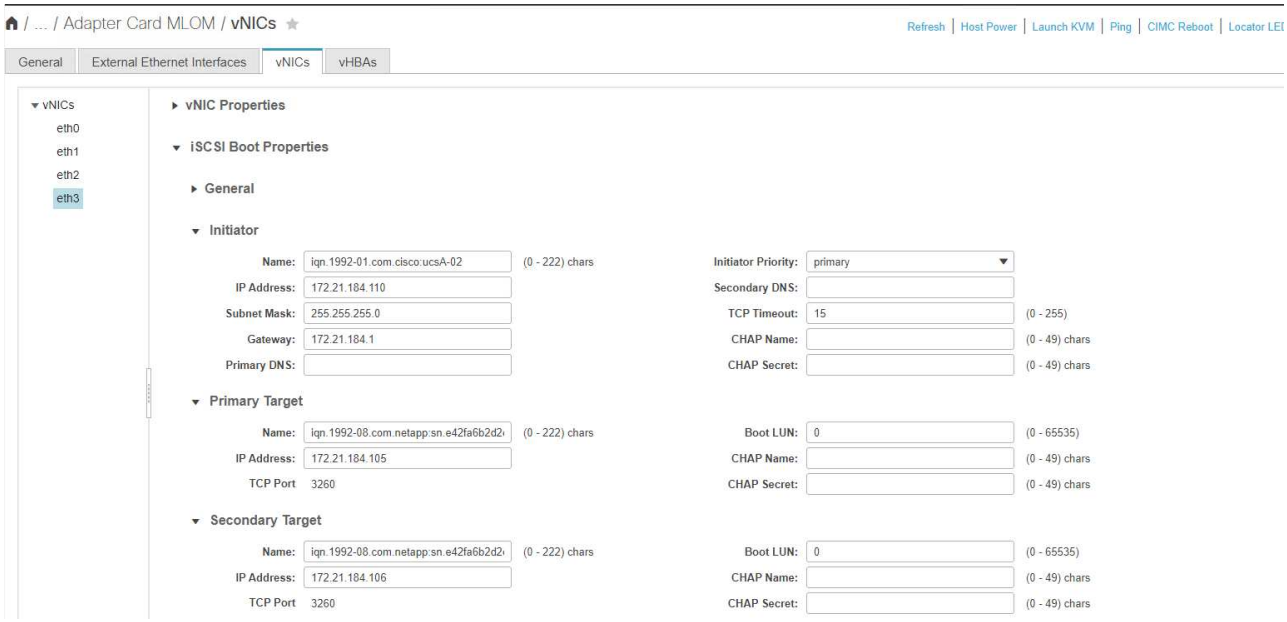
8. プライマリターゲットの詳細を入力します。
   - name ：インフラ SVM の IQN 番号
   - IP アドレス： iscsi_dlif01a の IP アドレス
   - ブート LUN ： 0
9. セカンダリターゲットの詳細を入力します。
   - name ：インフラ SVM の IQN 番号
   - IP アドレス： iSCSI_lif02a の IP アドレス
   - ブート LUN ： 0

> ストレージ IQN 番号を取得するには 'vserver iscsi show コマンドを実行します

> 各 vNIC の IQN 名を必ず記録してください。これらのファイルはあとで必要になります。さらに、イニシエータの IQN 名は、各サーバおよび iSCSI vNIC で一意である必要があります。

10. [Save Changes] をクリックします。
11. vNIC eth3 を選択し、 Host Ethernet Interfaces セクションの上部にある iSCSI Boot ボタンをクリックします。
12. 手順を繰り返して eth3 を設定します。

13. イニシエータの詳細を入力します。
    - 名前：`\<<var_ucsa_initiator_name_b>`
    - IP アドレス：`\<<var_esxi_HostB_iSCSIb_ip>`
    - サブネットマスク：`<<var_esxi_HostB_iSCSIb_mask>>
    - ゲートウェイ：`<<var_esxi_HostB_iSCSIb_gateway>>



14. プライマリターゲットの詳細を入力します。
    - name ：インフラ SVM の IQN 番号
    - IP アドレス： iscsi_dlif01b の IP アドレス
    - ブート LUN ： 0
15. セカンダリターゲットの詳細を入力します。
    - name ：インフラ SVM の IQN 番号
    - IP アドレス： iscsi_dlif02b の IP アドレス
    - ブート LUN ： 0

> ストレージ IQN 番号は、「 vserver iscsi show 」コマンドを使用して取得できます。

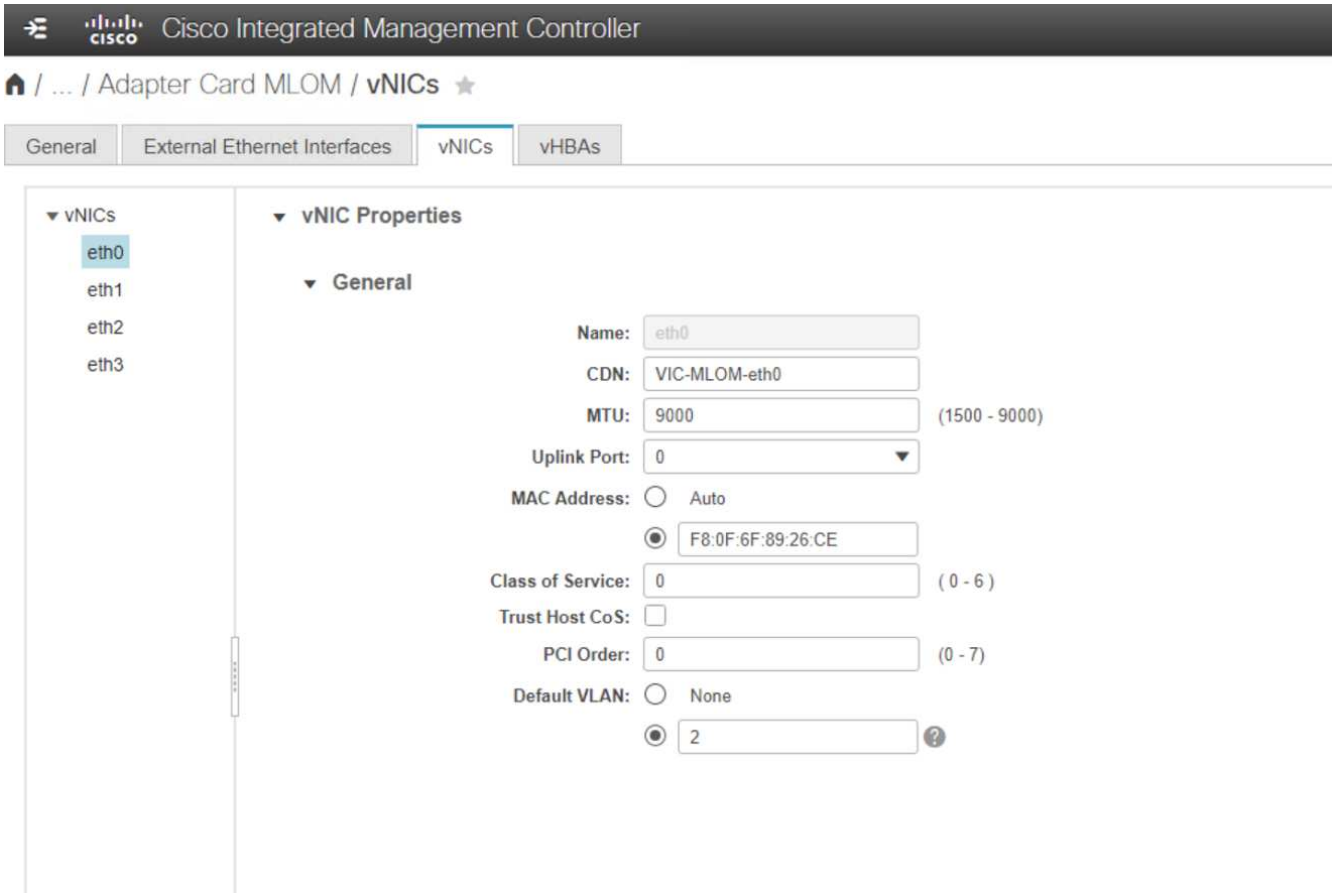
> 各 vNIC の IQN 名を必ず記録してください。これらのファイルはあとで必要になります。

16. [Save Changes] をクリックします。
17. このプロセスを繰り返して、 Cisco UCS サーバ B の iSCSI ブートを設定します

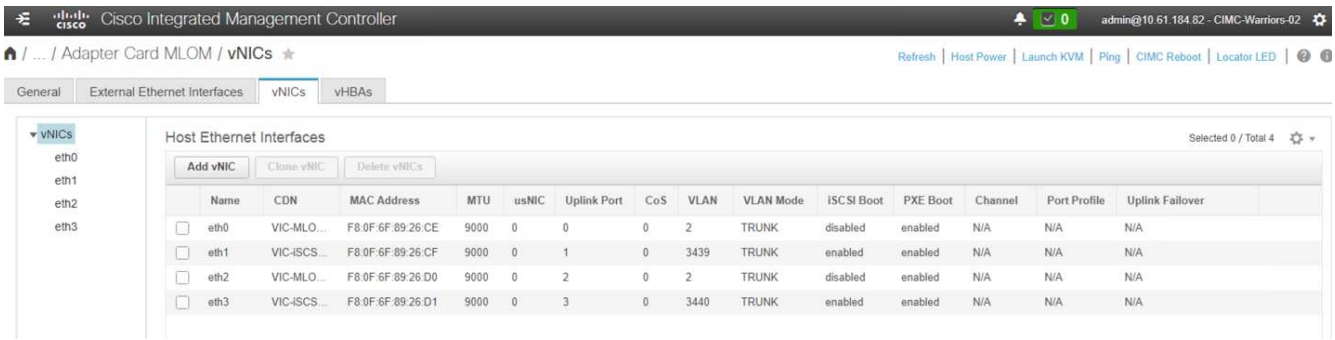
ESXi の vNIC を設定します

ESXi の vNIC を設定するには、次の手順を実行します。

1. CIMC インターフェイスブラウザウィンドウで、 [Inventory] をクリックし、右側のペインで [Cisco VIC adapters] をクリックします。
2. [Networking] > [Adapter Card mLOM] で [vNICs] タブを選択し、その下の vNIC を選択します。
3. eth0 を選択し、 Properties をクリックします。
4. MTU を 9000 に設定します。[Save Changes] をクリックします。
5. VLAN をネイティブ VLAN 2 に設定します。



6. eth1 に手順 3 と 4 を繰り返し、アップリンクポートが eth1 に 1 に設定されていることを確認します。



この手順は、最初の Cisco UCS サーバノードごと、および環境に追加する Cisco UCS サーバノードごとに繰り返す必要があります。

"次の記事：NetApp AFF ストレージ導入手順 （パート2）"

NetApp AFF ストレージ導入手順（パート 2 ）

ONTAP SAN ブートストレージをセットアップします

iSCSI igroup を作成します

この手順には、サーバ構成から iSCSI イニシエータの IQN が必要です。

igroup を作成するには、クラスタ管理ノードの SSH 接続から次のコマンドを実行します。この手順で作成した 3 つの igroup を表示するには、「 igroup show 」コマンドを実行します。

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-A -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-B -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

この手順は、 Cisco UCS C シリーズサーバを追加するときに実行する必要があります。

ブート LUN を igroup にマッピングします

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -igroup
VM-Host-Infra-A -lun-id 0
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -igroup
VM-Host-Infra-B -lun-id 0
```

この手順は、 Cisco UCS C シリーズサーバを追加するときに実行する必要があります。

"次の記事：VMware vSphere 6.7U2の導入手順"

VMware vSphere 6.7U2 導入手順

ここでは、 FlexPod Express 構成に VMware ESXi 6.7U2 をインストールする手順について説明します。以下に記載する導入手順は、前のセクションで説明した環境変数用にカスタマイズされたものです。

このような環境に VMware ESXi をインストールするには、複数の方法があります。この手順は、 Cisco UCS C シリーズサーバ用 CIMC インターフェイスの仮想 KVM コンソールと仮想メディア機能を使用して、リモートインストールメディアを個々のサーバにマッピングします。

この手順は、 Cisco UCS サーバ A および Cisco UCS サーバ B に対して実行する必要があります

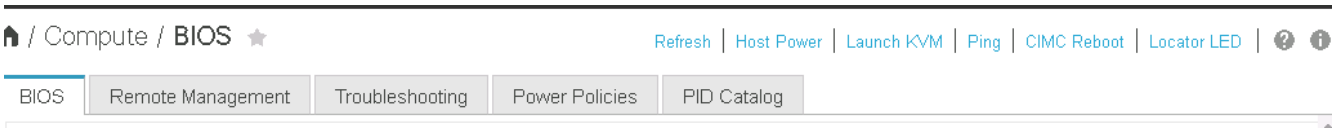
クラスタに追加するノードに対してこの手順を完了しておく必要があります。

Cisco UCS C シリーズスタンドアロンサーバの CIMC インターフェイスにログインします

以下に、 Cisco UCS C シリーズスタンドアロンサーバの CIMC インターフェイスにログインする手順について説明します。仮想 KVM を実行するには CIMC インターフェイスにログインする必要があります。これにより、管理者はリモートメディアを使用したオペレーティングシステムのインストールを開始できます。

すべてのホスト

1. Web ブラウザに移動し、 Cisco UCS C シリーズの CIMC インターフェイスの IP アドレスを入力します。この手順では CIMC GUI アプリケーションを起動します。
2. 管理ユーザ名とクレデンシャルを使用して、 CIMC UI にログインします。
3. メインメニューで、サーバータブを選択します。
4. Launch KVM Console をクリックします。



5. 仮想 KVM コンソールから、 [Virtual Media](仮想メディア) タブを選択します。
6. [CD/DVD のマップ] を選択します。

最初に [仮想デバイスのアクティブ化] をクリックする必要があります。プロンプトが表示されたら、 [このセッションを受け入れる] を選択

7. VMware ESXi 6.7U2 インストーラの ISO イメージファイルを参照して、 [開く] をクリックします。Map Device をクリックします。
8. 電源メニューを選択し、システムの電源再投入（コールドブート）を選択します。はいをクリックします。

VMware ESXi をインストールします

以下に、各ホストに VMware ESXi をインストールする手順について説明します。

ESXi 6.7U2 Cisco カスタムイメージをダウンロードします

1. に移動します "VMware vSphere のダウンロードページ" カスタム ISO の場合。
2. ESXi 6.7U2 Install CD の Cisco Custom Image の横にある Go to Downloads をクリックします。
3. ESXi 6.7U2 Install CD （ ISO ）用の Cisco Custom Image をダウンロードします。
4. システムが起動すると、 VMware ESXi インストールメディアがマシンによって検出されます。
5. 表示されるメニューから VMware ESXi インストーラを選択します。インストーラがロードされます。これには数分かかることがあります。
6. インストーラのロードが完了したら、 Enter キーを押してインストールを続行します。
7. エンドユーザライセンス契約を読んだ後、同意して F11 キーを押してインストールを続行します。

8. ESXi のインストールディスクとして設定した NetApp LUN を選択し、 Enter キーを押してインストールを続行します。

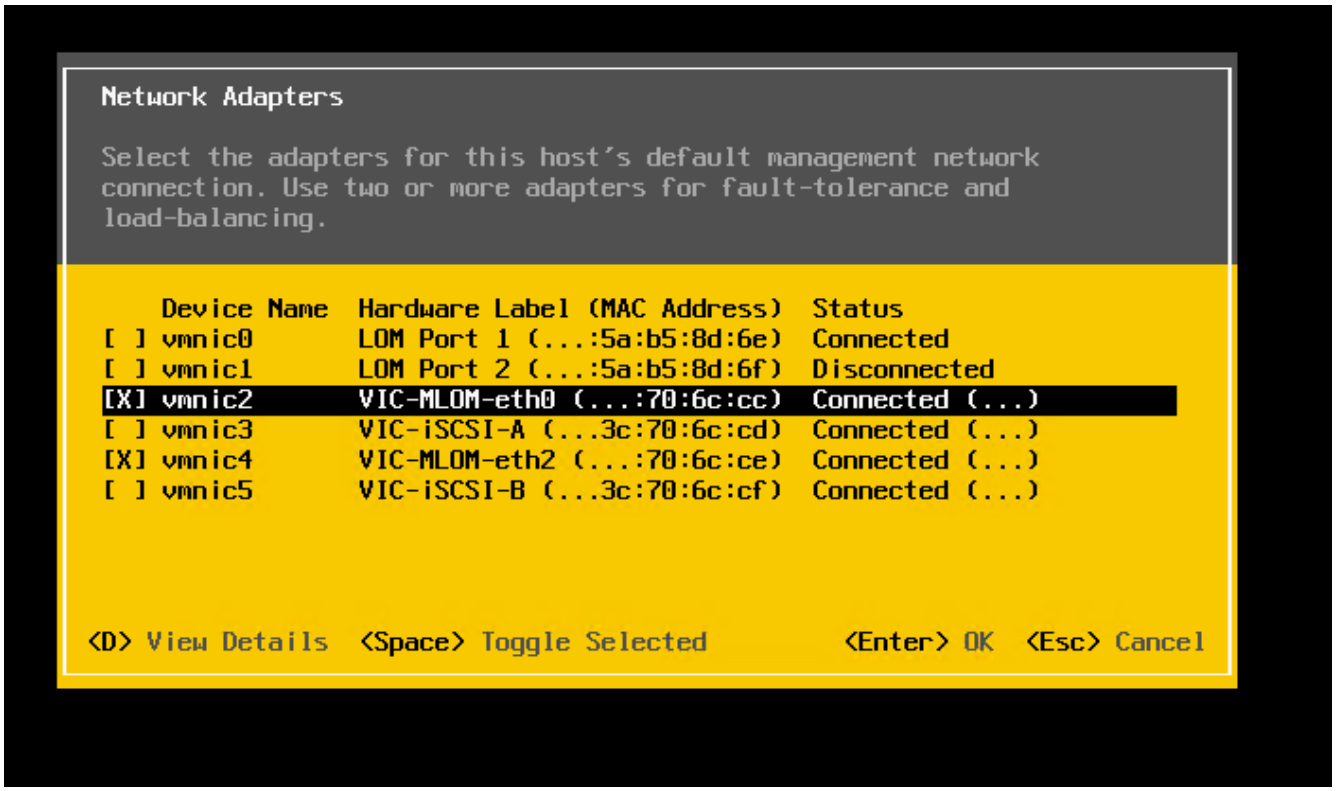
9. 適切なキーボードレイアウトを選択し、 Enter キーを押します。
10. ルートパスワードを入力して確定し、 Enter キーを押します。
11. 既存のパーティションがボリュームから削除されていることを示す警告が表示されます。F11 キーを押してインストールを続行します。ESXi のインストール後にサーバがリブートします。

VMware ESXi ホスト管理ネットワークをセットアップします

以下に、 VMware ESXi ホストごとに管理ネットワークを追加する手順について説明します。

すべてのホスト

1. サーバのリブートが完了したら、 F2 キーを押してシステムをカスタマイズするオプションを入力します。
2. インストールプロセスで入力したログイン名と root パスワードを使用してログインします。
3. Configure Management Network （管理ネットワークの設定）オプションを選択します。
4. [ネットワークアダプタ] を選択し、 Enter キーを押します。
5. vSwitch0 に使用するポートを選択します。Enter キーを押します。
6. CIMC の eth0 および eth1 に対応するポートを選択します。



7. VLAN （オプション）を選択し、 Enter キーを押します。
8. VLAN ID 「 \<mgmt_vlan_id>` 」を入力します。Enter キーを押します。
9. Configure Management Network （管理ネットワークの設定）メニューから、 IPv4 Configuration （ IPv4 設定）を選択して管理インターフェイスの IP アドレスを設定します。Enter キーを押します。
10. 矢印キーを使用して [Set Static IPv4 Address] をハイライトし、スペースバーを使用してこのオプションを選択します。
11. VMware ESXi ホスト「 \<ESXi_host_mgmt_ip>> 」を管理するための IP アドレスを入力します。
12. VMware ESXi ホスト「 \ <ESXi_host_mgmt_netmask>> 」のサブネットマスクを入力します。
13. VMware ESXi ホスト「 \<ESXi_host_mgmt_gateway>` 」のデフォルトゲートウェイを入力します。
14. Enter キーを押して、 IP 設定の変更を確定します。
15. IPv6 設定メニューを表示します。
16. IPv6 を有効にする（再起動が必要）オプションを選択解除して IPv6 を無効にするには、スペースバーを使用します。Enter キーを押します。
17. DNS 設定を指定するメニューを表示します。
18. IP アドレスは手動で割り当てられるため、 DNS 情報も手動で入力する必要があります。
19. プライマリ DNS サーバの IP アドレス「 \ <nameserver_ip>` 」を入力します。
20. （任意）セカンダリ DNS サーバの IP アドレスを入力します。
21. VMware ESXi ホスト名の FQDN として、「 \ <ESXi_host_fqdn>> 」を入力します。
22. Enter キーを押して、 DNS 設定の変更を確定します。
23. Esc キーを押して、管理ネットワークの設定サブメニューを終了します。

24. Y キーを押して変更を確定し、サーバーを再起動します。
25. トラブルシューティングオプションを選択し、 ESXi シェルと SSH を有効にします。

> これらのトラブルシューティングオプションは、お客様のセキュリティポリシーに従って検証後に無効にすることができます。

26. メインコンソール画面に戻るには、 Esc キーを 2 回押します。
27. 画面上部の CIMC マクロ > 静的マクロ > Alt-F ドロップダウンメニューから Alt-F1 をクリックします。
28. ESXi ホストの適切なクレデンシャルを使用してログインします。
29. プロンプトで、次の esxcli コマンドのリストを順次入力してネットワーク接続を有効にします。

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

ESXi ホストを設定

次の表の情報を使用して、各 ESXi ホストを設定します。

詳細（ **Detail** ）	詳細値
ESXi ホスト名	\<ESXi_host_fqdn>> のように指定します
ESXi ホスト管理 IP	\<ESXi_host_mgmt_IP>
ESXi ホスト管理マスク	\<ESXi_host_mgmt_netmask>>
ESXi ホスト管理ゲートウェイ	\<ESXi_host_mgmt_gateway>>
ESXi ホストの NFS IP	\ <ESXi_host_nfs_ip>>
ESXi ホストの NFS マスク	\ <ESXi_host_nfs_netmask>> の順にクリックします
ESXi ホストの NFS ゲートウェイ	\<ESXi_host_nfs_gateway>>
ESXi ホスト vMotion IP	\<ESXi_host_vMotion_IP> です
ESXi ホストの vMotion マスク	\<ESXi_host_vMotion_netmask>>
ESXi ホストの vMotion ゲートウェイ	\ <ESXi_host_vMotion_gateway>> の順に選択します
ESXi ホスト iSCSI-A IP	\<ESXi_host_iscsi-a_IP> です
ESXi ホスト iSCSI-A マスク	\ <ESXi_host_iscsi-A netmask >> の順にクリックします
ESXi ホスト iSCSI-A ゲートウェイ	\<ESXi_host_iscsi-a_gateway>>
ESXi ホスト iSCSI-B IP	\<ESXi_host_iscsi-B_IP> です
ESXi ホスト iSCSI-B マスク	\<ESXi_host_iscsi-B_netmask>>
ESXi ホスト iSCSI-B ゲートウェイ	\<ESXi_host_scs-b_gateway>>

ESXi ホストにログインします

ESXi ホストにログインするには、次の手順を実行します。

1. Web ブラウザでホストの管理 IP アドレスを開きます。
2. root アカウントとインストールプロセスで指定したパスワードを使用して、 ESXi ホストにログインします。
3. VMware Customer Experience Improvement Program に関する声明をお読みください。適切な応答を選択したら、 [OK] をクリックします。

iSCSI ブートを設定します

iSCSI ブートを設定するには、次の手順を実行します。

1. 左側の [ネットワーク] を選択します。
2. 右側の [Virtual Switches] タブを選択します。

3. iScsiBootvSwitch をクリックします。
4. [設定の編集] を選択します
5. MTU を 9000 に変更し、 [保存] をクリックします。
6. iSCSIBootPG ポートの名前を iSCSIBootPG-A に変更します

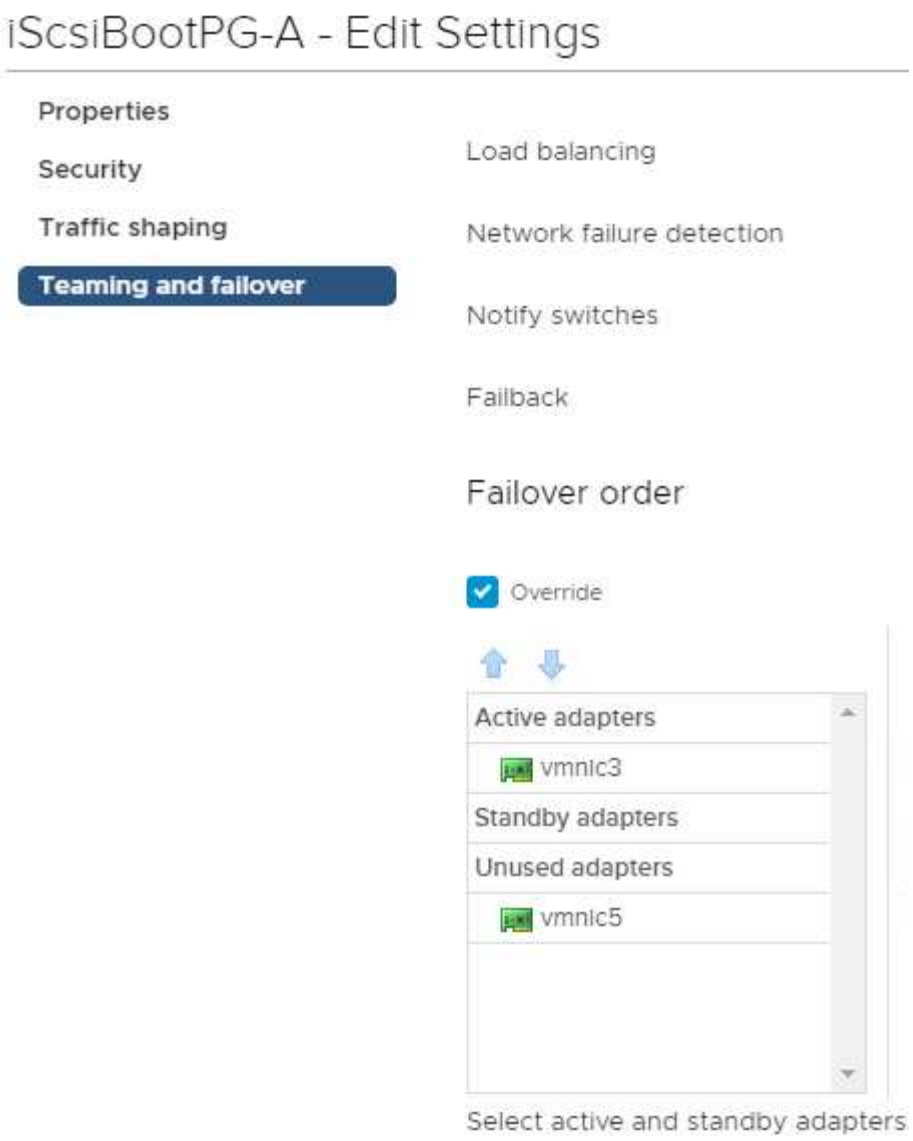
> この構成では、 vmnic3 と vmnic5 が iSCSI ブートに使用されます。ESXi ホストに NIC がほかにもある場合は、 vmnic 番号が異なることがあります。iSCSI ブートに使用されている NIC を確認するには、 CIMC の iSCSI vNIC 上の MAC アドレスを ESXi の vmnic に照合します。

7. 中央のペインで、 [VMkernel NICs] タブを選択します。
8. Add VMkernel NIC を選択します。

a. 新しいポートグループ名として、 iScsiBootPG-B を指定します
b. 仮想スイッチの iScsiBootvSwitch を選択します。
c. VLAN ID に「 \<iSCSIb_vlan_id>` 」と入力します。
d. MTU を 9000 に変更します。
e. IPv4 設定を展開します。
f. 静的設定を選択します。
g. アドレスとして「 \\<var_hosta_iSCSIb_ip>> 」と入力します。
h. Subnet Mask には「 \<<var_hosta_iSCSIb_mask>> 」と入力します。
i. Create をクリックします。 .

> iScsiBootPG-A で MTU を 9000 に設定します

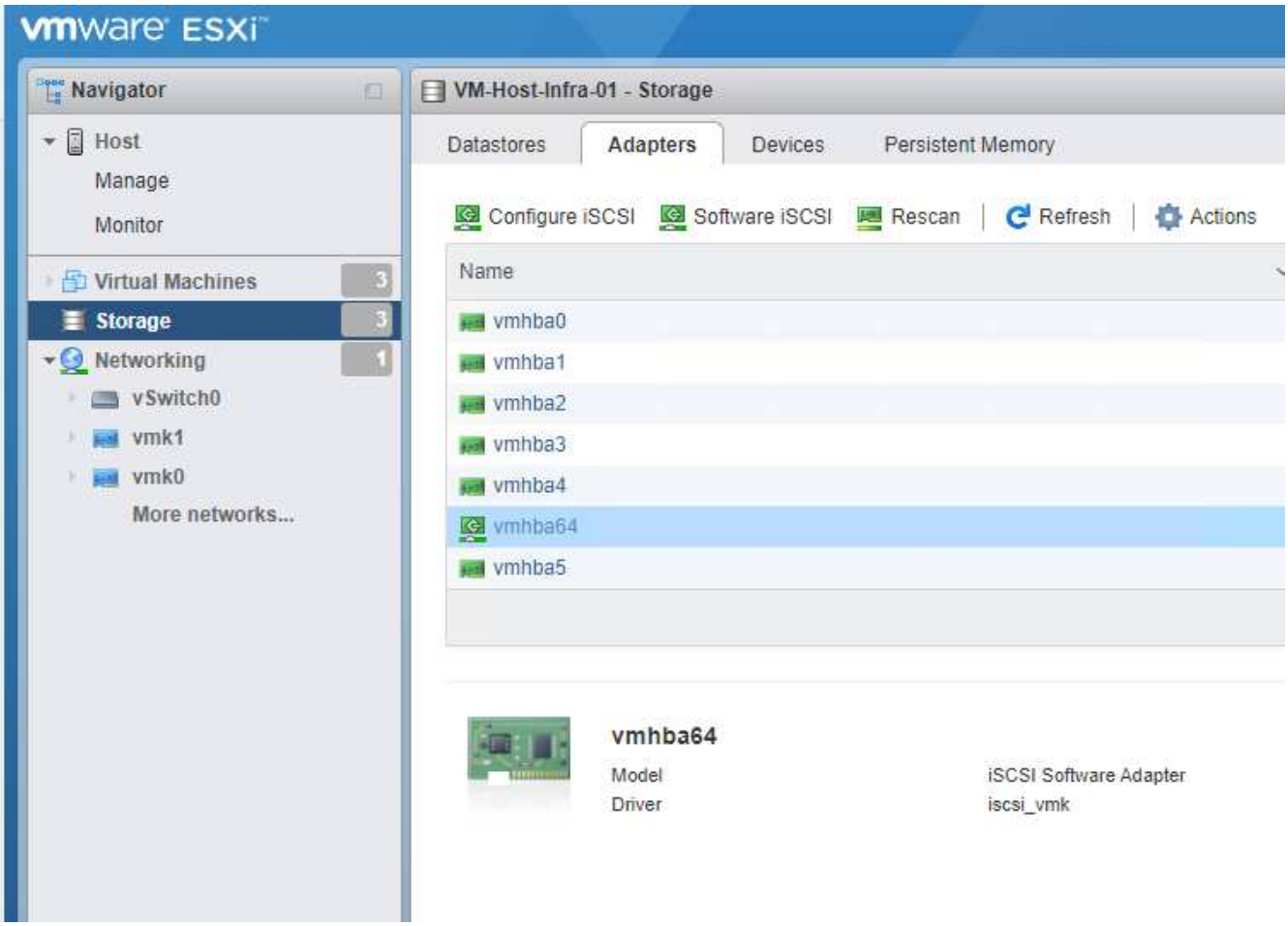
9. フェイルオーバーを設定するには、次の手順を実行します。
   a. iSCSIBootPG の設定の編集 - A > 階層化とフェイルオーバー > フェイルオーバー順序 > vmnic3 をクリックします。vmnic3 がアクティブで、 vmnic5 が未使用である。
   b. iSCSIBootPG-B で設定の編集 > チーム化とフェイルオーバー > フェイルオーバー順序 > vmnic5 をクリックします。vmnic5 がアクティブで、 vmnic3 が未使用である。



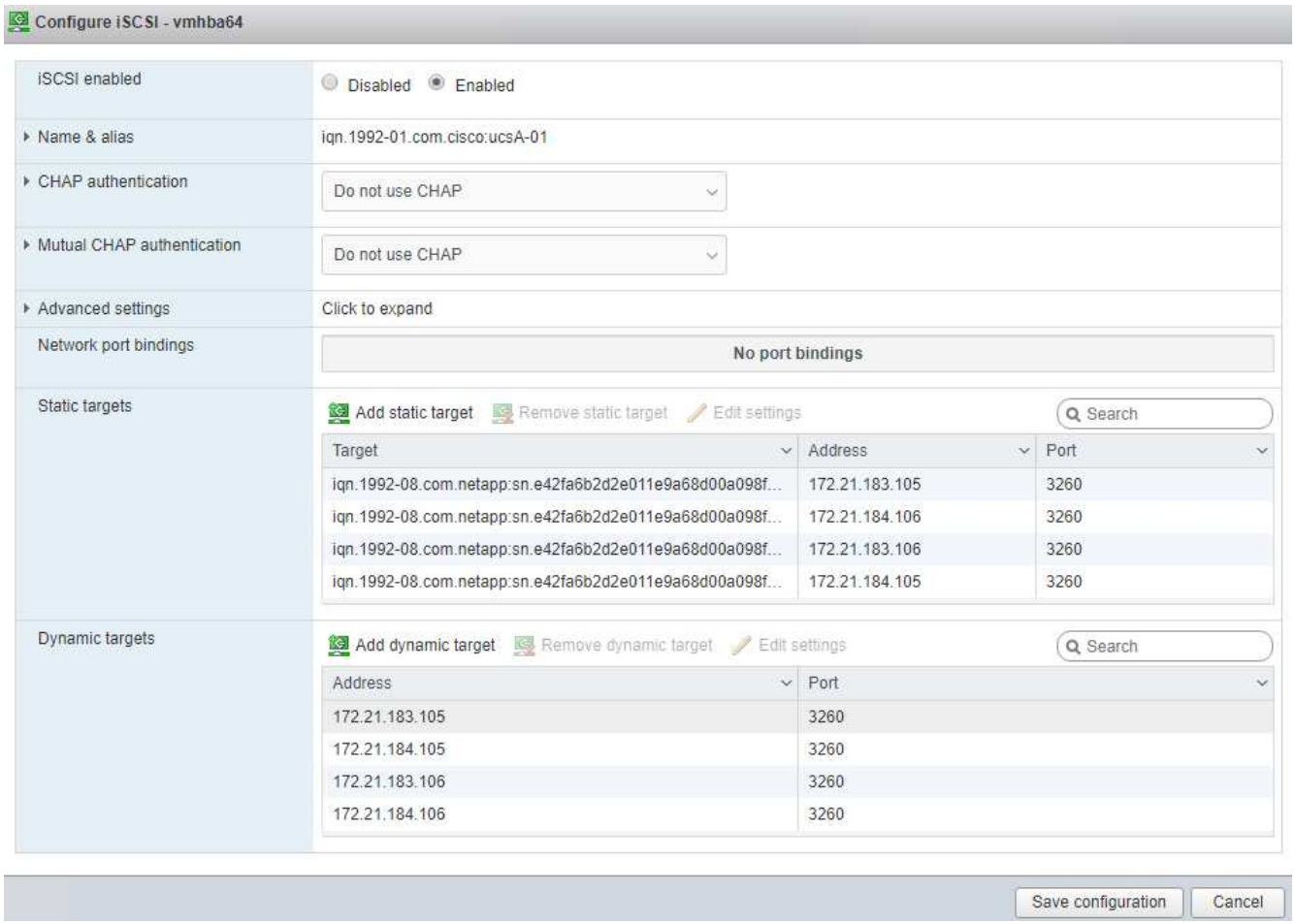
iSCSI マルチパスを設定します

ESXi ホストで iSCSI マルチパスを設定するには、次の手順を実行します。

1. 左側のナビゲーションペインで Storage （ストレージ）を選択します。アダプタをクリックします。
2. iSCSI ソフトウェアアダプタを選択し、 Configure iSCSI （ iSCSI の設定）をクリックします。



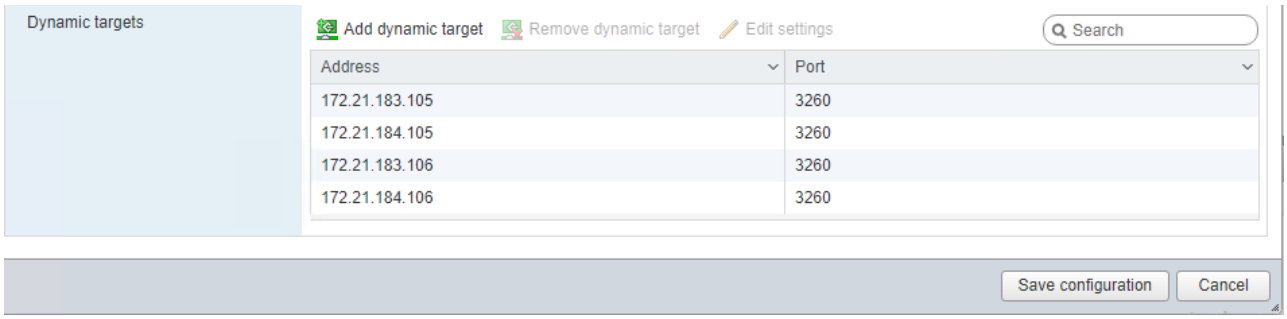
3. [動的ターゲット] で、 [動的ターゲットの追加] をクリックします。



4. IP アドレス「 iscsi_dlif01a 」を入力します。

   a. IP アドレス 'iSCSI_lif01b'iSCSI_lif02a'iSCSI_lif02b' で繰り返します

   b. [Save Configuration] をクリックします。



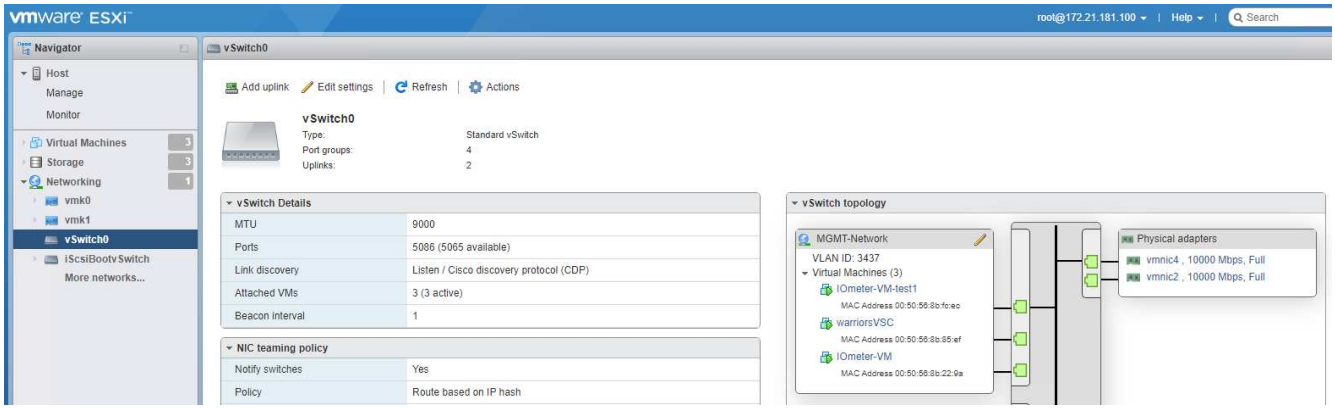
> iSCSI LIF の IP アドレスは、ネットアップクラスタで network interface show コマンドを実行するか、 System Manager の Network Interfaces タブで確認できます。

ESXi ホストを設定

ESXi ブートを設定するには、次の手順を実行します。

1. 左側のナビゲーションペインで、 [ネットワーク] を選択します。

2. vSwitch0 を選択します。



3. 設定の編集を選択します。
4. MTU を 9000 に変更します。
5. NIC チーミングを展開し、 vmnic2 と vmnic4 の両方がアクティブに設定され、 NIC チーミングとフェイルオーバーが IP ハッシュに基づいてルートに設定されていることを確認します。

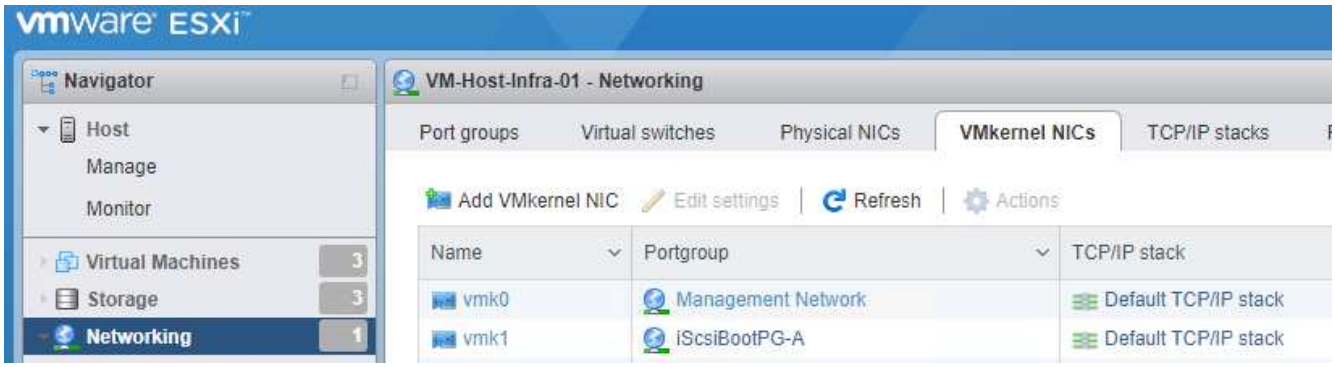
> ロードバランシングの IP ハッシュ方式では、スタティック（モードオン）ポートチャネルで SRC-DST-IP EtherChannel を使用して、基盤となる物理スイッチを適切に設定する必要があります。スイッチの設定ミスが原因で接続が断続的に発生する可能性があります。その場合は、ポートチャネル設定のトラブルシューティング中に、 Cisco スイッチに関連付けられている 2 つのアップリンクポートのいずれかを一時的にシャットダウンして ESXi 管理 vmkernel ポートへの通信をリストアします。

ポートグループと **VMkernel NIC** を設定します

ポートグループと VMkernel NIC を設定するには、次の手順を実行します。

1. 左側のナビゲーションペインで、 [ネットワーク] を選択します。
2. Port Groups タブを右クリックします。

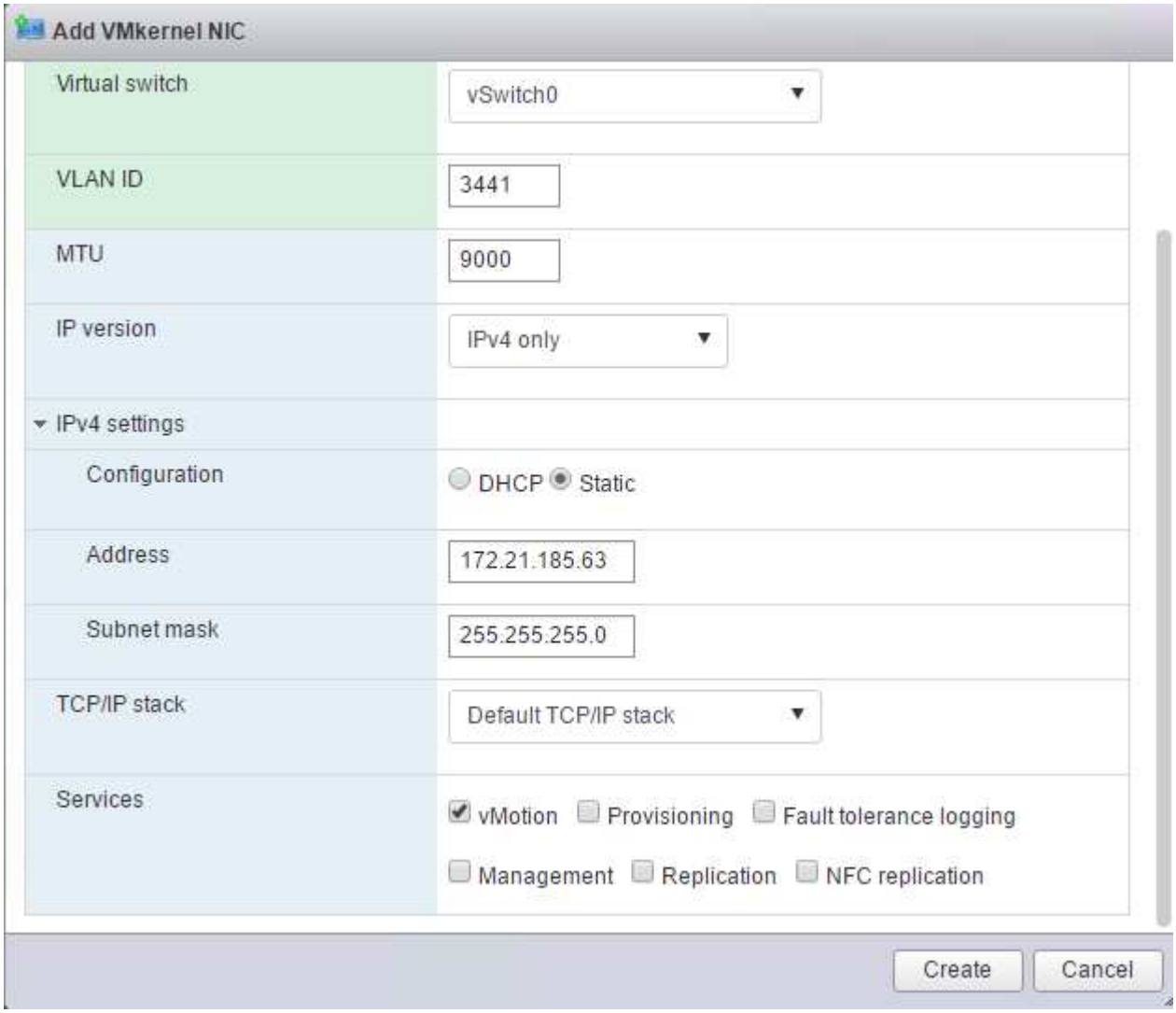
3. [VM Network] を右クリックし、 [Edit] を選択します。VLAN ID を「 <<var_vm_traffic_vlan>> 」に変更します。
4. [Add Port Group] をクリックします。
   a. ポートグループに MGMT-Network という名前を付けます。
   b. VLAN ID に「 \ <mgmt_vlan>> 」と入力します。
   c. vSwitch0 が選択されていることを確認してください。
   d. [保存] をクリックします .
5. [VMkernel NICs] タブをクリックします。



6. Add VMkernel NIC を選択します。
   a. [新しいポートグループ] を選択します。
   b. ポートグループに「 NFS-Network 」という名前を付けます。
   c. VLAN ID として「 \<nfs_vlan_id>` 」と入力します。
   d. MTU を 9000 に変更します。
   e. IPv4 設定を展開します。
   f. 静的設定を選択します。
   g. アドレスとして「 \<<var_hosta_nfs_ip>> 」と入力します。
   h. [サブネットマスク] に「 \<<var_hosta_nfs_mask>> 」と入力します。
   i. Create をクリックします。 .
7. この手順を繰り返して、 vMotion VMkernel ポートを作成します。
8. Add VMkernel NIC を選択します。
   a. [新しいポートグループ] を選択します。
   b. ポートグループに vMotion という名前を付けます。
   c. VLAN ID に「 \<VMotion_vlan_id>> 」と入力します。
   d. MTU を 9000 に変更します。
   e. IPv4 設定を展開します。
   f. 静的設定を選択します。
   g. アドレスとして「 <<var_hosta_VMotion_ip>> 」と入力します。

h. Subnet Mask には「 \<<var_hosta_vMotion mask>> 」と入力します。

i. IPv4 の設定後に vMotion チェックボックスが選択されていることを確認します。

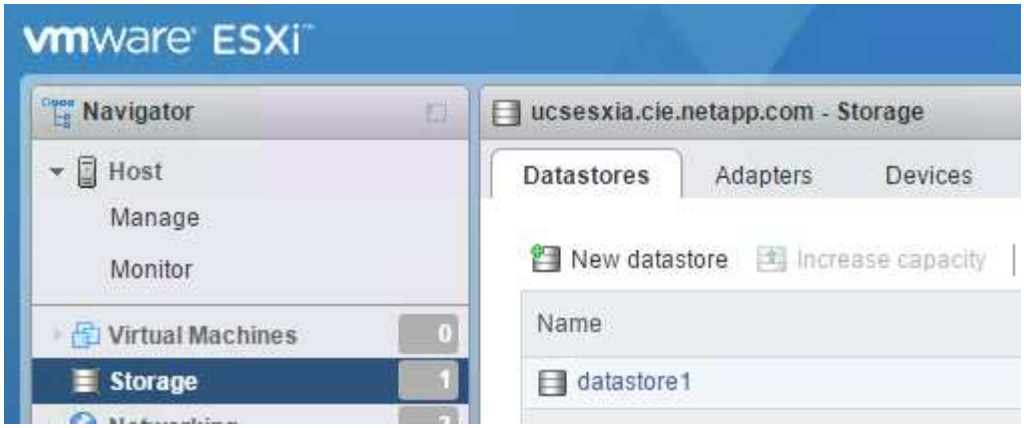


ESXi ネットワークの設定には、ライセンスで許可されている場合に VMware vSphere Distributed Switch を使用するなどの方法が多数あります。ビジネス要件を満たす必要がある場合は、 FlexPod Express で代替ネットワーク構成がサポートされます。

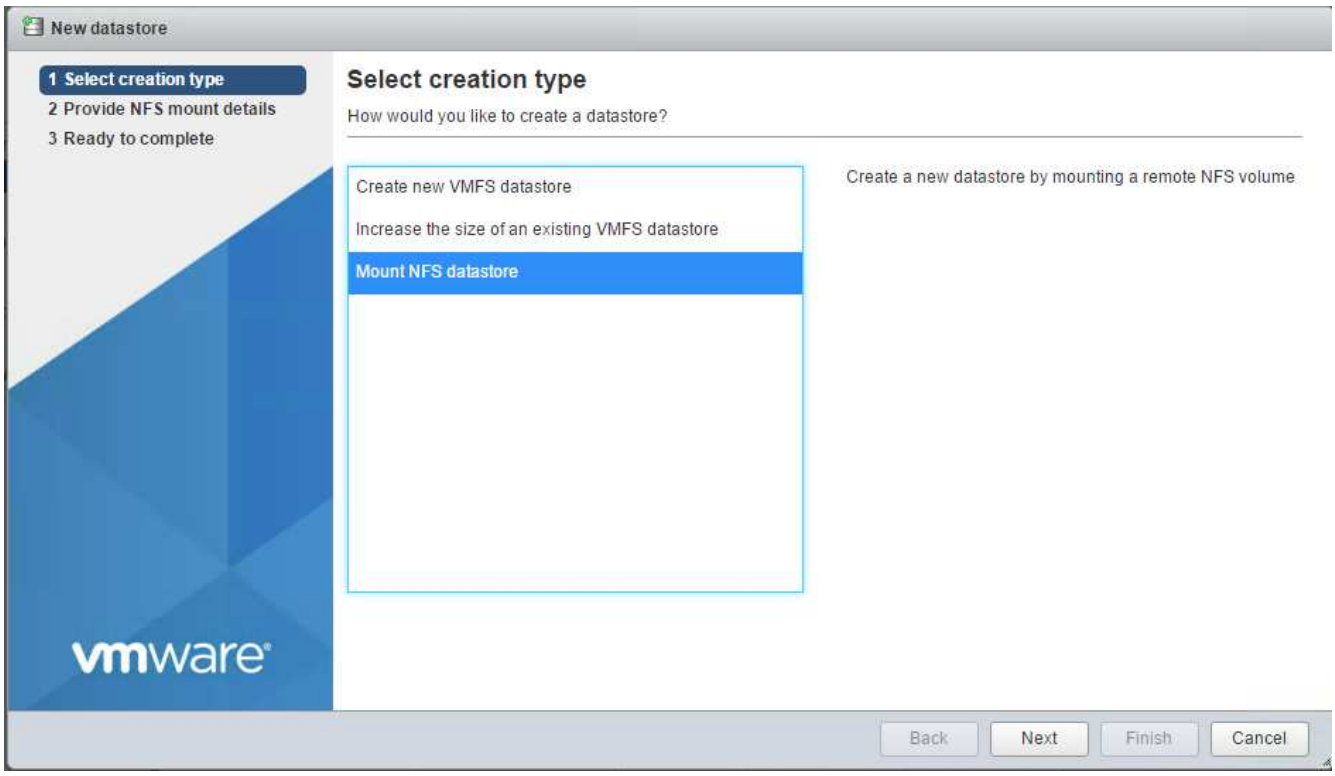
最初のデータストアをマウント

最初にマウントされるデータストアは 'infra_datastore.vm のデータストアと 'infra_swap データストアであり 'VM スワップファイル用です

1. 左側のナビゲーションペインで [ストレージ] をクリックし、 [新しいデータストア] をクリックします。



2. マウント NFS データストアを選択します。



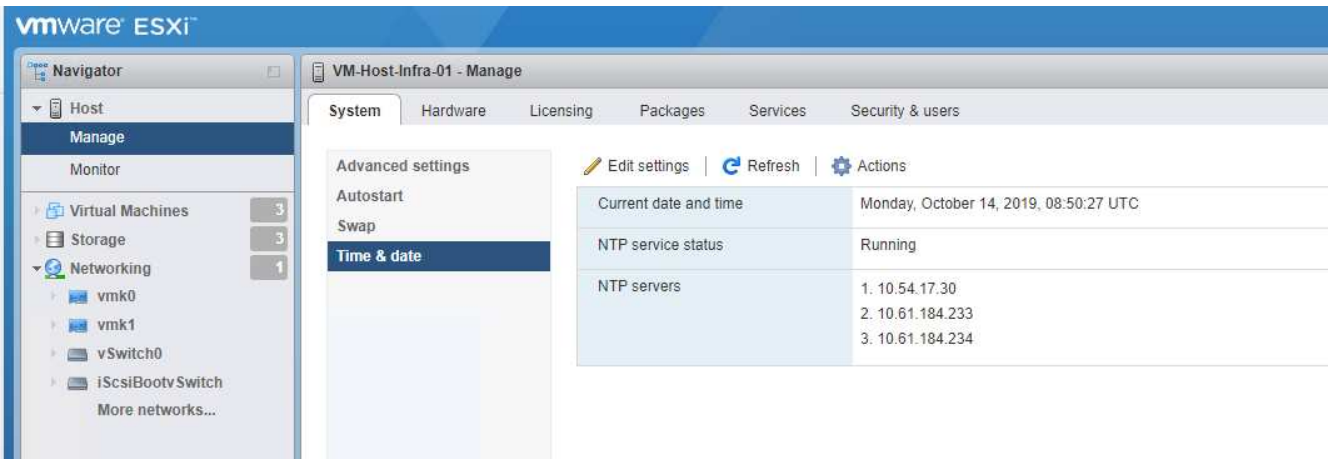
3. Provide NFS Mount Details （ NFS マウントの詳細の提供）ページに次の情報を入力します。
   - 名前： 'infra_datastore.
   - NFS サーバ : `\<<var_nodeA_nfs_lif>`
   - 共有 : 「 /infra_datastore 」
   - NFS 3 が選択されていることを確認します。
4. 完了をクリックします。[最近のタスク] ペインにタスクの完了が表示されます。
5. この手順を繰り返して 'infra_swap' データストアをマウントします
   - 名前： infra_swap
   - NFS サーバ : `\<<var_nodeA_nfs_lif>`
   - 共有 :`/infra_swap

◦ NFS 3 が選択されていることを確認します。

NTP を設定します

ESXi ホストの NTP を設定するには、次の手順を実行します。

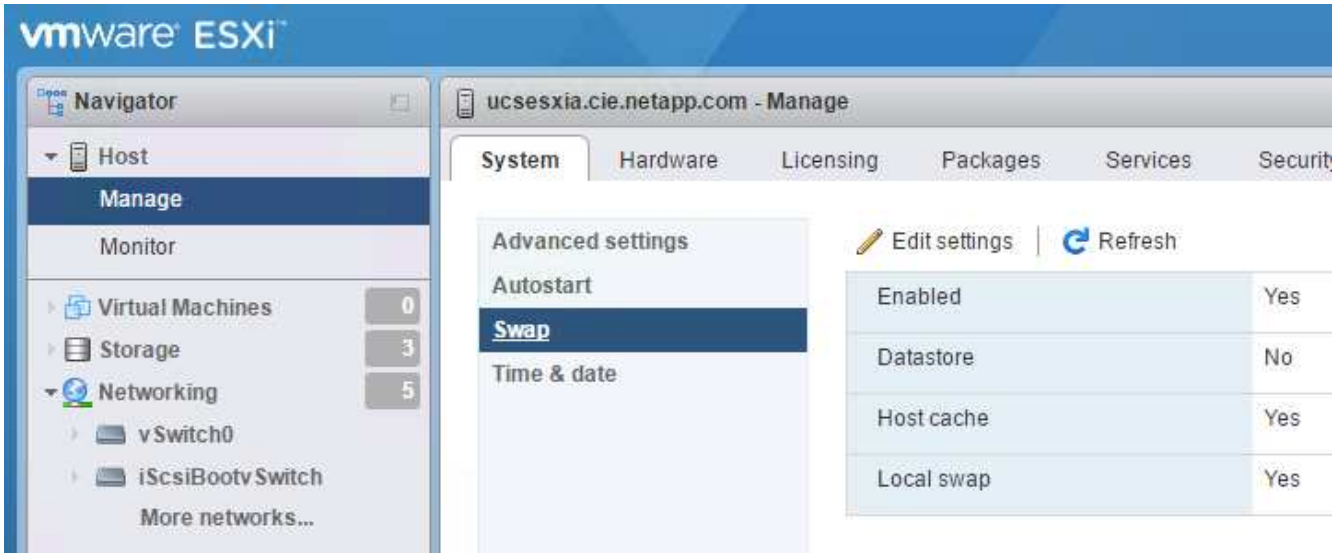
1. 左側のナビゲーションペインで、 [管理] をクリックします。右側のペインで [システム] を選択し、 [時刻と日付] をクリックします。
2. Use Network Time Protocol （ NTP クライアントを有効にする）を選択します。
3. NTP サービスのスタートアップポリシーとして、 Start and Stop With Host を選択します。
4. NTP サーバとして「 <<var_ntp>> 」と入力します。複数の NTP サーバを設定できます。
5. [保存] をクリックします .



VM スワップファイルの場所を移動します

以下に、 VM スワップファイルの場所を移動する手順について説明します。

1. 左側のナビゲーションペインで、 [管理] をクリックします。右側のペインでシステムを選択し、スワップをクリックします。



2. 設定の編集をクリックします。データストアのオプションから 'infra_swap' を選択します

3. [保存] をクリックします .

"次の記事：VMware vCenter Server 6.7U2のインストール手順"

VMware vCenter Server 6.7U2 のインストール手順

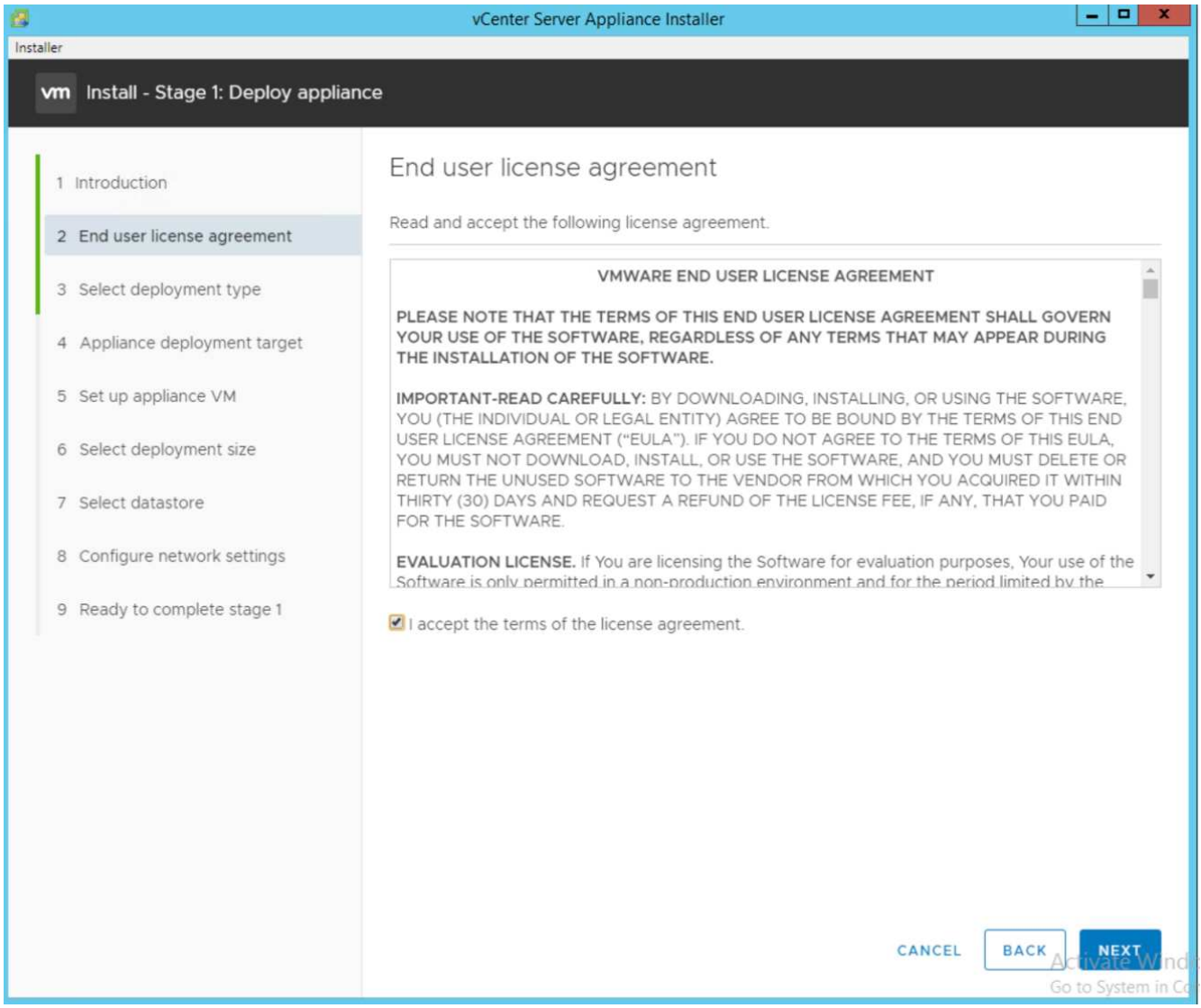
このセクションでは、 FlexPod 構成に VMware vCenter Server 6.7 をインストールする詳細な手順について説明します。

FlexPod Express では、 VMware vCenter Server Appliance （ VCSA ）を使用します。

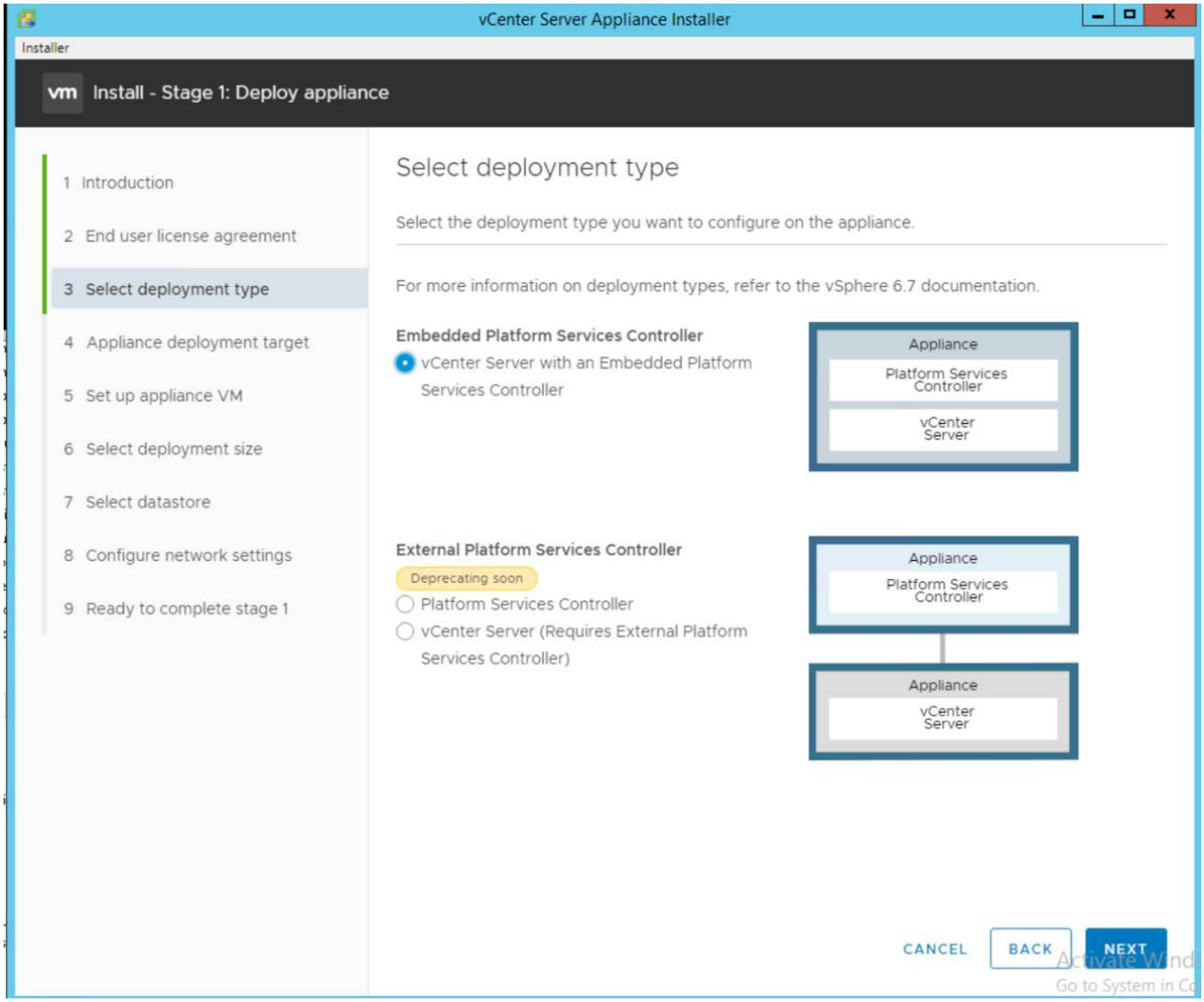
VMware vCenter Server Appliance をダウンロードします

VMware vCenter Server Appliance （ VCSA ）をダウンロードするには、次の手順を実行します。

1. vCSA をダウンロードします。ESXi ホストの管理時に Get vCenter Server アイコンをクリックして、ダウンロードリンクにアクセスします。
2. vCSA を VMware サイトからダウンロードします。
3. インストール可能な Microsoft Windows vCenter Server がサポートされますが、 VMware では新しい導入に vCSA を推奨します。
4. ISO イメージをマウントします。
5. VCSA -ui-installer > win32 ディレクトリに移動します。「 installer.exe 」をダブルクリックします。
6. [インストール] をクリックします
7. [はじめに] ページで [次へ] をクリックします。

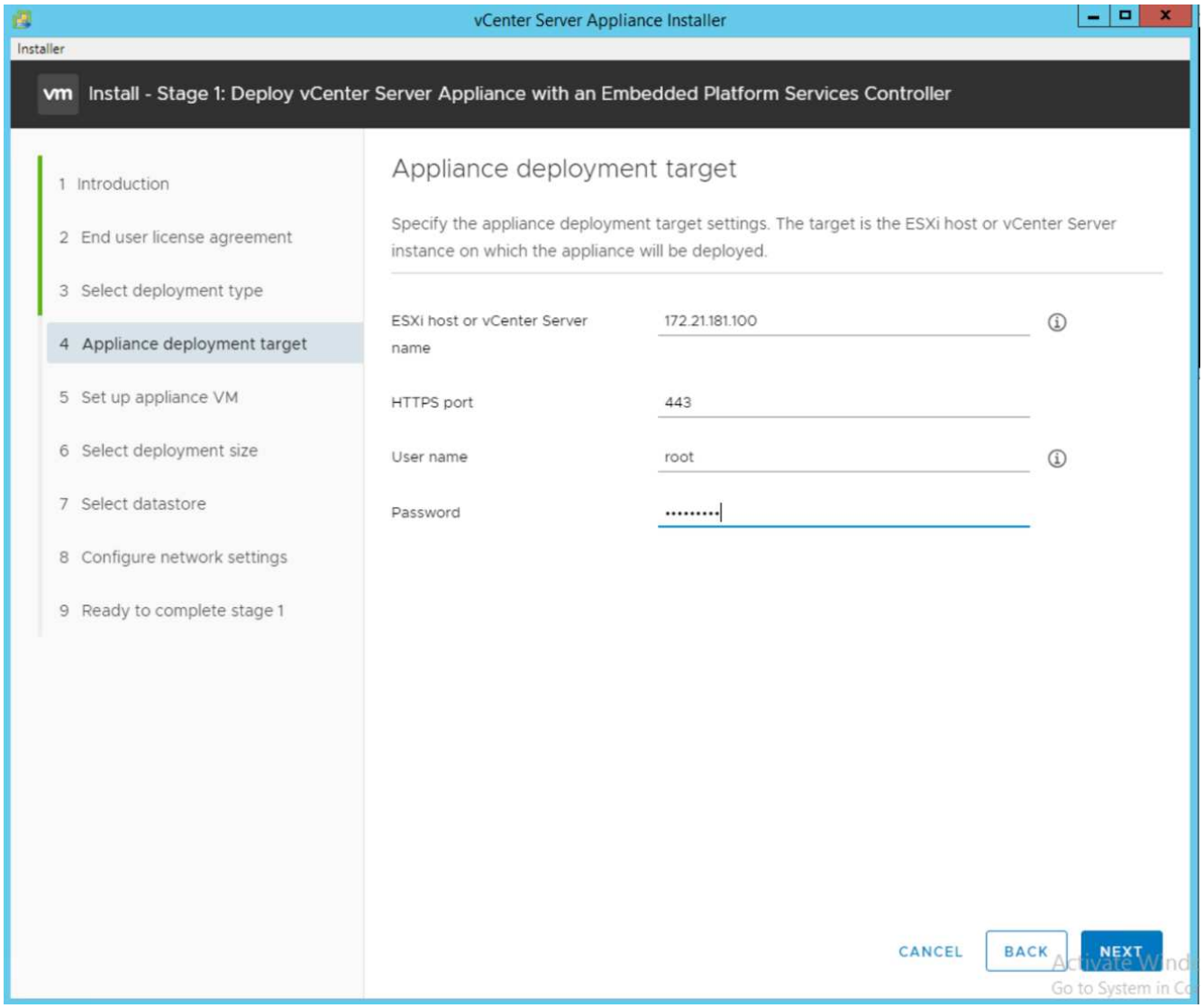


8. 展開タイプとして、 Embedded Platform Services Controller を選択します。

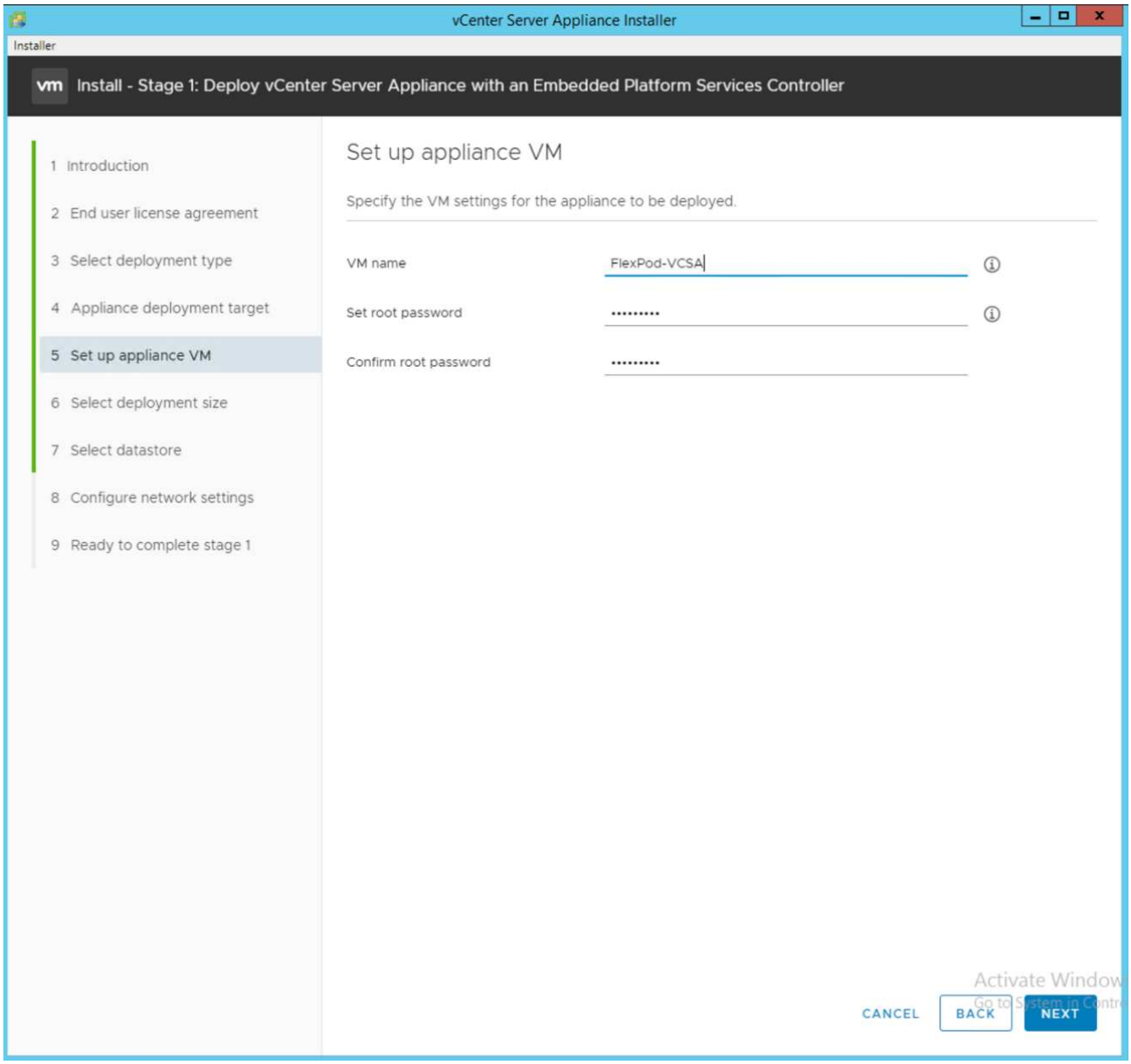


必要に応じて、 FlexPod Express 解決策の一部として、外部プラットフォームサービスコントローラの導入もサポートされます。

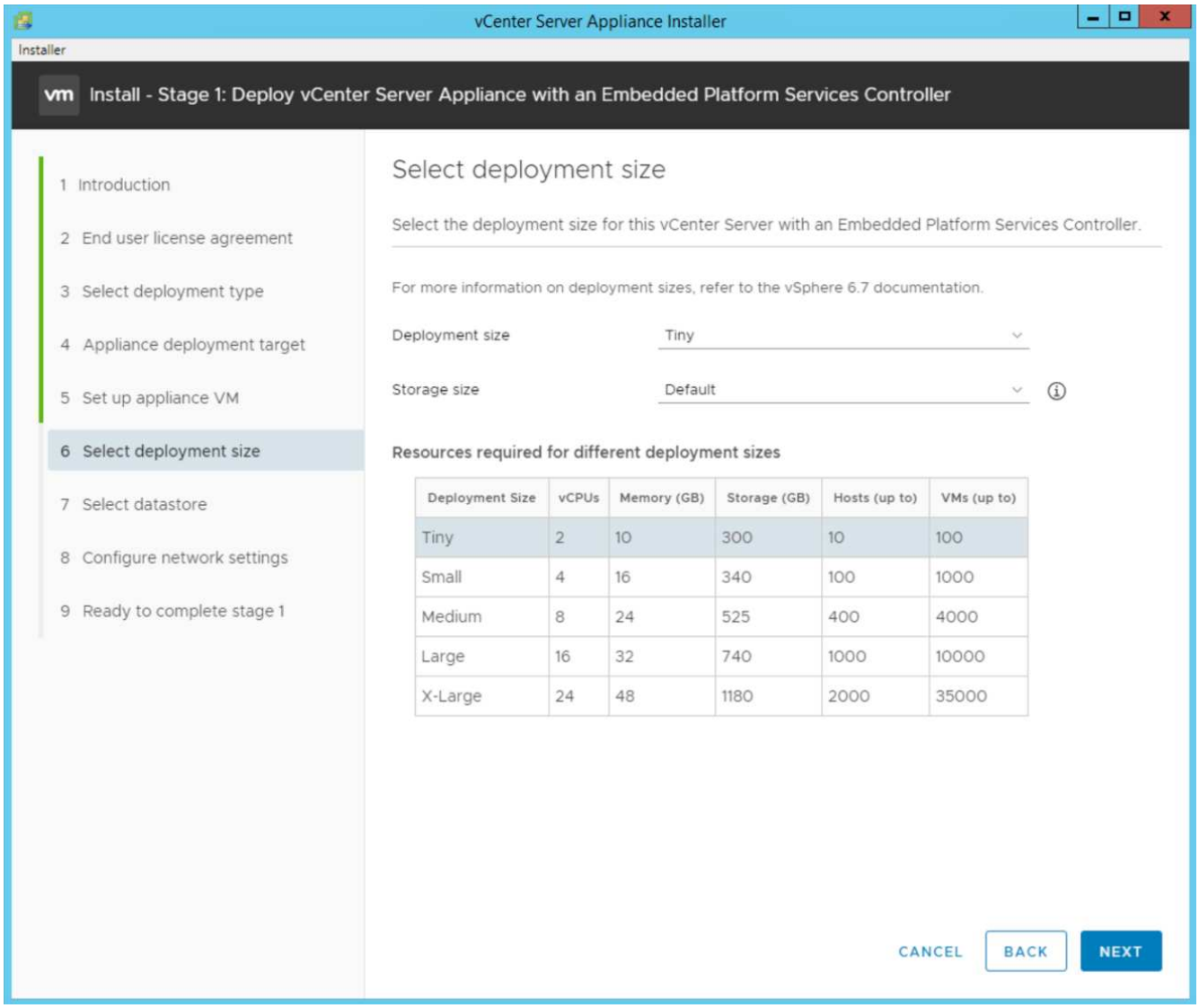
9. アプライアンス導入ターゲットで、導入した ESXi ホストの IP アドレス、ルートユーザ名、および root パスワードを入力します。



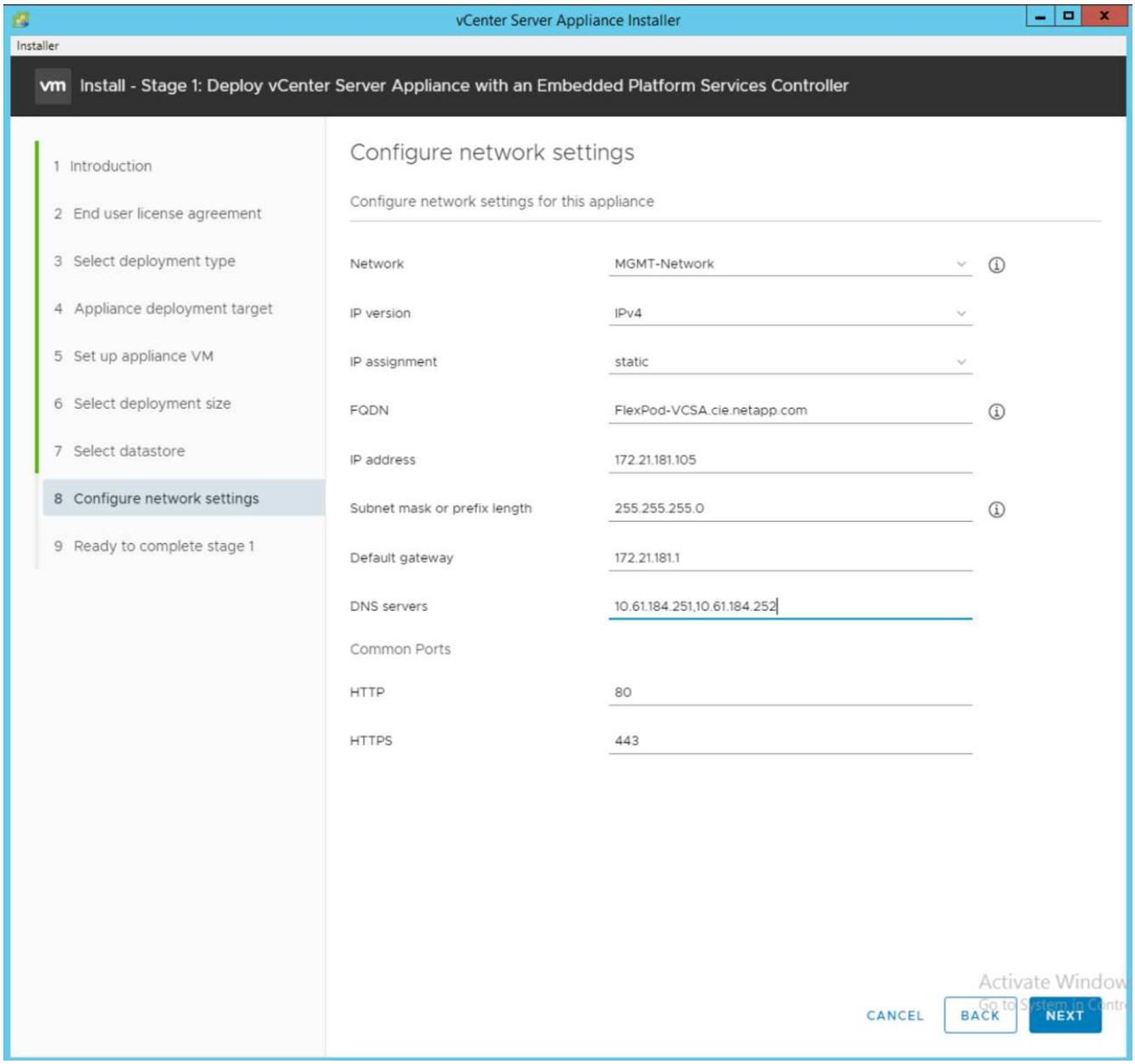
10. vCSA に VM 名および root パスワードとして入力し、 vCSA に使用するアプライアンス VM を設定します。



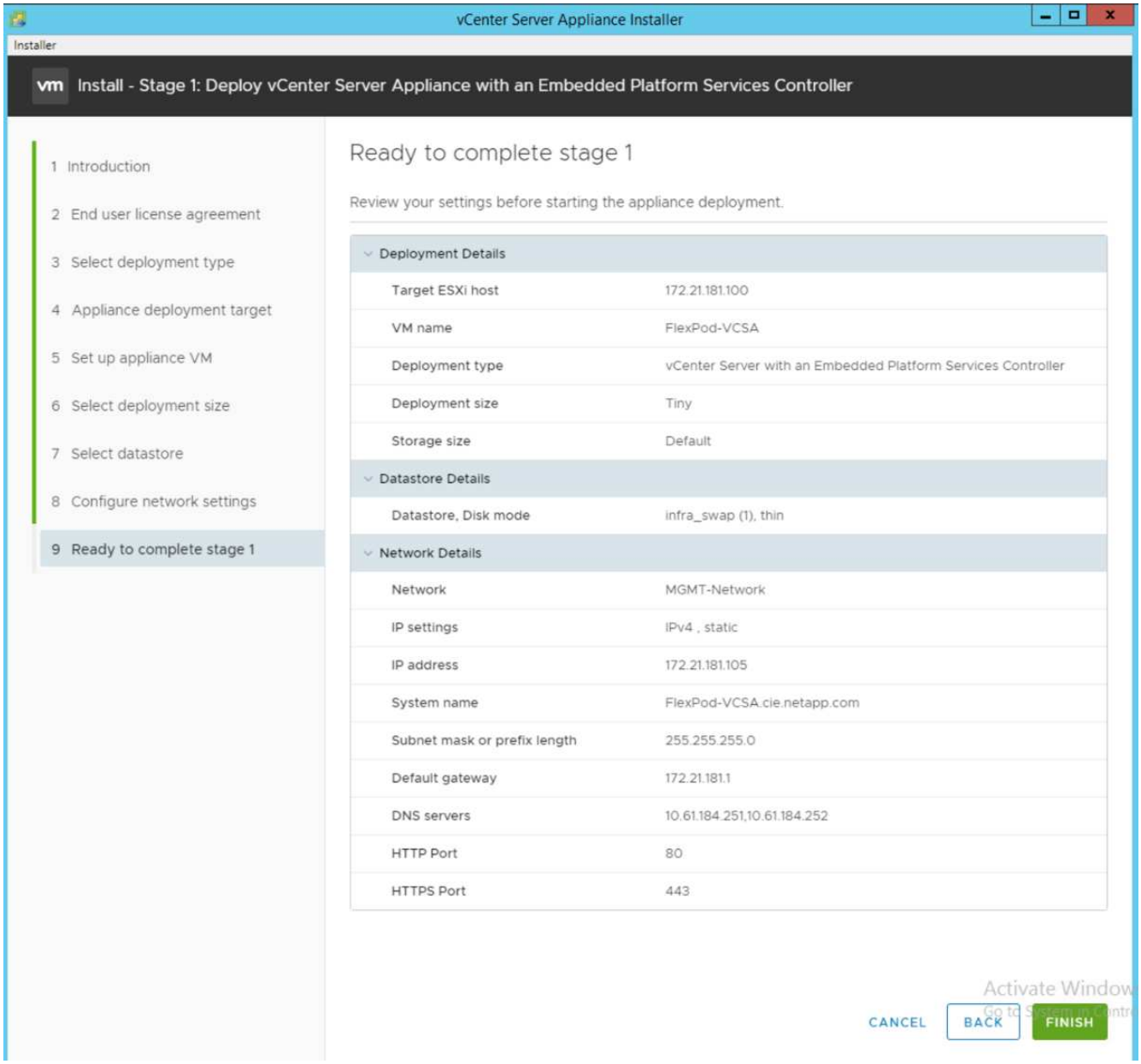
11. 環境に最も適した導入サイズを選択してください。次へをクリックします。



12. 「 infra_datastore 」データストアを選択します。次へをクリックします。
13. Configure network settings （ネットワーク設定の設定）ページで次の情報を入力し、 Next （次へ）をクリックします。
    a. MGMT - Network （ネットワーク）を選択します。
    b. vCSA に使用する FQDN または IP を入力します。
    c. 使用する IP アドレスを入力します。
    d. 使用するサブネットマスクを入力します。
    e. デフォルトゲートウェイを入力します。
    f. DNS サーバを入力します。
14. 「ステージ 1 を完了する準備ができました」ページで、入力した設定が正しいことを確認します。完了をクリックします。

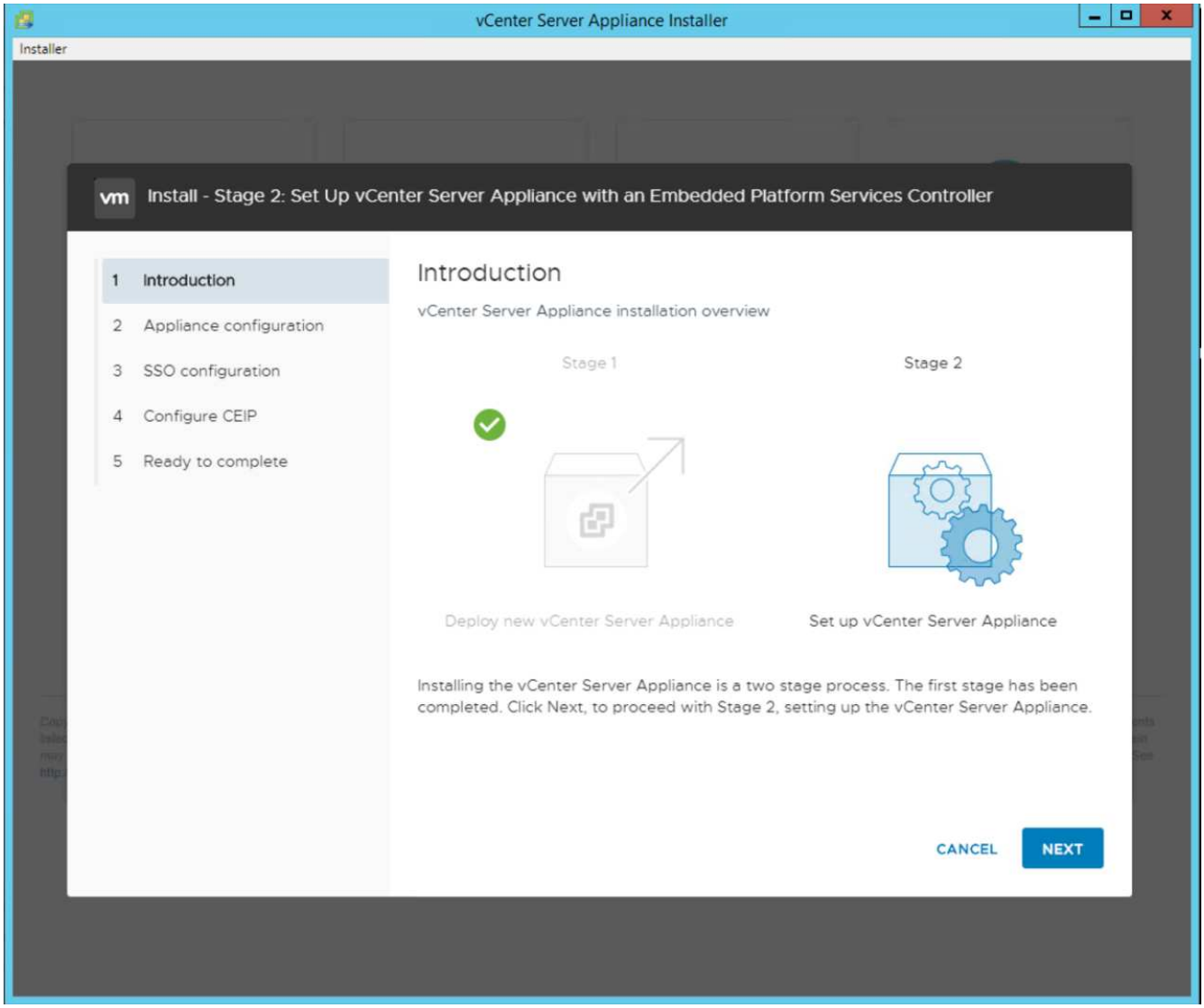


15. アプライアンスの導入を開始する前に、第 1 段階の設定を確認してください。

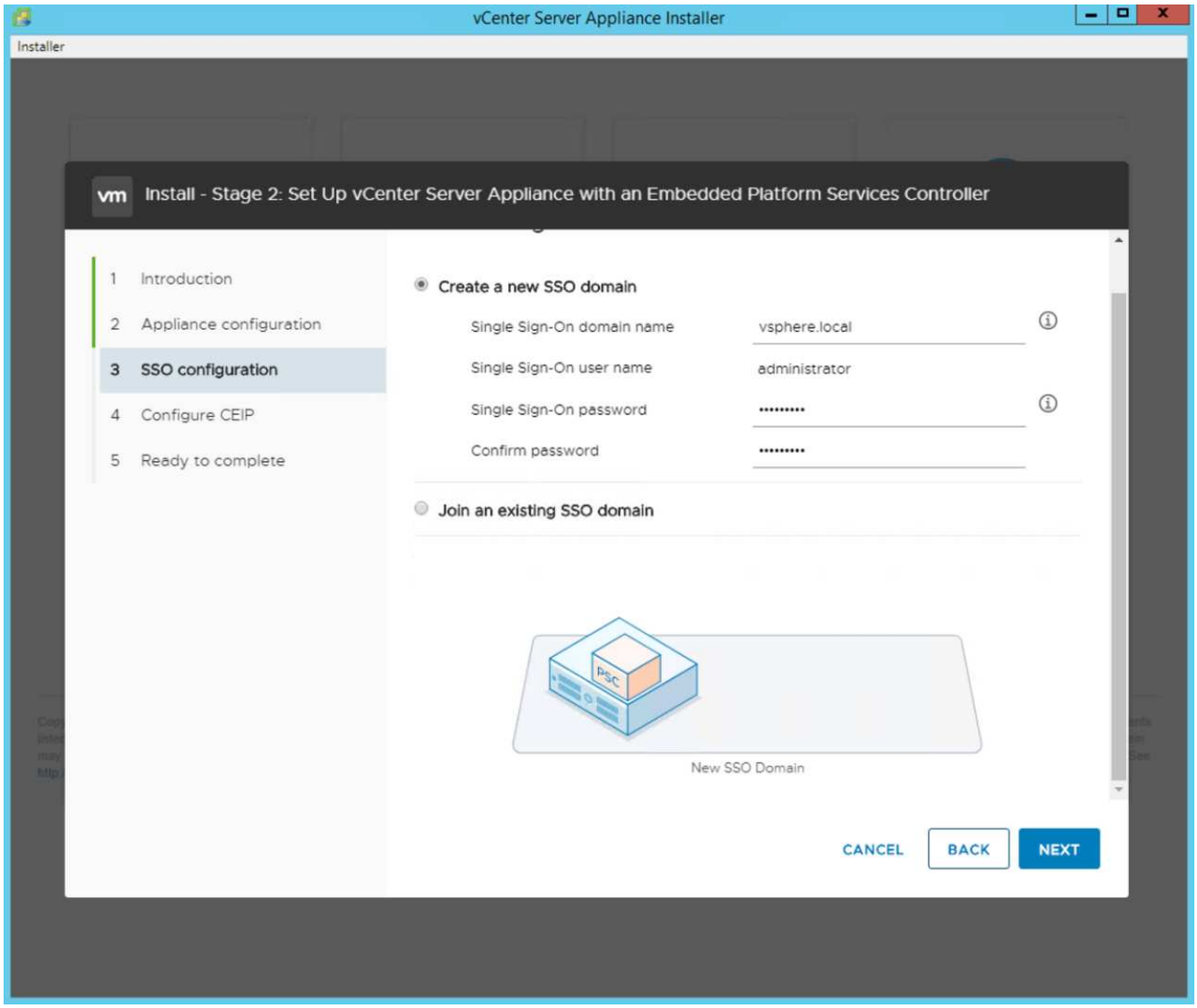


vCSA がインストールされます。このプロセスには数分かかります。

16. ステージ 1 が完了すると、完了したことを示すメッセージが表示されます。「続行」をクリックしてステージ 2 の設定を開始します。
17. 「ステージ 2 の紹介」ページで、「次へ」をクリックします。

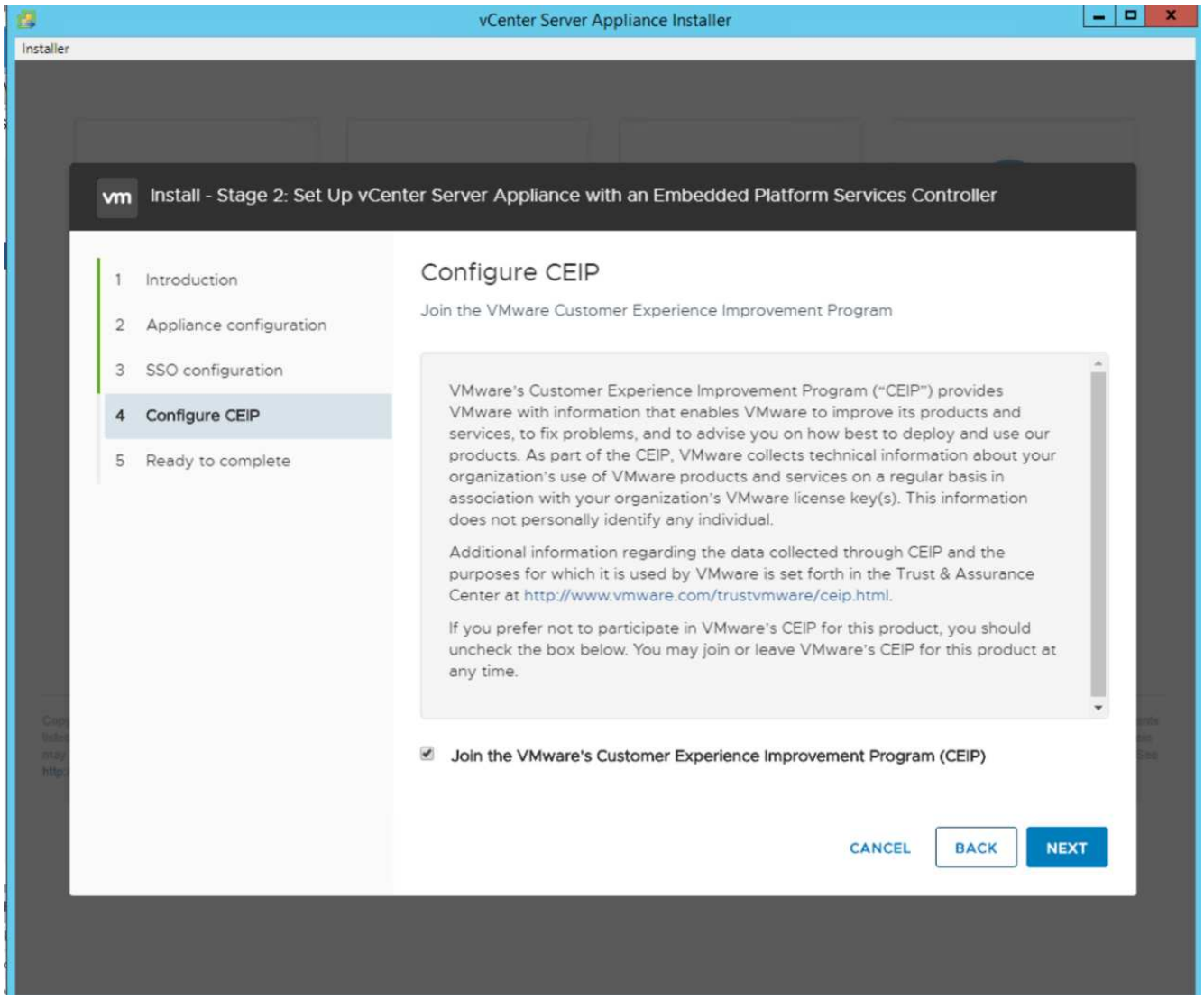


18. NTP サーバのアドレスとして「 \<<var_ntp_id>> 」と入力します。複数の NTP IP アドレスを入力できます。
19. vCenter Server High Availability （ HA ；高可用性）を使用する場合は、 SSH アクセスが有効になっていることを確認してください。
20. SSO ドメイン名、パスワード、およびサイト名を設定します。次へをクリックします。

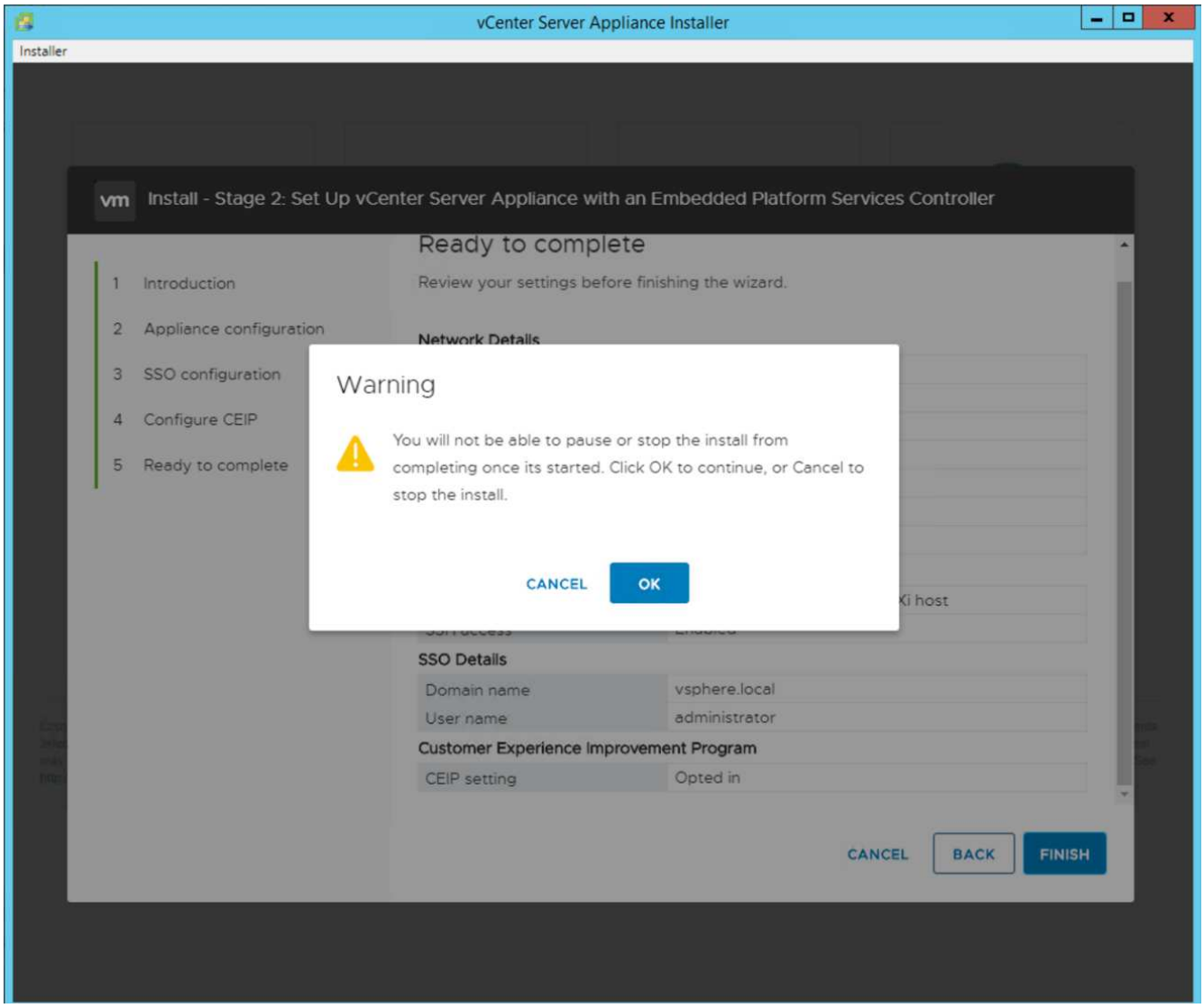


特に 'vSpher.local' ドメイン名から外れる場合は ' これらの値を参考にしてください

21. 必要に応じて、 VMware カスタマーエクスペリエンスプログラムに参加します。次へをクリックします。



22. 設定の概要を確認します。[完了] をクリックするか、 [戻る] ボタンを使用して設定を編集します。
23. インストールの開始後に、インストールを一時停止または終了できないことを示すメッセージが表示されます。[OK] をクリックして続行します。



アプライアンスの設定が続行されます。これには数分かかります。

セットアップが正常に完了したことを示すメッセージが表示されます。

24. インストーラが vCenter Server にアクセスするために提供するリンクはクリック可能です。

"次の記事：VMware vCenter Server 6.7U2とvSphereクラスタリング構成"

VMware vCenter Server 6.7U2 と **vSphere** クラスタリング構成

VMware vCenter Server 6.7 および vSphere クラスタリングを設定するには、次の手順を実行します。

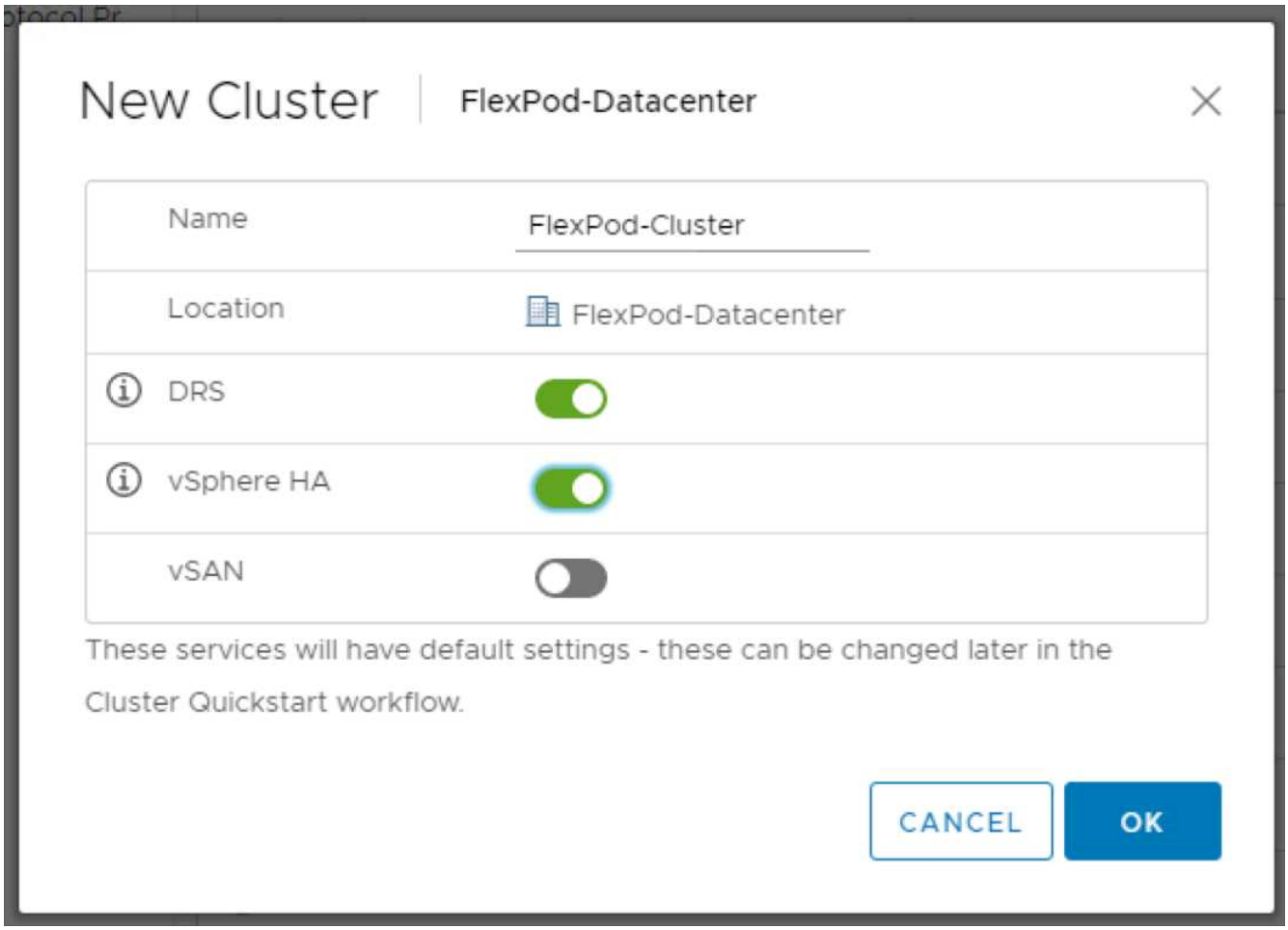
1. 「 \ https://\<<FQDN 」または「 vCenter の IP >>/vsphere-client/` 」に移動します。
2. vSphere Client の起動をクリックします。
3. vCSA のセットアッププロセスで入力したユーザ名 mailto ： administrator@vspehre.loca l [administrator^] @vsphere.local および SSO パスワードを使用してログインします。
4. vCenter 名を右クリックし、 New Datacenter を選択します。

5. データセンターの名前を入力し、 [OK] をクリックします。

vSphere クラスタを作成します

vSphere クラスタを作成するには、次の手順を実行します。

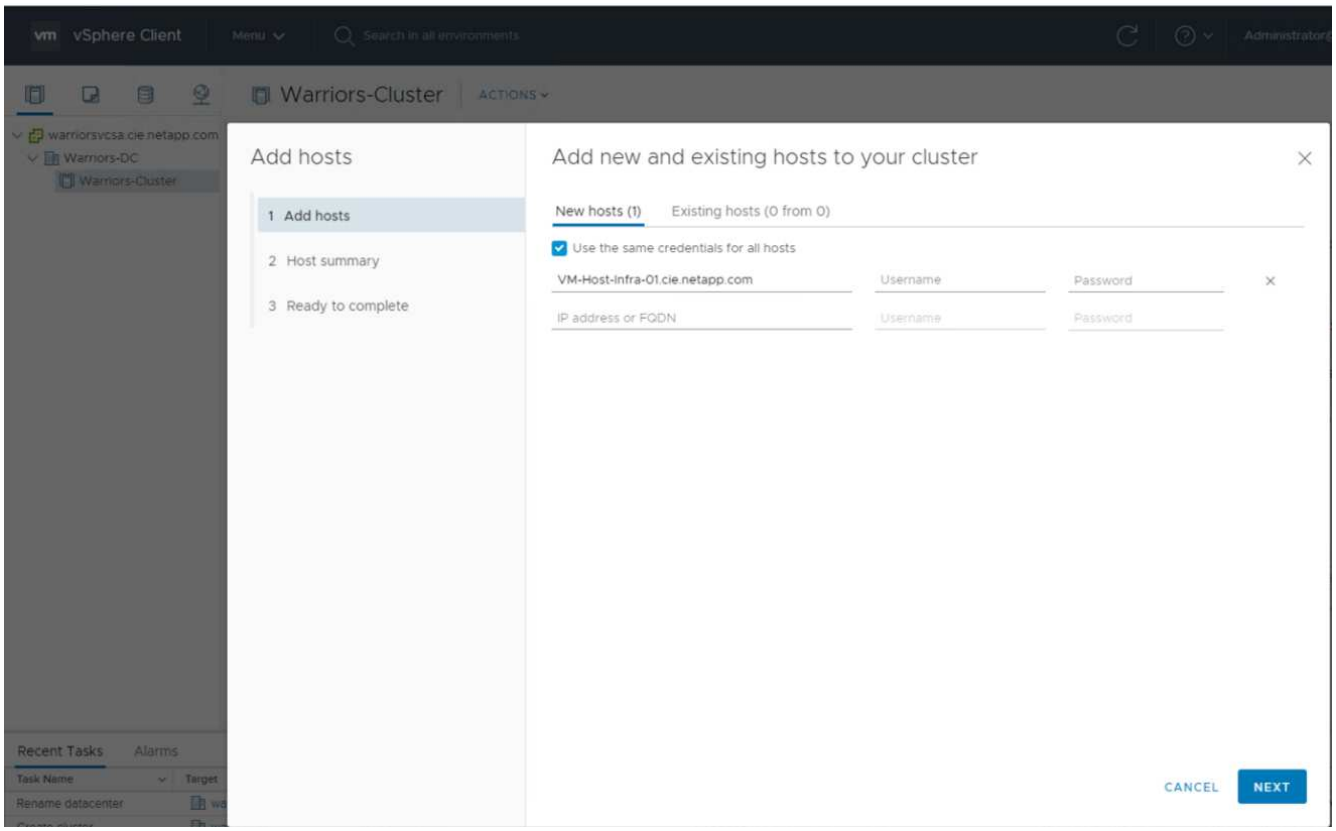
1. 新しく作成したデータセンターを右クリックし、 [New Cluster] を選択します。
2. クラスタの名前を入力します。
3. チェックボックスをオンにして DR と vSphere HA を有効にします。
4. [OK] をクリックします。



ESXi ホストをクラスタに追加

ESXi ホストをクラスタに追加するには、次の手順を実行します。

1. クラスタを右クリックし、 Add Host （ホストの追加）を選択します。



2. ESXi ホストをクラスタに追加するには、次の手順を実行します。
   a. ホストの IP または FQDN を入力します。次へをクリックします。
   b. root ユーザ名とパスワードを入力します。次へをクリックします。
   c. Yes をクリックして、ホストの証明書を VMware 証明書サーバによって署名された証明書に置き換えます。
   d. [Host Summary] ページで [Next] をクリックします。
   e. 緑の + アイコンをクリックして、 vSphere ホストにライセンスを追加します。
3. この手順は、必要に応じてあとで実行できます。
   a. [次へ] をクリックして、ロックダウンモードを無効のままに
   b. [VM の場所] ページで [次へ] をクリックします。
   c. [Ready to Complete] ページを確認します。[戻る] ボタンを使用して変更を行うか、 [完了] を選択します。
4. Cisco UCS ホスト B に対して手順 1 と 2 を繰り返します

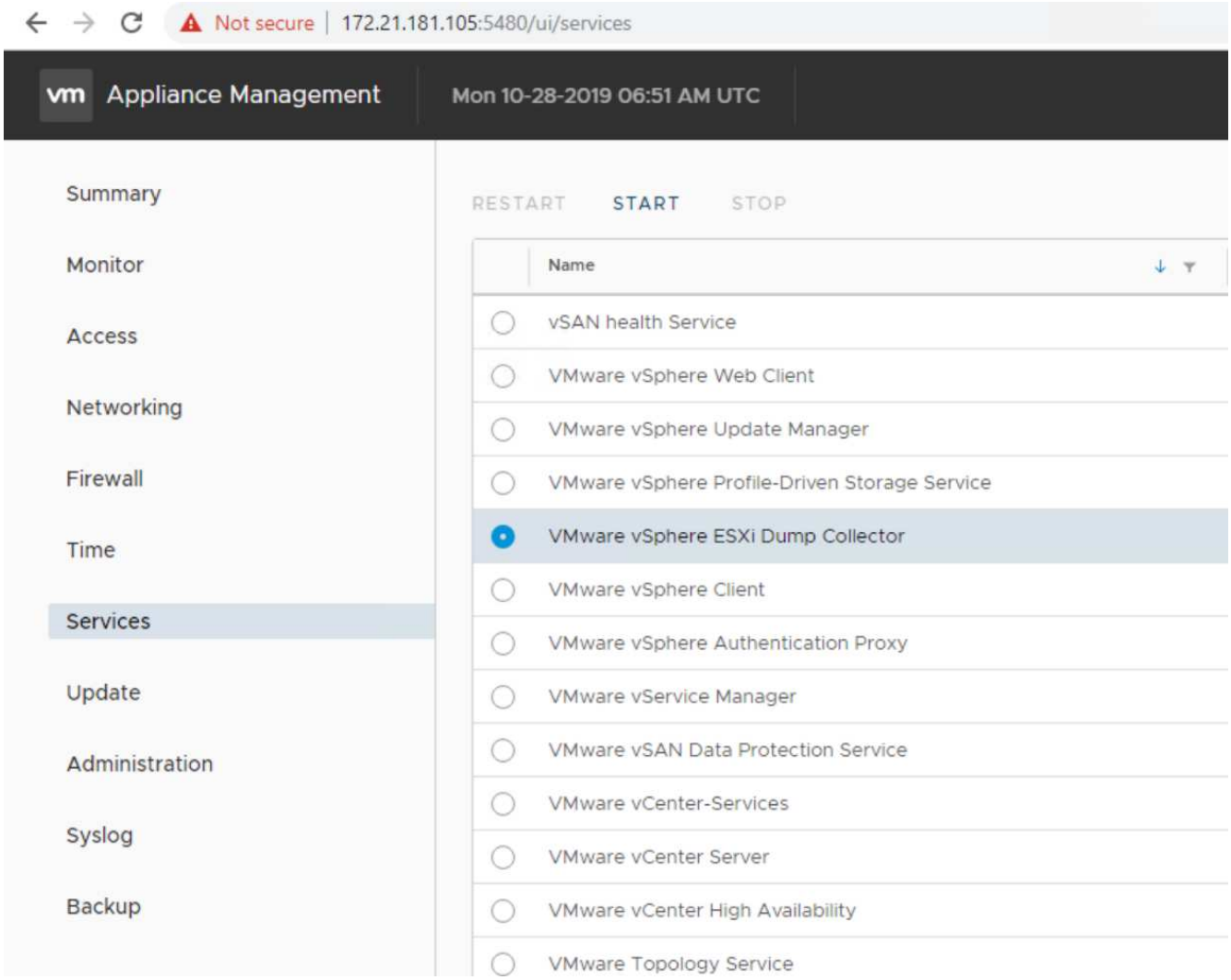
> FlexPod 構成にホストを追加する場合は、この手順を実行する必要があります。

ESXi ホストにコアダンプを設定します

ESXi ホストにコアダンプを設定するには、次の手順を実行します。

1. https ： // にログインします "vCenter" IP:5480/ の場合は、ユーザ名に root を入力し、 root パスワードを入力します。

2. services をクリックして、 VMware vSphere ESXi Dump Collector を選択します。
3. VMware vSphere ESXi Dump コレクタサービスを開始します。



4. SSH を使用して管理 IP ESXi ホストに接続し、ユーザ名に「 root 」と入力して、 root パスワードを入力します。
5. 次のコマンドを実行します。

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

6. 最終コマンドを入力すると、「 Verified the configured netdump server is running 」というメッセージが表示されます。

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
 vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
erified the configured netdump server is running
```

FlexPod Express にホストを追加する場合は、このプロセスを完了する必要があります。

この検証で使用する「 IP_address_OF_CORE_DUMP_collector 」は、 vCenter の IP です。

"次の記事：NetApp Virtual Storage Console 9.6の導入手順"

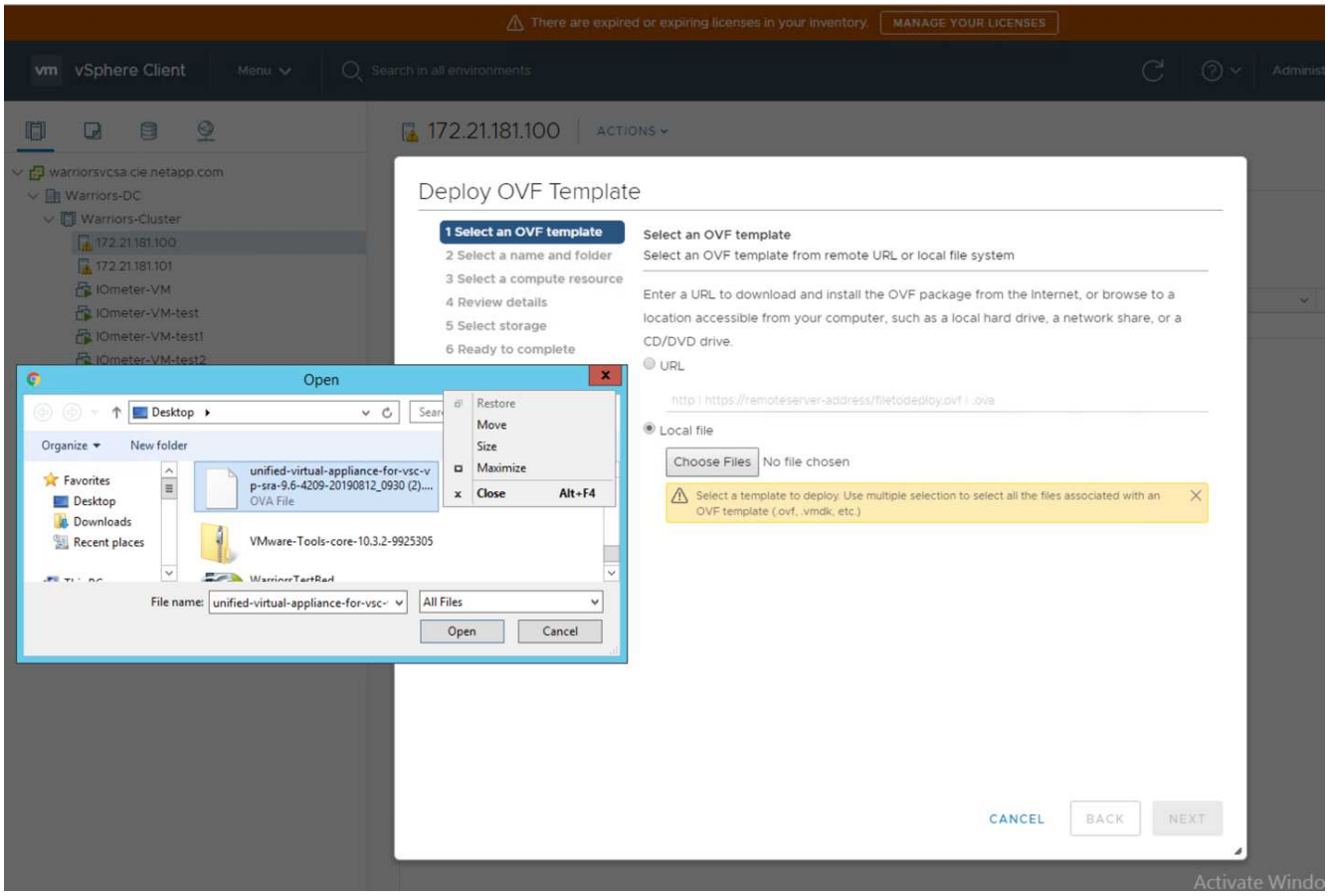
NetApp Virtual Storage Console 9.6 の導入手順

このセクションでは、 NetApp Virtual Storage Console （ VSC ）の導入手順について説明します。

Virtual Storage Console 9.6 をインストールします

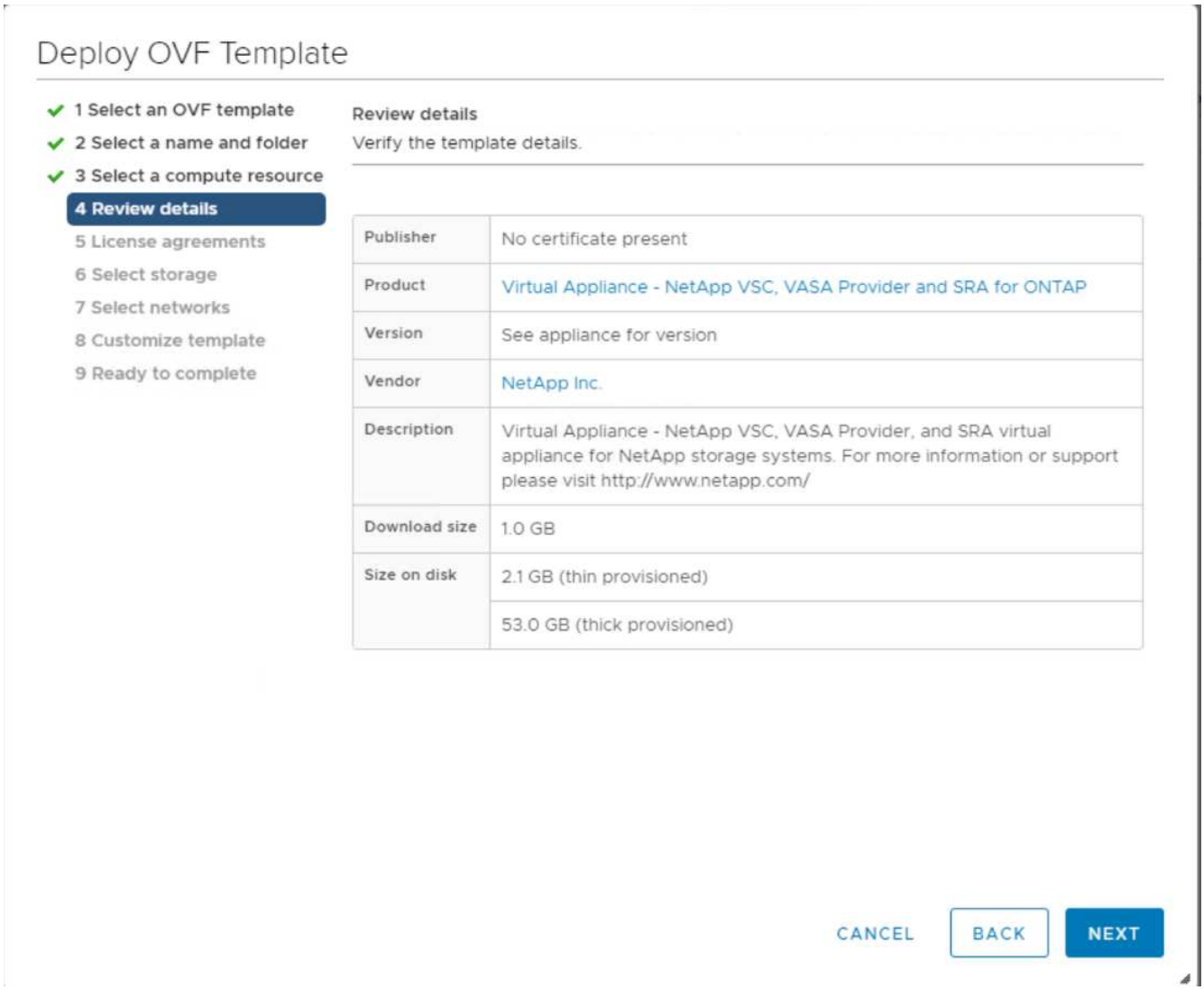
Open Virtualization Format （ OVF ）導入を使用して VSC 9.6 ソフトウェアをインストールする手順は、次のとおりです。

1. vSphere Web Client > Host Cluster > Deploy OVF Template に移動します。
2. ネットアップサポートサイトからダウンロードした VSC OVF ファイルを参照します。

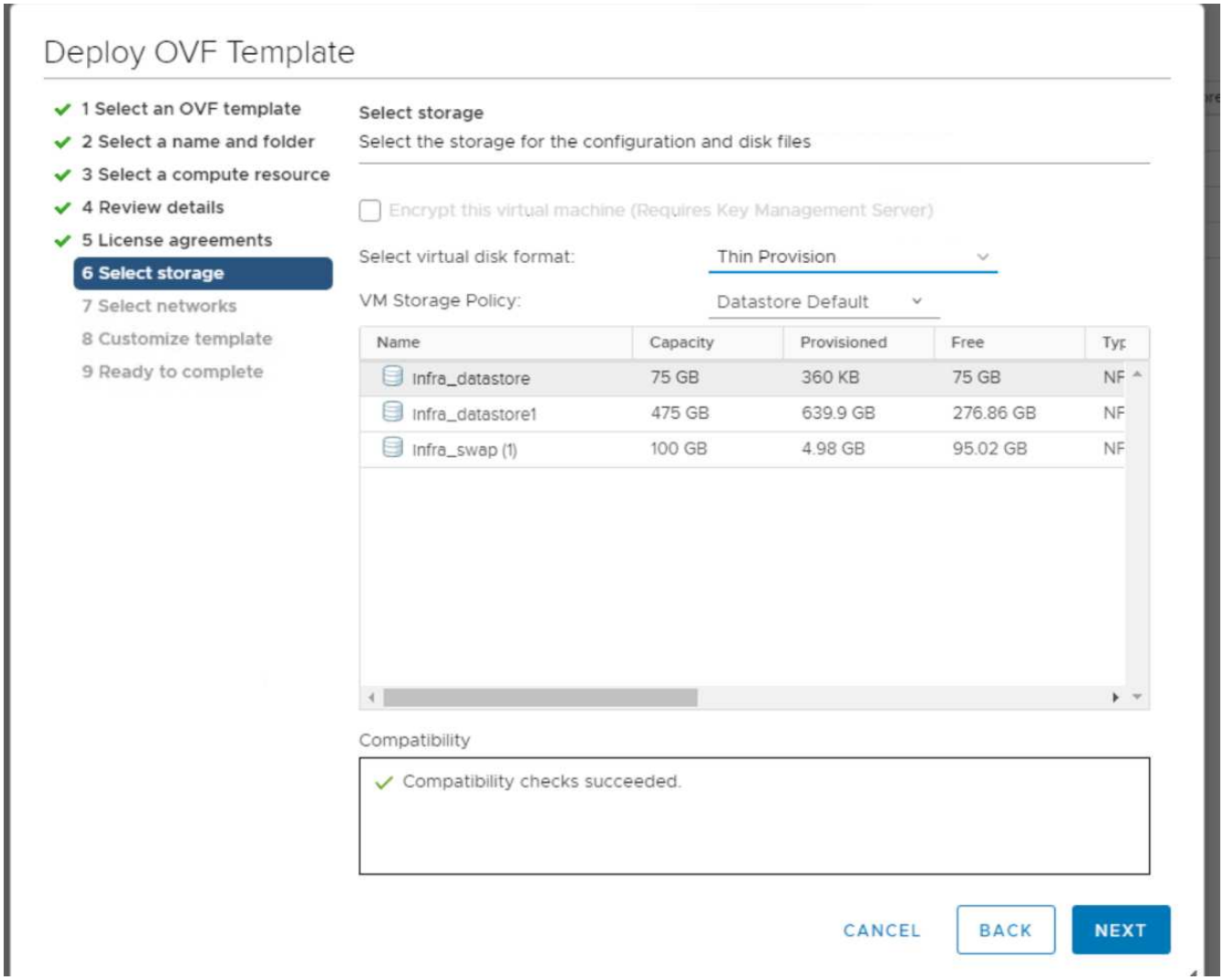


3. VM 名を入力し、導入先のデータセンターまたはフォルダを選択します。次へをクリックします。

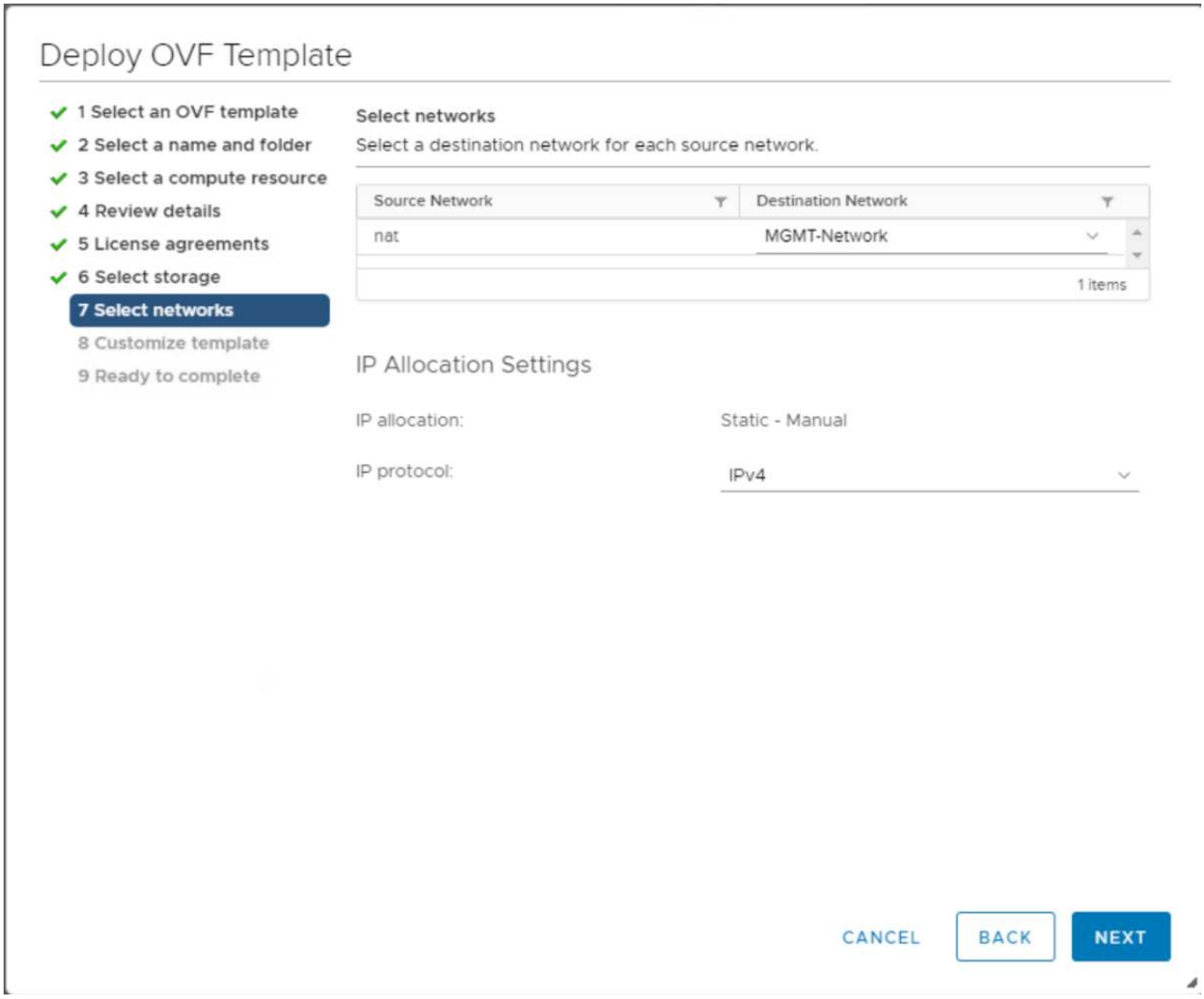
4. 「 FlexPod - Cluster ESXi 」クラスタを選択し、「 Next 」をクリックします。
5. 詳細を確認し、 [次へ] をクリックします。



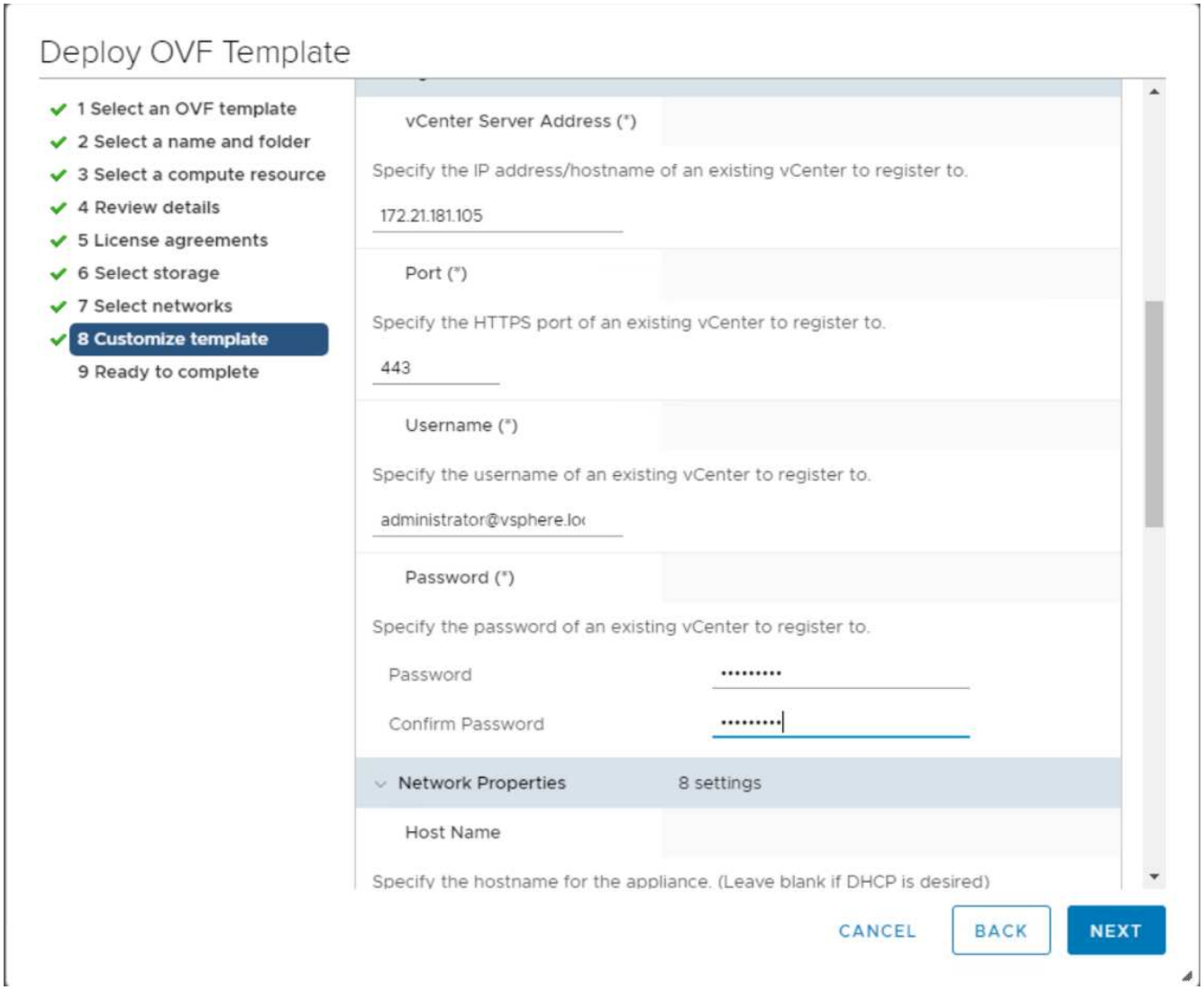
6. [Accept （同意）] をクリックしてライセンスを受け入れ、 [Next] をクリックします。
7. シンプロビジョニング仮想ディスク形式と NFS データストアの 1 つを選択します。次へをクリックします。



8. [Select Networks] (ネットワークの選択) から宛先ネットワークを選択し、 [Next] (次へ) をクリックします。



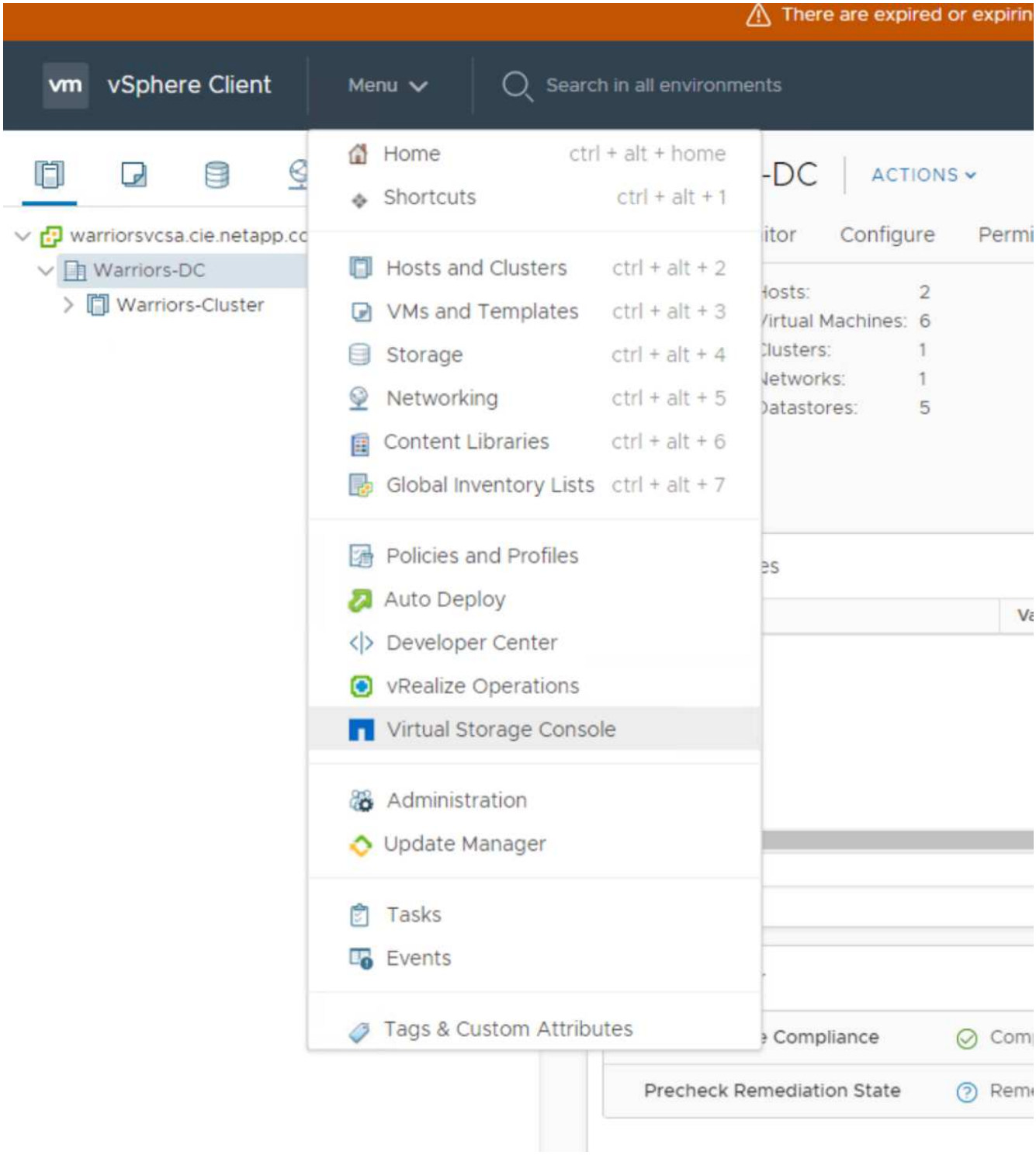
9. テンプレートのカスタマイズで、 VSC 管理者パスワード、 vCenter 名または IP アドレス、およびその他の設定の詳細を入力し、次へをクリックします。



10. 入力した設定の詳細を確認し、 Finish をクリックして NetApp-VSC VM の導入を完了します。
11. NetApp-VSC VM の電源をオンにして、 VM コンソールを開きます。
12. NetApp - VSC VM のブートプロセス中に、 VMware Tools のインストールを求めるプロンプトが表示されます。vCenter で、 [NetApp-VSC VM] -[ゲスト OS] -[VMware Tools のインストール] を選択します。

```
Booting VSC, VASA Provider, and SRA virtual appliance...Please wait...
VMware Tools OVF vCenter configuration not found.
VMware Tools OVF vCenter configuration not found.
VMware Tools OVF vCenter configuration not found.

VMware Tools installation


Before you can continue the VSC, VASA Provider, and SRA virtual appliance
installation, you must install the VMware Tools:

  1.  Select VM > Guest OS > Install VMware Tools.

                    OR

      Click on "Install VMware Tools" pop-up box on the vSphere Web Client.

  2.  Follow the prompts provided by the VMware Tools wizard.

Once you click on mount, the installation process will automatically continue.
```

13. OVF テンプレートのカスタマイズ時に、ネットワーク設定と vCenter の登録情報が提供されました。そのため、 NetApp-VSC VM の実行後、 VSC 、 vSphere API for Storage Awareness （ VASA ）、および VMware Storage Replication Adapter （ SRA ）が vCenter に登録されます。
14. vCenter Client からログアウトし、再度ログインします。ホームメニューから、 NetApp VSC がインストールされていることを確認します。



NetApp NFS VAAI Plug-in をダウンロードしてインストールします

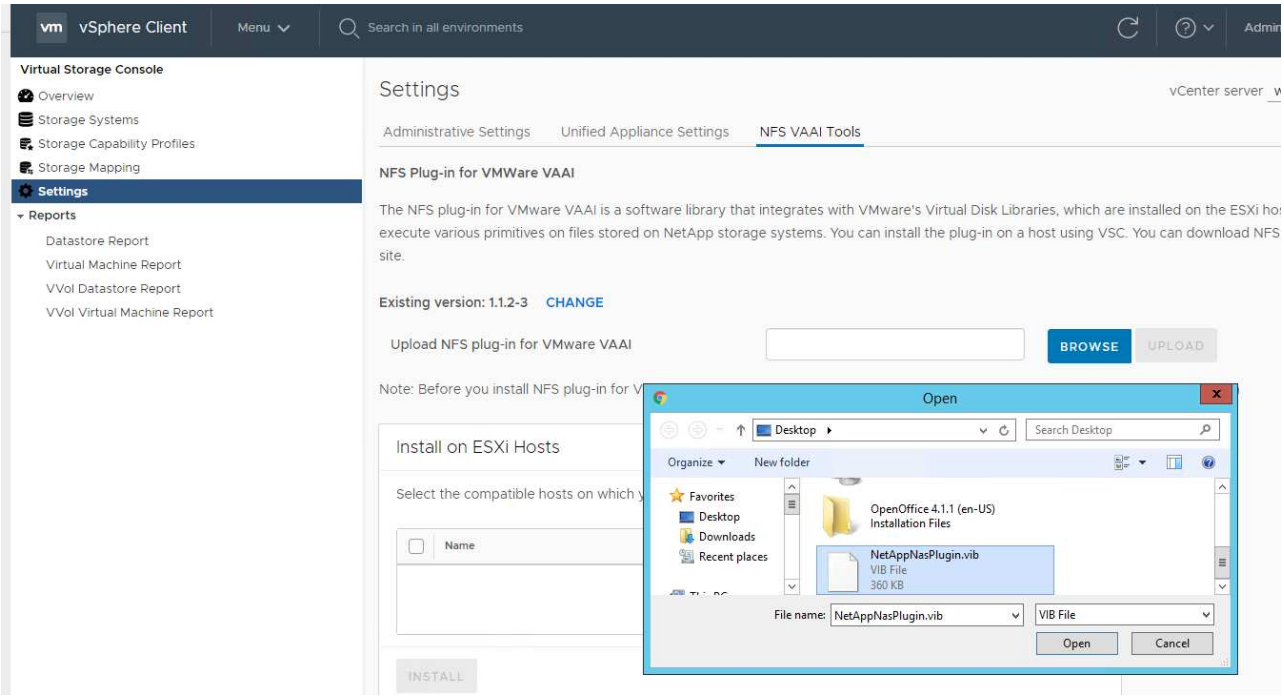
NetApp NFS VAAI Plug-in をダウンロードしてインストールするには、次の手順を実行します。

1. NetApp NFS Plug-in 1.1.2 for VMware' をダウンロードしますNFS プラグインのダウンロードページから VIB ファイルをダウンロードし、ローカルマシンまたは管理ホストに保存します。
2. NetApp NFS Plug-in for VMware VAAI をダウンロードします。
   a. にアクセスします "ソフトウェアダウンロードページ"。

b. 下にスクロールして、 NetApp NFS Plug-in for VMware VAAI をクリックします。

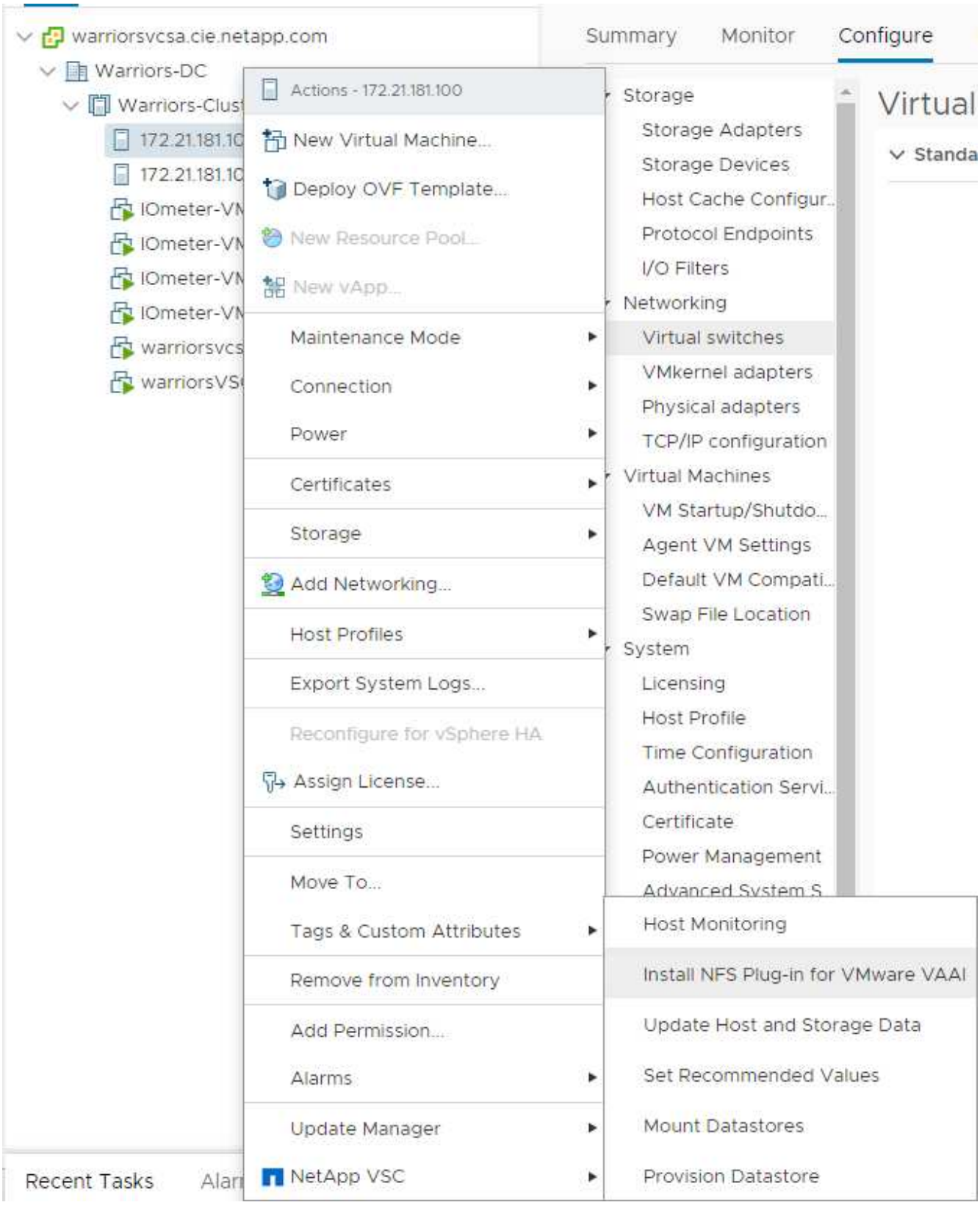
c. vSphere Web Client のホーム画面で、 Virtual Storage Console を選択します。

d. Virtual Storage Console > Settings > NFS VAAI Tools で、ファイルを選択し、ダウンロードしたプラグインが格納されている場所を参照して、 NFS Plug-in をアップロードします。



3. アップロードをクリックして、プラグインを vCenter に転送します。

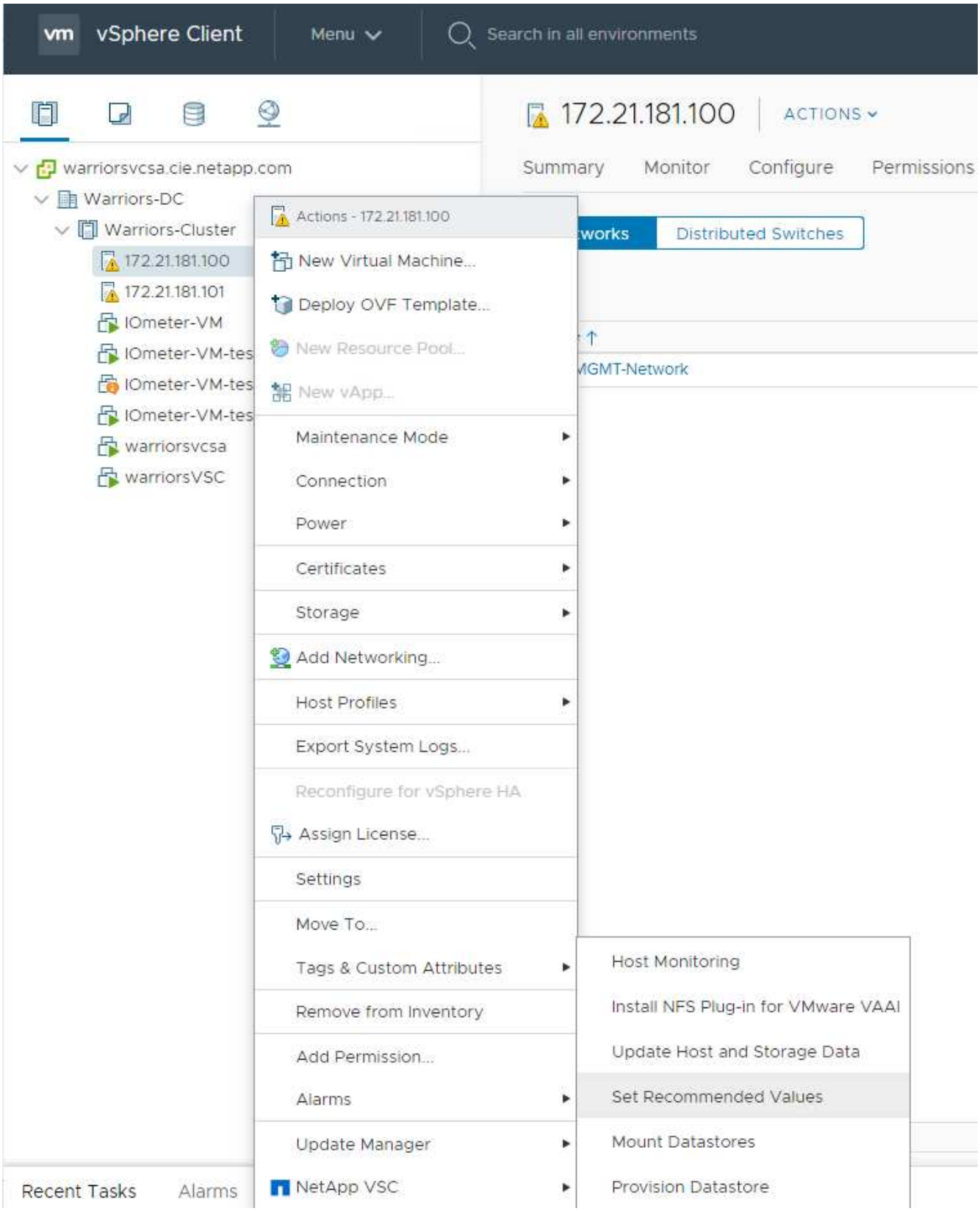
4. ホストを選択し、 NetApp VSC > Install NFS Plug-in for VMware VAAI の順に選択します。



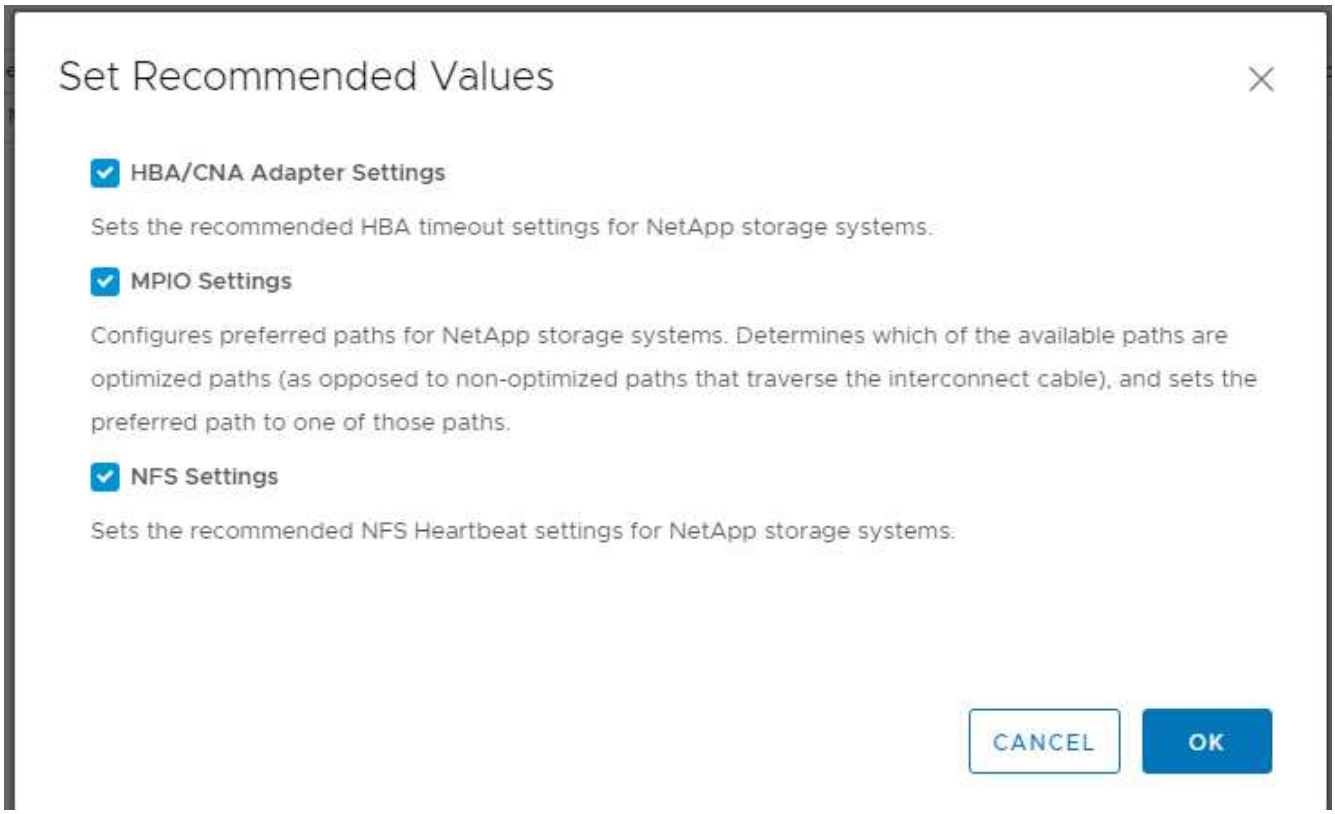
ESXi ホストのストレージ設定を最適化します

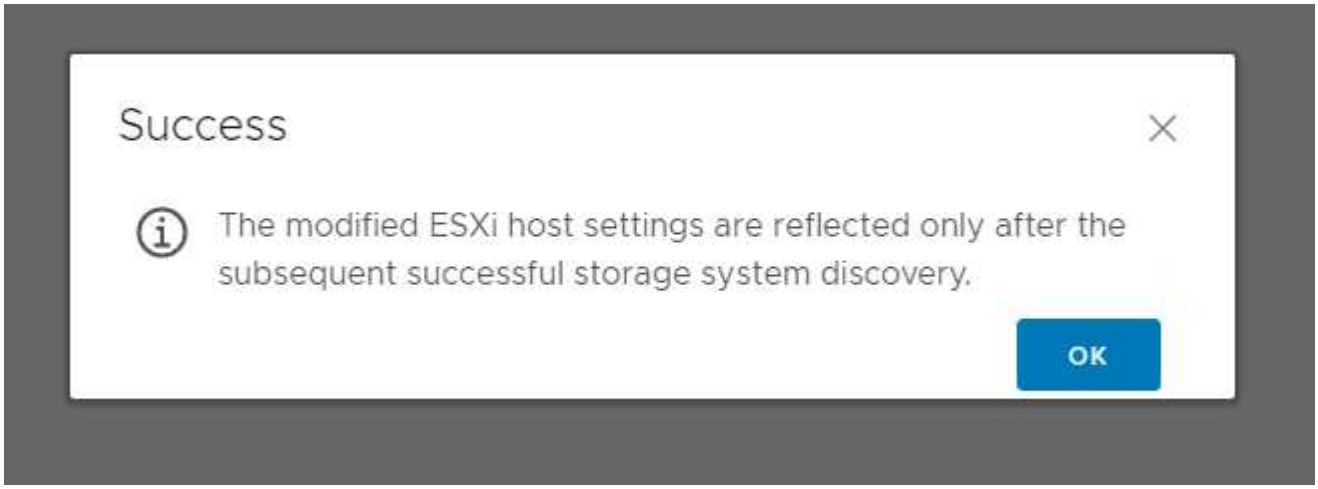
VSC を使用すると、ネットアップストレージコントローラに接続されているすべての ESXi ホストに対して、ストレージ関連の設定を自動的に構成できます。これらの設定を使用するには、次の手順を実行します。

1. ホーム画面で、 vCenter > Hosts and Clusters を選択します。各 ESXi ホストを右クリックし、 NetApp VSC > Set Recommended Values を選択します。



2. 選択した vSphere ホストに適用する設定を確認してください。[OK] をクリックして設定を適用します。





3. これらの設定を適用したら、 ESXi ホストをリブートします。

まとめ

FlexPod Express は、業界をリードするコンポーネントを使用した検証済みの設計を提供することで、シンプルで効果的な解決策を実現します。コンポーネントの追加による拡張により、 FlexPod Express は特定のビジネスニーズに合わせて調整できます。FlexPod Express は、中小規模の企業や、特定用途向けのソリューションを必要とする企業向けに設計されています。

謝辞

著者はジョンジョージをこの設計への彼のサポートそして貢献のために認めたいと思う。

追加情報の参照先

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。

ネットアップの製品マニュアル

http://docs。 "ネットアップ".com

FlexPod エクスプレスガイド

NVA-1139 - 設計： FlexPod Express with Cisco UCS C シリーズ and NetApp AFF C190 シリーズ

"https://www.netapp.com/us/media/nva-1139-design.pdf"

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	2019年11月	初版リリース

FlexPod Express with Cisco UCS C シリーズおよび AFF A220 シリーズ設計ガイド

NVA-1125 設計： FlexPod Express with Cisco UCS C シリーズ and AFF A220 Series

ネットアップ、 Savita Kumari とのパートナーシップ：

業界のトレンドは、共有インフラとクラウドコンピューティングへの大規模なデータセンターの移行を示しています。さらに、リモートオフィスやブランチオフィスにもシンプルで効果的な解決策を導入し、データセンターで慣れ親しんでいるテクノロジを活用しています。

FlexPod Express は、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus ファミリースイッチ、および NetApp AFF を基盤とした、事前設計されたベストプラクティスのデータセンターアーキテクチャです。FlexPod Express のコンポーネントは、 FlexPod Datacenter と同様に、小規模な IT インフラ環境全体での管理面の相乗効果を実現します。FlexPod Datacenter と FlexPod Express は、仮想化に最適なプラットフォームで、ベアメタルのオペレーティングシステムやエンタープライズワークロードに最適です。

"次のページ：プログラムの概要"

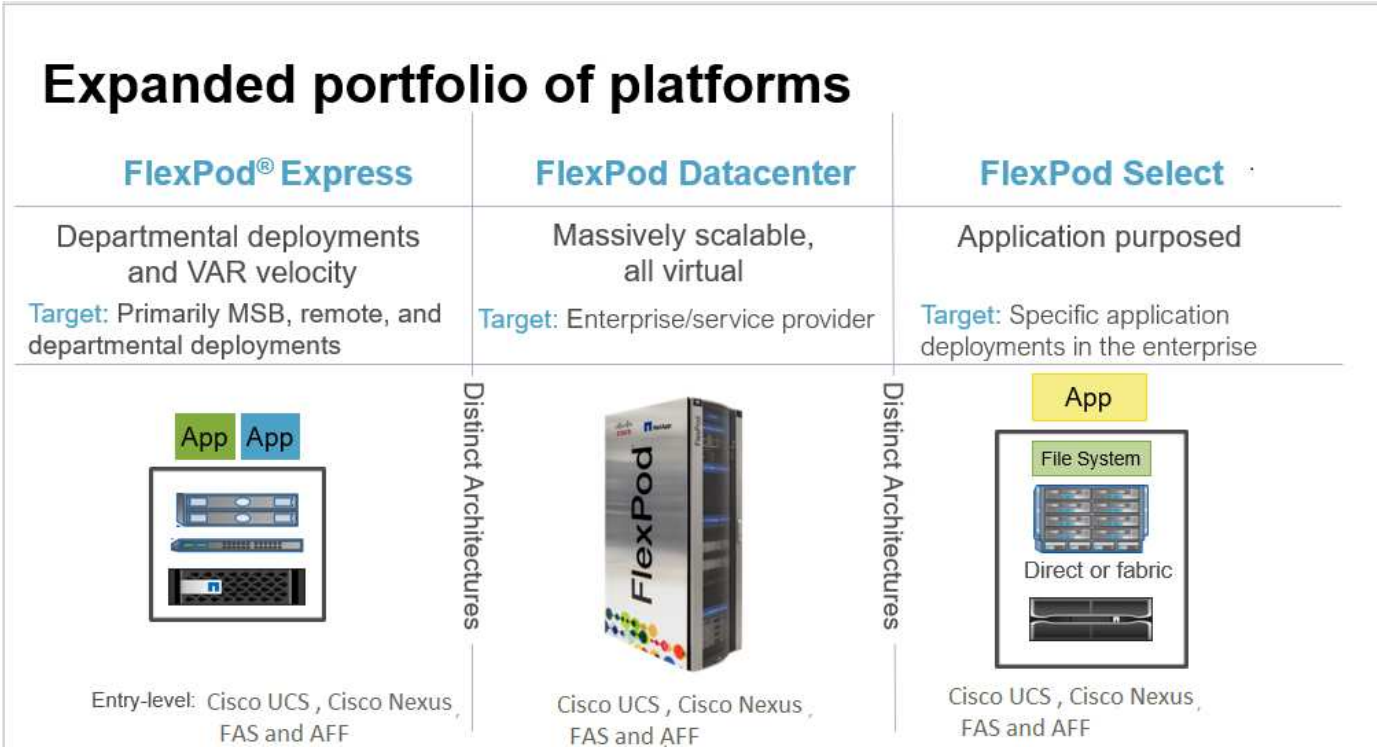
プログラムの概要

FlexPod コンバージドインフラのポートフォリオ

FlexPod リファレンスアーキテクチャは、 Cisco Validated Design （ CVD ）または NetApp Verified Architectures （ NVA ）として提供されます。CVD または NVA のお客様の要件に基づく差異は、それらの違いによってサポートされない構成が導入されない場合に許容されます。

次の図に示すように、 FlexPod ポートフォリオには、 FlexPod Express 、 FlexPod Datacenter 、 FlexPod Select の 3 つのソリューションが含まれています。

- * FlexPod Express. * は、 Cisco とネットアップのテクノロジで構成されるエントリレベルの解決策を提供します。
- * FlexPod * Datacenter * は、さまざまなワークロードやアプリケーションに最適な多目的基盤を提供します。
- * FlexPod Select * は、 FlexPod データセンターの最良の側面を組み込み、特定のアプリケーションにインフラストラクチャを調整します。



NetApp Verified Architecture プログラム

NVA プログラムは、ネットアップソリューションの検証済みアーキテクチャをお客様に提供します。NVA は、 NetApp 解決策には次の資質があることを意味します。

- 入念にテストされています
- あらかじめ規定されている
- 導入リスクを最小限に抑えます
- 運用開始までの時間を短縮

このガイドでは、 VMware vSphere を使用した FlexPod Express の設計について詳しく説明します。また、この設計では、 NetApp ONTAP 9.4 ソフトウェア、 Cisco Nexus 3172P スイッチ、および Cisco UCS C220 M5 サーバをハイパーバイザーノードとして実行する、まったく新しい AFF A220 システムを活用しています。

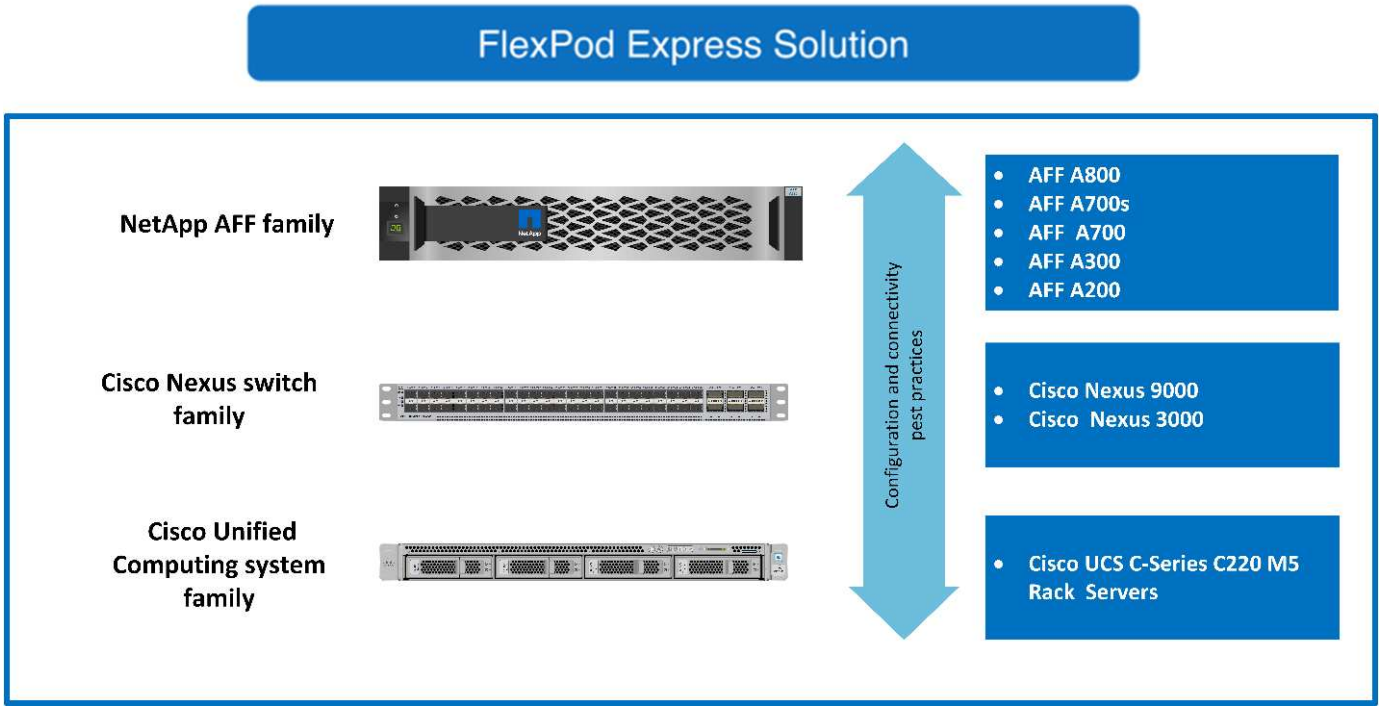
このドキュメントは AFF A220 で検証済みですが、この解決策は FAS2700 もサポートしています。

"次の手順：解決策の概要"

解決策の概要

FlexPod Express は、混在仮想化ワークロードを実行するように設計されています。リモートオフィス、ブランチオフィス、中堅企業を対象としています。また、特定の目的に専用の解決策を実装したい大規模企業にも最適です。この新しい解決策 for FlexPod Express には、 NetApp ONTAP 9.4 、 NetApp AFF A220 、 VMware vSphere 6.7 などの新しいテクノロジが追加されています。

次の図に、 FlexPod Express 解決策に含まれるハードウェアコンポーネントを示します。



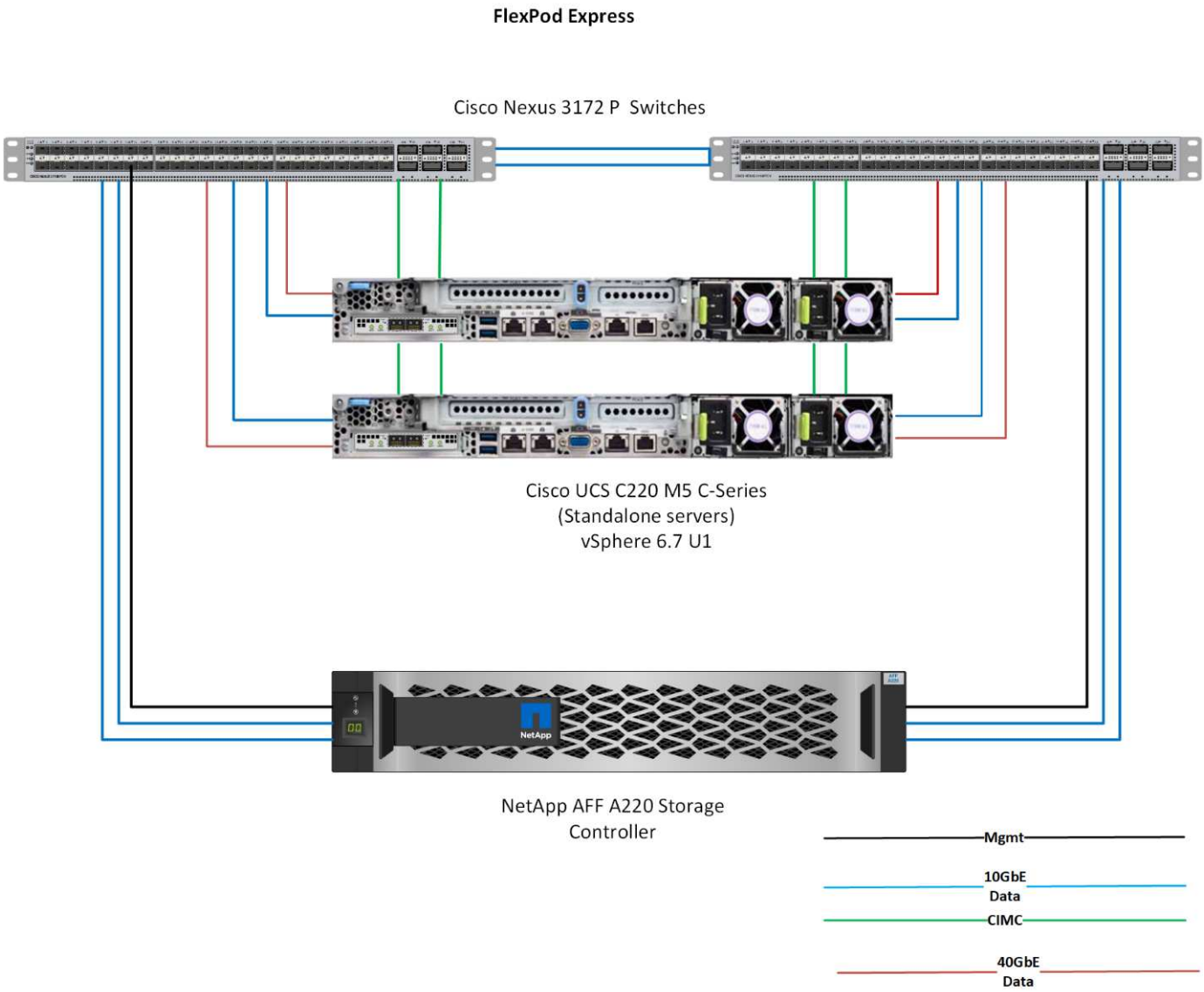
対象読者

本ドキュメントは、 IT の効率化と IT のイノベーションを実現するために構築されたインフラを活用したいお客様を対象としています。本ドキュメントが対象とする主な読者は、セールスエンジニア、フィールドコンサルタント、プロフェッショナルサービス担当者、 IT マネージャーなどです。 パートナー様のエンジニア、お客様

解決策テクノロジ

この解決策は、ネットアップ、 Cisco 、 VMware の最新テクノロジを活用しています。この解決策には、 ONTAP 9.4 ソフトウェア、デュアル Cisco Nexus 3172P スイッチ、 VMware vSphere 6.7 を実行する Cisco

UCS C220 M5 ラックサーバを実行する新しい NetApp AFF A220 システムが搭載されています。この検証済み解決策では、 10 ギガビットイーサネット（ 10GbE ）テクノロジを使用しています。次の図は概要を示しています。また、 FlexPod Express アーキテクチャが組織の進化するビジネスニーズに適応できるように、 2 つのハイパーバイザーノードを一度に追加して拡張する方法についても説明します。



40GbE は検証されていませんが、サポートされるインフラです。

"次のステップ：テクノロジの要件"

テクノロジ要件

FlexPod Express では、選択したハイパーバイザーとネットワークの速度に応じて、ハードウェアコンポーネントとソフトウェアコンポーネントを組み合わせる必要があります。また FlexPod 、ハイパーバイザーノードをシステムに追加するために必要なハードウェアコンポーネントが 2 つのユニットに配置されます。

ハードウェア要件

選択したハイパーバイザーに関係なく、すべての FlexPod Express 構成で同じハードウェアが使用されます。そのため、ビジネス要件が変わっても、どちらのハイパーバイザーも同じ FlexPod Express ハードウェア上で実行できます。

次の表に、すべての FlexPod 構成に必要なハードウェアコンポーネントと、解決策の実装に必要なハードウェアコンポーネントを示します。解決策の特定の実装で使用されるハードウェアコンポーネントは、お客様の要件に応じて異なる場合があります。

ハードウェア	数量
AFF A220 2 ノードクラスタ	1.
Cisco UCS C220 M5 サーバ	2.
Cisco Nexus 3172P スイッチ	2.
Cisco UCS C220 M5 ラックサーバ用 Cisco UCS Virtual Interface Card （ VIC ；仮想インターフェイスカード） 1387	2.
Cisco CVR-QSFP-SFP10G アダプタ	4.

ソフトウェア要件

次の表に、 FlexPod Express 解決策のアーキテクチャを実装するために必要なソフトウェアコンポーネントを示します。

次の表に、 FlexPod Express の基本実装に必要なソフトウェアを示します。

ソフトウェア	バージョン	詳細
Cisco Integrated Management Controller （ CIMC ）	3.1.3	C220 M5 ラックサーバ用
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Cisco Nexus 3172P スイッチの場合
NetApp ONTAP	9.4	AFF A220 コントローラの場合

次の表に、 FlexPod Express のすべての VMware vSphere 環境に必要なソフトウェアを示します。

ソフトウェア	バージョン
VMware vCenter Server Appliance の略	6.7
VMware vSphere ESXi の場合	6.7
NetApp VAAI Plug-in for ESXi	1.1.2

"次のステップ：設計の選択肢。"

設計の選択肢

この設計の設計プロセスでは、次のテクノロジが採用されました。各テクノロジは、

FlexPod Express Infrastructure 解決策の特定の目的に使用されます。

AFF 9.4 を搭載した NetApp ONTAP A220 シリーズ

この解決策は、 NetApp AFF A220 と ONTAP 9.4 の 2 つの最新ネットアップ製品を活用しています。

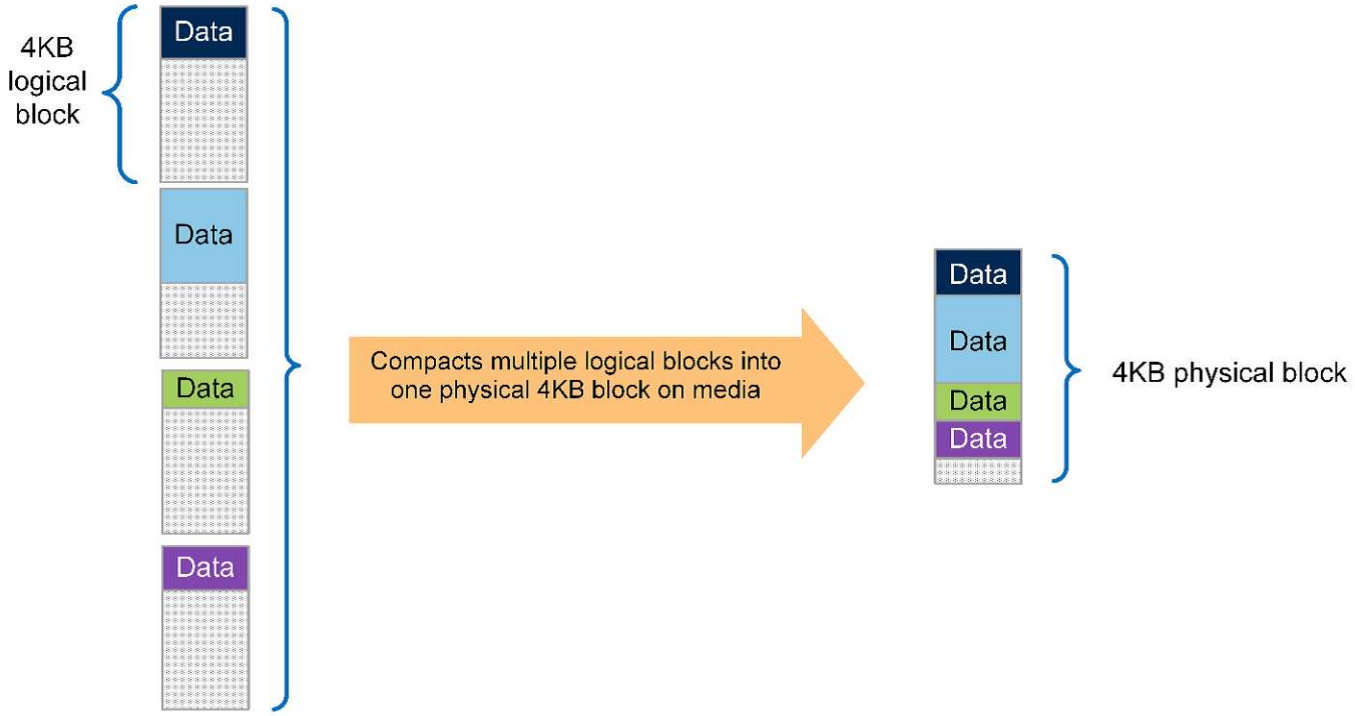
AFF A220 システム

AFF A220 ハードウェアシステムの詳細については、を参照してください "AFF A-Series のホームページ"。

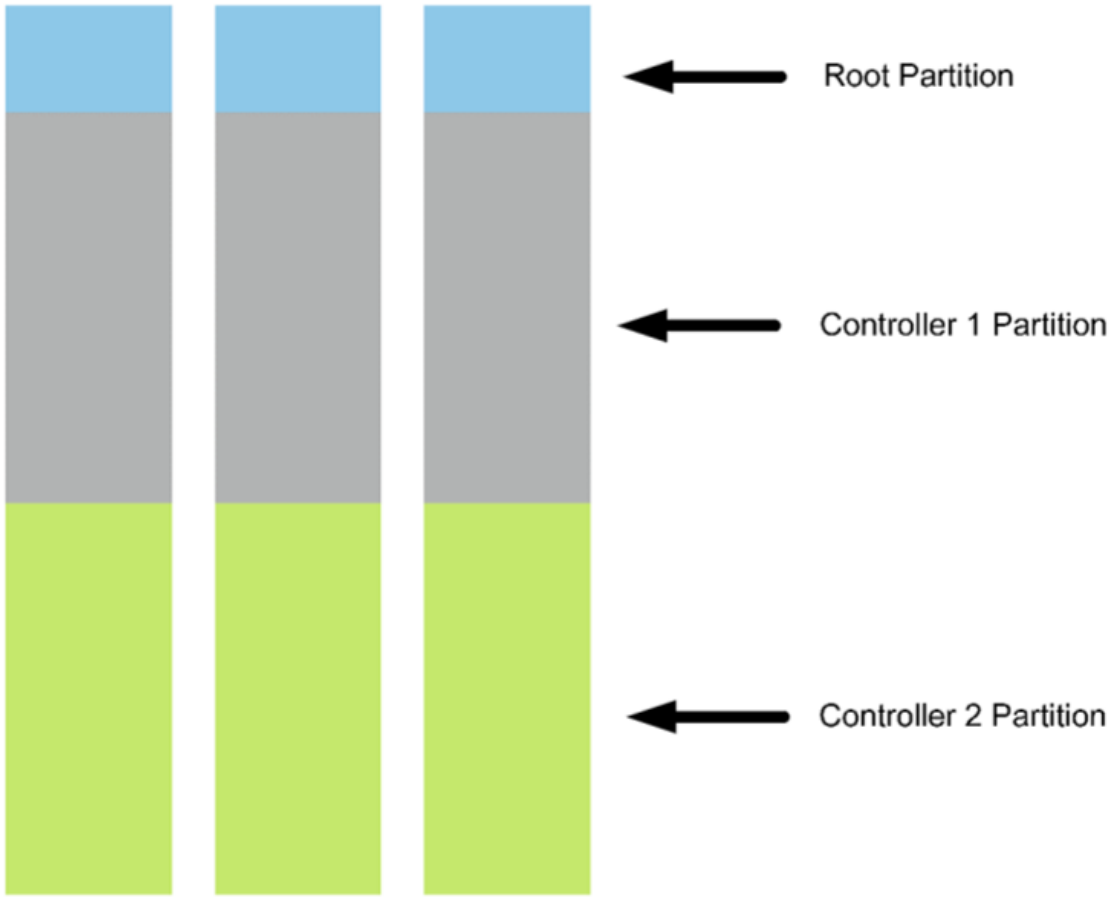
ONTAP 9.4 ソフトウェア

NetApp AFF A220 システムは、新しい ONTAP 9.4 ソフトウェアを使用します。ONTAP 9.4 は、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す。新しいレベルのシンプルさと柔軟性、強力なデータ管理機能、ストレージ効率化機能、業界をリードするクラウド統合機能を兼ね備えています。

ONTAP 9.4 には、 FlexPod Express 解決策に最適な機能がいくつかあります。最も重要なのは、ストレージ効率化に対するネットアップの取り組みです。これは、小規模環境で最も重要な機能の 1 つです。ONTAP 9.4 では、重複排除、圧縮、シンプロビジョニングなどのネットアップの Storage Efficiency 機能に、新たなコンパクション機能が追加されています。NetApp WAFL システムは常に 4KB ブロックを書き込むため、コンパクションでは、ブロックが割り当てられた 4KB のスペースを使用していない場合、複数のブロックが 4KB ブロックにまとめられます。次の図に、このプロセスを示します。



また、ルートデータのパーティショニングは AFF A220 システムでも利用できます。このパーティショニングにより、ルートアグリゲートと 2 つのデータアグリゲートをシステム内のディスクにストライピングできるようになります。したがって、 2 ノードの AFF A220 クラスタの両方のコントローラでは、アグリゲート内のすべてのディスクのパフォーマンスを利用できます。次の図を参照してください。



これらは、 FlexPod Express 解決策を補完するいくつかの主要機能です。ONTAP 9.4 のその他の機能の詳細については、を参照してください "ONTAP 9 データ管理ソフトウェアのデータシート"。また、ネットアップを参照してください "ONTAP 9 ドキュメンテーション・センター"ONTAP 9.4 用に更新されました。

Cisco Nexus 3000 シリーズ

Cisco Nexus 3172P は、 1/10/40/100Gbps スイッチを備えた、堅牢でコスト効率に優れたスイッチです。ユニファイドファブリックファミリの一部である Cisco Nexus 3172PQ スイッチは、トップオブラックのデータセンター環境向けのコンパクトな 1 ラックユニット（ 1RU ）スイッチです。（次の図を参照）。 最大 72 個の 1 / 10GbE ポートを 1RU または 48 個の 1 / 10GbE に搭載し、さらに 6 個の 40GbE ポートを 1RU に搭載しています。また、物理レイヤの柔軟性を最大限に高めるために、 1/10/40Gbps もサポートしています。

すべての Cisco Nexus シリーズモデルは、基盤となる同じオペレーティングシステムである NX-OS を実行するため、 FlexPod Express および FlexPod Datacenter ソリューションでは複数の Cisco Nexus モデルがサポートされます。

パフォーマンスの仕様は次のとおりです。

- すべてのポートでのラインレートトラフィックスループット（レイヤ 2 とレイヤ 3 の両方）
- 最大設定可能な MTU （最大 9216 バイト）（ジャンボフレーム）

Cisco Nexus 3172 スイッチの詳細については、を参照してください "Cisco Nexus 3172PQ 、 3172TQ 、 3172TQ-32T 、 3172PQ-XL 、および 3172TQ-XL スイッチのデータシート"。

Cisco UCS C-Series

Cisco UCS C シリーズラックサーバは FlexPod Express 用に選択されました。多くの設定オプションを使用することで、 FlexPod Express 環境の特定の要件に合わせて調整できます。

Cisco UCS C シリーズラックサーバは、業界標準のフォームファクタでユニファイドコンピューティングを提供し、 TCO の削減と即応性の向上を実現します。

Cisco UCS C シリーズラックサーバには、次のような利点があります。

- フォームファクタに依存しない Cisco UCS へのエントリポイント
- アプリケーションを簡単かつ迅速に導入
- ユニファイドコンピューティングの革新性と利点をラックサーバに拡張
- 使い慣れたラックパッケージに独自のメリットをもたらし、お客様の選択肢を拡大

Cisco UCS C220 M5 ラックサーバ（前の図）は、業界で最も汎用性の高い汎用エンタープライズインフラおよびアプリケーションサーバの 1 つです。高密度の 2 ソケットラックサーバで、仮想化、コラボレーション、ベアメタルなど、さまざまなワークロードに業界最高レベルのパフォーマンスと効率性を提供します。Cisco UCS C シリーズラックサーバは、スタンドアロンサーバとして導入することも、 Cisco UCS の一部として導入することもできます。これにより、シスコの標準ベースのユニファイドコンピューティングの革新的な技術を活用して、お客様の TCO を削減し、ビジネスの俊敏性を高めることができます。

C220 M5 サーバの詳細については、を参照してください "Cisco UCS C220 M5 ラックサーバデータシート"。

C220 M5 ラックサーバ用の接続オプション

C220 M5 ラックサーバの接続オプションは次のとおりです。

- * Cisco UCS VIC 1387 *

  Cisco UCS VIC 1387 （次の図）は、 modular-LAN-on-motherboard （ mLOM ）フォームファクタで、デュアルポート拡張 QSFP+ 40GbE および FC over Ethernet （ FCoE ）を提供します。mLOM スロットは、 Peripheral Component Interconnect Express （ PCIe ）スロットを使用せずに Cisco VIC を取り付けるために使用できるため、 I/O の拡張性が向上します。

Cisco UCS VIC 1387 アダプタの詳細については、を参照してください "Cisco UCS 仮想インターフェイスカード 1387" データシート：

- * CVR-QSFP-SFP10G アダプタ *

  Cisco QSA モジュールは QSFP ポートを SFP または SFP+ ポートに変換します。このアダプタを使用すると、任意の SFP+ または SFP モジュールまたはケーブルを使用して、ネットワークの反対側の低速ポートに接続できます。この柔軟性により、高密度の 40GbE QSFP プラットフォームを最大限に活用することで、コスト効率の高い 40GbE への移行が可能になります。このアダプタは、 SFP+ 光ファイバとケーブル接続をすべてサポートし、複数の 1GbE SFP モジュールをサポートします。このプロジェクトは 10GbE 接続を使用して検証されており、 VIC 1387 が 40GbE で使用されているため、 CVR-QSFP-SFP10G アダプタ（次の図）が変換に使用されます。

VMware vSphere 6.7

VMware vSphere 6.7 は、 FlexPod Express で使用するハイパーバイザーオプションの 1 つです。VMware vSphere を使用すると、購入したコンピューティング容量が十分に使用されていることを確認しながら、組織の電力および冷却のフットプリントを削減できます。また、 VMware vSphere を使用すると、ハードウェア障害からの保護（ VMware High Availability 、 VMware HA ）が可能になり、 vSphere ホストのクラスタ全体（ VMware Distributed Resource Scheduler 、 VMware DRS ）でリソースの負荷分散を計算できます。

VMware vSphere 6.7 では、カーネルのみが再起動されるため、ハードウェアを再起動することなく、

vSphere ESXi をロードする場所で「クイックブート」を実行できます。この機能は、 Quick Boot ホワイトリストにあるプラットフォームとドライバでのみ使用できます。vSphere 6.7 では、 vSphere Client の機能が拡張され、 vSphere Web Client の機能の約 90% を使用できます。

vSphere 6.7 では、 VMware がこの機能を拡張して、ホスト単位ではなく、 Enhanced vMotion Compatibility （ EVC ）を仮想マシン（ VM ）単位で設定できるようにしました。vSphere 6.7 でも、 VMware はインスタントクローンの作成に使用できる API を公開しています。

vSphere 6.7 U1 の機能には、次のようなものがあります。

- すべての機能を備えた HTML5 Web ベース vSphere Client です
- NVIDIA GRID vGPU VM の vMotionインテル ® FPGA のサポート。
- vCenter Server Converge Tool で、外部 PSC から内部 PCS への移行が実施されました。
- VSAN （ HCI の更新）の機能拡張
- 強化されたコンテンツ・ライブラリ

vSphere 6.7 U1 の詳細については、を参照してください "vCenter Server 6.7 Update 1 の新機能"。この解決策は vSphere 6.7 で検証済みですが、他のコンポーネントとの互換性を確認する任意の vSphere バージョンを NetApp Interoperability Matrix Tool でサポートします。ネットアップでは、 vSphere 6.7U1 を修正機能と拡張機能として導入することを推奨します。

ブートアーキテクチャ

FlexPod Express ブートアーキテクチャでサポートされているオプションは次のとおりです。

- iSCSI SAN LUN
- Cisco FlexFlash SD カード
- ローカルディスク

FlexPod データセンターは iSCSI LUN からブートされるため、 FlexPod の管理性も解決策 Express の iSCSI ブートを使用して強化されます。

"次：解決策の検証："

解決策の検証

Cisco とネットアップは、お客様にとって最高のインフラプラットフォームとして機能するように設計、構築された FlexPod Express を提供しています。業界をリードするコンポーネントで設計されているため、お客様は FlexPod Express をインフラ基盤として信頼できます。FlexPod ポートフォリオの基本原則に従い、 FlexPod Express アーキテクチャは、シスコおよびネットアップのデータセンターアーキテクトおよびエンジニアによって徹底的にテストされました。冗長性と可用性から個々の機能に至るまで、 FlexPod Express アーキテクチャ全体が検証され、お客様の信頼を獲得し、設計プロセスに信頼を築きます。

VMware vSphere 6.7 は、 FlexPod Express インフラコンポーネントで検証済みです。この検証では、ハイパーバイザー用の 10GbE アップリンク接続オプションを使用しました。

"次は終わりです"

まとめ

FlexPod Express は、業界をリードするコンポーネントを使用した検証済みの設計を提供することで、シンプルで効果的な解決策を実現します。拡張性を備え、ハイパーバイザープラットフォームにオプションを提供することで、 FlexPod Express は特定のビジネスニーズに合わせてカスタマイズできます。FlexPod Express は、中小規模の企業、リモートオフィスやブランチオフィスなど、特定用途向けのソリューションを必要とする企業を念頭に置いて設計されています。

"次へ：追加情報の検索場所。"

追加情報の参照先

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、次のドキュメントおよび Web サイトを参照してください。

- NetApp のドキュメント

  "https://docs.netapp.com"

- 『 FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 Deployment Guide 』

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

『 FlexPod Express with Cisco UCS C Series and AFF A220 Series Deployment Guide 』

NVA-1123-deploy ： FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 deployment guide 』

ネットアップ、 Savita Kumari 氏

協力：

業界のトレンドは、共有インフラとクラウドコンピューティングへの大規模なデータセンターの移行を示しています。さらに、リモートオフィスやブランチオフィスにもシンプルで効果的な解決策を導入し、データセンターでよく使用されているテクノロジを活用することができます。

FlexPod Express は、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus ファミリースイッチ、およびネットアップストレージテクノロジを基盤とした、事前設計されたベストプラクティスのデータセンターアーキテクチャです。FlexPod Express システムのコンポーネントは、 FlexPod Datacenter と同様

に、小規模な IT インフラ環境全体での管理面の相乗効果を実現します。FlexPod Datacenter と FlexPod Express は、仮想化に最適なプラットフォームで、ベアメタルのオペレーティングシステムやエンタープライズワークロードに最適です。

FlexPod Datacenter と FlexPod Express は、ベースライン構成が可能で、多種多様なユースケースや要件に対応できるよう、サイズ設定と最適化が可能な柔軟性を備えています。FlexPod データセンターを利用している既存のお客様は、使い慣れたツールを使用して FlexPod Express システムを管理できます。FlexPod Express の新規のお客様は、環境の拡大に合わせて FlexPod データセンターの管理を容易に行うことができます。

FlexPod Express は、リモートオフィス、ブランチオフィス、中堅企業に最適なインフラ基盤です。また、専用のワークロードにインフラを提供したいお客様にも最適な解決策です。

FlexPod Express は、ほぼすべてのワークロードに適した、管理しやすいインフラを提供します。

解決策の概要

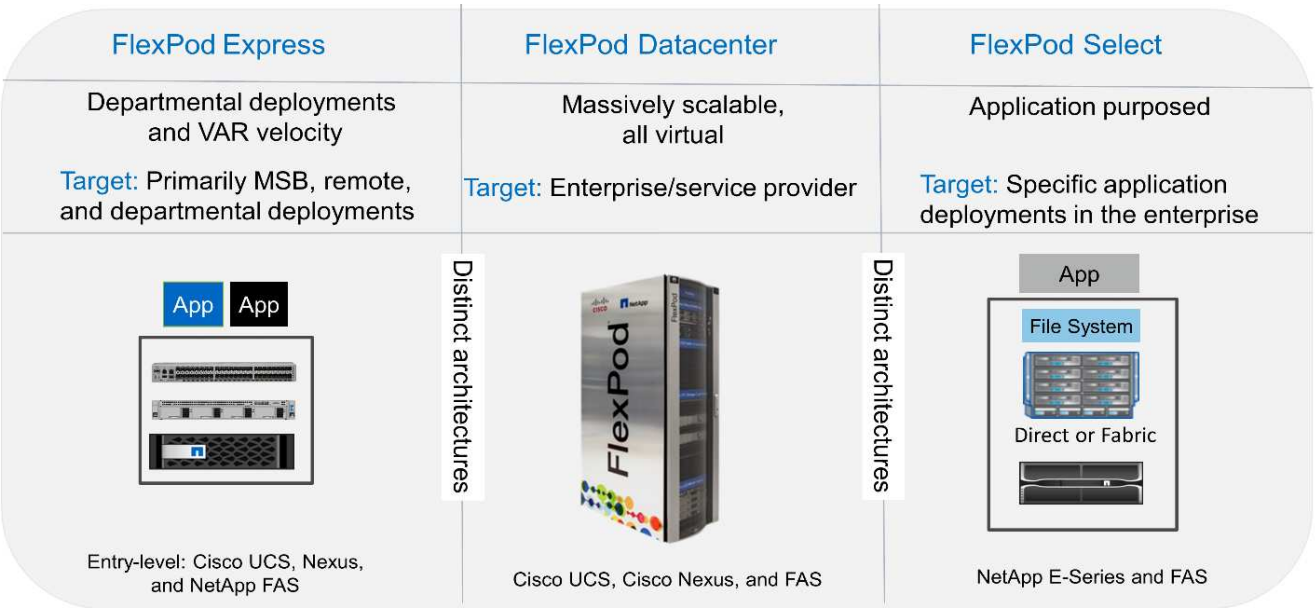
この FlexPod Express 解決策は、 FlexPod コンバージドインフラプログラムの一部です。

FlexPod 統合インフラプログラム

FlexPod リファレンスアーキテクチャは、 Cisco Validated Design （ CVD ；シスコ検証済み設計）または NetApp Verified Architectures （ NVA ；ネットアップ検証済みアーキテクチャ）として提供されます。これらのバリエーションでサポートされない構成が作成されない場合、特定の CVD または NVA からのお客様の要件に基づく差異は認められます。

次の図に示すように、 FlexPod プログラムには、 FlexPod Express 、 FlexPod Datacenter 、 FlexPod Select の 3 つのソリューションが含まれています。

- * FlexPod Express. * は、 Cisco とネットアップが提供するテクノロジを搭載したエントリレベルの解決策をお客様に提供します。
- * FlexPod * Datacenter * は、さまざまなワークロードやアプリケーションに最適な多目的基盤を提供します。
- * FlexPod Select * は、 FlexPod データセンターの最良の側面を組み込み、特定のアプリケーションにインフラストラクチャを調整します。



NetApp Verified Architecture プログラム

NetApp Verified Architecture プログラムは、ネットアップソリューションの検証済みアーキテクチャを提供するものです。NetApp Verified Architecture は、 NetApp 解決策アーキテクチャに次の品質を提供します。

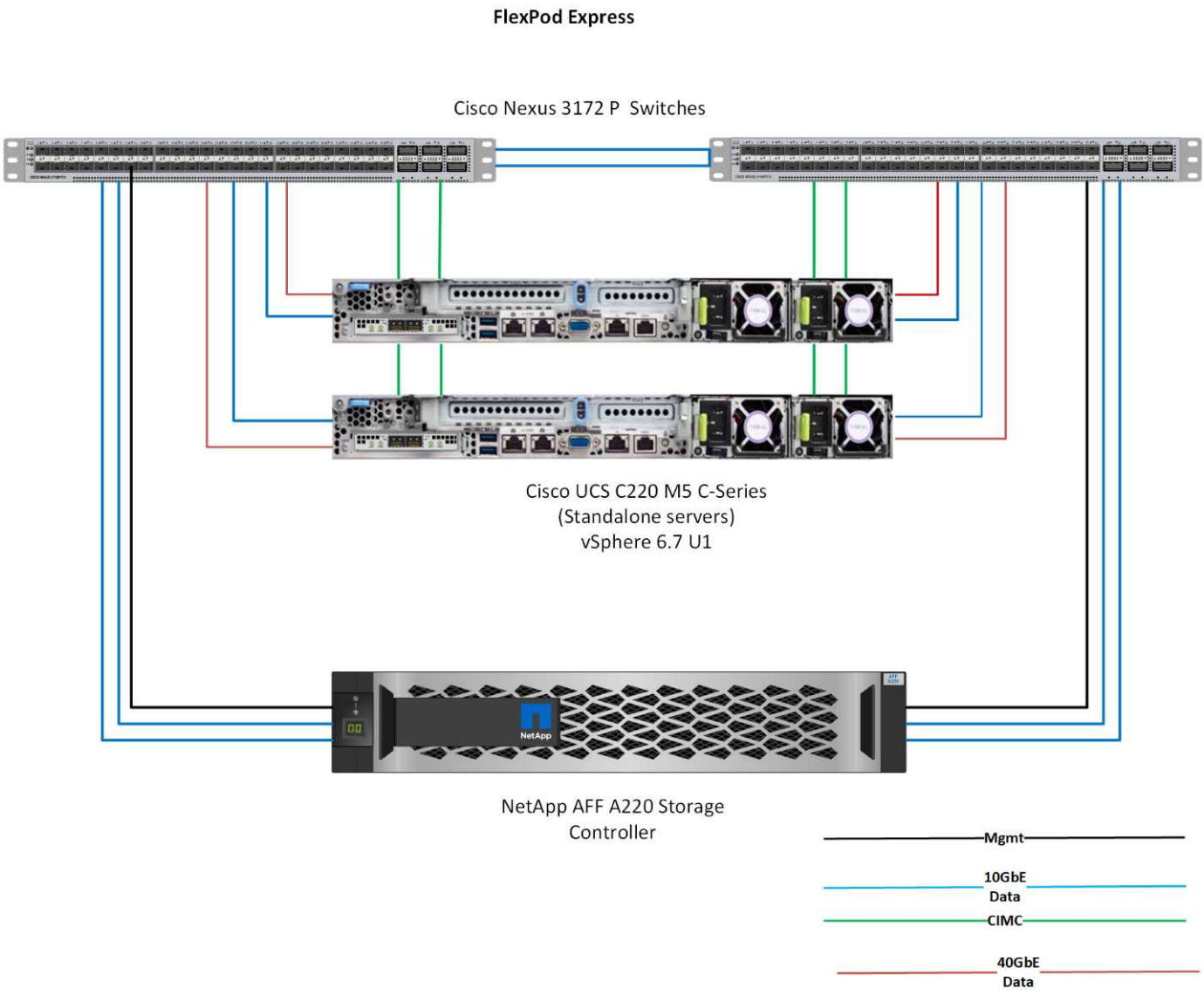
- 入念にテストされています
- あらかじめ規定されている
- 導入リスクを最小限に抑えます
- 運用開始までの時間を短縮

このガイドでは、 VMware vSphere を使用した FlexPod Express の設計について詳しく説明します。また、この設計では、 NetApp ONTAP 9.4 、 Cisco Nexus 3172P 、 Cisco UCS C シリーズ C220 M5 サーバをハイパーバイザーノードとして実行する、まったく新しい AFF A220 システムを使用します。

解決策テクノロジ

この解決策は、ネットアップ、 Cisco 、 VMware の最新テクノロジを活用しています。この解決策は、ONTAP 9.4 を実行する新しい NetApp AFF A220 、デュアル構成の Cisco Nexus 3172P スイッチ、および VMware vSphere 6.7 を実行する Cisco UCS C220 M5 ラックサーバを搭載しています。この検証済み解決策は 10GbE テクノロジを使用しています。また、 FlexPod Express アーキテクチャが組織の進化するビジネスニーズに適応できるように、 2 つのハイパーバイザノードを一度に追加することでコンピューティング容量を拡張する方法についても説明します。

次の図は、 FlexPod Express と VMware vSphere 10GbE アーキテクチャを示しています。



この検証では、 10GbE 接続と、 40GbE である Cisco UCS VIC 1387 を使用します。10GbE 接続を実現するために、 CVR-QSFP-SFP10G アダプタを使用します。

ユースケースの概要

FlexPod Express 解決策は、次のようないくつかのユースケースに適用できます。

- リモートオフィスまたはブランチオフィス
- 中堅・中小企業向け
- コスト効率に優れた専用の解決策が必要な環境

FlexPod Express は、仮想ワークロードと混在ワークロードに最適です。

この解決策は vSphere 6.7 で検証済みですが、他のコンポーネントとの互換性を確認する任意の vSphere バージョンを NetApp Interoperability Matrix Tool でサポートします。ネットアップでは、 vSphere 6.7U1 を修正機能と拡張機能として導入することを推奨します。

vSphere 6.7 U1 の機能には、次のものがあります。

- すべての機能を備えた HTML5 Web ベース vSphere Client です
- NVIDIA GRID vGPU VM の vMotionインテル ® FPGA のサポート
- vCenter Server Converge Tool で、外部 PSC から内部 PCS への移行が実施されました
- vSAN に関する機能拡張（ HCI の更新）
- 強化されたコンテンツ・ライブラリ

vSphere 6.7 U1 の詳細については、を参照してください "vCenter Server 6.7 Update 1 の新機能"。

テクノロジ要件

FlexPod Express システムには、ハードウェアコンポーネントとソフトウェアコンポーネントを組み合わせて使用する必要があります。FlexPod Express では、システムにハイパーバイザーノードを追加するために必要なハードウェアコンポーネントについても、 2 つのユニット単位で説明します。

ハードウェア要件

選択したハイパーバイザーに関係なく、すべての FlexPod Express 構成で同じハードウェアが使用されます。そのため、ビジネス要件が変わっても、どちらのハイパーバイザーも同じ FlexPod Express ハードウェア上で実行できます。

次の表に、すべての FlexPod 構成に必要なハードウェアコンポーネントを示します。

ハードウェア	数量
AFF A220 HA ペア	1.
Cisco C220 M5 サーバ	2.
Cisco Nexus 3172P スイッチ	2.
C220 M5 サーバ用の Cisco UCS 仮想インターフェイスカード（ VIC ） 1387	2.
CVR-QSFP-SFP10G アダプタです	4.

次の表に、 10GbE を実装する場合の基本構成に加えて、必要なハードウェアを示します。

ハードウェア	数量
Cisco UCS C220 M5 サーバ	2.
Cisco VIC 1387	2.
CVR-QSFP-SFP10G アダプタです	4.

ソフトウェア要件

次の表に、 FlexPod Express ソリューションのアーキテクチャを実装するために必要なソフトウェアコンポーネントを示します。

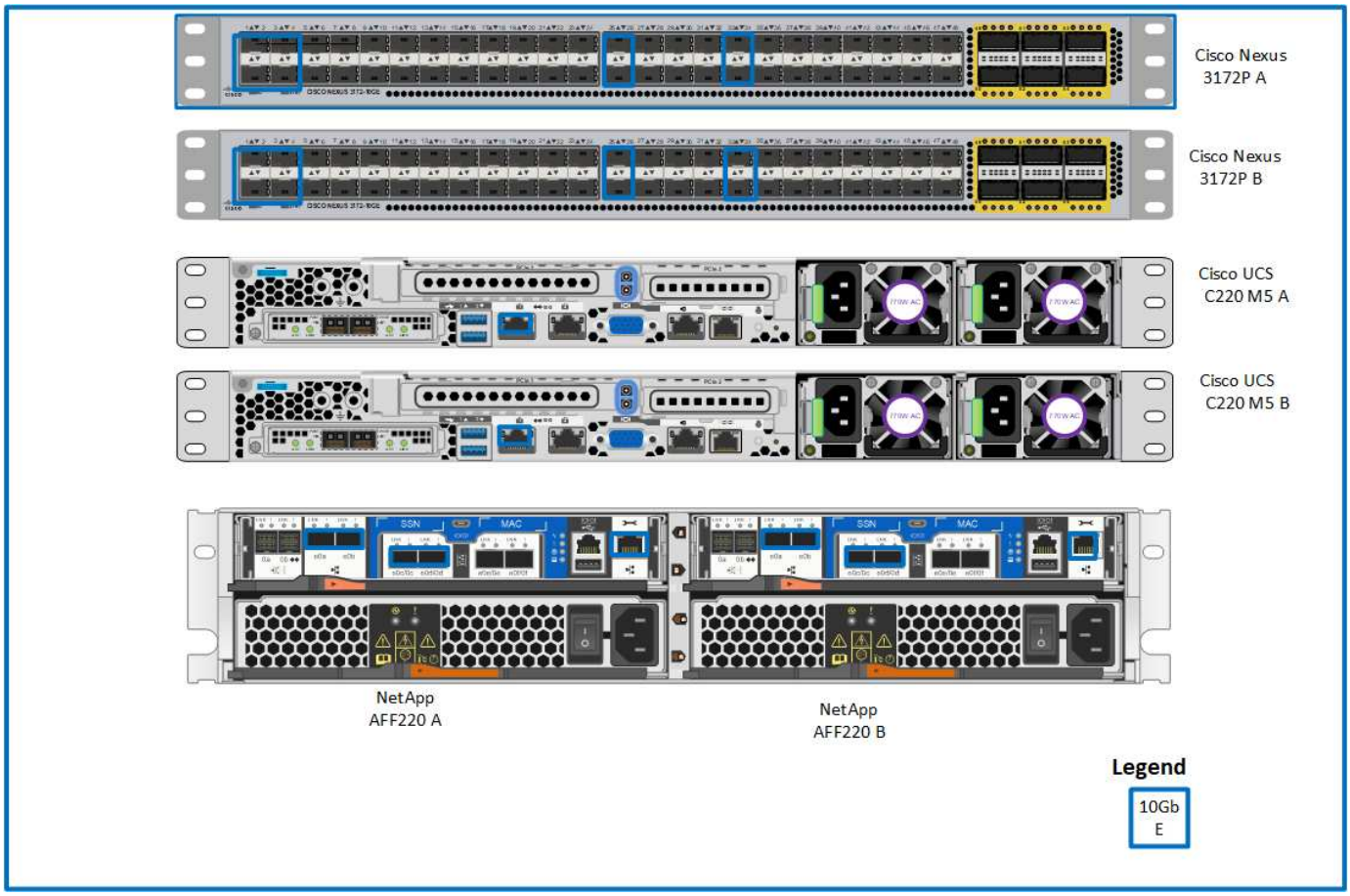
ソフトウェア	バージョン	詳細
Cisco Integrated Management Controller （ CIMC ）	3.1 （ 3G ）	Cisco UCS C220 M5 ラックサーバの場合
Cisco nenic ドライバ	1.0.25.0	VIC 1387 インターフェイスカード用
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Cisco Nexus 3172P スイッチの場合
NetApp ONTAP	9.4	AFF A220 コントローラの場合

次の表に、 FlexPod Express でのすべての VMware vSphere の実装に必要なソフトウェアを示します。

ソフトウェア	バージョン
VMware vCenter Server Appliance の略	6.7
VMware vSphere ESXi ハイパーバイザー	6.7
NetApp VAAI Plug-in for ESXi	1.1.2

FlexPod エクスプレスケーブル接続情報

次の図に、リファレンス検証のケーブル接続を示します。



次の表に、 Cisco Nexus スイッチ 3172P A のケーブル接続情報を示します

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
Cisco Nexus スイッチ 3172P A	Eth1/1	NetApp AFF A220 ストレージコントローラ A	e0c
	Eth1/2	NetApp AFF A220 ストレージコントローラ B	e0c
	Eth1/3	Cisco UCS C220 C シリーズスタンドアロンサーバ A	CVR-QSFP-SFP10G アダプタ搭載の MLOM1
	Eth1/4	Cisco UCS C220 C シリーズスタンドアロンサーバ B	CVR-QSFP-SFP10G アダプタ搭載の MLOM1
	Eth1/25	Cisco Nexus スイッチ 3172P B	Eth1/25
	Eth1/26	Cisco Nexus スイッチ 3172P B	Eth1/26
	Eth1/33	NetApp AFF A220 ストレージコントローラ A	e0M
	Eth1/34	Cisco UCS C220 C シリーズスタンドアロンサーバ A	CIMC

次の表に、 Cisco Nexus スイッチ 3172P B のケーブル接続情報を示します

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
Cisco Nexus スイッチ 3172P B	Eth1/1	NetApp AFF A220 ストレージコントローラ A	e0d
	Eth1/2	NetApp AFF A220 ストレージコントローラ B	e0d
	Eth1/3	Cisco UCS C220 C シリーズスタンドアロンサーバ A	CVR-QSFP-SFP10G アダプタ搭載の MLOM2
	Eth1/4	Cisco UCS C220 C シリーズスタンドアロンサーバ B	CVR-QSFP-SFP10G アダプタ搭載の MLOM2
	Eth1/25	Cisco Nexus スイッチ 3172P A	Eth1/25
	Eth1/26	Cisco Nexus スイッチ 3172P A	Eth1/26
	Eth1/33	NetApp AFF A220 ストレージコントローラ B	e0M
	Eth1/34	Cisco UCS C220 C シリーズスタンドアロンサーバ B	CIMC

次の表に、 NetApp AFF A220 ストレージコントローラ A のケーブル接続情報を示します

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
NetApp AFF A220 ストレージコントローラ A	e0a	NetApp AFF A220 ストレージコントローラ B	e0a
	e0b	NetApp AFF A220 ストレージコントローラ B	e0b
	e0c	Cisco Nexus スイッチ 3172P A	Eth1/1
	e0d	Cisco Nexus スイッチ 3172P B	Eth1/1
	e0M	Cisco Nexus スイッチ 3172P A	Eth1/33

次の表に、 NetApp AFF A220 ストレージコントローラ B のケーブル接続情報を示します

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
NetApp AFF A220 ストレージコントローラ B	e0a	NetApp AFF A220 ストレージコントローラ A	e0a
	e0b	NetApp AFF A220 ストレージコントローラ A	e0b
	e0c	Cisco Nexus スイッチ 3172P A	Eth1/2
	e0d	Cisco Nexus スイッチ 3172P B	Eth1/2
	e0M	Cisco Nexus スイッチ 3172P B	Eth1/33

導入手順

このドキュメントでは、完全な冗長性と高可用性を備えた FlexPod Express システムの構成について詳しく説明します。この冗長性を反映するために、各手順で設定するコンポーネントをコンポーネント A またはコンポーネント B と呼びますたとえば、このドキュメントでプロビジョニングされている 2 台のネットアップストレージコントローラは、コントローラ A とコントローラ B で識別されます。スイッチ A とスイッチ B は Cisco Nexus スイッチのペアを表します。

また、このドキュメントでは、複数の Cisco UCS ホストをプロビジョニングする手順についても説明します。これらのホストは、サーバ A 、サーバ B などとして順次識別されます。

環境に関連する情報をステップに含める必要があることを示すために、コマンド構造の一部として「 \ <text>> 」が表示されます。「 vlan create 」コマンドについては、次の例を参照してください。

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

本ドキュメントでは、 FlexPod Express 環境を完全に構成する方法について説明します。このプロセスでは、さまざまな手順で、お客様固有の命名規則、 IP アドレス、および VLAN （仮想 LAN ）スキームを入力する必要があります。次の表に、このガイドで説明する導入に必要な VLAN を示します。このテーブルは、特定のサイト変数に基づいて作成し、ドキュメントの設定手順を実装するために使用できます。

> 別々のインバンド管理 VLAN とアウトオブバンド管理 VLAN を使用する場合は、それらの間にレイヤ 3 ルートを作成する必要があります。この検証では、共通の管理 VLAN を使用しました。

AN 名	**VLAN** の目的	このドキュメントの検証で使用された **ID**
管理 VLAN	管理インターフェイス用の VLAN	3437
ネイティブ VLAN	タグなしフレームが割り当てられている VLAN	2.
NFS VLAN	NFS トラフィック用の VLAN	3438
VMware vMotion VLAN	ある物理ホストから別の物理ホストへの仮想マシンの移動用に指定された VLAN	3441
仮想マシンのトラフィック VLAN	仮想マシンアプリケーショントラフィック用の VLAN	3442
iSCSI-A VLAN	ファブリック A の iSCSI トラフィック用 VLAN	3439
iSCSI-B VLAN	ファブリック B の iSCSI トラフィック用 VLAN	3440

VLAN 番号は、 FlexPod Express の設定全体で必要になります。VLAN は「 <<var_xxxx_vlan>> 」と呼ばれます。「 xxxx 」は VLAN の目的（ iSCSI-A など）です。

次の表は、作成された VMware 仮想マシンを示しています。

仮想マシンの概要	ホスト名
VMware vCenter Server の各機能を使用し	

Cisco Nexus 3172P Deployment 手順の略

次のセクションでは、 FlexPod Express 環境で使用する Cisco Nexus 3172P スイッチの構成について詳しく説明します。

Cisco Nexus 3172P スイッチの初期セットアップ

次の手順では、 FlexPod Express の基本環境で使用するように Cisco Nexus スイッチを設定する方法について説明します。

この手順は、 NX-OS ソフトウェアリリース 7.0(3) i7(5) を実行している Cisco Nexus 3172P を使用していることを前提としています。

1. スイッチのコンソールポートを最初にブートして接続すると、 Cisco NX-OS セットアップが自動的に開始されます。この初期構成では、スイッチ名、 mgmt0 インターフェイス構成、および Secure Shell （ SSH ）セットアップなどの基本的な設定を行います。
2. FlexPod Express 管理ネットワークは、さまざまな方法で構成できます。3172P スイッチ上の mgmt0 インターフェイスは、既存の管理ネットワークに接続することも、バックツーバック構成で 3172P スイッチの mgmt0 インターフェイスを接続することもできます。ただし、このリンクは、 SSH トラフィックなどの外部管理アクセスには使用できません。

   この導入ガイドでは、 FlexPod Express Cisco Nexus 3172P スイッチを既存の管理ネットワークに接続しています。

3. Cisco Nexus 3172P スイッチを設定するには、スイッチの電源をオンにし、画面の指示に従います。ここでは、両方のスイッチの初期セットアップを示しますが、スイッチ固有の情報については適切な値に置き換えてください。

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

4. 設定の概要が表示され、編集するかどうかの確認を求められます。設定が正しい場合は、「n」と入力します。

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. その後、この設定を使用するかどうかを確認するメッセージが表示され、保存します。その場合は、「y」と入力します。

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus スイッチ B について、この手順を繰り返します

高度な機能を有効にします

追加の設定オプションを提供するには、 Cisco NX-OS で特定の高度な機能をイネーブルにする必要があります。

> 「 interface-vlan 」機能は、このマニュアル全体で説明されている「 back-to-back 」「 m Mgmt0 」オプションを使用する場合にのみ必要です。この機能を使用すると、インターフェイス VLAN （スイッチ仮想インターフェイス）に IP アドレスを割り当てることができます。これにより、スイッチへのインバンド管理通信（ SSH 経由など）が可能になります。

1. Cisco Nexus スイッチ A およびスイッチ B で適切な機能をイネーブルにするには、コマンド「（ config t ）」を使用してコンフィギュレーションモードを開始し、次のコマンドを実行します。

```
feature interface-vlan
feature lacp
feature vpc
```

   ポートチャネルのデフォルトのロードバランシングハッシュでは、ソースおよびデスティネーションの IP アドレスを使用して、ポートチャネルのインターフェイス全体のロードバランシングアルゴリズムを決定します。ハッシュアルゴリズムにソースおよびデスティネーションの IP アドレス以外にもデータを提供することで、ポートチャネルのメンバー全体へのより均等なロードバランシングを実現できます。同じ理由から、ソースおよびデスティネーションの TCP ポートをハッシュアルゴリズムに追加することを推奨します。

2. 構成モード（ config t ）から次のコマンドを入力し、 Cisco Nexus スイッチ A およびスイッチ B のグローバルポートチャネルロードバランシング設定を行います。

```
port-channel load-balance src-dst ip-l4port
```

グローバルスパニングツリーコンフィギュレーションを実行します。

Cisco Nexus プラットフォームでは、ブリッジアシュアランスと呼ばれる新しい保護機能を使用します。ブリッジアシュアランスは、スパニングツリーアルゴリズムを実行していないデバイスでデータトラフィックの転送を継続する単方向リンクやその他のソフトウェア障害から保護するのに役立ちます。ポートは、プラットフォームに応じて、ネットワークやエッジなどのいくつかの状態のいずれかに配置できます。

すべてのポートがデフォルトでネットワークポートとみなされるように、ブリッジアシュアランスを設定することを推奨します。この設定により、ネットワーク管理者は各ポートの設定を確認することになります。また、未識別のエッジポートや、ブリッジアシュアランス機能が有効になっていないネイバーなど、最も一般的な構成エラーも表示されます。また、スパニングツリーでブロックするポートの数が少なすぎない方が、多くのポートをブロックする方が安全で、デフォルトのポートの状態でネットワーク全体の安定性を高めることができます。

サーバ、ストレージ、アップリンクスイッチを追加するときは、スパニングツリーの状態に細心の注意を払ってください。追加する構成がブリッジアシュアランスをサポートしていない場合は特に注意が必要です。このような場合は、ポートをアクティブにするためにポートタイプの変更が必要になることがあります。

Bridge Protocol Data Unit （ BPDU; ブリッジプロトコルデータユニット）ガードは、別の保護レイヤとしてデフォルトでエッジポートでイネーブルになっています。ネットワーク内のループを防止するために、このインターフェイス上で BPDU が別のスイッチから受信された場合、この機能はポートをシャットダウンします。

Cisco Nexus スイッチ A およびスイッチ B で、構成モード（「 config t 」）から次のコマンドを実行し、デフォルトのポートタイプや BPDU ガードなどのデフォルトのスパニングツリーオプションを設定します。

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

VLAN を定義します

VLAN の異なるポートを個別に設定する前に、スイッチ上にレイヤ 2 VLAN を定義する必要があります。また、 VLAN に名前を付けておくと、今後のトラブルシューティングを簡単に行うことができます。

コンフィギュレーションモード（ config t` ）から次のコマンドを実行して、 Cisco Nexus スイッチ A およびスイッチ B 上のレイヤ 2 VLAN を定義し、説明します。

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

アクセスポートと管理ポートの説明を設定します

レイヤ 2 VLAN に名前を割り当てる場合と同様に、すべてのインターフェイスに説明を設定すると、プロビジョニングとトラブルシューティングの両方に役立ちます。

各スイッチの構成モード（ config t ）から、 FlexPod Express の大規模構成の次のポート説明を入力します。

Cisco Nexus スイッチ A

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus スイッチ **B**

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

サーバおよびストレージの管理インターフェイスを設定します

サーバとストレージの管理インターフェイスで使用する VLAN は、通常、どちらも 1 つだけです。そのため、管理インターフェイスポートをアクセスポートとして設定します。各スイッチの管理 VLAN を定義し、スパニングツリーポートタイプをエッジに変更します。

構成モード（ config t ）から次のコマンドを入力して、サーバとストレージの両方の管理インターフェイスのポート設定を行います。

Cisco Nexus スイッチ A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus スイッチ B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

仮想ポートチャネルのグローバル設定を実行します

仮想ポートチャネル（ vPC ）を使用すると、 2 つの異なる Cisco Nexus スイッチに物理的に接続されたリンクを、 3 番目のデバイスに対する単一のポートチャネルとして認識できます。3 番目のデバイスには、スイッチ、サーバ、またはその他のネットワークデバイスを使用できます。vPC はレイヤ 2 マルチパスを提供します。これにより、帯域幅を増やし、ノード間で複数のパラレルパスを有効にし、代替パスが存在する場合はトラフィックをロードバランシングすることで、冗長性を確保できます。

vPC には次の利点があります。

- 1 つのデバイスが 2 つのアップストリームデバイス間でポートチャネルを使用できるようにする
- スパニングツリープロトコルのブロックポートの排除
- ループフリートポロジを提供する
- 使用可能なすべてのアップリンク帯域幅を使用する
- リンクまたはデバイスのいずれかに障害が発生した場合に、高速コンバージェンスを提供します
- リンクレベルの耐障害性を提供します
- 高可用性の実現を支援します

vPC 機能を正しく機能させるには、 2 つの Cisco Nexus スイッチ間でいくつかの初期セットアップを行う必要があります。バックツーバックの mgmt0 構成を使用する場合は、インターフェイスに定義されたアドレスを使用し、 ping を使用してそれらのアドレスが通信できることを確認します[switch_A/B_mgmt0_ip_addr]vrf' management コマンド

構成モード（ config t ）から次のコマンドを実行し、両方のスイッチの vPC グローバル構成を設定します。

Cisco Nexus スイッチ A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus スイッチ B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

ストレージポートチャネルを設定します

ネットアップストレージコントローラでは、 Link Aggregation Control Protocol （ LACP ）を使用してネットワークにアクティブ / アクティブ接続できます。LACP は、スイッチ間でネゴシエーションとロギングの両方を行うため、 LACP の使用を推奨します。ネットワークは vPC 用に設定されているため、ストレージからのアクティブ / アクティブ接続を可能にして、別々の物理スイッチに接続できます。各コントローラには、各スイッチへのリンクが 2 つあります。ただし、 4 つのリンクすべてが同じ vPC とインターフェイスグループ（ ifgrp ）に属します。

構成モード（ config t ）から各スイッチに対して次のコマンドを実行し、個々のインターフェイスと、NetApp AFF コントローラに接続されたポートのポートチャネル構成を設定します。

1. スイッチ A およびスイッチ B で次のコマンドを実行して、ストレージコントローラ A のポートチャネルを設定します。

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. スイッチ A とスイッチ B で次のコマンドを実行して、ストレージコントローラ B のポートチャネルを設定します

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

この解決策検証では、 9 、 000 の MTU が使用されています。ただし、アプリケーションの要件に基づいて、適切な MTU 値を設定できます。FlexPod 解決策全体で同じ MTU 値を設定することが重要です。コンポーネント間の MTU 設定が正しくないと、パケットが破棄されてこれらのパケットが破棄されます。

サーバ接続を設定します

Cisco UCS サーバには 2 ポートの仮想インターフェイスカード VIC1387 があり、 iSCSI を使用した ESXi オペレーティングシステムのデータトラフィックおよびブートに使用されます。これらのインターフェイスは互いにフェイルオーバーするように設定されているため、単一リンク以上の冗長性が追加されます。これらのリンクを複数のスイッチに分散させることで、あるスイッチが完全に停止した場合でもサーバの運用を継続する

ことができます。

構成モード（ config t ）から次のコマンドを実行して、各サーバに接続されているインターフェイスのポート設定を行います。

Cisco Nexus スイッチ **A** ： **Cisco UCS** サーバ **A** と **Cisco UCS** サーバ **B** の構成

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

Cisco Nexus スイッチ **B** ： **Cisco UCS** サーバ **A** および **Cisco UCS** サーバ **B** の構成

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

この解決策検証では、 9 、 000 の MTU が使用されています。ただし、アプリケーションの要件に基づいて、適切な MTU 値を設定できます。FlexPod 解決策全体で同じ MTU 値を設定することが重要です。コンポーネント間の MTU 設定が正しくないと、パケットが破棄され、これらのパケットを再送信する必要があります。これは、解決策の全体的なパフォーマンスに影響します。

Cisco UCS サーバを追加して解決策を拡張するには、新しく追加したサーバがスイッチ A および B に接続されているスイッチポートを使用して、上記のコマンドを実行します

既存のネットワークインフラへのアップリンク

使用可能なネットワークインフラに応じて、 FlexPod 環境をアップリンクするためのいくつかの方法や機能があります。既存の Cisco Nexus 環境がある場合は、 vPC を使用して、 FlexPod 環境に含まれている Cisco Nexus 3172P スイッチをインフラにアップリンクすることを推奨します。必要に応じて、 10GbE インフラ解決策の場合は 10GbE アップリンク、 1GbE インフラ解決策の場合は 1GbE アップリンクが使用されます。前

述の手順を使用して、既存の環境へのアップリンク vPC を作成できます。設定が完了したら、必ず copy run start を実行して各スイッチに設定を保存してください。

"次のセクション：『 NetApp Storage Deployment 手順』（パート 1 ）"

ネットアップストレージ導入手順（パート **1** ）

このセクションでは、 NetApp AFF ストレージ導入手順について説明します。

NetApp ストレージコントローラ **AFF2xx** シリーズのインストール

NetApp Hardware Universe の略

NetApp Hardware Universe （ HWU ）アプリケーションは、特定の ONTAP バージョンでサポートされているハードウェアコンポーネントとソフトウェアコンポーネントを提供します。ONTAP ソフトウェアで現在サポートされているネットアップのすべてのストレージアプライアンスに関する構成情報を提供します。また、コンポーネントの互換性の表も示します。

使用するハードウェアコンポーネントとソフトウェアコンポーネントが、インストールする ONTAP のバージョンでサポートされていることを確認します。

1. にアクセスします "HWU" システム設定ガイドを表示するアプリケーション。コントローラタブをクリックして、 ONTAP ソフトウェアの異なるバージョンとネットアップストレージアプライアンスの互換性を必要な仕様で確認します。
2. または、ストレージアプライアンス別にコンポーネントを比較するには、ストレージシステムの比較をクリックします。

コントローラ **AFF2XX** シリーズの前提条件
ストレージシステムの物理的な場所を計画するには、 NetApp Hardware Universe を参照してください。次のセクションを参照してください。電力要件、サポートされる電源コード、およびオンボードポートとケーブル

ストレージコントローラ

のコントローラの物理的な設置手順に従います "AFF A220 のドキュメント"。

NetApp ONTAP 9.4

設定ワークシート

セットアップスクリプトを実行する前に、製品マニュアルから構成ワークシートに情報を記入してください。設定ワークシートは、で使用できます "ONTAP 9.4 ソフトウェアセットアップガイド"。

このシステムは、 2 ノードスイッチレスクラスタ構成でセットアップされます。

次の表に、 ONTAP 9.4 のインストールと設定の情報を示します。

クラスタの詳細	クラスタの詳細の値
クラスタノード A の IP アドレス	<<var_nodeA_mgmt_ip>>

クラスタの詳細	クラスタの詳細の値
クラスタノード A のネットマスク	<<var_nodeA_mgmt_mask>> を使用します
クラスタノード A のゲートウェイ	<<var_nodeA_mgmt_gateway>> を使用します
クラスタノードの名前	<<var_nodeA>> を使用します
クラスタノード B の IP アドレス	<<var_nodeB_mgmt_ip>>
クラスタノード B のネットマスク	<<var_nodeB_mgmt_mask>> を使用します
クラスタノード B のゲートウェイ	<<var_nodeB_mgmt_gateway>> を使用します
クラスタノード B の名前	<<var_nodeB>> を使用します
ONTAP 9.4 の URL	<<var_url_boot_software>> を参照してください
クラスタの名前	\<<var_clustername> を使用します
クラスタ管理 IP アドレス	<<var_clustermgmt_ip>>
クラスタ B ゲートウェイ	<<var_clustermgmt_gateway>> を使用します
クラスタ B のネットマスク	<<var_clustermgmt_mask>> を使用します
ドメイン名	<<var_domain_name>> を参照してください
DNS サーバ IP （複数入力できます）	<<var_dns_server_ip>>
NTP サーバ IP （複数入力可能）	<<var_ntp_server_ip>>

ノード **A** を設定

ノード A を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

2. システムをブートできるようにします。

   ```
   autoboot
   ```

3. Ctrl+C キーを押してブートメニューを表示します。

   ONTAP 9.4 がブートしているソフトウェアのバージョンでない場合は、次の手順に進み、新しいソフトウェアをインストールします。ブートしているバージョンが ONTAP 9.4 の場合は、オプション 8 と y を選択してノードをリブートします。その後、手順 14 に進みます。

4. 新しいソフトウェアをインストールするには ' オプション 7 を選択します
5. アップグレードを実行するには 'y' を入力します
6. ダウンロードに使用するネットワーク・ポートに e0M を選択します

7. 今すぐ再起動するには 'y' を入力します
8. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. ソフトウェアを検索できる URL を入力します。

> ping 可能な Web サーバを指定する必要があります。

```
<<var_url_boot_software>>
```

10. ユーザ名が入力されていない場合は、 Enter キーを押します。
11. 新しくインストールしたソフトウェアを ' 次回の再起動に使用するデフォルトとして設定するには 'y' を入力します
12. ノードを再起動するには 'y' を入力します

    新しいソフトウェアをインストールするときに、 BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

13. Ctrl+C キーを押してブートメニューを表示します。
14. [Clean Configuration] で [4] を選択し、 [Initialize All Disks] を選択します。
15. ディスクをゼロにするには 'y' を入力し ' 構成をリセットして ' 新しいファイル・システムをインストールします
16. ディスク上のすべてのデータを消去するには 'y' を入力します

    ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。ノード A のディスクの初期化中も、ノード B の設定を続行できます。

17. ノード A を初期化している間に、ノード B の設定を開始します

ノード **B** を設定

ノード B を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Ctrl+C キーを押してブートメニューを表示します。

```
autoboot
```

3. プロンプトが表示されたら、 Ctrl-C キーを押します。

   ONTAP 9.4 がブートしているソフトウェアのバージョンでない場合は、次の手順に進み、新しいソフトウェアをインストールします。ブートしているバージョンが ONTAP 9.4 の場合は、オプション 8 と y を選択してノードをリブートします。その後、手順 14 に進みます。

4. 新しいソフトウェアをインストールするには、オプション 7 を選択します。
5. アップグレードを実行するには 'y' を入力します
6. ダウンロードに使用するネットワーク・ポートに e0M を選択します
7. 今すぐ再起動するには 'y' を入力します
8. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. ソフトウェアを検索できる URL を入力します。

   ping 可能な Web サーバを指定する必要があります。

```
<<var_url_boot_software>>
```

10. ユーザ名が入力されていない場合は、 Enter キーを押します。
11. 新しくインストールしたソフトウェアを ' 次回の再起動に使用するデフォルトとして設定するには 'y' を入力します
12. ノードを再起動するには 'y' を入力します

    新しいソフトウェアをインストールするときに、 BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

13. Ctrl+C キーを押してブートメニューを表示します。
14. Clean Configuration および Initialize All Disks のオプション 4 を選択します。
15. ディスクをゼロにするには 'y' を入力し ' 構成をリセットして ' 新しいファイル・システムをインストールします
16. ディスク上のすべてのデータを消去するには 'y' を入力します

    ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。

ストレージコントローラ A （ノード A ）のコンソールポートに接続されているコンソールポートプログラムから、ノードセットアップスクリプトを実行します。このスクリプトは、ノードでの ONTAP 9.4 の初回ブート時に表示されます。

> ONTAP 9.4 ではノードとクラスタのセットアップ手順が少し変更されました。クラスタセットアップウィザードを使用してクラスタの最初のノードを設定できるようになりました。 System Manager を使用してクラスタを設定します。

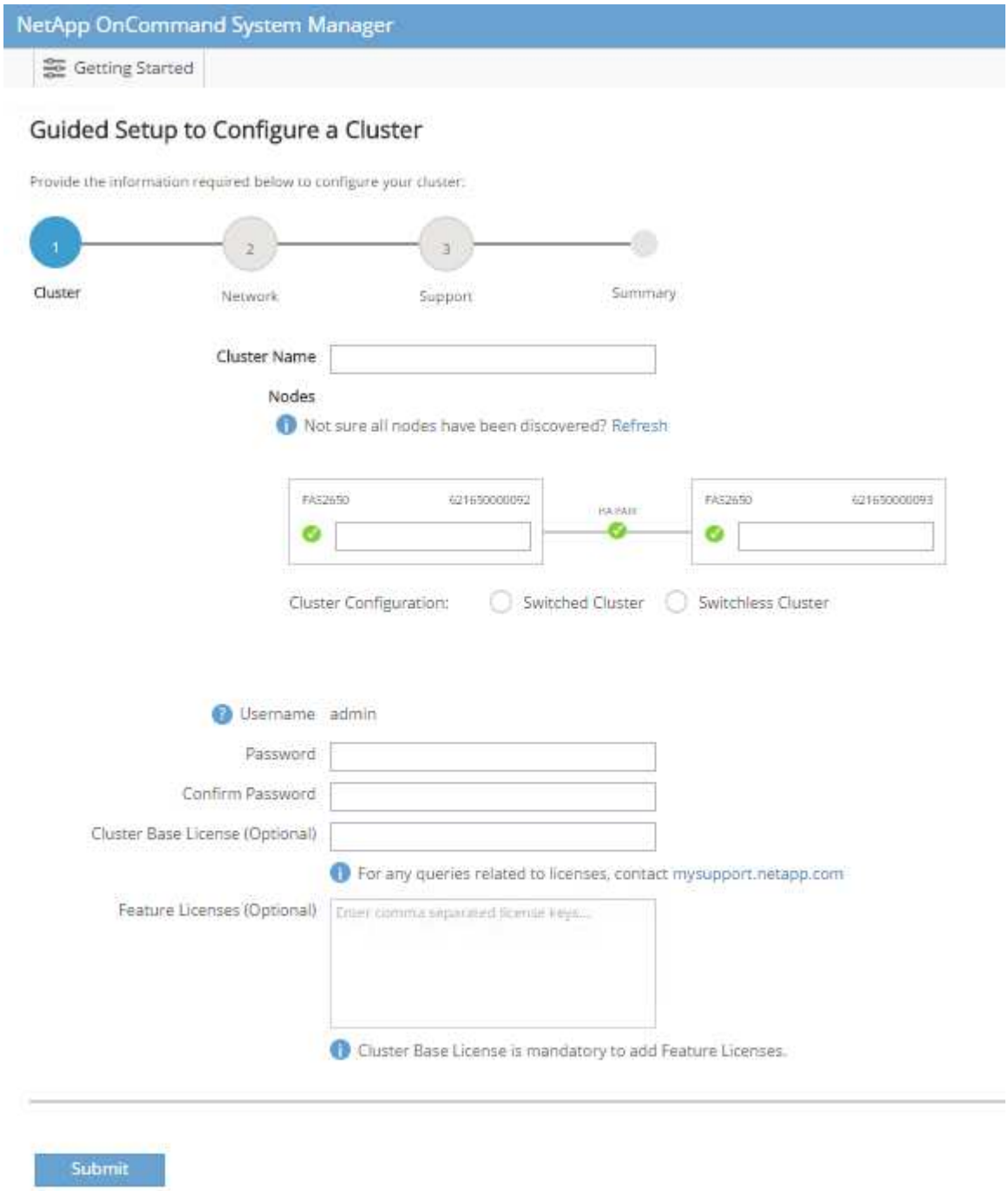
1. プロンプトに従ってノード A をセットアップします

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. ノードの管理インターフェイスの IP アドレスに移動します。

   クラスタのセットアップは、 CLI を使用して実行することもできます。このドキュメントでは、 NetApp System Manager のセットアップガイドを使用したクラスタセットアップについて説明します。

3. クラスタを設定するには、セットアップガイドをクリックします。
4. クラスタ名には「 \<<var_clustername>> 」を、設定する各ノードには「 <<var_nodeA>` 」と「 \<<var_nodeB>> 」を入力します。ストレージシステムに使用するパスワードを入力します。クラスタタイプに「スイッチレスクラスタ」を選択します。クラスタベースライセンスを入力します。



5. クラスタ、 NFS 、および iSCSI の機能ライセンスを入力することもできます。
6. クラスタの作成中を示すステータスメッセージが表示されます。このステータスメッセージは、複数のステータスを切り替えます。このプロセスには数分かかります。
7. ネットワークを設定します
   a. [IP Address Range] オプションを選択解除します。

b. Cluster Management IP Address フィールドに「 <<var_clustermgmt_ip>> 」、 Netmask フィールドに「 \var_clustermgmt_mask>> 」と入力します。また、 Gateway フィールドに「 <<var_clustermgmt_gateway>> 」と入力します。使用する方法 Port フィールドのを選択し、ノード A の e0M を選択します

c. ノード A のノード管理 IP がすでに入力されています。ノード B には '\<<var_nodeA_mgmt_ip>> を入力します

d. [DNS Domain Name] フィールドに「 <<var_domain_name>` 」と入力します。[DNS Server IP Address] フィールドに「 \<<var_dns_server_ip>> 」と入力します。

   DNS サーバの IP アドレスは複数入力できます。

e. Primary NTP Server フィールドに「 <<var_ntp_server_ip>> 」と入力します。

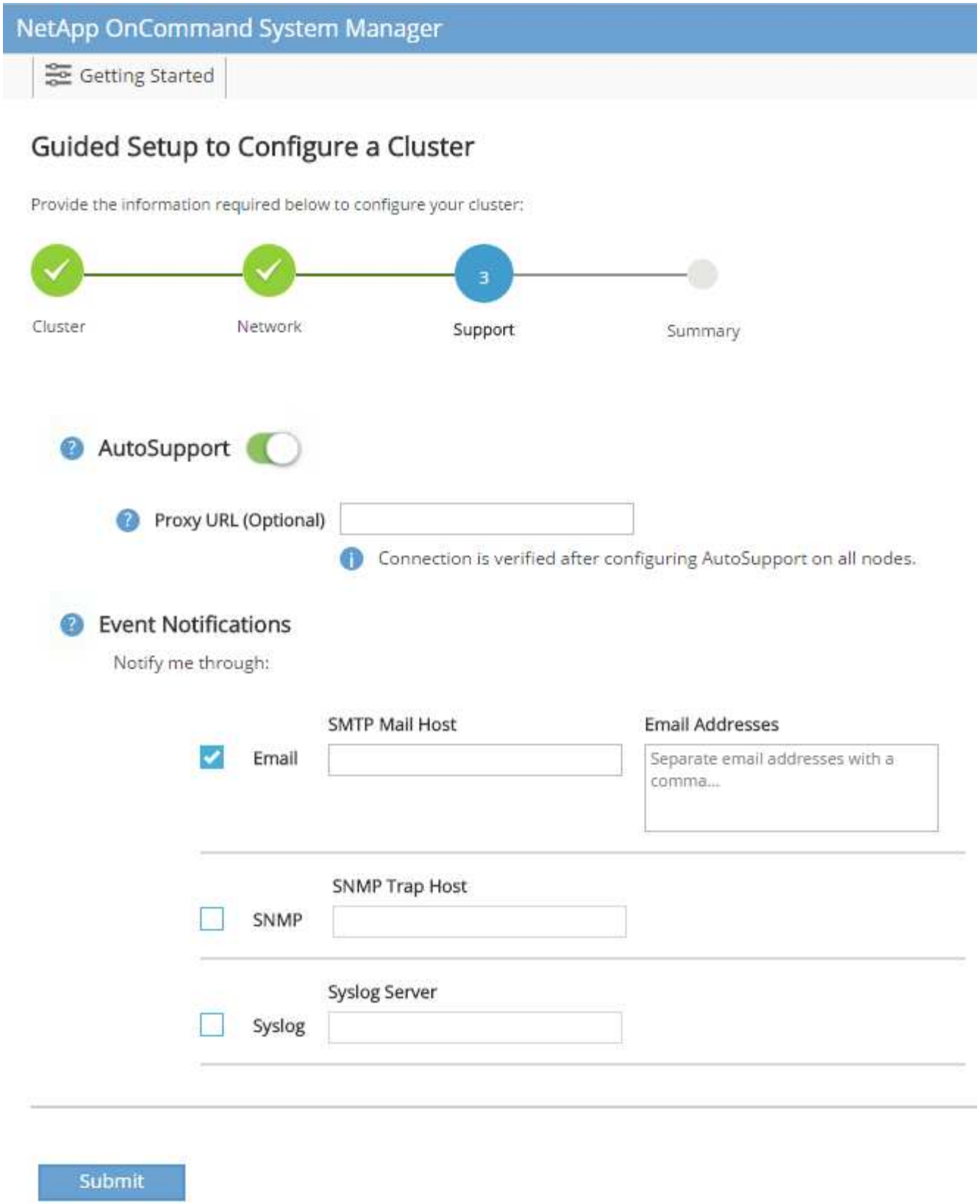
   代替 NTP サーバを入力することもできます。

8. サポート情報を設定します。

   a. AutoSupport へのアクセスにプロキシが必要な環境の場合は、プロキシの URL をプロキシの URL に入力します。

   b. イベント通知に使用する SMTP メールホストと E メールアドレスを入力します。

      続行するには、少なくともイベント通知方式を設定する必要があります。いずれかの方法を選択できます。



9. クラスタ構成が完了したことが示されたら、 Manage Your Cluster （クラスタの管理）をクリックしてストレージを構成します。

ストレージノードとベースクラスタの設定が完了したら、ストレージクラスタの設定に進むことができます。

すべてのスペアディスクを初期化します

クラスタ内のすべてのスペアディスクを初期化するには、次のコマンドを実行します。

```
disk zerospares
```

オンボード **UTA2** ポートパーソナリティを設定します

1. ucadmin show コマンドを実行して、現在のモードとポートの現在のタイプを確認します。

```
AFF A220::> ucadmin show
                       Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. 使用中のポートの現在のモードが「 cna 」であり、現在のタイプが「 target 」に設定されていることを確認します。そうでない場合は、次のコマンドを使用してポートパーソナリティを変更します。

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

前のコマンドを実行するには、ポートをオフラインにする必要があります。ポートをオフラインにするには、次のコマンドを実行します。

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

ポートパーソナリティを変更した場合、変更を有効にするには、各ノードをリブートする必要があります。

管理論理インターフェイス（ **LIF** ）の名前変更

管理 LIF の名前を変更するには、次の手順を実行します。

1. 現在の管理 LIF の名前を表示します。

```
network interface show -vserver <<clustername>>
```

2. クラスタ管理 LIF の名前を変更します。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. ノード B の管理 LIF の名前を変更します。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

クラスタ管理で自動リバートを設定する

クラスタ管理インターフェイスで 'auto-revert パラメータを設定します

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

サービスプロセッサのネットワークインターフェイスをセットアップする

各ノードのサービスプロセッサに静的 IPv4 アドレスを割り当てるには、次のコマンドを実行します。

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

サービスプロセッサの IP アドレスは、ノード管理 IP アドレスと同じサブネット内にある必要があります。

ONTAP でストレージフェイルオーバーを有効にします

ストレージフェイルオーバーが有効になっていることを確認するには、フェイルオーバーペアで次のコマンド

を実行します。

1. ストレージフェイルオーバーのステータスを確認

```
storage failover show
```

\<<var_nodeA>>` と \<<var_nodeB>> の両方がテイクオーバーを実行できる必要があります。ノードでテイクオーバーを実行できる場合は、ステップ 3 に進みます。

2. 2 つのノードのどちらかでフェイルオーバーを有効にします。

```
storage failover modify -node <<var_nodeA>> -enabled true
```

フェイルオーバーは、片方のノードで有効にすれば、両方のノードで有効になります。

3. 2 ノードクラスタの HA ステータスを確認

この手順は、ノードが 3 つ以上のクラスタには適用されません。

```
cluster ha show
```

4. ハイアベイラビリティが構成されている場合は、ステップ 6 に進みます。ハイアベイラビリティが設定されている場合は、コマンドの実行時に次のメッセージが表示されます。

```
High Availability Configured: true
```

5. HA モードは 2 ノードクラスタでのみ有効にします。

> ノードが 3 つ以上のクラスタの場合は、このコマンドを実行しないでください。フェイルオーバーで問題が発生します。

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. ハードウェアアシストが正しく設定されていることを確認し、必要に応じてパートナーの IP アドレスを変更

```
storage failover hwassist show
```

「 Keep Alive Status: Error: Did not receive hwassist keep alive alerts from partner 」というメッセージは、ハードウェアアシストが設定されていないことを示します。ハードウェアアシストを設定するには、次のコマンドを実行します。

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP でジャンボフレーム **MTU** ブロードキャストドメインを作成します

MTU が 9000 のデータブロードキャストドメインを作成するには、次のコマンドを実行します。

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

デフォルトのブロードキャストドメインからデータポートを削除します

10GbE のデータポートは iSCSI / NFS トラフィックに使用されます。これらのポートはデフォルトドメインから削除する必要があります。ポート e0e と e0f は使用されないため、デフォルトのドメインからも削除する必要があります。

ブロードキャストドメインからポートを削除するには、次のコマンドを実行します。

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 ポートではフロー制御を無効にします

ネットアップでは、外部デバイスに接続されているすべての UTA2 ポートでフロー制御を無効にすることをベストプラクティスとして推奨します。フロー制御を無効にするには、次のコマンドを実行します。

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

ONTAP で ifgrp LACP を設定します

このタイプのインターフェイスグループには複数のイーサネットインターフェイスと LACP をサポートするスイッチが必要です。スイッチが正しく設定されていることを確認します。

クラスタのプロンプトで、次の手順を実行します。

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

NetApp ONTAP でジャンボフレームを設定します

ジャンボフレーム（一般に MTU サイズが 9 、 000 バイトのフレーム）を使用するように ONTAP ネットワークポートを設定するには、クラスタシェルから次のコマンドを実行します。

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

ONTAP で **VLAN** を作成します

ONTAP で VLAN を作成するには、次の手順を実行します。

1. NFS VLAN ポートを作成し、データブロードキャストドメインに追加します。

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. iSCSI VLAN ポートを作成し、データブロードキャストドメインに追加します。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN ポートを作成します。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

ONTAP でアグリゲートを作成する

ONTAP のセットアッププロセスで、ルートボリュームを含むアグリゲートが作成されます。追加のアグリゲートを作成するには、アグリゲート名、アグリゲートを作成するノード、アグリゲートに含まれるディスク数を確認します。

アグリゲートを作成するには、次のコマンドを実行します。

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

構成内で少なくとも 1 つのディスクをスペアとして保持します（最も大きいディスクを選択してください）。ディスクのタイプとサイズごとに少なくとも 1 つのスペアを用意しておくことを推奨します。

ディスクは 5 本から始めて、追加のストレージが必要になったときにアグリゲートにディスクを追加できます。

ディスクの初期化が完了するまで、アグリゲートを作成することはできません。aggr show コマンドを実行して、アグリゲートの作成ステータスを表示します。「 aggr1 」 _「 nodeA 」がオンラインになるまで、次の手順に進まないでください。

ONTAP でタイムゾーンを設定します

時刻の同期を設定し、クラスタのタイムゾーンを設定するには、次のコマンドを実行します。

```
timezone <<var_timezone>>
```

> たとえば、米国東部では、タイムゾーンは「アメリカ / ニューヨーク」です。タイムゾーン名の入力を開始したら、 Tab キーを押して使用可能なオプションを表示します。

ONTAP で **SNMP** を設定します

SNMP を設定するには、次の手順を実行します。

1. 場所や連絡先などの SNMP 基本情報を設定します。ポーリング時に ' この情報は 'sysLocation' 変数と SNMP の sysContact' 変数として表示されます

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. リモートホストに送信する SNMP トラップを設定します。

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

ONTAP で **SNMPv1** を設定します

SNMPv1 を設定するには、コミュニティと呼ばれる共有シークレットのプレーンテキストパスワードを設定します。

```
snmp community add ro <<var_snmp_community>>
```

> 「 snmp community delete all 」コマンドは慎重に使用してください。他の監視製品にコミュニティストリングが使用されている場合、このコマンドはそれらを削除します。

ONTAP で **SNMPv3** を設定します

SNMPv3 では、認証用のユーザを定義および設定する必要があります。SNMPv3 を設定するには、次の手順を実行します。

1. 「 securitysnmpusers 」コマンドを実行して、エンジン ID を表示します。
2. 「 mpv3user 」という名前のユーザを作成します。

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 信頼できるエンティティのエンジン ID を入力し、認証プロトコルとして「 mD5 」を選択します。
4. プロンプトが表示されたら、認証プロトコルのパスワードとして最低 8 文字のパスワードを入力します。
5. プライバシープロトコルとして「 es 」を選択します。
6. プロンプトが表示されたら、プライバシープロトコルのパスワードとして最低 8 文字のパスワードを入力します。

ONTAP で AutoSupport HTTPS を設定します

NetApp AutoSupport ツールは、サポート概要情報を HTTPS 経由でネットアップに送信します。AutoSupport を設定するには、次のコマンドを実行します。

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Storage Virtual Machine を作成

インフラ Storage Virtual Machine （ SVM ）を作成するには、次の手順を実行します。

1. vserver create コマンドを実行します

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. NetApp VSC のインフラ SVM アグリゲートリストにデータアグリゲートを追加します。

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS と iSCSI を残して、未使用のストレージプロトコルを SVM から削除します。

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. インフラ SVM で NFS プロトコルを有効にして実行します。

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. NetApp NFS VAAI プラグインの「 VM vStorage 」パラメータをオンにします。次に、 NFS が設定されて

いることを確認します。

```
`vserver nfs modify -vserver Infra-SVM -vstorage enabled`
`vserver nfs show `
```

> コマンドは、 Storage Virtual Machine が以前はサーバと呼ばれていたため、コマンドラインでは「 vserver 」の前に配置されます。

ONTAP で **NFSv3** を設定します

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ESXi ホスト A の NFS IP アドレス	<<var_esxi_hostA_nfs_ip>>
ESXi ホスト B の NFS IP アドレス	<<var_esxi_hostB_nfs_ip>> を追加します

SVM に NFS を設定するには、次のコマンドを実行します。

1. デフォルトのエクスポートポリシーに各 ESXi ホスト用のルールを作成します。
2. 作成する各 ESXi ホストにルールを割り当てます。各ホストには独自のルールインデックスがあります。最初の ESXi ホストのルールインデックスは 1 、 2 番目の ESXi ホストのルールインデックスは 2 のようになります。

```
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 2 -protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule show
```

3. エクスポートポリシーをインフラ SVM ルートボリュームに割り当てます。

```
volume modify -vserver Infra-SVM -volume rootvol -policy default
```

> エクスポートポリシーは、 vSphere のセットアップ後にインストールするように選択した場合に自動的に処理されます。インストールしない場合は、 Cisco UCS C シリーズサーバを追加するときにエクスポートポリシールールを作成する必要があります。

ONTAP で **iSCSI** サービスを作成します

iSCSI サービスを作成するには、次の手順を実行します。

1. SVM で iSCSI サービスを作成します。また、このコマンドでは iSCSI サービスが開始され、 SVM の iSCSI IQN が設定されます。iSCSI が設定されていることを確認します。

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP で **SVM** ルートボリュームの負荷共有ミラーを作成

1. インフラ SVM ルートボリュームの負荷共有ミラーとなるボリュームを各ノードに作成します。

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. ルートボリュームのミラー関係を 15 分ごとに更新するジョブスケジュールを作成します。

```
job schedule interval create -name 15min -minutes 15
```

3. ミラーリング関係を作成

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. ミラーリング関係を初期化し、作成されたことを確認します。

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

ONTAP で **HTTPS** アクセスを設定する

ストレージコントローラへのセキュアなアクセスを設定するには、次の手順を実行します。

1. 証明書コマンドにアクセスするには、権限レベルを上げてください。

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 通常は、自己署名証明書がすでに存在します。次のコマンドを実行して証明書を確認します。

```
security certificate show
```

3. 表示されている各 SVM の証明書の共通名は、 SVM の DNS FQDN と一致する必要があります。4 つのデフォルト証明書を削除して、認証局の自己署名証明書または証明書に置き換える必要があります。

   証明書を作成する前に期限切れになった証明書を削除することを推奨します。「 securitycertificate delete 」コマンドを実行して、期限切れの証明書を削除します。次のコマンドでは、タブ補完を使用して、デフォルトの証明書を選択して削除します。

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 自己署名証明書を生成してインストールするには、次のコマンドを 1 回限りのコマンドとして実行します。インフラ SVM とクラスタ SVM のサーバ証明書を生成します。これらのコマンドの実行に役立つように、タブ補完を使用してください。

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 次の手順で必要なパラメータの値を取得するには、「 securitycertificate show 」コマンドを実行します。
6. 作成した各証明書を ' – server-enabled true' および– client-enabled false' パラメータを使用して有効にしますタブ補完を使用してください。

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL と HTTPS アクセスを設定して有効にし、 HTTP アクセスを無効にします。

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

これらのコマンドの一部で、エントリが存在しないことを示すエラーメッセージが返されますが、これは通常の動作であり問題ありません。

8. admin 権限レベルにリバートしてセットアップを作成し、 SVM を Web で使用できるようにします。

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

ONTAP で **NetApp FlexVol** ボリュームを作成します

NetApp FlexVol ボリュームを作成するには、ボリューム名、サイズ、およびボリュームが存在するアグリゲートを入力します。2 つの VMware データストアボリュームと 1 つのサーバブートボリュームを作成します。

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP で重複排除を有効にします

適切なボリュームで重複排除を有効にするには、次のコマンドを実行します。

```
volume efficiency on -vserver Infra-SVM -volume infra_datastore_1
volume efficiency on -vserver Infra-SVM -volume esxi_boot
```

ONTAP で LUN を作成します

2 つのブート LUN を作成するには、次のコマンドを実行します。

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cisco UCS C シリーズサーバを追加する場合は、追加のブート LUN を作成する必要があります。

ONTAP に iSCSI LIF を作成

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ストレージノード A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
ストレージノード A の iSCSI LIF01A ネットワークマスク	<<var_nodeA_iscsi_lif01a _mask>> をクリックします
ストレージノード A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
ストレージノード A の iSCSI LIF01B ネットワークマスク	<<var_nodeA_iscsi_lif01b_mask>> をクリックします
ストレージノード B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
ストレージノード B iSCSI LIF01A ネットワークマスク	<<var_nodeB_iscsi_lif01a_mask>> を選択します
ストレージノード B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
ストレージノード B iSCSI LIF01B ネットワークマスク	<<var_nodeB_iscsi_lif01b_mask>> をクリックします

1. 各ノードに 2 つずつ、 4 つの iSCSI LIF を作成します。

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

ONTAP に **NFS LIF** を作成します

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ストレージノード A NFS LIF 01 IP	<<var_nodeA_nfs_lif_01_ip>>
ストレージノード A NFS LIF 01 のネットワークマスク	<<var_nodeA_nfs_lif_01_mask>> を参照してください
ストレージノード B の NFS LIF 02 IP	<<var_nodeB_nfs_lif_02_ip>>
ストレージノード B の NFS LIF 02 ネットワークマスク	<<var_nodeB_nfs_lif_02_mask>> を参照してください

1. NFS LIF を作成します。

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface show
```

インフラ **SVM** 管理者を追加

次の表に、この設定を完了するために必要な情報を示します。

詳細（**Detail**）	詳細値
vsmgmt IP	<<var_svm_mgmt_ip>> を追加します
vsmgmt ネットワークマスク	<<var_SVM_mgmt_mask>> を使用します
vsmgmt デフォルトゲートウェイ	<<var_SVM_mgmt_gateway>> を使用します

インフラ SVM 管理者および SVM 管理論理インターフェイスを管理ネットワークに追加するには、次の手順を実行します。

1. 次のコマンドを実行します。

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port  e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true
```

> ここで指定する SVM 管理 IP は、ストレージクラスタ管理 IP と同じサブネット内にある必要があります。

2. SVM 管理インターフェイスの外部へのアクセスを許可するデフォルトルートを作成します。

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. SVM の vsadmin ユーザのパスワードを設定し、ユーザのロックを解除します。

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver Infra-SVM
```

"次のステップ： Cisco UCS C シリーズラックサーバ導入手順"

Cisco UCS C シリーズラックサーバ導入手順

ここでは、 FlexPod Express 構成で使用する Cisco UCS C シリーズスタンドアロンラックサーバを設定するための詳細な手順について説明します。

Cisco Integrated Management Server の **Cisco UCS C** シリーズスタンドアロンサーバの初期セットアップを実行します

Cisco UCS C シリーズスタンドアロンサーバの CIMC インターフェイスの初期セットアップを行うには、次の手順を実行します。

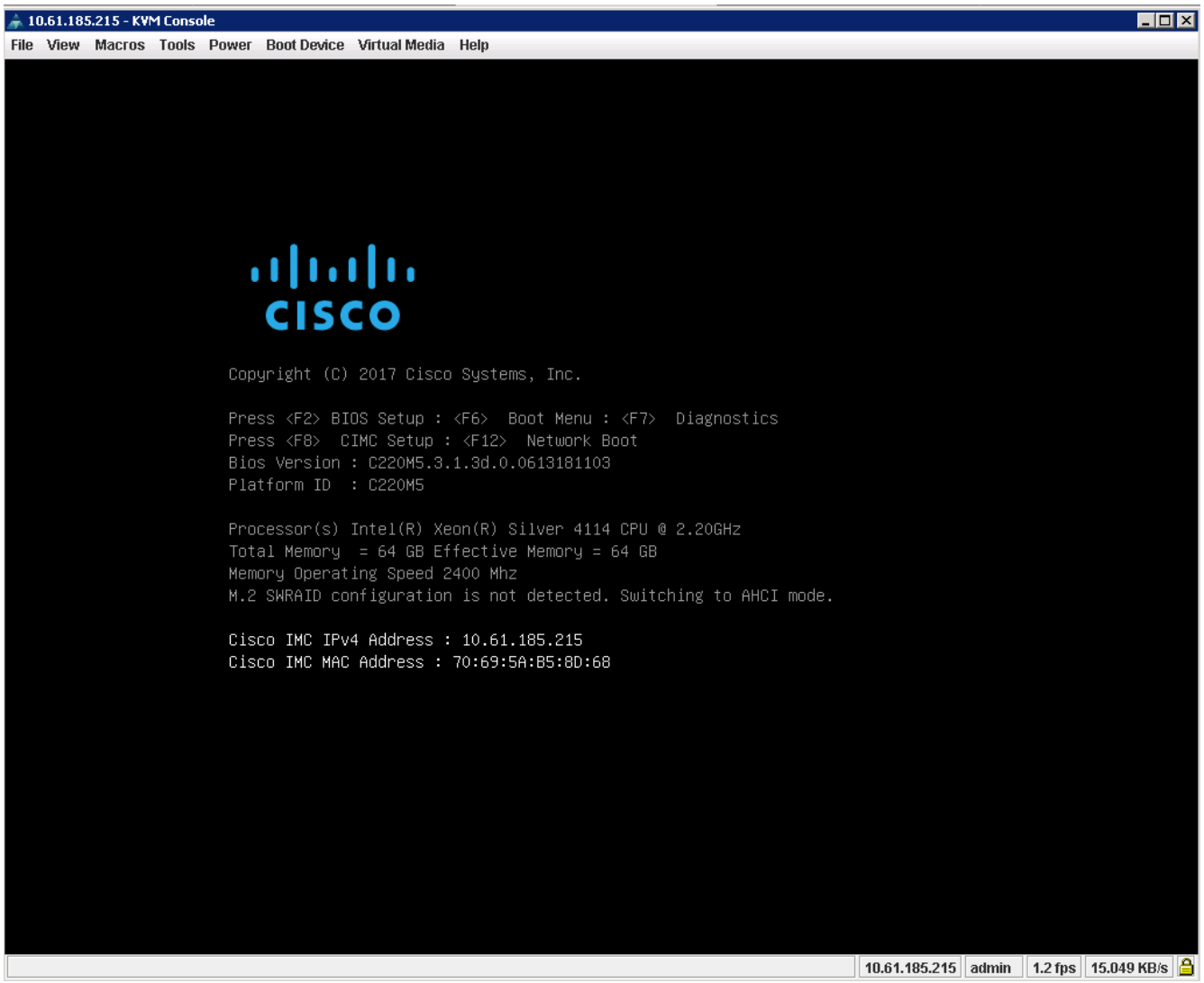
次の表に、 Cisco UCS C シリーズスタンドアロンサーバごとに CIMC を設定するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
CIMC IP アドレス	\<CIMC_IP>>
CIMC サブネットマスク	\<CIMC_netmask>>
CIMC デフォルトゲートウェイ	\<CIMC_Gateway>> のようになります

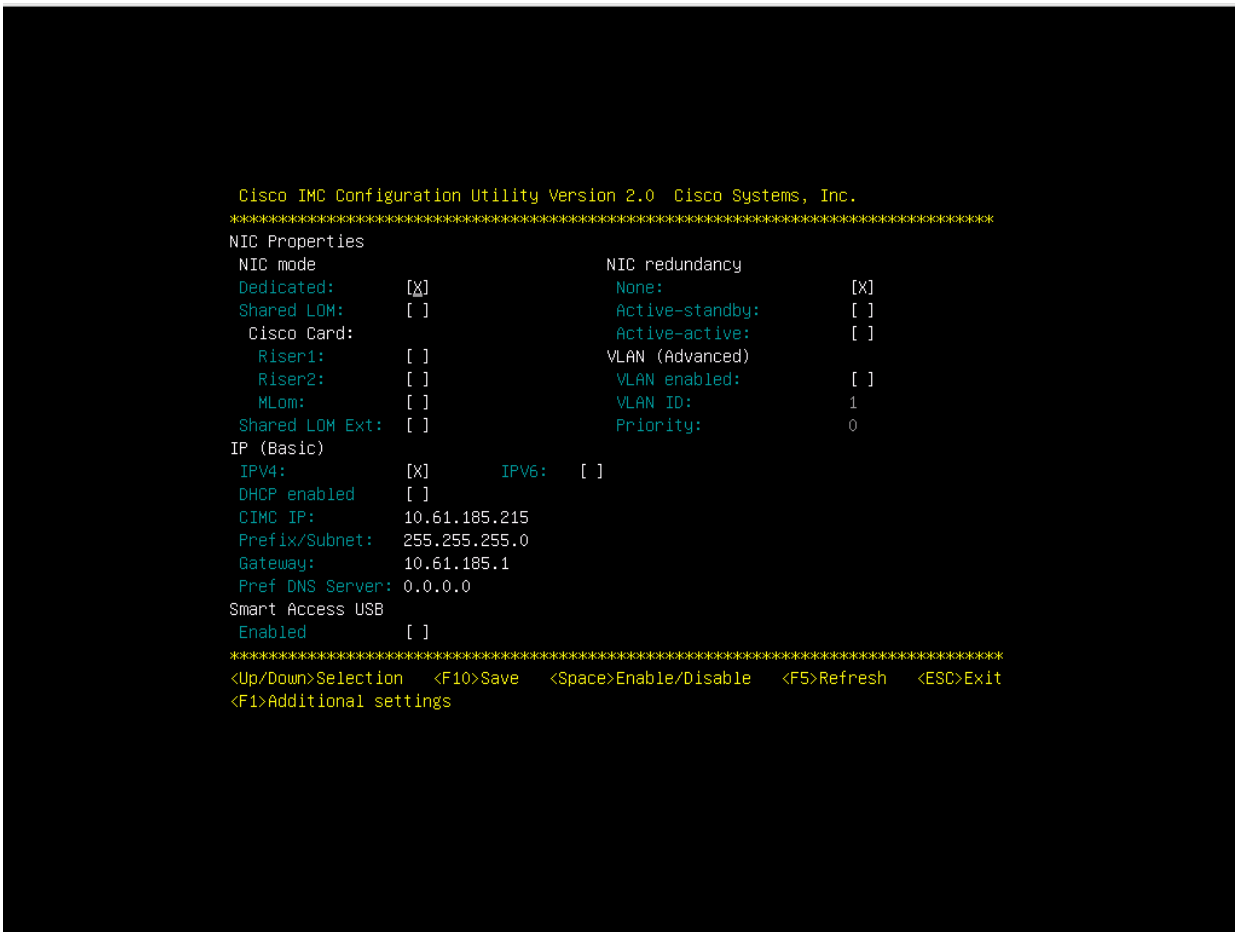
この検証で使用されている CIMC バージョンは、 CIMC 3.1.3 （ g ）です。

すべてのサーバ

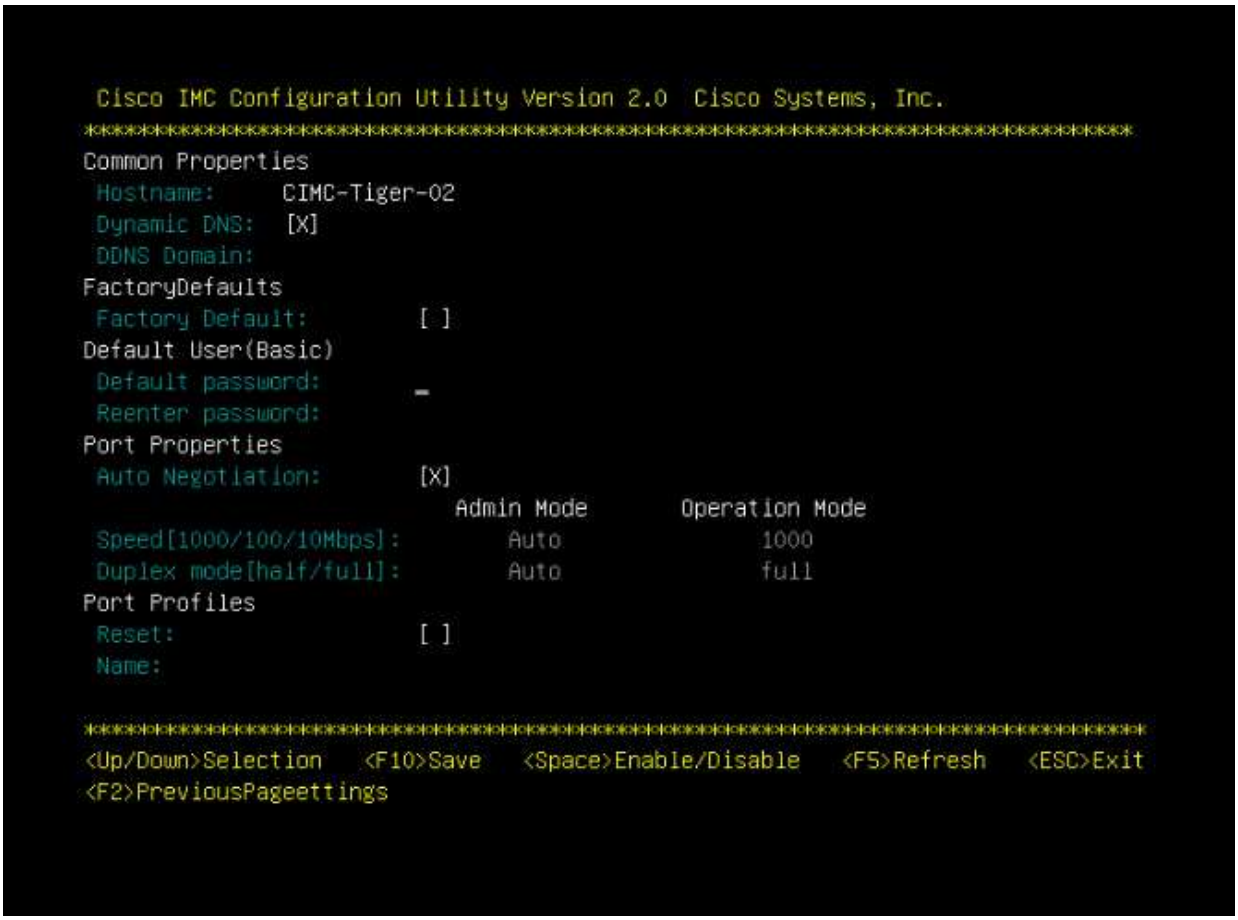
1. Cisco KVM （キーボード、ビデオ、およびマウス）ドングル（サーバに付属）を、サーバ前面の KVM ポートに取り付けます。VGA モニタと USB キーボードを、 KVM ドングルの対応するポートに接続します。
2. サーバの電源を入れ、 CIMC 設定を開始するかどうか確認するプロンプトが表示されたら F8 キーを押します。



3. CIMC 設定ユーティリティで、次のオプションを設定します。
   - ネットワークインターフェイスカード（ NIC ）モード：
     - 専用 [X]
   - IP （ベーシック）：
     - IPv4 ： [X]
     - DHCP が有効になっています： []
     - CIMC IP ： \<CIMC_IP>>
     - プレフィックス / サブネット： \<CIMC_netmask>>
     - ゲートウェイ： \<CIMC_gateway>>
   - VLAN （ Advanced ）： VLAN タギングを無効にする場合は、オフのままにします。
     - NIC の冗長性
     - なし： [X]



4. F1 キーを押して、その他の設定を表示します。
   - 共通プロパティ：
     - ホスト名： \<ESXi_host_name>>
     - 動的 DNS ： []
     - 工場出荷時のデフォルト：オフのままにします。
   - デフォルトユーザ（ basic ）：
     - デフォルトのパスワード： \<admin_password>>
     - パスワード「 \<admin_password>> 」を再入力します
     - ポートのプロパティ：デフォルト値を使用します。
     - ポートプロファイル：クリアしたままにします。



5. F10 キーを押し、 CIMC インターフェイス設定を保存します。
6. 設定を保存したら、 Esc キーを押して終了します。

Cisco UCS C シリーズサーバの iSCSI ブートを設定します

この FlexPod Express 構成では、 iSCSI ブートに VIC1387 が使用されます。

次の表に、 iSCSI ブートの設定に必要な情報を示します。

斜体のフォントは、 ESXi ホストごとに一意の変数を示します。

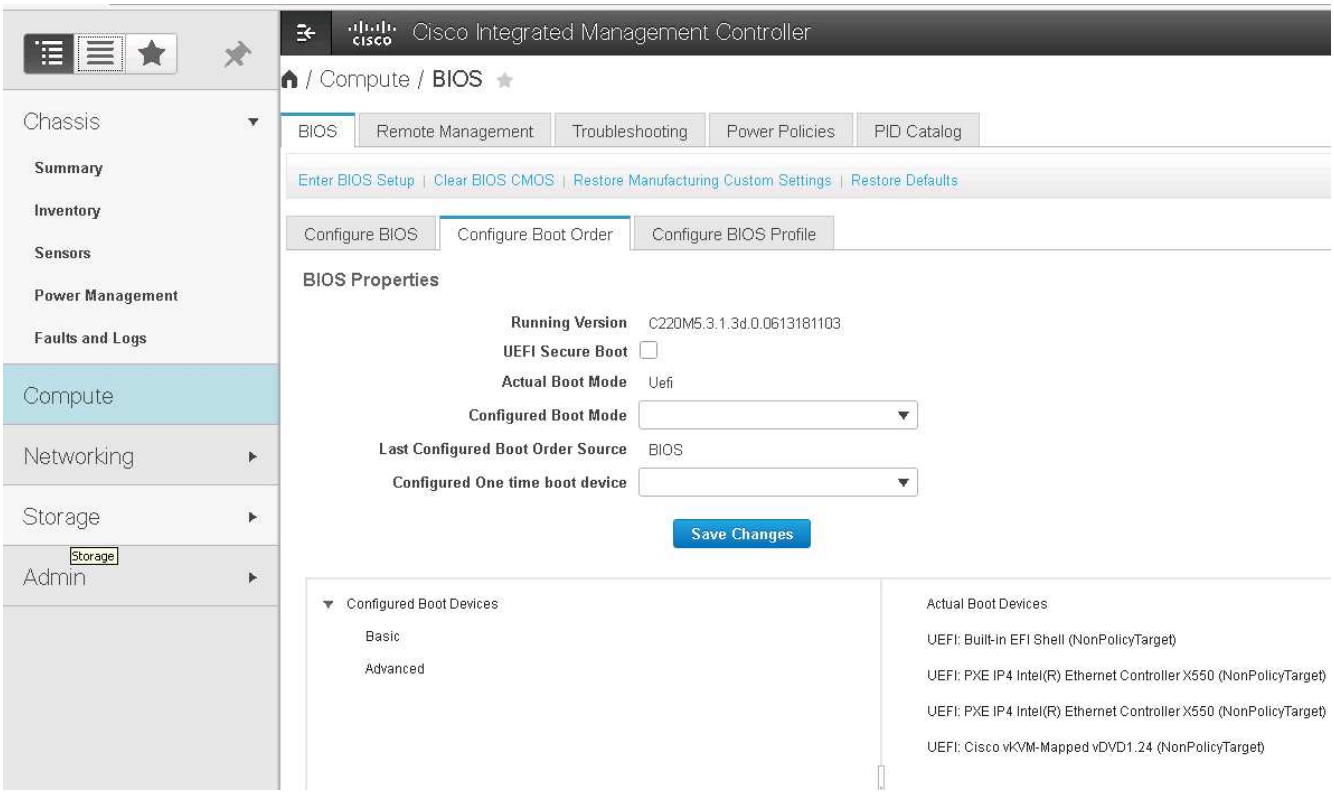
詳細（ **Detail** ）	詳細値
ESXi ホストイニシエータの名前	<<var_UCS_initiator_name_a>> を参照してください
ESXi ホスト iSCSI-A IP	<<var_esxi_host_iscsia_ip>>
ESXi ホスト iSCSI - ネットワークマスク	<<var_esxi_host_iscsia_mask>> を指定します
ESXi ホスト iSCSI A のデフォルトゲートウェイ	<<var_esxi_host_iscsia_gateway>> を指定します
ESXi ホストイニシエータ B の名前	<<var_UCS_initiator_name_b>> を参照してください
ESXi ホスト iSCSI-B IP	<<var_esxi_host_iSCSIb_ip>>
ESXi ホストの iSCSI-B ネットワークマスク	<<var_esxi_host_iSCSIb_mask>> を指定します
ESXi ホスト iSCSI-B ゲートウェイ	<<var_esxi_host_iSCSIb_gateway>> を指定します

詳細（ **Detail** ）	詳細値
IP アドレス iSCSI_lif01a	
IP アドレス iSCSI_lif02a	
IP アドレス iSCSI_lif01b	
IP アドレス iSCSI_lif02b	
インフラ SVM IQN	

起動順序の設定

ブート順の設定を行うには、次の手順を実行します。

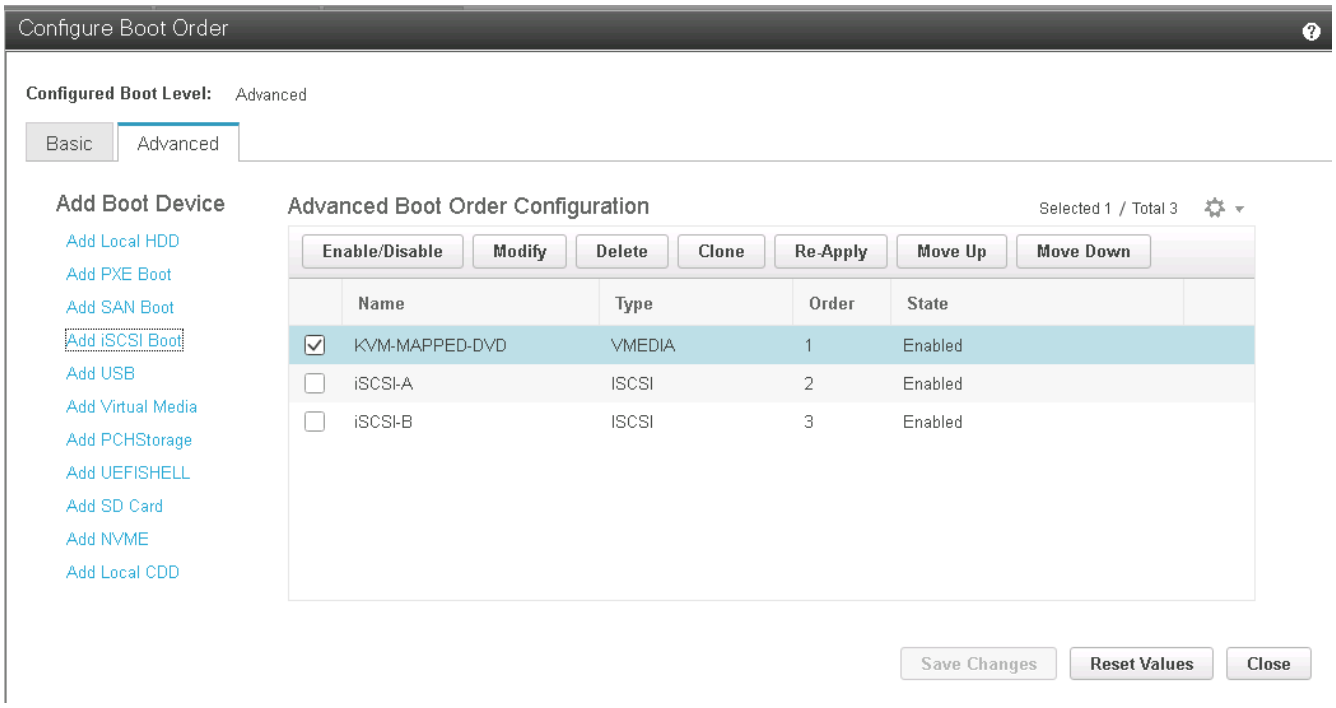
1. CIMC インターフェイスのブラウザウィンドウで、 [Server （サーバ）] タブをクリックし、 [BIOS （ BIOS ）] を選択します。
2. Configure Boot Order （起動順序の設定）をクリックし、 OK をクリックします。



3. [起動デバイスの追加] の下のデバイスをクリックし、 [詳細設定] タブに移動して、次のデバイスを設定します。
   - 仮想メディアを追加します
     - 名前： KVM-CD-DVD
     - サブタイプ： KVM マップ DVD
     - 状態：有効
     - 順序： 1.

- iSCSI ブートを追加します。
  - 名前： iSCSI-A
  - 状態：有効
  - ご注文： 2.
  - スロット： mLOM
  - ポート： 0
- Add iSCSI Boot をクリックします。
  - 名前： iSCSI-B
  - 状態：有効
  - 順序： 3.
  - スロット： mLOM
  - ポート： 1.

4. Add Device をクリックします。
5. [変更の保存] をクリックし、 [閉じる] をクリックします。



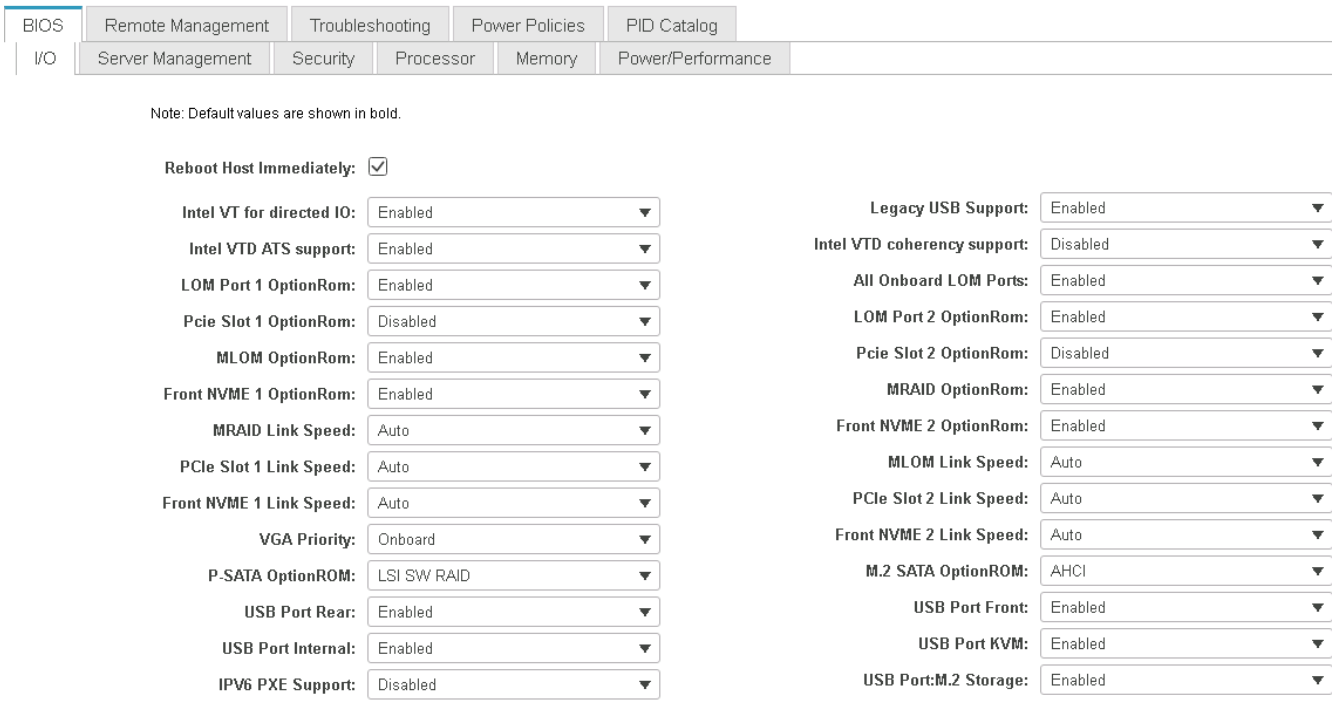
6. サーバをリブートして、新しいブート順序でブートします。

RAID コントローラを無効にする（存在する場合）

C シリーズサーバに RAID コントローラが搭載されている場合は、次の手順を実行します。SAN 構成からのブートでは RAID コントローラは必要ありません。必要に応じて、サーバから RAID コントローラを物理的に取り外すこともできます。

1. CIMC の左側のナビゲーションペインで BIOS をクリックします。

2. [Configure BIOS] を選択します。
3. 下にスクロールして [PCIe Slot:HBA Option ROM] を表示します。
4. 値が無効になっていない場合は、 disabled に設定します。



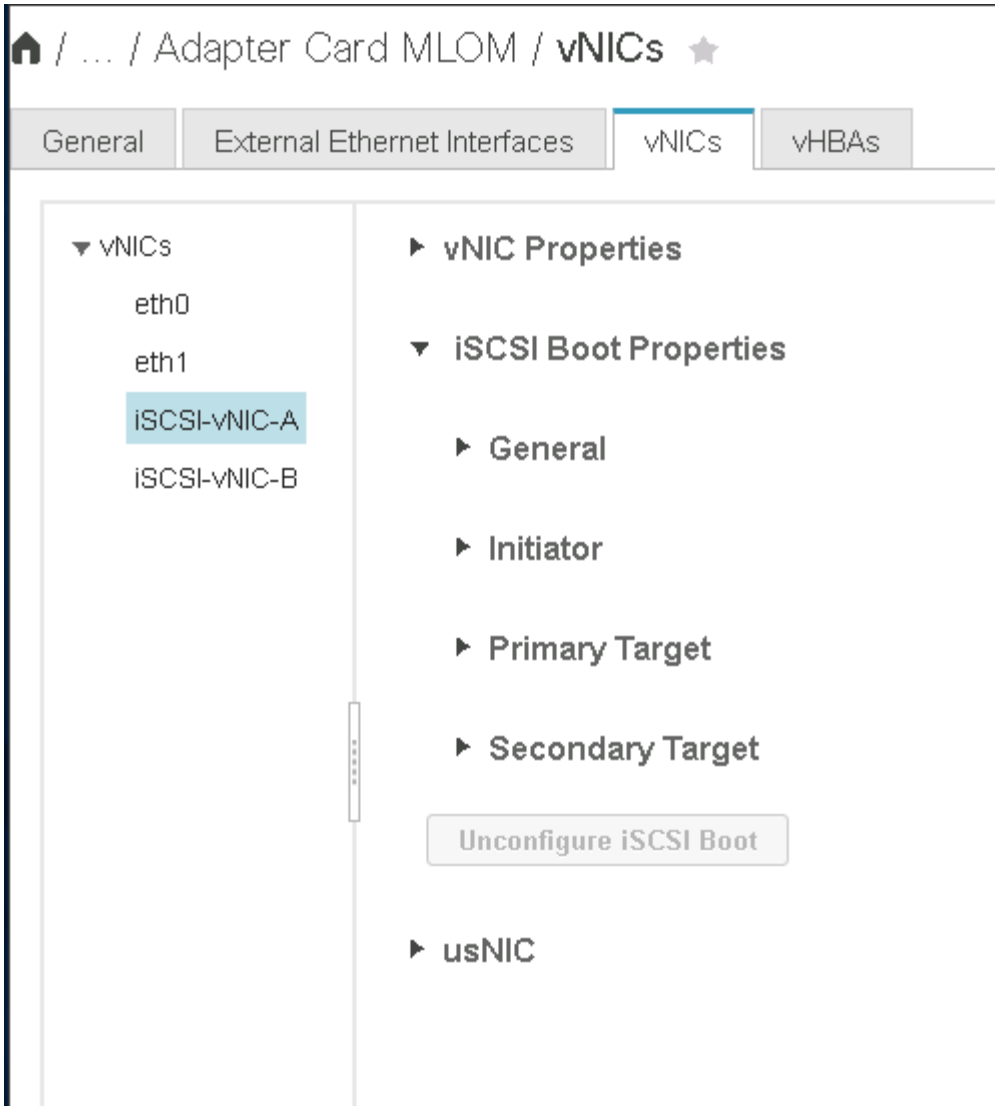
iSCSI ブート用に **Cisco VIC1387** を設定します

以下の設定手順は、 Cisco VIC 1387 で iSCSI ブートを使用する場合の手順です。

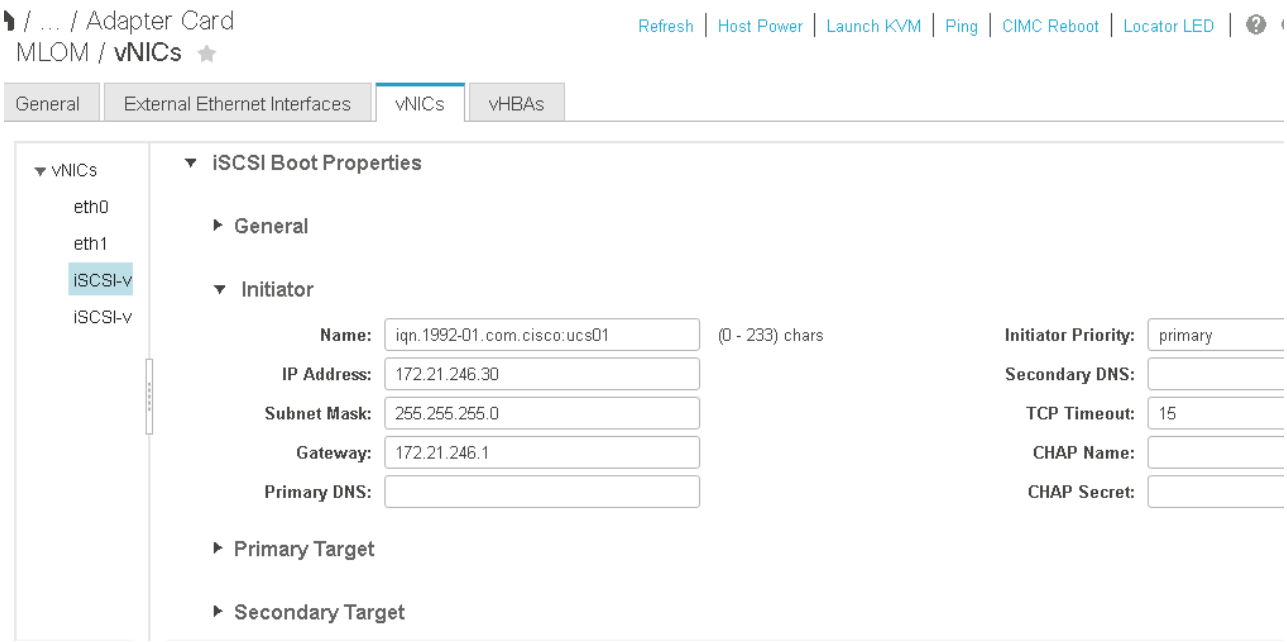
iSCSI vNIC を作成します

1. [追加] をクリックして vNIC を作成します。
2. [Add vNIC] セクションで、次の設定を入力します。
   - 名前： iscsi-vNIC-A
   - MTU ： 9000
   - デフォルト VLAN ： `\<<var_iscsi_vlan_a>`
   - VLAN モード：トランク
   - Enable PXE boot: チェック

3. [Add vNIC] をクリックし、 [OK] をクリックします。
4. このプロセスを繰り返して、 2 番目の vNIC を追加します。
   a. vNIC に「 iscsi-vnic-B 」という名前を付けます。
   b. VLAN として「 <<var_iscsi_vlan_b>> 」と入力します。
   c. アップリンクポートを「 1 」に設定します。
5. 左側の vNIC [iSCSI-vNIC-A] を選択します。



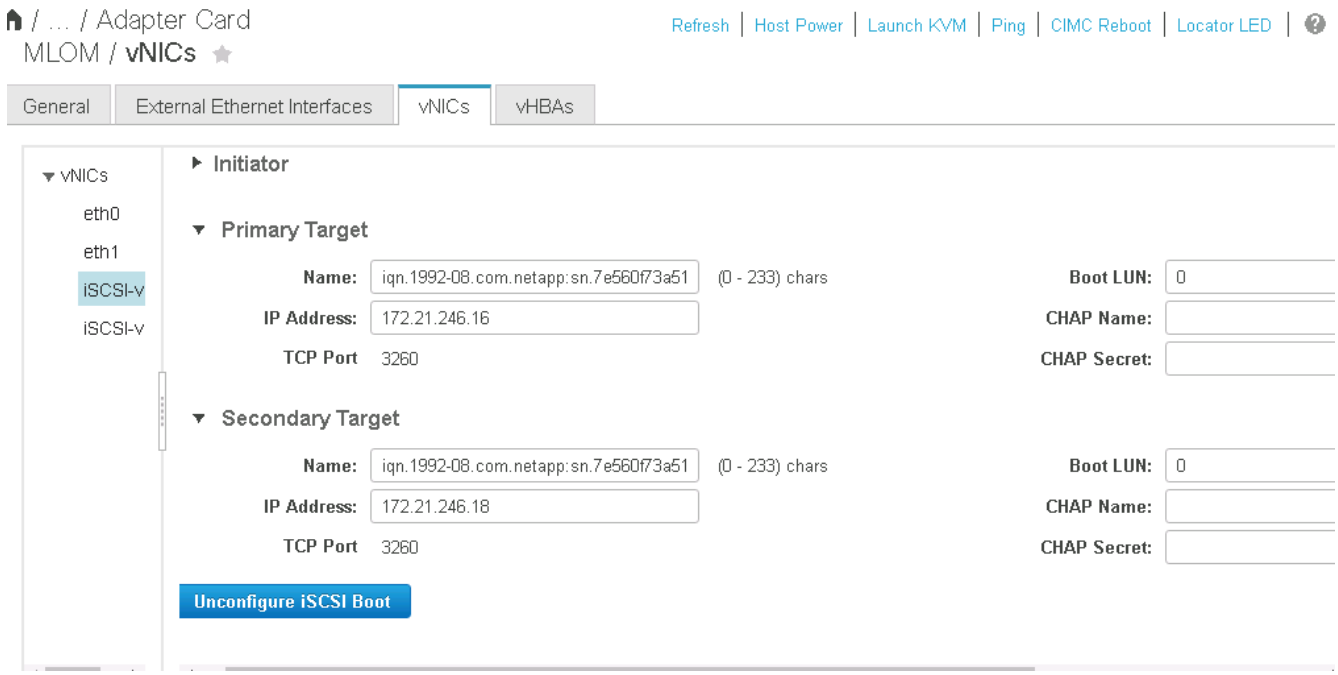
6. iSCSI Boot Properties （iSCSI 起動プロパティ）で、イニシエータの詳細を入力します。
   - 名前： <<var_ucsa_initiator_name_a>>
   - IP アドレス： <<var_esxi_hosta_iscsia_ip>>
   - サブネットマスク： <<var_esxi_hosta_iscsia_mask>>
   - ゲートウェイ： <<var_esxi_hosta_iscsia_gateway>>



7. プライマリターゲットの詳細を入力します。
   - name ：インフラ SVM の IQN 番号
   - IP アドレス： iSCSI_lif01a の IP アドレス
   - ブート LUN ： 0
8. セカンダリターゲットの詳細を入力します。
   - name ：インフラ SVM の IQN 番号
   - IP アドレス：「 iSCSI_lif02a 」の IP アドレス
   - ブート LUN ： 0

   ストレージ IQN 番号を取得するには 'vserver iscsi show コマンドを実行します

   各 vNIC の IQN 名を必ず記録してください。これらのファイルはあとで必要になります。



9. iSCSI の設定をクリックします。
10. vNIC [iSCSI-vNIC-B] を選択し、 [Host Ethernet Interfaces] セクションの上部にある [iSCSI Boot] ボタンをクリックします。
11. このプロセスを繰り返して 'iSCSI-vNIC-B' を設定します
12. イニシエータの詳細を入力します。
    - 名前：`\<<var_ucsa_initiator_name_b>`
    - IP アドレス：`\<<var_esxi_HostB_iSCSIb_ip>`
    - サブネットマスク：`<<var_esxi_HostB_iSCSIb_mask>>
    - ゲートウェイ：`<<var_esxi_HostB_iSCSIb_gateway>>
13. プライマリターゲットの詳細を入力します。
    - name ：インフラ SVM の IQN 番号
    - IP アドレス：「 iscsi_dlif01b 」の IP アドレス
    - ブート LUN ： 0
14. セカンダリターゲットの詳細を入力します。
    - name ：インフラ SVM の IQN 番号
    - IP アドレス：「 iscsi_dlif02b 」の IP アドレス
    - ブート LUN ： 0

    ストレージ IQN 番号は、「 vserver iscsi show 」コマンドを使用して取得できます。

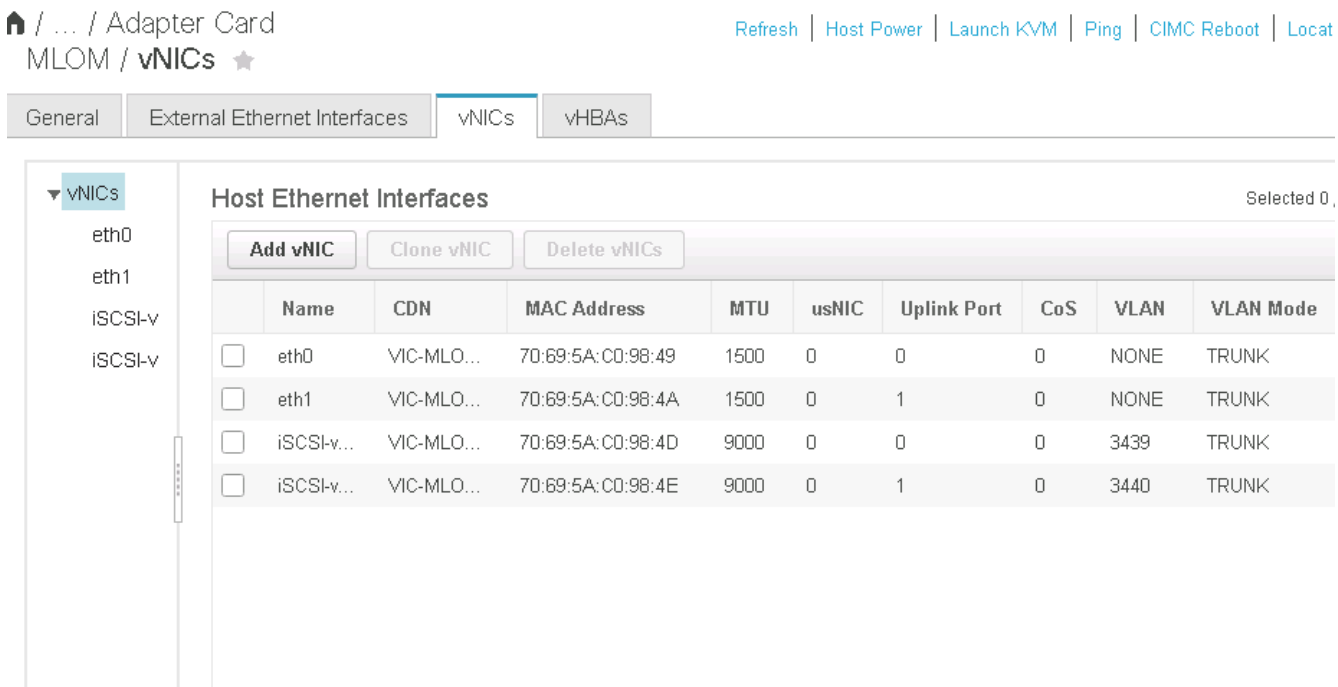
    各 vNIC の IQN 名を必ず記録してください。これらのファイルはあとで必要になります。

15. iSCSI の設定をクリックします。

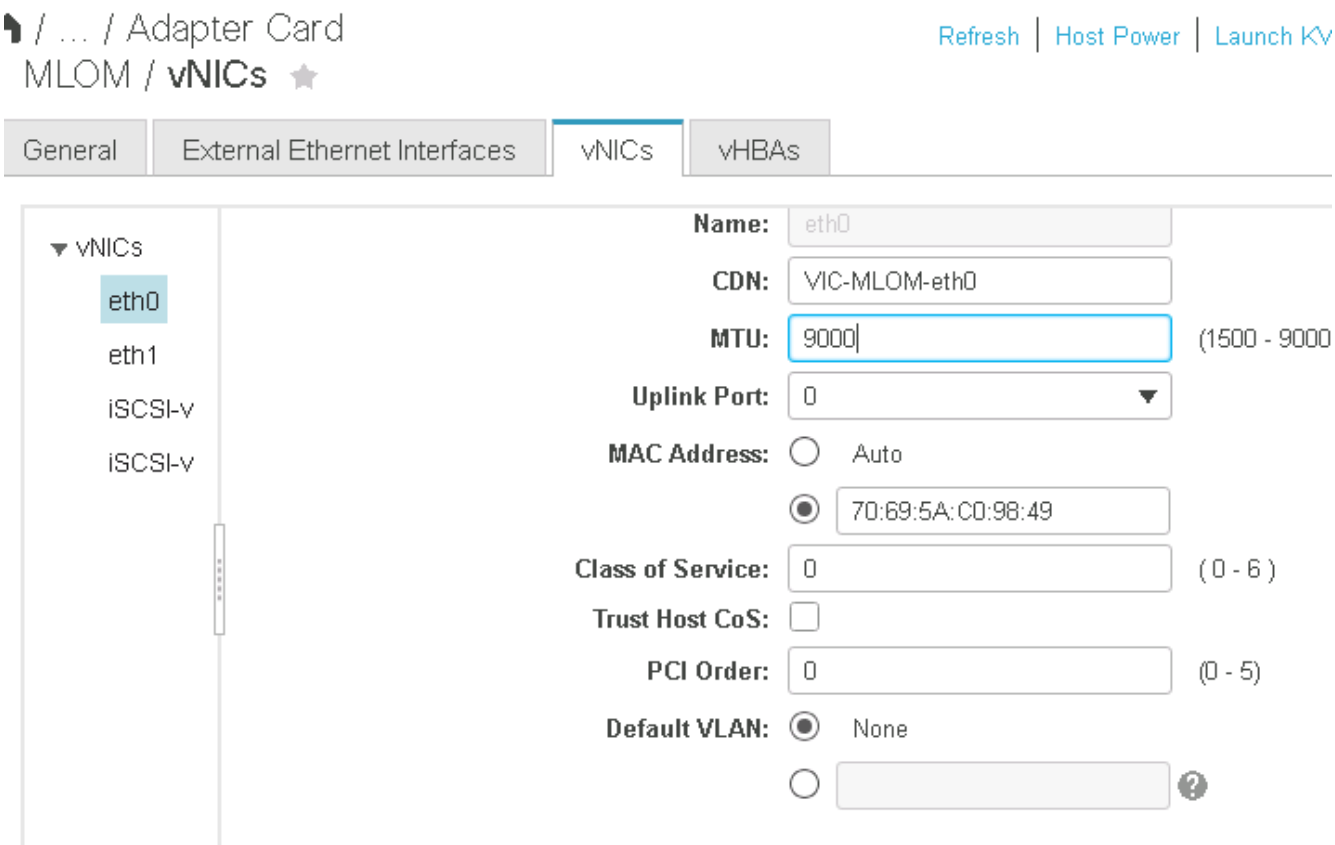
16. このプロセスを繰り返して、 Cisco UCS サーバ B の iSCSI ブートを設定します

ESXi の vNIC を設定します

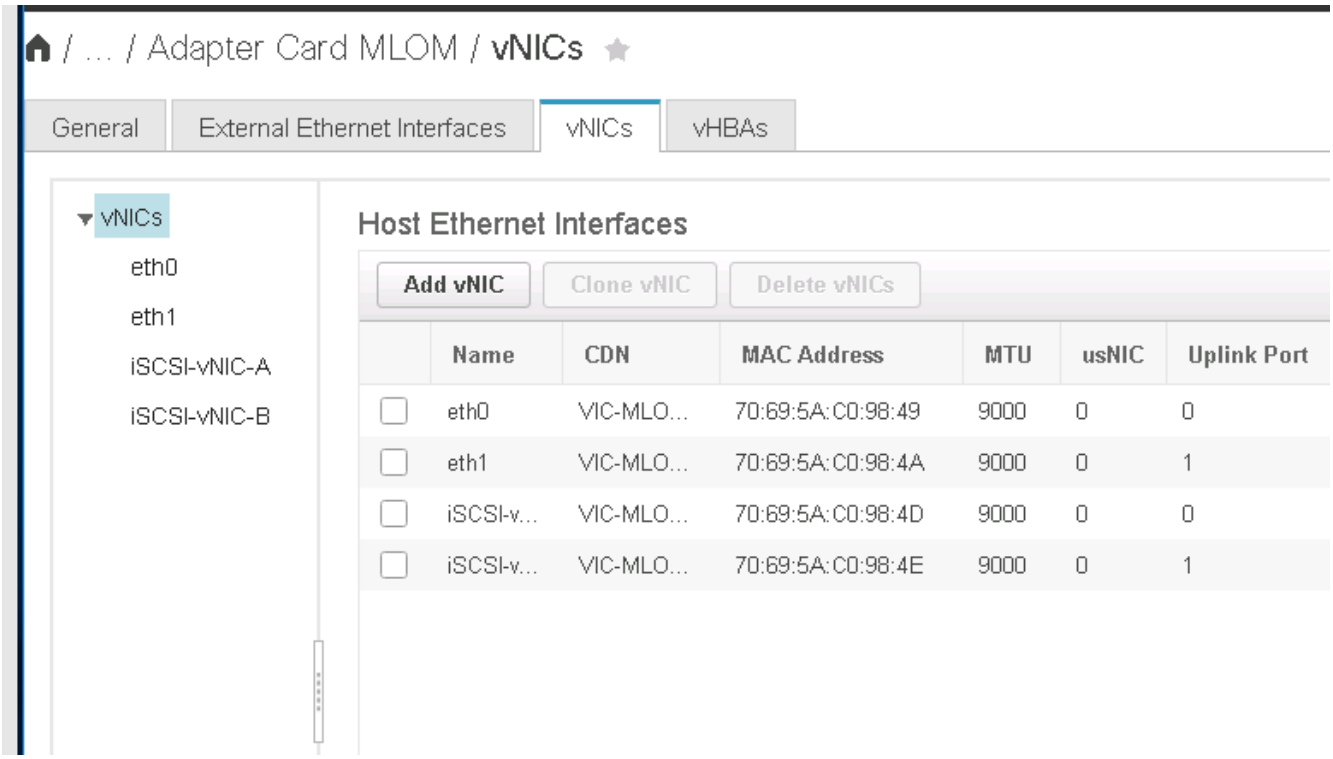
1. CIMC インターフェイスブラウザウィンドウで、 [Inventory] をクリックし、右側のペインで [Cisco VIC adapters] をクリックします。
2. [アダプタカード] で、 [Cisco UCS VIC 1387] を選択し、その下の vNIC を選択します。



3. eth0 を選択し、 Properties をクリックします。
4. MTU を 9000 に設定します。[Save Changes] をクリックします。



5. eth1 について手順 3 と 4 を繰り返し、 eth1 のアップリンクポートが「 1 」に設定されていることを確認します。



この手順は、最初の Cisco UCS サーバノードごと、および環境に追加する Cisco UCS サーバノードごとに繰り返す必要があります。

"次のセクション：『 NetApp AFF Storage Deployment 手順』（パート 2 ）"

NetApp AFF ストレージ導入手順（パート 2 ）

ONTAP SAN ブートストレージのセットアップ

iSCSI igroup を作成します

igroup を作成するには、次の手順を実行します。

この手順には、サーバ構成から iSCSI イニシエータの IQN が必要です。

1. クラスタ管理ノードの SSH 接続から、次のコマンドを実行します。この手順で作成された 3 つの igroup を表示するには、 igroup show コマンドを実行します。

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-A -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-B -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

> この手順は、 Cisco UCS C シリーズサーバを追加するときに実行する必要があります。

ブート LUN を igroup にマッピングします

ブート LUN を igroup にマッピングするには、クラスタ管理 SSH 接続から次のコマンドを実行します。

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- A -igroup
VM-Host-Infra- A -lun-id 0
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- B -igroup
VM-Host-Infra- B -lun-id 0
```

> この手順は、 Cisco UCS C シリーズサーバを追加するときに実行する必要があります。

"次のステップ： VMware vSphere 6.7 Deployment 手順。"

VMware vSphere 6.7 の導入手順

このセクションでは、 FlexPod Express 構成に VMware ESXi 6.7 をインストールする手順について説明します。以下に記載する導入手順は、前のセクションで説明した環境変数用にカスタマイズされたものです。

このような環境に VMware ESXi をインストールするには、複数の方法があります。この手順は、 Cisco UCS C シリーズサーバ用 CIMC インターフェイスの仮想 KVM コンソールと仮想メディア機能を使用して、リモー

トインストールメディアを個々のサーバにマッピングします。

> この手順は、 Cisco UCS サーバ A および Cisco UCS サーバ B に対して実行する必要があります

クラスタに追加するノードに対してこの手順を完了しておく必要があります。

Cisco UCS C シリーズスタンドアロンサーバの CIMC インターフェイスにログインします

以下に、 Cisco UCS C シリーズスタンドアロンサーバの CIMC インターフェイスにログインする手順について説明します。仮想 KVM を実行するには CIMC インターフェイスにログインする必要があります。これにより、管理者はリモートメディアを使用したオペレーティングシステムのインストールを開始できます。

すべてのホスト

1. Web ブラウザに移動し、 Cisco UCS C シリーズの CIMC インターフェイスの IP アドレスを入力します。この手順では CIMC GUI アプリケーションを起動します。
2. 管理ユーザ名とクレデンシャルを使用して、 CIMC UI にログインします。
3. メインメニューで、サーバータブを選択します。
4. Launch KVM Console をクリックします。

5. 仮想 KVM コンソールから、 [Virtual Media](仮想メディア) タブを選択します。
6. [CD/DVD のマップ] を選択します。

> 最初に [仮想デバイスのアクティブ化] をクリックする必要があります。プロンプトが表示されたら、 [このセッションを受け入れる] を選択

7. VMware ESXi 6.7 インストーラの ISO イメージファイルを参照して、 [開く] をクリックします。Map Device をクリックします。
8. 電源メニューを選択し、システムの電源再投入（コールドブート）を選択します。はいをクリックします。

VMware ESXi をインストールします

以下に、各ホストに VMware ESXi をインストールする手順について説明します。

ESXi 6.7 Cisco カスタムイメージをダウンロードします

1. に移動します "VMware vSphere のダウンロードページ" カスタム ISO の場合。
2. Cisco Custom Image for ESXi 6.7 GA Install CD の横にある Go to Downloads をクリックします。
3. ESXi 6.7 GA Install CD （ ISO ）用の Cisco Custom Image をダウンロードします。

すべてのホスト

1. システムが起動すると、 VMware ESXi インストールメディアがマシンによって検出されます。
2. 表示されるメニューから VMware ESXi インストーラを選択します。

   インストーラがロードされます。これには数分かかります。

3. インストーラのロードが完了したら、 Enter キーを押してインストールを続行します。
4. エンドユーザライセンス契約を読んだ後、同意して F11 キーを押してインストールを続行します。
5. ESXi のインストールディスクとして設定した NetApp LUN を選択し、 Enter キーを押してインストールを続行します。

6. 適切なキーボードレイアウトを選択し、 Enter キーを押します。
7. ルートパスワードを入力して確定し、 Enter キーを押します。
8. 既存のパーティションがボリュームから削除されていることを示す警告が表示されます。F11 キーを押してインストールを続行します。ESXi のインストール後にサーバがリブートします。

VMware ESXi ホスト管理ネットワークをセットアップします

以下に、 VMware ESXi ホストごとに管理ネットワークを追加する手順について説明します。

すべてのホスト

1. サーバのリブートが完了したら、 F2 キーを押してシステムをカスタマイズするオプションを入力します。
2. インストールプロセスで入力したログイン名と root パスワードを使用してログインします。
3. Configure Management Network （管理ネットワークの設定）オプションを選択します。
4. [ネットワークアダプタ] を選択し、 Enter キーを押します。
5. vSwitch0 に使用するポートを選択します。Enter キーを押します。

   CIMC の eth0 および eth1 に対応するポートを選択します。

6. VLAN （オプション）を選択し、 Enter キーを押します。
7. VLAN ID 「 \<mgmt_vlan_id>` 」を入力します。Enter キーを押します。
8. Configure Management Network （管理ネットワークの設定）メニューから、 IPv4 Configuration （ IPv4 設定）を選択して管理インターフェイスの IP アドレスを設定します。Enter キーを押します。
9. 矢印キーを使用して [Set Static IPv4 address](静的 IPv4 アドレスの設定) をハイライトし、スペースバーを使用してこのオプションを選択します。
10. VMware ESXi ホスト「 \<ESXi_host_mgmt_ip>> 」を管理するための IP アドレスを入力します。
11. VMware ESXi ホスト「 \<ESXi_host_mgmt_netmask>>.' 」のサブネットマスクを入力します
12. VMware ESXi ホスト「 \<ESXi_host_mgmt_gateway>` 」のデフォルトゲートウェイを入力します。
13. Enter キーを押して、 IP 設定の変更を確定します。
14. IPv6 設定メニューを表示します。
15. IPv6 を有効にする（再起動が必要）オプションを選択解除して IPv6 を無効にするには、スペースバーを使用します。Enter キーを押します。
16. DNS 設定を指定するメニューを表示します。
17. IP アドレスは手動で割り当てられるため、 DNS 情報も手動で入力する必要があります。
18. プライマリ DNS サーバの IP アドレスを入力します[nameserver_ip]。
19. （任意）セカンダリ DNS サーバの IP アドレスを入力します。
20. VMware ESXi ホスト名の FQDN を入力します：[esxi_host_fqdn]。
21. Enter キーを押して、 DNS 設定の変更を確定します。
22. Esc キーを押して、管理ネットワークの設定サブメニューを終了します。
23. Y キーを押して変更を確定し、サーバーを再起動します。
24. Esc キーを押して、 VMware コンソールからログアウトします。

ESXi ホストを設定

各 ESXi ホストを設定するには、次の表の情報が必要です。

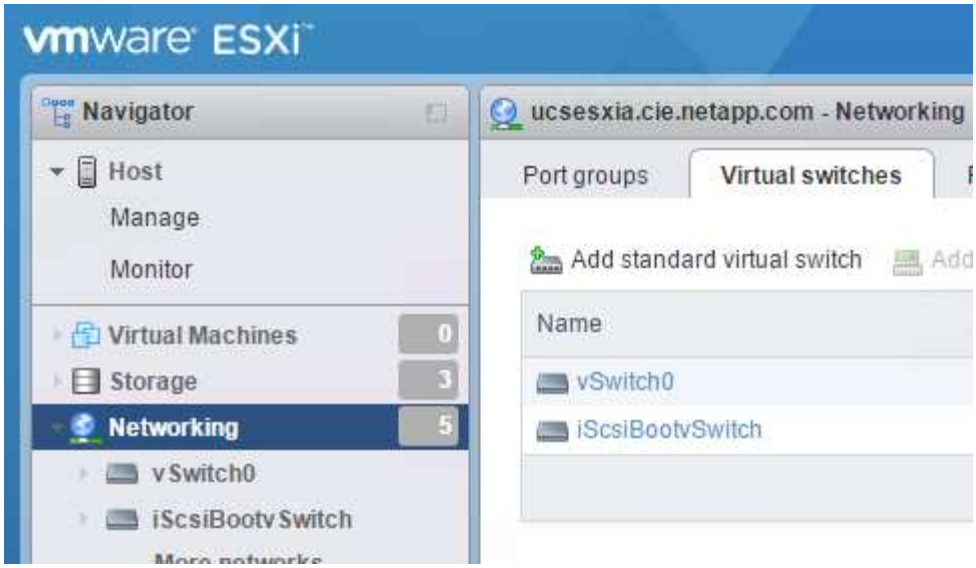
詳細（ **Detail** ）	価値
ESXi ホスト名	
ESXi ホスト管理 IP	
ESXi ホスト管理マスク	
ESXi ホスト管理ゲートウェイ	
ESXi ホストの NFS IP	
ESXi ホストの NFS マスク	
ESXi ホストの NFS ゲートウェイ	
ESXi ホスト vMotion IP	
ESXi ホストの vMotion マスク	
ESXi ホストの vMotion ゲートウェイ	
ESXi ホスト iSCSI-A IP	
ESXi ホスト iSCSI-A マスク	
ESXi ホスト iSCSI-A ゲートウェイ	
ESXi ホスト iSCSI-B IP	
ESXi ホスト iSCSI-B マスク	
ESXi ホスト iSCSI-B ゲートウェイ	

ESXi ホストにログインします

1. Web ブラウザでホストの管理 IP アドレスを開きます。
2. root アカウントとインストールプロセスで指定したパスワードを使用して、 ESXi ホストにログインします。
3. VMware Customer Experience Improvement Program に関する声明をお読みください。適切な応答を選択したら、 [OK] をクリックします。

iSCSI ブートを設定します

1. 左側の [ネットワーク] を選択します。
2. 右側の [Virtual Switches] タブを選択します。

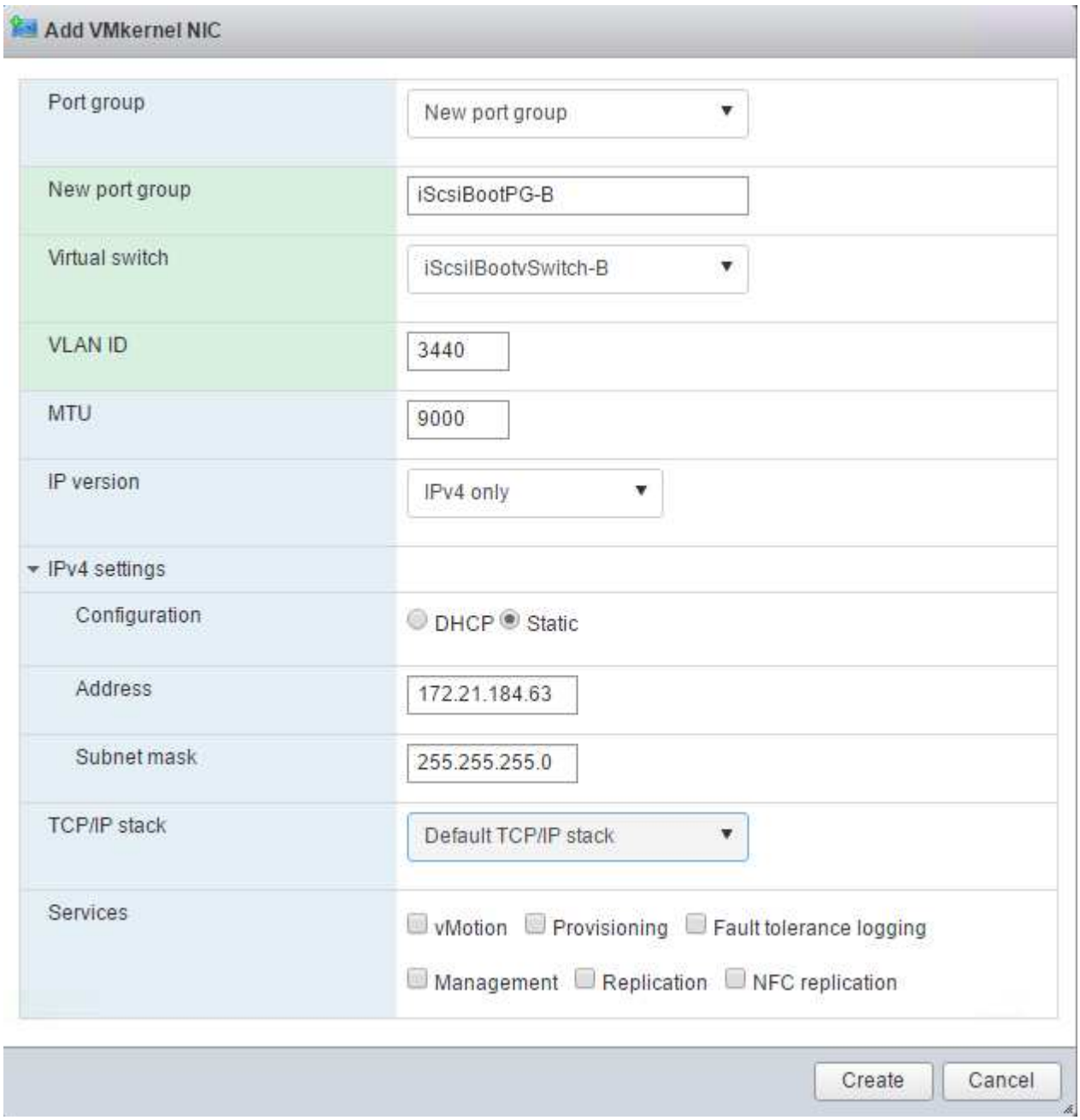


3. iScsiBootvSwitch をクリックします。
4. [設定の編集] を選択します
5. MTU を 9000 に変更し、 [保存] をクリックします。
6. 左側のナビゲーションペインで Networking （ネットワーク）をクリックして、 Virtual Switches （仮想スイッチ）タブに戻ります。
7. Add Standard Virtual Switch をクリックします。
8. vSwitch 名に「 iScsiBootvSwitch -B 」という名前を付けます。
   - MTU を 9000 に設定します。
   - アップリンク 1 のオプションから vmnic3 を選択します。
   - 追加をクリックします。

> この構成では、 vmnic2 と vmnic3 が iSCSI ブートに使用されます。ESXi ホストに NIC がほかにもある場合は、 vmnic 番号が異なることがあります。iSCSI ブートに使用されている NIC を確認するには、 CIMC の iSCSI vNIC 上の MAC アドレスを ESXi の vmnic に照合します。

9. 中央のペインで、 [VMkernel NICs] タブを選択します。
10. Add VMkernel NIC を選択します。
    - 新しいポートグループ名として、「 iScsiBootPG-B' 」を指定します。
    - 仮想スイッチに対して、 iScsiBootvSwitch -B を選択します。
    - VLAN ID に「 \<iSCSIb_vlan_id>` 」と入力します。
    - MTU を 9000 に変更します。
    - IPv4 設定を展開します。
    - 静的設定を選択します。
    - アドレスとして「 \\<var_hosta_iSCSIb_ip>> 」と入力します。
    - Subnet Mask には「 \<<var_hosta_iSCSIb_mask>> 」と入力します。

◦ Create をクリックします。 .

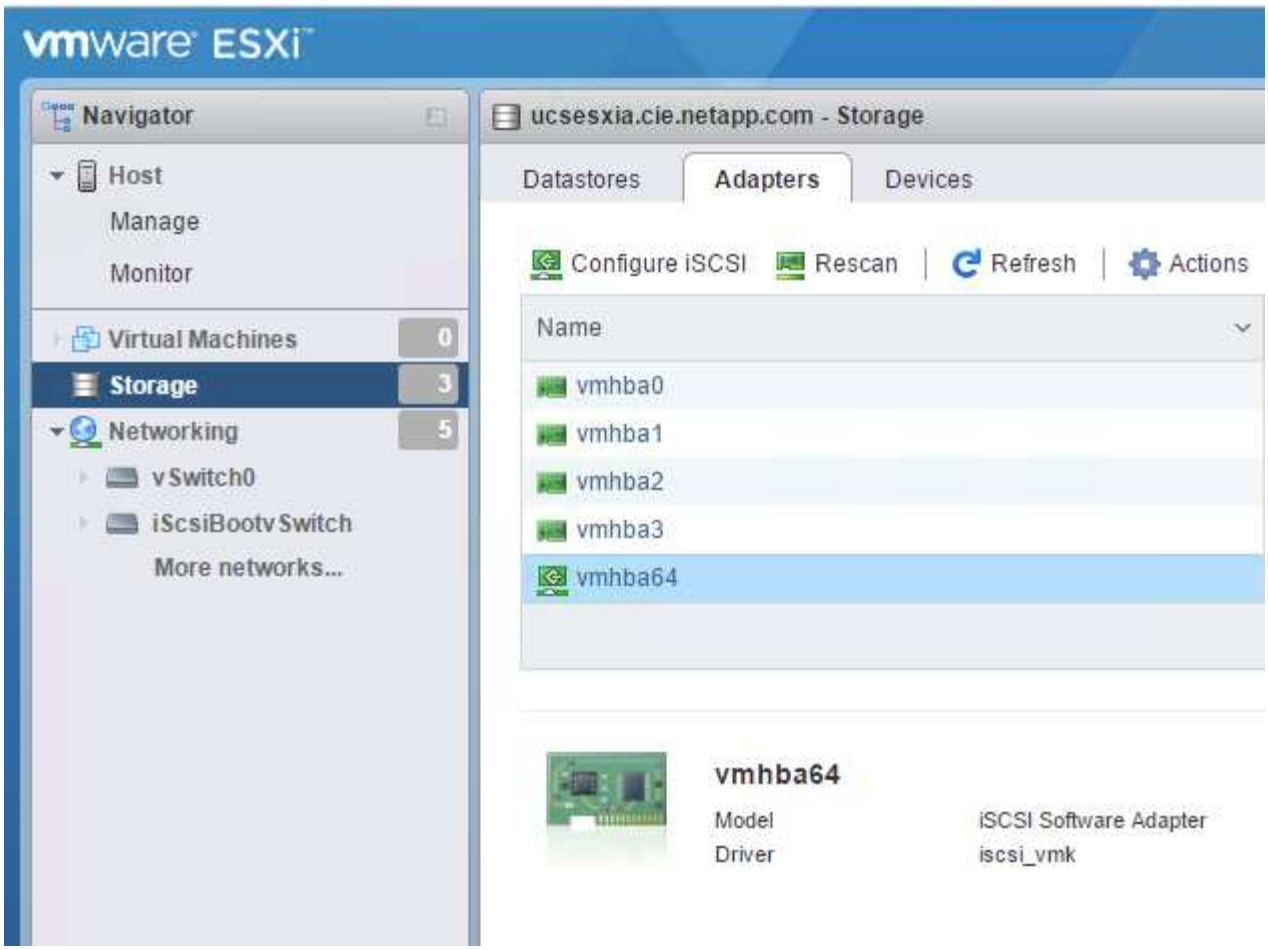


「 iScsiBootPG-A 」で MTU を 9000 に設定します

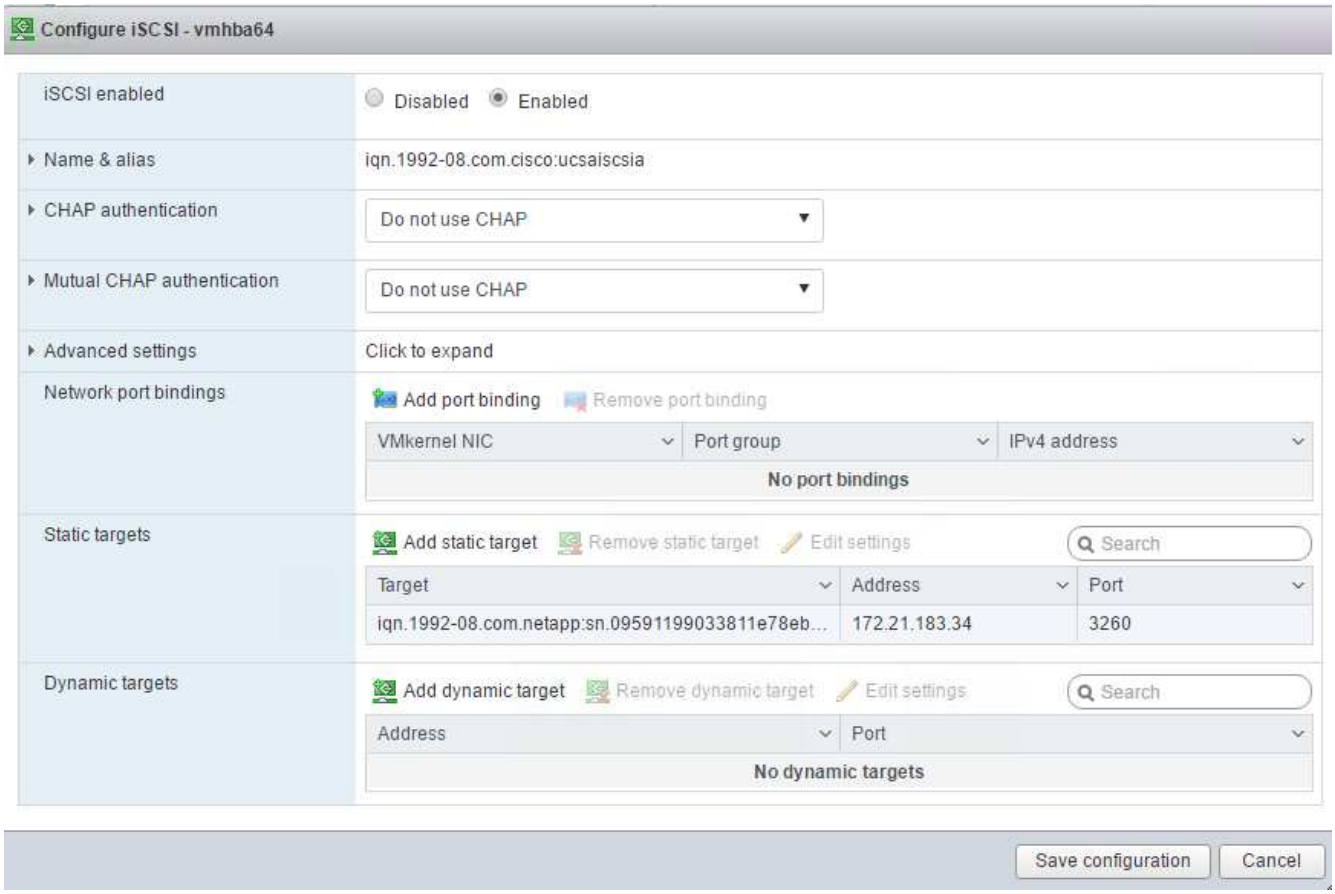
iSCSI マルチパスを設定します

ESXi ホストで iSCSI マルチパスを設定するには、次の手順を実行します。

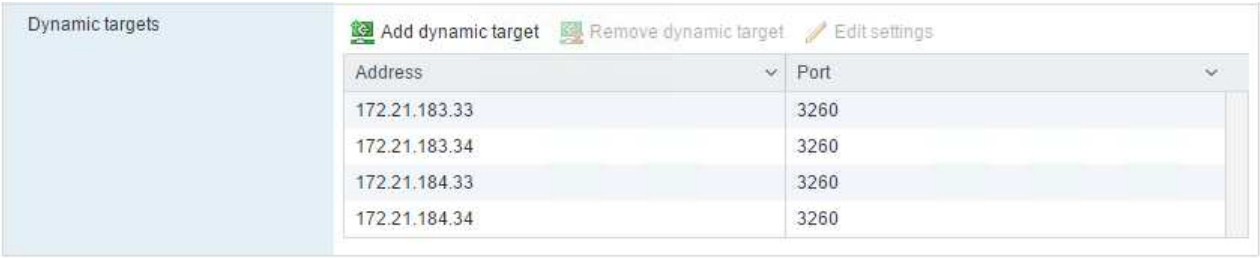
1. 左側のナビゲーションペインで Storage （ストレージ）を選択します。アダプタをクリックします。
2. iSCSI ソフトウェアアダプタを選択し、 Configure iSCSI （ iSCSI の設定）をクリックします。



3. [動的ターゲット] で、 [動的ターゲットの追加] をクリックします。



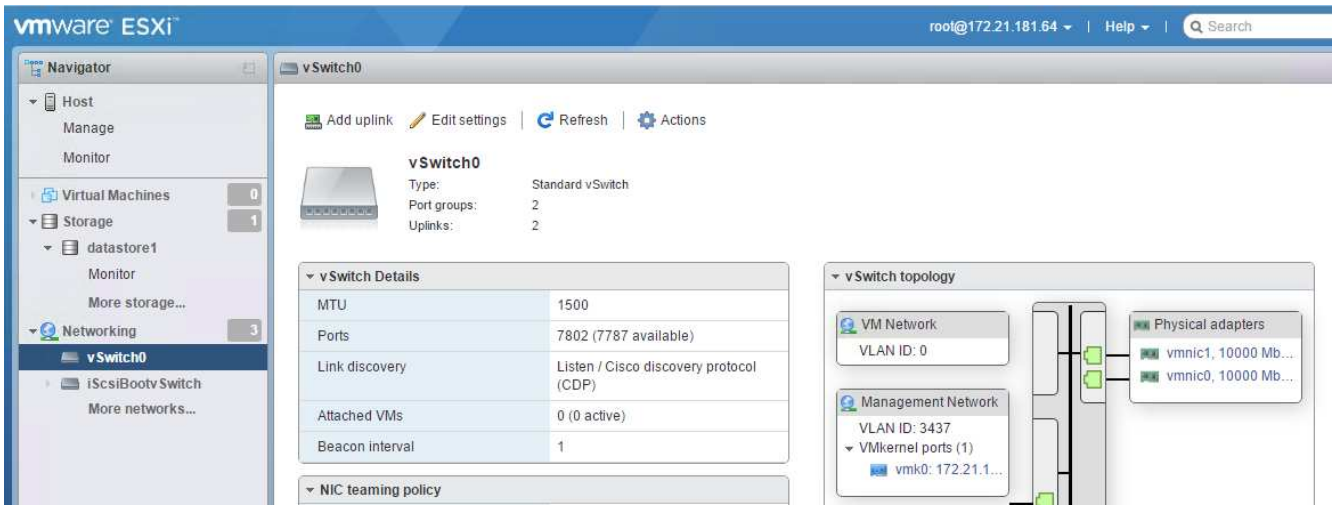
4. IP アドレス「 iscsi_dlif01a 」を入力します。
   - IP アドレス 'iSCSI_lif01b'iSCSI_lif02a'iSCSI_lif02b' で繰り返します
   - [Save Configuration] をクリックします。



iSCSI LIF の IP アドレスは、ネットアップクラスタで「 network interface show 」コマンドを実行するか、 OnCommand の System Manager の Network Interfaces タブで確認できます。

ESXi ホストを設定

1. 左側のナビゲーションペインで、 [ネットワーク] を選択します。
2. vSwitch0 を選択します。



3. 設定の編集を選択します。
4. MTU を 9000 に変更します。
5. NIC チーミングを展開し、 vmnic0 と vmnic1 の両方がアクティブに設定されていることを確認します。

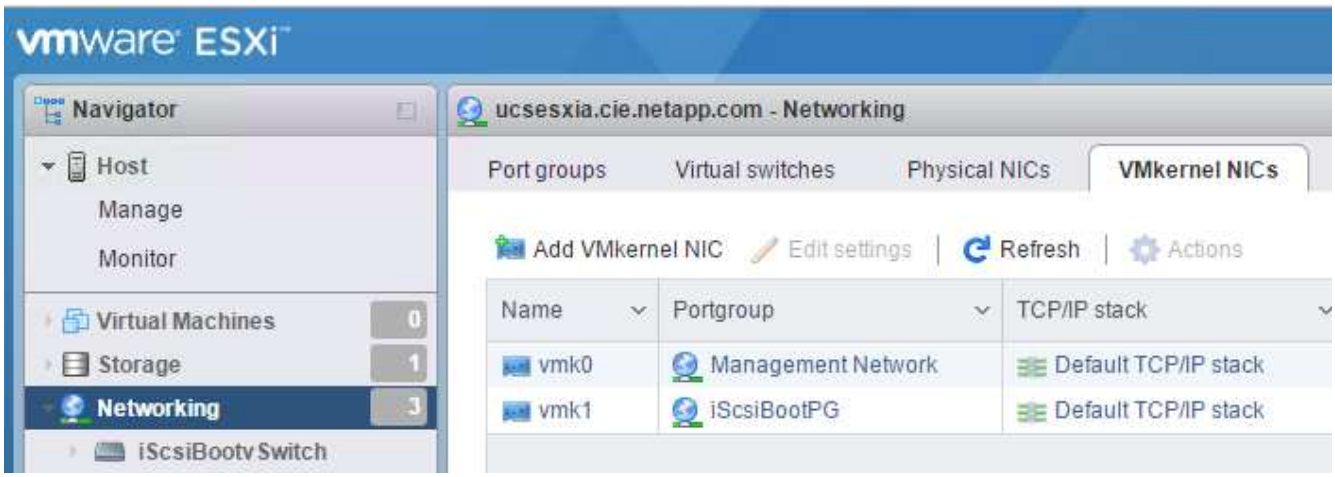
ポートグループと **VMkernel NIC** を設定します

1. 左側のナビゲーションペインで、 [ネットワーク] を選択します。
2. Port Groups タブを右クリックします。

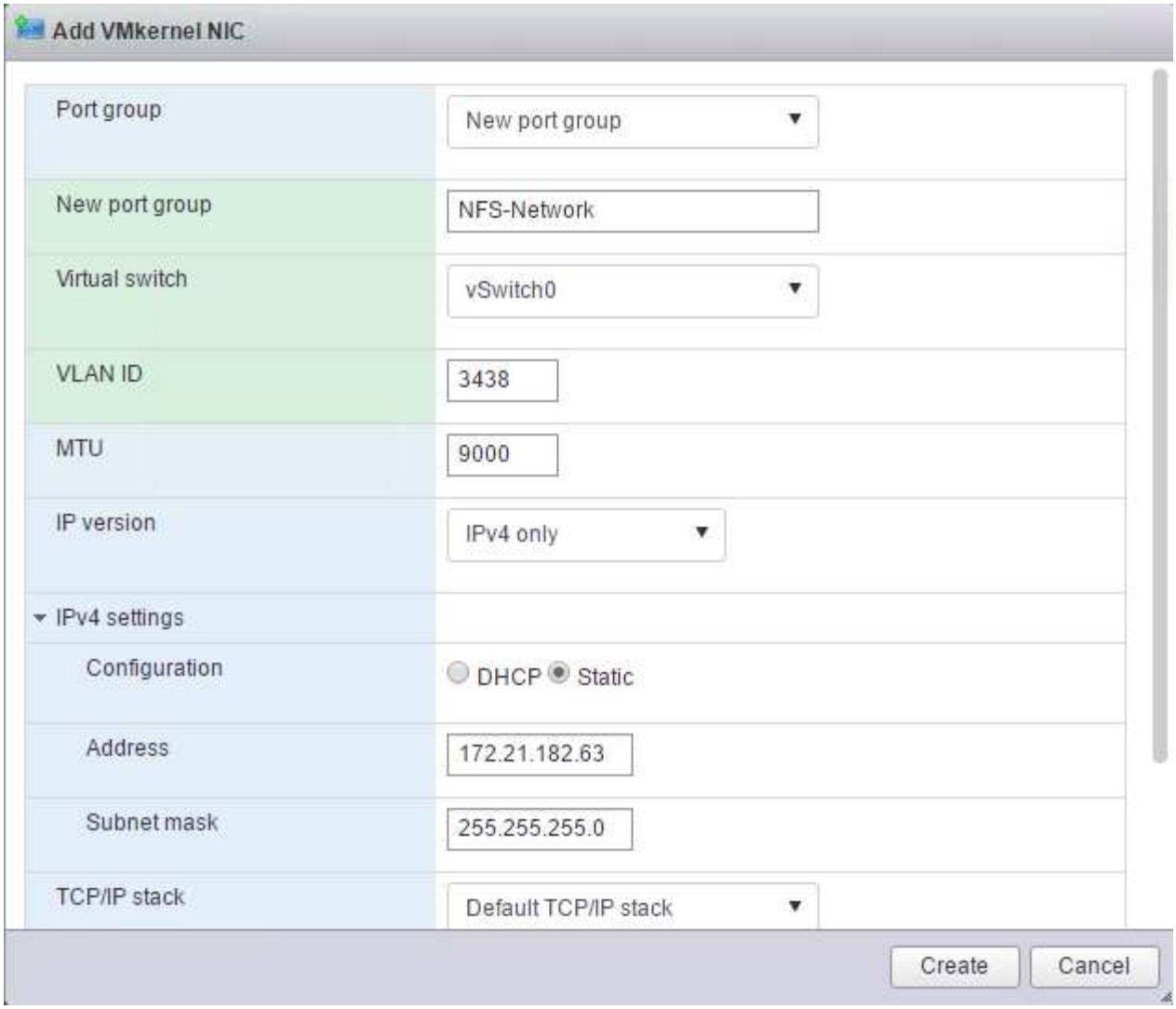
3. [VM Network] を右クリックし、 [Edit] を選択します。VLAN ID を「 <<var_vm_traffic_vlan>> 」に変更します。
4. [Add Port Group] をクリックします。
   - ポートグループに「 MGMT-Network 」という名前を付けます。
   - VLAN ID に「 \ <mgmt_vlan>> 」と入力します。
   - vSwitch0 が選択されていることを確認してください。

- 追加をクリックします。

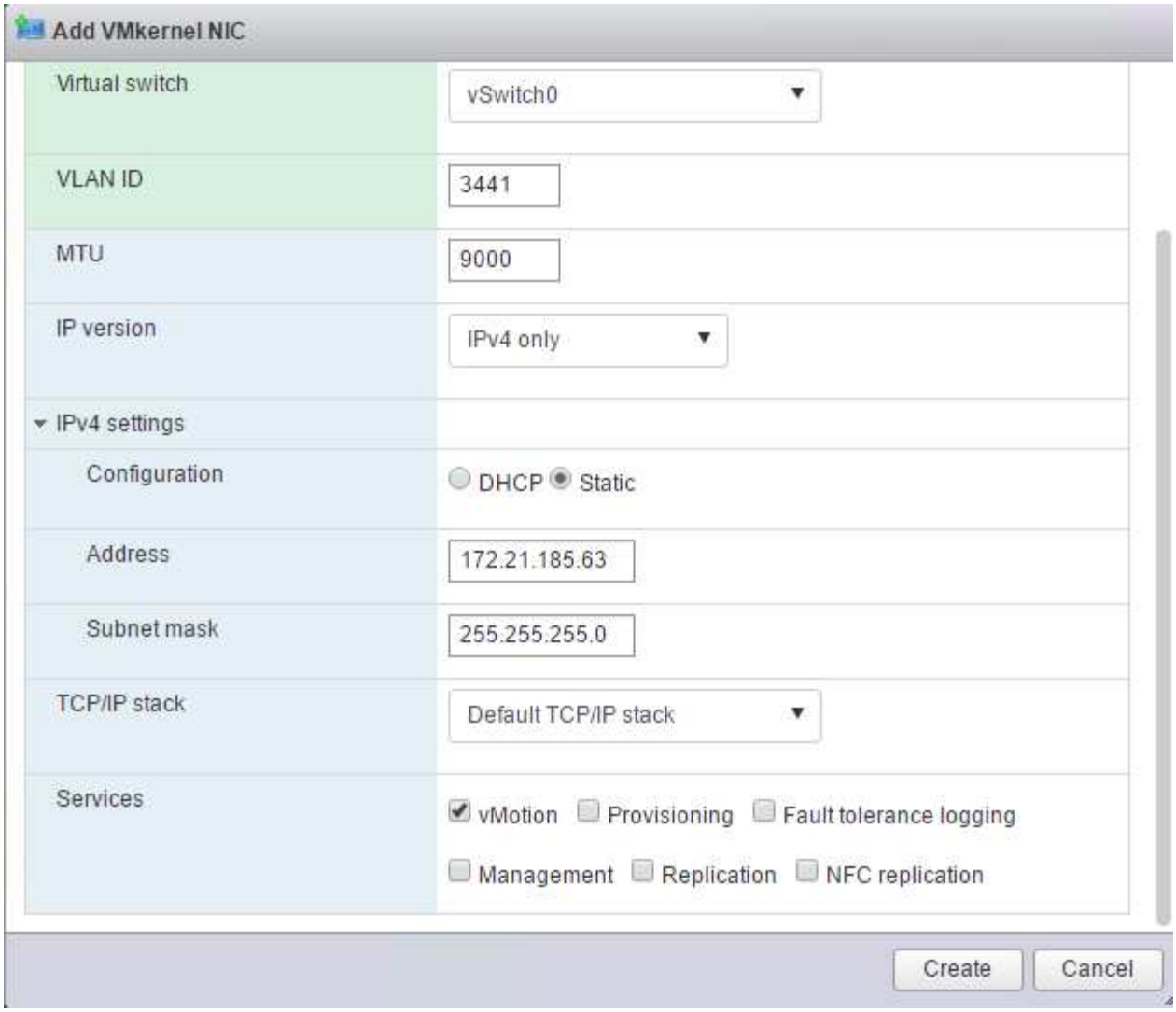
5. [VMkernel NICs] タブをクリックします。



6. Add VMkernel NIC を選択します。
   - [新しいポートグループ] を選択します。
   - ポートグループに「 NFS-Network 」という名前を付けます。
   - VLAN ID として「 \<nfs_vlan_id>` 」と入力します。
   - MTU を 9000 に変更します。
   - IPv4 設定を展開します。
   - 静的設定を選択します。
   - アドレスとして「 \<<var_hosta_nfs_ip>> 」と入力します。
   - [サブネットマスク] に「 \<<var_hosta_nfs_mask>> 」と入力します。
   - Create をクリックします。 .



7. この手順を繰り返して、 vMotion VMkernel ポートを作成します。
8. Add VMkernel NIC を選択します。
   a. [新しいポートグループ] を選択します。
   b. ポートグループに vMotion という名前を付けます。
   c. VLAN ID に「 \<VMotion_vlan_id>> 」と入力します。
   d. MTU を 9000 に変更します。
   e. IPv4 設定を展開します。
   f. 静的設定を選択します。
   g. アドレスとして「 <<var_hosta_VMotion_ip>> 」と入力します。
   h. Subnet Mask には「 \<<var_hosta_vMotion mask>> 」と入力します。
   i. IPv4 の設定後に vMotion チェックボックスが選択されていることを確認します。

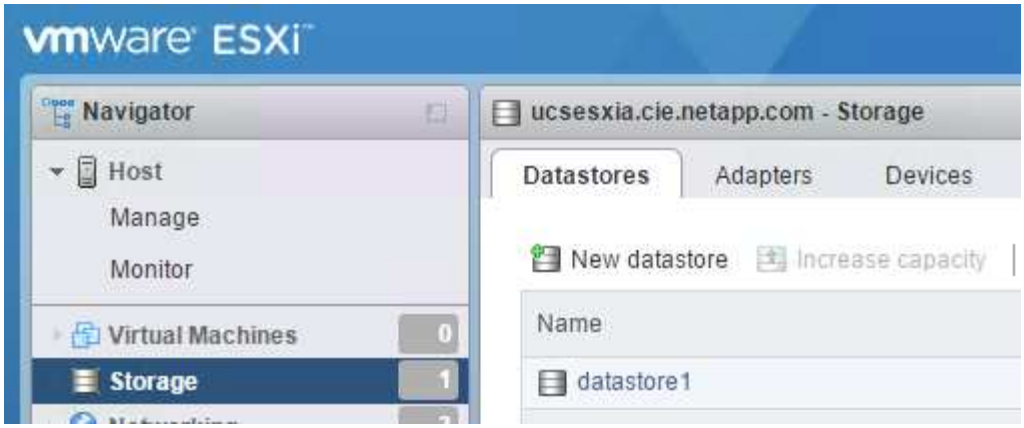


ESXi ネットワークの設定には、ライセンスで許可されている場合に VMware vSphere Distributed Switch を使用するなどの方法が多数あります。ビジネス要件を満たす必要がある場合は、 FlexPod Express で代替ネットワーク構成がサポートされます。

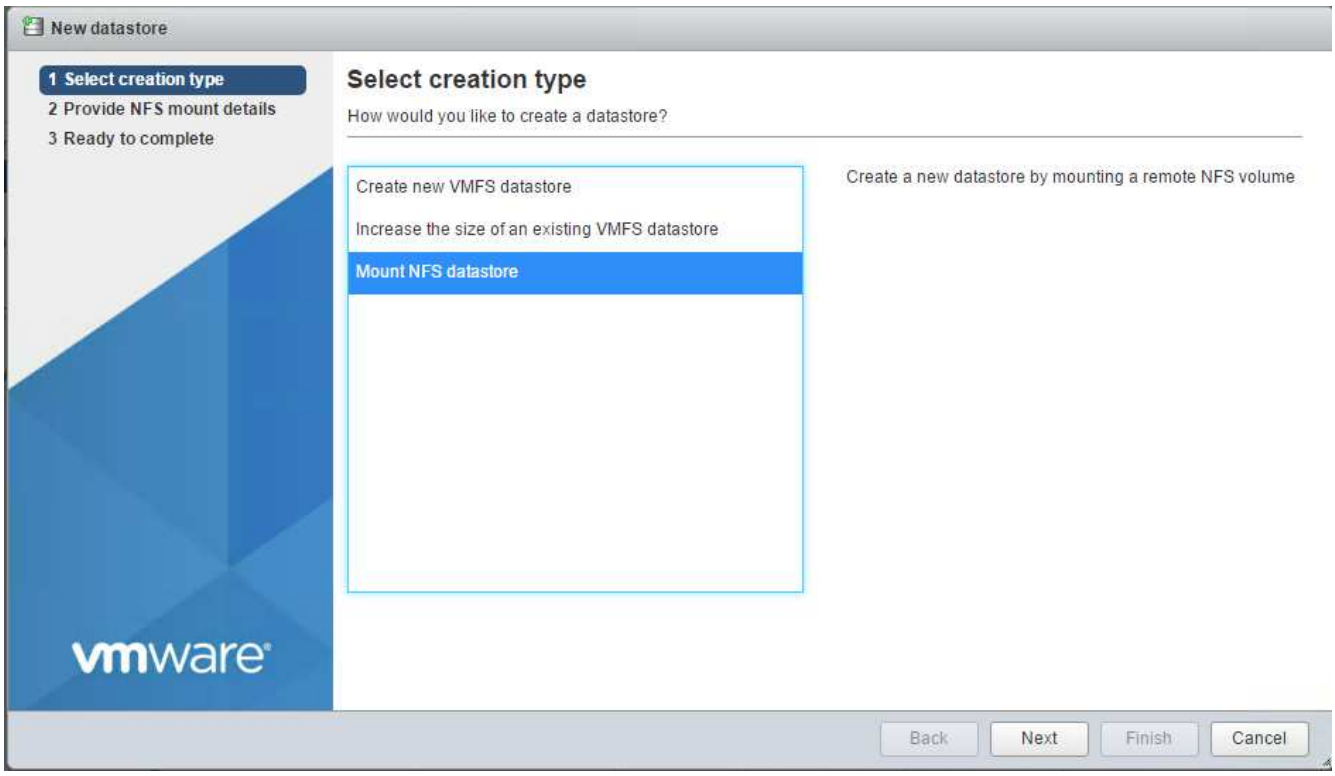
最初のデータストアをマウント

最初にマウントするデータストアは、仮想マシン用の infra_datastore_1 データストア、仮想マシンのスワップファイル用の infra_swap データストアです。

1. 左側のナビゲーションペインで [ストレージ] をクリックし、 [新しいデータストア] をクリックします。



2. マウント NFS データストアを選択します。



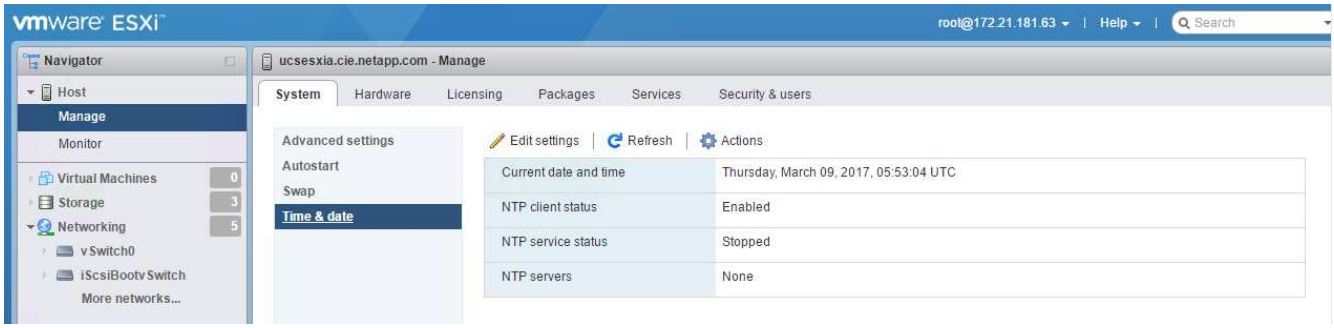
3. 次に、 Provide NFS Mount Details （ NFS マウントの詳細の提供）ページに次の情報を入力します。
   - 名前： 'infra_datastore_1'
   - NFS サーバ : `\<<var_nodeA_nfs_lif>`
   - 共有： /infra_datastor_1
   - NFS 3 が選択されていることを確認します。
4. 完了をクリックします。[最近のタスク] ペインにタスクの完了が表示されます。
5. 同じ手順で infra_swap データストアをマウントします。
   - 名前： infra_swap
   - NFS サーバ : `\<<var_nodeA_nfs_lif>`
   - 共有 :`/infra_swap

- NFS 3 が選択されていることを確認します。

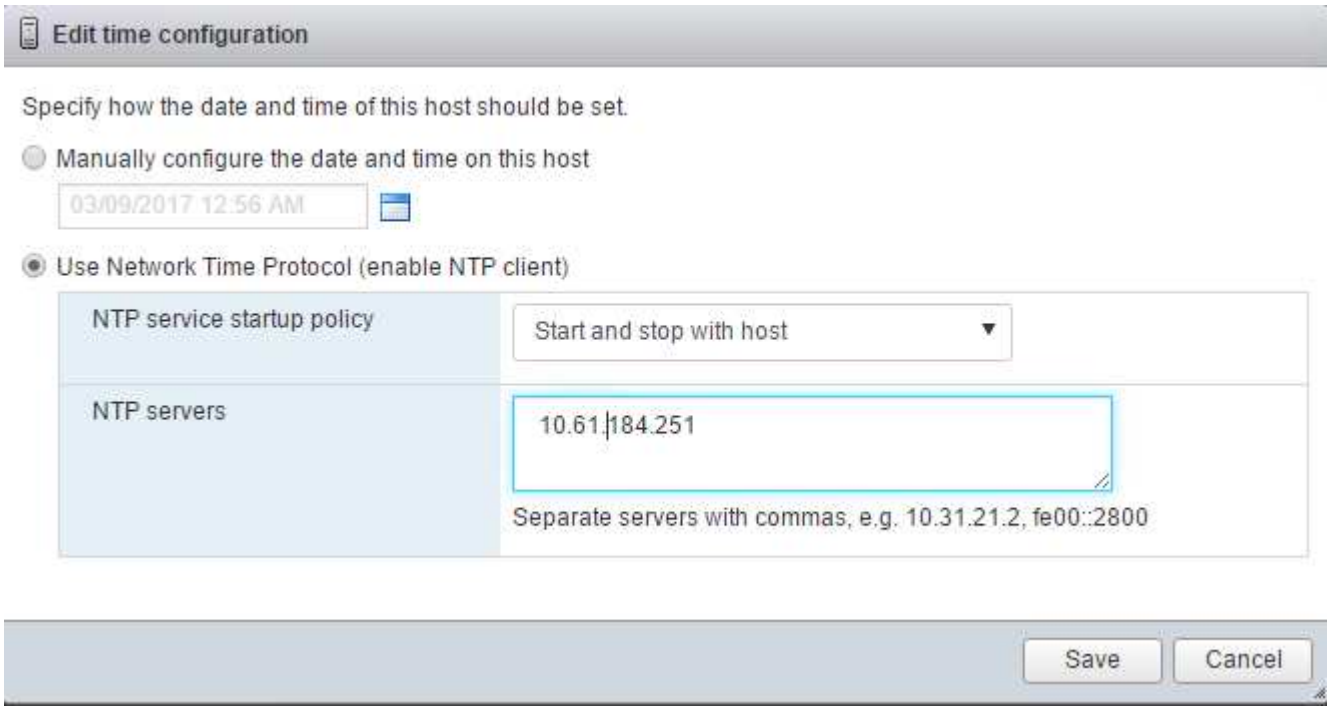
NTP を設定します

ESXi ホストの NTP を設定するには、次の手順を実行します。

1. 左側のナビゲーションペインで、 [管理] をクリックします。右側のペインで [システム] を選択し、 [時刻と日付] をクリックします。



2. Use Network Time Protocol （ NTP クライアントを有効にする）を選択します。
3. NTP サービスのスタートアップポリシーとして、 Start and Stop With Host を選択します。
4. NTP サーバとして「 <<var_ntp>> 」と入力します。複数の NTP サーバを設定できます。
5. [保存] をクリックします .

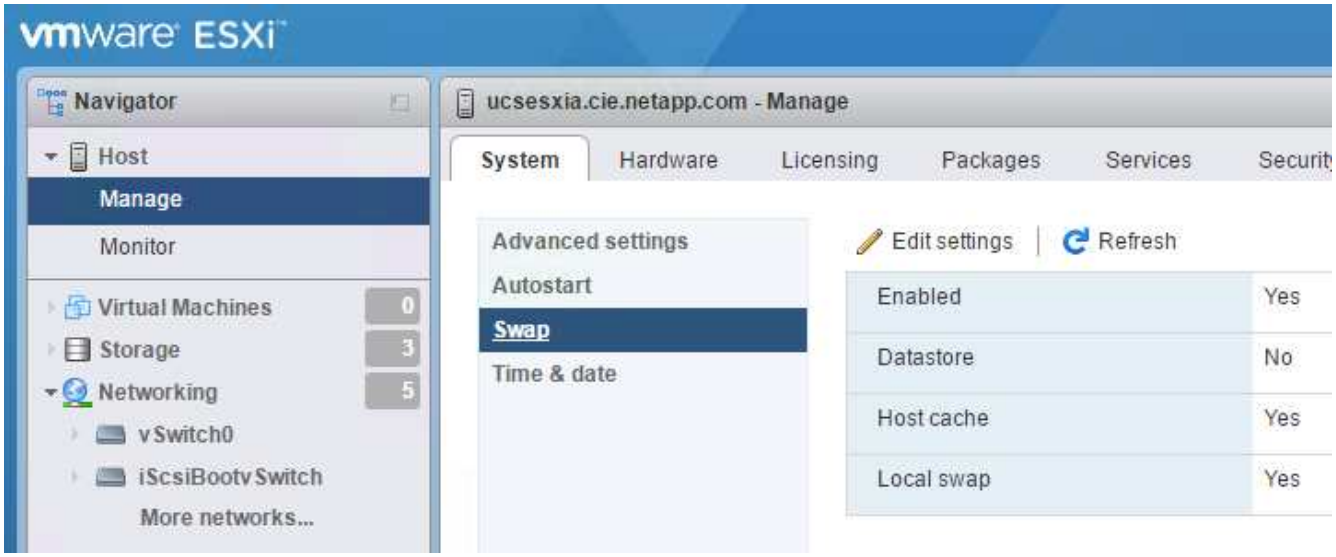


仮想マシンのスワップファイルの場所を移動します

ここでは、仮想マシンのスワップファイルの場所を移動する手順について説明します。

1. 左側のナビゲーションペインで、 [管理] をクリックします。右側のペインでシステムを選択し、スワッ

プをクリックします。



2. 設定の編集をクリックします。データストアのオプションから infra_swap を選択します。

3. [保存] をクリックします .

NetApp NFS Plug-in 1.0.20 for VMware VAAI をインストールします

NetApp NFS Plug-in 1.0.20 for VMware VAAI をインストールするには、次の手順を実行します。

1. 次のコマンドを入力して、 VAAI が有効になっていることを確認します。

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

VAAI が有効な場合、次のような出力が表示されます。

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. VAAI が有効になっていない場合は、次のコマンドを入力して VAAI を有効にします。

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

これらのコマンドの出力は次のとおりです。

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. NetApp NFS Plug-in for VMware VAAI をダウンロードします。
   a. にアクセスします "ソフトウェアダウンロードページ"。
   b. 下にスクロールして、 NetApp NFS Plug-in for VMware VAAI をクリックします。
   c. ESXi プラットフォームを選択します。
   d. 最新のプラグインのオフラインバンドル（ .zip ）またはオンラインバンドル（ .vib ）をダウンロードします。
4. ESX CLI を使用して、 ESXi ホストにプラグインをインストールします。
5. ESXi ホストをリブートします。

```
[root@vm-host-infra-04:~] ls /vmfs/volumes/datastore1/NetAppNasPlugin.vib
/vmfs/volumes/datastore1/NetAppNasPlugin.vib
[root@vm-host-infra-04:~] esxcli software vib install -v /vmfs/volumes/datastore1/NetAppNasPlugin.vib
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.1.2-3
   VIBs Removed:
   VIBs Skipped:
[root@vm-host-infra-04:~]
```

"次の手順： VMware vCenter Server 6.7 をインストールします"

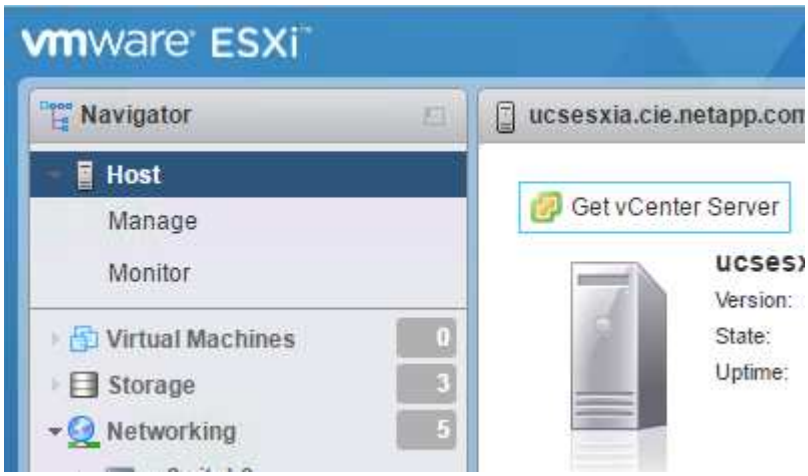
VMware vCenter Server 6.7 をインストールする

このセクションでは、 FlexPod 構成に VMware vCenter Server 6.7 をインストールする詳細な手順について説明します。

FlexPod Express では、 VMware vCenter Server Appliance （ VCSA ）を使用します。

VMware vCenter Server Appliance をダウンロードします

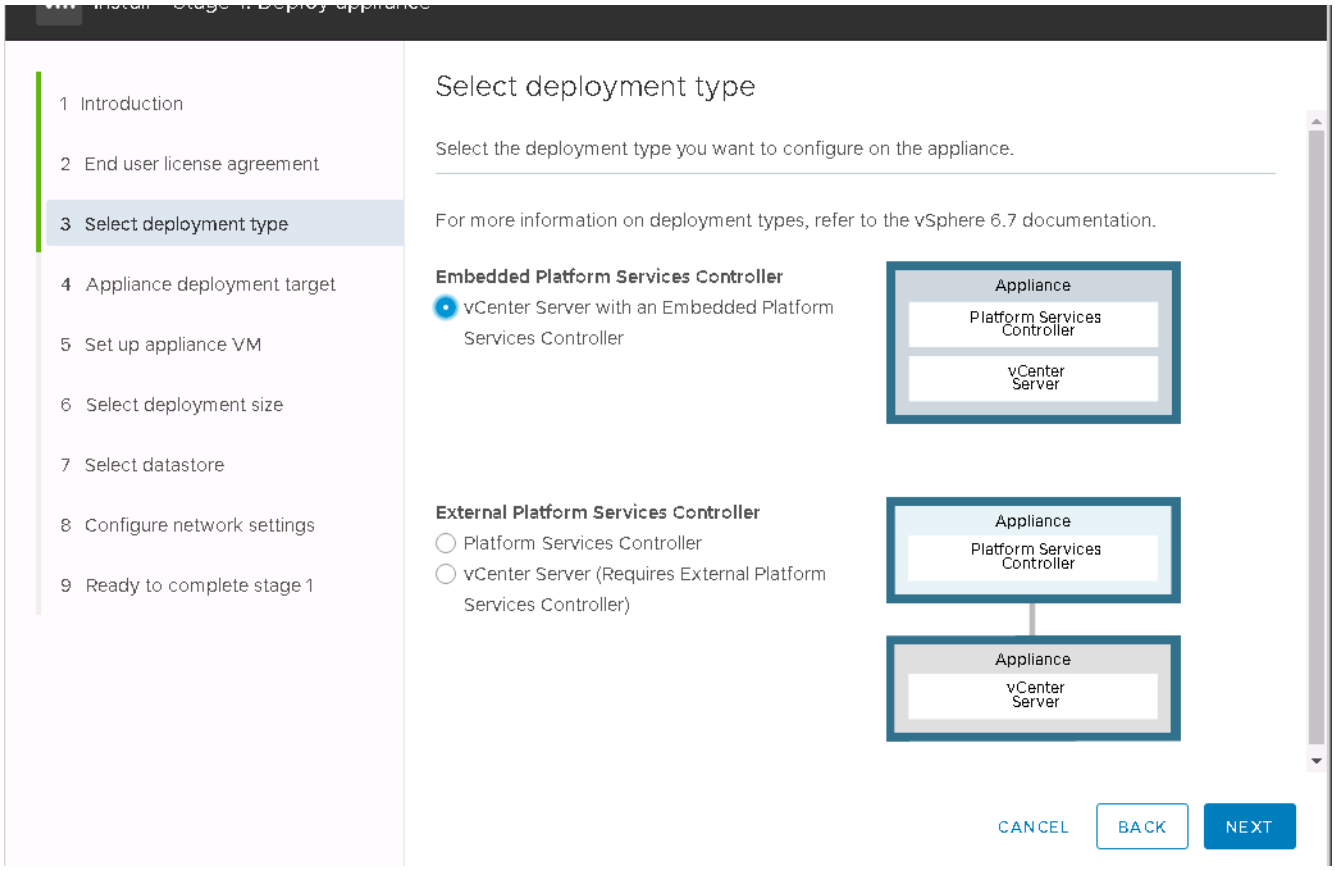
1. vCSA をダウンロードします。ESXi ホストの管理時に Get vCenter Server アイコンをクリックして、ダウンロードリンクにアクセスします。



2. vCSA を VMware サイトからダウンロードします。

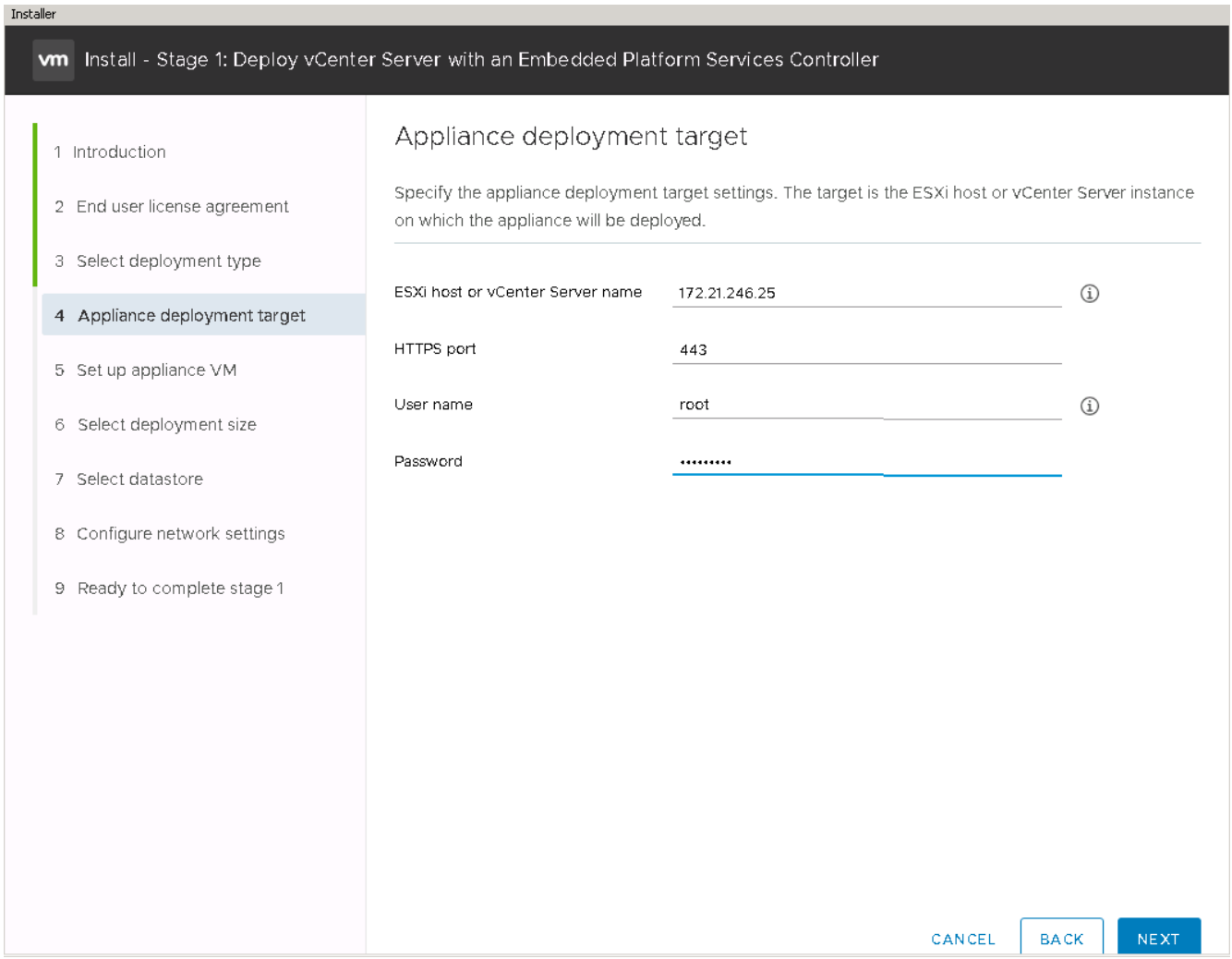
インストール可能な Microsoft Windows vCenter Server がサポートされますが、 VMware では新しい導入に vCSA を推奨します。

3. ISO イメージをマウントします。
4. VCSA -ui-installer > win32 ディレクトリに移動します。installer.exe をダブルクリックします。
5. [インストール] をクリックします
6. [はじめに] ページで [次へ] をクリックします。
7. エンドユーザライセンス契約に同意します。
8. 展開タイプとして、 Embedded Platform Services Controller を選択します。

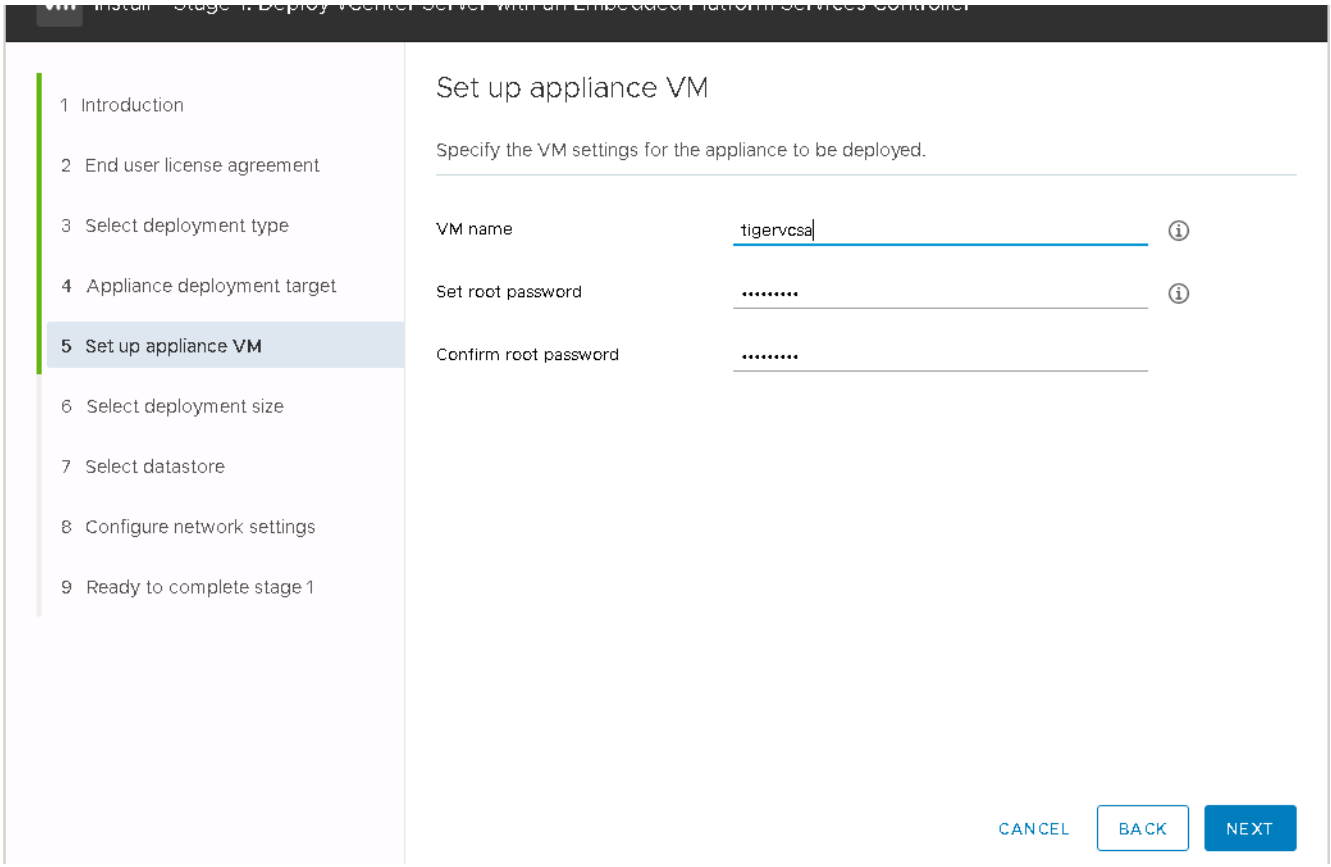


必要に応じて、 FlexPod Express 解決策の一部として、外部プラットフォームサービスコントローラの導入もサポートされます。

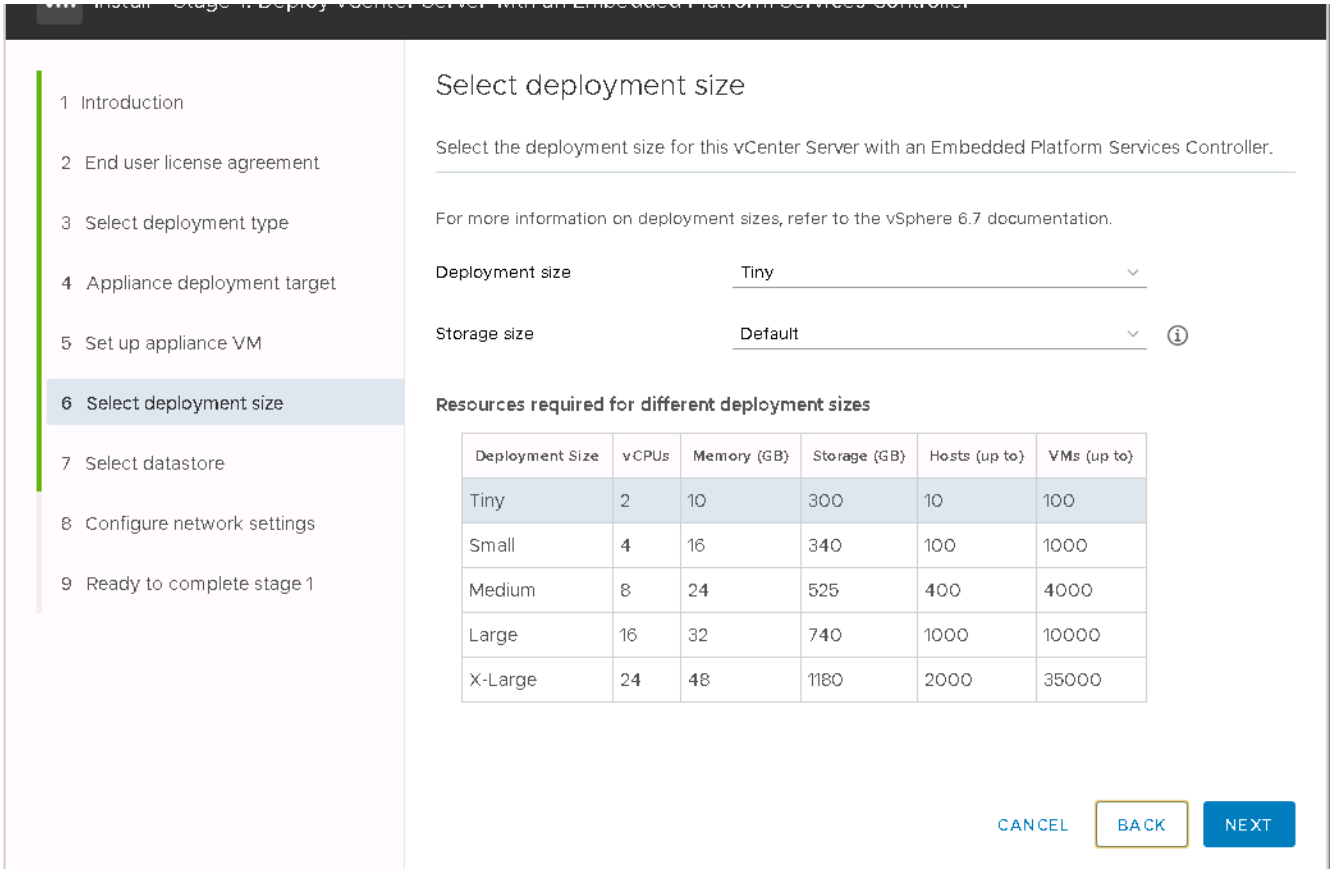
9. アプライアンス導入ターゲットで、導入した ESXi ホストの IP アドレス、および root ユーザ名と root パスワードを入力します。



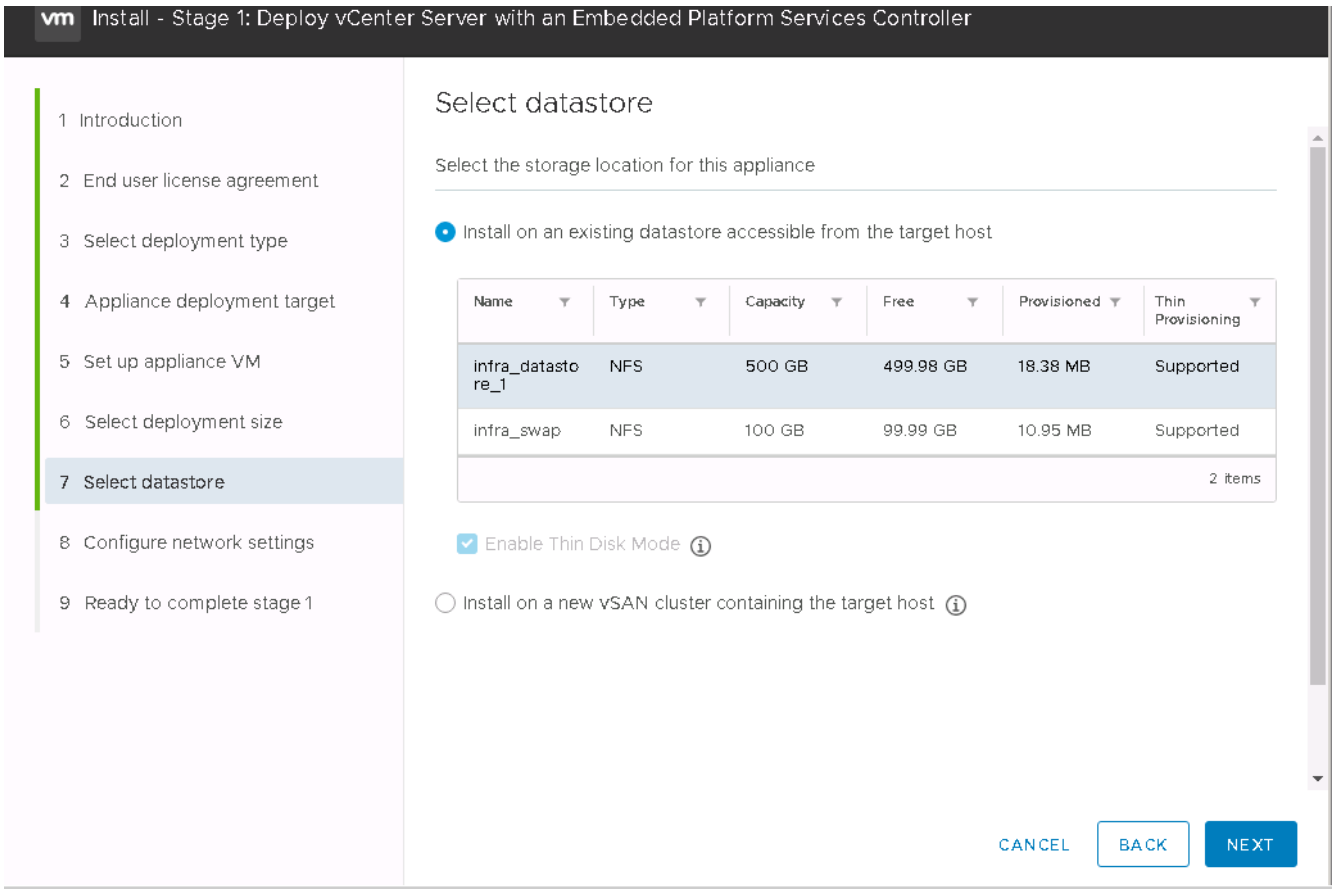
10. VCSA を VM 名として「 VCSA 」に入力し、 VCSA に使用するルート・パスワードを設定します。



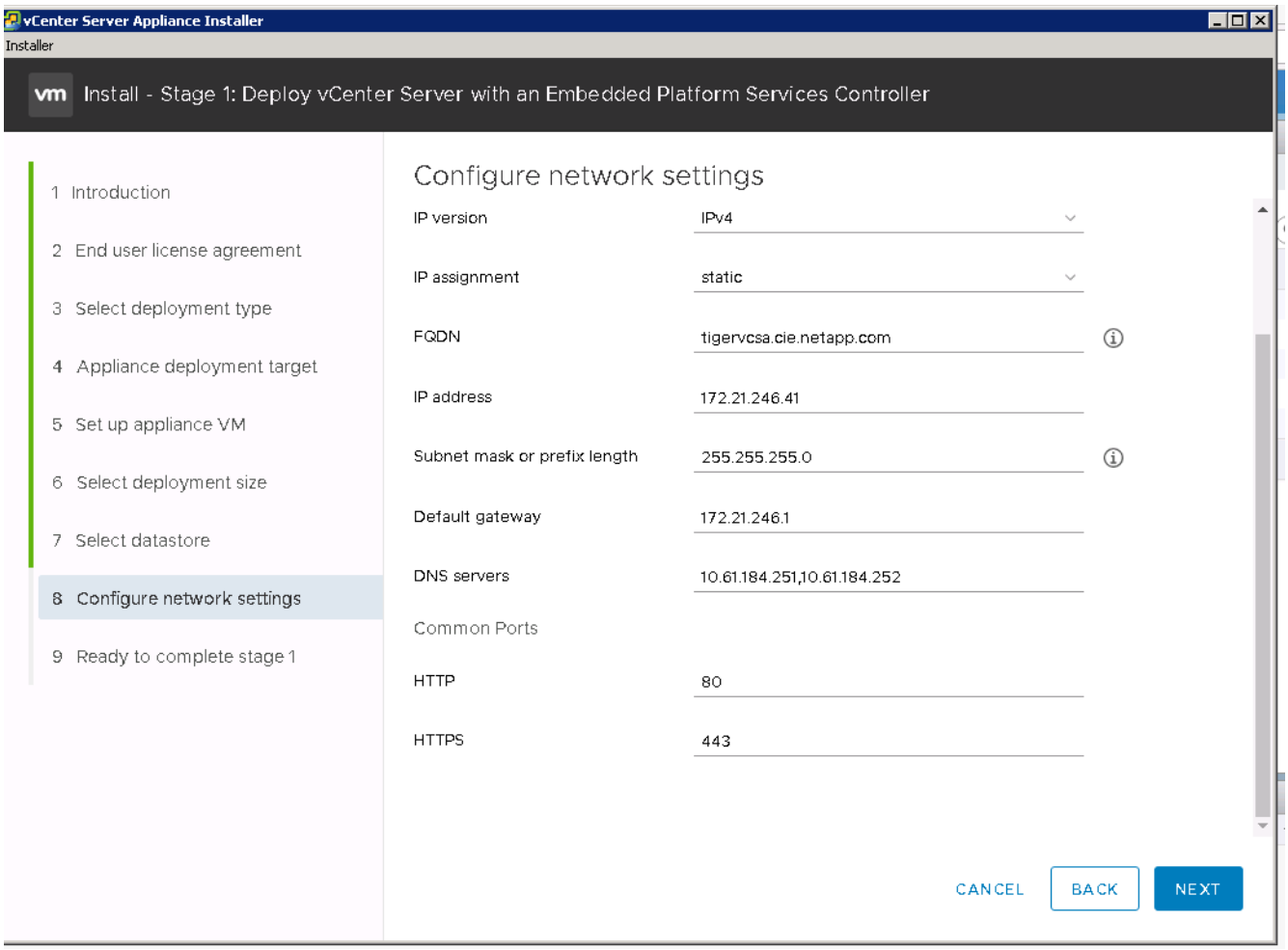
11. 環境に最も適した導入サイズを選択してください。次へをクリックします。



12. infra_datastore_1 データストアを選択します。次へをクリックします。

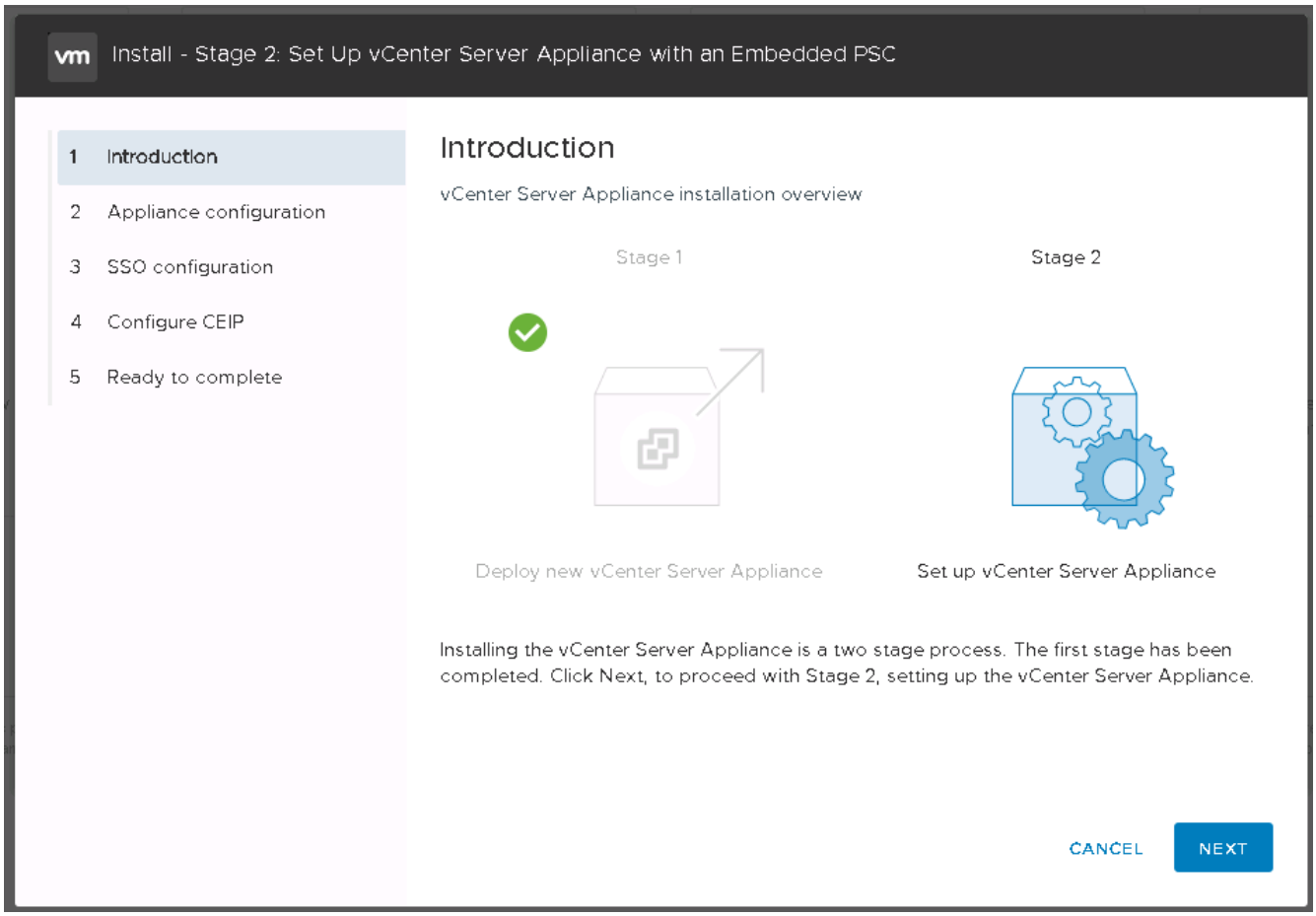


13. Configure network settings （ネットワーク設定の設定）ページで次の情報を入力し、 Next （次へ）をクリックします。
    a. MGMT - Network （ネットワーク）を選択します。
    b. vCSA に使用する FQDN または IP を入力します。
    c. 使用する IP アドレスを入力します。
    d. 使用するサブネットマスクを入力します。
    e. デフォルトゲートウェイを入力します。
    f. DNS サーバを入力します。
14. 「ステージ 1 を完了する準備ができました」ページで、入力した設定が正しいことを確認します。完了をクリックします。



vCSA がインストールされます。このプロセスには数分かかります。

15. ステージ 1 が完了すると、完了したことを示すメッセージが表示されます。「続行」をクリックしてステージ 2 の設定を開始します。
16. 「ステージ 2 の紹介」ページで、「次へ」をクリックします。



17. NTP サーバのアドレスとして「 \<<var_ntp_id>> 」と入力します。複数の NTP IP アドレスを入力できます。

    vCenter Server High Availability （ HA ；高可用性）を使用する場合は、 SSH アクセスが有効になっていることを確認してください。

18. SSO ドメイン名、パスワード、およびサイト名を設定します。次へをクリックします。

    特に vSphere.local ドメイン名から外れる場合は、これらの値を参考にしてください。

19. 必要に応じて、 VMware カスタマーエクスペリエンスプログラムに参加します。次へをクリックします。
20. 設定の概要を確認します。[完了] をクリックするか、 [戻る] ボタンを使用して設定を編集します。
21. インストールの開始後に、インストールを一時停止または終了できないことを示すメッセージが表示されます。[OK] をクリックして続行します。

    アプライアンスの設定が続行されます。これには数分かかります。

    セットアップが正常に完了したことを示すメッセージが表示されます。

    インストーラが vCenter Server にアクセスするために提供するリンクはクリック可能です。

"次の手順： VMware vCenter Server 6.7 と vSphere クラスタリングを設定します。"

VMware vCenter Server 6.7 および **vSphere** クラスタリングを設定する

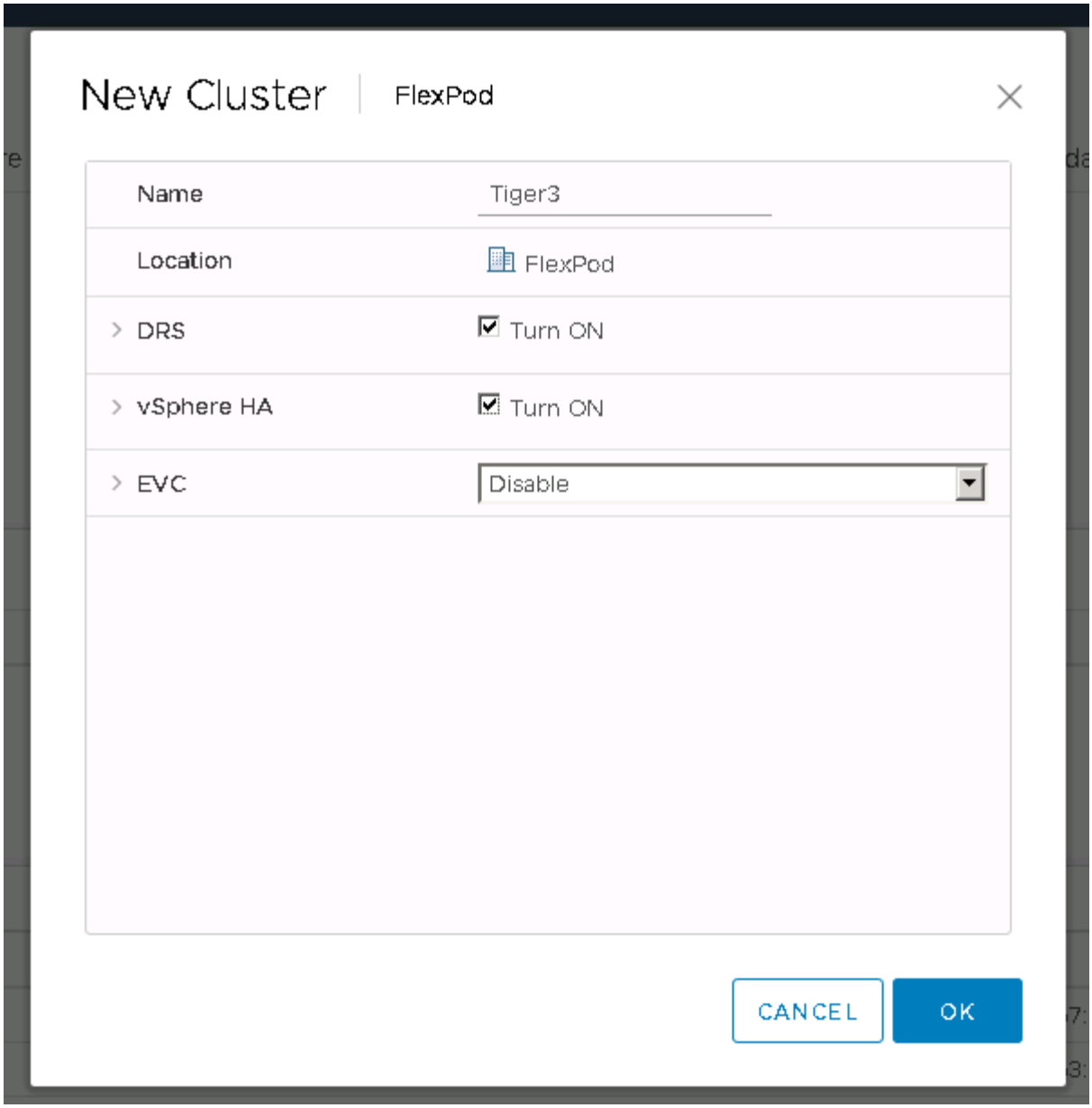
VMware vCenter Server 6.7 および vSphere クラスタリングを設定するには、次の手順を実行します。

1. https://\<<FQDN または IP of vCenter >> /vsphere-client/ に移動します。
2. vSphere Client の起動をクリックします。
3. vCSA のセットアッププロセスで入力したユーザ名 mailto ： administrator@vspehre.loca l [administrator@vsphere.loca l^] と SSO パスワードを使用してログインします。
4. vCenter 名を右クリックし、 New Datacenter を選択します。
5. データセンターの名前を入力し、 [OK] をクリックします。

vSphere クラスタを作成します

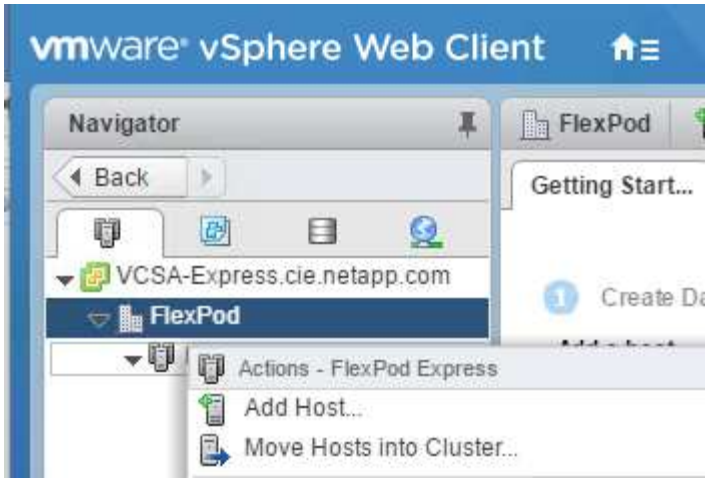
vSphere クラスタを作成するには、次の手順を実行します。

1. 新しく作成したデータセンターを右クリックし、 [New Cluster] を選択します。
2. クラスタの名前を入力します。
3. チェックボックスをオンにして DR と vSphere HA を有効にします。
4. [OK] をクリックします。



ESXi ホストをクラスタに追加

1. クラスタを右クリックし、 Add Host （ホストの追加）を選択します。



2. ESXi ホストをクラスタに追加するには、次の手順を実行します。
   a. ホストの IP または FQDN を入力します。次へをクリックします。
   b. root ユーザ名とパスワードを入力します。次へをクリックします。
   c. Yes をクリックして、ホストの証明書を VMware 証明書サーバによって署名された証明書に置き換えます。
   d. [Host Summary] ページで [Next] をクリックします。
   e. 緑の + アイコンをクリックして、 vSphere ホストにライセンスを追加します。

      この手順は、必要に応じてあとで実行できます。

   f. [次へ] をクリックして、ロックダウンモードを無効のままに
   g. [VM の場所] ページで [次へ] をクリックします。
   h. [Ready to Complete] ページを確認します。[戻る] ボタンを使用して変更を行うか、 [完了] を選択します。
3. Cisco UCS ホスト B に対して手順 1 と 2 を繰り返しますFlexPod 構成にホストを追加する場合は、この手順を実行する必要があります。

ESXi ホストにコアダンプを設定します

1. SSH を使用して管理 IP ESXi ホストに接続し、ユーザ名に「 root 」と入力して、 root パスワードを入力します。
2. 次のコマンドを実行します。

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

3. 最終コマンドを入力すると、「 Verified the configured netdump server is running 」というメッセージが表示されます。

FlexPod Express にホストを追加する場合は、このプロセスを完了する必要があります。

まとめ

FlexPod Express は、業界をリードするコンポーネントを使用した検証済みの設計を提供することで、シンプルで効果的な解決策を実現します。FlexPod Express は、コンポーネントを追加することで拡張できるため、特定のビジネスニーズに合わせてカスタマイズできます。FlexPod Express は、中小規模の企業や、専用のソリューションを必要とする ROBO などの企業を念頭に置いて設計されました。

追加情報の参照先

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。

- ネットアップの製品マニュアル

  "http://docs.netapp.com"

- FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 Design Guide 』

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

FlexPod Express と VMware vSphere 6.7U1 、および直接接続型の IP ベースストレージを搭載した NetApp AFF A220

NVA-1131 - 導入： VMware vSphere 6.7U1 搭載の FlexPod Express と、直接接続型の IP ベースのストレージを搭載した NetApp AFF A220

ネットアップ、 Sree Lakshmi Lanka です

業界のトレンドは、共有インフラとクラウドコンピューティングへの大規模なデータセンターの移行を示しています。さらに、リモートオフィスやブランチオフィスにもシンプルで効果的な解決策を導入し、データセンターでよく使用されているテクノロジを活用することができます。

FlexPod Express は、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus ファミリースイッチ、およびネットアップストレージテクノロジを基盤とした、事前設計されたベストプラクティスアーキテクチャです。FlexPod Express システムのコンポーネントは、 FlexPod Datacenter と同様に、小規模な IT インフラ環境全体での管理面の相乗効果を実現します。FlexPod Datacenter と FlexPod Express は、仮想化、ベアメタル OS 、エンタープライズワークロードに最適なプラットフォームです。

FlexPod Datacenter と FlexPod Express は、ベースライン構成が可能で、多種多様なユースケースや要件に対応できるよう、サイジングと最適化が可能な汎用性を備えています。FlexPod データセンターを利用している既存のお客様は、使い慣れたツールを使用して FlexPod Express システムを管理できます。FlexPod Express の新規のお客様は、環境の拡大に合わせて FlexPod データセンターの管理を容易に行うことができます。

FlexPod Express は、リモートオフィスやブランチオフィス（ ROBO ）、中堅企業向けの最適なインフラ基盤です。また、専用のワークロードにインフラを提供したいお客様にも最適な解決策です。

FlexPod Express は、ほぼすべてのワークロードに適した、管理しやすいインフラを提供します。

解決策の概要

この FlexPod Express 解決策は、 FlexPod コンバージドインフラプログラムの一部です。

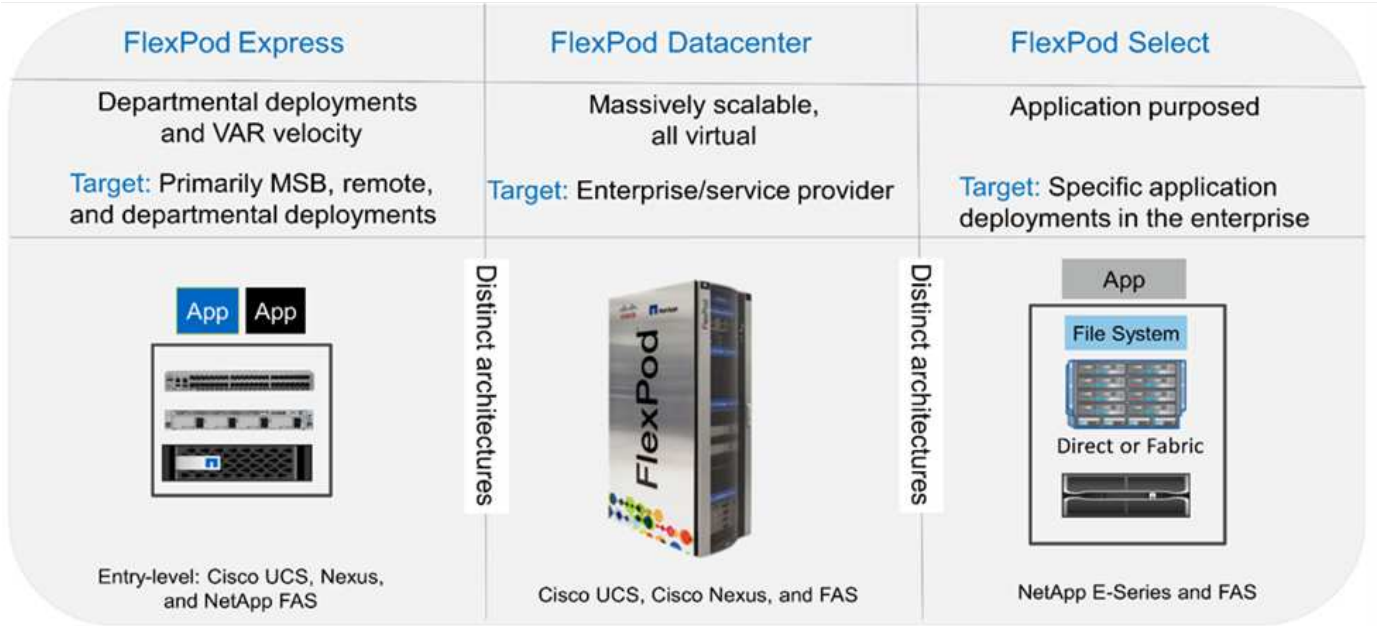
FlexPod 統合インフラプログラム

FlexPod リファレンスアーキテクチャは、 Cisco Validated Design （ CVD ；シスコ検証済み設計）または NetApp Verified Architectures （ NVA ；ネットアップ検証済みアーキテクチャ）として提供されます。これらのバリエーションでサポートされない構成が作成されない場合、特定の CVD または NVA からのお客様の要件に基づく差異は認められます。

次の図に示すように、 FlexPod プログラムには、 FlexPod Express 、 FlexPod Datacenter 、 FlexPod Select の 3 つのソリューションが含まれています。

- * FlexPod Express * は、 Cisco とネットアップが提供するテクノロジを搭載したエントリレベルの解決策をお客様に提供します。
- * FlexPod Datacenter * は、さまざまなワークロードやアプリケーションに最適な多目的基盤を提供します。
- * FlexPod Select * は、 FlexPod データセンターの最良の側面を組み込み、特定のアプリケーションにインフラストラクチャを調整します。

次の図に、解決策の技術コンポーネントを示します。



NetApp Verified Architecture プログラム

NVA プログラムは、ネットアップソリューションの検証済みアーキテクチャをお客様に提供します。NVA は、次の品質を持つ NetApp 解決策アーキテクチャを示しています。

- 入念にテストされています
- あらかじめ規定されている
- 導入リスクを最小限に抑えます
- 運用開始までの時間を短縮

このガイドでは、ネットアップストレージが直接接続された FlexPod Express の設計について詳しく説明します。次のセクションでは、この解決策の設計に使用されるコンポーネントについて説明します。

ハードウェアコンポーネント

- NetApp AFF A220
- Cisco UCS Mini
- Cisco UCS B200 M5
- Cisco UCS VIC 140/1480
- Cisco Nexus 3000 シリーズスイッチ

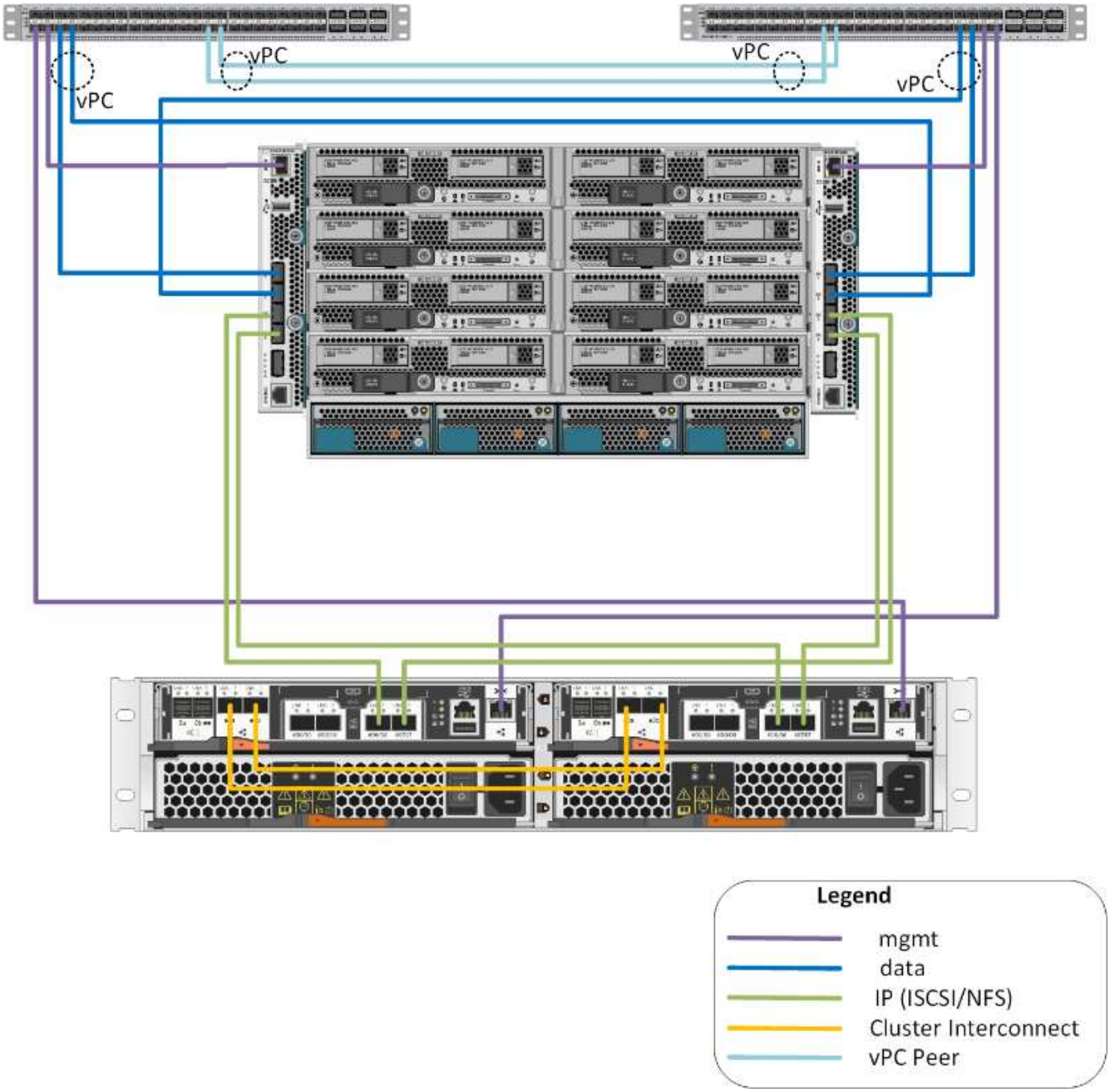
ソフトウェアコンポーネント

- NetApp ONTAP 9.5.
- VMWare vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Cisco NXOS ファームウェア 7.0(3) I6(1)

解決策テクノロジ

この解決策は、ネットアップ、 Cisco 、 VMware の最新テクノロジを活用しています。ONTAP 9.5 を実行する新しい NetApp AFF A220 、 Cisco Nexus 31108PCV スイッチが 2 台、 VMware vSphere 6.7U1 を実行する Cisco UCS B200 M5 サーバが搭載されています。検証済みのこの解決策では、 10GbE テクノロジ経由で Direct Connect IP ストレージを使用します。

次の図は、 FlexPod Express と VMware vSphere 6.7U1 IP ベースの Direct Connect アーキテクチャを示しています。



ユースケースの概要

FlexPod Express 解決策は、次のようないくつかのユースケースに適用できます。

- ROBOs
- 中堅・中小企業向け
- コスト効率に優れた専用の解決策が必要な環境

FlexPod Express は、仮想ワークロードと混在ワークロードに最適です。

テクノロジ要件

FlexPod Express システムには、ハードウェアコンポーネントとソフトウェアコンポーネントを組み合わせて使用する必要があります。FlexPod Express では、システムにハイパーバイザーノードを追加するために必要なハードウェアコンポーネントについても、 2 つのユニット単位で説明します。

ハードウェア要件

選択したハイパーバイザーに関係なく、すべての FlexPod Express 構成で同じハードウェアが使用されます。そのため、ビジネス要件が変わっても、どちらのハイパーバイザーも同じ FlexPod Express ハードウェア上で実行できます。

次の表に、すべての FlexPod 構成に必要なハードウェアコンポーネントを示します。

ハードウェア	数量
AFF A220 HA ペア	1.
Cisco UCS B200 M5 サーバ	2.
Cisco Nexus 31108PCV スイッチ	2.
Cisco UCS B200 M5 サーバの Cisco UCS Virtual Interface Card （ VIC ；仮想インターフェイスカード） 1440	2.
2 つの統合 UCS-fi-M6324 ファブリックインターコネクトを備えた Cisco UCS Mini	1.

ソフトウェア要件

次の表に、 FlexPod Express ソリューションのアーキテクチャを実装するために必要なソフトウェアコンポーネントを示します。

ソフトウェア	バージョン	詳細
Cisco UCS Manager の略	4.0 （ 1b ）	Cisco UCS Fabric Interconnect FI_6324UP の場合
Cisco Blade ソフトウェア	4.0 （ 1b ）	Cisco UCS B200 M5 サーバの場合
Cisco nenic ドライバ	1.0.25.0	Cisco VIC 1440 インターフェイスカードの場合
Cisco NX-OS	7.0 （ 3 ） I6 （ 1 ）	Cisco Nexus 31108PCV スイッチの場合
NetApp ONTAP	9.5	AFF A220 コントローラの場合

次の表に、 FlexPod Express のすべての VMware vSphere 環境に必要なソフトウェアを示します。

ソフトウェア	バージョン
VMware vCenter Server Appliance の略	6.7U1

ソフトウェア	バージョン
VMware vSphere ESXi ハイパーバイザー	6.7U1

FlexPod エクスプレスケーブル接続情報

リファレンス検証のケーブル接続については、次の表で説明します。

次の表に、 Cisco Nexus スイッチ 31108PCV A のケーブル接続情報を示します

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
Cisco Nexus スイッチ 31108PCV A	Eth1/1	NetApp AFF A220 ストレージコントローラ A	e0M
	Eth1/2	Cisco UCS-mini FIA	mgmt0 （管理）
	Eth1/3	Cisco UCS-mini FIA	Eth1/1
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/1
	ETH 1/13	Cisco NX 31108PCV B	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV B	ETH 1/14

次の表に、 Cisco Nexus スイッチ 31108PCV B のケーブル接続情報を示します

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
Cisco Nexus スイッチ 31108PCV B	Eth1/1	NetApp AFF A220 ストレージコントローラ B	e0M
	Eth1/2	Cisco UCS-mini FI-B	mgmt0 （管理）
	Eth1/3	Cisco UCS-mini FIA	Eth1/2
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/2
	ETH 1/13	Cisco NX 31108PCV A	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV A	ETH 1/14

次の表に、 NetApp AFF A220 ストレージコントローラ A のケーブル接続情報を示します

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
NetApp AFF A220 ストレージコントローラ A	e0a	NetApp AFF A220 ストレージコントローラ B	e0a
	e0b	NetApp AFF A220 ストレージコントローラ B	e0b
	e0e	Cisco UCS-mini FIA	Eth1/3
	e0f	Cisco UCS-mini FI-B	Eth1/3
	e0M	Cisco NX 31108PCV A	Eth1/1

次の表に、 NetApp AFF A220 ストレージコントローラ B のケーブル接続情報を示します

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
NetApp AFF A220 ストレージコントローラ B	e0a	NetApp AFF A220 ストレージコントローラ B	e0a
	e0b	NetApp AFF A220 ストレージコントローラ B	e0b
	e0e	Cisco UCS-mini FIA	Eth1/4
	e0f	Cisco UCS-mini FI-B	Eth1/4
	e0M	Cisco NX 31108PCV B	Eth1/1

次の表に、 Cisco UCS Fabric Interconnect A のケーブル接続情報を示します

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
Cisco UCS ファブリックインターコネクト A	Eth1/1	Cisco NX 31108PCV A	Eth1/3
	Eth1/2	Cisco NX 31108PCV B	Eth1/3
	Eth1/3	NetApp AFF A220 ストレージコントローラ A	e0e
	Eth1/4	NetApp AFF A220 ストレージコントローラ B	e0e
	mgmt0 （管理）	Cisco NX 31108PCV A	Eth1/2

次の表に、 Cisco UCS ファブリックインターコネクト B のケーブル接続情報を示します

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
Cisco UCS ファブリックインターコネクト B	Eth1/1	Cisco NX 31108PCV A	Eth1/4
	Eth1/2	Cisco NX 31108PCV B	Eth1/4
	Eth1/3	NetApp AFF A220 ストレージコントローラ A	e0f
	Eth1/4	NetApp AFF A220 ストレージコントローラ B	e0f
	mgmt0 （管理）	Cisco NX 31108PCV B	Eth1/2

導入手順

このドキュメントでは、完全な冗長性と高可用性を備えた FlexPod Express システムの構成について詳しく説明します。この冗長性を反映するために、各手順で設定するコンポーネントをコンポーネント A またはコンポーネント B と呼びますたとえば、このドキュメントでプロビジョニングされている 2 台のネットアップストレージコントローラは、コントローラ A とコントローラ B で識別されます。スイッチ A とスイッチ B は Cisco Nexus スイッチのペアを表します。ファブリックインターコネクト A とファブリックインターコネクト B は、 2 つの統合 Nexus ファブリックインターコネクトです。

また、このドキュメントでは、複数の Cisco UCS ホストをプロビジョニングする手順についても説明しま

す。これらのホストは、サーバ A 、サーバ B などとして順次識別されます。

環境に関連する情報をステップに含める必要があることを示すために、コマンド構造の一部として「 \ <text>> 」が表示されます。「 vlan create 」コマンドについては、次の例を参照してください。

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

本ドキュメントでは、 FlexPod Express 環境を完全に構成する方法について説明します。このプロセスでは、さまざまな手順で、お客様固有の命名規則、 IP アドレス、および VLAN （仮想 LAN ）スキームを入力する必要があります。次の表に、このガイドで説明する導入に必要な VLAN を示します。このテーブルは、特定のサイト変数に基づいて作成し、ドキュメントの設定手順を実装するために使用できます。

> 別々のインバンド管理 VLAN とアウトオブバンド管理 VLAN を使用する場合は、それらの間にレイヤ 3 ルートを作成する必要があります。この検証では、共通の管理 VLAN を使用しました。

VLAN 名	**VLAN** の目的	このドキュメントの検証に使用する **ID**
管理 VLAN	管理インターフェイス用の VLAN	18
ネイティブ VLAN	タグなしフレームが割り当てられている VLAN	2.
NFS VLAN	NFS トラフィック用の VLAN	104
VMware vMotion VLAN	ある物理ホストから別の物理ホストへの仮想マシン（ VM ）の移動用に指定された VLAN	103
VM トラフィック VLAN	VM アプリケーショントラフィック用の VLAN	102
iSCSI-A VLAN	ファブリック A の iSCSI トラフィック用 VLAN	124
iSCSI-B VLAN	ファブリック B の iSCSI トラフィック用 VLAN	125

VLAN 番号は、 FlexPod Express の設定全体で必要になります。VLAN は「 <<var_xxxx_vlan>> 」と呼ばれます。「 xxxx 」は VLAN の目的（ iSCSI-A など）です。

次の表は、作成された VMware VM を示しています。

VM 概要の略	ホスト名
VMware vCenter Server の各機能を使用し	Seahawks-vcsa.cie.netapp.com

Cisco Nexus 31108PCV 導入手順

このセクションでは、 FlexPod Express 環境で使用される Cisco Nexus 31308PCV スイッチ構成について詳しく説明します。

Cisco Nexus 31108PCV スイッチの初期設定

ここでは、 FlexPod Express の基本環境で使用する Cisco Nexus スイッチの設定方法について説明します。

> この手順は、 NX-OS ソフトウェアリリース 7.0(3) I6(1) を実行する Cisco Nexus 31108PCV を使用していることを前提としています。

1. スイッチのコンソールポートを最初にブートして接続すると、 Cisco NX-OS セットアップが自動的に開始されます。この初期構成では、スイッチ名、 mgmt0 インターフェイス構成、および Secure Shell （ SSH ）セットアップなどの基本的な設定を行います。
2. FlexPod Express 管理ネットワークは、さまざまな方法で構成できます。31108PCV スイッチの mgmt0 インターフェイスは、既存の管理ネットワークに接続することも、 31108PCV スイッチの mgmt0 インターフェイスをバックツーバック構成で接続することもできる。ただし、このリンクは、 SSH トラフィックなどの外部管理アクセスには使用できません。

   この導入ガイドでは、 FlexPod Express Cisco Nexus 31108PCV スイッチが既存の管理ネットワークに接続されています。

3. Cisco Nexus 31108PCV スイッチを設定するには、スイッチの電源をオンにし、画面に表示される指示に従って両方のスイッチの初期セットアップを行い、スイッチ固有の情報に適切な値を置き換えます。

   ```
   This setup utility will guide you through the basic configuration of the
   system. Setup configures only enough connectivity for management of the
   system.
   ```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. 設定の概要が表示され、設定を編集するかどうかを確認するメッセージが表示されます。設定が正しい場合は、「n」と入力します。

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. その後、この設定を使用するかどうかを確認するメッセージが表示され、保存します。その場合は、「y」と入力します。

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus スイッチ B について、手順 1~5 を繰り返します

高度な機能を有効にします

追加の設定オプションを提供するには、 Cisco NX-OS で特定の高度な機能をイネーブルにする必要があります。

1. Cisco Nexus スイッチ A およびスイッチ B で適切な機能をイネーブルにするには、コンフィギュレーションモードを開始するには、コマンド「（ config t ）」を使用し、次のコマンドを実行します。

```
feature interface-vlan
feature lacp
feature vpc
```

> ポートチャネルのデフォルトのロードバランシングハッシュでは、ソースおよびデスティネーションの IP アドレスを使用して、ポートチャネルのインターフェイス全体のロードバランシングアルゴリズムを決定します。ハッシュアルゴリズムにソースおよびデスティネーションの IP アドレス以外にもデータを提供することで、ポートチャネルのメンバー全体へのより均等なロードバランシングを実現できます。同じ理由から、ソースおよびデスティネーションの TCP ポートをハッシュアルゴリズムに追加することを推奨します。

2. 構成モード（ config t ）から次のコマンドを実行し、 Cisco Nexus スイッチ A およびスイッチ B のグローバルポートチャネルロードバランシング構成を設定します。

```
port-channel load-balance src-dst ip-l4port
```

グローバルスパニングツリーコンフィギュレーションを実行します。

Cisco Nexus プラットフォームでは、ブリッジアシュアランスと呼ばれる新しい保護機能を使用します。ブリッジアシュアランスは、スパニングツリーアルゴリズムを実行していないデバイスでデータトラフィックの転送を継続する単方向リンクやその他のソフトウェア障害から保護するのに役立ちます。ポートは、プラットフォームに応じて、ネットワークやエッジなどのいくつかの状態のいずれかに配置できます。

すべてのポートがデフォルトでネットワークポートとみなされるように、ブリッジアシュアランスを設定することを推奨します。この設定により、ネットワーク管理者は各ポートの設定を確認することになります。また、未識別のエッジポートや、ブリッジアシュアランス機能が有効になっていないネイバーなど、最も一般的な構成エラーも表示されます。また、スパニングツリーでブロックするポートの数が少なすぎない方が、多くのポートをブロックする方が安全で、デフォルトのポートの状態でネットワーク全体の安定性を高めることができます。

サーバ、ストレージ、アップリンクスイッチを追加するときは、スパニングツリーの状態に細心の注意を払ってください。追加する構成がブリッジアシュアランスをサポートしていない場合は特に注意が必要です。このような場合は、ポートをアクティブにするためにポートタイプの変更が必要になることがあります。

Bridge Protocol Data Unit （ BPDU; ブリッジプロトコルデータユニット）ガードは、別の保護レイヤとしてデフォルトでエッジポートでイネーブルになっています。ネットワーク内のループを防止するために、このインターフェイス上で BPDU が別のスイッチから受信された場合、この機能はポートをシャットダウンします。

Cisco Nexus スイッチ A およびスイッチ B で、構成モード（「 config t 」）から次のコマンドを実行し、デフォルトのポートタイプや BPDU ガードなどのデフォルトのスパニングツリーオプションを設定します。

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

VLAN を定義します

VLAN の異なるポートを個別に設定する前に、レイヤ 2 VLAN をスイッチ上に定義する必要があります。また、 VLAN に名前を付けておくと、今後のトラブルシューティングを簡単に行うことができます。

コンフィギュレーションモード（ config t` ）から次のコマンドを実行して、 Cisco Nexus スイッチ A およびスイッチ B 上のレイヤ 2 VLAN を定義し、説明します。

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

アクセスポートと管理ポートの説明を設定します

レイヤ 2 VLAN に名前を割り当てる場合と同様に、すべてのインターフェイスに説明を設定すると、プロビジョニングとトラブルシューティングの両方に役立ちます。

各スイッチの構成モード（ config t ）から、 FlexPod Express の大規模構成の次のポート説明を入力します。

Cisco Nexus スイッチ A

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Cisco Nexus スイッチ **B**

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

サーバおよびストレージの管理インターフェイスを設定します

サーバとストレージの管理インターフェイスで使用する VLAN は、通常、どちらも 1 つだけです。そのため、管理インターフェイスポートをアクセスポートとして設定します。各スイッチの管理 VLAN を定義し、スパニングツリーポートタイプをエッジに変更します。

構成モード (`config t`) から次のコマンドを実行して ' サーバとストレージの両方の管理インタフェースのポート設定を構成します

Cisco Nexus スイッチ **A**

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus スイッチ **B**

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

NTP 配信インターフェイスを追加します

Cisco Nexus スイッチ **A**

グローバルコンフィギュレーションモードから、次のコマンドを実行します。

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Cisco Nexus スイッチ **B**

グローバルコンフィギュレーションモードから、次のコマンドを実行します。

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

仮想ポートチャネルのグローバル設定を実行します

仮想ポートチャネル（ vPC ）を使用すると、 2 つの異なる Cisco Nexus スイッチに物理的に接続されたリンクを、 3 番目のデバイスに対する単一のポートチャネルとして認識できます。3 番目のデバイスには、スイッチ、サーバ、またはその他のネットワークデバイスを使用できます。vPC はレイヤ 2 マルチパスを提供します。これにより、帯域幅を増やし、ノード間で複数のパラレルパスを有効にし、代替パスが存在する場合はトラフィックをロードバランシングすることで、冗長性を確保できます。

vPC には次の利点があります。

- 1 つのデバイスが 2 つのアップストリームデバイス間でポートチャネルを使用できるようにする
- スパニングツリープロトコルのブロックポートの排除
- ループフリートポロジを提供する
- 使用可能なすべてのアップリンク帯域幅を使用する
- リンクまたはデバイスのいずれかに障害が発生した場合に、高速コンバージェンスを提供します
- リンクレベルの耐障害性を提供します
- 高可用性の実現を支援します

vPC 機能を正しく機能させるには、 2 つの Cisco Nexus スイッチ間でいくつかの初期セットアップを行う必要があります。バックツーバックの mgmt0 構成を使用する場合は、インターフェイスに定義されたアドレスを使用し、 ping `\<switch_a/B_mgmt0_ip_addr>> vrf ' management コマンドを使用してそれらのアドレスで通信が可能であることを確認します。

構成モード（ config t ）から次のコマンドを実行し、両方のスイッチの vPC グローバル構成を設定します。

Cisco Nexus スイッチ **A**

```
vpc domain 1
 role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

Cisco Nexus スイッチ B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

この解決策検証では、最大伝送ユニット（ MTU ） 9 、 000 が使用されました。ただし、アプリケーションの要件に基づいて、適切な MTU 値を設定できます。FlexPod 解決策全体で同じ MTU 値を設定することが重要です。コンポーネント間の MTU 設定が正しくないと、パケットが破棄されます。

既存のネットワークインフラへのアップリンク

使用可能なネットワークインフラに応じて、 FlexPod 環境をアップリンクするためのいくつかの方法や機能があります。既存の Cisco Nexus 環境がある場合は、 vPC を使用して、 FlexPod 環境に含まれる Cisco Nexus 31108PVC スイッチをインフラにアップリンクすることを推奨します。必要に応じて、 10GbE インフラ解決策の場合は 10GbE アップリンク、 1GbE インフラ解決策の場合は 1GbE アップリンクがサポートされます。前述の手順を使用して、既存の環境へのアップリンク vPC を作成できます。設定が完了したら、必ず copy run start を実行して各スイッチに設定を保存してください。

ネットアップストレージ導入手順（パート **1** ）

このセクションでは、 NetApp AFF ストレージ導入手順について説明します。

NetApp ストレージコントローラ **AFF2xx** シリーズインストールガイド

NetApp Hardware Universe の略

。 "NetApp Hardware Universe の略" （ HWU ）アプリケーションは、特定の ONTAP バージョンでサポートされているハードウェアコンポーネントとソフトウェアコンポーネントを提供します。ONTAP ソフトウェアで現在サポートされているネットアップのすべてのストレージアプライアンスに関する構成情報を提供します。また、コンポーネントの互換性の表も示します。

使用するハードウェアコンポーネントとソフトウェアコンポーネントが、インストールする ONTAP のバージョンでサポートされていることを確認します。

1. にアクセスします "HWU" システム設定ガイドを表示するアプリケーション。ストレージシステムの比較タブを選択して、 ONTAP ソフトウェアのバージョンとネットアップストレージアプライアンスの互換性を必要な仕様で確認します。
2. または、ストレージアプライアンス別にコンポーネントを比較するには、ストレージシステムの比較をクリックします。

コントローラ **AFF2XX** シリーズの前提条件
ストレージシステムの物理的な場所を計画するには、次のセクションを参照してください。電力要件サポートされる電源コードオンボードポートとケーブル

ストレージコントローラ

のコントローラの物理的な設置手順に従います "AFF A220 のドキュメント"。

設定ワークシート

セットアップスクリプトを実行する前に、製品マニュアルから構成ワークシートに情報を記入してください。設定ワークシートは、で使用できます "ONTAP 9.5 ソフトウェアセットアップガイド" （で使用できます "ONTAP 9 ドキュメンテーション・センター"）。次の表は、 ONTAP 9.5 のインストールと設定の情報を示しています。

このシステムは、 2 ノードスイッチレスクラスタ構成でセットアップされます。

クラスタの詳細	クラスタの値
クラスタノード A の IP アドレス	<<var_nodeA_mgmt_ip>>
クラスタノード A のネットマスク	<<var_nodeA_mgmt_mask>> を使用します
クラスタノード A のゲートウェイ	<<var_nodeA_mgmt_gateway>> を使用します
クラスタノードの名前	<<var_nodeA>> を使用します
クラスタノード B の IP アドレス	<<var_nodeB_mgmt_ip>>
クラスタノード B のネットマスク	<<var_nodeB_mgmt_mask>> を使用します
クラスタノード B のゲートウェイ	<<var_nodeB_mgmt_gateway>> を使用します
クラスタノード B の名前	<<var_nodeB>> を使用します
ONTAP 9.5 の URL	<<var_url_boot_software>> を参照してください
クラスタの名前	\<<var_clustername> を使用します
クラスタ管理 IP アドレス	<<var_clustermgmt_ip>>
クラスタ B ゲートウェイ	<<var_clustermgmt_gateway>> を使用します
クラスタ B のネットマスク	<<var_clustermgmt_mask>> を使用します
ドメイン名	<<var_domain_name>> を参照してください
DNS サーバ IP （複数入力できます）	<<var_dns_server_ip>>
NTP サーバ A の IP	<switch-A-ntp-ip>>
NTP サーバ B の IP	<switch-b-ntp-ip>>

ノード **A** を設定

ノード A を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. システムをブートできるようにします。

```
autoboot
```

3. Ctrl+C キーを押してブートメニューを表示します。

   ONTAP 9 の場合：5 は起動しているソフトウェアのバージョンではありません。次の手順に進んで新しいソフトウェアをインストールしてください。ONTAP 9 の場合：5 はブートしているバージョンです。オプション 8 と y を選択してノードをリブートします。その後、手順 14 に進みます。

4. 新しいソフトウェアをインストールするには ' オプション 7 を選択します
5. アップグレードを実行するには 'y' を入力します
6. ダウンロードに使用するネットワーク・ポートに e0M を選択します
7. 今すぐ再起動するには 'y' を入力します
8. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. ソフトウェアを検索できる URL を入力します。

   ping 可能な Web サーバを指定する必要があります。

10. ユーザ名が入力されていない場合は、 Enter キーを押します。
11. 新しくインストールしたソフトウェアを ' 次回の再起動に使用するデフォルトとして設定するには 'y' を入力します
12. ノードを再起動するには 'y' を入力します

    新しいソフトウェアをインストールするときに、 BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

13. Ctrl+C キーを押してブートメニューを表示します。
14. [Clean Configuration] で [4] を選択し、 [Initialize All Disks] を選択します。
15. ディスクをゼロにするには 'y' を入力し ' 構成をリセットして ' 新しいファイル・システムをインストールします
16. ディスク上のすべてのデータを消去するには 'y' を入力します

    ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。ノード A のディスクの初期化中も、ノード B の設定を続行できます。

17. ノード A を初期化している間に、ノード B の設定を開始します

ノード **B** を設定

ノード B を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Ctrl+C キーを押してブートメニューを表示します。

```
autoboot
```

3. プロンプトが表示されたら、 Ctrl-C キーを押します。

   ONTAP 9 の場合：5 は起動しているソフトウェアのバージョンではありません。次の手順に進んで新しいソフトウェアをインストールしてください。ブートしているバージョンが ONTAP 9.4 の場合は、オプション 8 と y を選択してノードをリブートします。その後、手順 14 に進みます。

4. 新しいソフトウェアをインストールするには、オプション 7 を選択します。
5. アップグレードを実行するには 'y' を入力します
6. ダウンロードに使用するネットワーク・ポートに e0M を選択します
7. 今すぐ再起動するには 'y' を入力します
8. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. ソフトウェアを検索できる URL を入力します。

   ℹ ping 可能な Web サーバを指定する必要があります。

```
<<var_url_boot_software>>
```

10. ユーザ名が入力されていない場合は、 Enter キーを押します
11. 新しくインストールしたソフトウェアを ' 次回の再起動に使用するデフォルトとして設定するには 'y' を入力します
12. ノードを再起動するには 'y' を入力します

    新しいソフトウェアをインストールするときに、 BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

13. Ctrl+C キーを押してブートメニューを表示します。
14. Clean Configuration および Initialize All Disks のオプション 4 を選択します。

15. ディスクをゼロにするには 'y' を入力し ' 構成をリセットして ' 新しいファイル・システムをインストールします
16. ディスク上のすべてのデータを消去するには 'y' を入力します

    ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。

ノード **A** の設定およびクラスタ構成を継続します

ストレージコントローラ A （ノード A ）のコンソールポートに接続されているコンソールポートプログラムから、ノードセットアップスクリプトを実行します。このスクリプトは、 ONTAP 9.5 をノードで初めてブートしたときに表示されます。

ONTAP 9.5 では、ノードとクラスタのセットアップ手順が少し変更されています。クラスタセットアップウィザードを使用してクラスタの最初のノードを設定できるようになりました。 System Manager を使用してクラスタを設定します。

1. プロンプトに従ってノード A をセットアップします

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. ノードの管理インターフェイスの IP アドレスに移動します。

> クラスタのセットアップは、 CLI を使用して実行することもできます。このドキュメントでは、 NetApp System Manager のセットアップガイドを使用したクラスタセットアップについて説明します。

3. クラスタを設定するには、セットアップガイドをクリックします。
4. クラスタ名には「 \<<var_clustername>> 」を、設定する各ノードには「 <<var_nodeA>` 」と「 \<<var_nodeB>> 」を入力します。ストレージシステムに使用するパスワードを入力します。クラスタタイプに「スイッチレスクラスタ」を選択します。クラスタベースライセンスを入力します。
5. クラスタ、 NFS 、および iSCSI の機能ライセンスを入力することもできます。
6. クラスタの作成中を示すステータスメッセージが表示されます。このステータスメッセージは、複数のステータスを切り替えます。このプロセスには数分かかります。
7. ネットワークを設定します
   a. [IP Address Range] オプションを選択解除します。

b. Cluster Management IP Address フィールドに「 <<var_clustermgmt_ip>> 」、 Netmask フィールドに「 \var_clustermgmt_mask>> 」と入力します。また、 Gateway フィールドに「 <<var_clustermgmt_gateway>> 」と入力します。Port フィールドの … セレクタを使用して、ノード A の e0M を選択します

c. ノード A のノード管理 IP がすでに入力されています。ノード B には '\<<var_nodeA_mgmt_ip>> を入力します

d. [DNS Domain Name] フィールドに「 <<var_domain_name>` 」と入力します。[DNS Server IP Address] フィールドに「 \<<var_dns_server_ip>> 」と入力します。

   DNS サーバの IP アドレスは複数入力できます。

e. Primary NTP Server フィールドに「 \ <switch-a-ntp-ip>> 」と入力します。

   代替 NTP サーバを「 \ <switch-b-ntp-ip>> 」として入力することもできます。

8. サポート情報を設定します。

   a. AutoSupport へのアクセスにプロキシが必要な環境の場合は、プロキシの URL をプロキシの URL に入力します。

   b. イベント通知に使用する SMTP メールホストと E メールアドレスを入力します。

      続行するには、少なくともイベント通知方式を設定する必要があります。いずれかの方法を選択できます。

9. クラスタ構成が完了したことが示されたら、 Manage Your Cluster （クラスタの管理）をクリックしてストレージを構成します。

ストレージクラスタ構成を継続

ストレージノードとベースクラスタの設定が完了したら、ストレージクラスタの設定に進むことができます。

すべてのスペアディスクを初期化します

クラスタ内のすべてのスペアディスクを初期化するには、次のコマンドを実行します。

```
disk zerospares
```

オンボード **UTA2** ポートパーソナリティを設定します

1. ucadmin show コマンドを実行して、現在のモードとポートの現在のタイプを確認します。

```
AFFA220-Clus::> ucadmin show
                       Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. 使用中のポートの現在のモードが「 cna 」であり、現在のタイプが「 target 」に設定されていることを確認します。設定されていない場合は、次のコマンドを実行してポートパーソナリティを変更します。

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

前のコマンドを実行するには、ポートをオフラインにする必要があります。ポートをオフラインにするには、次のコマンドを実行します。

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

ポートパーソナリティを変更した場合、変更を有効にするには、各ノードをリブートする必要があります。

Cisco Discovery Protocol を有効にします

ネットアップストレージコントローラで Cisco Discovery Protocol （ CDP ）を有効にするには、次のコマンドを実行します。

```
node run -node * options cdpd.enable on
```

すべてのイーサネットポートでリンクレイヤ検出プロトコルを有効にします

次のコマンドを実行して、ストレージスイッチとネットワークスイッチ間のリンクレイヤ検出プロトコル（LLDP）ネイバー情報の交換を有効にします。このコマンドは、クラスタ内のすべてのノードのすべてのポートで LLDP を有効にします。

```
node run * options lldp.enable on
```

管理論理インターフェイスの名前を変更します

管理論理インターフェイス（LIF）の名前を変更するには、次の手順を実行します。

1. 現在の管理 LIF の名前を表示します。

   ```
   network interface show –vserver <<clustername>>
   ```

2. クラスタ管理 LIF の名前を変更します。

   ```
   network interface rename –vserver <<clustername>> –lif
   cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
   ```

3. ノード B の管理 LIF の名前を変更します。

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
   ```

クラスタ管理で自動リバートを設定する

クラスタ管理インターフェイスで 'auto-revert パラメータを設定します

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

サービスプロセッサのネットワークインターフェイスをセットアップする

各ノードのサービスプロセッサに静的 IPv4 アドレスを割り当てるには、次のコマンドを実行します。

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

サービスプロセッサの IP アドレスは、ノード管理 IP アドレスと同じサブネット内にある必要があります。

ONTAP でストレージフェイルオーバーを有効にします

ストレージフェイルオーバーが有効になっていることを確認するには、フェイルオーバーペアで次のコマンドを実行します。

1. ストレージフェイルオーバーのステータスを確認

   ```
   storage failover show
   ```

   \<<var_nodeA>>` と \<<var_nodeB>> の両方がテイクオーバーを実行できる必要があります。ノードでテイクオーバーを実行できる場合は、ステップ 3 に進みます。

2. 2 つのノードのどちらかでフェイルオーバーを有効にします。

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. 2 ノードクラスタの HA ステータスを確認

   この手順は、ノードが 3 つ以上のクラスタには適用されません。

   ```
   cluster ha show
   ```

4. ハイアベイラビリティが構成されている場合は、ステップ 6 に進みます。ハイアベイラビリティが設定されている場合は、コマンドの実行時に次のメッセージが表示されます。

   ```
   High Availability Configured: true
   ```

5. HA モードは 2 ノードクラスタでのみ有効にします。

   ノードが 3 つ以上のクラスタの場合は、このコマンドを実行しないでください。フェイルオーバーで問題が発生します。

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. ハードウェアアシストが正しく設定されていることを確認し、必要に応じてパートナーの IP アドレスを変更

```
storage failover hwassist show
```

「 Keep Alive Status: Error: Did not receive hwassist keep alive alerts from partner 」というメッセージは、ハードウェアアシストが設定されていないことを示します。ハードウェアアシストを設定するには、次のコマンドを実行します。

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP でジャンボフレーム **MTU** ブロードキャストドメインを作成します

MTU が 9000 のデータブロードキャストドメインを作成するには、次のコマンドを実行します。

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

デフォルトのブロードキャストドメインからデータポートを削除します

10GbE のデータポートは iSCSI / NFS トラフィックに使用されます。これらのポートはデフォルトドメインから削除する必要があります。ポート e0e と e0f は使用されないため、デフォルトのドメインからも削除する必要があります。

ブロードキャストドメインからポートを削除するには、次のコマンドを実行します。

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 ポートではフロー制御を無効にします

ネットアップでは、外部デバイスに接続されているすべての UTA2 ポートでフロー制御を無効にすることをベストプラクティスとして推奨します。フロー制御を無効にするには、次のコマンドを実行します。

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```

ONTAP への Cisco UCS Mini の直接接続は、 LACP をサポートしていません。

NetApp ONTAP でジャンボフレームを設定します

ジャンボフレーム（一般に MTU サイズが 9 、 000 バイトのフレーム）を使用するように ONTAP ネットワークポートを設定するには、クラスタシェルから次のコマンドを実行します。

```
AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

ONTAP で VLAN を作成します

ONTAP で VLAN を作成するには、次の手順を実行します。

1. NFS VLAN ポートを作成し、データブロードキャストドメインに追加します。

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

2. iSCSI VLAN ポートを作成し、データブロードキャストドメインに追加します。

```
network port vlan create -node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN ポートを作成します。

```
network port vlan create -node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

ONTAP でアグリゲートを作成する

ONTAP のセットアッププロセスで、ルートボリュームを含むアグリゲートが作成されます。追加のアグリゲートを作成するには、アグリゲート名、アグリゲートを作成するノード、アグリゲートに含まれるディスク数を確認します。

アグリゲートを作成するには、次のコマンドを実行します。

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

構成内で少なくとも 1 つのディスクをスペアとして保持します（最も大きいディスクを選択してください）。ディスクのタイプとサイズごとに少なくとも 1 つのスペアを用意しておくことを推奨します。

ディスクは 5 本から始めて、追加のストレージが必要になったときにアグリゲートにディスクを追加できます。

ディスクの初期化が完了するまで、アグリゲートを作成することはできません。aggr show コマンドを実行して、アグリゲートの作成ステータスを表示します。「 aggr1_nodeA 」がオンラインになるまで、次の手順に進まないでください。

ONTAP でタイムゾーンを設定します

時刻の同期を設定し、クラスタのタイムゾーンを設定するには、次のコマンドを実行します。

```
timezone <<var_timezone>>
```

> たとえば、米国東部では、タイムゾーンは「アメリカ / ニューヨーク」です。タイムゾーン名の入力を開始したら、 Tab キーを押して使用可能なオプションを表示します。

ONTAP で **SNMP** を設定します

SNMP を設定するには、次の手順を実行します。

1. 場所や連絡先などの SNMP 基本情報を設定します。ポーリング時に ' この情報は 'sysLocation' 変数と SNMP の sysContact' 変数として表示されます

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. リモートホストに送信する SNMP トラップを設定します。

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

ONTAP で **SNMPv1** を設定します

SNMPv1 を設定するには、コミュニティと呼ばれる共有シークレットのプレーンテキストパスワードを設定します。

```
snmp community add ro <<var_snmp_community>>
```

> 「 snmp community delete all 」コマンドは慎重に使用してください。他の監視製品にコミュニティストリングが使用されている場合、このコマンドはそれらを削除します。

ONTAP で **SNMPv3** を設定します

SNMPv3 では、認証用のユーザを定義および設定する必要があります。SNMPv3 を設定するには、次の手順を実行します。

1. 「 securitysnmpusers 」コマンドを実行して、エンジン ID を表示します。
2. 「 mpv3user 」という名前のユーザを作成します。

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 信頼できるエンティティのエンジン ID を入力し、認証プロトコルとして「 mD5 」を選択します。
4. プロンプトが表示されたら、認証プロトコルのパスワードとして最低 8 文字のパスワードを入力します。
5. プライバシープロトコルとして「 es 」を選択します。
6. プロンプトが表示されたら、プライバシープロトコルのパスワードとして最低 8 文字のパスワードを入力します。

ONTAP で AutoSupport HTTPS を設定します

NetApp AutoSupport ツールは、サポート概要情報を HTTPS 経由でネットアップに送信します。AutoSupport を設定するには、次のコマンドを実行します。

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Storage Virtual Machine を作成

インフラ Storage Virtual Machine （ SVM ）を作成するには、次の手順を実行します。

1. vserver create コマンドを実行します

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. NetApp VSC のインフラ SVM アグリゲートリストにデータアグリゲートを追加します。

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS と iSCSI を残して、未使用のストレージプロトコルを SVM から削除します。

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. インフラ SVM で NFS プロトコルを有効にして実行します。

```
nfs create -vserver Infra-SVM -udp disabled
```

5. NetApp NFS VAAI プラグインの「 VM vStorage 」パラメータをオンにします。次に、 NFS が設定されて

いることを確認します。

```
vserver nfs modify -vserver Infra-SVM -vstorage enabled
vserver nfs show
```

SVM は以前はサーバと呼ばれていたため、コマンドラインでは「 vserver 」の前にコマンドが配置されます

ONTAP で **NFSv3** を設定します

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ESXi ホスト A の NFS IP アドレス	<<var_esxi_hostA_nfs_ip>>
ESXi ホスト B の NFS IP アドレス	<<var_esxi_hostB_nfs_ip>> を追加します

SVM に NFS を設定するには、次のコマンドを実行します。

1. デフォルトのエクスポートポリシーに各 ESXi ホスト用のルールを作成します。
2. 作成する各 ESXi ホストにルールを割り当てます。各ホストには独自のルールインデックスがあります。最初の ESXi ホストのルールインデックスは 1 、 2 番目の ESXi ホストのルールインデックスは 2 のようになります。

```
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid falsevserver export-
policy rule create -vserver Infra-SVM -policyname default -ruleindex 2
-protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys -rwrule
sys -superuser sys -allow-suid false
vserver export-policy rule show
```

3. エクスポートポリシーをインフラ SVM ルートボリュームに割り当てます。

```
volume modify -vserver Infra-SVM -volume rootvol -policy default
```

エクスポートポリシーは、 vSphere のセットアップ後にインストールするように選択した場合に自動的に処理されます。インストールしない場合は、 Cisco UCS B シリーズサーバを追加するときにエクスポートポリシールールを作成する必要があります。

ONTAP で **iSCSI** サービスを作成します

iSCSI サービスを作成するには、次の手順を実行します。

1. SVM で iSCSI サービスを作成します。また、このコマンドでは iSCSI サービスが開始され、 SVM に iSCSI Qualified Name （ IQN ）が設定されます。iSCSI が設定されていることを確認します。

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP で **SVM** ルートボリュームの負荷共有ミラーを作成

ONTAP で SVM ルートボリュームの負荷共有ミラーを作成するには、次の手順を実行します。

1. インフラ SVM ルートボリュームの負荷共有ミラーとなるボリュームを各ノードに作成します。

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate
aggr1_nodeA -size 1GB -type DPvolume create -vserver Infra_Vserver
-volume rootvol_m02 -aggregate aggr1_nodeB -size 1GB -type DP
```

2. ルートボリュームのミラー関係を 15 分ごとに更新するジョブスケジュールを作成します。

```
job schedule interval create -name 15min -minutes 15
```

3. ミラーリング関係を作成

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. ミラーリング関係を初期化し、作成されたことを確認します。

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

ONTAP で **HTTPS** アクセスを設定する

ストレージコントローラへのセキュアなアクセスを設定するには、次の手順を実行します。

1. 証明書コマンドにアクセスするには、権限レベルを上げてください。

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 通常は、自己署名証明書がすでに存在します。次のコマンドを実行して証明書を確認します。

```
security certificate show
```

3. 表示されている各 SVM の証明書の共通名は、 SVM の DNS 完全修飾ドメイン名（ FQDN ）と一致している必要があります。4 つのデフォルト証明書を削除して、認証局の自己署名証明書または証明書に置き換える必要があります。

   証明書を作成する前に期限切れになった証明書を削除することを推奨します。「 securitycertificate delete 」コマンドを実行して、期限切れの証明書を削除します。次のコマンドでは、タブ補完を使用して、デフォルトの証明書を選択して削除します。

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. 自己署名証明書を生成してインストールするには、次のコマンドを 1 回限りのコマンドとして実行します。インフラ SVM とクラスタ SVM のサーバ証明書を生成します。これらのコマンドの実行に役立つように、タブ補完を使用してください。

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 次の手順で必要なパラメータの値を取得するには、「 securitycertificate show 」コマンドを実行します。
6. 作成した各証明書を ' – server-enabled true' および– client-enabled false' パラメータを使用して有効にしますタブ補完を使用してください。

```
security ssl modify [TAB] ...
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL と HTTPS アクセスを設定して有効にし、 HTTP アクセスを無効にします。

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

これらのコマンドの一部で、エントリが存在しないことを示すエラーメッセージが返されますが、これは通常の動作であり問題ありません。

8. admin 権限レベルにリバートしてセットアップを作成し、 SVM を Web で使用できるようにします。

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

ONTAP で **NetApp FlexVol** ボリュームを作成します

NetApp FlexVol ® ボリュームを作成するには、ボリューム名、サイズ、およびボリュームが存在するアグリゲートを入力します。2 つの VMware データストアボリュームと 1 つのサーバブートボリュームを作成します。

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP で重複排除を有効にします

適切なボリュームで 1 日に 1 回重複排除を有効にするには、次のコマンドを実行します。

```
volume efficiency modify –vserver Infra-SVM –volume esxi_boot –schedule
sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_1
–schedule sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_2
–schedule sun-sat@0
```

ONTAP で **LUN** を作成します

2 つのブート論理ユニット番号（ LUN ）を作成するには、次のコマンドを実行します。

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled
```

Cisco UCS C シリーズサーバを追加する場合は、追加のブート LUN を作成する必要があります。

ONTAP に **iSCSI LIF** を作成

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ストレージノード A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
ストレージノード A の iSCSI LIF01A ネットワークマスク	<<var_nodeA_iscsi_lif01a _mask>> をクリックします
ストレージノード A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
ストレージノード A の iSCSI LIF01B ネットワークマスク	<<var_nodeA_iscsi_lif01b_mask>> をクリックします
ストレージノード B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
ストレージノード B iSCSI LIF01A ネットワークマスク	<<var_nodeB_iscsi_lif01a_mask>> を選択します
ストレージノード B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
ストレージノード B iSCSI LIF01B ネットワークマスク	<<var_nodeB_iscsi_lif01b_mask>> をクリックします

1. 各ノードに 2 つずつ、 4 つの iSCSI LIF を作成します。

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

ONTAP に **NFS LIF** を作成します

次の表に、この設定を完了するために必要な情報を示します。

詳細（ **Detail** ）	詳細値
ストレージノード A NFS LIF 01 A IP	<<var_nodeA_nfs_lif_01_a_ip>>
ストレージノード A NFS LIF 01 のネットワークマスク	<<var_nodeA_nfs_lif_01_a_mask>> を参照してください
ストレージノード A NFS LIF 01 b IP	<<var_nodeA_nfs_lif_01_b_ip>>
ストレージノード A NFS LIF 01 b ネットワークマスク	<<var_nodeA_nfs_lif_01_b_mask>> を参照してください
ストレージノード B の NFS LIF 02 A IP	<<var_nodeB_nfs_lif_02_a_ip>>
ストレージノード B の NFS LIF 02 A ネットワークマスク	<<var_nodeB_nfs_lif_02.a_mask>> を参照してください
ストレージノード B の NFS LIF 02 b IP	<<var_nodeB_nfs_lif_02_b_ip>>
ストレージノード B の NFS LIF 02 b ネットワークマスク	<<var_nodeB_nfs_lif_02_b_mask>> を参照してください

1. NFS LIF を作成します。

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> –address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface show
```

インフラ **SVM** 管理者を追加

次の表に、この設定を完了するために必要な情報を示します。

詳細（**Detail**）	詳細値
vsmgmt IP	<<var_svm_mgmt_ip>> を追加します
vsmgmt ネットワークマスク	<<var_SVM_mgmt_mask>> を使用します
vsmgmt デフォルトゲートウェイ	<<var_SVM_mgmt_gateway>> を使用します

インフラ SVM 管理者および SVM 管理 LIF を管理ネットワークに追加するには、次の手順を実行します。

1. 次のコマンドを実行します。

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

ここで指定する SVM 管理 IP は、ストレージクラスタ管理 IP と同じサブネット内にある必要があります。

2. SVM 管理インターフェイスの外部へのアクセスを許可するデフォルトルートを作成します。

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>> network route show
```

3. SVM 「 vsadmin 」ユーザのパスワードを設定し、ユーザのロックを解除します。

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver
```

Cisco UCS サーバの構成

FlexPod の Cisco UCS ベース

FlexPod 環境で Cisco UCS 6324 ファブリックインターコネクトの初期セットアップを実行します。

このセクションでは、 Cisco UCS Manger を使用して、 FlexPod ROBO 環境で使用する Cisco UCS を設定する手順について詳しく説明します。

Cisco UCS ファブリックインターコネクト 6324 A

Cisco UCS は、アクセスレイヤネットワークとサーバを使用します。この高性能な次世代サーバシステムは、データセンターにワークロードの即応性と拡張性をもたらします。

Cisco UCS Manager 4.0(1b) は、ファブリックインターコネクトを Cisco UCS シャーシに統合する 6324 ファブリックインターコネクトをサポートし、より小規模な導入環境に解決策を統合します。Cisco UCS Mini により、システム管理が簡素化され、低規模な導入のためのコストが削減されます。

ハードウェアコンポーネントとソフトウェアコンポーネントは、シスコのユニファイドファブリックをサポートしています。ユニファイドファブリックは、単一の統合ネットワークアダプタ上で複数のタイプのデータセンタートラフィックを処理します。

システムの初期セットアップ

Cisco UCS ドメイン内のファブリックインターコネクトに初めてアクセスすると、セットアップウィザードによって、システムの設定に必要な次の情報の入力が求められます。

- インストール方法（ GUI または CLI ）
- セットアップモード（フルシステムバックアップまたは初期セットアップからリストア）
- システム構成の種類（スタンドアロンまたはクラスタ構成）
- システム名
- 管理パスワード
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス

- デフォルトゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- DNS サーバの IPv4 アドレスまたは IPv6 アドレス
- デフォルトのドメイン名

次の表に、 Fabric Interconnect A で Cisco UCS の初期設定を完了するために必要な情報を示します

詳細（ **Detail** ）	詳細 / 値
システム名	\<<var_UCS_clustername> を使用します
管理パスワード	<<var_password>>
管理 IP アドレス：ファブリックインターコネクト A	<<var_ucsa_mgmt_ip>> を追加します
管理ネットマスク： Fabric Interconnect A	<<var_ucsa_mgmt_mask>> を使用します
デフォルトゲートウェイ： Fabric Interconnect A	<<var_ucsa_mgmt_gateway>> を使用します
クラスタの IP アドレス	<<var_UCS_cluster_ip>>
DNS サーバの IP アドレス	<<var_nameserver_ip>>
ドメイン名	<<var_domain_name>> を参照してください

FlexPod 環境で使用するように Cisco UCS を設定するには、次の手順を実行します。

1. 最初の Cisco UCS 6324 ファブリックインターコネクト A のコンソールポートに接続します

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. コンソールに表示される設定を確認します。正しい場合は、回答は設定を適用して保存します。
3. ログインプロンプトで設定が保存されたことを確認します。

次の表に、ファブリックインターコネクト B で Cisco UCS の初期設定を完了するために必要な情報を示します

詳細（ **Detail** ）	詳細 / 値
システム名	\<<var_UCS_clustername> を使用します
管理パスワード	<<var_password>>
管理 IP アドレス - FI B	<<var_UCSB_mgmt_ip>> を追加します
管理ネットマスク - FI B	<<var_UCSB_mgmt_mask>> を使用します
デフォルトゲートウェイ - FI B	<<var_UCSB_mgmt_gateway>> を使用します
クラスタの IP アドレス	<<var_UCS_cluster_ip>>
DNS サーバの IP アドレス	<<var_nameserver_ip>>
ドメイン名（ Domain Name ）	<<var_domain_name>> を参照してください

1. 2 番目の Cisco UCS 6324 ファブリックインターコネクト B のコンソールポートに接続します

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. ログインプロンプトで、設定が保存されたことを確認します。

Cisco UCS Manager にログインします。

Cisco Unified Computing System （ UCS ）環境にログインするには、次の手順を実行します。

1. Web ブラウザを開き、 Cisco UCS ファブリックインターコネクトクラスタのアドレスに移動します。

   Cisco UCS Manager が起動するように 2 つ目のファブリックインターコネクトを設定した後、 5 分以上待つ必要があります。

2. Launch UCS Manager リンクをクリックして、 Cisco UCS Manager を起動します。
3. 必要なセキュリティ証明書を受け入れます。
4. プロンプトが表示されたら、ユーザ名に admin を入力し、管理者パスワードを入力します。
5. Login をクリックして、 Cisco UCS Manager にログインします。

Cisco UCS Manager ソフトウェアバージョン 4.0(1b)

このマニュアルでは、 Cisco UCS Manager ソフトウェアバージョン 4.0(1b) を使用することを前提としています。Cisco UCS Manager ソフトウェアおよび Cisco UCS 6324 ファブリックインターコネクトソフトウェアのアップグレードについては、を参照してください "Cisco UCS Manager インストールおよびアップグレードガイド"

Cisco UCS Call Home を設定する

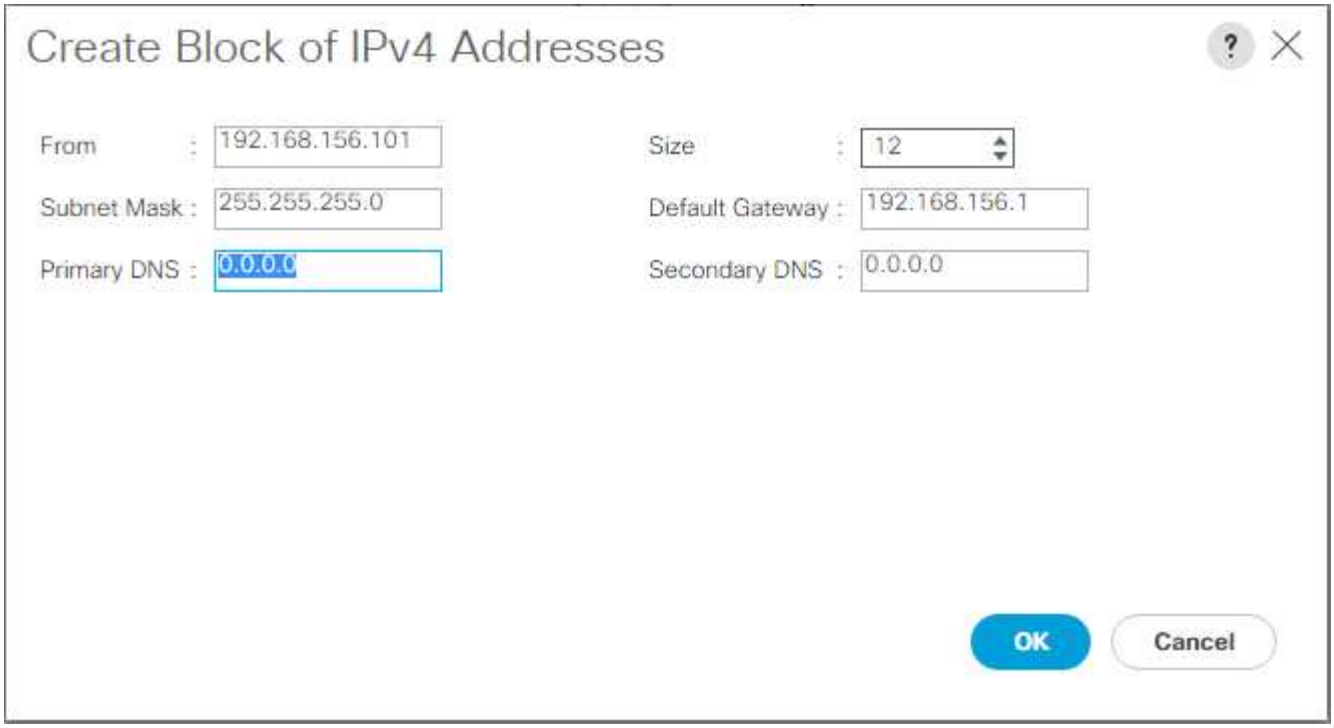
Cisco UCS Manager で Call Home を設定することを強く推奨します。Call Home を設定すると、サポートケースの解決が迅速になります。Call Home を設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Admin をクリックします。
2. [すべて]>[通信管理]>[コールホーム] の順に選択します。
3. 状態をオンに変更します。
4. 管理設定に従ってすべてのフィールドに入力し、 [変更の保存] をクリックして [OK] をクリックし、 Call Home の設定を完了します。

キーボード、ビデオ、マウスアクセス用の IP アドレスのブロックを追加します

Cisco UCS 環境で帯域内サーバのキーボード、ビデオ、マウス（ KVM ）アクセス用の IP アドレスブロックを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [Pools] > [root] > [IP Pools] を展開します。
3. [IP Pool ext-mgmt] を右クリックし、 [Create Block of IPv4 Addresses] を選択します。
4. ブロックの開始 IP アドレス、必要な IP アドレスの数、およびサブネットマスクとゲートウェイの情報を入力します。



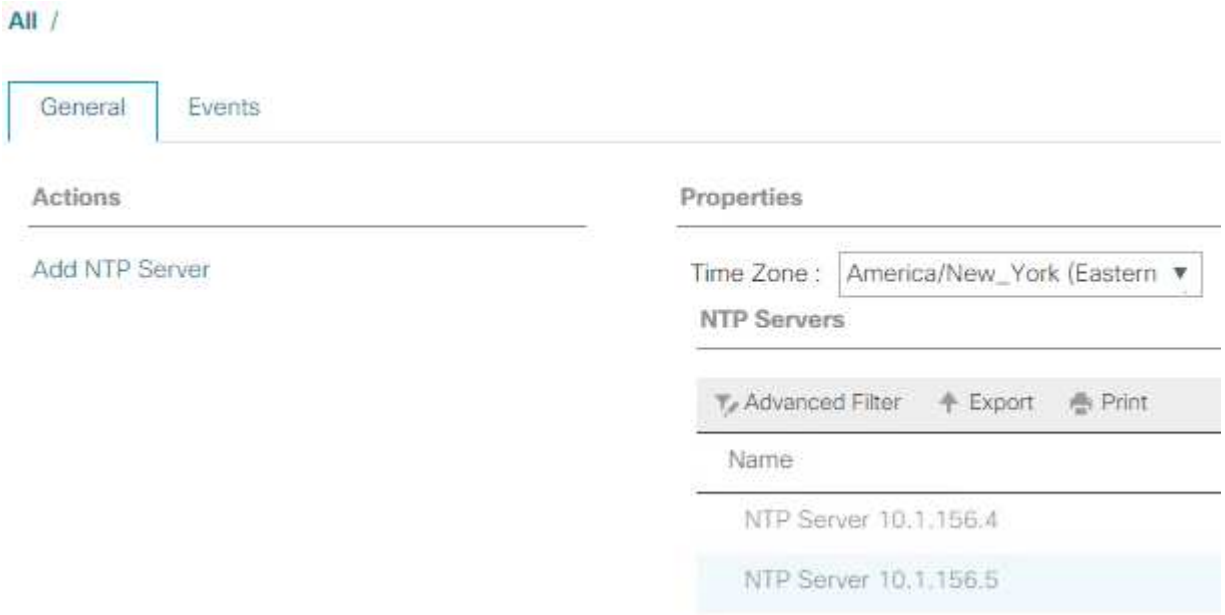
5. [OK] をクリックして、ブロックを作成する。
6. 確認メッセージで [OK] をクリックします。

Cisco UCS を NTP に同期する

Cisco UCS 環境を Nexus スイッチの NTP サーバと同期させるには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Admin をクリックします。
2. ［すべて］ > ［タイムゾーン管理］ を展開します。
3. ［タイムゾーン］ を選択します。
4. [プロパティ] ペインで、 [タイムゾーン] メニューから適切なタイムゾーンを選択します。
5. [Save Changes] をクリックし、 [OK] をクリックします。
6. Add NTP Server をクリックします。
7. 「 <switch-a-ntp-ip> 」または「 <nexus-a-mgmt-ip>` 」と入力し、 [OK] をクリックします。[OK] をクリックします。

8. Add NTP Server をクリックします。
9. 「 <switch-b-ntp-ip>`` 」または「 <nexus-B-mgmt-ip>` 」と入力し、 [OK] をクリックします。確認の [OK] をクリックします。



シャーシ検出ポリシーを編集します

検出ポリシーを設定することで、 Cisco UCS B シリーズシャーシの追加やファブリックエクステンダの追加が簡素化され、 Cisco UCS C シリーズの接続性がさらに向上します。シャーシ検出ポリシーを変更するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [Equipment] をクリックし、 2 番目のリストで [Equipment] を選択します。
2. 右側のペインで、 [ポリシー] タブを選択します。
3. Global Policies （グローバルポリシー）で、シャーシまたはファブリックエクステンダ（ FEX ）とファブリックインターコネクト間でケーブル接続されているアップリンクポートの最小数と一致するように、 Chassis/FEX Discovery Policy （シャーシ /FEX 検出ポリシー）を設定します。
4. Link Grouping Preference を Port Channel に設定します。設定する環境に大量のマルチキャストトラフィックが含まれている場合は、 Multicast Hardware Hash （マルチキャストハードウェアハッシュ）設定を

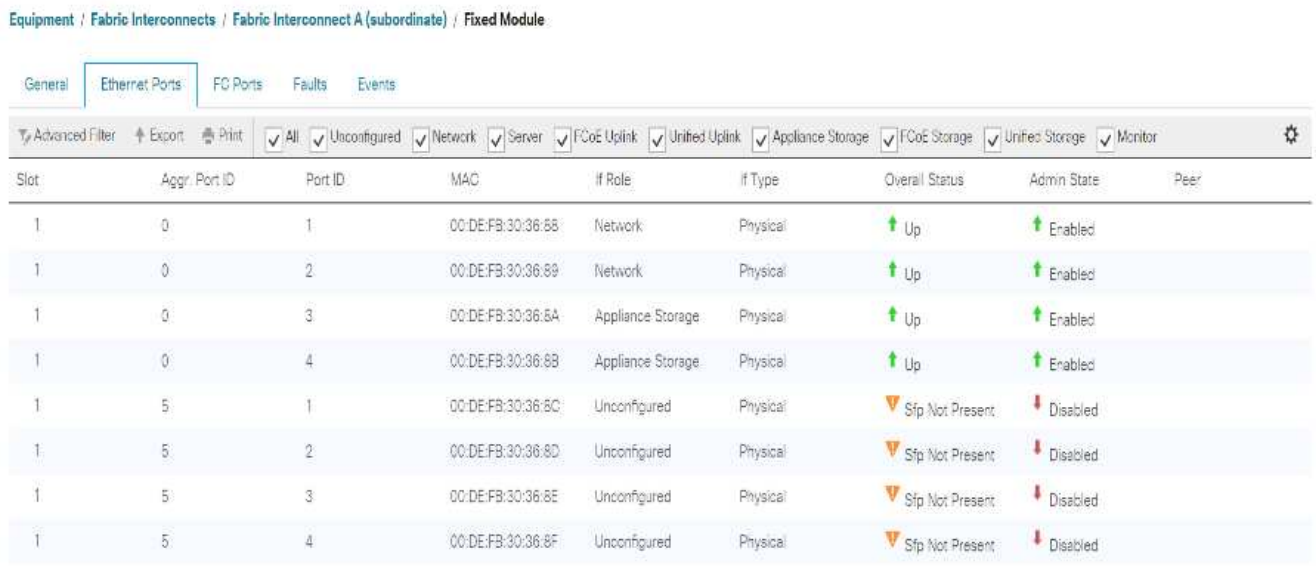
Enabled （有効）に設定します。

5. [Save Changes] をクリックします。
6. [OK] をクリックします。

サーバ、アップリンク、およびストレージポートを有効にします

サーバポートとアップリンクポートをイネーブルにするには、次の手順を実行します。

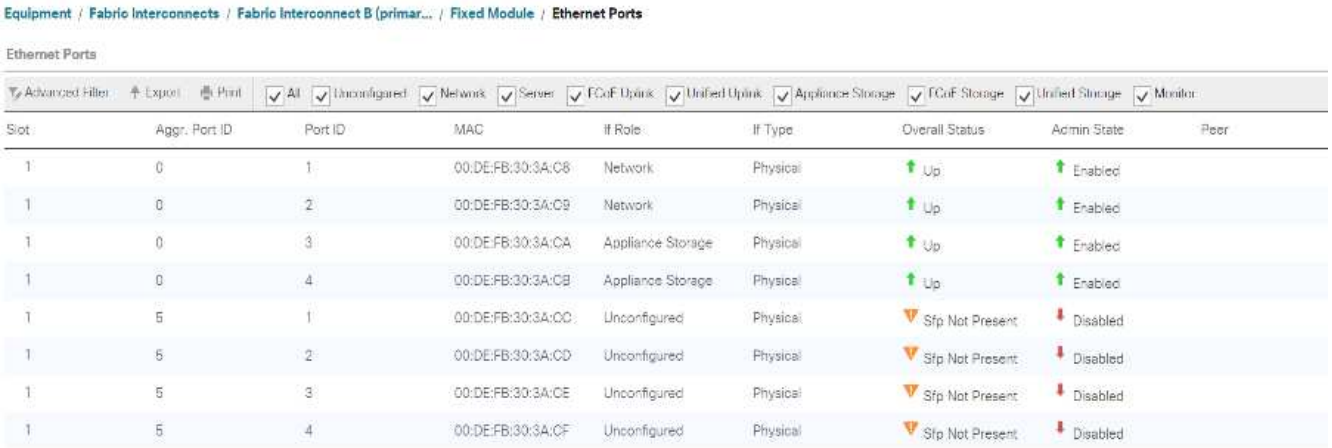
1. Cisco UCS Manager のナビゲーションペインで、 Equipment タブを選択します。
2. Equipment > Fabric Interconnects > Fabric Interconnect A > Fixed Module の順に展開します。
3. [Ethernet ポート] を展開します。
4. Cisco Nexus 31108 スイッチに接続されているポート 1 と 2 を選択し、右クリックして、 [Configure as Uplink Port] を選択します。
5. Yes をクリックしてアップリンクポートを確認し、 OK をクリックします。
6. ネットアップストレージコントローラに接続されているポート 3 と 4 を選択し、右クリックして Configure as Appliance Port （アプライアンスポートとして設定）を選択します。
7. Yes をクリックして、アプライアンスのポートを確認します。
8. Configure as Appliance Port （アプライアンスポートとして設定）ウィンドウで、 OK をクリックします。
9. [OK] をクリックして確定します。
10. 左側のペインで、 Fabric Interconnect A の Fixed Module を選択します
11. [Ethernet Ports] タブで、 [If Role] カラムにポートが正しく設定されていることを確認します。スケーラビリティポートにポート C シリーズサーバが設定されている場合は、そのサーバをクリックしてポート接続を確認します。



Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:36:88	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:36:89	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:36:8A	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:36:8B	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:36:8C	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:36:8D	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:36:8E	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:36:8F	Unconfigured	Physical	Sfp Not Present	Disabled	

12. Equipment > Fabric Interconnects > Fabric Interconnect B > Fixed Module の順に展開します。
13. [Ethernet ポート] を展開します。

14. Cisco Nexus 31108 スイッチに接続されているイーサネットポート 1 および 2 を選択し、右クリックして、 Configure as Uplink Port （アップリンクポートとして設定）を選択します。
15. Yes をクリックしてアップリンクポートを確認し、 OK をクリックします。
16. ネットアップストレージコントローラに接続されているポート 3 と 4 を選択し、右クリックして Configure as Appliance Port （アプライアンスポートとして設定）を選択します。
17. Yes をクリックして、アプライアンスのポートを確認します。
18. Configure as Appliance Port （アプライアンスポートとして設定）ウィンドウで、 OK をクリックします。
19. [OK] をクリックして確定します。
20. 左側のペインで、 Fabric Interconnect B の Fixed Module を選択します
21. [Ethernet Ports] タブで、 [If Role] カラムにポートが正しく設定されていることを確認します。スケーラビリティポートにポート C シリーズサーバが設定されている場合は、そのサーバをクリックしてポート接続を確認します。



Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:3A:C8	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:3A:C9	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:3A:CA	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:3A:CB	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:3A:CC	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:3A:CD	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:3A:CE	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:3A:CF	Unconfigured	Physical	Sfp Not Present	Disabled	

Cisco Nexus 31108 スイッチへのアップリンクポートチャネルを作成します

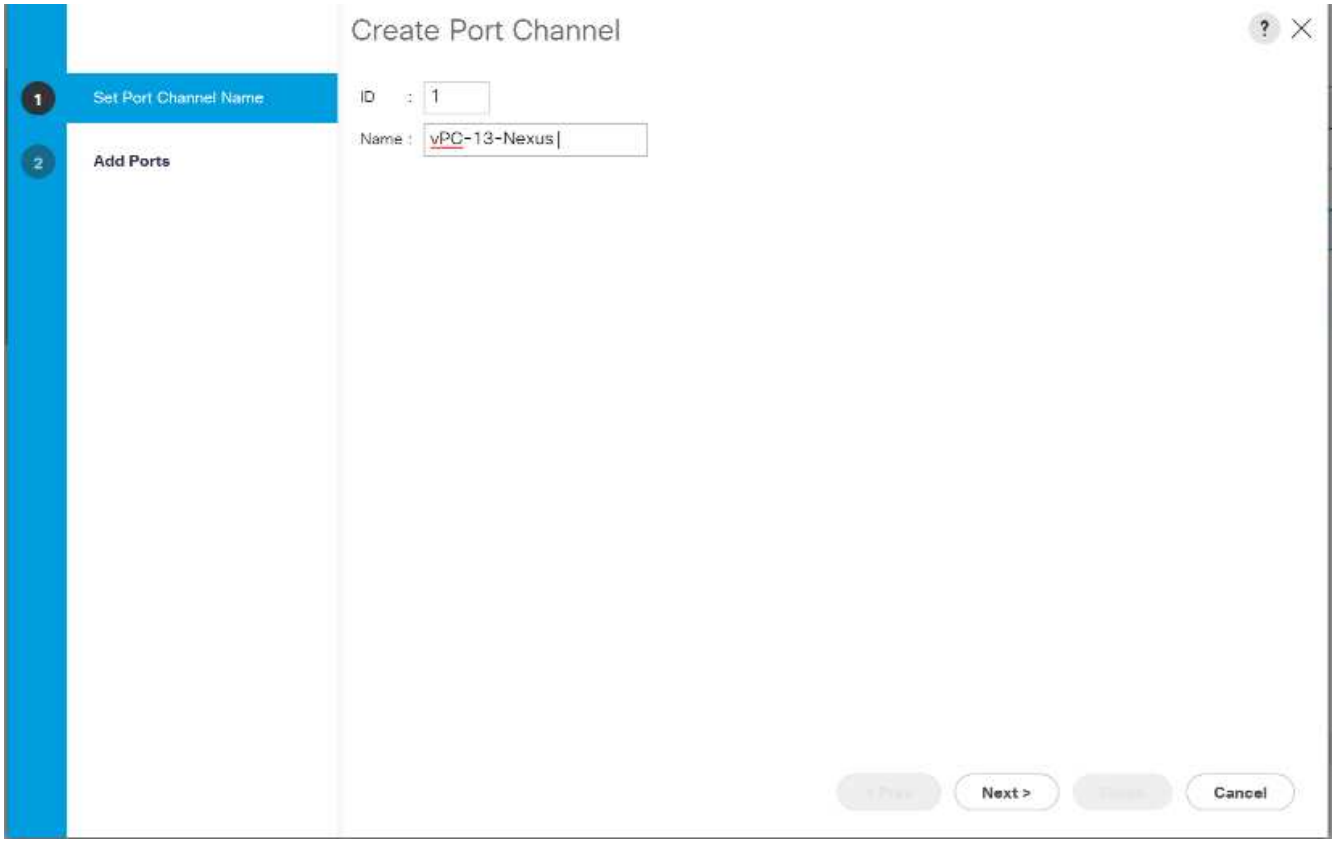
Cisco UCS 環境で必要なポートチャネルを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、ナビゲーションペインの [LAN] タブを選択します。

> この手順では、 2 つのポートチャネルが作成されます。 1 つはファブリック A から両方の Cisco Nexus 31108 スイッチへ、もう 1 つはファブリック B から両方の Cisco Nexus 31108 スイッチへです。標準スイッチを使用している場合は、それに応じてこの手順を変更します。ファブリックインターコネクト上で 1 ギガビットイーサネット（ 1GbE ）スイッチおよび GLC-T SFP を使用する場合は、ファブリックインターコネクト内のイーサネットポート 1/1 および 1/2 のインターフェイス速度を 1Gbps に設定する必要があります。

2. [LAN] > [LAN Cloud] で、 [Fabric A] ツリーを展開します。
3. [ポートチャネル] を右クリックします。
4. ポートチャネルの作成を選択します。

5. ポートチャネルの一意の ID として 13 を入力します。
6. ポートチャネルの名前として「 vPC-13-Nexus 」と入力します。
7. 次へをクリックします。



8. ポートチャネルに追加する次のポートを選択します。
   a. スロット ID 1 とポート 1
   b. スロット ID 1 とポート 2
9. >> をクリックして、ポートチャネルにポートを追加します。
10. Finish をクリックして、ポートチャネルを作成します。[OK] をクリックします。
11. [ポートチャネル] で、新しく作成したポートチャネルを選択します。

    ポートチャネルの全体的なステータスが up になっている必要があります。

12. ナビゲーションペインで、 [LAN] > [LAN Cloud] の下の [Fabric B] ツリーを展開します。
13. [ポートチャネル] を右クリックします。
14. ポートチャネルの作成を選択します。
15. ポートチャネルの一意の ID として「 14 」を入力します。
16. ポートチャネルの名前として「 vPC-14-Nexus 」と入力します。次へをクリックします。
17. ポートチャネルに追加する次のポートを選択します。
    a. スロット ID 1 とポート 1

b. スロット ID 1 とポート 2

18. >> をクリックして、ポートチャネルにポートを追加します。
19. Finish をクリックして、ポートチャネルを作成します。[OK] をクリックします。
20. [ポートチャネル] で、新しく作成したポートチャネルを選択します。
21. ポートチャネルの全体的なステータスが up になっている必要があります。

組織の作成（オプション）

組織は、リソースを整理し、 IT 組織内のさまざまなグループへのアクセスを制限することで、コンピューティングリソースのマルチテナンシーを実現するために使用されます。

> このドキュメントでは組織の使用は想定していませんが、この手順では組織の作成方法について説明します。

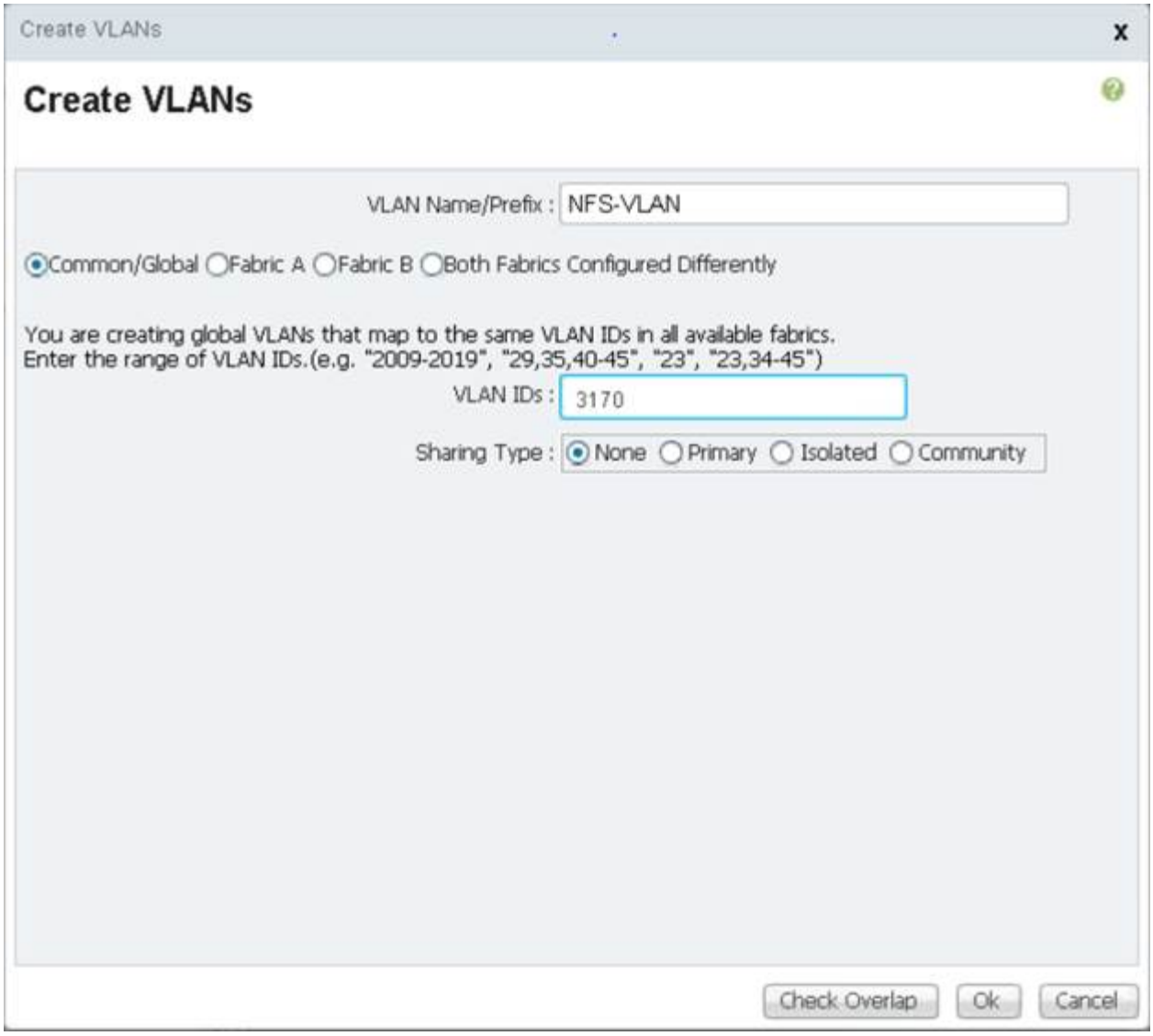
Cisco UCS 環境で組織を設定するには、次の手順を実行します。

1. Cisco UCS Manager で、ウィンドウ上部のツールバーの [新規作成（ New ）] メニューから、 [組織の作成（ Create Organization ）] を選択します。
2. 組織の名前を入力します。
3. オプション：組織の概要を入力します。[OK] をクリックします。
4. 確認メッセージで [OK] をクリックします。

ストレージアプライアンスのポートおよびストレージ **VLAN** を設定します

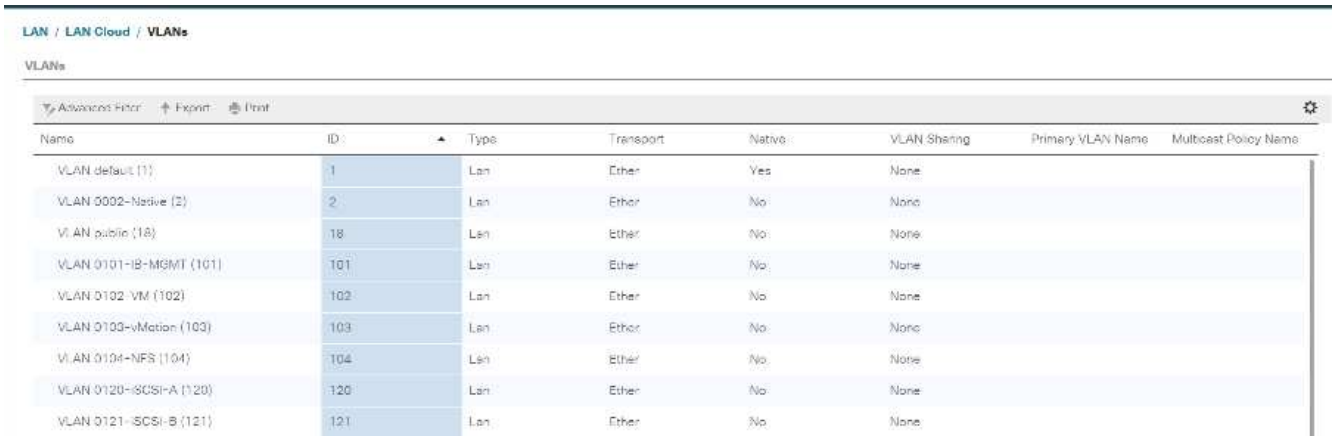
ストレージアプライアンスのポートとストレージ VLAN を設定するには、次の手順を実行します。

1. Cisco UCS Manager で、 [LAN] タブを選択します。
2. アプライアンスクラウドを拡張します。
3. アプライアンスクラウドの下の VLAN を右クリックします。
4. [Create VLANs] を選択します。
5. Infrastructure NFS VLAN の名前として「 nfs-vlan 」と入力します。
6. 共通 / グローバルを選択したままにします。
7. VLAN ID として「 <<var_nfs_vlan_id>> 」と入力します。
8. [共有タイプ] は [なし] のままにします。

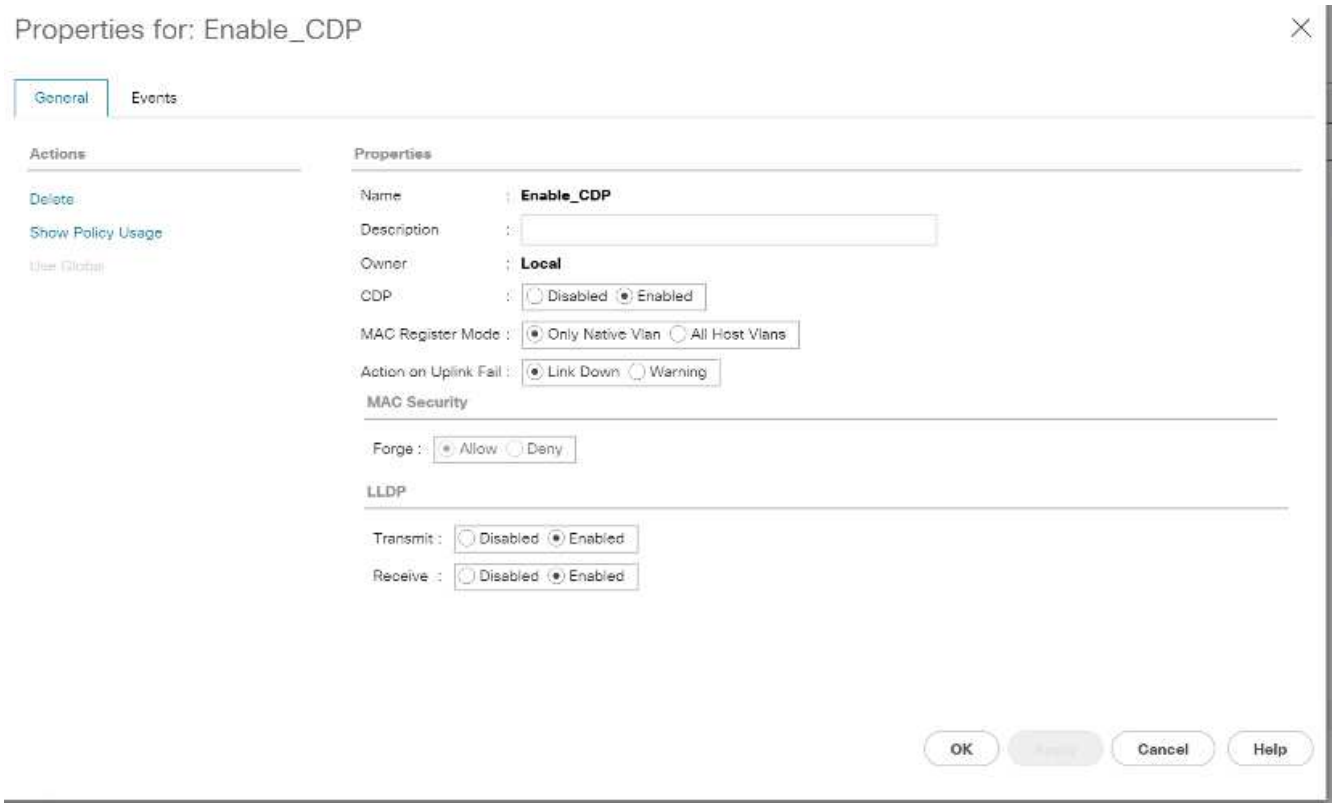


9. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。
10. アプライアンスクラウドの下の VLAN を右クリックします。
11. [Create VLANs] を選択します。
12. Infrastructure iSCSI Fabric A VLAN の名前として「 iSCSI-A-VLAN 」と入力します。
13. 共通 / グローバルを選択したままにします。
14. VLAN ID として「 <<var_iscsi-a_vlan_id>> 」と入力します。
15. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。
16. アプライアンスクラウドの下の VLAN を右クリックします。
17. [Create VLANs] を選択します。
18. インフラストラクチャ iSCSI ファブリック B VLAN の名前として「 iSCSI-B-VLAN 」と入力します。
19. 共通 / グローバルを選択したままにします。
20. VLAN ID として「 <<var_iscsi-b_vlan_id>> 」と入力します。
21. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。

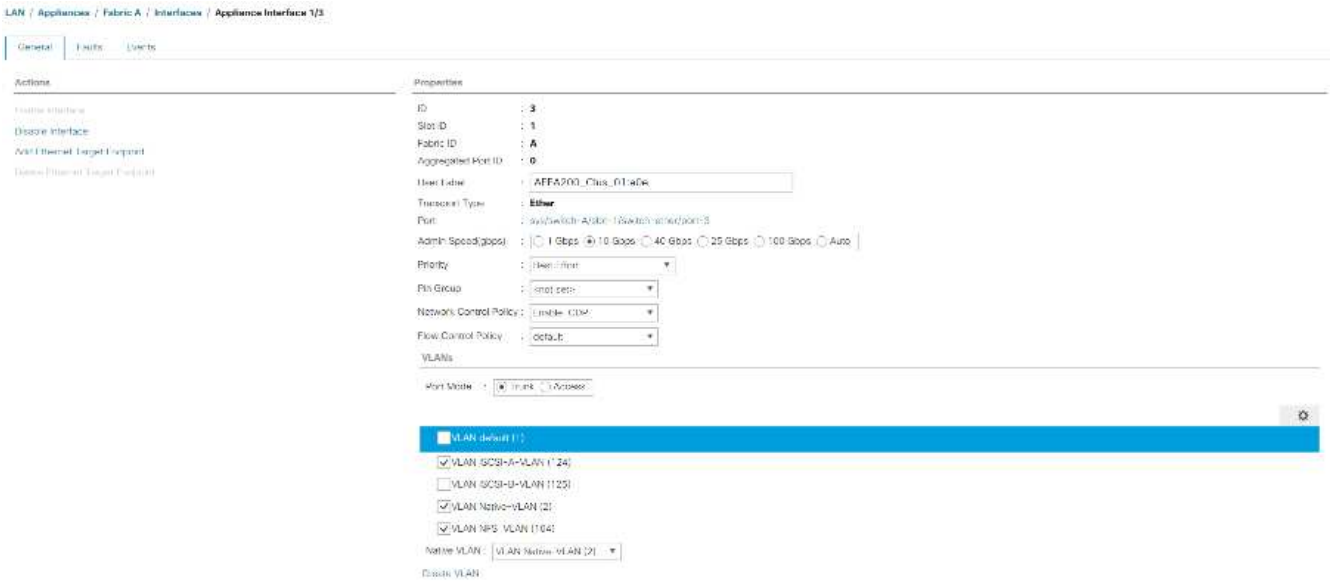
22. アプライアンスクラウドの下の VLAN を右クリックします。
23. [Create VLANs] を選択します。
24. ネイティブ VLAN の名前として「 Native - VLAN 」と入力します。
25. 共通 / グローバルを選択したままにします。
26. VLAN ID として「 <<var_native_vlan_id>> 」と入力します。
27. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。



28. ナビゲーションペインで、 [LAN] > [Policies] の下の [Appliances] を展開し、 [Network Control Policies] を右クリックします。
29. Create Network Control Policy を選択します。
30. ポリシーに「 Enable_cdp_LLPD 」という名前を付け、 CDP の横にある [有効] を選択します。
31. LLDP の送受信機能を有効にします。

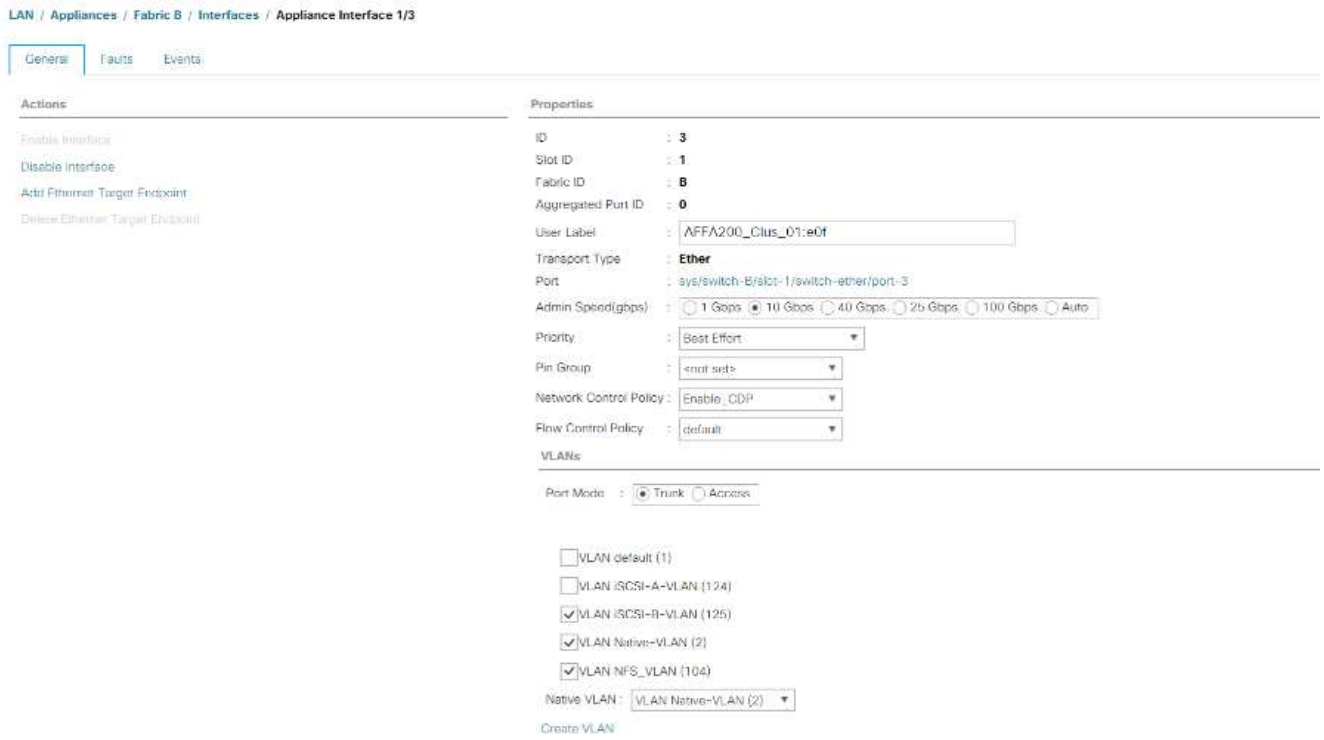


32. [OK] をクリックし、もう一度 [OK] をクリックしてポリシーを作成します。
33. ナビゲーションペインの [LAN] > [Appliances Cloud] で、 [Fabric A tree] を展開します。
34. [Interfaces] を展開します。
35. アプライアンス・インターフェイス 1/3 を選択します。
36. [User Label] フィールドに、「 <storage_controller_01_name> ： e0e 」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。
37. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
38. [VLANs] で、 iSCSI-A VLAN 、 NFS VLAN 、およびネイティブ VLAN を選択します。ネイティブ VLAN をネイティブ VLAN として設定します。デフォルトの VLAN 選択をクリアします。
39. [変更を保存して OK] をクリックします。



40. [Fabric A] の下にある [Appliance Interface] 1/4 を選択します
41. [User Label] フィールドに、「 <storage_controller_02_name> ： e0e 」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。
42. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
43. [VLANs] で、 iSCSI-A VLAN 、 NFS VLAN 、およびネイティブ VLAN を選択します。
44. ネイティブ VLAN をネイティブ VLAN として設定します。
45. デフォルトの VLAN 選択をクリアします。
46. [変更を保存して OK] をクリックします。
47. ナビゲーションペインの [LAN] > [Appliances Cloud] で、 [Fabric B] ツリーを展開します。
48. [Interfaces] を展開します。
49. アプライアンス・インターフェイス 1/3 を選択します。
50. [User Label] フィールドに、「 <storage_controller_01_name> ： e0f 」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。

51. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
52. [VLANs] で、 [iSCSI-B-VLAN] 、 [NFS VLAN] 、および [ネイティブ VLAN] を選択します。ネイティブ VLAN をネイティブ VLAN として設定します。デフォルト VLAN の選択を解除します。

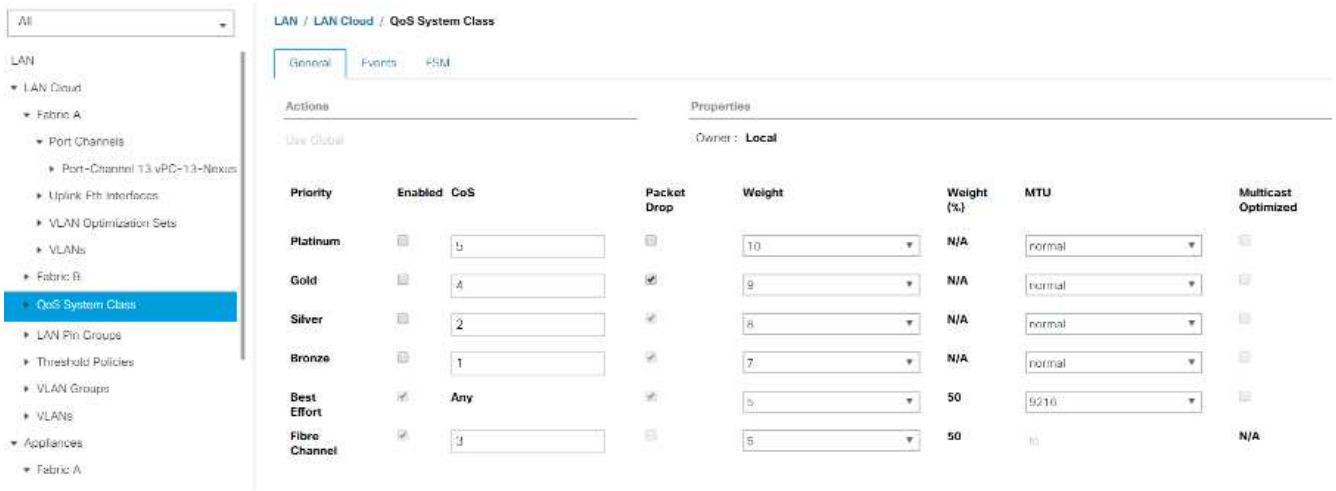


53. [変更を保存して OK] をクリックします。
54. [Fabric B] の下にある [Appliance Interface] 1/4 を選択します
55. [User Label] フィールドに、「 <storage_controller_02_name> ： e0f 」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。
56. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
57. [VLANs] で、 [iSCSI-B-VLAN] 、 [NFS VLAN] 、および [ネイティブ VLAN] を選択します。ネイティブ VLAN をネイティブ VLAN として設定します。デフォルト VLAN の選択を解除します。
58. [変更を保存して OK] をクリックします。

Cisco UCS ファブリックでジャンボフレームを設定します

Cisco UCS ファブリックでジャンボフレームを設定して QoS を有効にするには、次の手順を実行します。

1. Cisco UCS Manager のナビゲーションペインで、 [LAN] タブをクリックします。
2. [LAN] > [LAN Cloud] > [QoS System Class] の順に選択します。
3. 右側のペインで、 [全般] タブをクリックします。
4. [ベストエフォート] 行で、 [MTU] 列の下のボックスに 9216 と入力します。



5. [Save Changes] をクリックします。
6. [OK] をクリックします。

Cisco UCS シャーシを確認します

すべての Cisco UCS シャーシを確認するには、次の手順を実行します。

1. Cisco UCS Manager で、 [Equipment] タブを選択し、右側の [Equipment] タブを展開します。
2. 機器 > シャーシを展開します。
3. シャーシ 1 のアクションでシャーシの確認を選択します。
4. [OK] をクリックし、 [OK] をクリックしてシャーシの確認を完了します。
5. [閉じる] をクリックして、 [プロパティ] ウィンドウを閉じます。

Cisco UCS 4.0(1b) ファームウェアイメージをロードします

Cisco UCS Manager ソフトウェアと Cisco UCS Fabric Interconnect ソフトウェアをバージョン 4.0(1b) にアップグレードするには、を参照してください "Cisco UCS Manager インストールおよびアップグレードガイド"。

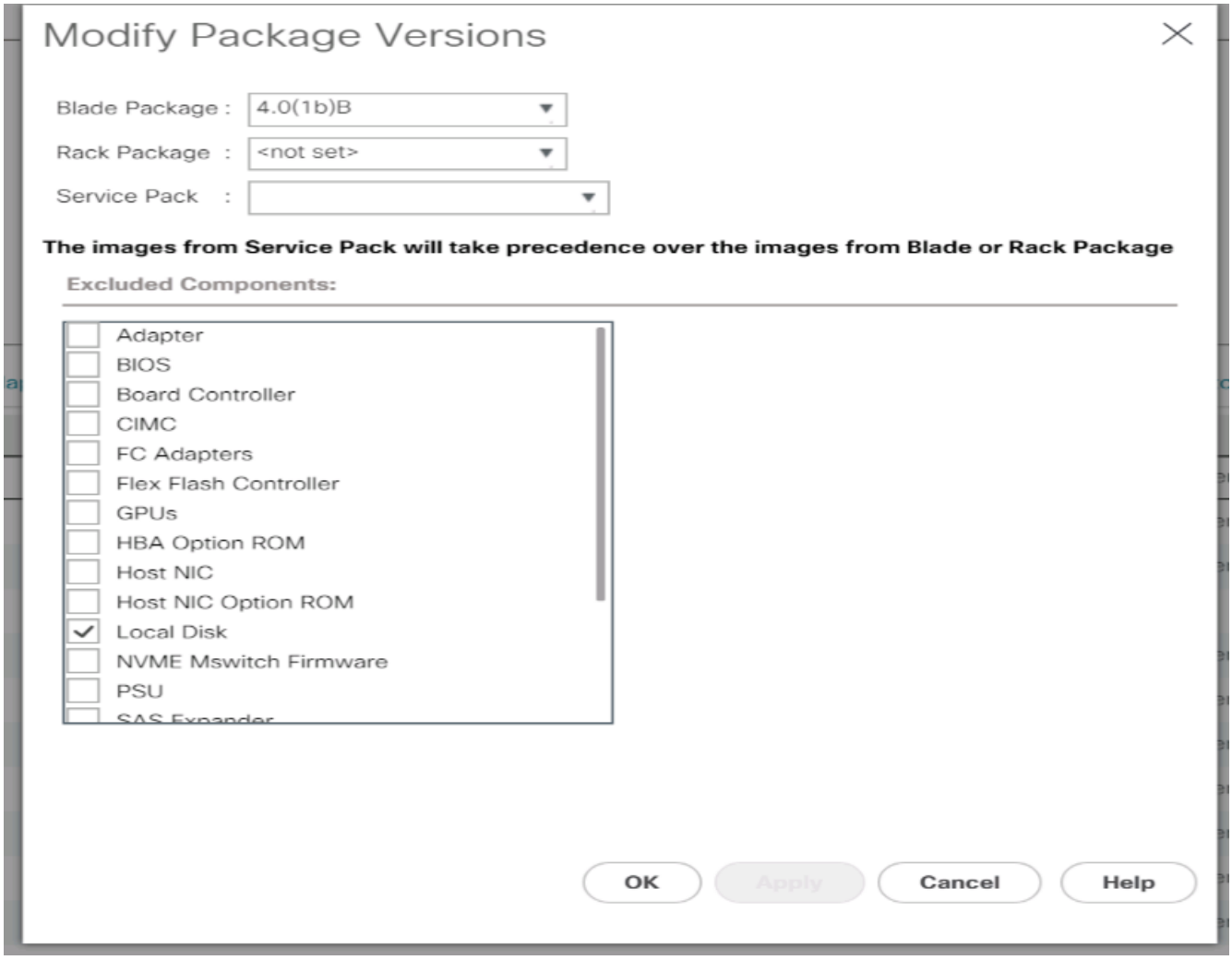
ホストファームウェアパッケージを作成する

ファームウェア管理ポリシーを使用すると、管理者は特定のサーバ設定に対応するパッケージを選択できます。これらのポリシーには、多くの場合、アダプタ、 BIOS 、ボードコントローラ、 FC アダプタ、ホストバスアダプタ（ HBA ）オプション ROM 、ストレージコントローラプロパティのパッケージが含まれています。

Cisco UCS 環境で特定のサーバ設定のファームウェア管理ポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. ホストファームウェアパッケージを展開します。
4. デフォルトを選択します。

5. アクションペインで、パッケージバージョンの変更を選択します。
6. 両方のブレードパッケージのバージョン 4.0(1b) を選択します。



7. [OK] をクリックし、もう一度 [OK] をクリックして、ホストファームウェアパッケージを変更します。

MAC アドレスプールを作成します

Cisco UCS 環境に必要な MAC アドレスプールを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. プール／ルートを選択します。

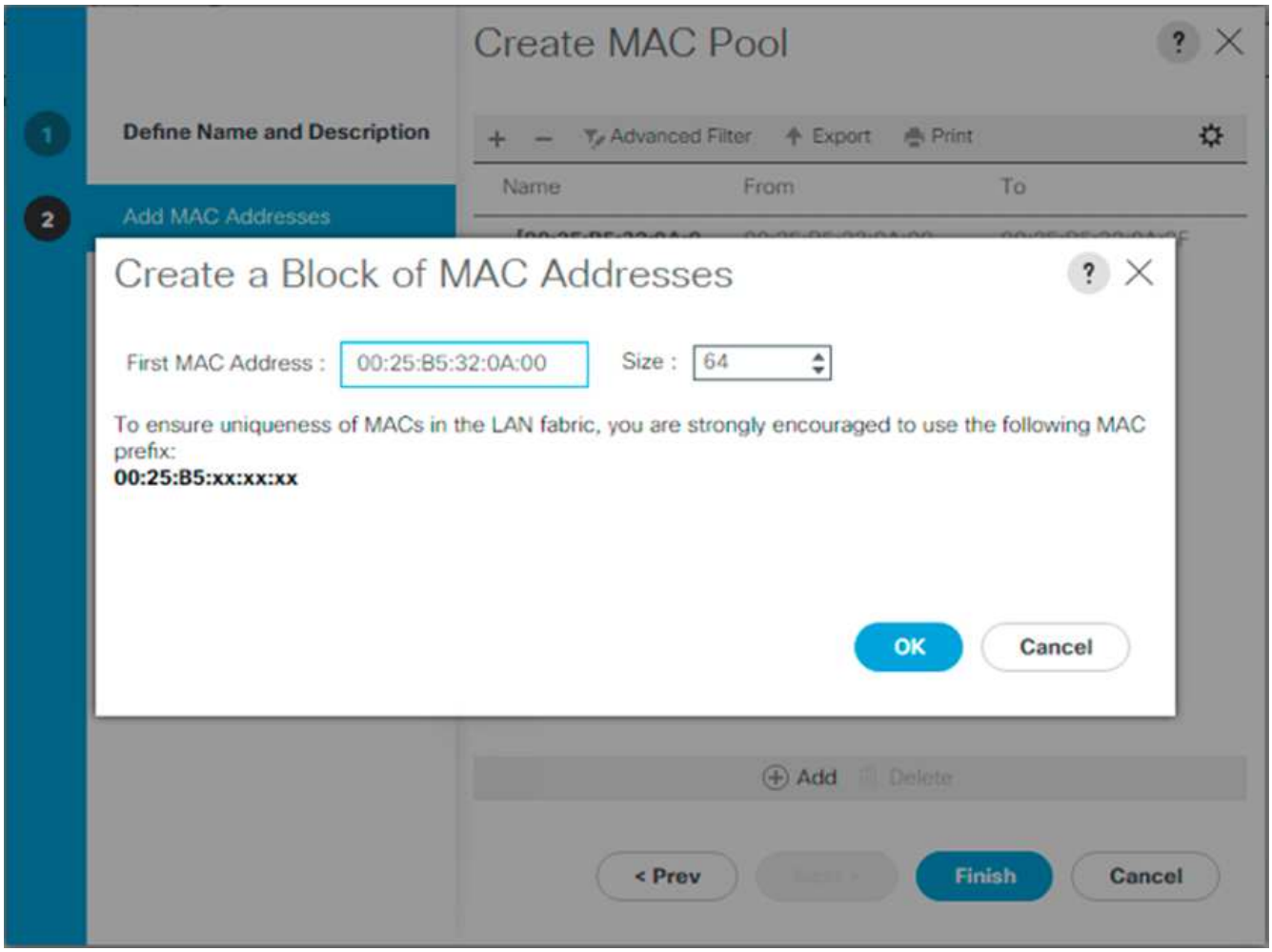
   この手順では、スイッチングファブリックごとに 1 つずつ、 2 つの MAC アドレスプールが作成されます。

3. ルート組織の下にある [MAC Pools] を右クリックします。
4. MAC アドレスプールを作成するには、 Create MAC Pool （ MAC プールの作成）を選択します。
5. MAC プールの名前として「 MAC-Pool-A 」と入力します。
6. オプション： MAC プールの概要を入力します。

7. 割り当て順序（ Assignment Order ）のオプションとして順次（ Sequential ）を選択します。次へをクリックします。
8. 追加をクリックします。
9. 開始 MAC アドレスを指定します。

> FlexPod 解決策では、開始 MAC アドレスの最後のオクテットに 0a を配置して、すべての MAC アドレスをファブリック A アドレスとして識別することを推奨します。この例では、最初の MAC アドレスとして 00 ： 25 ： B5 ： 32 ： 0a:00 を与える Cisco UCS ドメイン番号情報も組み込みました。

10. 使用可能なブレードまたはサーバリソースをサポートするのに十分な MAC アドレスプールのサイズを指定します。[OK] をクリックします。



11. 完了をクリックします。
12. 確認メッセージが表示されたら、 [OK] をクリックします。
13. ルート組織の下にある [MAC Pools] を右クリックします。
14. MAC アドレスプールを作成するには、 Create MAC Pool （ MAC プールの作成）を選択します。
15. MAC プールの名前として「 MAC-Pool-B 」と入力します。
16. オプション： MAC プールの概要を入力します。

17. 割り当て順序（ Assignment Order ）のオプションとして順次（ Sequential ）を選択します。次へをクリックします。
18. 追加をクリックします。
19. 開始 MAC アドレスを指定します。

> FlexPod 解決策の場合、このプール内のすべての MAC アドレスをファブリック B アドレスとして識別するために、開始 MAC アドレスの最後のオクテットの隣に 0B を配置することを推奨します。この例では、最初の MAC アドレスとして 00 ： 25 ： B5 ： 32 ： 0B ： 00 を与える Cisco UCS ドメイン番号情報も組み込みました。

20. 使用可能なブレードまたはサーバリソースをサポートするのに十分な MAC アドレスプールのサイズを指定します。[OK] をクリックします。
21. 完了をクリックします。
22. 確認メッセージが表示されたら、 [OK] をクリックします。

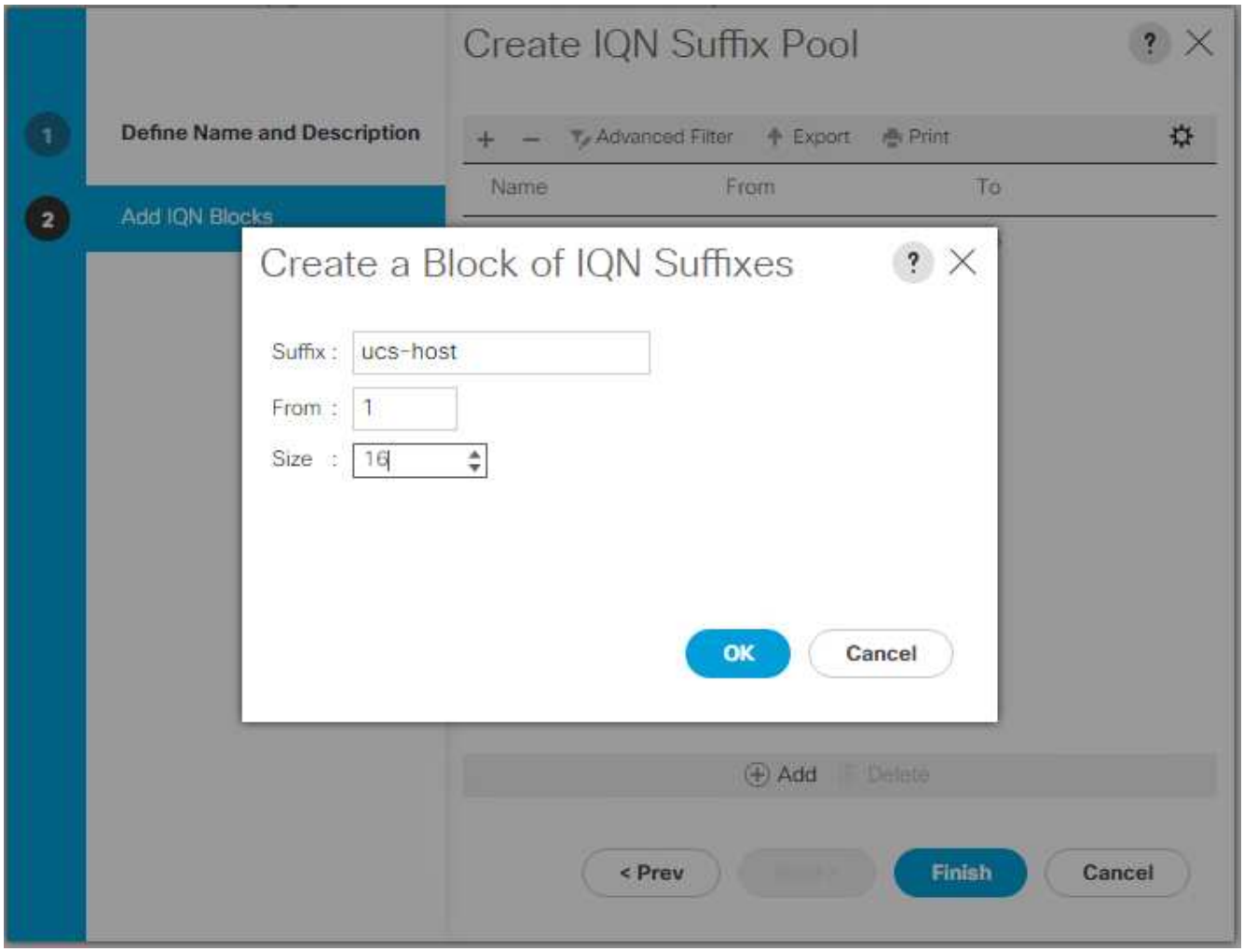
iSCSI IQN プールを作成します

Cisco UCS 環境に必要な IQN プールを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [SAN] をクリックします。
2. プール／ルートを選択します。
3. IQN プールを右クリックします。
4. IQN サフィックスプールの作成を選択して IQN プールを作成します。
5. IQN プールの名前として「 IQN -Pool 」と入力します。
6. オプション： IQN プールの概要を入力します。
7. プレフィックスとして「 iqn.1992-08.com.cisco` 」と入力します。
8. [割り当て順序] で [順次] を選択します。次へをクリックします。
9. 追加をクリックします。
10. サフィックスに「 UCS-host」 と入力します。

> 複数の Cisco UCS ドメインを使用している場合は、さらに具体的な IQN サフィックスを使用する必要があります。

11. [From] フィールドに 1 を入力します。
12. 使用可能なサーバリソースを十分にサポートできる IQN ブロックのサイズを指定してください。[OK] をクリックします。



13. 完了をクリックします。

iSCSI イニシエータの **IP** アドレスプールを作成します

Cisco UCS 環境に必要な IP プール iSCSI ブートを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. プール／ルートを選択します。
3. [IP Pools] を右クリックします。
4. Create IP Pool を選択します。
5. IP プール名として「 iSCSI-IP-Pool-A 」と入力します。
6. オプション： IP プールの概要を入力します。
7. 割り当て順序の [順次] を選択します。次へをクリックします。
8. Add をクリックして IP アドレスのブロックを追加します。
9. [From] フィールドに、 iSCSI IP アドレスとして割り当てる範囲の先頭を入力します。
10. サーバに対応できる十分なアドレスにサイズを設定してください。[OK] をクリックします。
11. 次へをクリックします。

12. 完了をクリックします。
13. [IP Pools] を右クリックします。
14. Create IP Pool を選択します。
15. IP プール名として「 iSCSI-IP-Pool-B 」と入力します。
16. オプション： IP プールの概要を入力します。
17. 割り当て順序の [順次] を選択します。次へをクリックします。
18. Add をクリックして IP アドレスのブロックを追加します。
19. [From] フィールドに、 iSCSI IP アドレスとして割り当てる範囲の先頭を入力します。
20. サーバに対応できる十分なアドレスにサイズを設定してください。[OK] をクリックします。
21. 次へをクリックします。
22. 完了をクリックします。

UUID サフィックスプールを作成します

Cisco UCS 環境に必要な Universally Unique Identifier （ UUID ）サフィックスプールを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. プール／ルートを選択します。
3. [UUID Suffix Pools] を右クリックします。
4. [Create UUID Suffix Pool] を選択します。
5. UUID サフィックスプールの名前として「 UUID - プール」と入力します。
6. オプション： UUID サフィックスプールの概要を入力します。
7. 接頭部は派生オプションのままにします。
8. 割り当て順序（ Assignment Order ）に順次（ Sequential ）を選択し
9. 次へをクリックします。
10. Add をクリックして UUID のブロックを追加します。
11. デフォルト設定の [From] フィールドをそのまま使用します。
12. 使用可能なブレードまたはサーバリソースをサポートするのに十分な UUID ブロックのサイズを指定します。[OK] をクリックします。
13. 完了をクリックします。
14. [OK] をクリックします。

サーバプールを作成します

Cisco UCS 環境に必要なサーバプールを設定するには、次の手順を実行します。

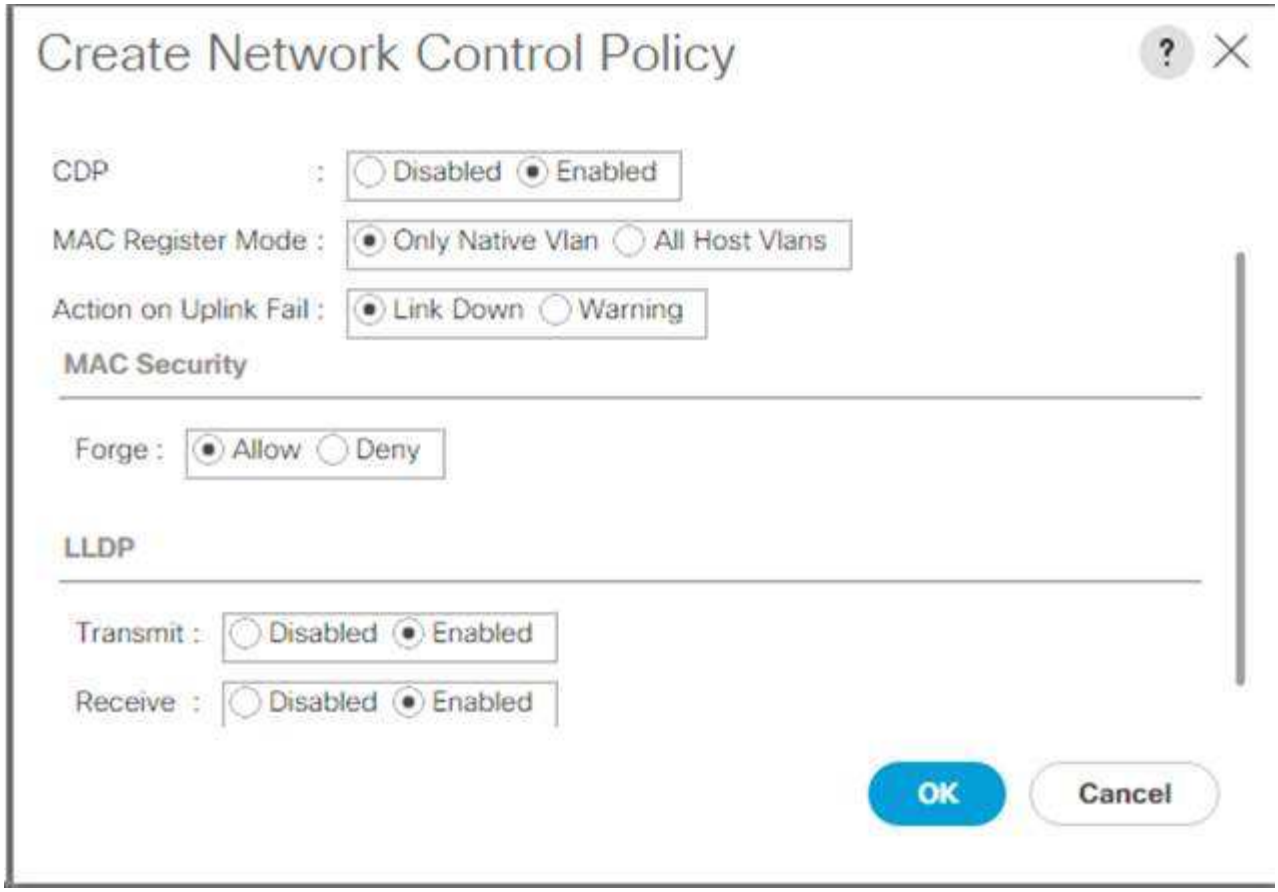
> 環境で必要とされる細分性を実現するために、固有のサーバプールを作成することを検討してください。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. プール／ルートを選択します。
3. [サーバープール] を右クリックします。
4. Create Server Pool を選択します。
5. サーバ・プールの名前として「 Infra-Pool 」と入力します。
6. オプション：サーバプールの概要を入力します。次へをクリックします。
7. VMware 管理クラスタに使用するサーバを 2 つ以上選択し '>> をクリックして Infra-Pool' Server プールに追加します
8. 完了をクリックします。
9. [OK] をクリックします。

Cisco Discovery Protocol と **Link Layer Discovery Protocol** のネットワーク制御ポリシーを作成します

Cisco Discovery Protocol （ CDP ）および Link Layer Discovery Protocol （ LLDP ）のネットワーク制御ポリシーを作成するには、次の手順を実行します。

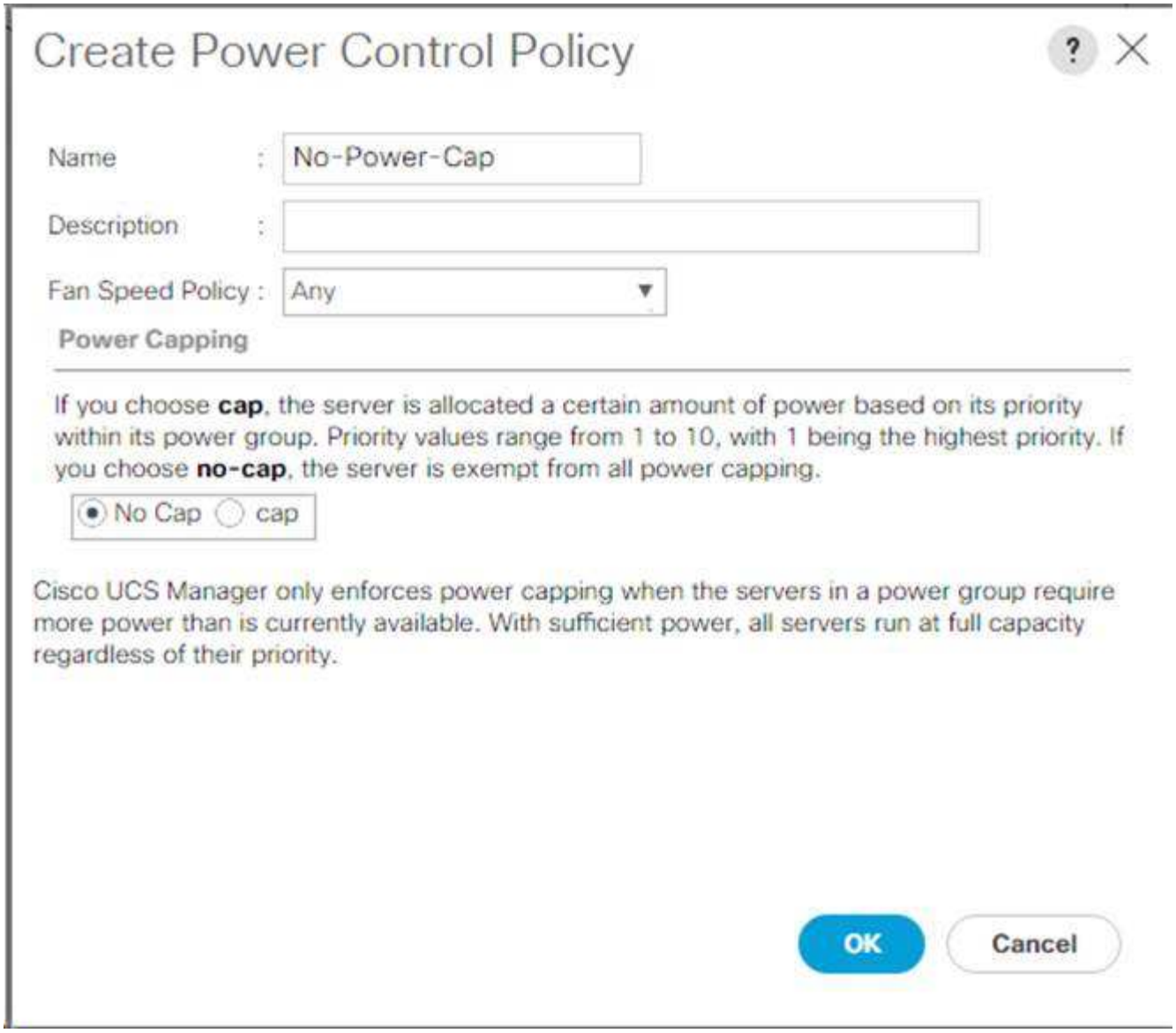
1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [ネットワーク制御ポリシー] を右クリックします。
4. Create Network Control Policy を選択します。
5. Enable-CDP-LLDP ポリシー名を入力します。
6. CDP の場合は、 Enabled オプションを選択します。
7. LLDP の場合は、下にスクロールして、送信と受信の両方で有効を選択します。
8. [OK] をクリックして、ネットワーク制御ポリシーを作成します。[OK] をクリックします。



電源制御ポリシーを作成します

Cisco UCS 環境の電源制御ポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers タブをクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [電源制御ポリシー] を右クリックします。
4. 電源制御ポリシーの作成を選択します。
5. 電源制御ポリシー名として No-Power-Cap と入力します。
6. 電力上限設定を [No Cap](キャップなし) に変更します
7. [OK] をクリックして、電源制御ポリシーを作成します。[OK] をクリックします。



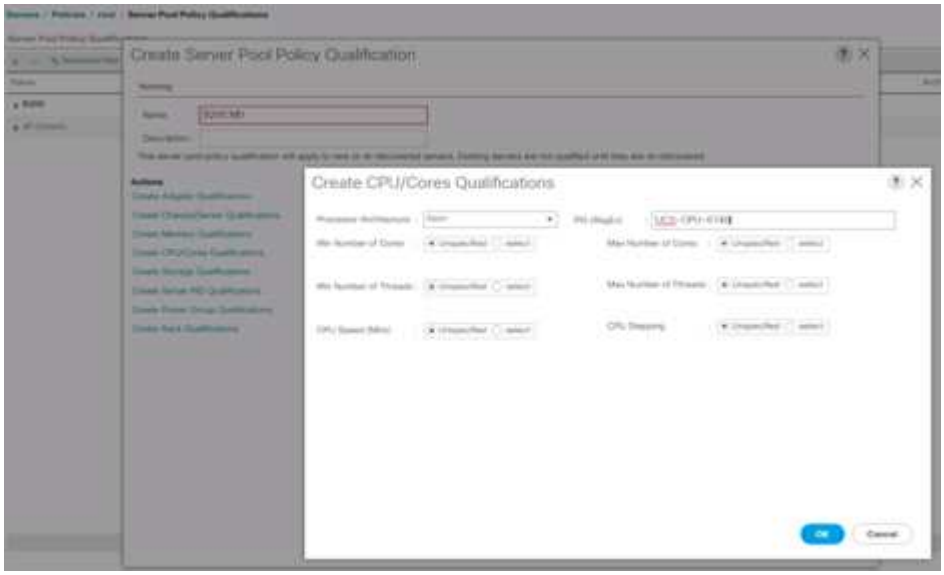
サーバプール認定ポリシーの作成（オプション）

Cisco UCS 環境のオプションのサーバプール認定ポリシーを作成するには、次の手順を実行します。

> この例では、 Intel E2660 v4 Xeon Broadwell プロセッサを搭載した Cisco UCS B シリーズサーバ用のポリシーを作成します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [サーバプールポリシーの条件] を選択します。
4. Create Server Pool Policy Qualification （サーバプールポリシーの作成条件）または Add （追加）を
5. ポリシーにインテルという名前を付けます。
6. Create CPU/ Cores Qualifications] を選択します。
7. プロセッサ / アーキテクチャに Xeon を選択します。

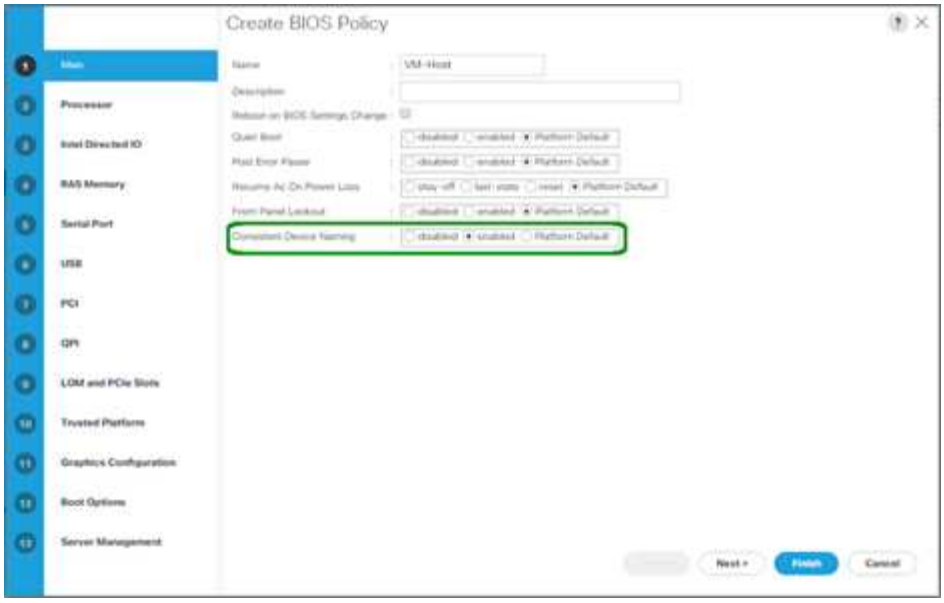
8. プロセス ID （ PID ）として「 <UCS-CPU-PID>` 」と入力します。
9. [OK] をクリックして、 CPU/ コアの資格情報を作成します。
10. [OK] をクリックしてポリシーを作成し、 [OK] をクリックして確認します。



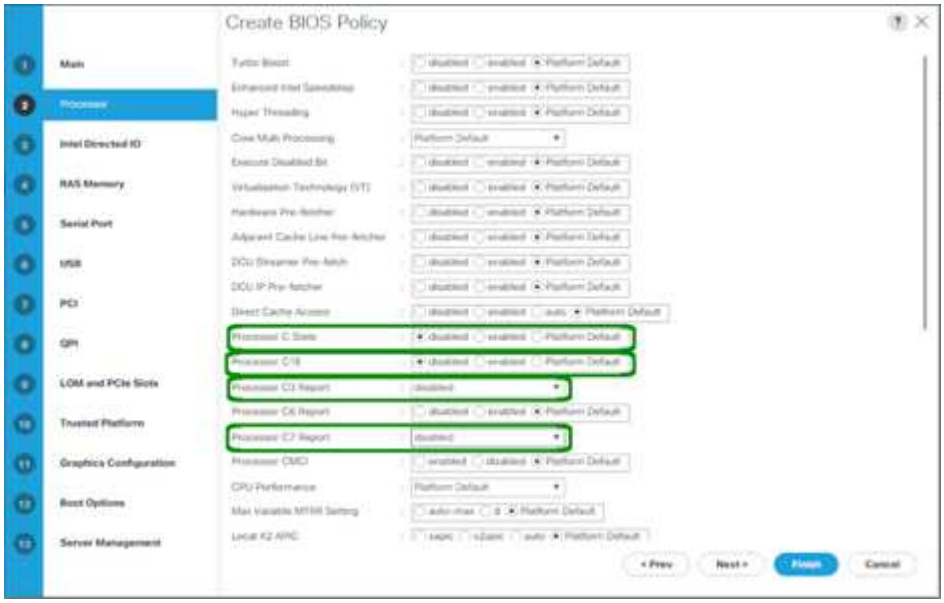
サーバ **BIOS** ポリシーを作成します

Cisco UCS 環境のサーバ BIOS ポリシーを作成するには、次の手順を実行します。

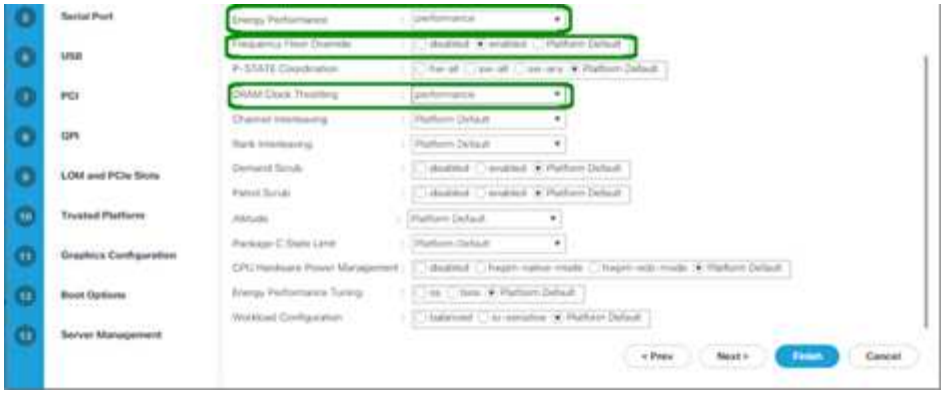
1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. BIOS Policies （ BIOS ポリシー）を右クリックします。
4. [Create BIOS Policy] を選択します。
5. BIOS ポリシー名として「 VM-Host 」と入力します。
6. Quiet Boot 設定を disabled に変更します。
7. 一貫したデバイス名を有効に変更します。



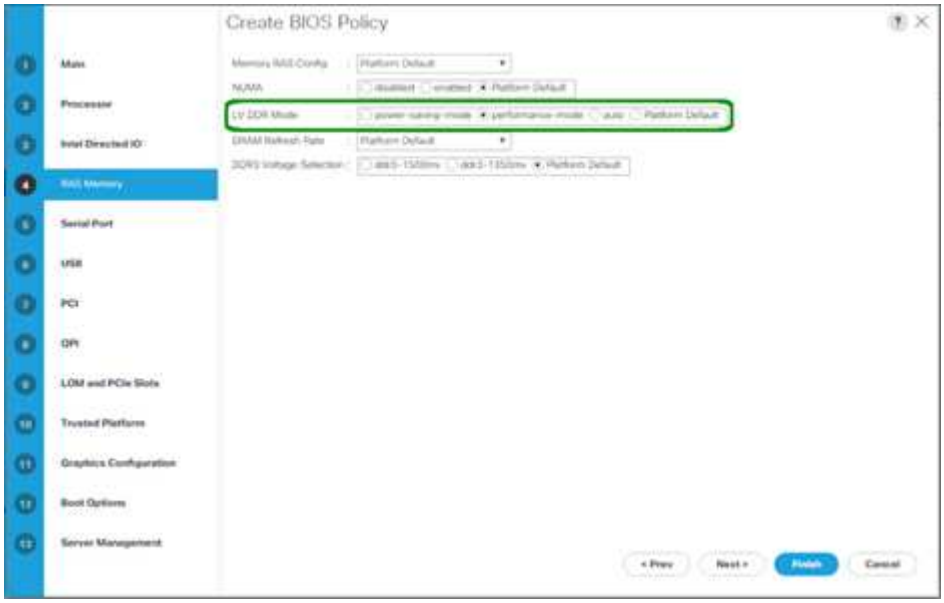
8. [プロセッサ] タブを選択し、次のパラメータを設定します。
   - プロセッサ C の状態：無効
   - プロセッサ C1E ：無効
   - プロセッサ C3 レポート : 無効
   - プロセッサ C7 レポート：無効



9. 残りのプロセッサオプションまで下にスクロールして、次のパラメータを設定します。
   - エネルギー性能：パフォーマンス
   - 周波数下限のオーバーライド：有効
   - DRAM Clock Throttling ：パフォーマンス



10. [RAS メモリ] をクリックして、次のパラメータを設定します。
    - LV DDR モード：パフォーマンスモード

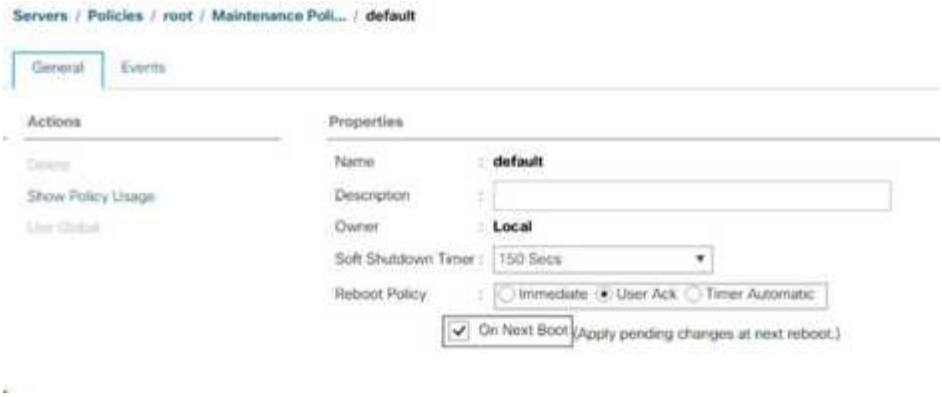


11. Finish をクリックして、 BIOS ポリシーを作成します。
12. [OK] をクリックします。

デフォルトのメンテナンスポリシーを更新する

デフォルトのメンテナンスポリシーを更新するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [メンテナンスポリシー]>[デフォルト] を選択します。
4. Reboot Policy を User Ack に変更します
5. [次のブート時] を選択して、メンテナンス時間をサーバー管理者に委任します。



6. [Save Changes] をクリックします。
7. [OK] をクリックして変更を確定します。

vNIC テンプレートを作成します

Cisco UCS 環境用に複数の仮想ネットワークインターフェイスカード（ vNIC ）テンプレートを作成するには、この項で説明する手順を実行します。

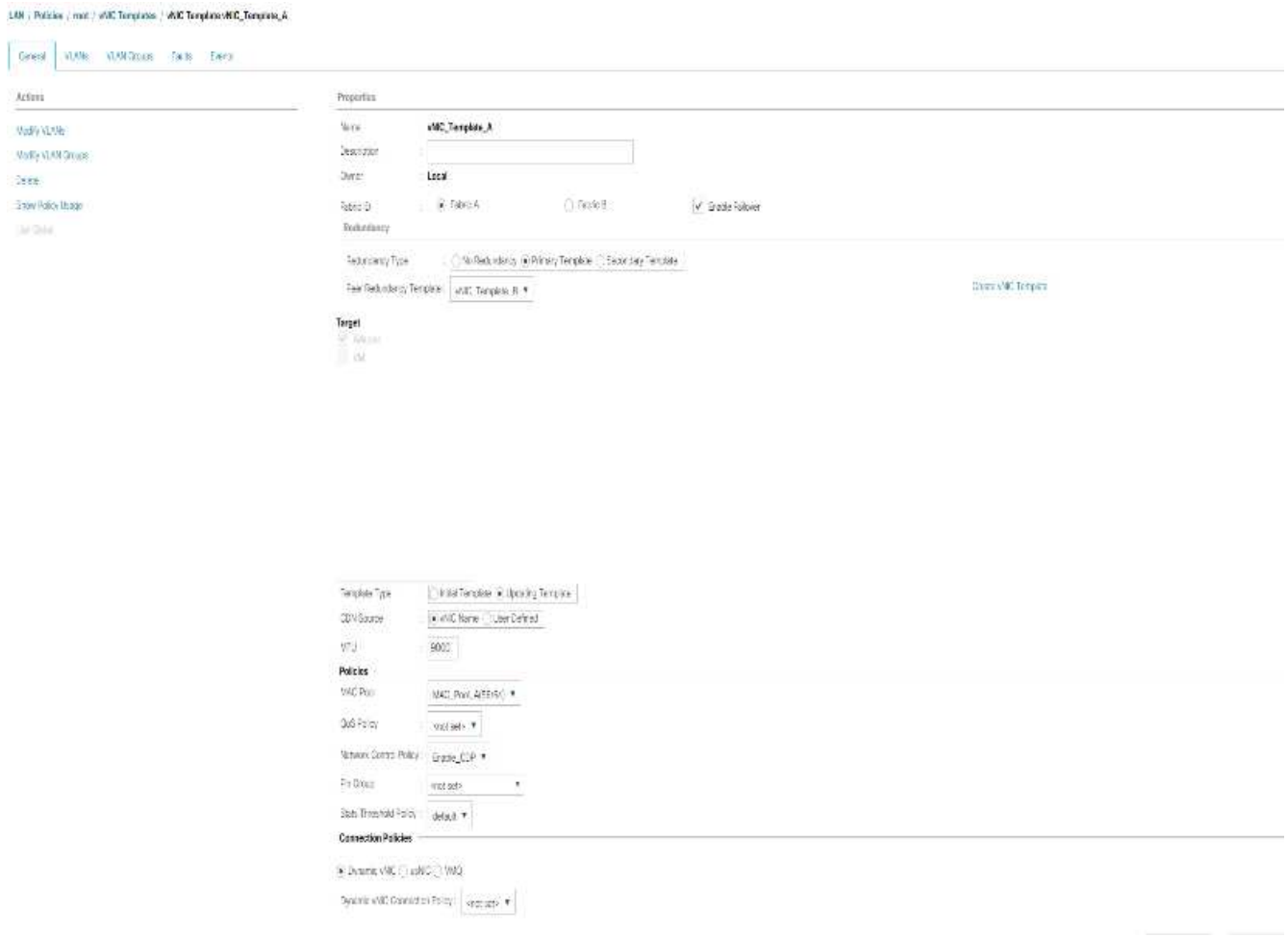
> 合計 4 つの vNIC テンプレートが作成されます。

インフラストラクチャ vNIC を作成します

インフラストラクチャ vNIC を作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [vNIC Templates] を右クリックします。
4. [Create vNIC Template] を選択します。
5. vNIC テンプレート名として「 ite -XX-vnic_a 」と入力します。
6. [テンプレートタイプ] として [更新テンプレート] を選択します。
7. [Fabric ID] に [Fabric A] を選択します
8. [Enable Failover] オプションが選択されていないことを確認します。
9. [冗長性タイプ] の [プライマリテンプレート] を選択します。
10. ピア冗長性テンプレートを「 <not set> 」のままにします。
11. [ターゲット] で、 [アダプタ] オプションのみが選択されていることを確認します。
12. ネイティブ VLAN として 'Native - VLAN' を設定します
13. CDN ソースの vNIC 名を選択します。
14. MTU の場合は 9000 と入力します。
15. [Permitted VLANs] で、 [Native - VLAN] 、 [Site-XX-IB-MGMT] 、 [Site-XX-NFS] 、 [Site-XX-VM-Traffic] を選択します。 および Site-XX-MvMotion複数選択するには、 Ctrl キーを使用します。
16. 選択をクリックします。これらの VLAN が Selected VLANs の下に表示されます。

17. [MAC Pool] リストで、 [M AC_Pool_A] を選択します。
18. [ネットワーク制御ポリシー] リストで、 [プール A] を選択します
19. [ネットワーク制御ポリシー] リストで、 [有効 - CDP-LLDP] を選択します。
20. [OK] をクリックして、 vNIC テンプレートを作成します。
21. [OK] をクリックします。

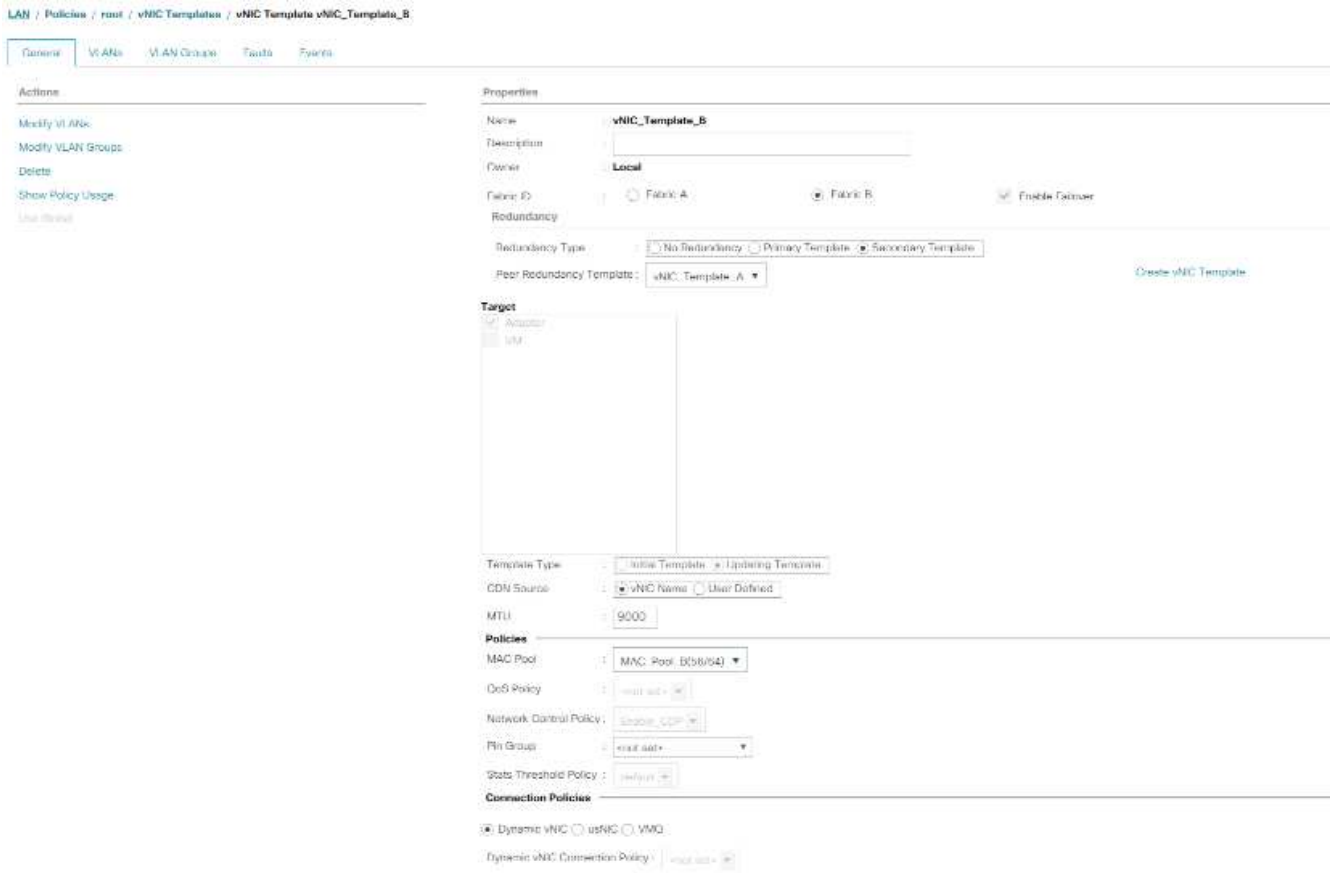


セカンダリ冗長テンプレート Infra-B を作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [vNIC Templates] を右クリックします。
4. [Create vNIC Template] を選択します。
5. vNIC テンプレート名として「 ite-XX-vnic_B 」と入力します。
6. [テンプレートタイプ] として [更新テンプレート] を選択します。
7. [Fabric ID] に [Fabric B] を選択します
8. [Enable Failover] オプションを選択します。

フェールオーバーを選択することは、ハードウェアレベルでリンクのフェールオーバー時間を改善し、仮想スイッチで検出されない NIC 障害の可能性を防ぐための重要なステップです。

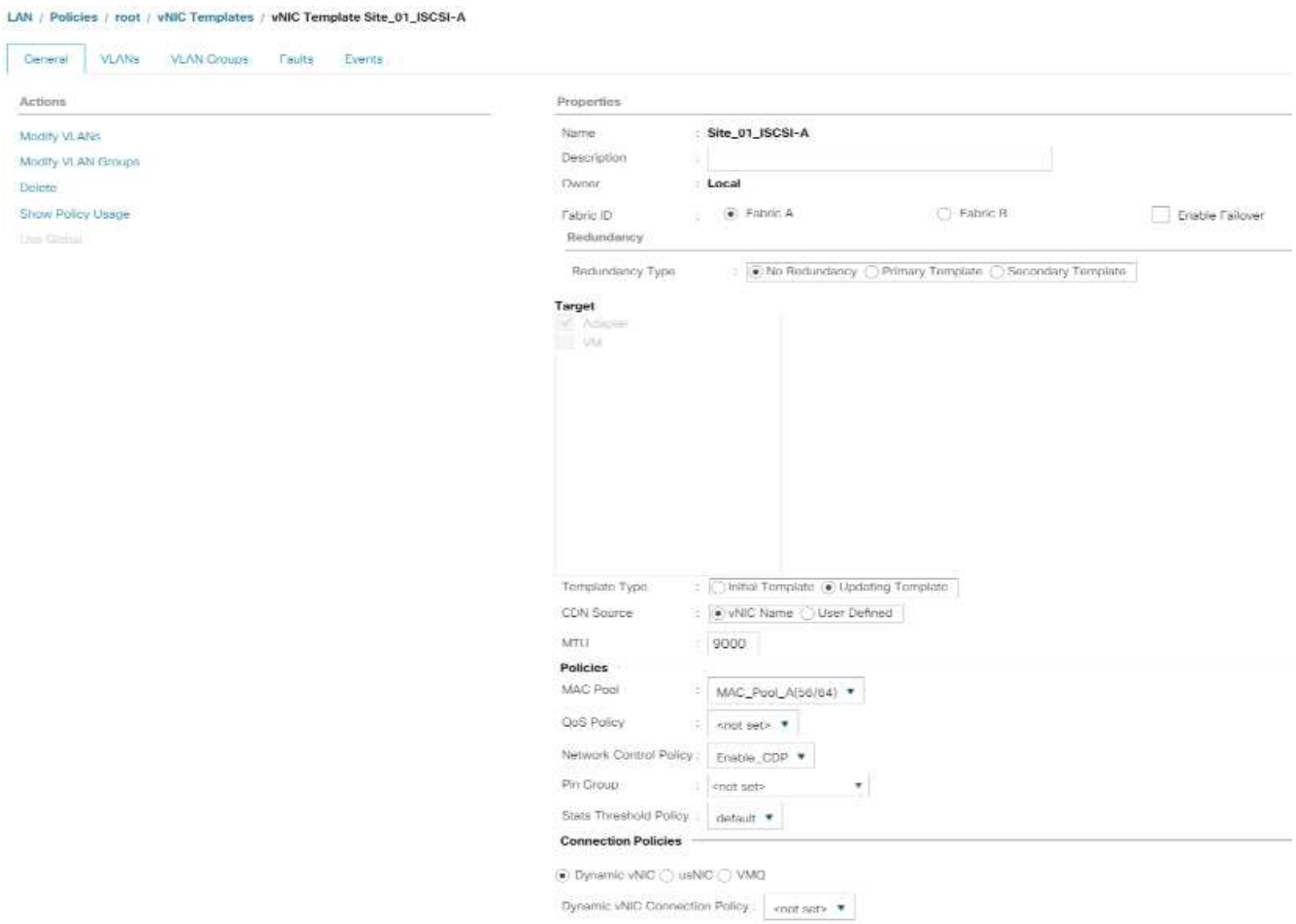
9. [冗長性タイプ] の [プライマリテンプレート] を選択します。
10. ピア冗長性テンプレートは 'vNIC_Template_A' のままにします
11. [ターゲット] で、 [アダプタ] オプションのみが選択されていることを確認します。
12. ネイティブ VLAN として 'Native - VLAN' を設定します
13. CDN ソースの vNIC 名を選択します。
14. MTU には '9000' と入力します
15. [Permitted VLANs] で、 [Native - VLAN] 、 [Site-XX-IB-MGMT] 、 [Site-XX-NFS] 、 [Site-XX-VM-Traffic] を選択します。 および Site-XX-MvMotion複数選択するには、 Ctrl キーを使用します。
16. 選択をクリックします。これらの VLAN が Selected VLANs の下に表示されます。
17. [MAC Pool] リストで、 [`M AC_Pool_b] を選択します。
18. [Network Control Policy] リストで、 [Pool-B] を選択します
19. [ネットワーク制御ポリシー] リストで、 [有効 - CDP-LLDP] を選択します。
20. [OK] をクリックして、 vNIC テンプレートを作成します。
21. [OK] をクリックします。



iSCSI vNIC を作成します

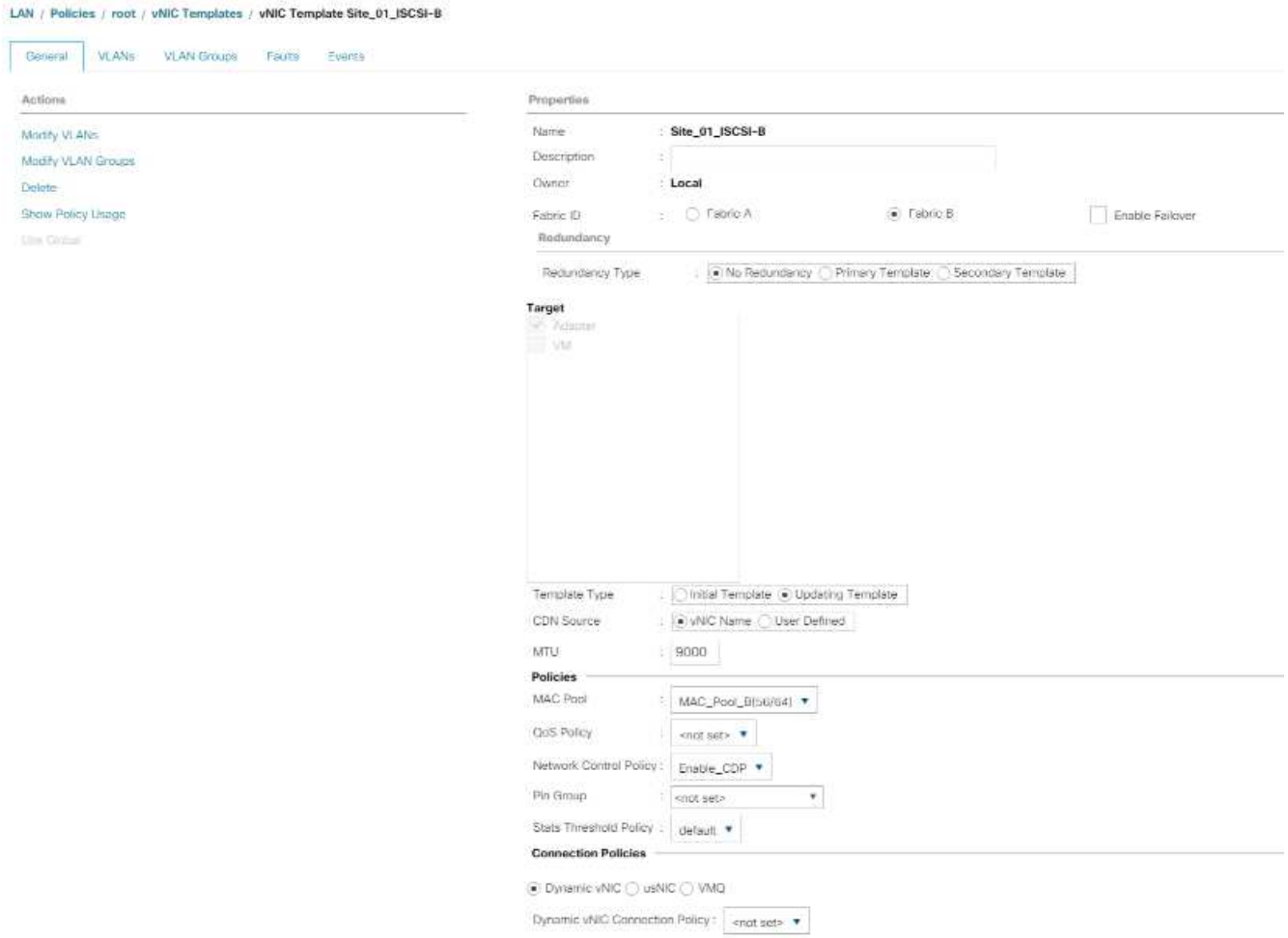
iSCSI vNIC を作成するには、次の手順を実行します。

1. 左側の [LAN] を選択します。
2. [ポリシー]>[ルート] を選択します。
3. [vNIC Templates] を右クリックします。
4. [Create vNIC Template] を選択します。
5. vNIC テンプレート名として「 'Site-01-iSCSI_A' 」を入力します。
6. [Fabric A] を選択します[Enable Failover] オプションは選択しないでください。
7. 冗長性タイプを冗長性なしに設定したままにします。
8. [ターゲット] で、 [アダプタ] オプションのみが選択されていることを確認します。
9. [テンプレートタイプ] で [テンプレートの更新] を選択します。
10. [VLANs] で、 [Site-01-iSCSI_A_VLAN] だけを選択します。
11. [Site-01-iSCSI_A_VLAN] をネイティブ VLAN として選択します。
12. CDN ソースに対して vNIC 名を設定したままにします。
13. MTU の下に 9000 と入力します。
14. MAC Pool リストから MAC-Pool-A を選択します
15. Network Control Policy リストから、 Enable-CDP-LLDP を選択します。
16. [OK] をクリックして、 vNIC テンプレートの作成を完了します。
17. [OK] をクリックします。



18. 左側の [LAN] を選択します。
19. [ポリシー]>[ルート] を選択します。
20. [vNIC Templates] を右クリックします。
21. [Create vNIC Template] を選択します。
22. vNIC テンプレート名として「 Site-01-iSCSI_B 」を入力します。
23. ファブリック B を選択します[Enable Failover] オプションは選択しないでください。
24. 冗長性タイプを冗長性なしに設定したままにします。
25. [ターゲット] で、 [アダプタ] オプションのみが選択されていることを確認します。
26. [テンプレートタイプ] で [テンプレートの更新] を選択します。
27. [VLANs] で、 [`s it-01-iscsi_B_VLAN] のみを選択します。
28. ネイティブ VLAN として [`s it-01-iSCSI_B_VLAN] を選択します。
29. CDN ソースに対して vNIC 名を設定したままにします。
30. MTU の下に 9000 と入力します。
31. [MAC Pool] リストから、 [`M AC-Pool-B] を選択します。
32. [ネットワーク制御ポリシー] リストから、 [有効 - CDP-LLDP-M] を選択します。
33. [OK] をクリックして、 vNIC テンプレートの作成を完了します。

34. [OK] をクリックします。



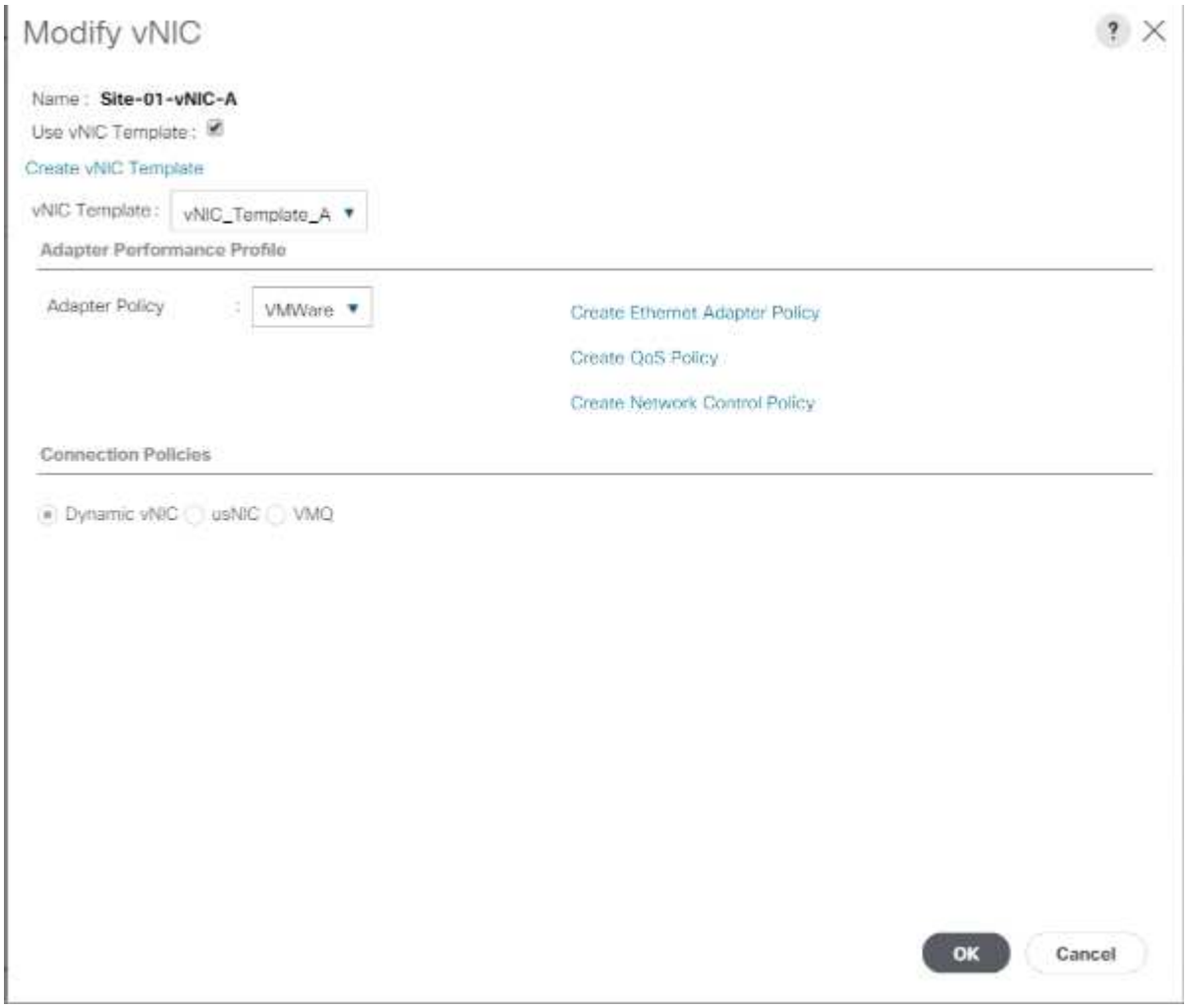
iSCSI ブート用の **LAN** 接続ポリシーを作成します

この手順環境は、 2 つの iSCSI LIF がクラスタノード 1 （「 iscsi_dlif01a 」および「 iscsi_dlif01b 」）にあり、 2 つの iSCSI LIF がクラスタノード 2 （「 iscsi_dlif02a 」および「 iscsi_dlif02b 」）にある Cisco UCS 環境です。また、 A LIF がファブリック A （ Cisco UCS 6324 A ）に接続され、 B LIF がファブリック B （ Cisco UCS 6324 B ）に接続されていると想定しています。

必要なインフラストラクチャ LAN 接続ポリシーを設定するには、次の手順を実行します。

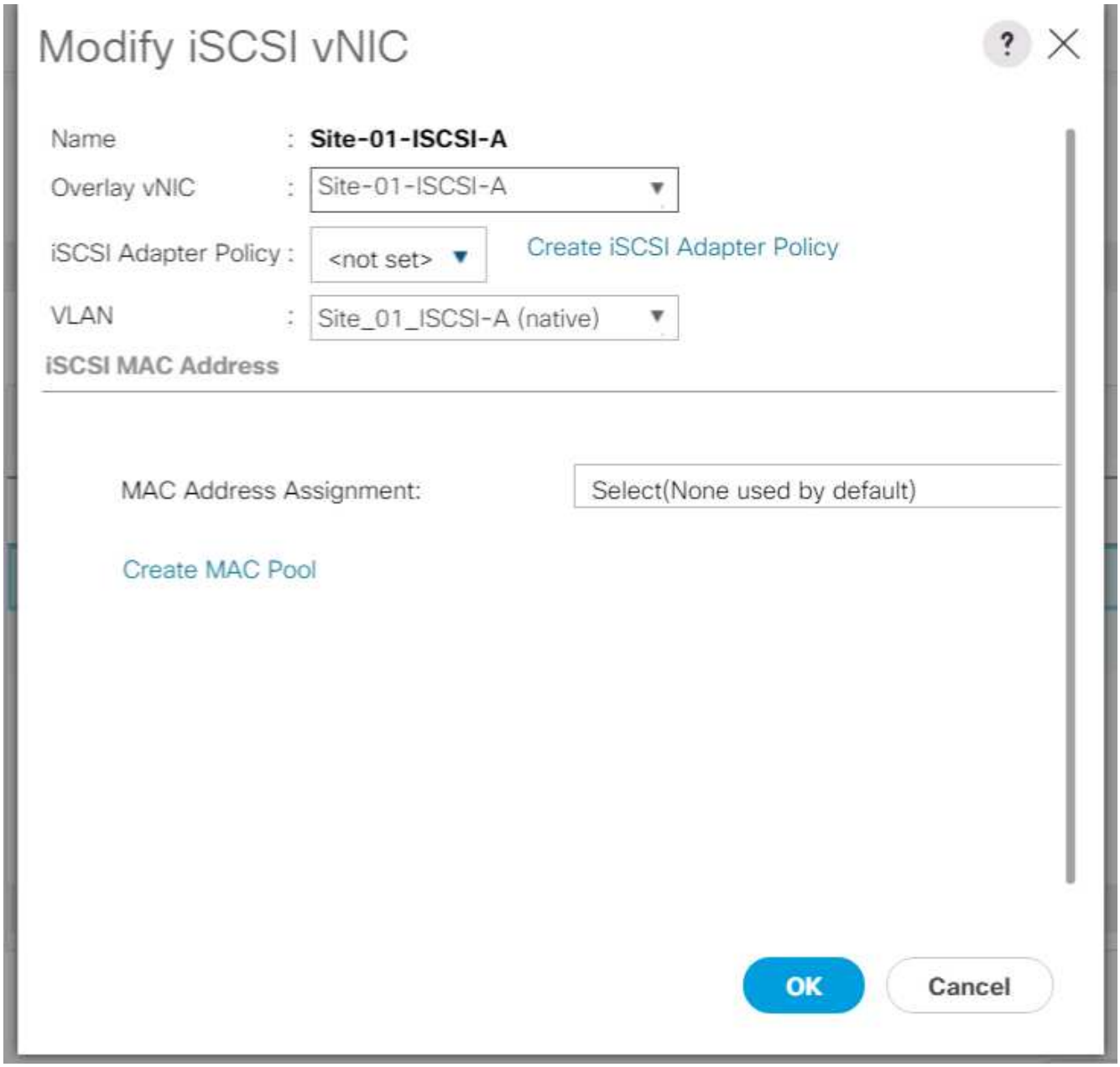
1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [LAN] > [Policies] > [root] を選択します。
3. [LAN 接続ポリシー] を右クリックします。
4. [Create LAN Connectivity Policy] を選択します。
5. ポリシー名として「 ite-XX-fFabric-a」 と入力します。
6. vNIC を追加するには、上部の Add オプションをクリックします。
7. [Create vNIC] ダイアログボックスで、 vNIC の名前として「 S`ite-01-vNIC-A` 」と入力します。

8. [Use vNIC Template] オプションを選択します。
9. [vNIC Template] リストで、 [vNIC_Template_A] を選択します。
10. [Adapter Policy] ドロップダウンリストから [VMware] を選択します。
11. [OK] をクリックして、この vNIC をポリシーに追加します。

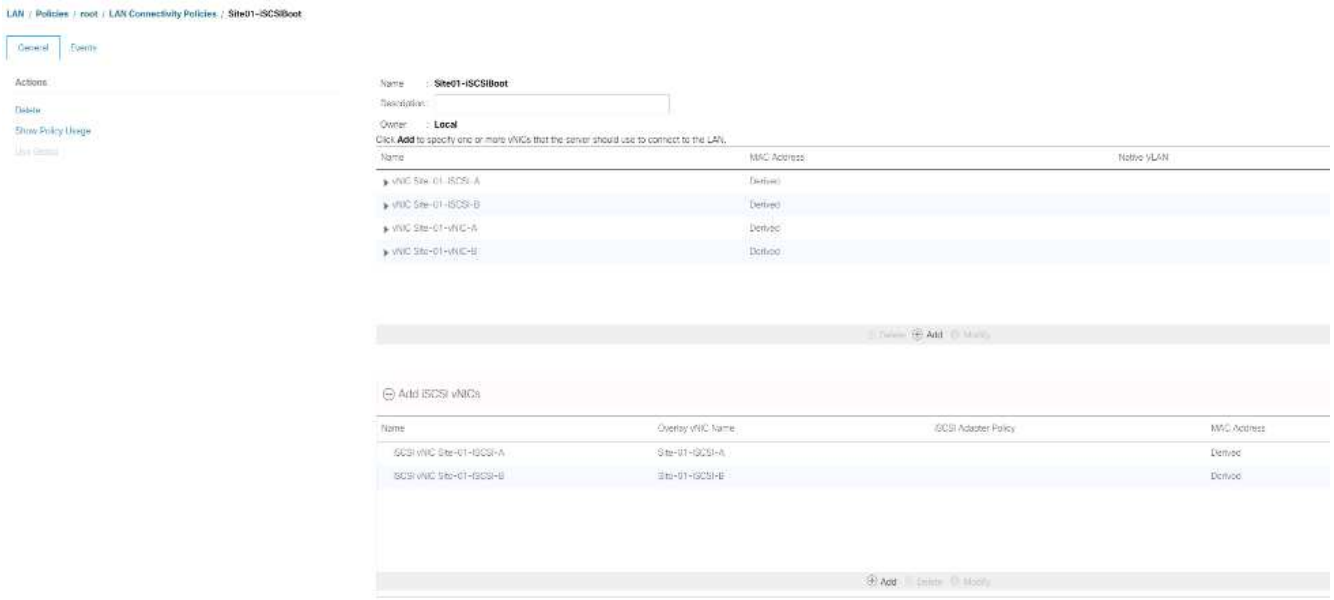


12. vNIC を追加するには、上部の Add オプションをクリックします。
13. [Create vNIC] ダイアログボックスで、 vNIC の名前として「 S`it-01-vNIC-B` 」と入力します。
14. [Use vNIC Template] オプションを選択します。
15. [vNIC Template] リストで、 [vNIC_Template_B] を選択します。
16. [Adapter Policy] ドロップダウンリストから [VMware] を選択します。
17. [OK] をクリックして、この vNIC をポリシーに追加します。
18. vNIC を追加するには、上部の Add オプションをクリックします。
19. [Create vNIC] ダイアログボックスで、 vNIC の名前として「 `sit-01-iscsi-A` 」と入力します。
20. [Use vNIC Template] オプションを選択します。
21. [vNIC Template] リストで、 [`site-01-iSCSI-A] を選択します。
22. [Adapter Policy] ドロップダウンリストから [VMware] を選択します。

23. [OK] をクリックして、この vNIC をポリシーに追加します。
24. vNIC を追加するには、上部の Add オプションをクリックします。
25. [Create vNIC] ダイアログボックスで、 vNIC の名前として「 S`ite-01-iSCSI-B` 」と入力します。
26. [Use vNIC Template] オプションを選択します。
27. [vNIC Template] リストで、 [`Site-01-iSCSI-B] を選択します。
28. [Adapter Policy] ドロップダウンリストから [VMware] を選択します。
29. [OK] をクリックして、この vNIC をポリシーに追加します。
30. Add iSCSI vNICs オプションを展開します。
31. [Add iSCSI vNICs] スペースの下側の [Add] オプションをクリックして、 iSCSI vNIC を追加します。
32. [Create iSCSI vNIC] ダイアログボックスで、 vNIC の名前として「 `Site-01-iSCSI-A 」を入力します。
33. [Overlay vNIC] を [`s ite -01-iSCSI-A] として選択します。
34. [iSCSI Adapter Policy] オプションは [Not Set] のままにします。
35. VLAN を「 ite-01-iSCSI-Site-A 」（ネイティブ）として選択します。
36. MAC アドレスの割り当てとして、 None （なし）（デフォルトで使用）を選択します。
37. [OK] をクリックして、 iSCSI vNIC をポリシーに追加します。



38. [Add iSCSI vNICs] スペースの下側の [Add] オプションをクリックして、 iSCSI vNIC を追加します。
39. [Create iSCSI vNIC] ダイアログボックスで、 vNIC の名前として「 `Site-01-iSCSI-B 」を入力します。
40. Overlay vNIC を Site-01-iSCSI-B として選択します
41. [iSCSI Adapter Policy] オプションは [Not Set] のままにします。
42. VLAN を「 ite-01-iSCSI-Site-B 」（ネイティブ）として選択します。
43. MAC アドレスの割り当てとして、 [なし] （デフォルトで使用）を選択します。
44. [OK] をクリックして、 iSCSI vNIC をポリシーに追加します。
45. [Save Changes] をクリックします。



VMware ESXi 6.7U1 インストールブート用の **vMedia** ポリシーを作成します

NetApp Data ONTAP のセットアップ手順では、 NetApp Data ONTAP と VMware ソフトウェアのホストに使用する HTTP Web サーバが必要です。ここで作成される vMedia ポリシーは、 VMware ESXi 6 をマッピングします。ESXi のインストールをブートするために Cisco UCS サーバに接続された 7U1 ISO 。このポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [Servers] を選択します。
2. [ポリシー]>[ルート] を選択します。
3. [vMedia Policies] を選択します。
4. [追加] をクリックして、新しい vMedia ポリシーを作成します。
5. ポリシーに「 esxi- 6.7U1-HTTP 」という名前を付けます。
6. 概要フィールドに ESXi 6.7U1 用のマウント ISO と入力します。
7. [マウント失敗時の再試行] で [はい] を選択します
8. 追加をクリックします。
9. マウントに esxi- 6.7U1-HTTP という名前を付けます。
10. CDD デバイスタイプを選択します。
11. HTTP プロトコルを選択します。
12. Web サーバの IP アドレスを入力します。

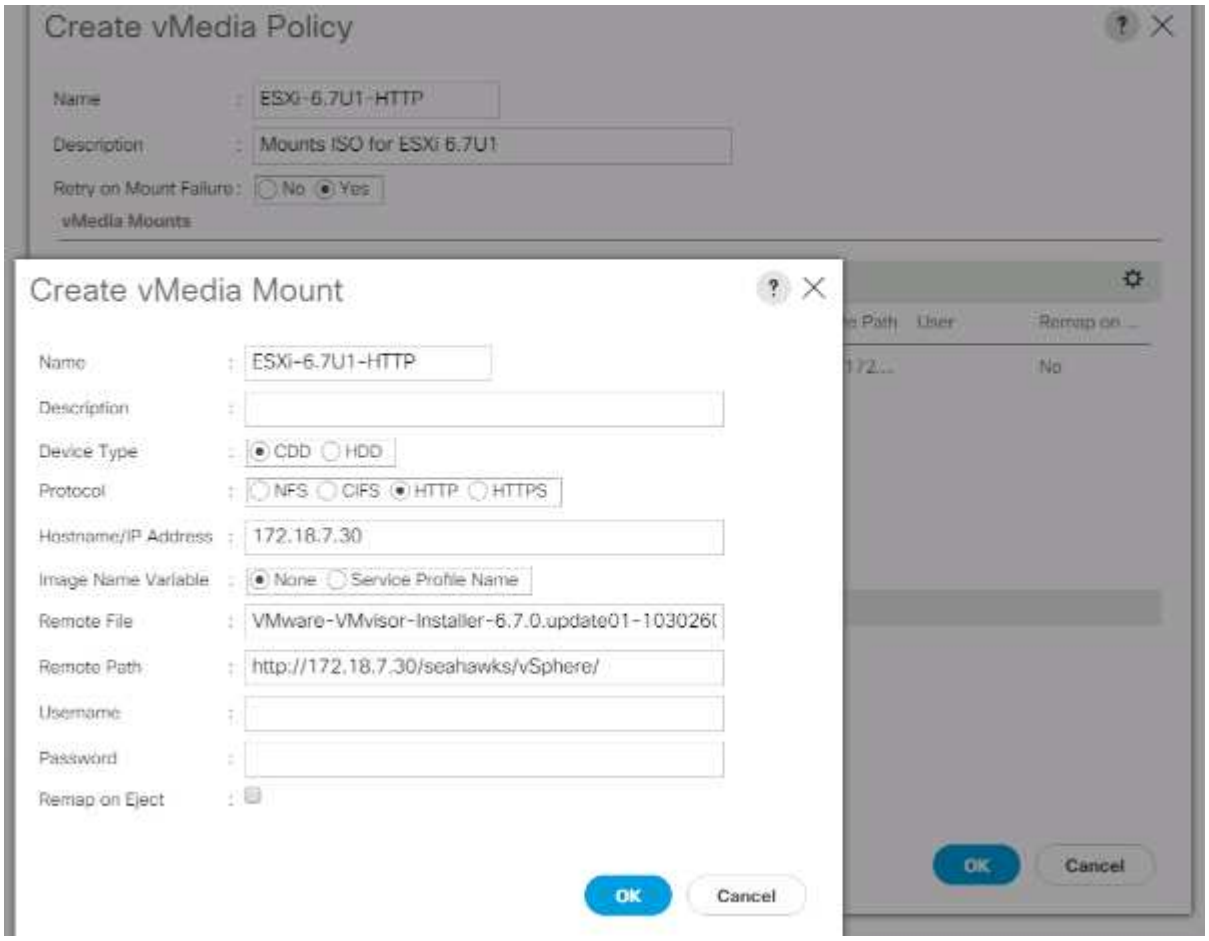
> DNS サーバの IP は KVM IP に入力されていなかったため、ホスト名ではなく Web サーバの IP を入力する必要があります。

13. リモートファイル名として「 VMware-VMvator-Installer-6.7.0.update01-10302608.x86_64 .iso 」と入力します。

    この VMware ESXi 6.7U1 ISO は、からダウンロードできます "VMware のダウンロード"。

14. [リモートパス] フィールドに ISO ファイルへの Web サーバパスを入力します。
15. [OK] をクリックして、 vMedia マウントを作成します。
16. [OK] をクリックし、もう一度 [OK] をクリックして、 vMedia ポリシーの作成を完了します。

    Cisco UCS 環境に追加された新しいサーバでは、 vMedia サービスプロファイルテンプレートを使用して ESXi ホストをインストールできます。SAN でマウントされたディスクが空の場合、初回ブート時に ESXi インストーラでホストがブートします。ESXi のインストール後、起動ディスクがアクセス可能である限り、 vMedia は参照されません。



iSCSI ブートポリシーを作成します

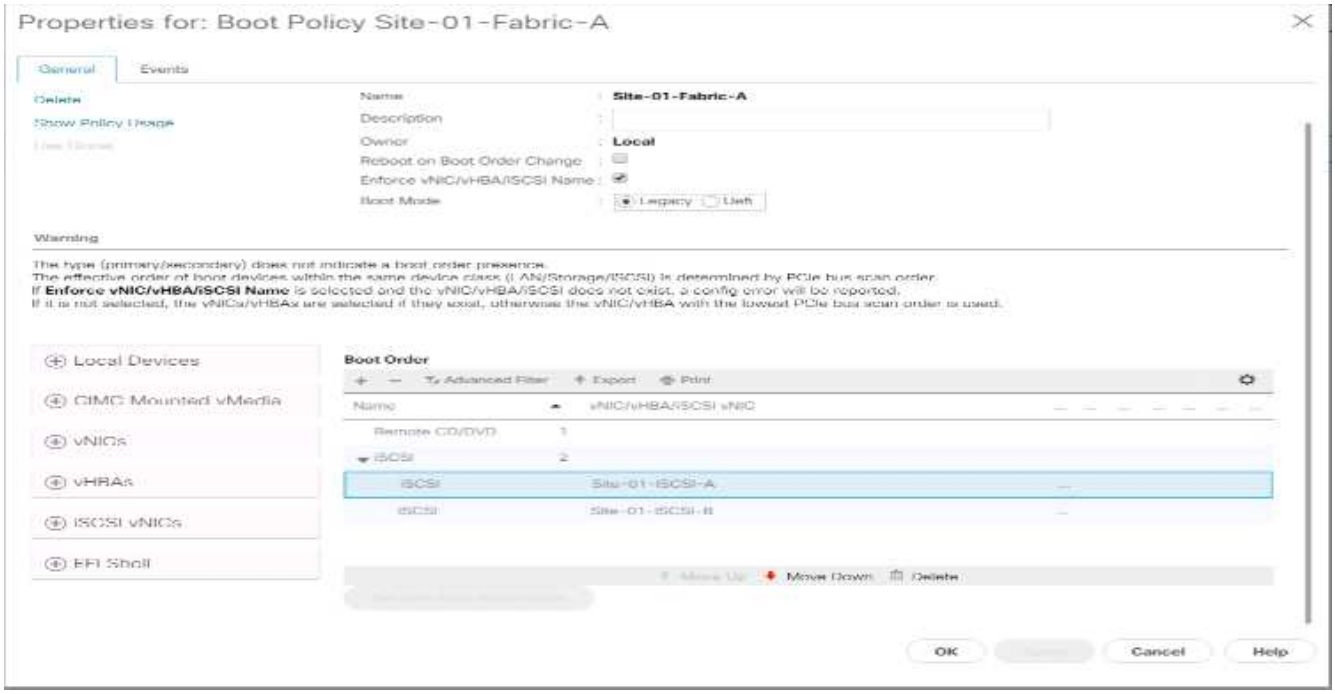
ここで説明する環境の手順は、 2 つの iSCSI 論理インターフェイス（ LIF ）がクラスタノード 1 （「 iscsi_dlif01a 」および「 iscsi_dlif01b 」）にあり、 2 つの iSCSI LIF がクラスタノード 2 （「 iscsi_dlif02a 」および「 iscsi_dlif02b 」）にある Cisco UCS 環境です。また、 A LIF がファブリック A （ Cisco UCS ファブリックインターコネクト A ）に接続され、 B LIF がファブリック B （ Cisco UCS ファブリックインターコネクト B ）に接続されていることも前提となります。

> この手順には、 1 つのブートポリシーが設定されています。このポリシーでは ' プライマリ・ターゲットを iSCSI lif01a に設定します

Cisco UCS 環境のブートポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。

2. [ポリシー]>[ルート] を選択します。
3. [Boot Policies] を右クリックします。
4. Create Boot Policy を選択します。
5. ブートポリシーの名前として「 'Site-01-Fabric-a' 」を入力します。
6. オプション：ブートポリシーの概要を入力します。
7. Boot Order Change オプションを選択解除したまま再起動します。
8. 起動モードはレガシーです。
9. [ローカルデバイス] ドロップダウンメニューを展開し、 [リモート CD/DVD の追加] を選択します。
10. [iSCSI vNICs] ドロップダウンメニューを展開し、 [Add iSCSI Boot] を選択します。
11. [Add iSCSI Boot] ダイアログボックスに「 'Site-01-iSCSI-A 」と入力します。[OK] をクリックします。
12. Add iSCSI Boot を選択します。
13. [Add iSCSI Boot] ダイアログボックスに「 'Site-01-iSCSI-B' 」と入力します。[OK] をクリックします。
14. [OK] をクリックして、ポリシーを作成します。



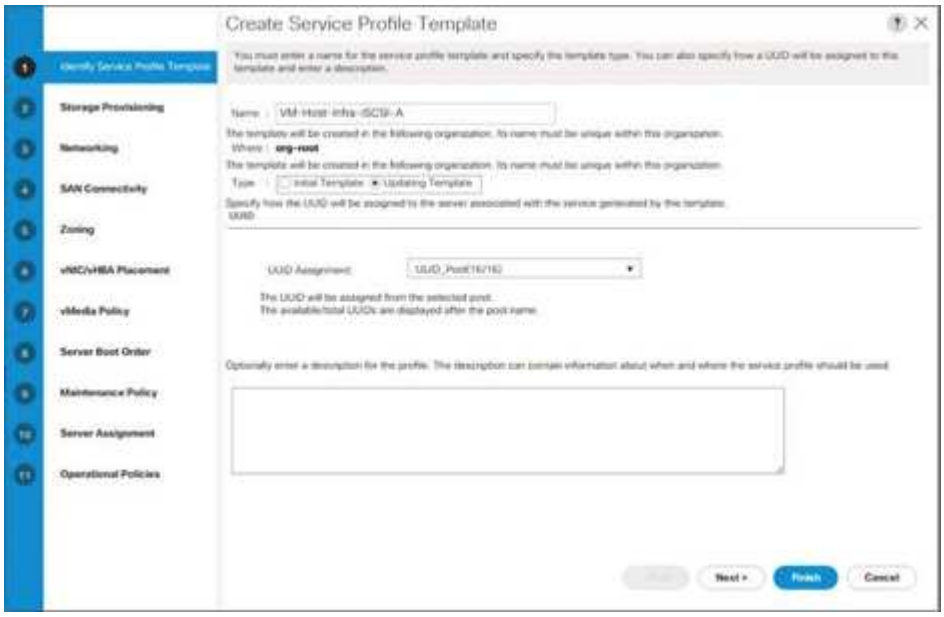
サービスプロファイルテンプレートを作成します

この手順では、ファブリック A ブート用にインフラ ESXi ホスト用のサービスプロファイルテンプレートが 1 つ作成されます。

サービスプロファイルテンプレートを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [サービスプロファイルテンプレート]>[ルート] を選択します。
3. ルートを右クリックします。

4. [サービスプロファイルテンプレートの作成] を選択して、 [サービスプロファイルテンプレートの作成] ウィザードを開きます。
5. サービス・プロファイル・テンプレートの名前として 'VM-Host-Infra-iSCSI-A を入力しますこのサービスプロファイルテンプレートは、ファブリック A のストレージノード 1 からブートするように設定されています
6. [テンプレートの更新] オプションを選択します。
7. [UUID] で、 [UUID_Pool] を UUID プールとして選択します。次へをクリックします。



ストレージプロビジョニングを設定する

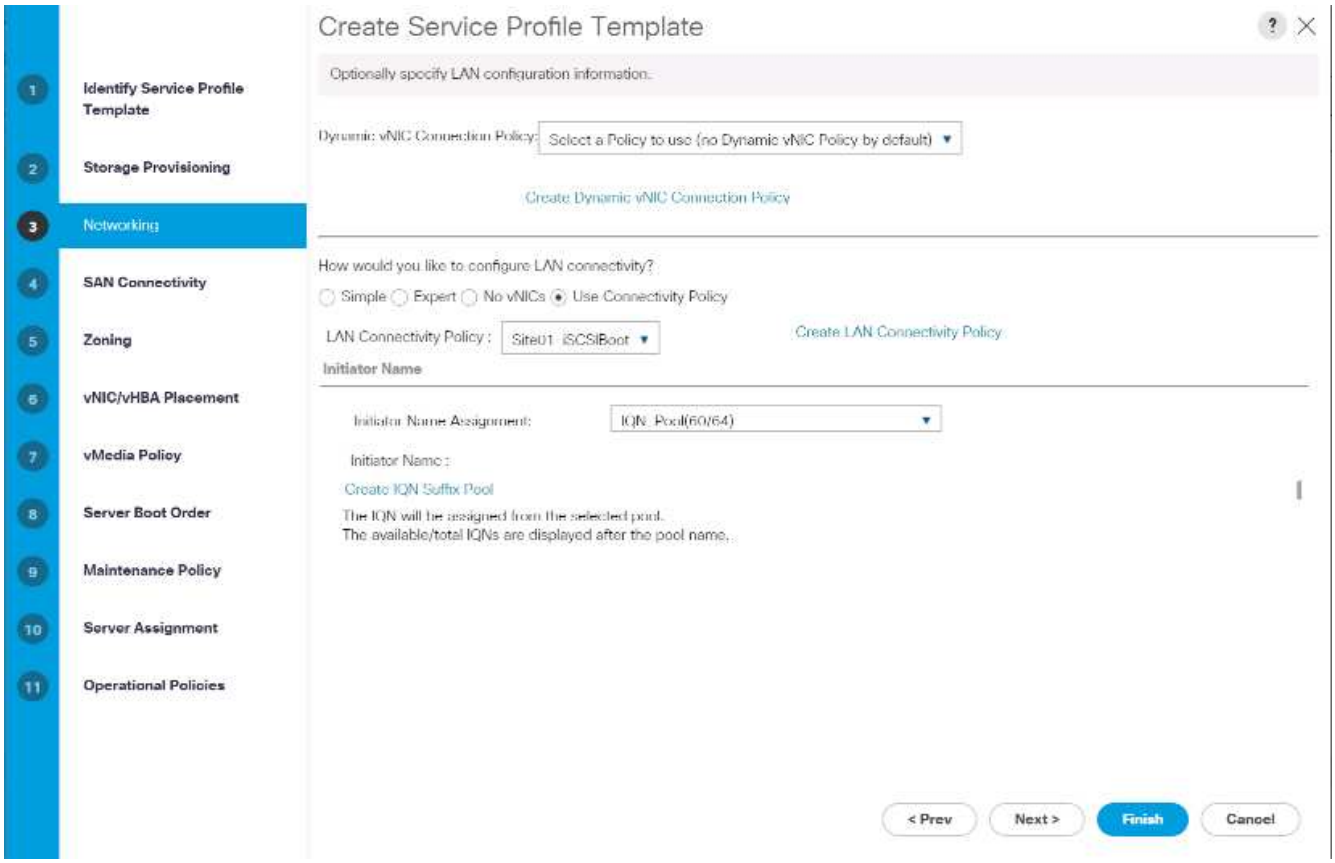
ストレージプロビジョニングを設定するには、次の手順を実行します。

1. 物理ディスクを持たないサーバーがある場合は、ローカルディスク設定ポリシーをクリックし、 SAN ブートローカルストレージポリシーを選択します。それ以外の場合は、デフォルトのローカルストレージポリシーを選択します。
2. 次へをクリックします。

ネットワークオプションを設定します

ネットワークオプションを設定するには、次の手順を実行します。

1. ダイナミック vNIC 接続ポリシーのデフォルト設定を保持します。
2. Use Connectivity Policy オプションを選択して、 LAN 接続を設定します。
3. [LAN Connectivity Policy] ドロップダウンメニューから [iSCSI-Boot] を選択します。
4. [イニシエータ名の割り当て] で [IQN_Pool] を選択します次へをクリックします。



SAN 接続を設定

SAN 接続を設定するには、次の手順を実行します。

1. vHBA の場合は、 SAN 接続を構成する方法を選択します。オプション
2. 次へをクリックします。

ゾーニングを設定します

ゾーニングを設定するには '[次へ] をクリックします

vNII/HBA の配置を設定します

vNII/HBA の配置を設定するには、次の手順を実行します。

1. 配置を選択 (Select Placement) ドロップダウンリストから ' 配置ポリシーをシステムが配置を実行できるようにします
2. 次へをクリックします。

vMedia ポリシーを設定します

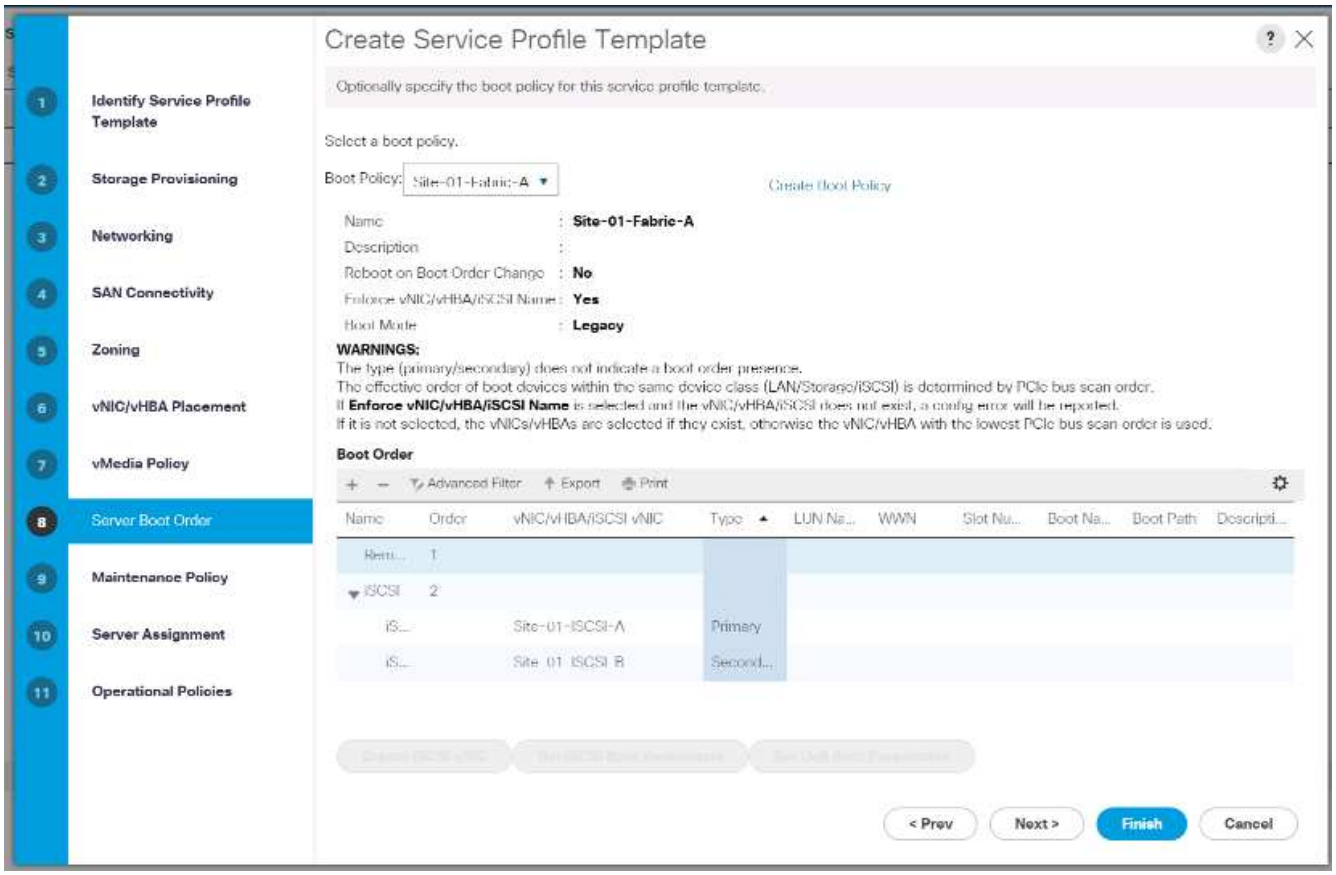
vMedia ポリシーを設定するには、次の手順を実行します。

1. vMedia ポリシーは選択しないでください。
2. 次へをクリックします。

サーバのブート順序を設定します

サーバのブート順序を設定するには、次の手順を実行します。

1. ブート・ポリシーに [Boot - Fabric-a] を選択します



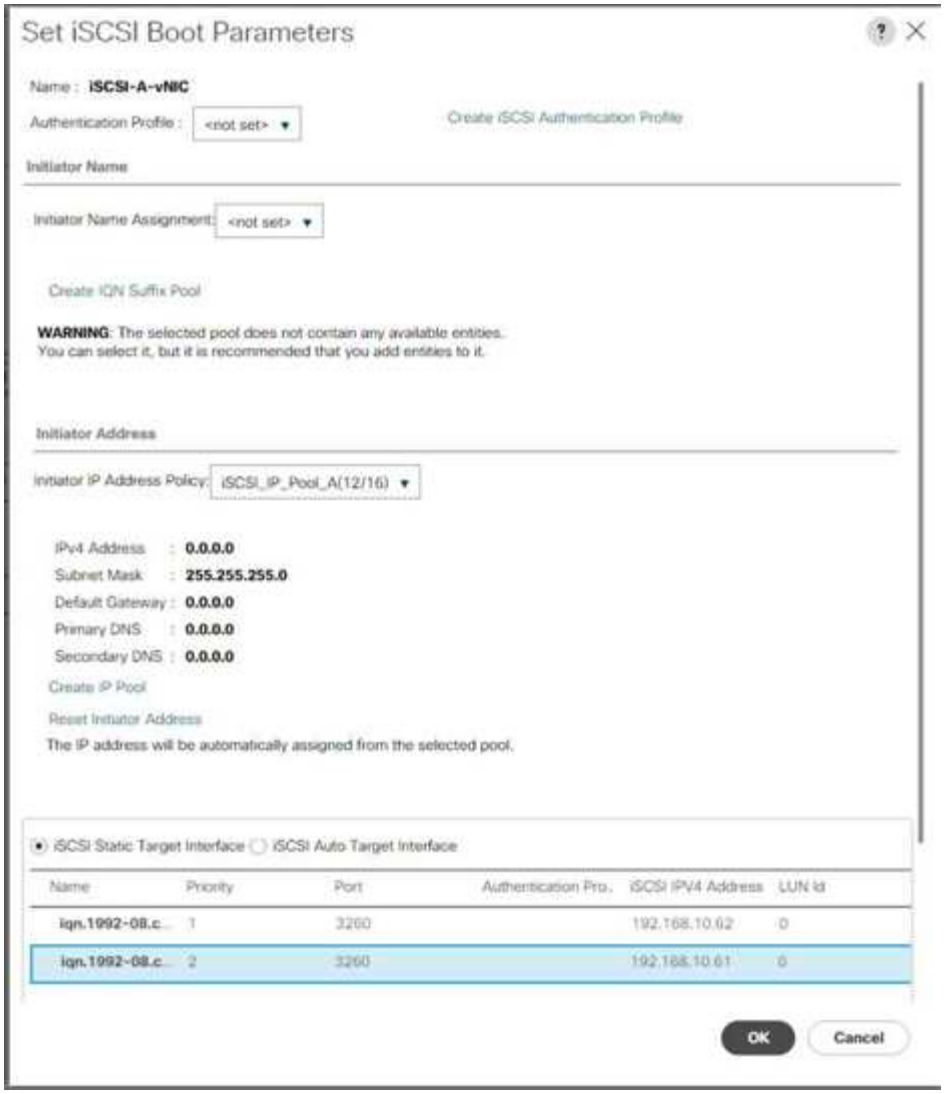
2. Boor 注文で、「ライト -01-iSCSI-A 」を選択します。
3. iSCSI 起動パラメータの設定をクリックします。
4. iSCSI ブートパラメータの設定ダイアログボックスで、環境に適した認証プロファイルを個別に作成していない限り、認証プロファイルオプションを Not Set のままにします。
5. [イニシエータ名の割り当て] ダイアログボックスは、前の手順で定義した単一のサービスプロファイルのイニシエータ名を使用するように設定されていないままにします。
6. 「 iSCSI_IP_Pool_A 」をイニシエータ IP アドレス・ポリシーとして設定します。
7. iSCSI Static Target Interface オプションを選択します。
8. 追加をクリックします。
9. iSCSI ターゲット名を入力します。Infra-SVM の iSCSI ターゲット名を取得するには ' ストレージ・クラスタ管理インタフェースにログインして 'iSCSI show コマンドを実行します

```
bb04-aff300::> iscsi show
          Target                          Target                          Status
Vserver   Name                            Alias                           Admin
--------- ------------------------------- ------------------------------- ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                       up
```

10. IPv4 Address フィールドに「 iSCSI_LIF_02a 」の IP アドレスを入力します。

11. OK をクリックして、 iSCSI 静的ターゲットを追加します。
12. 追加をクリックします。
13. iSCSI ターゲット名を入力します。
14. IPv4 Address フィールドに 'iSCSI_LIF_01a' の IP アドレスを入力します

15. OK をクリックして、 iSCSI 静的ターゲットを追加します。



ストレージノード 02 の IP を最初に、ストレージノード 01 の IP を 2 番目にして、ターゲット IP を入力しました。これは、ブート LUN がノード 01 にあることを前提としています。この手順で順序が使用されている場合、ホストはノード 01 へのパスを使用してブートします。

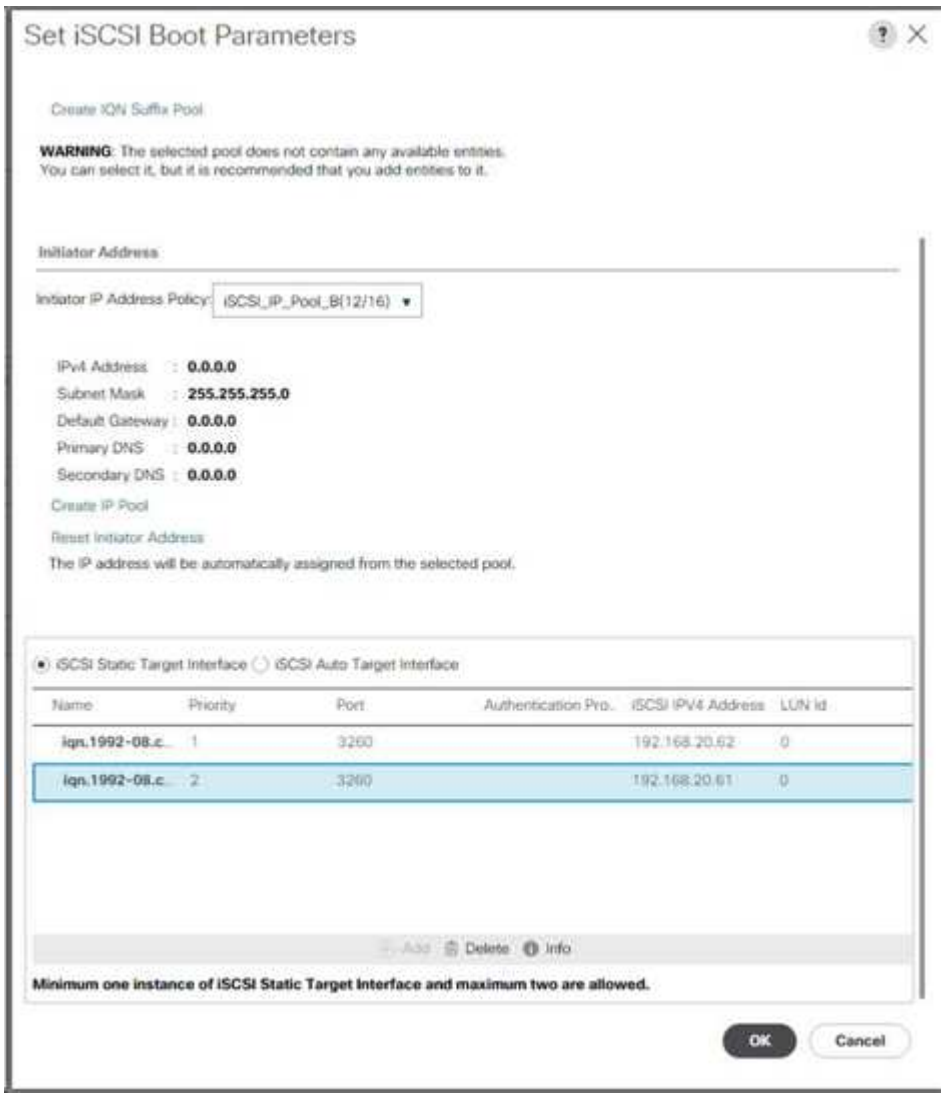
16. 起動順序で、 [iSCSI-B-vNIC] を選択します。
17. iSCSI 起動パラメータの設定をクリックします。
18. iSCSI ブートパラメータの設定ダイアログボックスで、環境に適した認証プロファイルを個別に作成していない限り、認証プロファイルオプションは Not Set のままにします。
19. [イニシエータ名の割り当て] ダイアログボックスは、前の手順で定義した単一のサービスプロファイルのイニシエータ名を使用するように設定されていないままにします。
20. イニシエータの IP アドレス・ポリシーとして 'iSCSI_IP_Pool_B' を設定します
21. iSCSI Static Target Interface オプションを選択します。
22. 追加をクリックします。
23. iSCSI ターゲット名を入力します。Infra-SVM の iSCSI ターゲット名を取得するには ' ストレージ・クラスタ管理インタフェースにログインして 'iSCSI show コマンドを実行します

```
bb04-aff300::> iscsi show
           Target                          Target                      Status
Vserver    Name                            Alias                       Admin
---------- ------------------------------- --------------------------- ------
Infra-SVM  iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                           Infra-SVM                   up
```

24. IPv4 Address フィールドに 'iSCSI_LIF_02b' の IP アドレスを入力します

25. OK をクリックして、 iSCSI 静的ターゲットを追加します。
26. 追加をクリックします。
27. iSCSI ターゲット名を入力します。
28. IPv4 Address フィールドに 'iSCSI_LIF_01b' の IP アドレスを入力します

29. OK をクリックして、 iSCSI 静的ターゲットを追加します。

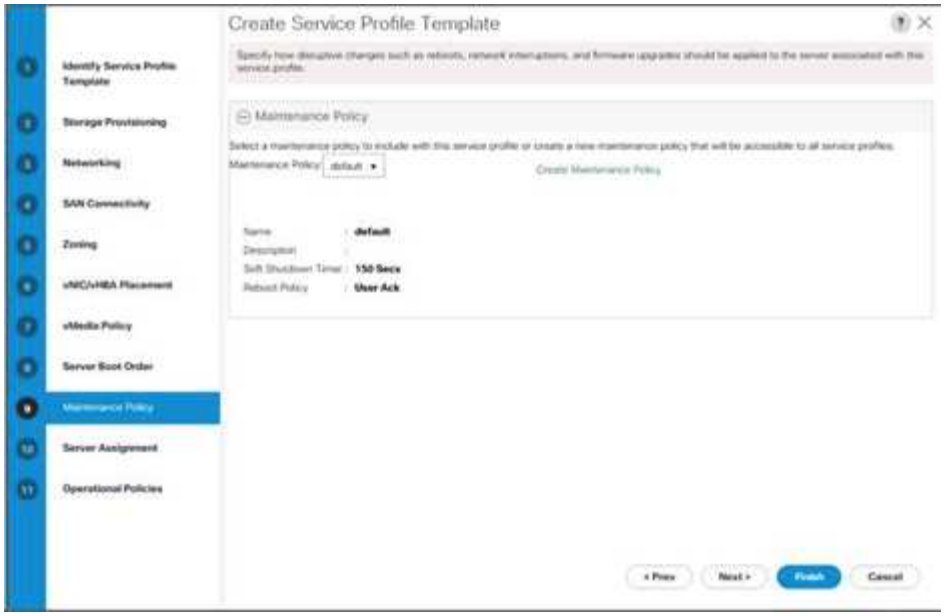


30. 次へをクリックします。

メンテナンスポリシーを設定する

メンテナンスポリシーを設定するには、次の手順を実行します。

1. メンテナンスポリシーをデフォルトに変更します。

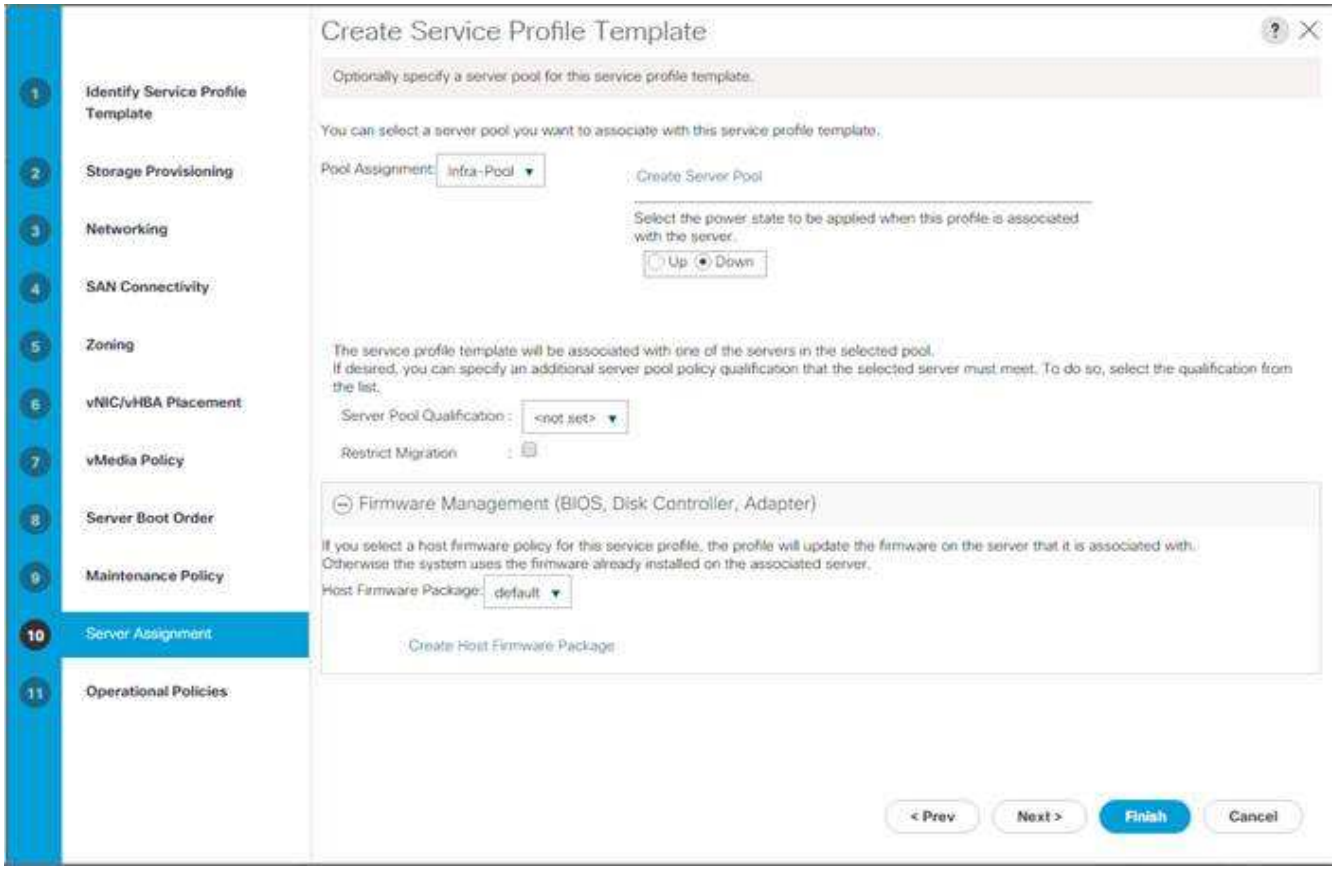


2. 次へをクリックします。

サーバの割り当てを設定します

サーバ割り当てを設定するには、次の手順を実行します。

1. ［プールの割り当て］ リストで ［インフラプール］ を選択します。
2. プロファイルがサーバーに関連付けられている場合に適用する電源状態として、 ［Down］ を選択します。
3. ページ下部のファームウェア管理を展開し、デフォルトポリシーを選択します。

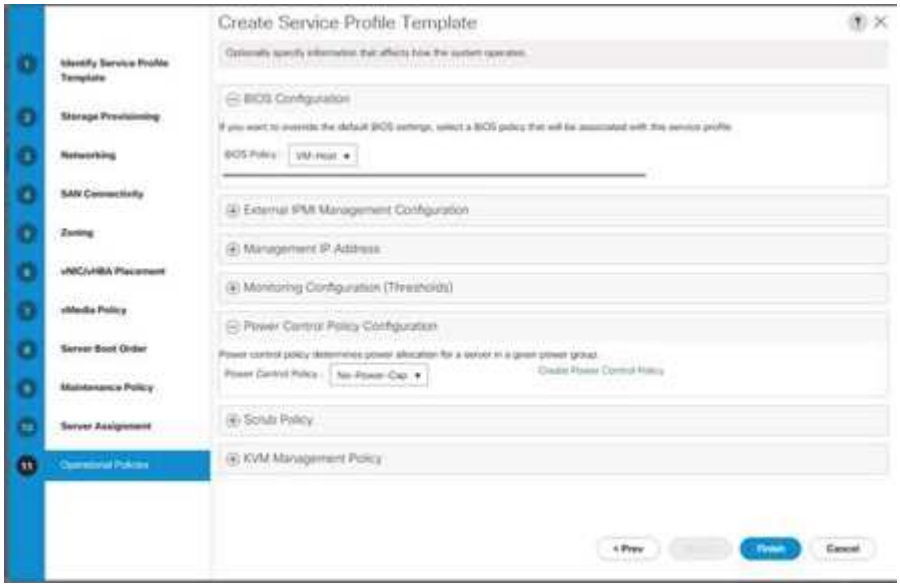


4. 次へをクリックします。

運用ポリシーを設定

運用ポリシーを設定するには、次の手順を実行します。

1. BIOS Policy ドロップダウンリストから VM-Host を選択します。
2. Power Control Policy Configuration （電源制御ポリシーの設定）を展開し、 Power Control Policy （電源制御ポリシー）ドロップダウンリストから No-Power-Cap （電源なし - 電力上限）を選択します。



3. [完了] をクリックして、サービスプロファイルテンプレートを作成します。
4. 確認メッセージで [OK] をクリックします。

vMedia 対応のサービスプロファイルテンプレートを作成します

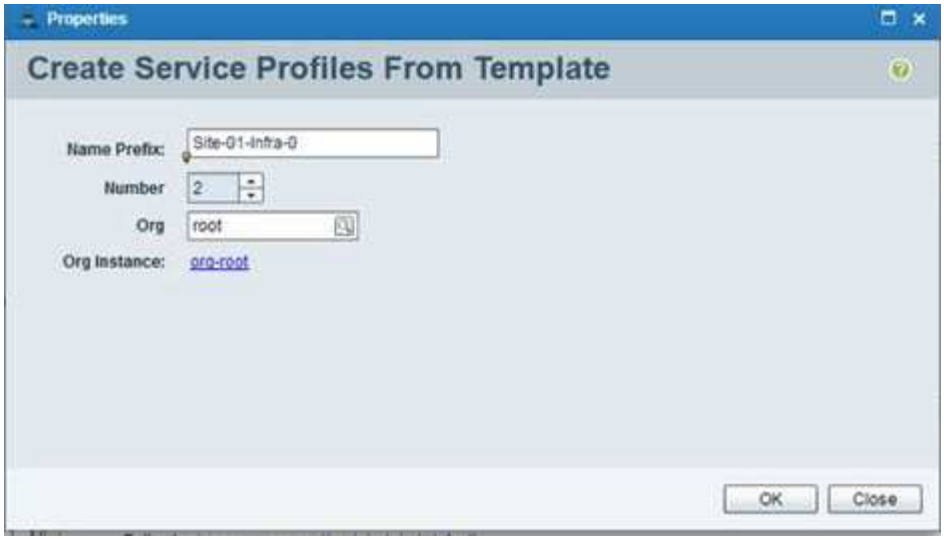
vMedia を有効にしてサービスプロファイルテンプレートを作成するには、次の手順を実行します。

1. UCS Manager に接続し、左側の [サーバ] をクリックします。
2. サービスプロファイルテンプレート > ルート > サービステンプレート VM-Host-Infra-iSCSI-A を選択します
3. [VM-Host-Infra-iSCSI-A] を右クリックし、 [クローンの作成] を選択します。
4. クローンに 'VM-Host-Infra-iSCSI-A-VM' という名前を付けます
5. 新しく作成した VM-Host-Infra-iSCSI-A-VM を選択し、右側の [vMedia Policy] タブを選択します。
6. Modify vMedia Policy をクリックします。
7. ESXi-6 を選択します。7U1 - HTTP vMedia Policy （ HTTP vMedia ポリシー）を選択し、 OK をクリックします。
8. [OK] をクリックして確定します。

サービスプロファイルを作成する

サービスプロファイルテンプレートからサービスプロファイルを作成するには、次の手順を実行します。

1. Cisco UCS Manager に接続し、左側の [サーバ] をクリックします。
2. ［ サーバー ］ > ［ サービスプロファイルテンプレート ］ > ［ ルート ］ > ［ サービステンプレート ］を展開します。
3. [アクション] で、 [テンプレートからサービスプロファイルを作成] をクリックし、次の手順を実行します。
   a. 命名プレフィックスとして「 `Site-01-Infra-0` 」を入力します。
   b. 作成するインスタンスの数として「 2 」を入力します。
   c. ルートを組織として選択します。
   d. [OK] をクリックして、サービスプロファイルを作成します。



4. 確認メッセージで [OK] をクリックします。
5. サービスプロファイル「 Site-01-Infra-01` 」および「 Site-01-Infra-02` 」が作成されていることを確認します。

> サービスプロファイルは、割り当てられたサーバプール内のサーバに自動的に関連付けられます。

ストレージ構成パート **2** ：ブート **LUN** とイニシエータグループ

ONTAP ブートストレージのセットアップ

igroup を作成します

イニシエータグループ（ igroup ）を作成するには、次の手順を実行します。

1. クラスタ管理ノードの SSH 接続から次のコマンドを実行します。

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-01 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-01-iqn>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-02 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-02-iqn>
igroup create -vserver Infra-SVM -igroup MGMT-Hosts -protocol iscsi
-ostype vmware -initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

> IQN 情報には、表 1 と表 2 の値を使用します。

2. 作成した 3 つの igroup を表示するには、「 igroup show 」コマンドを実行します。

ブート **LUN** を **igroup** にマッピングします

ブート LUN を igroup にマッピングするには、次の手順を実行します。

1. ストレージクラスタ管理 SSH 接続から、次のコマンドを実行します。

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- A
-igroup VM-Host-Infra-01 -lun-id 0lun map -vserver Infra-SVM -volume
esxi_boot -lun VM-Host-Infra- B -igroup VM-Host-Infra-02 -lun-id 0
```

VMware vSphere 6.7U1 導入手順

ここでは、 FlexPod Express 構成に VMware ESXi 6.7U1 をインストールする手順について説明します。手順が完了すると、ブートした 2 台の ESXi ホストがプロビジョニングされます。

VMware 環境に ESXi をインストールする方法はいくつかあります。これらの手順では、 Cisco UCS Manager に組み込まれている KVM コンソールと仮想メディア機能を使用して、リモートインストールメディアを個々のサーバにマッピングし、それらのブート LUN に接続する方法に焦点を当てています。

ESXi 6.7U1 用の Cisco カスタムイメージをダウンロードします

VMware ESXi カスタムイメージがダウンロードされていない場合は、次の手順を実行してダウンロードを完了します。

1. 次のリンクをクリックします。 VMware vSphere Hypervisor （ ESXi ） 6.7U1 。 ^
2. ユーザ ID とパスワードが必要です "VMware.com" このソフトウェアをダウンロードします。
3. 「 .iso 」ファイルをダウンロードします。

Cisco UCS Manager の略

Cisco UCS IP KVM を使用すると、管理者はリモートメディアを介して OS のインストールを開始できます。IP KVM を実行するには、 Cisco UCS 環境にログインする必要があります。

Cisco UCS 環境にログインするには、次の手順を実行します。

1. Web ブラウザを開き、 Cisco UCS クラスタアドレスの IP アドレスを入力します。このステップは、 Cisco UCS Manager アプリケーションを起動します。
2. HTML の下の [UCS Manager の起動] リンクをクリックして、 HTML 5 UCS Manager GUI を起動します。
3. セキュリティ証明書を承認するかどうかを尋ねられたら、必要に応じてを受け入れます。
4. プロンプトが表示されたら、ユーザ名として「 admin 」と入力し、管理パスワードを入力します。
5. Cisco UCS Manager にログインするには、 Login をクリックします。
6. メインメニューの左側にある [サーバー] をクリックします。
7. Servers > Service Profiles > root > 'VM-Host-Infra-01' を選択します
8. [VM-Host-Infra-01] を右クリックし '[KVM Console] を選択します
9. プロンプトに従って Java ベースの KVM コンソールを起動します。
10. Servers > Service Profiles > root > 'VM-Host-Infra-02' を選択します
11. [VM-Host-Infra-02] を右クリックします。KVM コンソールを選択します。

12. プロンプトに従って Java ベースの KVM コンソールを起動します。

VMware ESXi のインストールをセットアップする

ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

OS をインストールするサーバを準備するには、各 ESXi ホストで次の手順を実行します。

1. KVM ウィンドウで、仮想メディアをクリックします。
2. Activate Virtual Devices をクリックします。
3. 暗号化されていない KVM セッションを許可するかどうかを尋ねられたら、必要に応じて受け入れます。
4. [仮想メディア] をクリックし、 [CD/DVD のマップ] を選択します。
5. ESXi インストーラの ISO イメージファイルを参照し、開くをクリックします。
6. Map Device をクリックします。
7. KVM タブをクリックして ' サーバの起動を監視します
    - ESXi のインストール *

ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

VMware ESXi をホストの iSCSI ブート可能 LUN にインストールするには、各ホストで次の手順を実行します。

1. [Boot Server] を選択し、 [OK] をクリックして、サーバを起動します。次に、もう一度 [OK] をクリックします。
2. リブート時に、 ESXi インストールメディアがマシンで検出されます。表示されたブートメニューから ESXi インストーラを選択します。
3. インストーラのロードが完了したら、 Enter キーを押してインストールを続行します。
4. エンドユーザライセンス契約（ EULA ）を読んで同意します。F11 キーを押して確定し、続行します。
5. ESXi のインストールディスクとして設定していた LUN を選択し、 Enter キーを押してインストールを続行します。
6. 適切なキーボードレイアウトを選択し、 Enter キーを押します。
7. ルートパスワードを入力して確定し、 Enter キーを押します。
8. 選択したディスクが再パーティショニングされることを示す警告が表示されます。F11 キーを押してインストールを続行します。
9. インストールが完了したら、 [Virtual Media] タブを選択し、 ESXi インストールメディアの横にある P マークをクリアします。はいをクリックします。

    ESXi のインストールイメージのマッピングを解除して、サーバがインストーラではなく ESXi でリブートされるようにする必要があります。

10. インストールが完了したら、 Enter キーを押してサーバをリブートします。
11. Cisco UCS Manager では、現在のサービスプロファイルを vMedia 以外のサービスプロファイルテンプレートにバインドして、 ESXi インストール ISO over HTTP をマウントできないようにします。

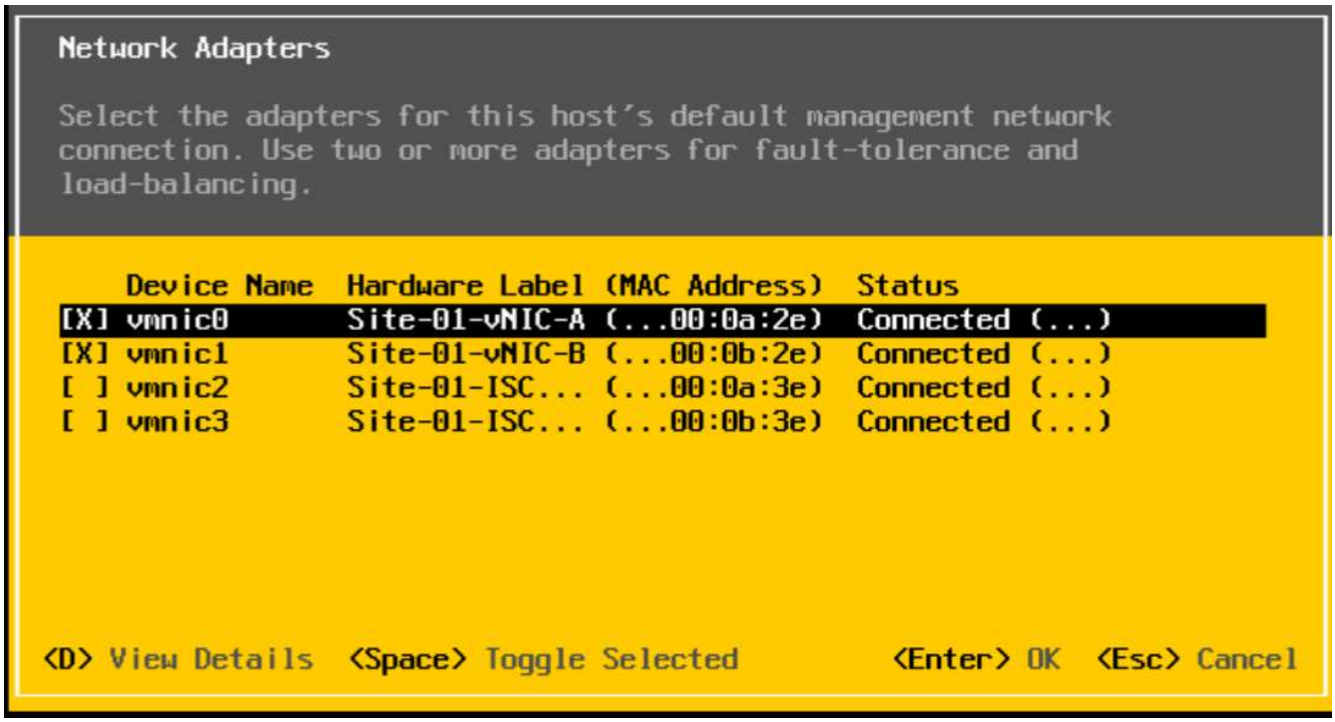
ESXi ホストの管理ネットワークをセットアップします

ホストの管理には、各 VMware ホストに管理ネットワークを追加する必要があります。VMware ホストの管理ネットワークを追加するには、各 ESXi ホストで次の手順を実行します。

ESXi ホスト VM-Host-Infra-01 と VM-Host-Infra-02

各 ESXi ホストから管理ネットワークにアクセスできるように設定するには、次の手順を実行します。

1. サーバーの再起動が完了したら、 F2 キーを押してシステムをカスタマイズします。
2. root としてログインし ' 対応するパスワードを入力し 'Enter キーを押してログインします
3. [トラブルシューティングオプション] を選択し、 Enter キーを押します。
4. [Enable ESXi Shell] を選択し、 Enter キーを押します。
5. SSH を有効にするを選択し、 Enter キーを押します。
6. Esc キーを押して、トラブルシューティングオプションメニューを終了します。
7. Configure Management Network （管理ネットワークの設定）オプションを選択し、 Enter キーを押します。
8. [ネットワークアダプタ] を選択し、 Enter キーを押します。
9. [ハードウェアラベル] フィールドの番号が [デバイス名] フィールドの番号と一致していることを確認します。
10. Enter キーを押します。



11. VLAN （オプション）オプションを選択し、 Enter キーを押します。
12. 「 <ib-mgmt-vlan-id> 」を入力し、 Enter キーを押します。
13. IPv4 Configuration （ IPv4 設定）を選択し、 Enter を押します。

14. スペースバーを使用して、静的 IPv4 アドレスとネットワーク設定を設定オプションを選択します。
15. 最初の ESXi ホストを管理するための IP アドレスを入力します。
16. 最初の ESXi ホストのサブネットマスクを入力します。
17. 最初の ESXi ホストのデフォルトゲートウェイを入力します。
18. Enter キーを押して、 IP 設定の変更を確定します。
19. DNS Configuration オプションを選択し、 Enter キーを押します。

> IP アドレスは手動で割り当てられるため、 DNS 情報も手動で入力する必要があります。

20. プライマリ DNS サーバの IP アドレスを入力します。
21. オプション：セカンダリ DNS サーバの IP アドレスを入力します。
22. 最初の ESXi ホストの FQDN を入力します。
23. Enter キーを押して、 DNS 設定の変更を確定します。
24. Esc キーを押して、 Configure Management Network （管理ネットワークの設定）メニューを終了します。
25. 管理ネットワークのテストを選択して管理ネットワークが正しく設定されていることを確認し、 Enter キーを押します。
26. Enter キーを押してテストを実行し、テストが完了したら Enter キーを再度押し、失敗した場合は環境を確認します。
27. Configure Management Network （管理ネットワークの設定）をもう一度選択し、 Enter キーを押します。
28. IPv6 設定オプションを選択し、 Enter キーを押します。
29. スペースバーを使用して、 [Disable IPv6 (restart required)] を選択し、 Enter キーを押します。
30. Esc キーを押して、 Configure Management Network サブメニューを終了します。
31. Y キーを押して変更を確認し、 ESXi ホストをリブートします。

VMware ESXi ホストの **VMkernel** ポート **vmk0 MAC** アドレスのリセット（オプション）

ESXi ホスト VM-Host-Infra-01 と VM-Host-Infra-02

デフォルトでは、管理 VMkernel ポート vmk0 の MAC アドレスは、配置されているイーサネットポートの MAC アドレスと同じです。ESXi ホストのブート LUN が異なる MAC アドレスを持つ別のサーバに再マッピングされた場合、 vmk0 では ESXi システム設定がリセットされないかぎり、割り当てられた MAC アドレスが保持されるため、 MAC アドレスの競合が発生します。vmk0 の MAC アドレスを、 VMware が割り当てたランダムな MAC アドレスにリセットするには、次の手順を実行します。

1. ESXi コンソールメニューのメイン画面で、 Ctrl+Alt+F1 キーを押して VMware コンソールのコマンドラインインターフェイスにアクセスします。UCSM KVM では、静的マクロのリストに Ctrl-Alt-F1 が表示されます。
2. root としてログインします。
3. 「 esxcfg-vmknic – l 」と入力して、インタフェース vmk0 の詳細な一覧を表示します。vmk0 は、管理ネットワークのポートグループの一部にする必要があります。vmk0 の IP アドレスおよびネットマスクに注意してください。

4. vmk0 を削除するには、次のコマンドを入力します。

```
esxcfg-vmknic –d “Management Network”
```

5. ランダム MAC アドレスを使用して vmk0 を再び追加するには、次のコマンドを入力します。

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. vmk0 がランダム MAC アドレスで再び追加されていることを確認します

```
esxcfg-vmknic –l
```

7. コマンド・ライン・インターフェイスからログアウトするには、「 exit 」と入力します。
8. ESXi コンソールメニューインターフェイスに戻るには、 Ctrl+Alt+F2 を押します。

VMware ホストクライアントを使用して **VMware ESXi** ホストにログインします

ESXi ホスト VM-Host-Infra-01

VMware Host Client を使用して VM-Host-Infra-01 ESXi ホストにログインするには、次の手順を実行します。

1. 管理ワークステーションで Web ブラウザを開き 'VM-Host-Infra-01' 管理 IP アドレスに移動します
2. ［ VMware ホストクライアントを開く ］ をクリックします。
3. ユーザ名に「 root 」と入力します。
4. root パスワードを入力します。
5. ログインをクリックして接続します。
6. この手順を繰り返して 'VM-Host-Infra-02' に別のブラウザタブまたはウィンドウでログインします

Cisco Virtual Interface Card （ VIC; 仮想インターフェイスカード）用の **VMware** ドライバのインストール

次の VMware VIC ドライバのオフラインバンドルをダウンロードして、管理ワークステーションに展開します。

- nenic ドライババージョン 1.0.25.0

ESXi は **VM-Host-Infra-01** と **VM-Host-Infra-02** をホストします

ESXi ホスト VM-Host-Infra-01 および VM-Host-Infra-02 に VMware VIC ドライバをインストールするには、次の手順を実行します。

1. 各ホストクライアントで、 Storage （ストレージ）を選択します。
2. datastore1 を右クリックし、 Browse を選択します。
3. データストアブラウザで、 [アップロード] をクリックします。

4. ダウンロードした VIC ドライバの保存先に移動し、 VMW-ESX-6.7.0-nenic-1.0.25.0 -offline_bundle -11271332.zip を選択します。
5. データストアブラウザで、 [アップロード] をクリックします。
6. [開く] をクリックして、このファイルを datastore1 にアップロードします。
7. 両方の ESXi ホストにファイルがアップロードされていることを確認してください。
8. 各ホストがメンテナンスモードになっていない場合は、メンテナンスモードにします。
9. 各 ESXi ホストへは、シェル接続または putty 端末から ssh を使用して接続します。
10. root パスワードを使用して root としてログインします。
11. 各ホストで次のコマンドを実行します。

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. 再起動が完了したら各ホストでホストクライアントにログインし、メンテナンスモードを終了します。

VMkernel ポートおよび仮想スイッチを設定します

ESXi ホスト VM-Host-Infra-01 と VM-Host-Infra-02

ESXi ホスト上の VMkernel ポートおよび仮想スイッチを設定するには、次の手順を実行します。

1. ホストクライアントで、左側の [ネットワーク] を選択します。
2. 中央のペインで、 [Virtual switches] タブを選択します。
3. vSwitch0 を選択します。
4. [設定の編集] を選択します
5. MTU を 9000 に変更します。
6. NIC チーミングを展開します。
7. フェイルオーバー順序（ Failover order ）セクションで、 vmnic1 を選択し、アクティブとしてマーク（ Mark active ）をクリックします。
8. vmnic1 のステータスがアクティブになっていることを確認します。
9. [保存] をクリックします .
10. 左側の [ネットワーク] を選択します。
11. 中央のペインで、 [Virtual switches] タブを選択します。
12. iScsiBootvSwitch を選択します。
13. [設定の編集] を選択します
14. MTU を 9000 に変更します
15. [保存] をクリックします .
16. [VMkernel NICs] タブを選択します。

17. 「 vmk1 iScsiBootPG 」を選択します。
18. [設定の編集] を選択します
19. MTU を 9000 に変更します。
20. IPv4 設定を展開し、 IP アドレスを UCS iSCSI-IP-Pool-A の外部のアドレスに変更します

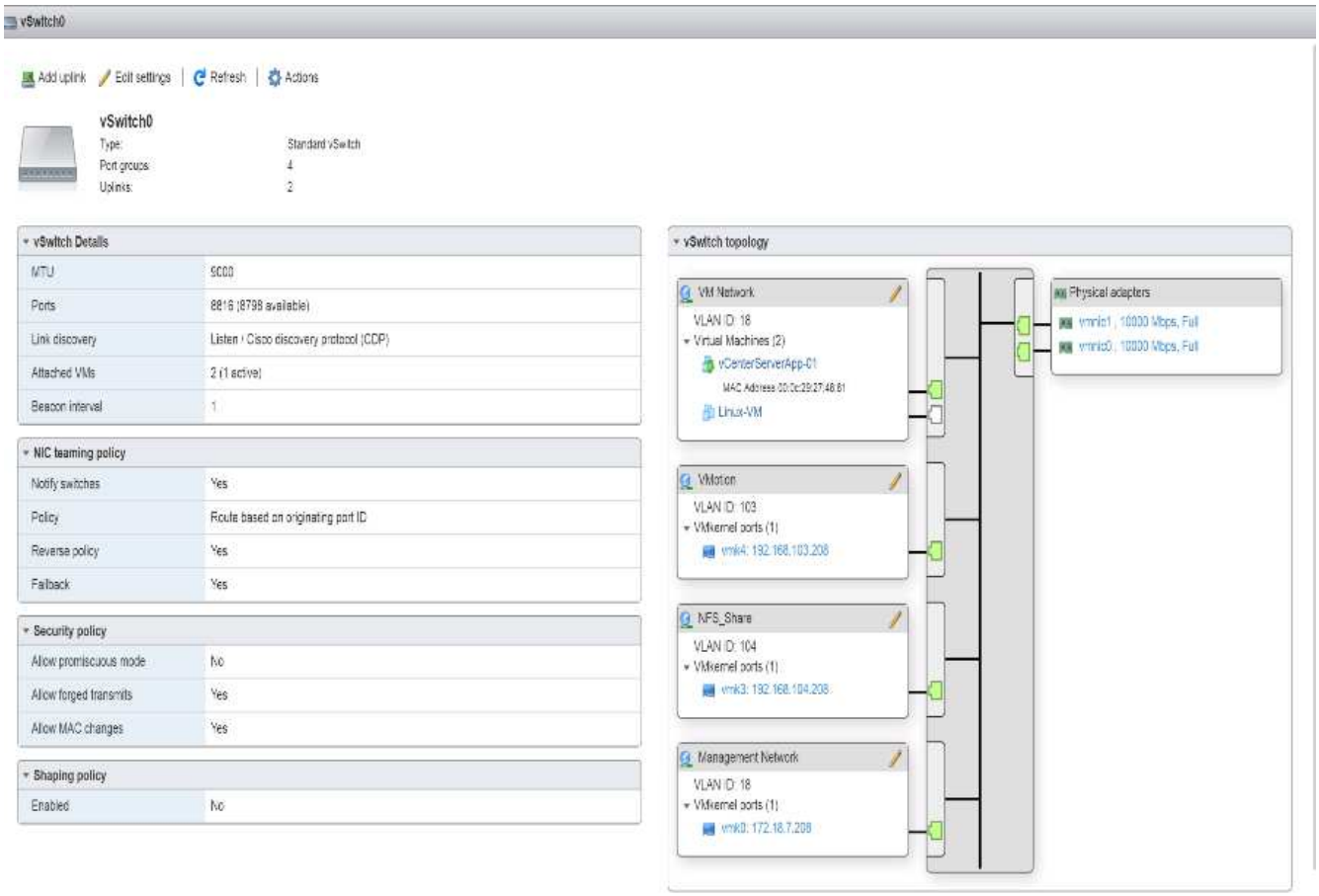
> Cisco UCS iSCSI IP プールアドレスを再割り当てする必要がある場合に IP アドレスの競合を回避するには、 iSCSI VMkernel ポートに対して同じサブネット内の異なる IP アドレスを使用することを推奨します。

21. [保存] をクリックします .
22. [Virtual switches] タブを選択します。
23. Add standard virtual switch を選択します。
24. vSwitch 名には「 iScsciBootvSwitch -B 」という名前を付けます。
25. MTU を 9000 に設定します。
26. [Uplink 1] ドロップダウンメニューから [vmnic3] を選択します。
27. 追加をクリックします。
28. 中央のペインで、 [VMkernel NICs] タブを選択します。
29. Add VMkernel NIC を選択します
30. 新しいポートグループ名として、 iScsiBootPG-B を指定します
31. 仮想スイッチに [iSciBootvSwitch -B] を選択します。
32. MTU を 9000 に設定します。VLAN ID は入力しないでください。
33. IPv4 設定では Static を選択し、 Configuration 内で Address と Subnet Mask を指定するオプションを展開します。

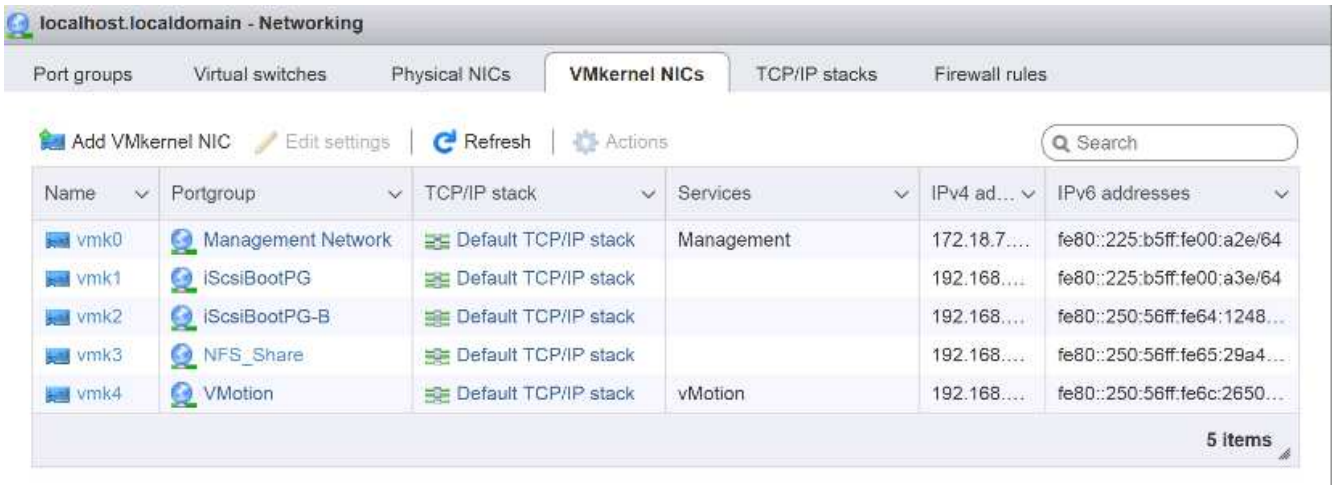
> IP アドレスの競合を避けるため、 Cisco UCS iSCSI IP プールアドレスを再割り当てする必要がある場合は、 iSCSI VMkernel ポートに対して同じサブネット内の異なる IP アドレスを使用することを推奨します。

34. Create をクリックします。 .
35. 左側で、 [ネットワーク] を選択し、 [ポートグループ] タブを選択します。
36. 中央のペインで、 [VM Network] を右クリックし、 [削除] を選択します。
37. Remove をクリックして、ポートグループの削除を完了します。
38. 中央のペインで、 Add port group （ポートグループの追加）を選択します。
39. ポートグループに「 Management Network 」という名前を付け、 VLAN ID フィールドに「 <ib-mgmt-vlan-id> 」と入力して、仮想スイッチ vSwitch0 が選択されていることを確認します。
40. [Add] をクリックして、 IB-MGMT ネットワークの編集を終了します。
41. 上部で、 [VMkernel NICs] タブを選択します。
42. Add VMkernel NIC をクリックします。
43. 新規ポートグループの場合は、 VMotion と入力します。

44. 仮想スイッチの場合は、 vSwitch0 を選択します。
45. VLAN ID に「 <VMotion-vlan-id> 」と入力します。
46. MTU を 9000 に変更します。
47. 静的 IPv4 設定を選択し、 IPv4 設定を展開します。
48. ESXi ホストの vMotion IP アドレスとネットマスクを入力します。
49. vMotion スタック TCP/IP スタックを選択します。
50. Services （サービス）で vMotion （ vMotion ）を選択
51. Create をクリックします。 .
52. Add VMkernel NIC をクリックします。
53. 新しいポートグループの場合は、 nfs_Share と入力します。
54. 仮想スイッチの場合は、 vSwitch0 を選択します。
55. VLAN ID に「 <infra-nfs-vlan-id> 」と入力します
56. MTU を 9000 に変更します。
57. 静的 IPv4 設定を選択し、 IPv4 設定を展開します。
58. ESXi ホストインフラの NFS IP アドレスとネットマスクを入力します。
59. サービスは選択しないでください。
60. Create をクリックします。 .
61. 仮想スイッチタブを選択して、 vSwitch0 を選択します。vSwitch0 VMkernel NIC のプロパティは、次の例のように設定します。



62. [VMkernel NICs] タブを選択して、設定済みの仮想アダプタを確認します。次の例のようなアダプタが表示されます。



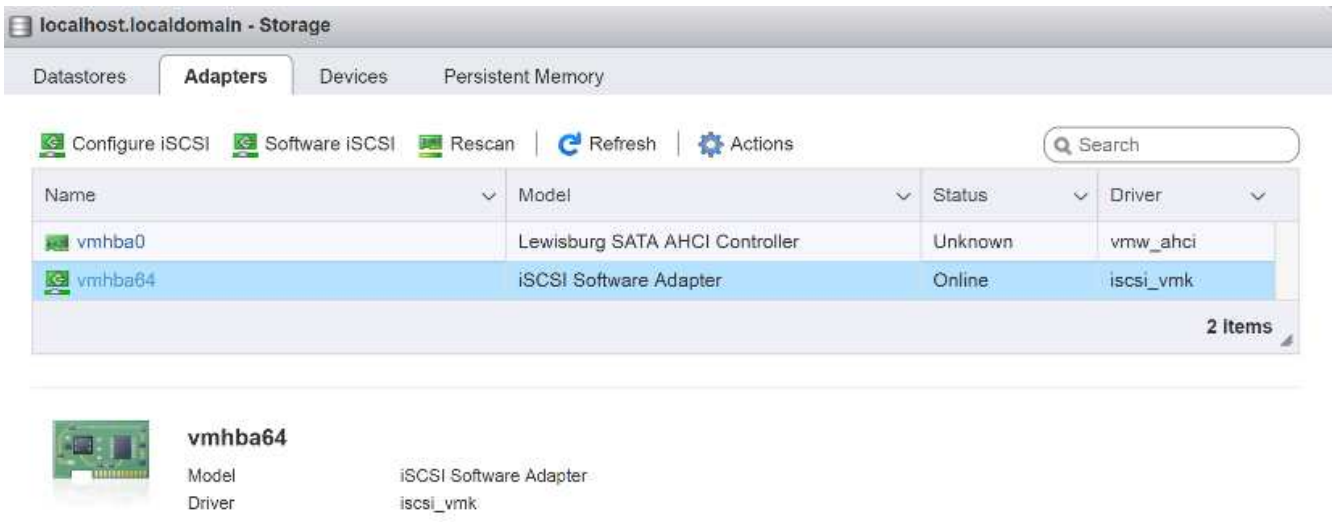
iSCSI マルチパスをセットアップします

ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

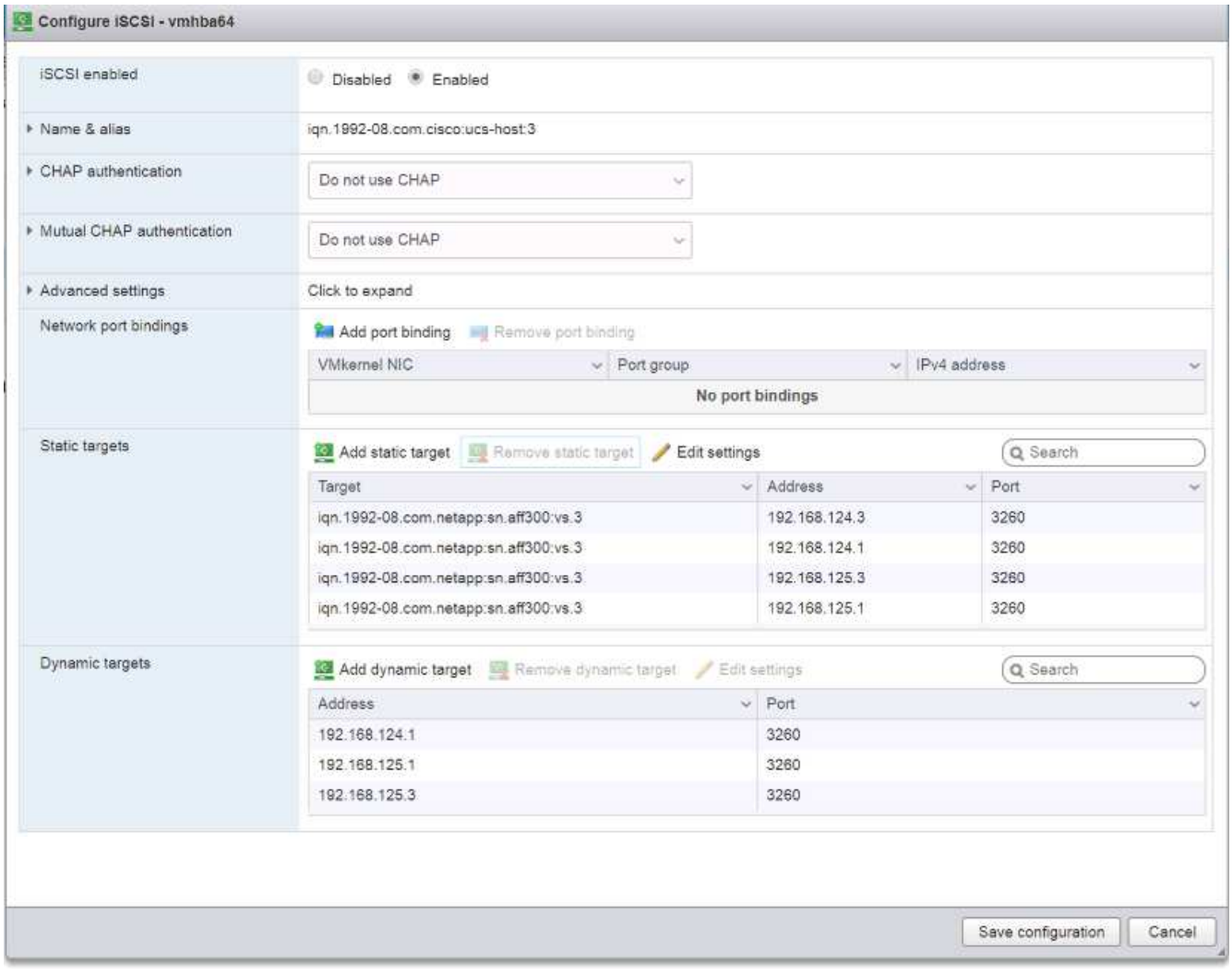
ESXi ホスト VM-Host-Infra-01 および VM-Host-Infra-02 で iSCSI マルチパスを設定するには、次の手順を実行します。

1. 各ホストクライアントで、左側の [ストレージ] を選択します。

2. 中央のペインで、 [アダプタ] をクリックします。
3. iSCSI ソフトウェアアダプタを選択し、 Configure iSCSI （ iSCSI の設定）をクリックします。



4. [動的ターゲット] で、 [動的ターゲットの追加] をクリックします。
5. IP アドレスに「 iscsi_dlif01a 」と入力します。
6. これらの IP アドレスの入力を繰り返します： 'iSCSI_lif01b’iSCSI_lif02a’iSCSI_lif02b'
7. [Save Configuration] をクリックします。



「 iscsi_lif 」の IP アドレスをすべて取得するには、 NetApp ストレージ・クラスタ管理インターフェイスにログインし、「 network interface show 」コマンドを実行します。

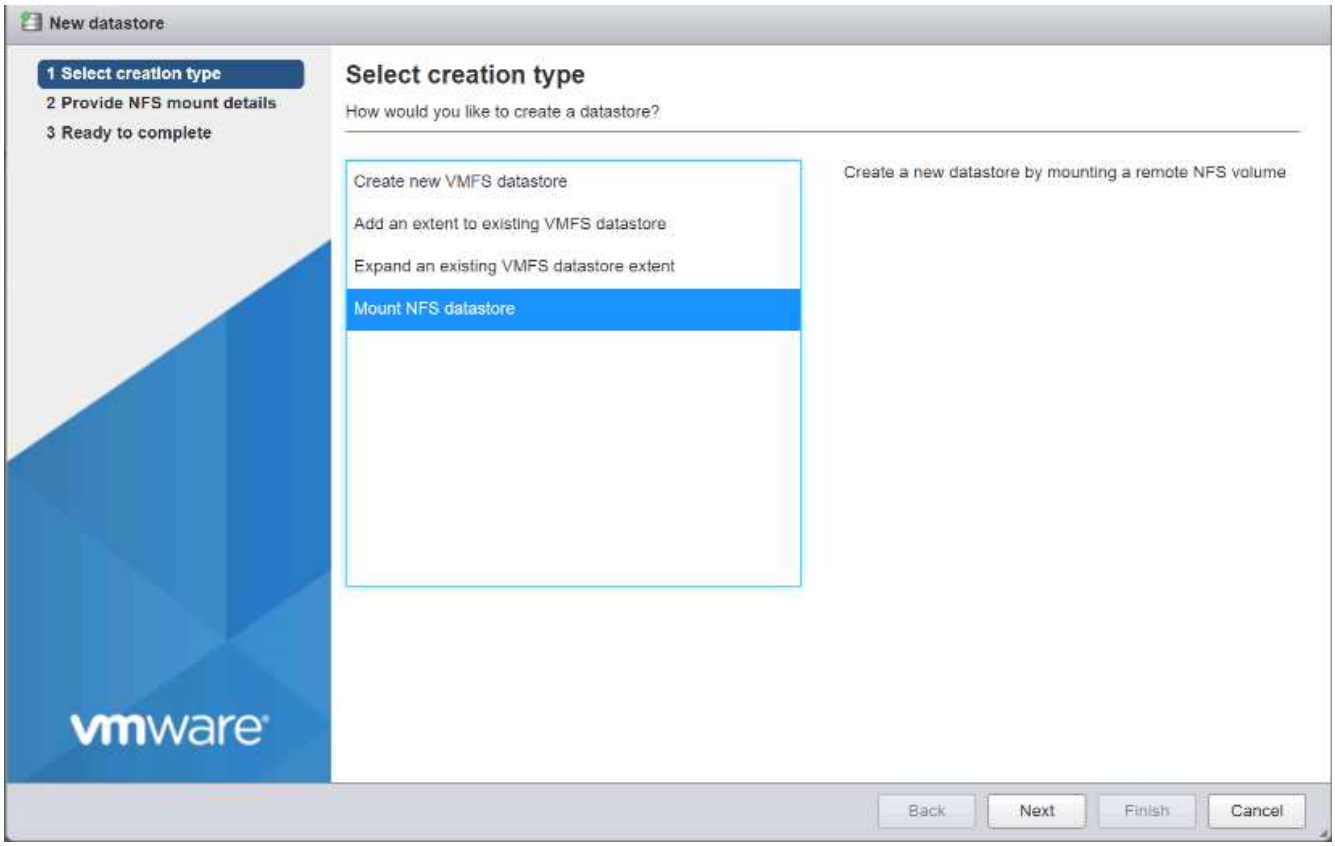
> ホストが自動的にストレージアダプタとターゲットを再スキャンし、静的ターゲットに追加します。

必要なデータストアをマウント

ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

必要なデータストアをマウントするには、各 ESXi ホストで次の手順を実行します。

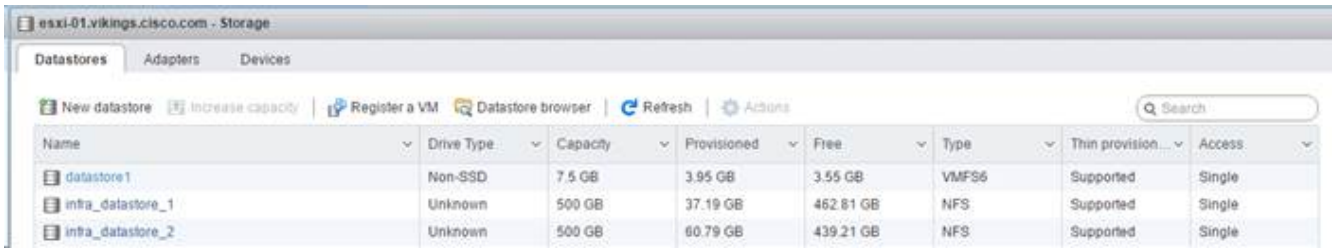
1. ホスト・クライアントで ' 左側の Storage を選択します
2. 中央のペインで、 [Datastores] を選択します。
3. 中央のペインで、 New Datastore （新規データストア）を選択して新しいデータストアを追加します。
4. [新規データストア] ダイアログボックスで、 [NFS データストアのマウント] を選択し、 [次へ] をクリックします。



5. [Provide NFS Mount Details] ページで、次の手順を実行します。
   a. データストア名として「 infra_datastore_1 」と入力します。
   b. NFS サーバの「 NFS_lif01_a 」 LIF の IP アドレスを入力します。
   c. NFS 共有の場合は '/infra_datastore_1' と入力します
   d. NFS のバージョンは NFS 3 のままにします。
   e. 次へをクリックします。

6. 完了をクリックします。これで、データストアがデータストアのリストに表示されます。
7. 中央のペインで、 New Datastore （新規データストア）を選択して新しいデータストアを追加します。
8. New Datastore （新規データストア）ダイアログボックスで、 Mount NFS Datastore （ NFS データストアのマウント）を選択し、 Next （次へ）をクリック

9. [Provide NFS Mount Details] ページで、次の手順を実行します。
    a. データストア名として「 infra_datastore_2 」と入力します。
    b. NFS サーバの「 nfs_lif02_a 」 LIF の IP アドレスを入力します。
    c. NFS 共有の場合は '/infra_datastore_2' と入力します
    d. NFS のバージョンは NFS 3 のままにします。
    e. 次へをクリックします。
10. 完了をクリックします。これで、データストアがデータストアのリストに表示されます。



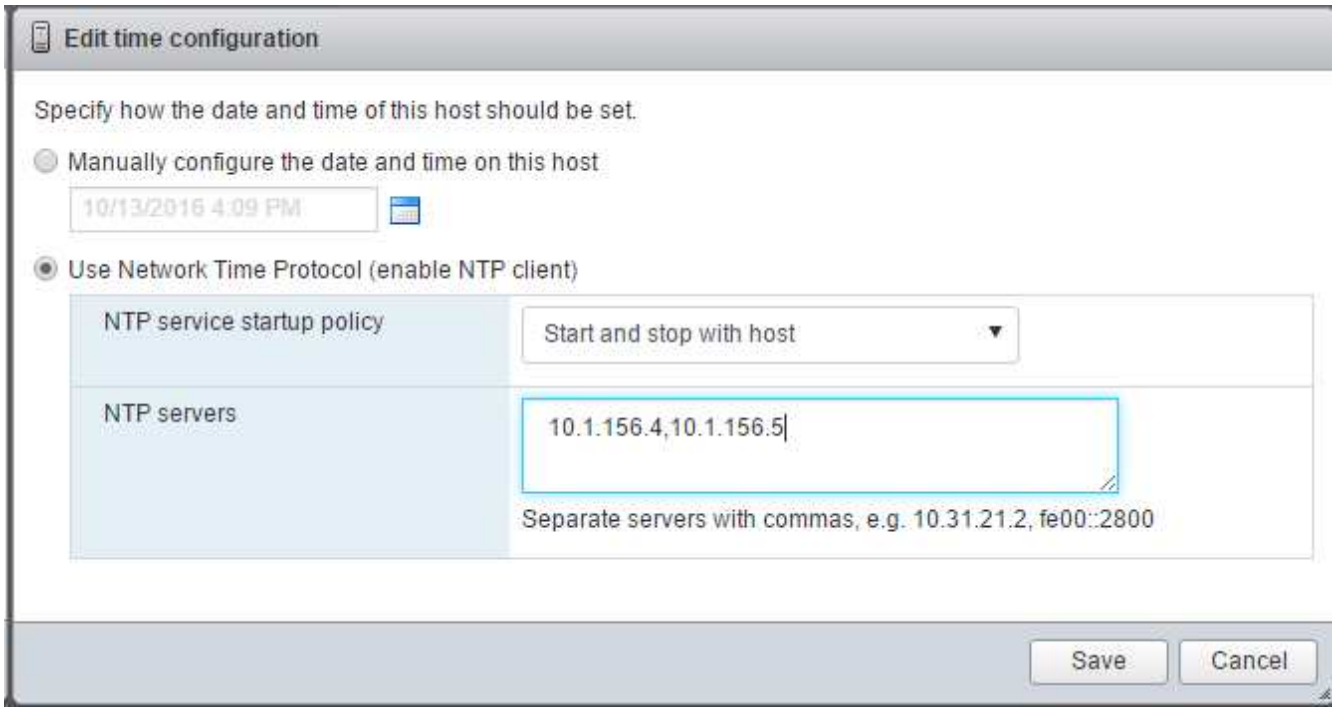
11. 両方の ESXi ホストに両方のデータストアをマウントします。

ESXi ホストで **NTP** を設定

ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

ESXi ホストで NTP を設定するには、各ホストで次の手順を実行します。

1. ホストクライアントから、左側の [管理] を選択します。
2. 中央のウィンドウ枠で、 [時刻と日付] タブを選択します。
3. 設定の編集をクリックします。
4. [ネットワークタイムプロトコルを使用する (NTP クライアントを有効にする)] が選択されていることを確認します。
5. ドロップダウンメニューを使用して、 Start （開始）および Stop with Host （ホストで停止）を選択します。
6. 2 つの Nexus スイッチの NTP アドレスを、カンマで区切って NTP サーバボックスに入力します。



7. Save をクリックして、設定の変更を保存します。
8. Actions > NTP service > Start の順に選択します。
9. NTP サービスが実行中で、クロックが正しい時刻に設定されたことを確認します

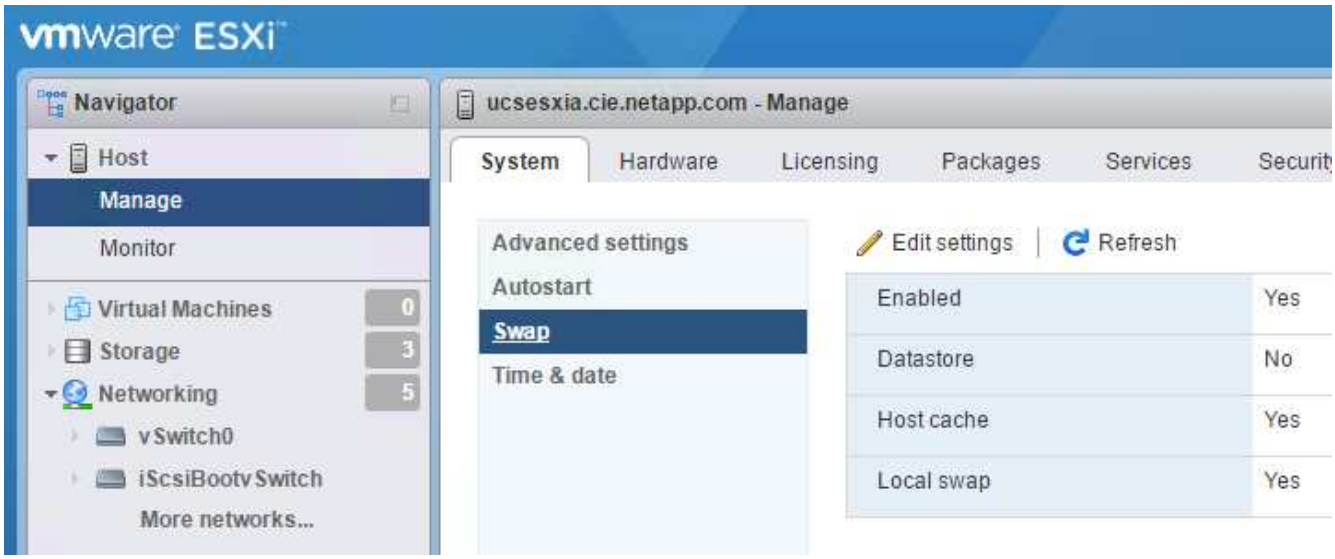
> NTP サーバの時間はホストの時間とは多少異なる場合があります。

ESXi ホストのスワップを設定

ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

ESXi ホストでホストのスワップを設定するには、各ホストで次の手順を実行します。

1. 左側のナビゲーションペインで、 [管理] をクリックします。右側のペインで System （システム）を選択し、 Swap （交換）をクリックします。



2. 設定の編集をクリックします。データストアのオプションから 'infra_swap' を選択します

3. [保存] をクリックします .

NetApp NFS Plug-in 1.1.2 for VMware VAAI をインストールします

NetApp NFS Plug-in 1 をインストールします。1.2 VMware VAAI の場合は、次の手順を実行します。

1. NetApp NFS Plug-in for VMware VAAI をダウンロードします。
   a. にアクセスします "ネットアップのソフトウェアダウンロードページ"。
   b. 下にスクロールして、 NetApp NFS Plug-in for VMware VAAI をクリックします。
   c. ESXi プラットフォームを選択します。
   d. 最新のプラグインのオフラインバンドル（ .zip ）またはオンラインバンドル（ .vib ）をダウンロードします。
2. NetApp NFS Plug-in for VMware VAAI ONTAP は IMT 9.5 への対応が保留中であり、相互運用性の詳細は NetApp IMT に近日中に公開されます。
3. ESX CLI を使用して、 ESXi ホストにプラグインをインストールします。

4. ESXi ホストをリブートします。

VMware vCenter Server 6.7 をインストールする

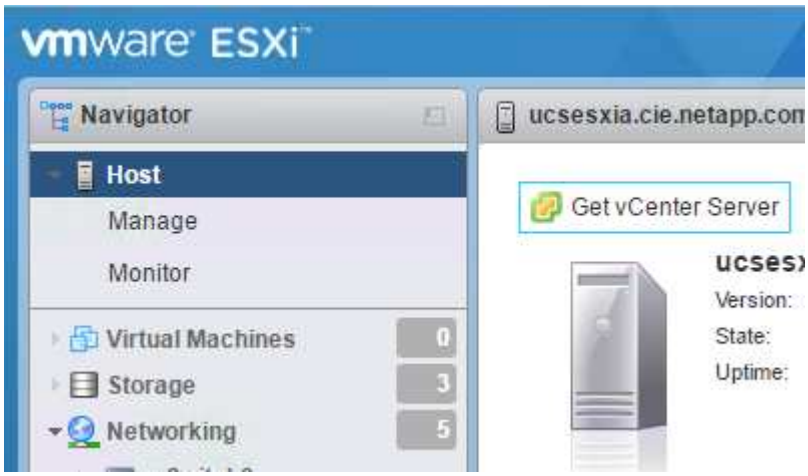
このセクションでは、 FlexPod 構成に VMware vCenter Server 6.7 をインストールする詳細な手順について説明します。

> FlexPod Express では、 VMware vCenter Server Appliance （ VCSA ）を使用します。

VMware vCenter Server Appliance をインストールする

vCSA をインストールするには、次の手順を実行します。

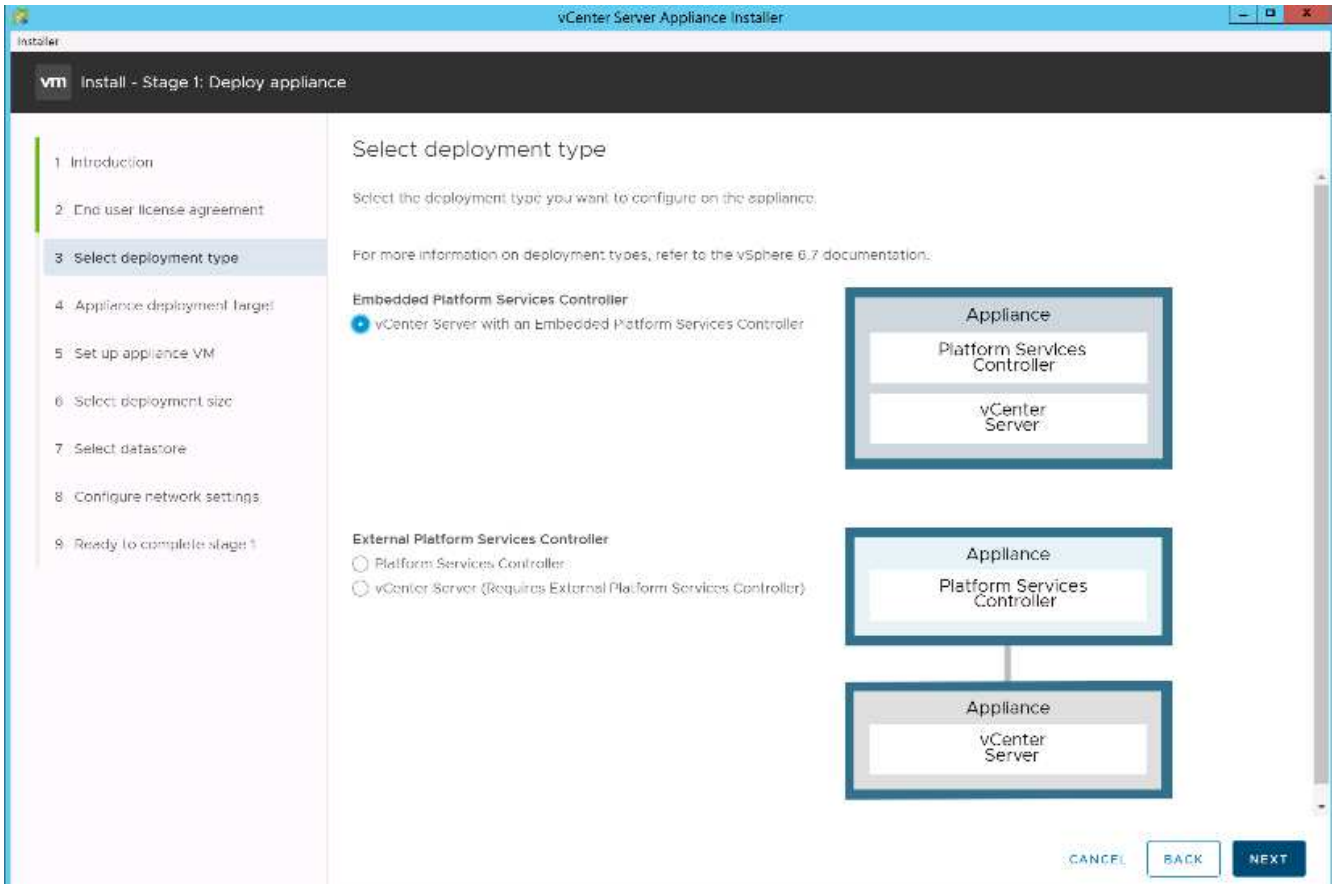
1. vCSA をダウンロードします。ESXi ホストの管理時に Get vCenter Server アイコンをクリックして、ダウンロードリンクにアクセスします。



2. vCSA を VMware サイトからダウンロードします。

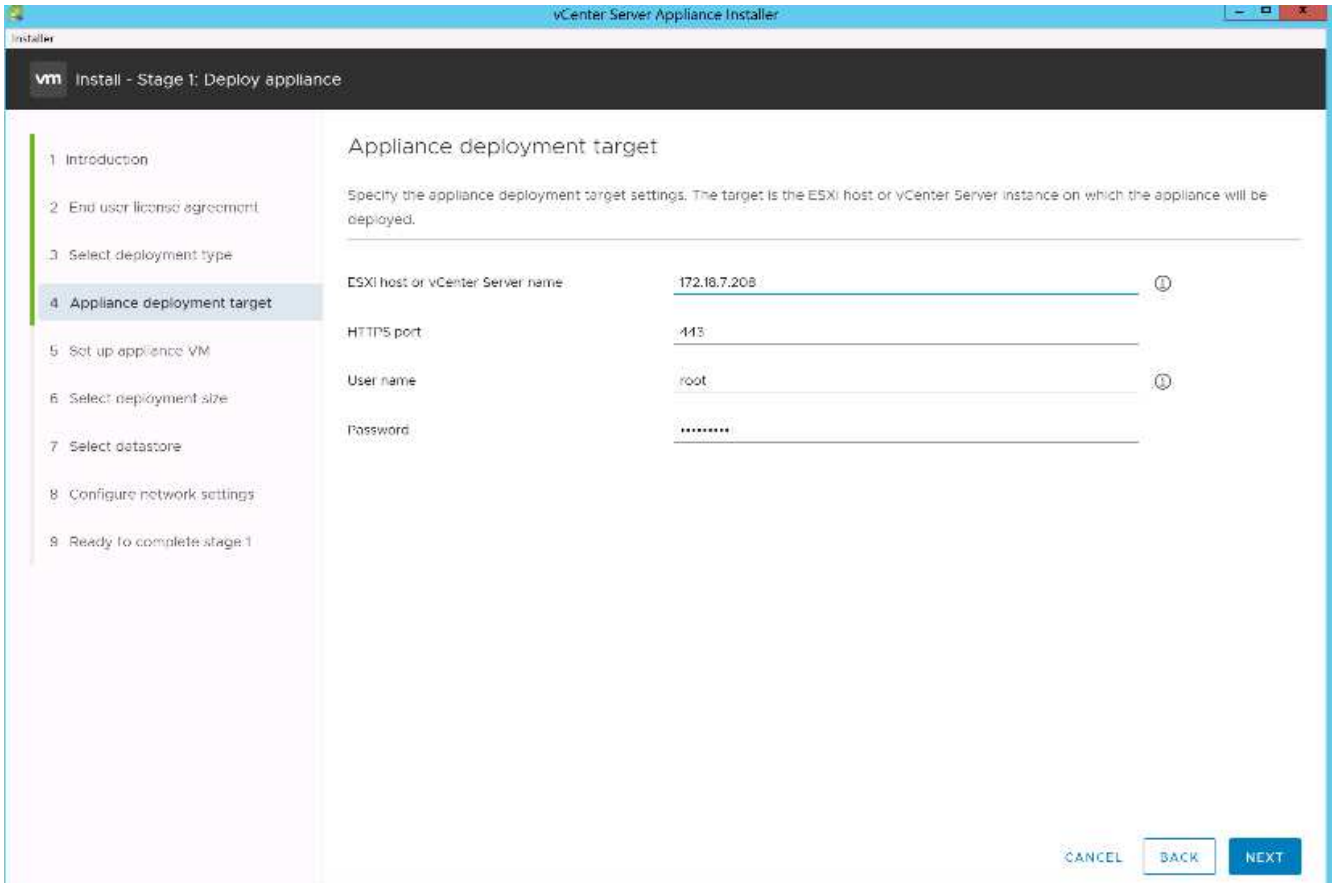
> インストール可能な Microsoft Windows vCenter Server がサポートされますが、 VMware では新しい導入に vCSA を推奨します。

3. ISO イメージをマウントします。
4. 「 VCSA -ui-sinstaller 」 > 「 win32 」ディレクトリに移動します。「 installer.exe 」をダブルクリックします。
5. [インストール] をクリックします
6. [はじめに] ページで [次へ] をクリックします。
7. EULA に同意します。
8. 展開タイプとして、 Embedded Platform Services Controller を選択します。

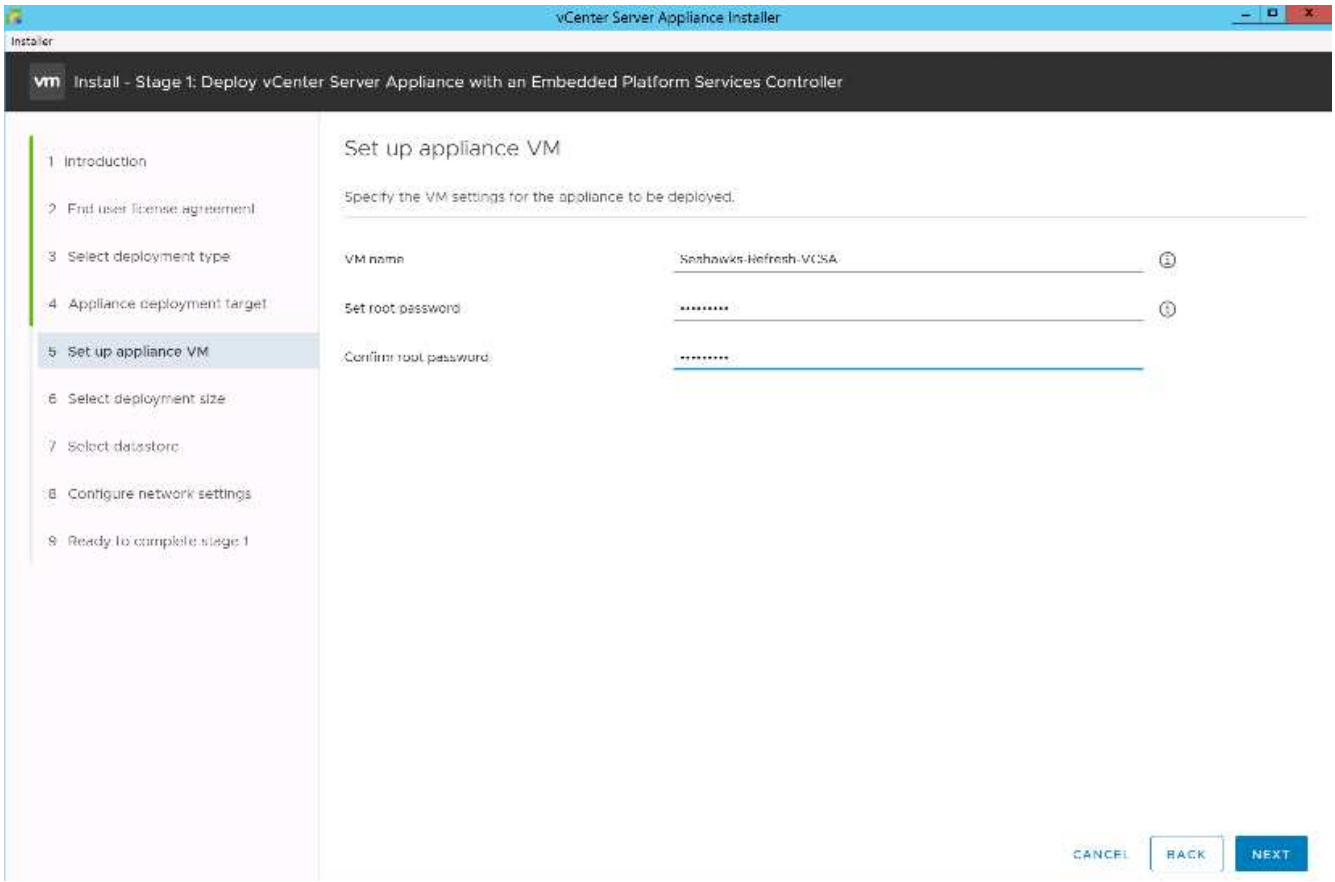


必要に応じて、 FlexPod Express 解決策の一部として、外部プラットフォームサービスコントローラの導入もサポートされます。

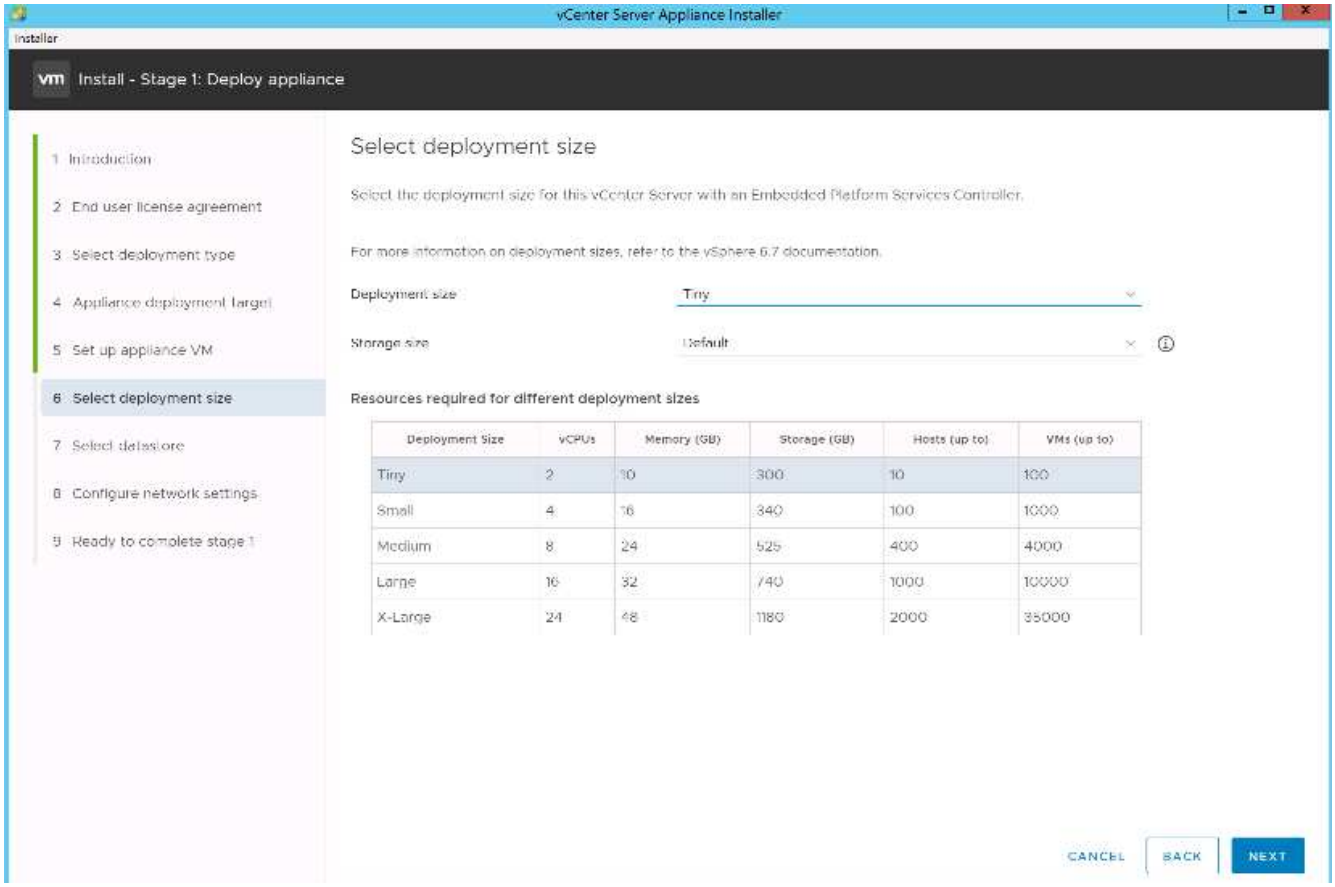
9. アプライアンス導入ターゲットページで、導入した ESXi ホストの IP アドレス、ルートユーザ名、および root パスワードを入力します。次へをクリックします。



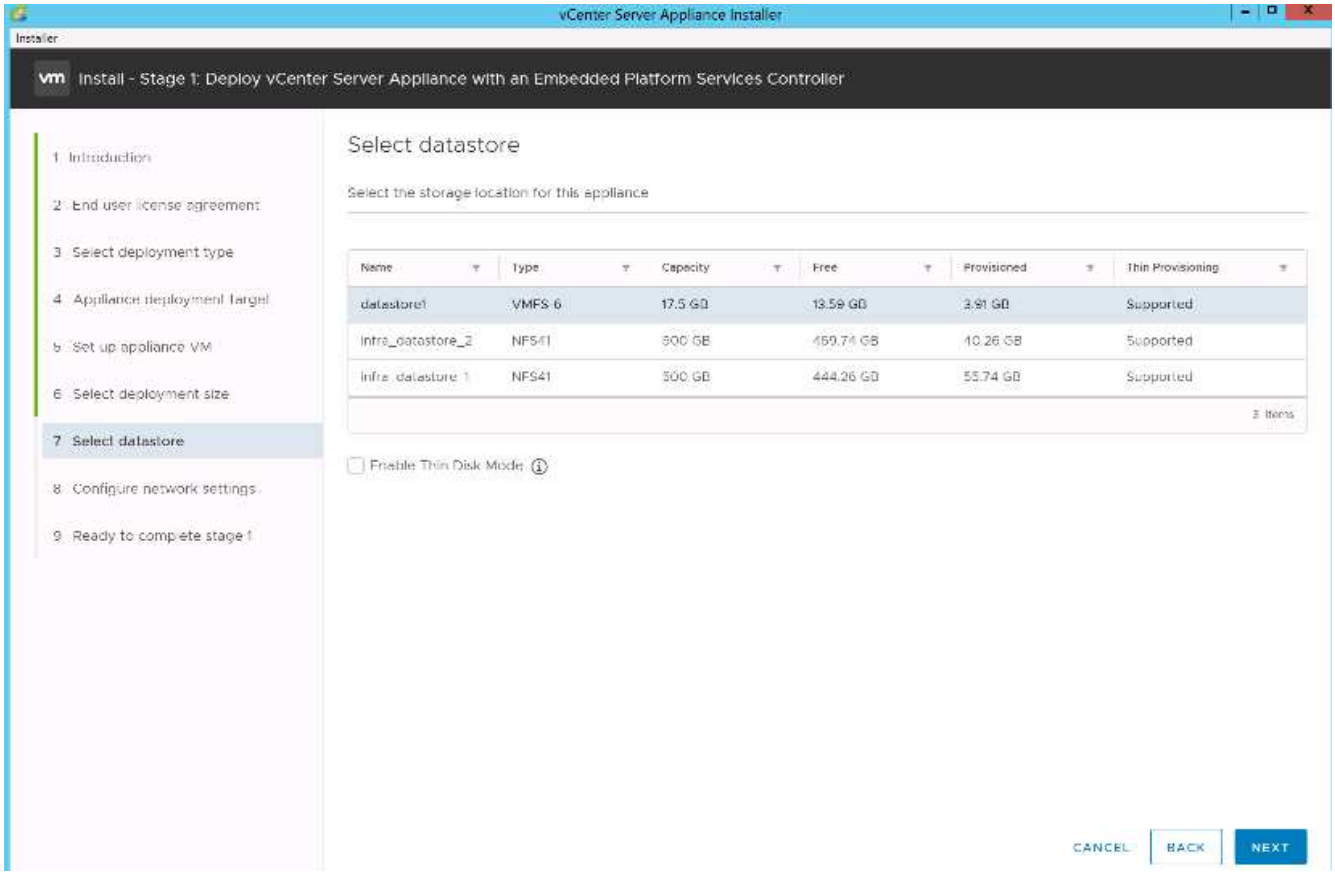
10. vCSA に VM 名および vCSA に使用するルートパスワードとして VCSA を入力して、アプライアンス VM を設定します。次へをクリックします。



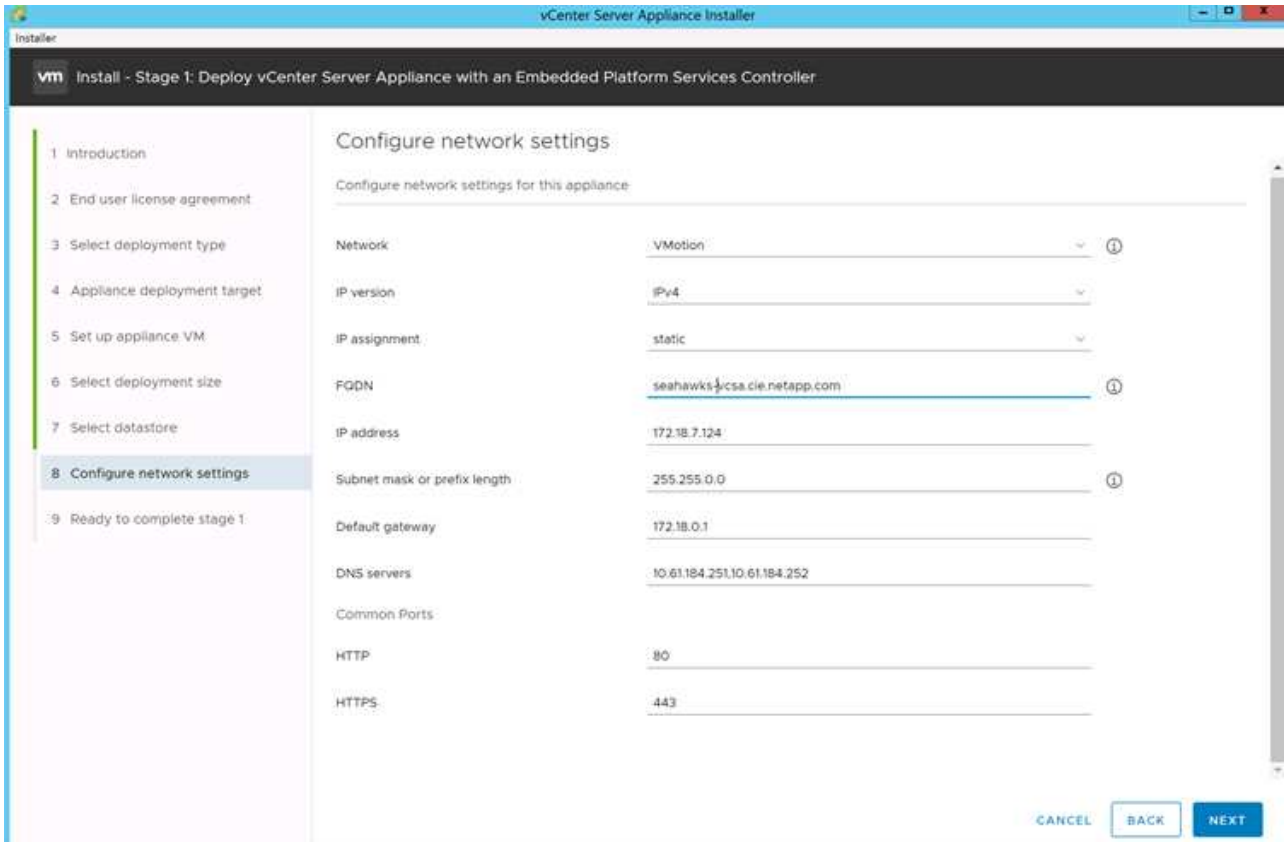
11. 環境に最も適した導入サイズを選択してください。次へをクリックします。



12. 「 infra_datastore_1' 」データストアを選択します。次へをクリックします。



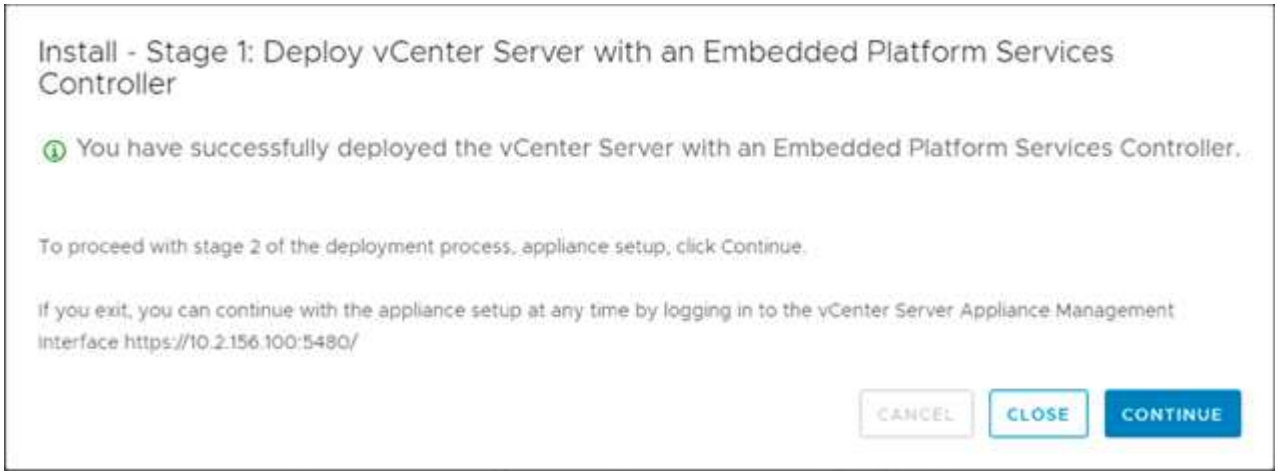
13. [Configure Network Settings] ページで次の情報を入力し、 [Next] をクリックします。
    a. ネットワークとして MGMT-Network を選択します。
    b. vCSA に使用する FQDN または IP を入力します。
    c. 使用する IP アドレスを入力します。
    d. 使用するサブネットマスクを入力します。
    e. デフォルトゲートウェイを入力します。
    f. DNS サーバを入力します。



14. 「ステージ 1 を完了する準備ができました」ページで、入力した設定が正しいことを確認します。完了をクリックします。

    vCSA がインストールされます。このプロセスには数分かかります。

15. ステージ 1 が完了すると、完了したことを示すメッセージが表示されます。「続行」をクリックしてステージ 2 の設定を開始します。



16. 「ステージ 2 の紹介」ページで、「次へ」をクリックします。
17. NTP サーバのアドレスとして「 \<<var_ntp_id>> 」と入力します。複数の NTP IP アドレスを入力できます。

    vCenter Server の高可用性機能を使用する場合は、 SSH アクセスが有効になっていることを確認してください。

18. SSO ドメイン名、パスワード、およびサイト名を設定します。次へをクリックします。

    特に 'vSpher.local' ドメイン名から外れる場合は ' これらの値を参考にしてください

19. 必要に応じて、 VMware カスタマーエクスペリエンスプログラムに参加します。次へをクリックします。
20. 設定の概要を確認します。[完了] をクリックするか、 [戻る] ボタンを使用して設定を編集します。
21. インストールの開始後に、インストールを一時停止または終了できないことを示すメッセージが表示されます。[OK] をクリックして続行します。

    アプライアンスの設定が続行されます。これには数分かかります。

    セットアップが正常に完了したことを示すメッセージが表示されます。

    > インストーラが vCenter Server にアクセスするために提供するリンクはクリック可能です。

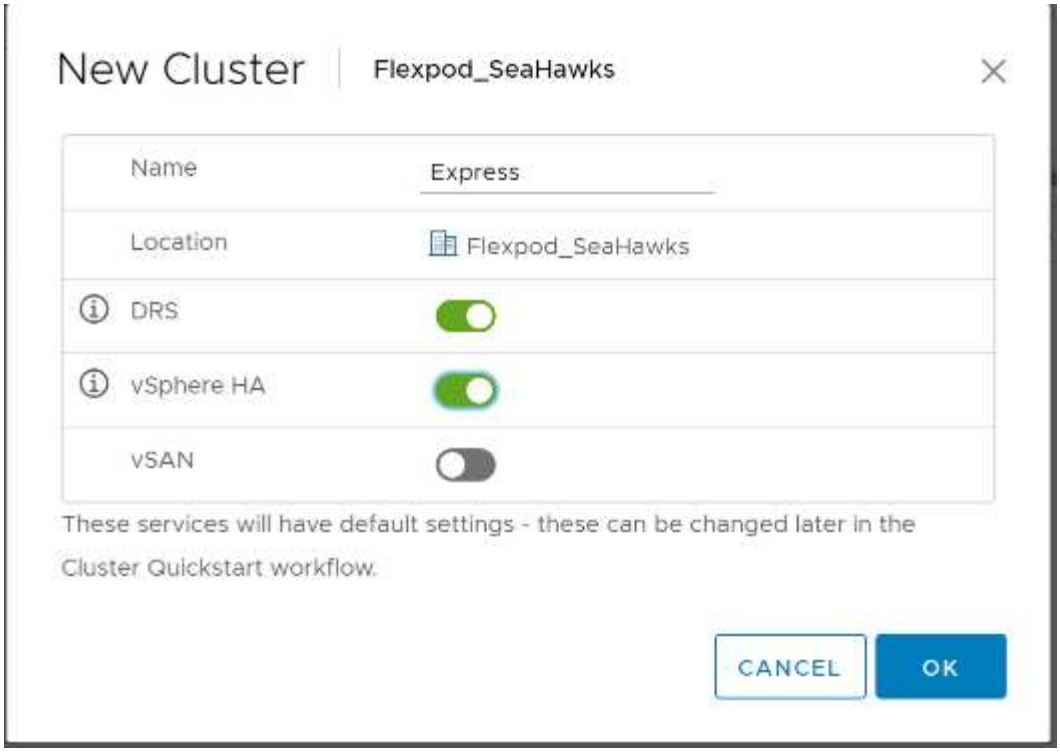
VMware vCenter Server 6.7 および **vSphere** クラスタリングを設定する

VMware vCenter Server 6.7 および vSphere クラスタリングを設定するには、次の手順を実行します。

1. https://\<<FQDN または IP of vCenter >> /vsphere-client/ に移動します。
2. vSphere Client の起動をクリックします。
3. vCSA のセットアッププロセスで入力したユーザ名 administrator@vsphere.loca と SSO パスワードを使用してログインします。
4. vCenter 名を右クリックし、 New Datacenter を選択します。
5. データセンターの名前を入力し、 [OK] をクリックします。
    - vSphere クラスタを作成 *

vSphere クラスタを作成するには、次の手順を実行します。

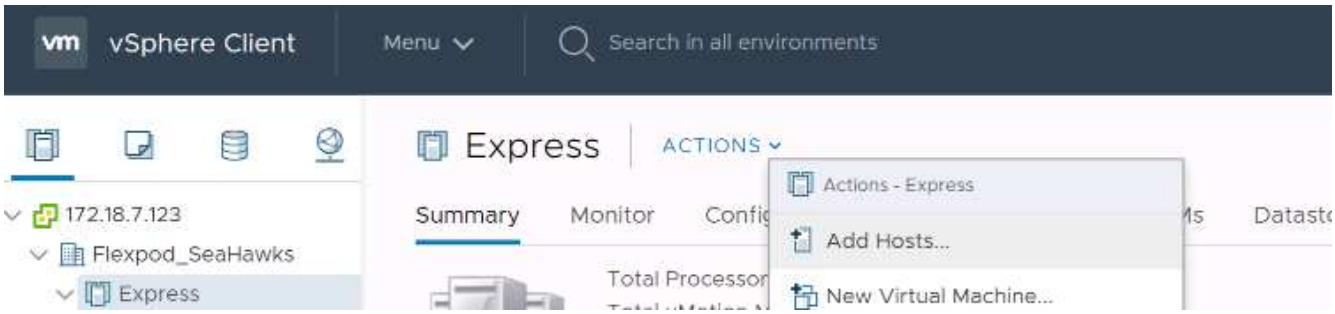
1. 新しく作成したデータセンターを右クリックし、 [New Cluster] を選択します。
2. クラスタの名前を入力します。
3. DRS と vSphere HA のオプションを選択して有効にします。
4. [OK] をクリックします。



- ESXi ホストをクラスタに追加 *

ESXi ホストをクラスタに追加するには、次の手順を実行します。

1. クラスタの Actions （アクション）メニューで Add Host （ホストの追加）を選択します。



2. ESXi ホストをクラスタに追加するには、次の手順を実行します。
   a. ホストの IP または FQDN を入力します。次へをクリックします。
   b. root ユーザ名とパスワードを入力します。次へをクリックします。
   c. Yes をクリックして、ホストの証明書を VMware 証明書サーバによって署名された証明書に置き換えます。
   d. [Host Summary] ページで [Next] をクリックします。
   e. 緑の + アイコンをクリックして、 vSphere ホストにライセンスを追加します。

      この手順は、必要に応じてあとで実行できます。

   f. [次へ] をクリックして、ロックダウンモードを無効のままに

g. [VM の場所] ページで [次へ] をクリックします。

h. [Ready to Complete] ページを確認します。[戻る] ボタンを使用して変更を行うか、 [完了] を選択します。

3. Cisco UCS ホスト B に対して手順 1 と 2 を繰り返します

FlexPod 構成にホストを追加する場合は、この手順を実行する必要があります。

ESXi ホストにコアダンプを設定します

iSCSI ブートホスト用の ESXi ダンプコレクタのセットアップ

VMware iSCSI ソフトウェアイニシエータを使用して iSCSI でブートされた ESXi ホストは、 vCenter の一部である ESXi ダンプコレクタにコアダンプを実行するように設定する必要があります。ダンプコレクタは、vCenter Appliance ではデフォルトで有効になっていません。この手順は、 vCenter の導入セクションの最後で実行する必要があります。ESXi Dump Collector をセットアップするには、次の手順を実行します。

1. vSphere Web Client に mailto ： administrator@vsphere.loca l [administrator@vsphere.loca l^] としてログインし、 [ホーム] を選択します。
2. 中央のペインで、システム構成をクリックします。
3. 左側のペインで、 [サービス] を選択します。
4. [Services] で、 [VMware vSphere ESXi Dump Collector] をクリックします。
5. 中央のペインで、緑の開始アイコンをクリックしてサービスを開始します。
6. [アクション] メニューの [スタートアップの種類の編集] をクリックします。
7. 自動を選択します。
8. [OK] をクリックします。
9. SSH を使用して、各 ESXi ホストに root として接続します。
10. 次のコマンドを実行します。

```
esxcli system coredump network set -v vmk0 -j <vcenter-ip>
esxcli system coredump network set -e true
esxcli system coredump network check
```

最後のコマンドを実行すると ' 構成された netdump サーバが動作していることを確認しましたというメッセージが表示されます

FlexPod Express にホストを追加する場合は、このプロセスを完了する必要があります。

まとめ

FlexPod Express は、業界をリードするコンポーネントを使用した検証済みの設計を提供することで、シンプルで効果的な解決策を実現します。FlexPod Express は、コンポーネントを追加することで拡張できるため、特定のビジネスニーズに合わせてカスタマ

イズできます。FlexPod Express は、中小規模の企業や、専用のソリューションを必要とする ROBO などの企業を念頭に置いて設計されました。

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。

- NVA-1130-design ： FlexPod Express with VMware vSphere 6.7U1 and NetApp AFF A220 with Direct-Attached IP = Based Storage NVA Design

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- AFF システムと FAS システムのドキュメントセンター

  "http://docs.netapp.com/platstor/index.jsp"

- ONTAP 9 ドキュメンテーション・センター

  "http://docs.netapp.com/ontap-9/index.jsp"

- ネットアップの製品マニュアル

  "https://docs.netapp.com"

FlexPod Express for VMware vSphere 7.0とCisco UCS MiniおよびNetApp AFF/FAS-NVA-Deployment

Jyh - ネットアップの陳氏をたたきます

FlexPod Express for VMware vSphere 7.0とCisco UCS MiniおよびNetApp AFF/FAS解決策 は、B200 M5ブレードサーバ、Cisco UCS 6324インシャーシファブリックインターコネクト、Cisco Nexus 31108PC-Vスイッチ、またはその他の準拠スイッチを搭載したCisco UCS Miniと、NetApp AFF A220、C190、FAS2700シリーズコントローラHAペアを活用します。 NetApp ONTAP 9.7データ管理ソフトウェアを実行します。このNetApp Verified Architecture（NVA）導入ドキュメントでは、インフラコンポーネントを設定し、VMware vSphere 7.0および関連ツールを導入して、信頼性と可用性に優れたFlexPod Expressベースの仮想インフラを作成するために必要な詳細な手順について説明します。

"FlexPod Express for VMware vSphere 7.0とCisco UCS MiniおよびNetApp AFF/FAS-NVA-Deployment"

FlexPod とセキュリティ

解決策、 FlexPod によるランサムウェア対策

TR-4802 ：『 FlexPod 、 the 解決策 to Ransomware 』

ネットアップ、 Arvind Ramakrinan 氏

協力：

ランサムウェアを理解するには、まず暗号化の重要なポイントを理解する必要があります。Cryptographical メソッドでは、共有秘密鍵（対称鍵暗号化）または鍵のペア（非対称鍵暗号化）を使用してデータを暗号化できます。このうちの 1 つは広く利用されている公開鍵で、もう 1 つは非公開の秘密鍵です。

ランサムウェアは、暗号化を使用して悪意のあるソフトウェアを構築する、暗号化に基づくマルウェアの一種です。このマルウェアは、対称キー暗号化と非対称キー暗号化の両方を利用して、被害者のデータをロックし、被害者のデータを復号化するための鍵を提供するように身代金を要求できます。

ランサムウェアの仕組み

次の手順では、ランサムウェアが暗号化を使用して、被害者による復号化やリカバリの範囲を伴わずに被害者のデータを暗号化する方法について説明します。

1. 攻撃者は、非対称キー暗号化のようにキーペアを生成します。生成された公開鍵はマルウェア内に置かれ、マルウェアは解放されます。
2. 被害者のコンピュータまたはシステムにマルウェアが侵入すると、擬似乱数生成器（ PRNG ）またはその他の実行可能な乱数生成アルゴリズムを使用してランダムな対称キーが生成されます。
3. マルウェアは、この対称キーを使用して被害者のデータを暗号化します。最終的には、マルウェアに埋め込まれた攻撃者の公開鍵を使用して、対称キーを暗号化します。このステップの出力は、暗号化された対称キーの非対称暗号テキストと、被害者のデータの対称暗号テキストです。
4. マルウェアは、被害者のデータとデータの暗号化に使用された対称キーをゼロ化（消去）し、リカバリの対象範囲を残しません。
5. これで、対称キーの非対称暗号テキストと、データの暗号化に使用された対称キーを取得するために支払わなければならない身代金の値が、 Victim に表示されます。
6. 被害者は身代金を支払って、攻撃者と非対称暗号テキストを共有します。攻撃者は自分の秘密鍵を使って暗号テキストを復号化し、その結果対称鍵が生成されます。
7. 攻撃者はこの対称キーを攻撃者と共有します。このキーを使用して、すべてのデータを復号化し、攻撃から回復できます。

課題

個人や組織がランサムウェア攻撃を受けた場合、次のような課題に直面します。

- 最も重要な課題は、組織または個人の生産性を即座に低下させることです。重要なファイルはすべて回復する必要があり、システムを保護する必要があるため、正常な状態に戻るのに時間がかかります。
- クライアントまたは顧客に属する機密情報を含むデータ侵害が発生し、組織が明確に回避したいという危機的状況につながる可能性があります。
- データが間違った手に入ったり、完全に消去されたりする可能性は非常に高いため、企業や個人にとって災害となる可能性のあるリターンポイントをゼロにすることができます。
- 身代金を支払った後、攻撃者がデータを復元するための鍵を提供する保証はありません。
- 身代金を支払っても機密データのブロードキャストを控えることは、攻撃者に保証されていません。
- 大規模な企業では、ランサムウェア攻撃の原因となった抜け穴を特定するのは面倒であり、すべてのシステムを保護するには多くの労力が必要です。

誰がリスクにさらされているか？

個人や大企業など、誰もがランサムウェア攻撃を受ける可能性があります。適切に定義されたセキュリティ対策や慣行を実装していない組織は、このような攻撃に対してさらに脆弱です。攻撃が大規模な組織に与える影響は、個人が耐えうる攻撃の数倍にも及ぶ可能性があります。

ランサムウェア攻撃はすべてのマルウェア攻撃の約 28% を占めています。つまり、マルウェアのインシデントが 4 つに 1 つ以上あり、ランサムウェア攻撃と言えます。ランサムウェアはインターネットを介して自動的に、または無差別に拡散する可能性があります。また、セキュリティ上の問題が発生した場合は、被害者のシステムに入り、他の接続されたシステムへの拡散を継続できます。攻撃者は、多くのファイル共有を実行したり、機密性の高い重要なデータを大量に取得したり、攻撃に対する保護を適切に維持したりする人や組織を標的にしている傾向があります。

攻撃者は、次の潜在的なターゲットに集中する傾向があります。

- 大学と学生コミュニティ
- 政府機関、政府機関
- 病院
- 銀行

これはターゲットの完全なリストではありません。これらのカテゴリのいずれかに該当しない場合は、攻撃から自分を守ることはできません。

ランサムウェアによるシステムへの移行やデータの拡散について教えてください。

ランサムウェアがシステムに移行したり、他のシステムに拡散したりする方法はいくつかあります。今日の世界では、ほとんどすべてのシステムがインターネット、 LAN 、 WAN などを介して相互に接続されています。これらのシステム間で生成および交換されるデータ量は増加しています。

ランサムウェアが拡散する最も一般的な方法には、データの共有やアクセスに日常的に使用する方法があります。

- E メール
- P2P ネットワーク
- ファイルのダウンロード
- ソーシャルネットワーキング

- モバイルデバイス
- 安全でないパブリックネットワークに接続しています
- Web URL へのアクセス

データ損失の影響

データ損失の影響は、企業が予想する以上に広範囲に及ぶ可能性があります。この影響は、ダウンタイムの期間、または組織がデータにアクセスできない期間によって異なります。攻撃が長ければ長いほど、組織の収益、ブランド、評判への影響は大きくなります。また、組織は法的な問題に直面し、生産性が大幅に低下する可能性もあります。

これらの問題は時間の経過とともに継続して発生するため、攻撃に対する対応方法によっては、拡大が始まり、組織の文化が変化する可能性があります。今日の世界では、組織に関する情報が急速に広まり、否定的なニュースが原因によってその評判に永久的な損害を与える可能性があります。企業は、データ損失に対する大きなペナルティに直面する可能性があり、結果としてビジネスの停止につながる可能性があります。

財務的影響

最近の "McAfee レポート"サイバー犯罪によって発生するグローバルコストは約 6 億ドルで、世界の GDP の約 0.8 %に相当します。この金額を世界的に増加するインターネット経済の 4.2 兆ドルと比較すると、成長に 14% の税金がかかることになります。

ランサムウェア攻撃は、このような金銭的コストを大幅に負担します。2018 年には、ランサムウェア攻撃によって発生したコストは約 80 億ドルでした。 2019 年には 115 億ドルに達すると予測されています。

解決策とは何ですか？

ダウンタイムを最小限に抑えたランサムウェア攻撃からのリカバリは、プロアクティブなディザスタリカバリ計画を実装することでのみ可能です。攻撃から回復する機能は優れていますが、攻撃を完全に阻止することが理想的です。

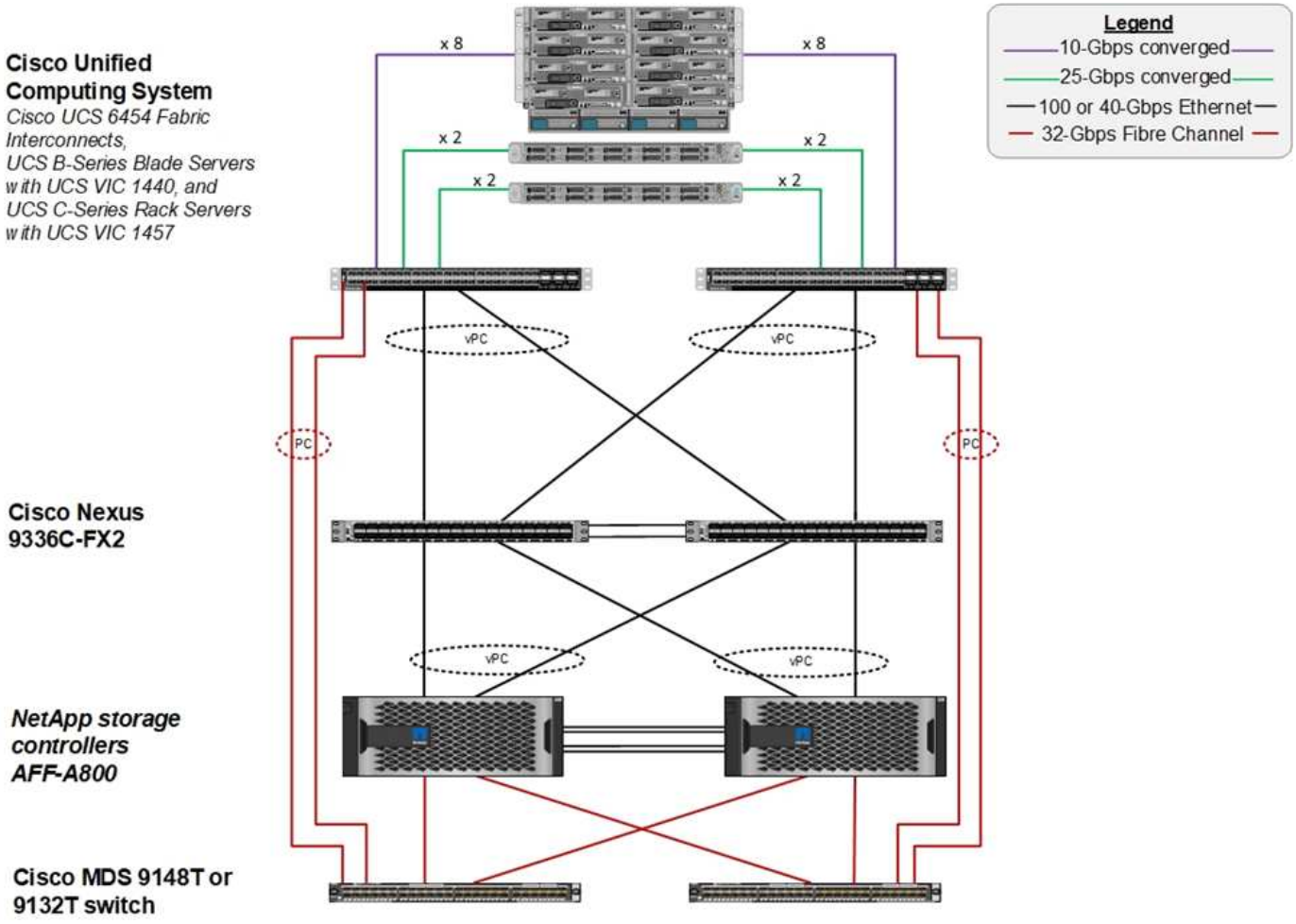
攻撃を防止するためにレビューと修正が必要な領域はいくつかありますが、攻撃を防止または復旧するためのコアコンポーネントはデータセンターです。

ネットワーク、コンピューティング、ストレージのエンドポイントを保護するデータセンターの設計と機能は、日常業務の安全な環境を構築する上で重要な役割を果たします。このドキュメントでは、 FlexPod ハイブリッドクラウドインフラストラクチャの機能が、攻撃の発生時に迅速にデータをリカバリするのにどのように役立つか、また攻撃を防御するのにどのように役立つかを説明します。

FlexPod の概要

FlexPod は、 Cisco Unified Computing System （ Cisco UCS ）サーバ、 Cisco Nexus ファミリーのスイッチ、 Cisco MDS ファブリックスイッチ、ネットアップストレージアレイを 1 つの柔軟なアーキテクチャに統合した、事前設計済みの統合された検証済みアーキテクチャです。FlexPod ソリューションは、単一点障害のない高可用性を実現するとともに、コスト効率と設計の柔軟性を維持して、さまざまなワークロードをサポートするように設計されています。FlexPod 設計では、さまざまなハイパーバイザーやベアメタルサーバをサポートでき、お客様のワークロードの要件に応じてサイジングや最適化も可能です。

次の図は FlexPod アーキテクチャを示しており、スタックのすべてのレイヤの高可用性を明確に示しています。ストレージ、ネットワーク、コンピューティングのインフラコンポーネントは、コンポーネントの 1 つに障害が発生した場合に、稼働しているパートナーに瞬時にフェイルオーバーできるように構成されます。



FlexPod システムの主な利点は、複数のワークロードに対して事前に設計、統合、検証されていることです。解決策の検証ごとに、詳細な設計ガイドと導入ガイドが公開されています。これらのドキュメントには、FlexPod でワークロードをシームレスに実行するために採用する必要があるベストプラクティスが含まれています。これらのソリューションは、業界最高レベルのコンピューティング、ネットワーク、ストレージ製品と、インフラ全体のセキュリティと強化に重点を置いた多数の機能で構成されています。

"IBM の X-Force Threat Intelligence Index を参照してください" 州、「不正なクラウドインフラストラクチャの歴史的な 424% の増加など、侵害されたレコードの 3 分の 2 を担当する人的ミス」

FlexPod システムでは、 Cisco Validated Design （ CVD ）および NetApp Verified Architectures （ NVA ）に記載されているベストプラクティスに従って、インフラのエンドツーエンドのセットアップを実行する Ansible プレイブックを使用して、インフラの構成ミスを回避できます。

ランサムウェアからの保護対策

ここでは、 NetApp ONTAP データ管理ソフトウェアの主な機能と、ランサムウェア攻撃から効果的に保護してリカバリするために使用できる Cisco UCS および Cisco Nexus のツールについて説明します。

ストレージ： **NetApp ONTAP**

ONTAP ソフトウェアには、データ保護に役立つさまざまな機能が用意されています。そのほとんどは、ONTAP システムをお持ちのお客様には無償で提供されています。次の機能を常に使用して、攻撃からデータを保護できます。

- * NetApp Snapshot テクノロジ。 * Snapshot コピーは、ボリュームの読み取り専用イメージであり、ファイルシステムの「ある瞬間」の状態をキャプチャしたものです。これらのコピーによって、システムパフォーマンスへの影響がなく、データが保護されると同時に、大量のストレージスペースが消費されることもありません。Snapshot コピーの作成スケジュールを作成することを推奨します。また、マルウェアの中には、感染後数週間または数か月後に休止して再アクティブ化できるものがあるため、長期の保存期間を維持する必要があります。攻撃が発生した場合、感染前に作成された Snapshot コピーを使用してボリュームをロールバックできます。
- * NetApp SnapRestore テクノロジ。 * SnapRestore データ・リカバリ・ソフトウェアは、データ破損からのリカバリや、ファイルの内容のみの復元に非常に役立ちます。SnapRestore はボリュームの属性をリバートせず、 Snapshot コピーからアクティブファイルシステムにファイルをコピーすることで、管理者が達成できる処理よりもはるかに高速です。データのリカバリ速度は、できるだけ多くのファイルをリカバリする必要がある場合に役立ちます。攻撃が発生した場合、この非常に効率的なリカバリプロセスにより、ビジネスを迅速にオンラインに戻すことができます。
- * NetApp SnapCenter テクノロジ。 * SnapCenter ソフトウェアは、ネットアップのストレージベースのバックアップ機能とレプリケーション機能を使用して、アプリケーションと整合性のあるデータ保護を実現します。このソフトウェアは、エンタープライズアプリケーションと統合され、アプリケーション固有およびデータベース固有のワークフローを提供して、アプリケーション、データベース、仮想インフラの管理者のニーズを満たします。SnapCenter は、使いやすいエンタープライズプラットフォームを提供し、アプリケーション、データベース、ファイルシステム全体でデータ保護をセキュアに調整、管理します。アプリケーションと整合性のあるデータ保護を提供できるかどうかは、整合性のある状態へのアプリケーションのリストアをより迅速に行えるようにするため、データリカバリの際に重要になります。
- * NetApp SnapLock テクノロジ。 * SnapLock は、消去や書き換えが不可能な状態でファイルを保存し、コミットできる特殊な目的のボリュームを提供します。FlexVol ボリュームに保存されているユーザーの本番データは、 NetApp SnapMirror または SnapVault テクノロジを使用して、それぞれ SnapLock ボリュームにミラーリングまたは保存できます。SnapLock ボリューム内のファイル、ボリューム自体、およびホストアグリゲートは、保持期間が終了するまで削除できません。
- * NetApp FPolicy テクノロジ。 * 特定の拡張子を持つファイルの操作を禁止することにより、 FPolicy ソフトウェアを使用して攻撃を防止します。FPolicy イベントは、特定のファイル操作に対してトリガーできます。イベントはポリシーに関連付けられており、ポリシーは使用する必要があるエンジンを呼び出します。ポリシーにはランサムウェアを含む可能性のある一連のファイル拡張子を設定できます。拡張子が許可されていないファイルで許可されていない操作を実行しようとすると、 FPolicy によりその操作が実行されなくなります。

ネットワーク： **Cisco Nexus**

Cisco NX-OS ソフトウェアは、ネットワーク異常およびセキュリティの検出を強化する NetFlow 機能をサポートしています。NetFlow は、ネットワーク上のすべてのカンバセーション、通信に関係する側、使用されているプロトコル、およびトランザクションの期間のメタデータをキャプチャします。情報を集約して分析すると、正常な動作に関する洞察を得ることができます。

収集されたデータを使用すると、疑わしいアクティビティのパターンを識別することもできます。たとえば、マルウェアがネットワーク全体に拡散し、これが気付かない場合があります。

NetFlow では、フローを使用してネットワークモニタリングの統計情報を提供します。フローは、送信元インターフェイス（または VLAN ）に着信し、キーの値が同じパケットの単方向ストリームです。キーは、パケット内のフィールドの識別された値です。フローレコードを使用してフローを作成し、フローに固有のキーを

定義します。フローエクスポータを使用して、 Cisco StealthWatch などのリモート NetFlow コレクタに NetFlow が収集するデータをエクスポートできます。StealthWatch では、この情報を使用してネットワークを継続的に監視し、ランサムウェアの発生が発生した場合にリアルタイムの脅威検出およびインシデント応答フォレンジックを提供します。

コンピューティング： **Cisco UCS**

Cisco UCS は、 FlexPod アーキテクチャのコンピューティングエンドポイントです。複数のシスコ製品を使用して、スタックのこのレイヤをオペレーティングシステムレベルで保護することができます。

コンピューティングレイヤまたはアプリケーションレイヤには、次の主要製品を実装できます。

- * エンドポイント向けの Cisco Advanced Malware Protection （ AMP ）。 * Microsoft Windows および Linux オペレーティングシステムでサポートされているこの解決策は、防止、検出、および応答機能を統合しています。このセキュリティソフトウェアは、セキュリティ侵害の防止、侵入ポイントでのマルウェアのブロック、ファイルおよびプロセスのアクティビティの継続的な監視と分析を行い、フロントライン防御を回避できる脅威を迅速に検出、阻止、修復します。

  AMP の Malicious Activity Protection （ MAP ）コンポーネントは、すべてのエンドポイントアクティビティを継続的に監視し、エンドポイント上の実行中のプログラムのランタイム検出と異常な動作のブロックを提供します。たとえば、エンドポイントの動作がランサムウェアを示している場合、攻撃の原因となっているプロセスは終了し、エンドポイントの暗号化を防ぎ、攻撃を停止します。

- * 電子メールセキュリティに関するシスコの高度なマルウェア対策。 * 電子メールは、マルウェアを拡散し、サイバー攻撃を実行するための主要な手段となっています。平均して、 1 日に約 1 、 000 億通の電子メールが交換されます。これにより、攻撃者はユーザーのシステムに非常に優れた侵入ベクトルを与えることができます。そのため、この種の攻撃を防御することは絶対に不可欠です。

  AMP は、ゼロデイ攻撃や悪意のある添付ファイルに隠された不潔なマルウェアなどの脅威を電子メールで分析します。また、業界をリードする URL インテリジェンスを使用して、悪意のあるリンクに対抗します。スピアフィッシング、ランサムウェア、その他の高度な攻撃から高度な保護を提供します。

- * 次世代侵入防御システム（ NGIPS ）。 * Cisco firepower NGIPS は、データセンターの物理アプライアンスとして、または VMware の仮想アプライアンスとして導入できます（ NGIPSv for VMware ）。この非常に効果的な侵入防御システムは、信頼性の高いパフォーマンスと低い総所有コストを実現します。オプションのサブスクリプションライセンスで脅威からの保護を拡張して、 AMP 、アプリケーションの可視化と制御、および URL フィルタリング機能を提供できます。仮想化された NGIPS は、仮想マシン（ VM ）間のトラフィックを検査し、リソースが限られたサイトで NGIPS ソリューションの導入と管理を容易にして、物理資産と仮想資産の両方の保護を強化します。

FlexPod でデータを保護し、リカバリできます

このセクションでは、攻撃が発生した場合にエンドユーザーのデータをどのように回復できるか、および FlexPod システムを使用して攻撃を防御する方法について説明します。

テストベッドの概要

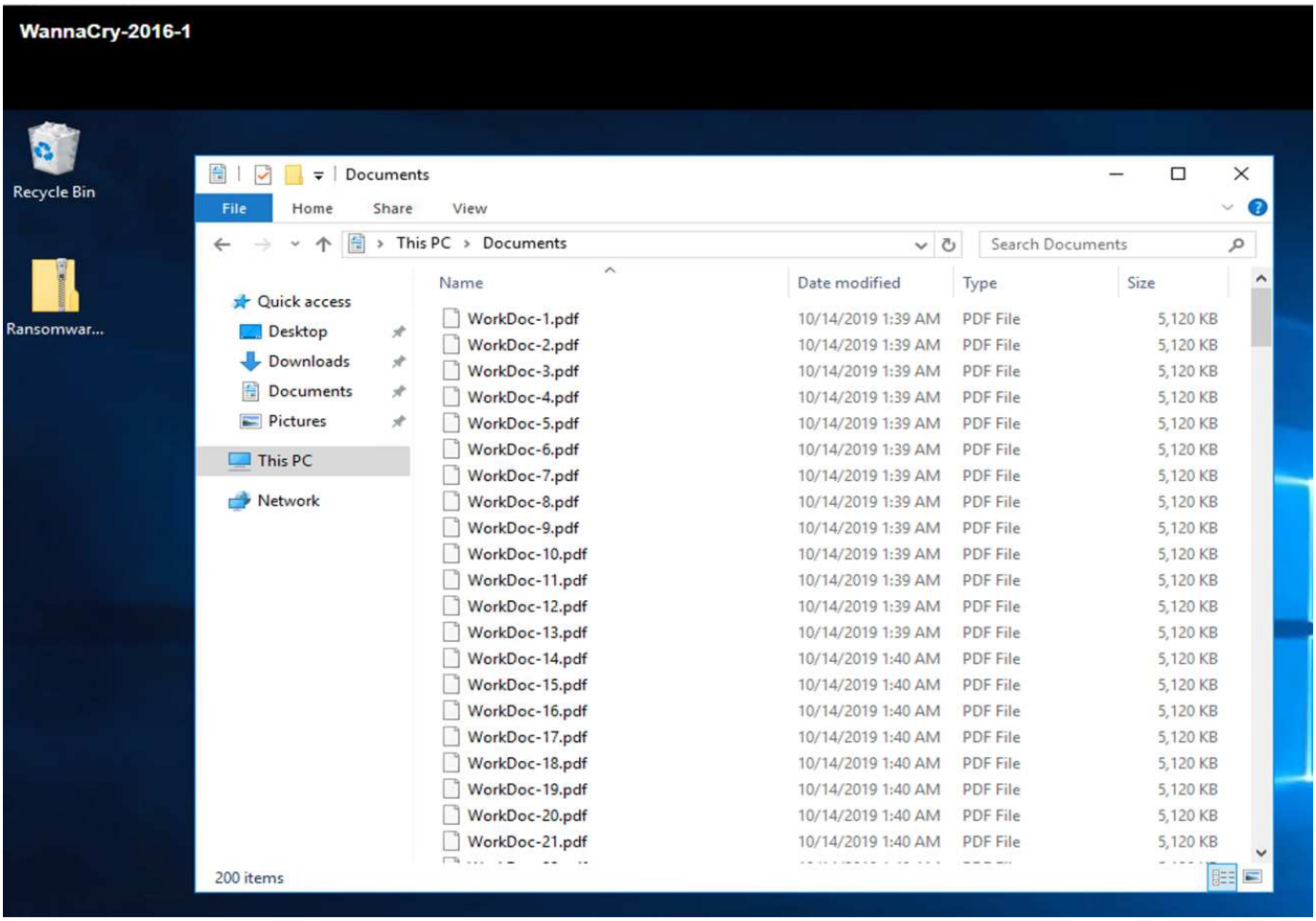
テストベッドは、 FlexPod の検出、修復、および防止を示すために、本ドキュメントの作成時点で使用可能な最新のプラットフォーム CVD で指定されているガイドラインに基づいて構築されています。 "FlexPod データセンターと VMware vSphere 6.7 U1 、 Cisco UCS 第 4 世代、および NetApp AFF A シリーズに関する CVD"。

NetApp ONTAP ソフトウェアの CIFS 共有を提供していた Windows 2016 VM は、 VMware vSphere インフラに導入されました。その後、特定の拡張子タイプのファイルが実行されないように、 CIFS 共有に NetApp FPolicy を設定しました。また、アプリケーションと整合性のある Snapshot コピーを作成するために、インフラ内の VM の Snapshot コピーを管理するために NetApp SnapCenter ソフトウェアを導入しました。

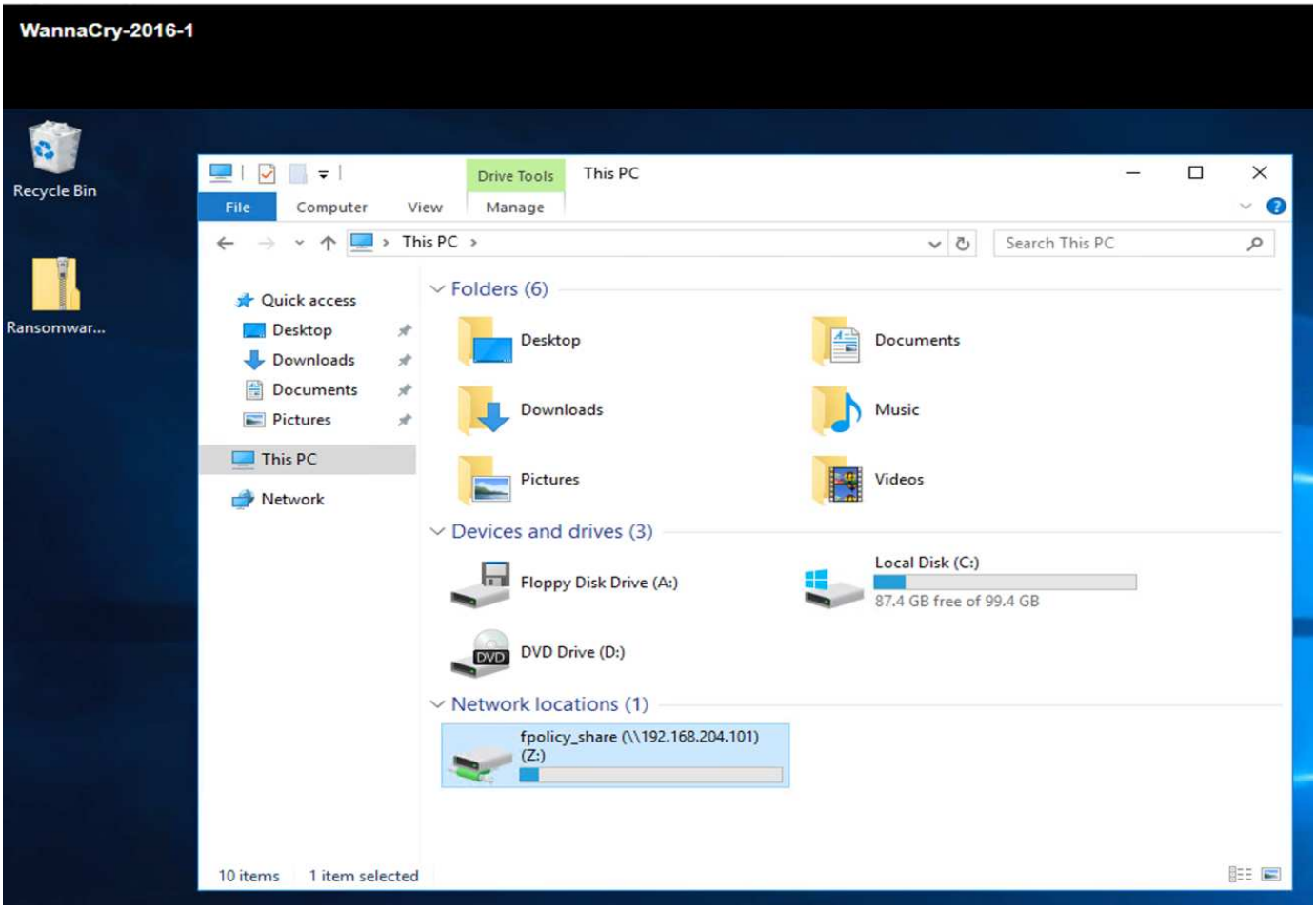
攻撃前の **VM** とそのファイルの状態

ここでは、 VM およびマッピングされている CIFS 共有に対する攻撃前のファイルの状態を示します。

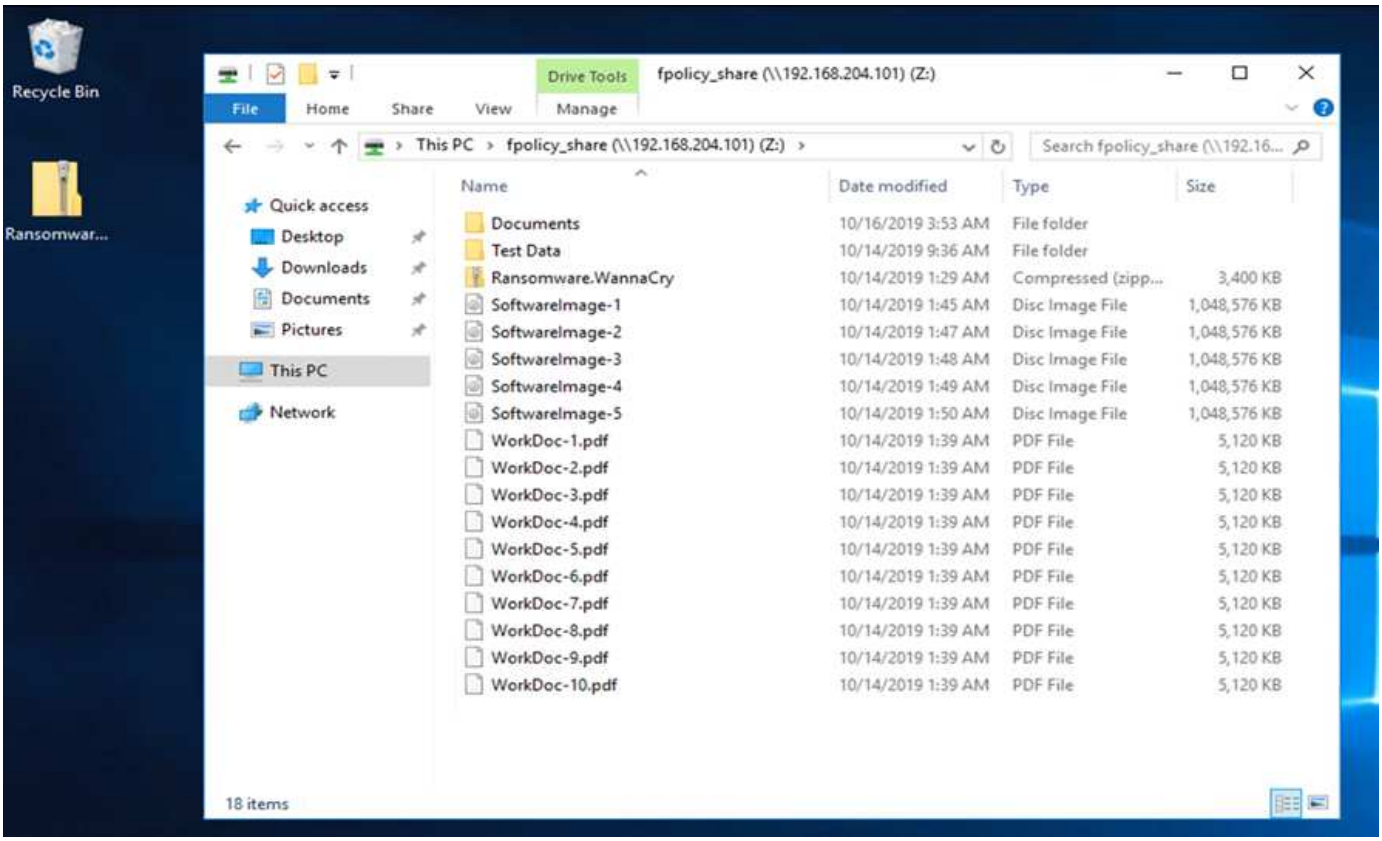
VM の Documents フォルダには、 WannaCry マルウェアによってまだ暗号化されていない PDF ファイルのセットがありました。



次のスクリーンショットは、 VM にマッピングされている CIFS 共有を示しています。



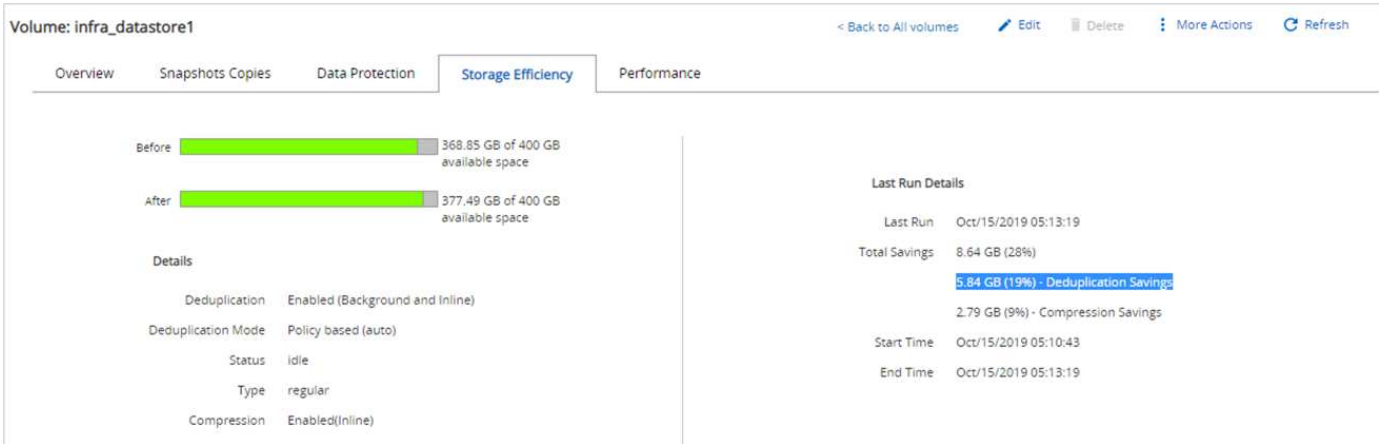
次のスクリーンショットは、 WannaCry マルウェアによってまだ暗号化されていない CIFS 共有 'fpolicy_share' 上のファイルを示しています。



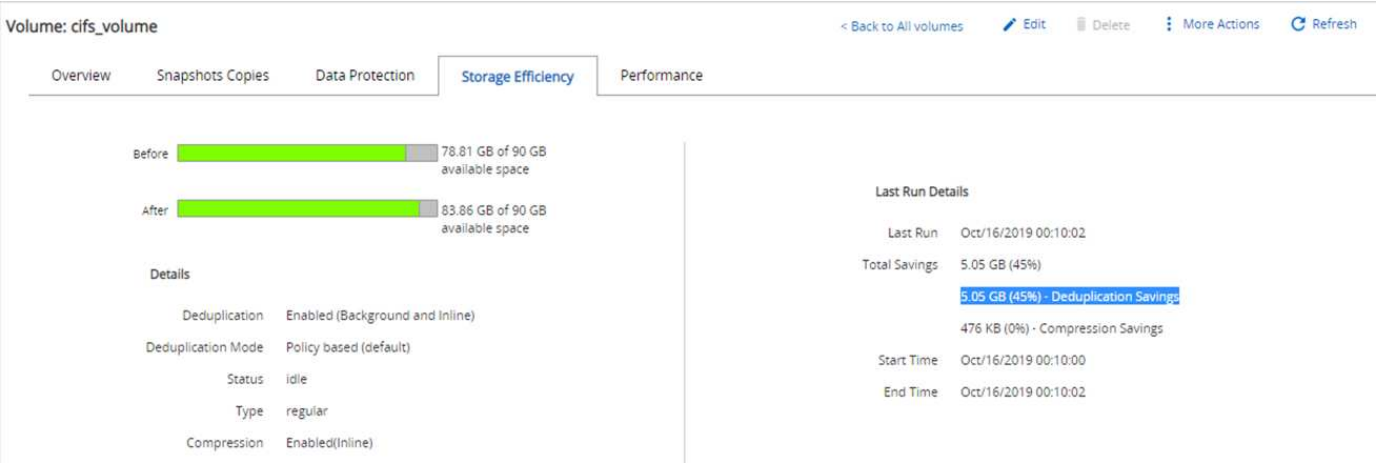
攻撃前の重複排除およびスナップショット情報

攻撃前の Snapshot コピーのストレージ効率の詳細およびサイズは、検出フェーズで参照用として示されます。

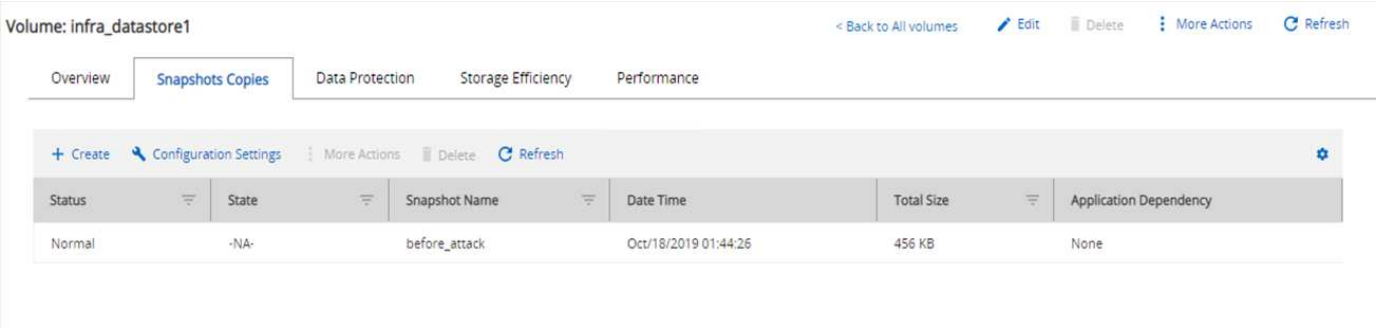
VM をホストするボリュームで重複排除を実行すると、ストレージを 19% 削減できました。



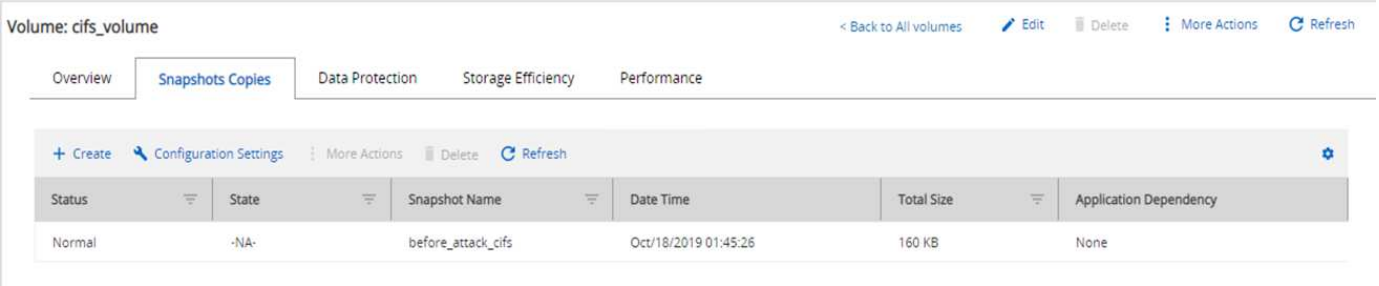
CIFS 共有「 fpolicy_share 」の重複排除により、 45% のストレージ節約を達成しました。



VM をホストしているボリュームの Snapshot コピーサイズとして、 456KB が観察されました。



CIFS 共有「 fpolicy_share 」に対しては、 160KB の Snapshot コピー・サイズが検出されました。



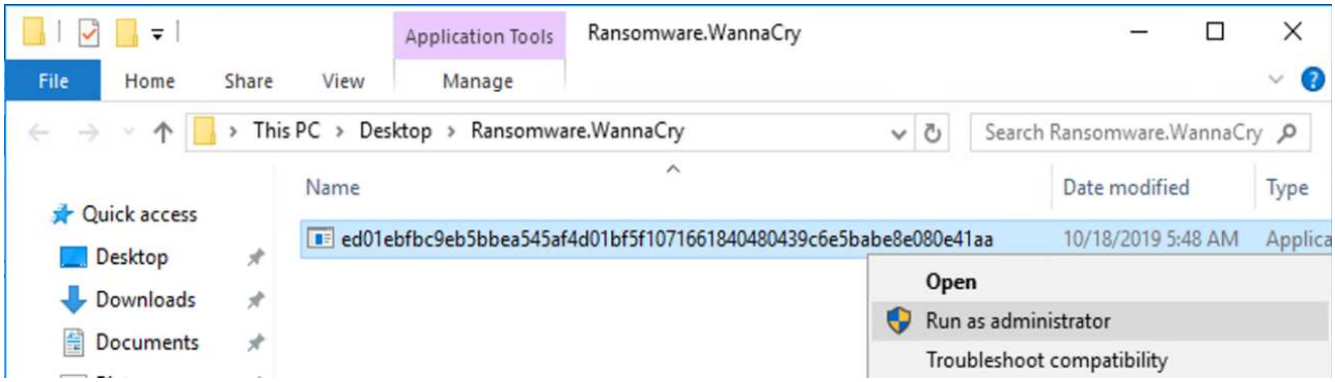
VM および CIFS 共有での WannaCry 感染

このセクションでは、 WannaCry マルウェアが FlexPod 環境にどのように導入されたか、および観察されたシステムにその後の変更がどのように加えられたかを説明します。

次の手順は、 WannaCry マルウェアバイナリが VM にどのように導入されたかを示しています。

1. 保護されたマルウェアが抽出されました。

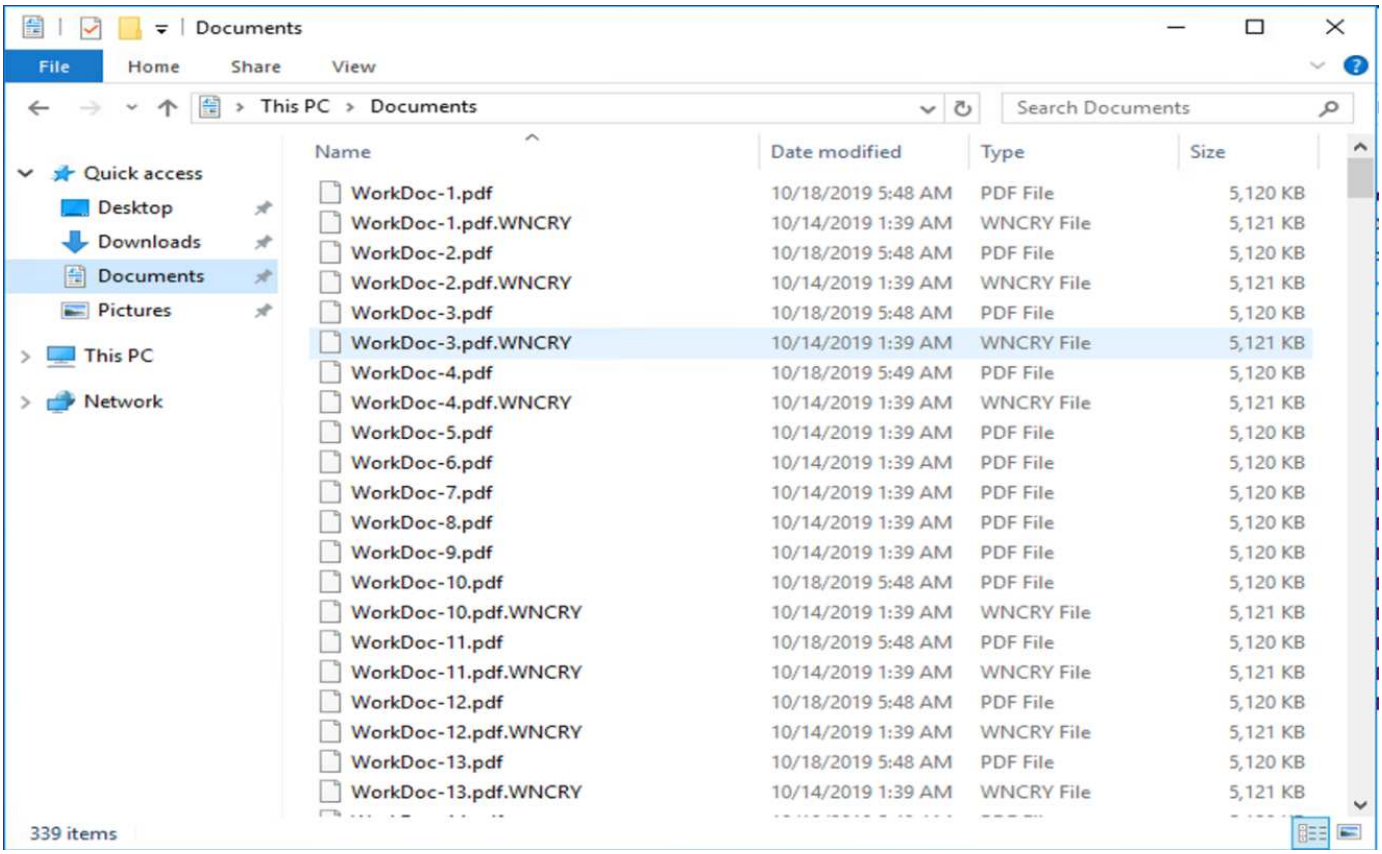
2. バイナリが実行されました。



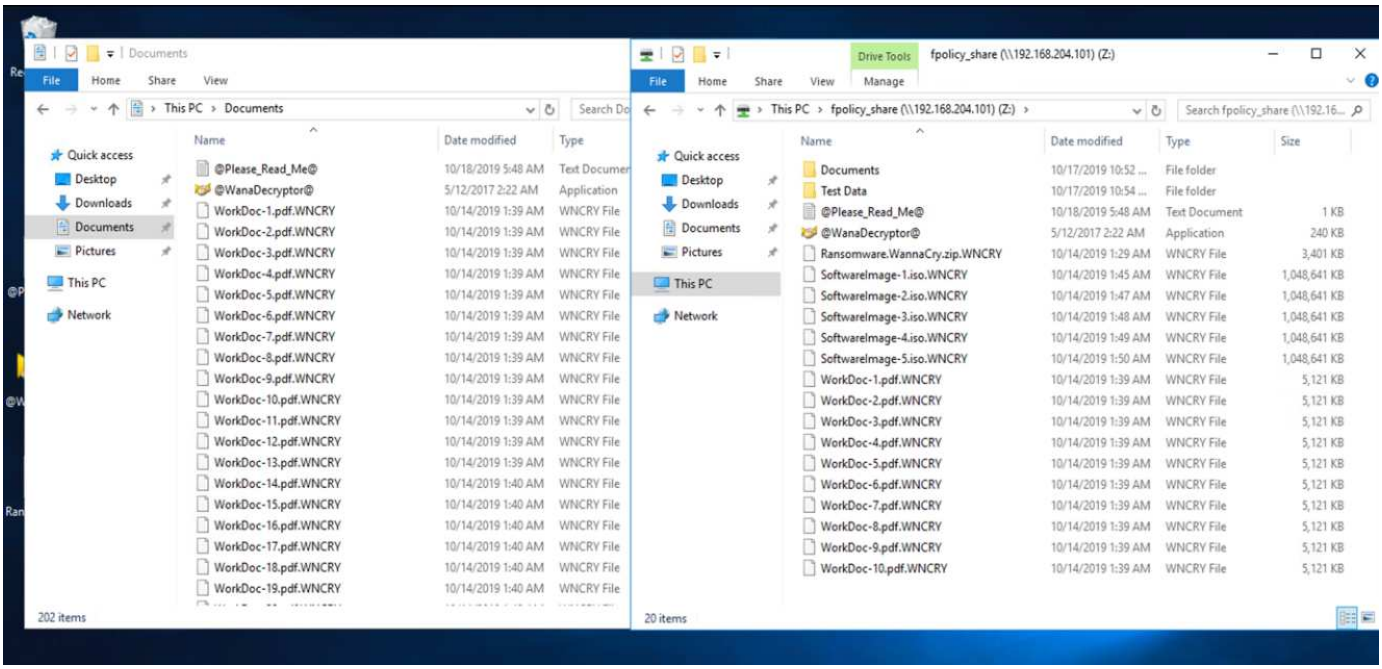
ケース **1** ： **WannaCry** は **VM** 内のファイルシステムを暗号化し、マッピングされた **CIFS** 共有を暗号化します

ローカルファイルシステムとマッピングされた CIFS 共有は、 WannaCry マルウェアによって暗号化されています。

マルウェアは WNCRY 拡張子でファイルを暗号化し始めます。



マルウェアは、ローカル VM およびマッピングされた共有内のすべてのファイルを暗号化します。

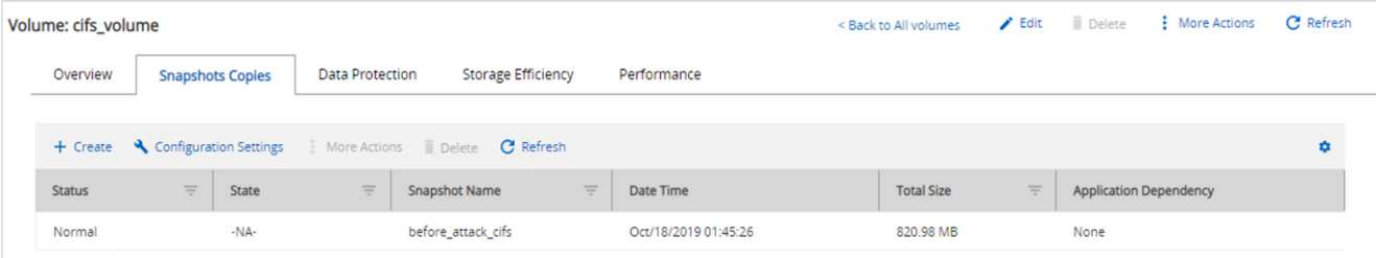


検出

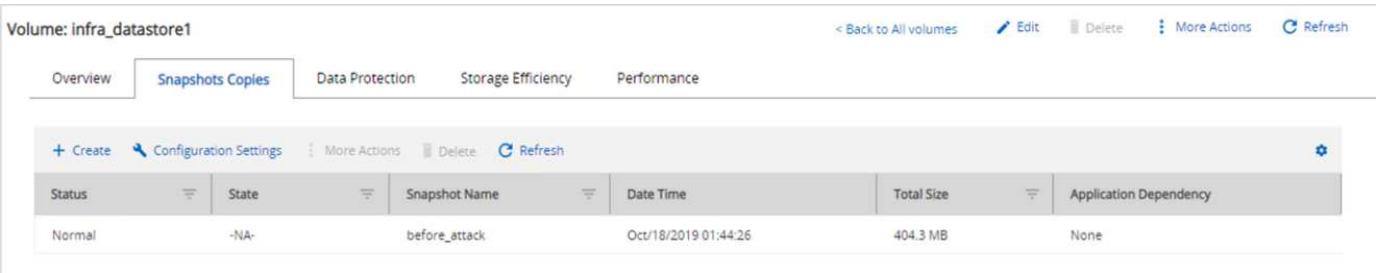
マルウェアがファイルの暗号化を開始した瞬間から、 Snapshot コピーのサイズが急激に増加し、ストレージ効率が急激に低下しました。

攻撃中に CIFS 共有をホストしているボリュームの Snapshot サイズが 820.98MB に急増していることが検出

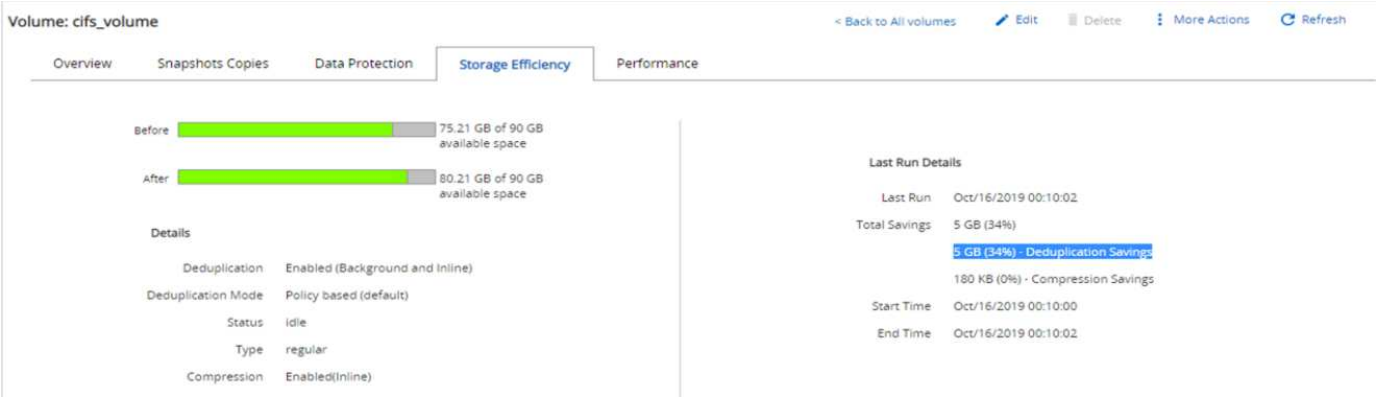
されました。



VM をホストしているボリュームの Snapshot コピーサイズが 404.3MB に増加していることが検出されました。



CIFS 共有をホストしているボリュームのストレージ効率は 34% に低下しています。



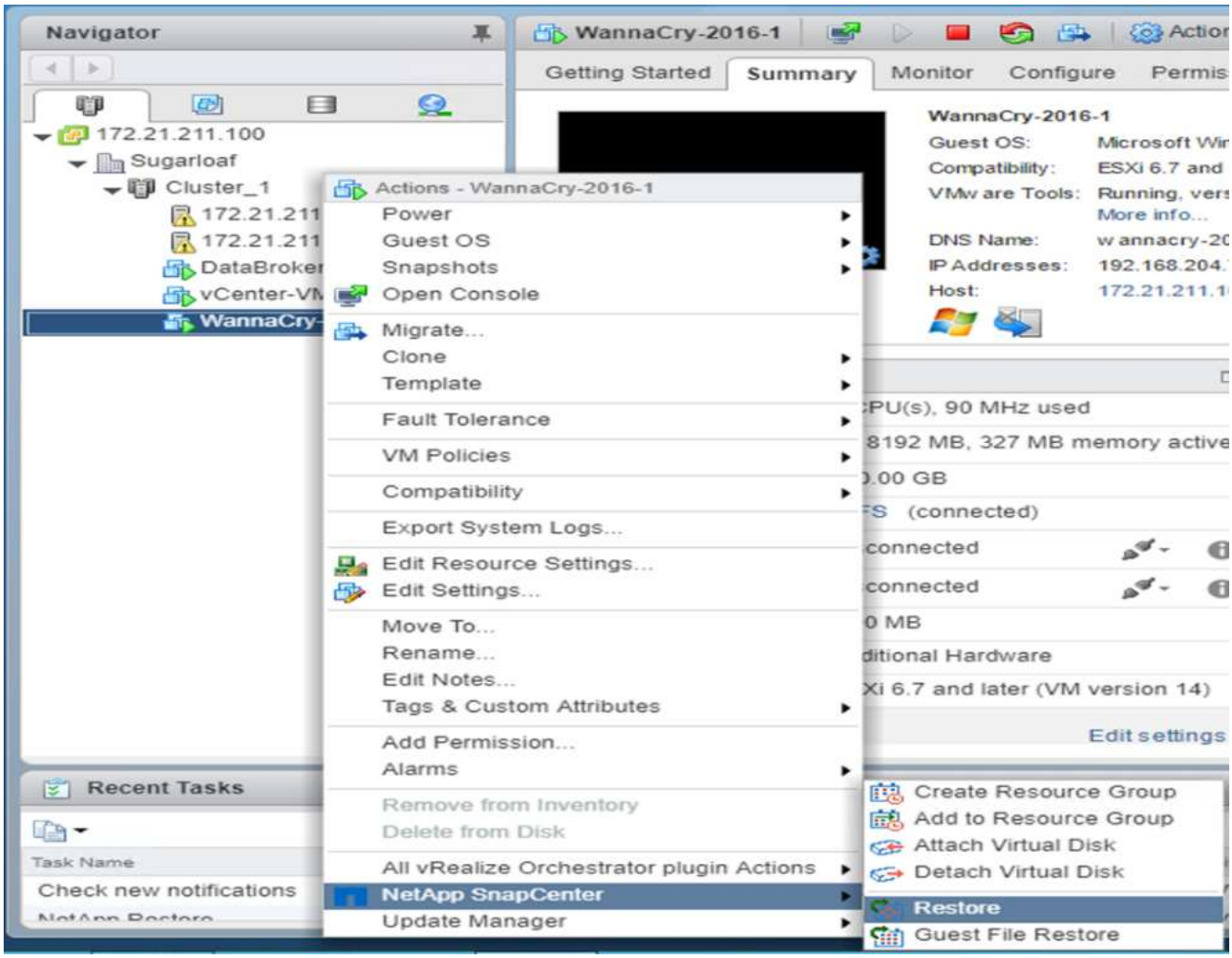
修正

攻撃の前に作成されたクリーンな Snapshot コピーを使用して、 VM およびマッピングされた CIFS 共有をリストアします。

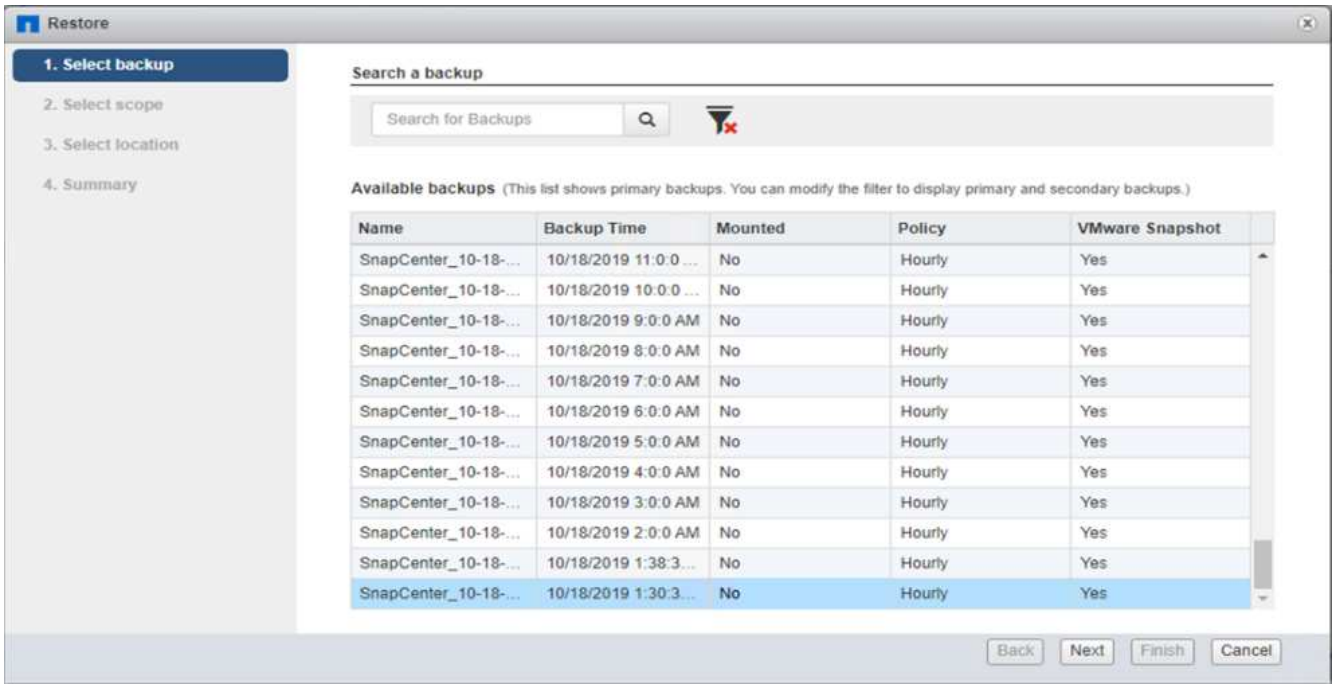
- リストア VM *

VM をリストアするには、次の手順を実行します。

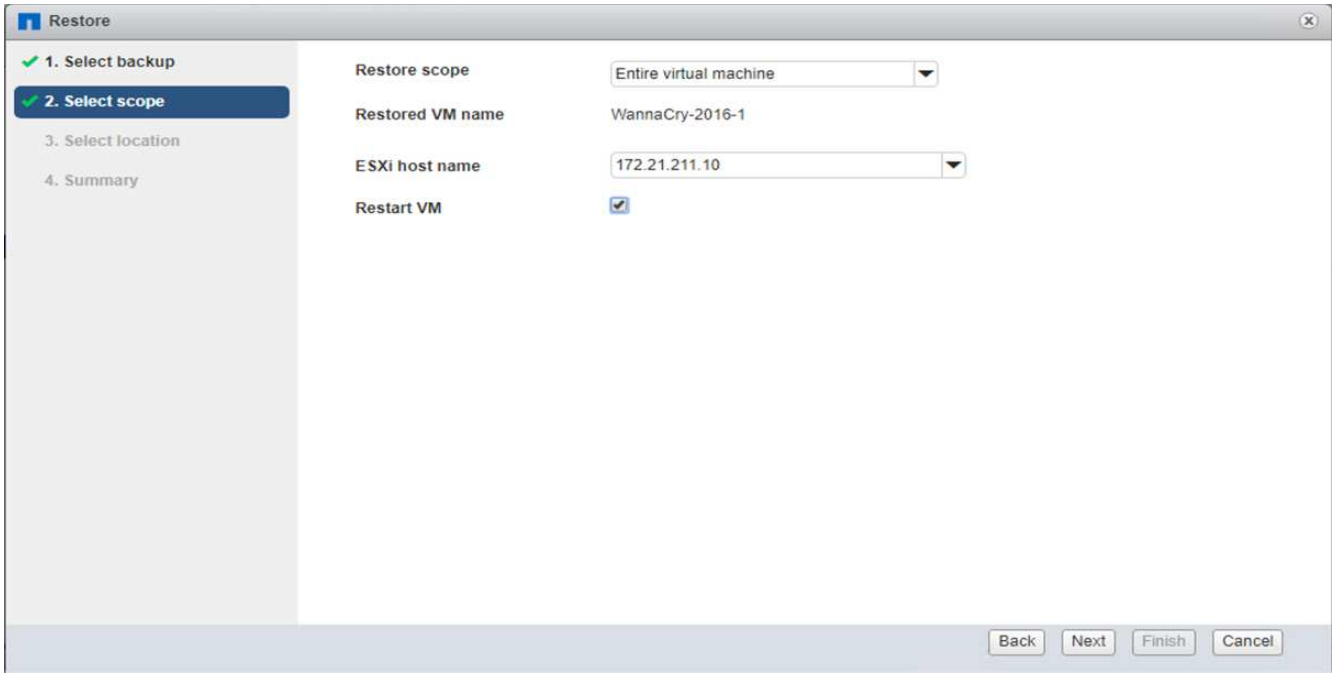
1. SnapCenter で作成した Snapshot コピーを使用して、 VM をリストアします。



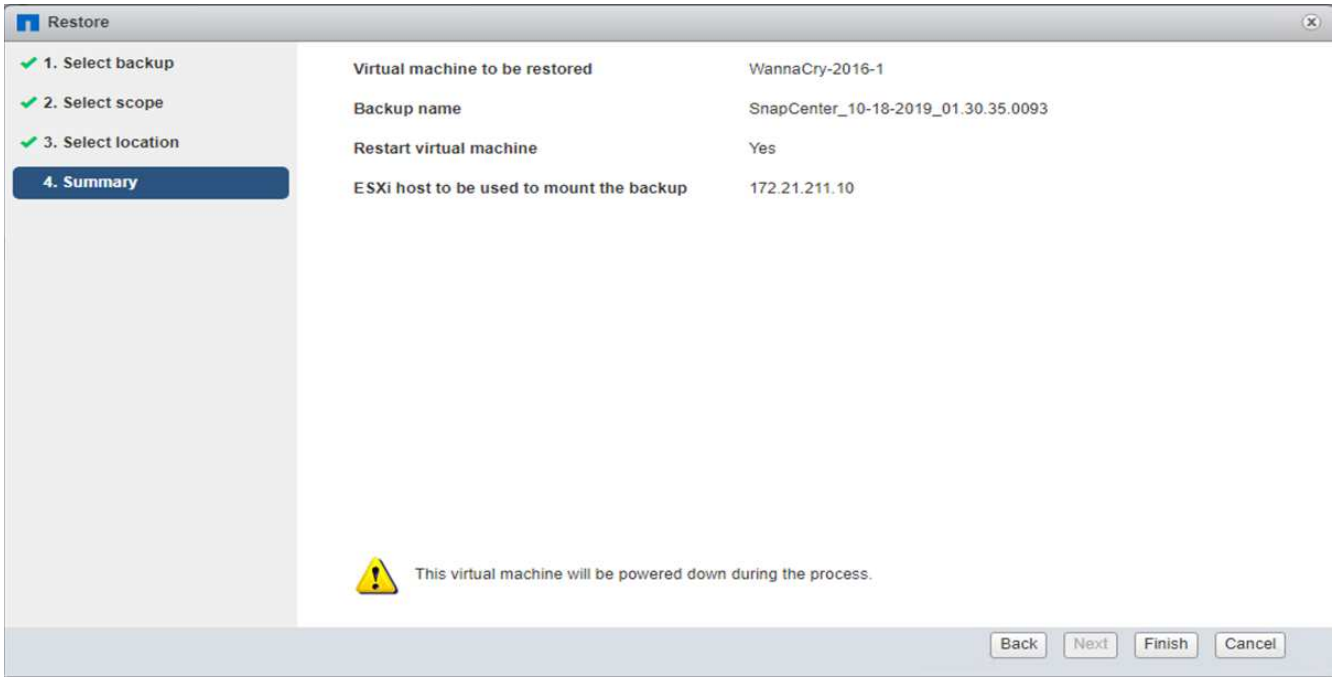
2. リストアに使用する VMware 整合性のある Snapshot コピーを選択します。



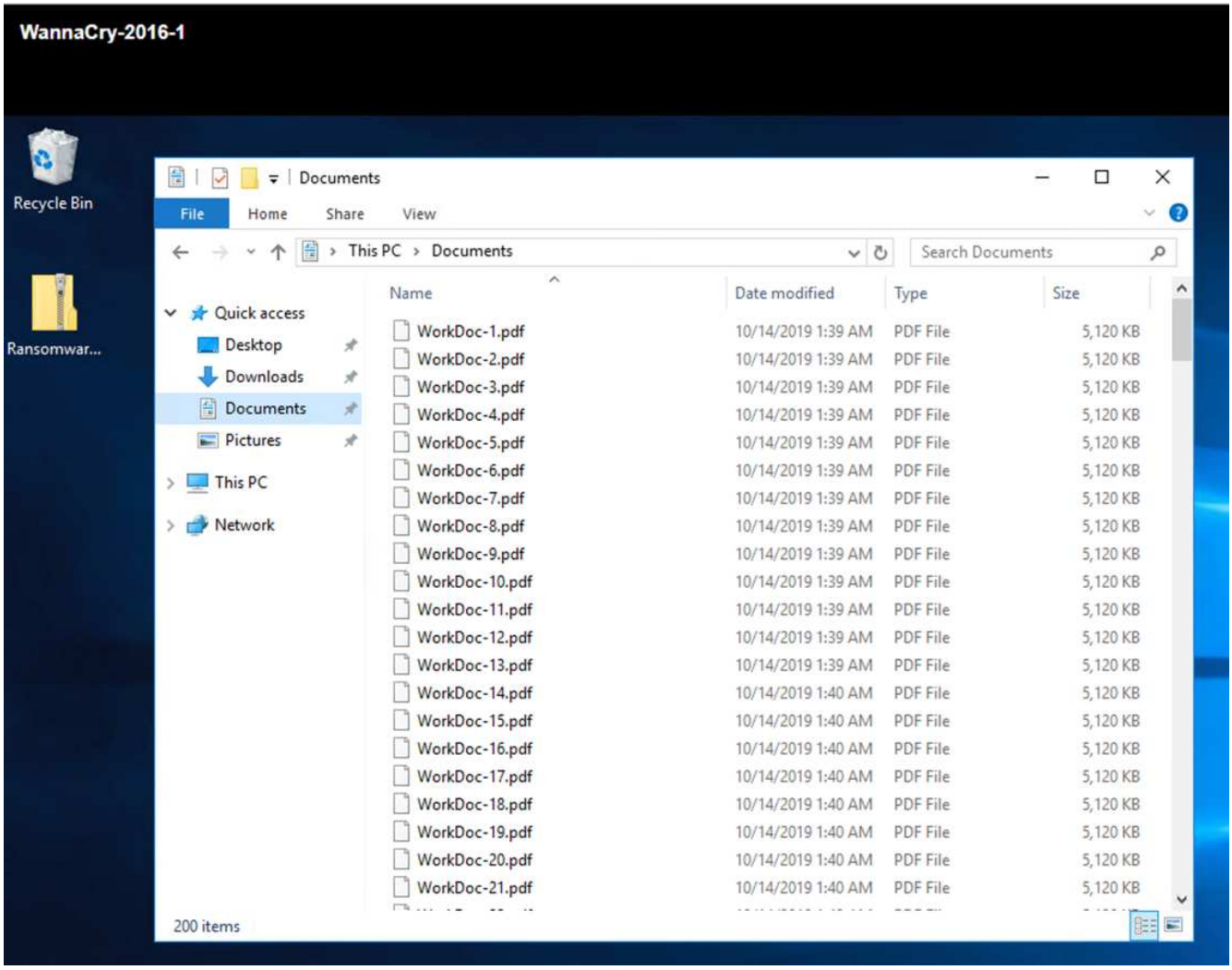
3. VM 全体がリストアされて再起動されます。



4. [完了] をクリックして、復元プロセスを開始します。



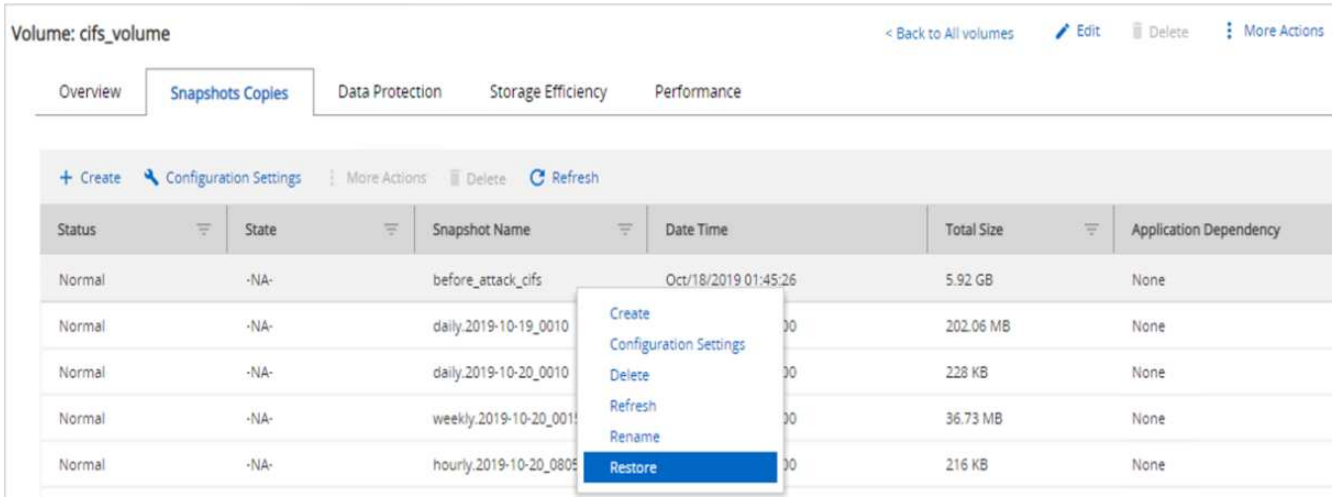
5. VM とそのファイルがリストアされます。



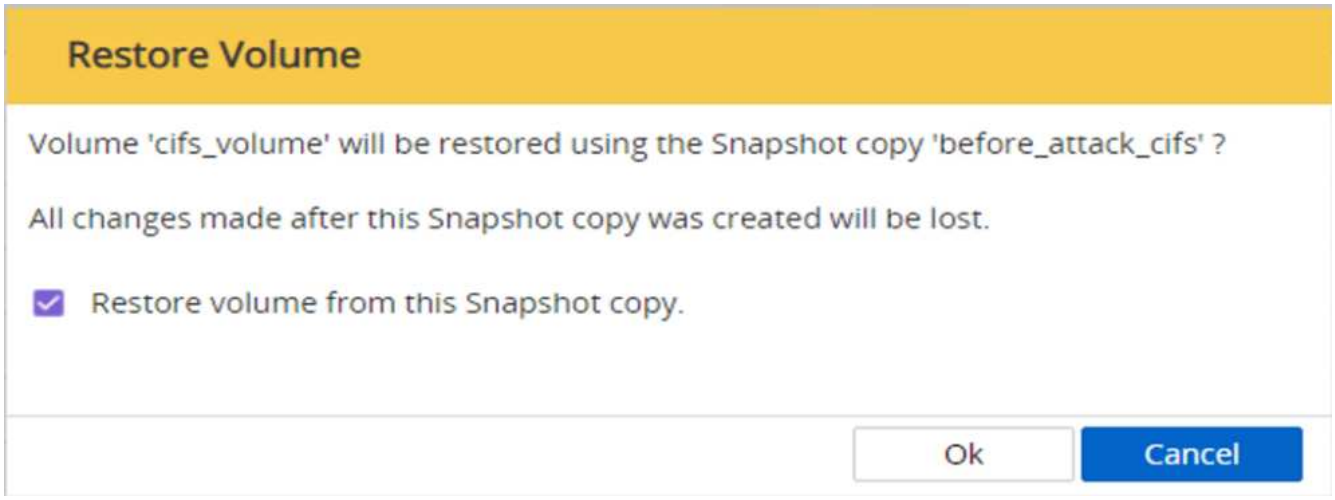
- CIFS 共有の復元 *

CIFS 共有をリストアするには、次の手順を実行します。

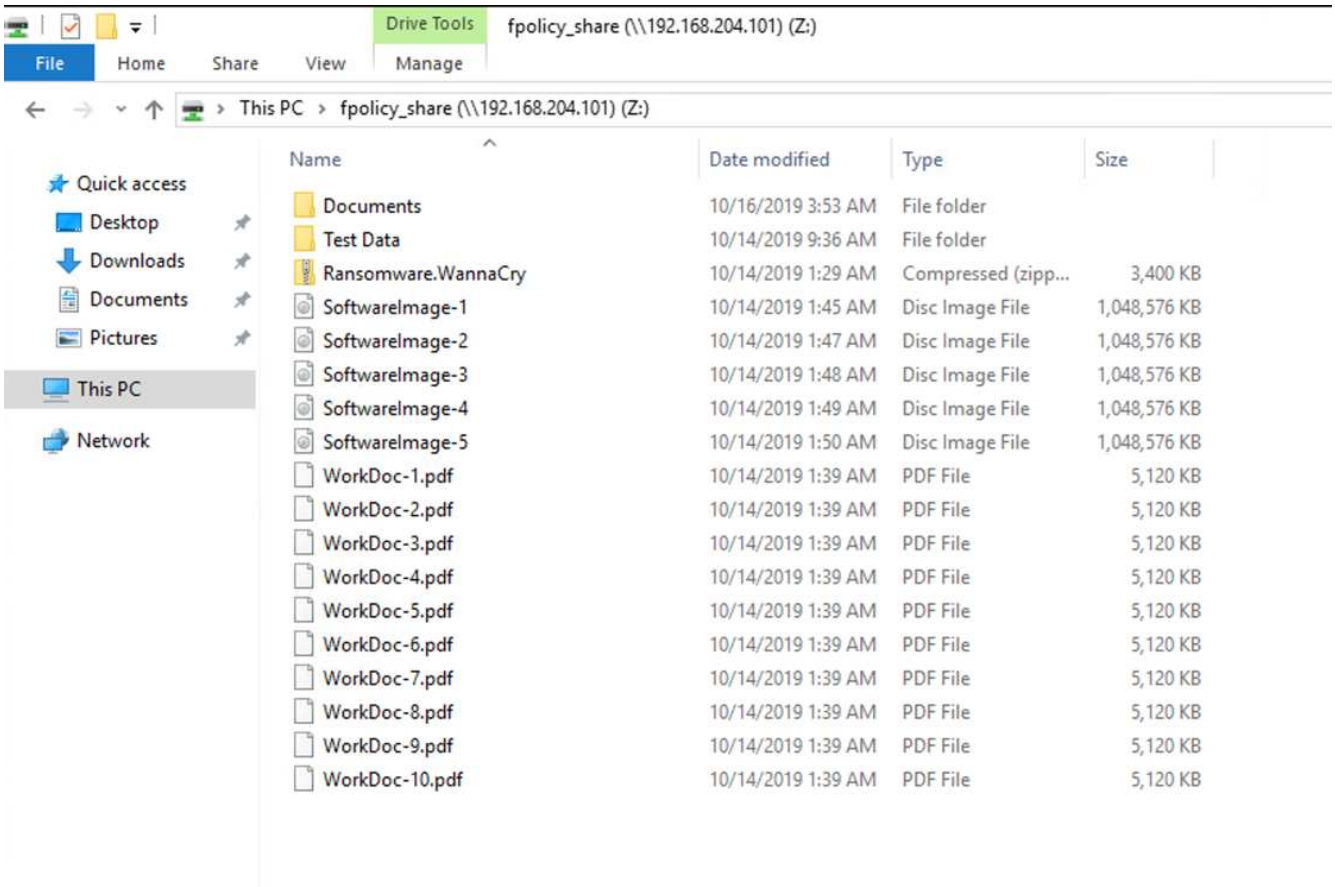
1. 攻撃の前に作成されたボリュームの Snapshot コピーを使用して、共有をリストアします。



2. [OK] をクリックしてリストア処理を開始します。



3. リストア後に CIFS 共有を表示する



ケース **2** ： **WannaCry** は **VM** 内のファイルシステムを暗号化し、 **FPolicy** で保護されているマッピングされた **CIFS** 共有を暗号化しようとします

防止

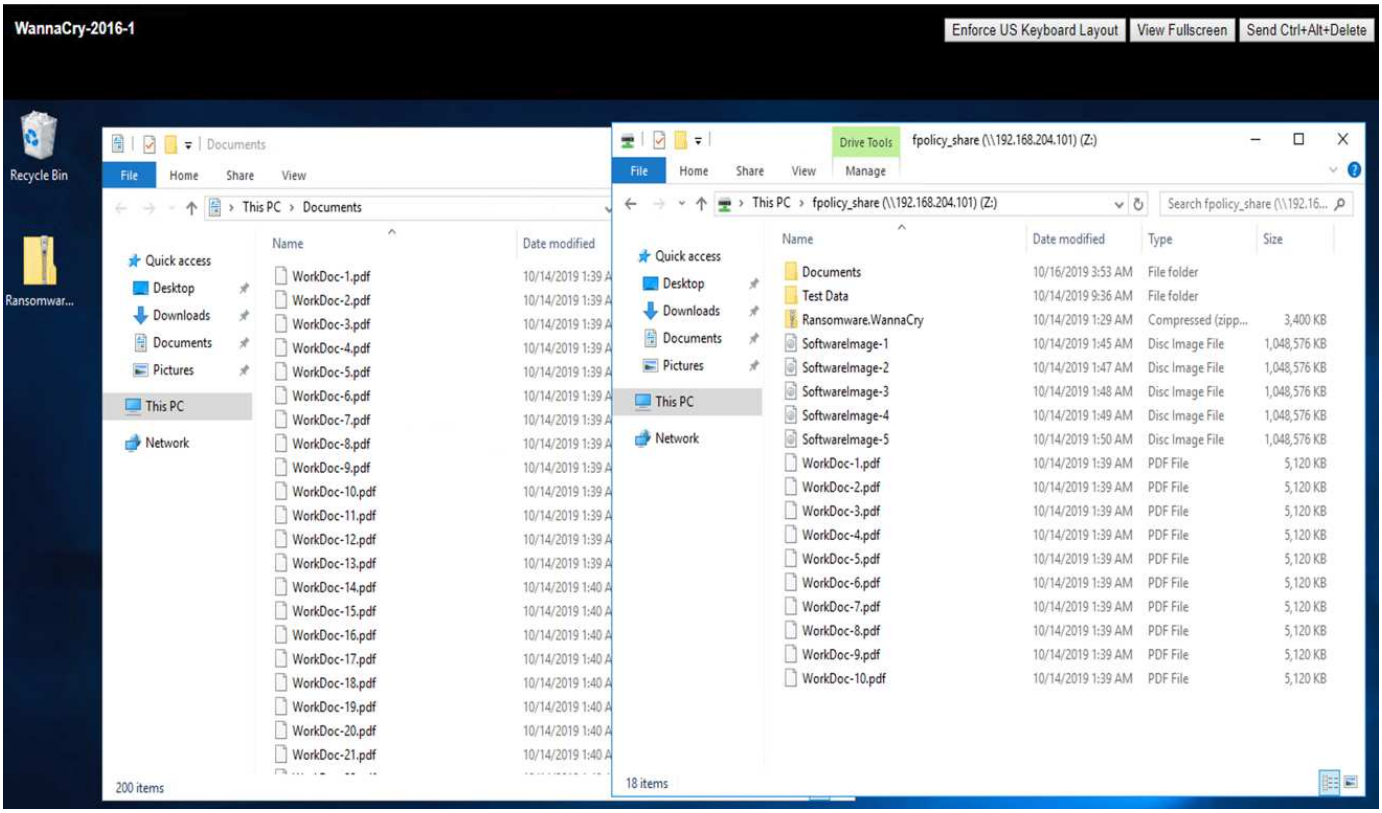
- FPolicy を設定 *

CIFS 共有に FPolicy を設定するには、 ONTAP クラスタで次のコマンドを実行します。

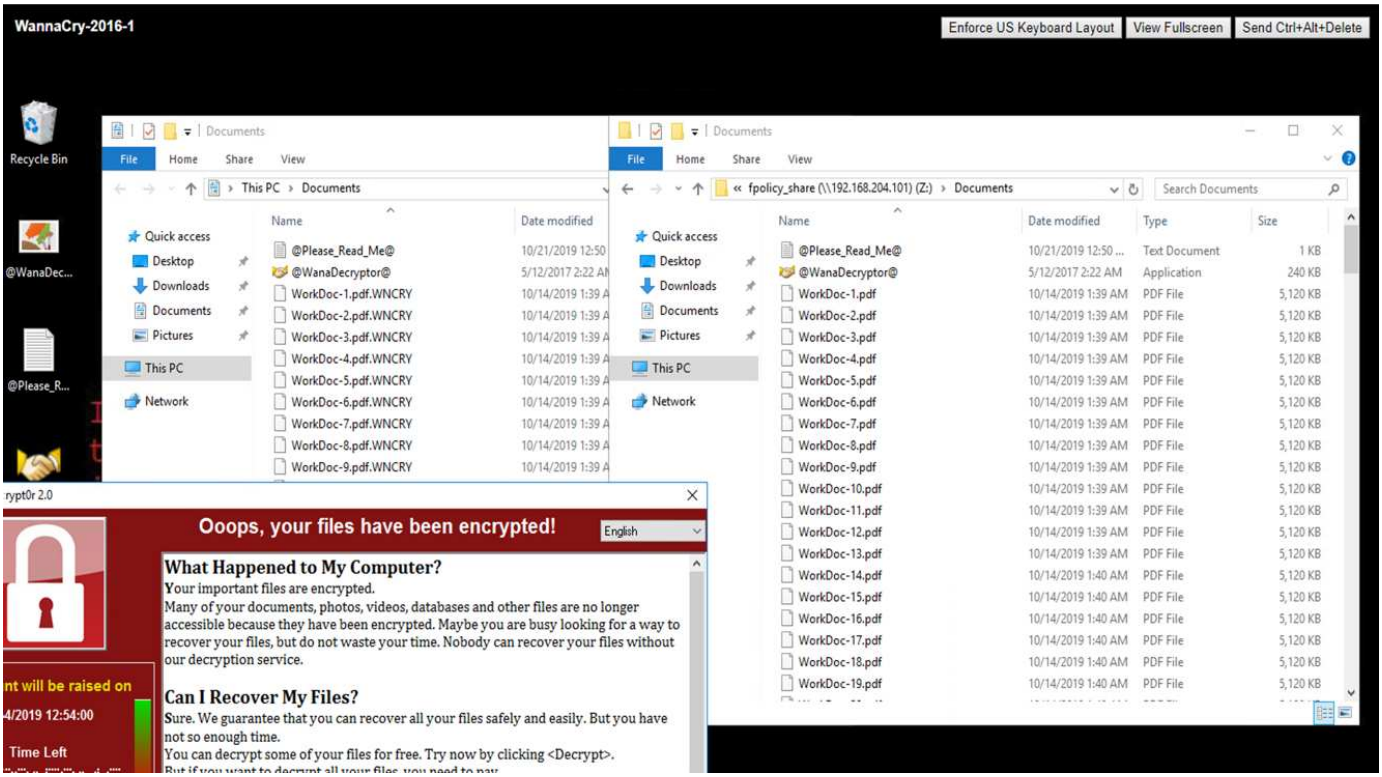
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

このポリシーでは、拡張子が WNCRY 、 Locky 、および ad4c のファイルは、ファイル操作の作成、名前変更、書き込み、または開くことができません。

攻撃前のファイルのステータスを表示します。ファイルは暗号化されておらず、クリーンなシステムにあります。



VM 上のファイルが暗号化されます。WannaCry マルウェアは CIFS 共有内のファイルの暗号化を試みますが、 FPolicy はファイルへの影響を防ぎます。



身代金を支払うことなく業務を継続

本ドキュメントで説明しているネットアップの機能は、攻撃を受けて数分以内にデータをリストアし、攻撃を未然に防ぐのに役立ちます。そのため、業務の中断を回避することができます。

Snapshot コピーのスケジュールは、目標復旧時点（ RPO ）を達成するように設定できます。Snapshot コピーベースのリストア処理は非常に高速なため、 RTO （目標復旧時間）は非常に低く抑えられます。

何よりも、攻撃の結果として身代金を支払わなくても、通常の運用にすばやく戻ることができます。

まとめ

ランサムウェアは組織犯罪の製品であり、攻撃者は倫理的に行動しません。身代金を受け取ったあとも、復号化の鍵を渡さないケースもあります。被害者は、データだけでなく多額の金銭も失うだけでなく、本番環境のデータ損失に伴う影響も被ることになります。

に従って "Forbes の記事です"では、身代金を支払ったあとにデータが戻ってくるのは、ランサムウェア攻撃者のわずか 19% です。そのため、攻撃が発生した場合に身代金を支払わないことを推奨します。金銭的な金銭的価値を提供することで、攻撃者のビジネスモデルに対する信頼が強化されます。

データのバックアップとリストアは、ランサムウェアからのリカバリの重要な要素です。そのため、ビジネス計画の不可欠な要素として含める必要があります。攻撃が発生した場合に復旧機能に妥協がないように、これらのオペレーションの実装には予算を割り当てる必要があります。

重要なのは、このプロセスで適切なテクノロジパートナーを選択することです。 FlexPod は、オールフラッシュ FAS システムで追加コストを発生させることなく、必要な機能のほとんどをネイティブに提供します。

謝辞

このドキュメントの作成にあたり、以下の方々のご協力に感謝します。

- ネットアップ、 Jorge Gomez Navarrete 氏
- ネットアップ、 Ganesh Kamath

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。

- NetApp Snapshot ソフトウェア

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- SnapCenter によるバックアップ管理

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- SnapLock によるデータコンプライアンス

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- ネットアップの製品マニュアル

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco Advanced Malware Protection （ AMP ）

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco StealthWatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

医療機関向けの **FIPS 140-2** セキュリティ準拠の **FlexPod** 解決策

TR-4892 ：『 FIPS 140-2 security Compliant FlexPod 解決策 **for HealthCare** 』

Cisco 、 NetApp John McAbel 、 JayaKishore Esanakula 氏

経済・臨床医療法（ HITECH ）の医療情報技術には、 Federal Information Processing Standard （ FIPS ） 140-2 認証済みの電子保護医療情報（ ePHI ）暗号化が必要です。ヘルス情報テクノロジ（ HIT ）アプリケーションおよびソフトウェアは、相互運用性プログラム（旧称は有意義な使用インセンティブプログラム）認定を取得するために FIPS 140-2 に準拠している必要があります。対象となるプロバイダーおよび病院は、メディケアおよびメディケイドインセンティブを受けるために FIPS 140-2 （レベル 1 ）に準

拠した HIT を使用し、メディケアおよびメディケイドセンター（ CMS ）からの払い戻しペナルティを回避する必要があります。FIPS 140-2 認定暗号化アルゴリズムは、に求められる技術的な保護手段として認定されています "セキュリティルール" Health Information Portability and Accountability Act （ HIPAA ：医療情報の相互運用性と説明責任に関する法律）。

FIPS 140-2 は、米国機密情報を保護するハードウェア、ソフトウェア、およびファームウェアの暗号モジュールのセキュリティ要件を設定する政府標準。米国では、この規格への準拠が義務付けられていますまた、金融サービスや医療などの規制産業でもよく使用されています。本テクニカルレポートでは、 FIPS 140-2 のセキュリティ標準を高水準で理解する方法を紹介します。また、医療機関が直面しているさまざまな脅威を理解するのにも役立ちます。最後に、このテクニカルレポートでは、 FIPS 140-2 準拠の FlexPod システムを使用して FlexPod コンバージドインフラに導入した医療資産を保護する方法について説明します。

適用範囲

このドキュメントは、 FIPS 140-2 のセキュリティコンプライアンスを必要とする 1 つ以上の医療 IT アプリケーションやソリューションをホスティングするための、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus 、 Cisco MDS 、および NetApp ONTAP ベースの FlexPod インフラの技術概要をまとめたものです。

対象者

本ドキュメントは、医療業界の技術リーダー、 Cisco とネットアップのパートナーソリューションエンジニア、およびプロフェッショナルサービス担当者を対象としています。本ドキュメントは、コンピューティングとストレージのサイジングの概念に加え、医療の脅威、医療セキュリティ、医療 IT システム、 Cisco UCS 、ネットアップストレージシステムに関する技術的な知識があることを前提としています。

"次は、医療業界におけるサイバーセキュリティの脅威です。"

医療業界におけるサイバーセキュリティの脅威

"前へ：はじめに。"

問題が発生するたびに、新型コロナウイルス感染症の流行により、このような機会の一例が提示されます。に従って "レポート" 新型コロナウイルス感染症対策は、米保健福祉省（ HHS ）サイバーセキュリティプログラムによってランサムウェア攻撃の数が増加したことに起因しています。2020 年 3 月第 3 週に 6,000 の新しいインターネット・ドメインが登録されました。ドメインの 50% 以上がマルウェアをホストしています。ランサムウェア攻撃は、 2020 年に医療データの侵害が発生し、 630 を超える医療機関と約 2,900 万件の医療記録に影響を及ぼしています。19 人のレイカー / サイトがこの伸長率を倍増させた。医療業界では、 2020 年にデータ侵害が最も多かったのは 24.5% です。

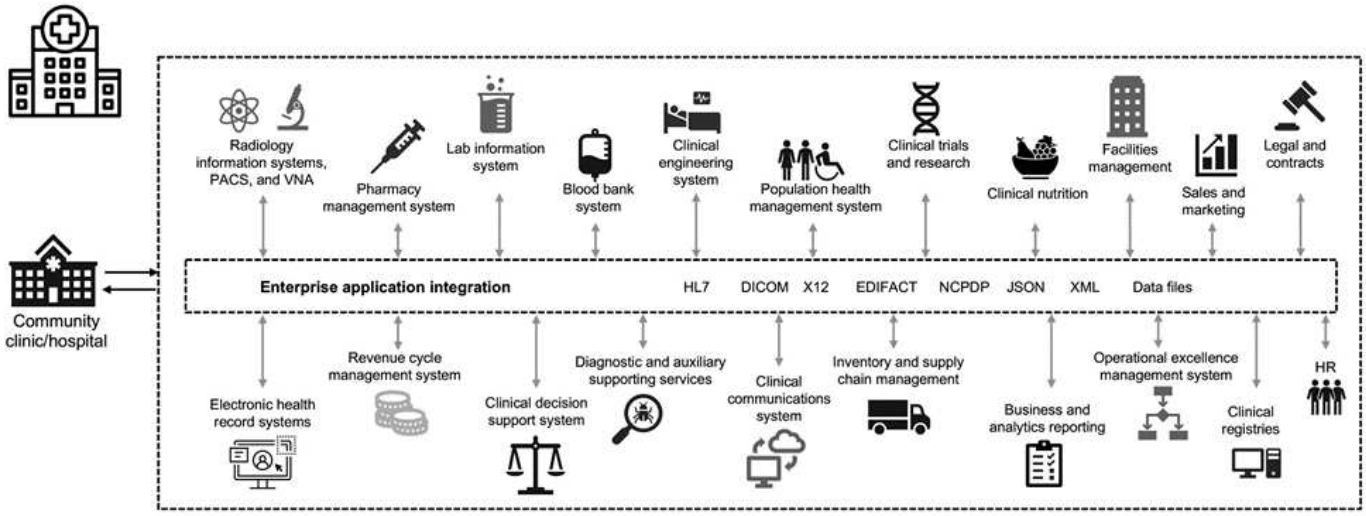
悪意のあるエージェントは、情報を販売するか、破壊または暴露を脅かして、保護された健康情報（ PHI ）のセキュリティおよびプライバシーを侵害しようとしました。ターゲットと大量ブロードキャストの試行は、ePHI への不正アクセスを得るために頻繁に行われます。2020 年後半の患者記録のうち、約 75% がビジネス関係者の侵害によるものでした。

次のリストの医療機関は、悪意のあるエージェントの標的になっていました。

- 病院システム

- ライフサイエンスラボ
- 研究室
- リハビリテーション施設
- 地域の病院や診療所

医療機関を構成するアプリケーションの多様性は否定できず、複雑さもますます増大しています。情報セキュリティ・オフィスは ' 膨大な IT システムと資産のガバナンスを提供するという課題に直面しています次の図は、一般的な病院システムの臨床的能力を示しています。



患者データはこの画像の中心にあります。患者データの消失と、デリケートな医療条件に関連する病状の消失は非常に現実的です。その他の重要な問題には、社会的排除、ブラックリスト、プロファイリング、ターゲットマーケティングの脆弱性、不正利用、支払者の権限を超えた医療情報に関する支払者に対する潜在的な金銭的責任などがあります。

医療への脅威は、本質的に多次元的なものであり、影響を及ぼします。世界各国の政府は、 ePHI を保護するためにさまざまな規定を制定しました。医療への脅威の悪影響と進化する性質により、医療機関はすべての脅威を防御することが困難になります。

以下に、医療業界で特定されている一般的な脅威のリストを示します。

- ランサムウェア攻撃
- 機密情報を含む機器またはデータの紛失または盗難
- フィッシング攻撃
- 患者の安全性に影響を与える可能性のある、接続された医療機器に対する攻撃
- 電子メールによるフィッシング攻撃
- 機器またはデータの紛失または盗難
- リモートデスクトッププロトコルの妥協
- ソフトウェアの脆弱性

医療機関は、デジタルエコシステムと同様に複雑な法的規制の環境で運用されています。この環境には、以下が含まれますが、これらに限定されません。

- 国立コーディネータオフィス（医療技術担当） ONC 認定電子医療情報技術相互運用性標準
- Medicare アクセスおよび子供の健康保険プログラムの再認可法 (MACRA) / 有意義な使用
- 食品医薬品局（ FDA ）に基づく複数の義務
- 共同委員会認定プロセス
- HIPAA の要件
- Hitch の要件
- 支払者の最低許容リスク基準
- プライバシーとセキュリティのルールを記述します
- 連邦情報セキュリティの近代化法の要件は、米国立衛生研究所などの機関を通じて、連邦政府との契約および研究助成金に組み込まれています
- クレジットカード業界の データ セキュリティ 標準 (PCI-DSS)
- 薬物乱用および精神保健管理（ SAMHSA ）の要件
- 金融処理法「 Gramm-Leach-Bliley Act
- 関連組織へのサービス提供に関するスターク法
- 高等教育に参加する機関向けの Family Educational Rights and Privacy Act （ FERPA ）
- 遺伝情報差別禁止法（ GINA ）
- 欧州連合の新しい一般データ保護規則（ GDPR ）

セキュリティアーキテクチャ標準は急速に進化しており、悪意のある攻撃者が医療情報システムに影響を与えないようになっています。その 1 つが FIPS 140-2 であり、 National Institute of Standards and Technology （ NIST ；米国標準技術研究所）で定義されています。FIPS 140-2 では、米国政府が詳しく公開されています政府による暗号モジュールの要件セキュリティ要件は、暗号モジュールの安全な設計および実装に関連する領域を対象としており、 HIT に適用できます。適切に定義された暗号化境界により、暗号モジュールを最新の状態に保ちながら、セキュリティ管理を容易にすることができます。これらの境界は、悪意のある攻撃者によって簡単に悪用される可能性のある暗号モジュールの脆弱性を防止するのに役立ちます。また、標準の暗号モジュールを管理するときに人為的ミスを防止することもできます。

NIST と Communications Security Establishment （ CSE ）は、 FIPS 140-2 認定レベルの暗号モジュールを認定する暗号モジュール検証プログラム（ CMVP ）を設立しました。FIPS 140-2 認定モジュールを使用する場合、連邦政府機関は、移動中だけでなく保管中も機密データや重要なデータを保護する必要があります。多くの医療システムでは、機密情報や貴重な情報を保護することが成功したため、 FIPS 140-2 暗号化モジュールを使用して、法的に必要な最低限のセキュリティレベルを超えて ePHI を暗号化することを選択しています。

FlexPod の FIPS 140-2 機能の活用と実装にかかる時間は、数日から数時間です。FIPS に準拠するようになることは、規模に関係なく、ほとんどの医療機関に求められる範囲内です。明確に定義された暗号化の境界と、十分に文書化されたシンプルな実装手順により、 FIPS 140-2 準拠の FlexPod アーキテクチャは、インフラストラクチャの強固なセキュリティ基盤を確立し、シンプルな拡張機能によってセキュリティ上の脅威に対する保護をさらに強化できます。

"次の例は、 FIPS 140-2 の概要を示しています。"

FIPS 140-2 の概要

"前の記事：医療業界におけるサイバーセキュリティの脅威。"

"FIPS 140-2" コンピュータおよび通信システムの機密情報を保護するセキュリティシステム内で使用される暗号モジュールのセキュリティ要件を指定します。暗号モジュールは、ハードウェア、ソフトウェア、ファームウェア、またはその組み合わせのセットである必要があります。FIPS 環境 暗号化アルゴリズム、キー生成、および暗号化境界内に含まれるキー管理ツール。FIPS 140-2 は、製品、アーキテクチャ、データ、エコシステムではなく、暗号モジュールに適用される点に注意してください。暗号モジュールは、このドキュメントで後述する重要な用語で定義されており、承認されたセキュリティ機能を実装する特定のコンポーネント（ハードウェア、ソフトウェア、ファームウェアのいずれか）です。また、 FIPS 140-2 では 4 つのレベルが規定されています。承認された暗号化アルゴリズムは、すべてのレベルで共通です。各セキュリティレベルの主な要素と要件は次のとおりです。

- * セキュリティレベル 1 *
  - 暗号モジュールの基本的なセキュリティ要件を指定します（少なくとも 1 つの承認されたアルゴリズムまたはセキュリティ機能が必要です）。
  - レベル 1 には、本番グレードのコンポーネントの基本要件を超える物理的なセキュリティメカニズムは必要ありません。
- * セキュリティレベル 2 *
  - コーティングやシール、取り外し可能なカバーや暗号モジュールのドアのロックなどの不正開封防止ソリューションを使用して、改ざん防止の要件を追加することで、物理的なセキュリティメカニズムを強化します。
  - 少なくとも、ロールベースアクセスコントロール（ RBAC ）が必要です。この RBAC では、暗号化モジュールがオペレータまたは管理者の許可を認証して、特定のロールを引き受け、対応する一連の機能を実行します。
- * セキュリティレベル 3 *
  - レベル 2 の不正改ざん防止要件を基に構築され、暗号化モジュール内の重要なセキュリティパラメータ（ CSP ）へのアクセスを防止しようとします。
  - レベル 3 で必要とされる物理的なセキュリティメカニズムは、物理的なアクセス、または暗号モジュールの使用または変更の試みを検出して応答する可能性が高いことを目的としています。たとえば、強力なエンクロージャ、改ざん検出、応答回路などがあり、暗号モジュールの取り外し可能なカバーを開いたときにすべてのプレーンテキスト CSP をゼロにします。
  - レベル 2 で指定された RBAC メカニズムのセキュリティを強化するために、 ID ベースの認証メカニズムが必要です。暗号モジュールは、オペレータの ID を認証し、オペレータが役割を使用して役割の機能を実行する権限を持っていることを確認します。
- * セキュリティレベル 4 *
  - FIPS 140-2 で最高レベルのセキュリティ。
  - 物理的に保護されていない環境での処理に最も有効なレベルです。
  - このレベルでは、物理的なセキュリティメカニズムは、物理的なアクセスでの不正な試みを検出して応答する責任を持つ、暗号モジュールに関する完全な保護を提供することを目的としています。
  - 暗号モジュールの侵入や露出は検出の可能性が高く、セキュアでない CSP やプレーンテキスト CSP がすべて初期化される可能性が高くなります。

"次に、コントロールプレーンとデータプレーンを比較します。"

コントロールプレーンとデータプレーンの比較

"以前： FIPS 140-2 の概要。"

FIPS 140-2 戦略を実装する場合は、保護対象を理解することが重要です。これは、コントロールプレーンとデータプレーンの 2 つの領域に簡単に分割できます。コントロールプレーンとは、ネットアップストレージコントローラ、 Cisco Nexus スイッチ、 Cisco UCS サーバへの管理アクセスなど、 FlexPod システム内のコンポーネントの制御と運用に影響する要素のことです。このレイヤでの保護は、管理者がデバイスへの接続や変更を行うために使用できるプロトコルと暗号化暗号化暗号化暗号化方式を制限することによって提供されます。データプレーンとは、 FlexPod システム内の PHI などの実際の情報を指します。これは、保存データを暗号化することで保護されます。 FIPS では、使用中の暗号モジュールが標準に準拠していることを確認できます。

"次に、 FlexPod の Cisco UCS コンピューティングと FIPS 140-2 を実行します。"

FlexPod Cisco UCS のコンピューティングと FIPS 140-2

"前：コントロールプレーンとデータプレーンの比較。"

FlexPod アーキテクチャは、 FIPS 140-2 に準拠した Cisco UCS サーバを使用して設計できます。米国に準拠しています…NIST 、 Cisco UCS サーバは、 FIPS 140-2 レベル 1 準拠モードで動作します。FIPS 準拠の Cisco コンポーネントの一覧については、を参照してください "シスコの FIPS 140 ページ"。Cisco UCS Manager は FIPS 140-2 認定済みです。

Cisco UCS とファブリックインターコネクト

Cisco UCS Manager は、 Cisco Fabric Interconnect （ FI ）から導入され、実行されます。

Cisco UCS および FIPS を有効にする方法の詳細については、を参照してください "Cisco UCS Manager のマニュアル"。

各ファブリック A および B で Cisco ファブリックインターコネクト上で FIPS モードをイネーブルにするには、次のコマンドを実行します。

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> Cisco UCS Manager Release 3.2(3) より前のリリースのクラスタの FI を FI に置き換えるには、交換用の FI をクラスタに追加する前に、既存の FI で FIPS モードをディセーブル（「 FIPS-mode 」をディセーブル）にします。クラスタが形成されると、 Cisco UCS Manager のブートアップの一環として、 FIPS モードが自動的に有効になります。

シスコは、コンピューティングまたはアプリケーションレイヤに実装可能な次の主要製品を提供しています。

- * エンドポイント向けの Cisco Advanced Malware Protection （ AMP ）。 * Microsoft Windows および Linux オペレーティングシステムでサポートされているこの解決策 は、防止、検出、および応答機能を統合しています。このセキュリティソフトウェアは、セキュリティ侵害の防止、侵入ポイントでのマルウェアのブロック、ファイルおよびプロセスのアクティビティの継続的な監視と分析を行い、フロントライン防御を回避できる脅威を迅速に検出、阻止、修復します。AMP の Malicious Activity Protection （ MAP ）コンポーネントは、すべてのエンドポイントアクティビティを継続的に監視し、エンドポイント上の実行中のプログラムのランタイム検出と異常な動作のブロックを提供します。たとえば、エンドポイントの動作がランサムウェアを示している場合、攻撃の原因となっているプロセスは終了し、エンドポイントの暗号化を防ぎ、攻撃を停止します。
- * 電子メールセキュリティのための AMP 。 * 電子メールはマルウェアを拡散させ、サイバー攻撃を実行するための主要な手段となっています。平均して、 1 日に約 1 、 000 億通の電子メールが交換されます。これにより、攻撃者はユーザーのシステムに非常に優れた侵入ベクトルを与えることができます。そのため、この種の攻撃を防御することは絶対に不可欠です。AMP は、ゼロデイ攻撃や悪意のある添付ファイルに隠された不潔なマルウェアなどの脅威を電子メールで分析します。また、業界をリードする URL インテリジェンスを使用して、悪意のあるリンクに対抗します。スピアフィッシング、ランサムウェア、その他の高度な攻撃から高度な保護を提供します。
- * 次世代侵入防御システム（ NGIPS ）。 * Cisco firepower NGIPS は、データセンターの物理アプライアンスとして、または VMware （ NGIPSv for VMware ）の仮想アプライアンスとして導入できます。この非常に効果的な侵入防御システムは、信頼性の高いパフォーマンスと低い総所有コストを実現します。オプションのサブスクリプションライセンスで脅威からの保護を拡張して、 AMP 、アプリケーションの可視化と制御、および URL フィルタリング機能を提供できます。仮想化された NGIPS は、仮想マシン（ VM ）間のトラフィックを検査し、リソースが限られたサイトで NGIPS ソリューションの導入と管理を容易にして、物理資産と仮想資産の両方の保護を強化します。

"次のセクションでは、 FlexPod のシスコネットワークと FIPS 140-2 について説明します。"

FlexPod シスコのネットワークおよび FIPS 140-2

"前のリリース： FlexPod Cisco UCS のコンピューティングと FIPS 140-2"

Cisco MDS

ソフトウェア 8.4.x を搭載した Cisco MDS 9000 シリーズプラットフォームは、です "FIPS 140-2 に準拠しています"。Cisco MDS は、 SNMPv3 および SSH 用の暗号モジュールおよび次のサービスを実装しています。

- 各サービスをサポートするセッション確立
- 各サービスの主要な派生機能をサポートする、基盤となるすべての暗号化アルゴリズム
- 各サービスのハッシュ化
- 各サービスの対称暗号化

FIPS モードをイネーブルにする前に、 MDS スイッチで次の作業を実行します。

1. パスワードは 8 文字以上にする必要があります。
2. Telnet を無効にします。ユーザは SSH のみを使用してログインする必要があります。
3. RADIUS/TACACS+ によるリモート認証をディセーブルにします。認証できるのは、スイッチに対してローカルなユーザだけです。
4. SNMP v1 および v2 を無効にします。SNMPv3 用に設定されたスイッチ上の既存のユーザアカウントは、認証に SHA 、プライバシーには AES/3DES だけを設定する必要があります。

5. VRRP を無効にします。
6. 認証用の MD5 または暗号化用の DES を持つすべての IKE ポリシーを削除します。認証に SHA を使用し、暗号化に 3DES/AES を使用するようにポリシーを変更します。
7. すべての SSH Server RSA1 キーペアを削除します。

MDS スイッチで FIPS モードを有効にして FIPS ステータスを表示するには、次の手順を実行します。

1. FIPS のステータスを表示します。

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048 ビットの SSH キーを設定します。

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS モードを有効にする。

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. FIPS のステータスを表示します。

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. コンフィギュレーションを実行コンフィギュレーションに保存します。

```
MDSSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. MDS スイッチを再起動します

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. FIPS のステータスを表示します。

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

詳細については、を参照してください "FIPS モードの有効化"。

Cisco Nexus の場合

Cisco Nexus 9000 シリーズスイッチ（バージョン 9.3 ）はです "FIPS 140-2 に準拠しています"。Cisco Nexus は、 SNMPv3 および SSH の暗号モジュールと次のサービスを実装します。

- 各サービスをサポートするセッション確立
- 各サービスの主要な派生機能をサポートする、基盤となるすべての暗号化アルゴリズム

- 各サービスのハッシュ化
- 各サービスの対称暗号化

FIPS モードを有効にする前に、 Cisco Nexus スイッチで次の作業を実行します。

1. Telnet を無効にします。ユーザは Secure Shell （ SSH ）のみを使用してログインする必要があります。
2. SNMPv1 および v2 を無効にします。SNMPv3 用に設定されたデバイス上の既存のユーザアカウントは、認証に SHA 、プライバシーには AES/3DES だけを設定する必要があります。
3. すべての SSH サーバ RSA1 キー・ペアを削除します
4. Cisco TrustSec セキュリティアソシエーションプロトコル（ SAP ）ネゴシエーション中に使用する HMAC-SHA1 メッセージ整合性チェック（ MIC ）をイネーブルにします。これを行うには、「 cts-manual' 」または「 cts-dot1x' 」モードから sap hash-calgorithm「 HMAC-sha-1 」コマンドを入力します。

Nexus スイッチで FIPS モードを有効にするには、次の手順を実行します。

1. 2048 ビットの SSH 鍵を設定します。

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048 ビットの SSH キーを設定します。

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS モードを有効にする。

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Nexus スイッチを再起動します。

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. FIPS のステータスを表示します。

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

さらに、 Cisco NX-OS ソフトウェアは、ネットワーク異常およびセキュリティの検出を強化する NetFlow 機能をサポートしています。NetFlow は、ネットワーク上のすべてのカンバセーション、通信に関係する側、使用されているプロトコル、およびトランザクションの期間のメタデータをキャプチャします。情報を集約して分析すると、正常な動作に関する洞察を得ることができます。収集されたデータを使用すると、疑わしいアクティビティのパターンを識別することもできます。たとえば、マルウェアがネットワーク全体に拡散し、これが気付かない場合があります。NetFlow では、フローを使用してネットワークモニタリングの統計情報を提供します。フローは、送信元インターフェイス（または VLAN ）に着信し、キーの値が同じパケットの単方向ストリームです。キーは、パケット内のフィールドの識別された値です。フローレコードを使用してフローを作成し、フローに固有のキーを定義します。フローエクスポータを使用して、 Cisco StealthWatch などのリモート NetFlow コレクタに NetFlow が収集するデータをエクスポートできます。StealthWatch では、この情報を使用してネットワークを継続的に監視し、ランサムウェアの発生が発生した場合にリアルタイムの脅威検出およびインシデント応答フォレンジックを提供します。

"次のセクションでは、 FlexPod の ONTAP ストレージと FIPS 140-2 について説明します。"

FlexPod の NetApp ONTAP ストレージと FIPS 140-2

"前のリリース： FlexPod のシスコネットワークと FIPS 140-2"

ネットアップは、さまざまなハードウェア、ソフトウェア、サービスを提供しています。これらのサービスには、この標準で検証済みの暗号モジュールのさまざまなコンポーネントを含めることができます。そのため、ネットアップでは、コントロールプレーンとデータプレーンに関して、 FIPS 140-2 への準拠にさまざまなアプローチを採用しています。

- ネットアップが提供する暗号モジュールには、転送中のデータと保管中のデータの暗号化についてレベル 1 の検証を実施した暗号モジュールが含まれています。
- ネットアップは、これらのコンポーネントのサプライヤによって FIPS 140-2 認定を受けたハードウェアモジュールとソフトウェアモジュールの両方を取得します。たとえば、 NetApp Storage Encryption 解決策 は、 FIPS レベル 2 の検証済みドライブを利用します。
- ネットアップ製品では、製品や機能が検証の範囲外であっても、標準に準拠した検証済みモジュールを使用できます。たとえば、 NetApp Volume Encryption （ NVE ）は FIPS 140-2 に準拠しています。別途検証されるわけではありませんが、レベル 1 で検証済みの NetApp 暗号化モジュールが使用されます。ご使用のバージョンの ONTAP に対する準拠の詳細については、 FlexPod SME にお問い合わせください。
- NetApp Cryptographic モジュールは FIPS 140-2 レベル 1 に準拠しています *
- NetApp Cryptographic Security Module （ NCSM ）は FIPS 140-2 レベル 1 に準拠しています。
- ネットアップの自己暗号化ドライブは FIPS 140-2 レベル 2 に準拠しています *

ネットアップは、元の機器メーカー（ OEM ）が FIPS 140-2 認定を取得した自己暗号化ドライブ（ SED ）を購入しています。これらのドライブを求めるお客様は、注文時に SED を指定する必要があります。ドライブはレベル 2 で検証されます。次のネットアップ製品では、検証済み SED を利用できます。

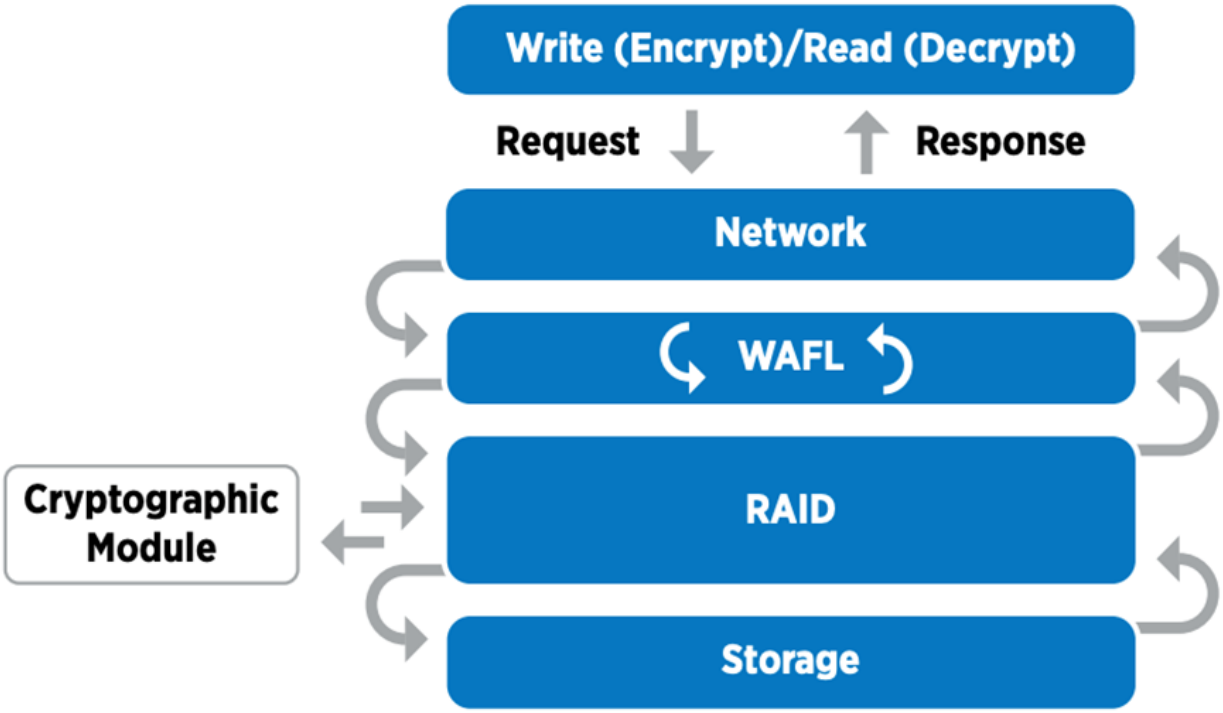
- AFF A シリーズおよび FAS ストレージシステム
- E シリーズおよび EF シリーズストレージシステム
- NetApp Aggregate Encryption および NetApp Volume Encryption *

NVE テクノロジと NetApp Aggregate Encryption （ NAE ）テクノロジを使用すると、ボリュームレベルとアグリゲートレベルでそれぞれデータを暗号化できるため、解決策 は物理ドライブに依存しません。

NVE は、 ONTAP 9.1 以降で使用可能なソフトウェアベースの保管データ暗号化解決策 で、 ONTAP 9.2 以降で FIPS 140-2 に準拠しています。NVE を使用すると、 ONTAP でボリュームごとにデータを暗号化して詳細に指定できます。NAE は ONTAP 9.6 で利用でき、 NVE の急成長です。 ONTAP は各ボリュームのデータを暗号化でき、ボリュームはアグリゲート全体でキーを共有できます。NVE と NAE はいずれも AES 256 ビット暗号化を使用します。データは、 SED を使用せずにディスクに保存することもできます。NVE および NAE を使用すると、暗号化が有効になっている場合でも Storage Efficiency 機能を使用できます。アプリケーションレイヤのみの暗号化では、 Storage Efficiency のすべてのメリットが損なわれています。NVE および NAE では、データがネットワークから NetApp WAFL を介して RAID レイヤに到着するため、ストレージ効率が維持されます。これにより、データを暗号化するかどうかが決まります。NAE では、ストレージ効率を高めるためにアグリゲート重複排除を使用できます。NVE ボリュームと NAE ボリュームは同じ NAE アグリゲート内で共存できます。NAE アグリゲートでは、暗号化されていないボリュームはサポートさ

プロセスの仕組みは次のとおりです。データが暗号化されると、 FIPS 140-2 レベル 1 認定の暗号化モジュールに送信されます。暗号モジュールはデータを暗号化して RAID レイヤに戻します。暗号化されたデータがデ

ィスクに送信されます。そのため、 NVE と NAE を組み合わせることで、データがディスクに転送される途中ですでに暗号化されています。読み取りは、逆のパスに従います。つまり、ディスクからのデータは暗号化された状態で RAID に送信され、暗号化モジュールによって復号化され、次の図に示すように、スタックの残りの部分が送信されます。



NVE は、 FIPS 140-2 レベル 1 に準拠したソフトウェア暗号化モジュールを使用します。

NVE の詳細については、を参照してください "NVE のデータシート"。

NVE でクラウド内のデータを保護する。Cloud Volumes ONTAP と Azure NetApp Files は、 FIPS 140-2 準拠の保存データ暗号化機能を提供できます。

ONTAP 9.7 以降では、 NVE ライセンスでオンボードまたは外部キー管理を使用すれば、新しく作成したアグリゲートとボリュームがデフォルトで暗号化されます。ONTAP 9.6 以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。アグリゲートに作成するボリュームはデフォルトで暗号化されます。このデフォルトの設定は、ボリュームを暗号化するときに無効にすることができます。

ONTAP NAE CLI コマンド

次の CLI コマンドを実行する前に、クラスタに必要な NVE ライセンスがあることを確認してください。

アグリゲートを作成して暗号化するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行した場合）。

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

非 NAE アグリゲートを NAE アグリゲートに変換するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行した場合）。

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

NAE アグリゲートを非 NAE アグリゲートに変換するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行している場合）。

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

ONTAP NVE CLI コマンド

ONTAP 9.6 以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。アグリゲートに作成するボリュームはデフォルトで暗号化されます。

NAE が有効になっているアグリゲートでボリュームを作成するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行した場合）。

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

ボリューム移動を行わずに既存ボリュームの「インプレース」暗号化を有効にするには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行している場合）。

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

ボリュームで暗号化が有効になっていることを確認するには、次の CLI コマンドを実行します。

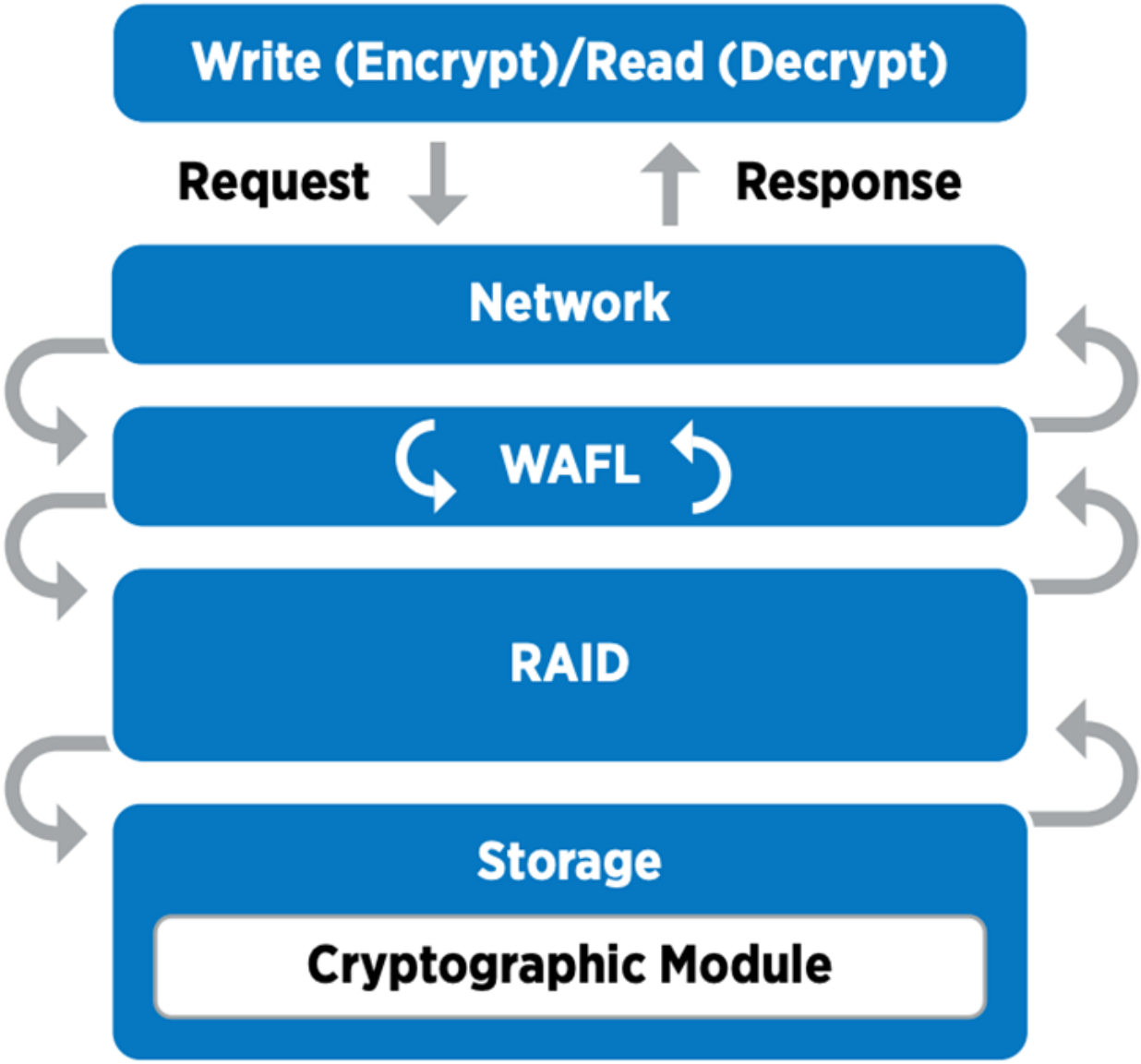
```
fp-health::> volume show -is-encrypted true
```

NSE の場合

NSE は、 SED を使用して、ハードウェアアクセラレーションメカニズムでデータ暗号化を実行します。

NSE は、 FIPS 140-2 レベル 2 自己暗号化ドライブを使用し、 AES 256 ビット透過的ディスク暗号化によって保存データを保護できるため、コンプライアンスの確保とスペアの返却が容易になります。ドライブは、暗

号化キーの生成を含め、次の図に示すように、すべてのデータ暗号化処理を内部的に実行します。データへの不正アクセスを防止するために、ストレージシステムは、ドライブの初回使用時に確立された認証キーを使用して、ドライブ自体を認証する必要があります。



NSE は、各ドライブでハードウェア暗号化を使用します。 FIPS 140-2 レベル 2 認定済みです。

NSE の詳細については、を参照してください "NSE のデータシート"。

キー管理

FIPS 140-2 規格は、次の図に示すように、境界によって定義された暗号モジュールを環境 にします。

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

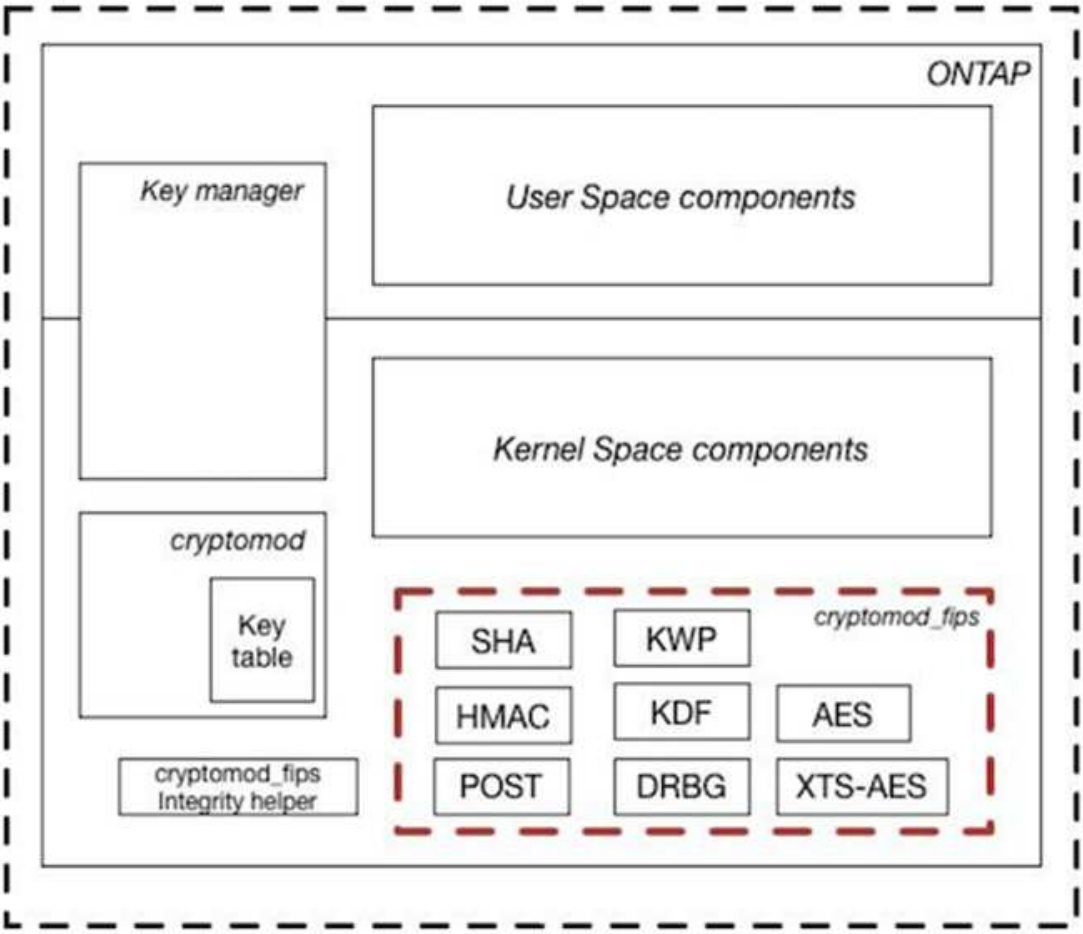


Figure 1 - Block Diagram

キー管理ツールは、 ONTAP で使用されるすべての暗号化キーを追跡します。NSE SED は、キー管理ツールを使用して NSE SED の認証キーを設定します。キー管理ツールを使用する場合は、 NVE と NAE 解決策 が組み合わされ、ソフトウェア暗号化モジュール、暗号化キー、およびキー管理ツールで構成されます。NVE は、ボリュームごとに、キー管理ツールが格納する一意の XTS-AES 256 データ暗号化キーを使用します。データボリュームに使用するキーは、そのクラスタ内のデータボリュームに一意のキーで、暗号化されたボリュームの作成時に生成されます。同様に、 NAE ボリュームはアグリゲートごとに一意の XTS-AES 256 データ暗号化キーを使用します。このキー管理ツールにも保存されます。NAE キーは、暗号化されたアグリゲートが作成されると生成されます。ONTAP は、キーをあらかじめ再生したり、再利用したり、プレーンテキストで表示したりすることはなく、キー管理ツールによって保存および保護されます。

外部キー管理ツールのサポート

ONTAP 9.3 以降では、 NVE ソリューションと NSE ソリューションの両方で外部キー管理機能がサポートされます。FIPS 140-2 規格の環境 特定のベンダーの実装で使用される暗号モジュール。ほとんどの場合、FlexPod と ONTAP のお客様は、（の）次のいずれかの検証済みソリューションを使用しています "NetApp Interoperability Matrix を参照してください") キー管理ツール：

- Gemalto または SafeNet AT のいずれかを指定します

- Vormetric （ Thales ）
- IBM SKLM
- Utimaco （旧称 Microfocus 、 HPE ）

NSE と NVMe SED の認証キーは、業界標準の OASIS Key Management Interoperability Protocol （ KMIP ）を使用して外部キーマネージャにバックアップされます。ストレージシステム、ドライブ、およびキー管理ツールのみがキーにアクセスでき、セキュリティドメイン外に移動してデータ漏洩を防止する場合は、ドライブのロックを解除できません。外部キー管理ツールでは、 NVE ボリュームの暗号化キーおよび NAE アグリゲートの暗号化キーも保存されます。コントローラとディスクを移動して外部キー管理ツールにアクセスできなくなった場合は、 NVE ボリュームと NAE ボリュームにアクセスできず、復号化できません。

次の例では、 store virtual machine （ SVM ）「 svmname1 」の外部キー管理ツールで使用されるサーバのリストに、 2 つのキー管理サーバを追加します。

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

FlexPod データセンターをマルチテナンシーシナリオで使用している場合、 ONTAP では、セキュリティ上の理由から SVM レベルでデータセンターをテナンシー環境から分離できます。

外部キー管理ツールのリストを確認するには、次の CLI コマンドを実行します。

```
fp-health::> security key-manager external show
```

暗号化を組み合わせることで二重暗号化（多層防御）を実現

データへのアクセスを分離し、データが常に保護されるようにする必要がある場合は、 NSE SED をネットワークレベルまたはファブリックレベルの暗号化と組み合わせることができます。NSE SED は、管理者が高レベルの暗号化を設定または設定ミスを忘れてしまった場合に、バックストップのように機能します。2 つの異なるレイヤの暗号化では、 NSE SED を NVE および NAE と組み合わせることができます。

NetApp ONTAP クラスタ全体のコントロールプレーン **FIPS** モード

NetApp ONTAP データ管理ソフトウェアには、お客様向けに高度なセキュリティをインスタンス化する、FIPS モードの構成が用意されています。この FIPS モードでは、コントロールプレーンの環境 のみが実行されます。FIPS モードを有効にすると、 FIPS 140-2 の主要な要素に基づいて、 Transport Layer Security v1 （ TLSv1 ）と SSLv3 は無効になり、 TLS v1.1 と TLS v1.2 のみが有効なままになります。

> FIPS モードの ONTAP クラスタ全体のコントロールペインは、 FIPS 140-2 レベル 1 に準拠しています。クラスタ全体の FIPS モードでは、 NCSM が提供するソフトウェアベースの暗号化モジュールを使用します。

クラスタ全体のコントロールプレーンの FIPS 140-2 準拠モードは、 ONTAP のすべての制御インターフェイスを保護します。デフォルトでは、 FIPS 140-2 のみのモードは無効になっていますが、 security config modify コマンドの 'is-fips-enabled ' パラメータを 'true' に設定すると、このモードを有効にできます。

ONTAP クラスタで FIPS モードを有効にするには、次のコマンドを実行します。

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

SSL FIPS モードが有効な場合は、 ONTAP から ONTAP 外部のクライアントまたはサーバコンポーネントへの SSL 通信に、 FIPS 準拠の SSL 暗号化が使用されます。

クラスタ全体の FIPS ステータスを表示するには、次のコマンドを実行します。

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"次のスライド：解決策 が FlexPod 統合インフラのメリットを提供"

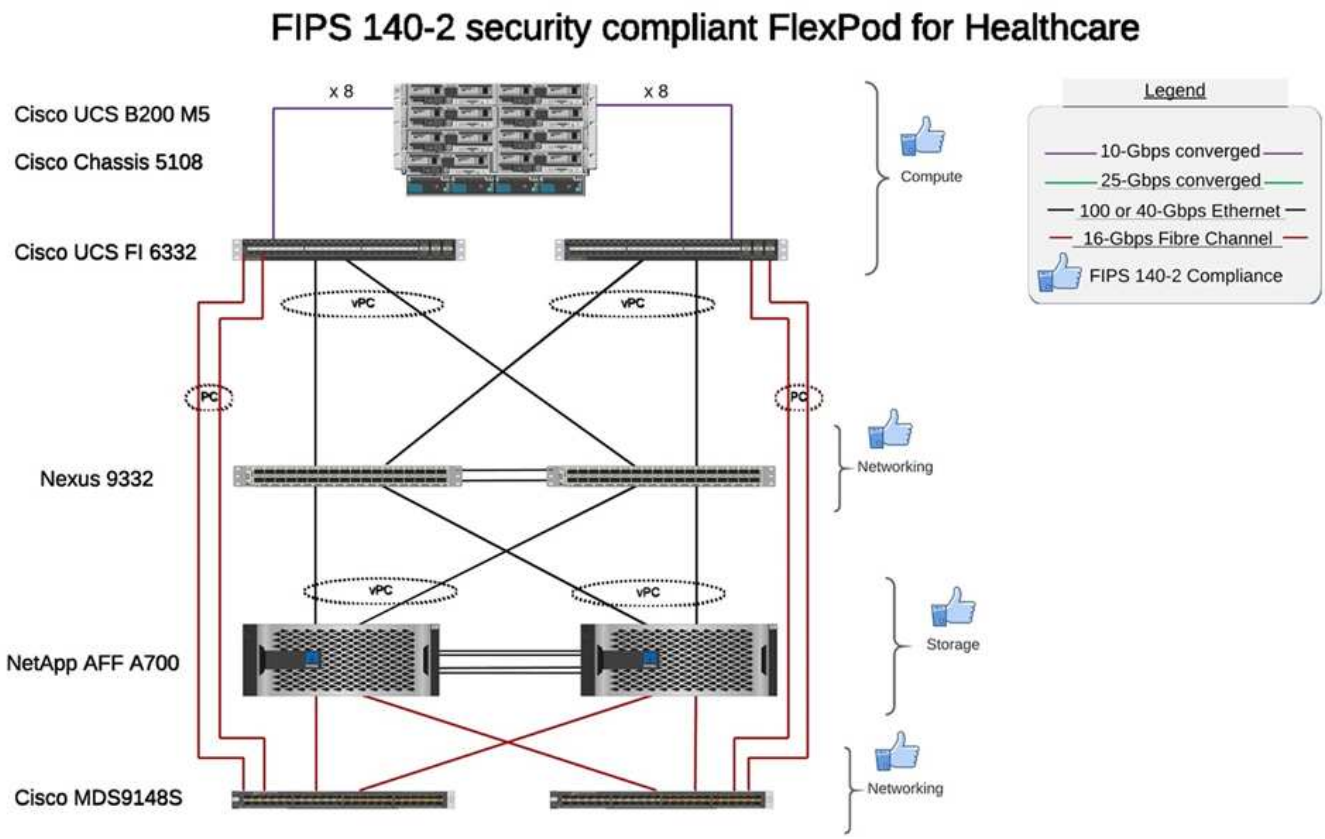
FlexPod コンバージドインフラの解決策 のメリット

"以前のリリース： FlexPod NetApp ONTAP ストレージおよび FIPS 140-2 。"

医療機関には、いくつかのミッションクリティカルなシステムがあります。最も重要なシステムの 2 つは、電子カルテ（ EHR ）システムと医療画像システムです。FlexPod システムにおける FIPS の設定を実証するために、オープンソースの EHR およびオープンソースの画像アーカイブおよび通信システム（ PACS ）システムを使用して、FlexPod システムのラボセットアップとワークロード検証を実施しました。EHR 機能、EHR 論理アプリケーションコンポーネント、および FlexPod システムに実装した場合の EHR システムのメリットの一覧については、を参照してください "TR-4881 ： 『 FlexPod for Electronic Health Record Systems 』"。医療画像システムの機能、論理アプリケーションコンポーネント、および FlexPod に実装された医療画像システムの利点については、を参照してください "TR-4865 ： FlexPod for Medical Imaging"。

FIPS のセットアップとワークロードの検証では、典型的な医療機関の代表的なワークロード特性を行使しました。たとえば、現実的な患者データのアクセスおよび変更シナリオを含むオープンソースの EHR システムをテストしました。さらに、医療用画像ワークロードを実行しました。このワークロードには、医療用（ DICOM ）オブジェクトのデジタル画像処理と通信が含まれていました。dcm ファイル形式メタデータを含む DICOM オブジェクトは、ファイルストレージとブロックストレージの両方に保存されています。さらに、仮想化された RedHat Enterprise Linux （ RHEL ）サーバにマルチパス機能も実装しています。DICOM オブジェクトは、 NFS 、 iSCSI を使用してマウントされた LUN 、および FC を使用してマウントされた LUN に保存しました。FIPS のセットアップと検証で、 FlexPod コンバージドインフラが期待以上のパフォーマンスをシームレスに実現したことがわかりました。

次の図は、 FIPS のセットアップと検証に使用される FlexPod システムを示しています。ネットアップはを活用しました "FlexPod データセンターと VMware vSphere 7.0 および NetApp ONTAP 9.7 Cisco Validated Design （ CVD ）" セットアッププロセスの実行中です。



解決策インフラのハードウェアコンポーネントとソフトウェアコンポーネント

次の 2 つの図に、 FlexPod で FIPS を有効にする際に使用するハードウェアコンポーネントとソフトウェアコンポーネントを示します。これらの表に記載されている推奨事項は例です。 NetApp SME と連携して、コンポーネントが組織に適していることを確認する必要があります。また、コンポーネントとバージョンがでサポートされていることを確認します "NetApp Interoperability Matrix Tool で確認できます" （ IMT ）および "シスコハードウェア互換性リスト（ HCL ）"。

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
コンピューティング	Cisco UCS 5108 シャーシ	1 または 2	
	Cisco UCS ブレードサーバ	B200 M5 × 3	それぞれに、 20 コア以上、 2.7GHz 、および 128-384GB RAM を 2 個搭載しています
	Cisco UCS 仮想インターフェイスカード（ VIC ）	Cisco UCS 1440	を参照してください
	Cisco UCS ファブリックインターコネクト × 2	6332	-
ネットワーク	Cisco Nexus スイッチ	Cisco Nexus 9332 × 2	-
ストレージネットワーク	SMB / CIFS 、 NFS 、または iSCSI プロトコル経由のストレージアクセス用の IP ネットワーク	上記と同じネットワークスイッチ	-

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
	FC 経由のストレージアクセス	Cisco MDS 9148S × 2	-
ストレージ	NetApp AFF A700 オールフラッシュストレージシステム	1 クラスタ	2 ノードクラスタ
	ディスクシェルフ	DS224C または NS224 ディスクシェルフ × 1	24 本のドライブをフル装備
	SSD の場合	容量が 24 、 2TB 以上	-

ソフトウェア	製品ファミリー	バージョンまたはリリース	詳細
様々	Linux の場合	RHEL 7.x	-
	Windows の場合	Windows Server 2012 R2 （ 64 ビット）	-
	NetApp ONTAP	ONTAP 9.7 以降	-
	Cisco UCS ファブリックインターコネクト	Cisco UCS Manager 4.1 以降	-
	Cisco Ethernet 3000 または 9000 シリーズスイッチ	9000 シリーズの場合、7.0(3) i7(7) 以降（ 3000 シリーズ用）、 9.2(4) 以降	-
	Cisco FC ： Cisco MDS 9132T	8.4(1a) 以降	-
	ハイパーバイザー	VMware vSphere ESXi 6.7 U2 以降	-
ストレージ	ハイパーバイザー管理システム	VMware vCenter Server 6.7 U3 （ vCSA ）以降	-
ネットワーク	NetApp Virtual Storage Console （ VSC ）	VSC 9.7 以降	-
	NetApp SnapCenter	SnapCenter 4.3 以降	-
	Cisco UCS Manager の略	4.1 （ 1c ）以降	
ハイパーバイザー	ESXi		
管理	ハイパーバイザー管理システム VMware vCenter Server 6.7 U3 （ vCSA ）以降		
	NetApp Virtual Storage Console （ VSC ）	VSC 9.7 以降	
	NetApp SnapCenter	SnapCenter 4.3 以降	
	Cisco UCS Manager の略	4.1 （ 1c ）以降	

"次： FlexPod のセキュリティに関するその他の考慮事項。"

FlexPod のセキュリティに関するその他の考慮事項

"前のスライド：解決策 が FlexPod コンバージドインフラのメリットを提供"

FlexPod インフラは、モジュラ型の統合型で、必要に応じて仮想化と拡張性に優れた、コスト効率の高いプラットフォームです。FlexPod プラットフォームでは、コンピューティング、ネットワーク、ストレージを個別にスケールアウトできるため、アプリケーションの導入時間が短縮されます。また、モジュラアーキテクチャにより、システムのスケールアウトやアップグレード時にもノンストップオペレーションが実現します。

HIT システムのさまざまなコンポーネントは、データを SMB/CIFS 、 NFS 、 ext4 、および NTFS ファイルシステムに格納する必要があります。つまり、この要件のインフラでは、 NFS 、 CIFS 、 SAN の各プロトコル経由でデータアクセスを提供する必要があります。1 つのネットアップストレージシステムでこれらのプロトコルをすべてサポートできるため、プロトコル固有のストレージシステムという従来の手法は必要ありません。さらに、 1 つのネットアップストレージシステムで複数の HIT ワークロード（ EHR 、 PACS 、 VNA 、ゲノム、 VDI など）をサポートし、 パフォーマンスレベルが保証され、設定も可能です。

HIT は、 FlexPod システムに導入されると、医療業界に固有の利点をいくつか提供します。次に、これらの利点の概要概要 を示します。

- * FlexPod セキュリティ * 。セキュリティは、 FlexPod システムの基盤にあります。ここ数年、ランサムウェアは脅威になっています。ランサムウェアは、暗号化を使用して悪意のあるソフトウェアを構築する暗号技術に基づいたマルウェアの一種です。このマルウェアは、対称キー暗号と非対称キー暗号の両方を使用して、被害者のデータをロックし、データを復号化するための鍵を提供するために身代金を要求できます。FlexPod 解決策 がランサムウェアなどの脅威を軽減する方法については、を参照してください "TR-4802 ：『 The 解決策 to Ransomware 』"。FlexPod インフラコンポーネントもあります "FIPS 140-2 に準拠しています"。
- * Cisco Intersight * Cisco Intersight は、クラウドベースの革新的な管理サービスプラットフォームであり、単一のコンソールでフルスタックの FlexPod 管理とオーケストレーションを実現します。Intersight プラットフォームでは、 FIPS 140-2 セキュリティ準拠の暗号モジュールが使用されています。このプラットフォームのアウトオブバンド管理アーキテクチャは、 HIPAA などの一部の標準や監査の範囲外になります。ネットワーク上の個々の識別可能なヘルス情報が、サイト間ポータルに送信されることはありません。
- * NetApp FPolicy テクノロジ。 * NetApp FPolicy （名前ファイルポリシーの変更）は、 NFS または SMB / CIFS プロトコル経由のファイルアクセスを監視および管理するための、ファイルアクセス通知フレームワークです。このテクノロジは、 ONTAP データ管理ソフトウェアに 10 年以上にわたって組み込まれており、ランサムウェアの検出に役立ちます。このゼロトラストエンジンは、アクセスコントロールリスト（ ACL ）の権限を超えた追加のセキュリティ対策を提供します。FPolicy の処理モードには、ネイティブと外部の 2 つがあります。
  - ネイティブモードでは、ファイル拡張子のブラックリストとホワイトリストの両方が提供されます。
  - 外部モードはネイティブモードと同じ機能を備えていますが、 ONTAP システムとは外部で実行される FPolicy サーバや、セキュリティ情報 / イベント管理（ SIEM ）システムと統合されています。ランサムウェアと戦う方法の詳細については、を参照してください "『 Fighting Ransomware ： Part 3 – ONTAP FPolicy 、 Another powerful Native （別名 Free ） Tool 』" ブログ
- * 保存データ * 。ONTAP 9 以降には、 FIPS 140-2 準拠の保管データ暗号化ソリューションが 3 つあります。
  - NSE は、自己暗号化ドライブを使用するハードウェア解決策 です。

- NVE は、あらゆるドライブタイプのあらゆるデータボリュームを暗号化できるソフトウェア解決策です。ボリュームごとに一意のキーを使用して有効にします。
- NAE は、あらゆるドライブタイプのあらゆるデータボリュームを暗号化できるソフトウェア解決策です。 NAE は、アグリゲートごとに固有のキーを使用して有効にします。

> ONTAP 9.7 以降では、 VE という名前の NetApp NVE ライセンスパッケージがある場合、NAE および NVE がデフォルトで有効になります。

- * 転送中のデータ * 。ONTAP 9.8 以降では、 Internet Protocol security （ IPSec ；インターネットプロトコルセキュリティ）により、クライアントと ONTAP SVM の間のすべての IP トラフィックをエンドツーエンドで暗号化できます。すべての IP トラフィックの IPSec データ暗号化には、 NFS 、 iSCSI 、 SMB/CIFS の各プロトコルが含まれます。IPSec では、 iSCSI トラフィックに対して転送中の暗号化オプションのみが提供されます。
- * ハイブリッドマルチクラウドデータファブリック全体でエンドツーエンドのデータ暗号化を実現 * 。データレプリケーショントラフィックに NSE や NVE およびクラスタピアリング暗号化（ CPE ）などの保管データ暗号化テクノロジを使用しているお客様は、 ONTAP 9.8 以降にアップグレードして IPsec を使用することで、ハイブリッドマルチクラウドデータファブリック全体でクライアントとストレージの間のエンドツーエンドの暗号化を使用できるようになりました。ONTAP 9 以降では、クラスタ全体のコントロールプレーンインターフェイスに対して、 FIPS 140-2 準拠モードを有効にできます。FIPS 140-2 専用モードは、デフォルトでは無効になっています。ONTAP 9.6 以降では、 CPE によって、 NetApp SnapMirror 、 NetApp SnapVault 、 NetApp FlexCache テクノロジなどの ONTAP データレプリケーション機能に対する TLS 1.2 AES-256 GCM 暗号化がサポートされます。暗号化は、 2 つのクラスタピア間での Pre-Shared Key （ PSK ；事前共有キー）を使用して設定されます。
- * セキュアマルチテナンシー * 。仮想化されたサーバとストレージ共有インフラのニーズの増大に対応し、特にデータベースとソフトウェアの複数のインスタンスをホストする場合に、施設固有の情報のセキュアマルチテナンシーを実現します。

"次は終わりです"

まとめ

"Previous ： FlexPod のセキュリティに関するその他の考慮事項。"

医療アプリケーションを FlexPod プラットフォームで実行することで、医療機関は FIPS 140-2 対応プラットフォームでより適切に保護されます。FlexPod は、コンピューティング、ネットワーク、ストレージのすべてのコンポーネントでマルチレイヤ保護を提供します。FlexPod のデータ保護機能は、保管中または転送中のデータを保護し、必要に応じてバックアップを安全に実行し、準備を整えます。

Cisco とネットアップの戦略的パートナーシップによって厳格にテストされた統合インフラである FlexPod 検証済み設計を活用することで、人為的ミスを回避できます。コンピューティング、ネットワーク、ストレージの各レイヤで FIPS 140-2 が有効な場合でも、予測可能な低レイテンシのシステムパフォーマンスと高可用性を提供するように設計された FlexPod システム。影響はほとんどありません。このアプローチにより、 HIT システムのユーザーに優れたユーザー体験と最適な応答時間が実現します。

"次：謝辞、バージョン履歴、および追加情報 の検索場所"

確認応答、バージョン履歴、および追加情報 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。

- 『 Cisco MDS 9000 Family NX-OS Security Configuration Guide 』

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 Series NX-OS Security Configuration Guide 、 Release 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp and Federal Information Processing Standard （ FIPS ） 140-2 』を参照できます

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- 『 NetApp ONTAP 9 Hardening Guide 』

  https://www.netapp.com/us/media/tr-4569.pdf

- NetApp Encryption パワーガイド』を参照してください

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- NVE および NAE のデータシート

  https://www.netapp.com/us/media/ds-3899.pdf

- NSE のデータシート

  https://www.netapp.com/us/media/ds-3213-en.pdf

- ONTAP 9 ドキュメンテーション・センター

  http://docs.netapp.com

- NetApp and Federal Information Processing Standard （ FIPS ） 140-2 』を参照できます

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco および FIPS 140-2 への準拠

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp Cryptographic Security Module の略

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- 中規模および大規模な医療機関向けのサイバーセキュリティの実践

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco and Cryptographic Module Validation Program （ CMVP ）

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp ストレージ暗号化、 NVMe 自己暗号化ドライブ、 NetApp Volume Encryption 、 NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp Volume Encryption および NetApp Aggregate Encryption の略

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp Storage Encryption の略

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- 電子医療記録システム用 FlexPod

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- 現在のデータ：クラウド対応フラッシュテクノロジを使用した Epic EHR 環境でパフォーマンスを向上

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- Epic EHR インフラ向け FlexPod データセンター

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Epic EHR 向け FlexPod データセンター導入ガイド

  https://www.netapp.com/media/10658-tr-4693.pdf

- MEDITECH ソフトウェア対応 FlexPod データセンターインフラ

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- FlexPod 規格は MEDITECH ソフトウェアにも対応しています

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- FlexPod for MEDITECH の指向性サイジングガイド

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- 医療用画像処理用の FlexPod

  https://www.netapp.com/media/19793-tr-4865.pdf

- 医療業界の AI

  https://www.netapp.com/us/media/na-369.pdf

- ヘルスケア向けの FlexPod で変革を促進

  https://flexpod.com/solutions/verticals/healthcare/

- Cisco とネットアップが提供する FlexPod

  https://flexpod.com/

謝辞

- ネットアップ、テクニカルマーケティングエンジニア、 Abhinav Singh 氏
- ネットアップ、解決策 Architect Healthcare （ Epic ）、 Brian O'Menahony 氏
- ネットアップ、 Pursuit Business Development Manager 、 Brian Pruitt 氏
- ネットアップシニアソリューションアーキテクト、 Arvind Ramakrinan 氏
- ネットアップ、 FlexPod グローバルフィールド CTO 、 Michael Hommer 氏

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	2021年4月	初版リリース

Cisco IntersightとNetApp ONTAP ストレージ

『Cisco Intersight with NetApp Storage Quick Start Guide』

協力：

はじめに

ネットアップと Cisco は提携を通じて、 FlexPod エコシステムの単一コンソールビューである Cisco Intersight を提供しています。このシンプルな統合により、 FlexPod インフラと FlexPod 解決策のすべてのコンポーネントを対象とした統合管理プラットフォームが実現します。Cisco Intersight を使用すると、ネットアップストレージ、 Cisco コンピューティング、 VMware のインベントリを監視できます。また、ワークフローをオーケストレーションまたは自動化して、ストレージと仮想化のタスクを並行して実行することもできます。

関連情報

詳細については、次のドキュメントと Web サイトを参照してください。

"TR 4883 ：『 FlexPod Datacenter with ONTAP 9.8 』、『 ONTAP Storage Connector for Cisco Intersight 』、および『 Cisco Intersight Managed Mode 』"

"Cisco Intersightヘルプセンター"

"Cisco Intersight の概要"

"『 Intersight Appliance Install and Upgrade Guide 』を参照してください"

新機能

このセクションでは、 Cisco Intersight と NetApp ONTAP ストレージに利用できる新機能を紹介します。

2024年1月

- リファレンスワークフローを使用したNetAppストレージオーケストレーションが、 "FlexPod Intersightワークフローリポジトリ"。GitHubの新しいリファレンスワークフローの詳細については、 "ユースケース 2 ：リファレンスワークフローを使用したネットアップストレージのオーケストレーション"。

2023年11月

- ユーザインターフェイスの[Inventory]セクションに[NVMeネームスペース]ページが追加されました。

2023年8月

NetApp Active IQ Unified Manager 9.13GAへのアップグレードは、最新リリースとの互換性とフル機能を確保するために必要です。

- [New NetApp SmartLUN]タスクが改善され、新しいイニシエータグループを作成する場合と既存のイニシエータグループを選択する場合の選択オプションが明確に表示されるようになりました。新しいイニシエータグループを作成するためのチェックボックスを選択すると、既存のイニシエータグループを選択するためのパラメータは使用できなくなります。新しいイニシエータグループを作成するためのチェックボックスをオフにすると、既存のイニシエータグループパラメータが使用可能になります。
- [New NetApp LUN Map]および[Remove NetApp LUN Map]のタスクが強化されました。これで、LUNとイニシエータグループ間の新しい関係が更新されます。タスクの実行時に、LUNとイニシエータグループの両方のUIインベントリがただちに更新されます。
- [Checks]ページは、ユーザが初めてログインしたときに正しくロードされるようになり、更新が不要になりました。

2023年7月

NetApp Active IQ Unified Manager 9.13GAへのアップグレードは、最新リリースとの互換性とフル機能を確保するために必要です。

- NetAppストレージタスクの名前が更新されました。名前を変更したタスクの完全なリストについては、ユースケース3デザイナフリーフォームを使用したカスタムワークフローを参照してください。
- NFSインターフェイスのIPアドレスが、新しいNetApp NASスマートボリュームタスクの出力として追加されました。
- ASUP転送がHTTPSであることが[Checks]タブに追加されました。
- すべての階層の正しい階層タイプが、階層のユーザーインターフェイスに正しく表示されるようになりました。
- すべての準拠ライセンスが[Licenses]ページに正しく表示されるようになりました。
- ホームディレクトリがないかどうかに関係なく、CIFS共有について正確な値が[Shares]ページに表示されるようになりました。
- [LUNs]ページの[Mapped]列でソートとフィルタリングが有効になりました。
- ソートとフィルタリングによって、[NTP Servers]ページの[Authentication Enabled]列が有効になりました。
- [チェック（Checks）]タブに、新しいチェックと次の対応するカテゴリを追加しました。
  - セキュリティ
  - ランサムウェア対策
  - 可用性
  - その他
- [Inventory]詳細ビューで、使用済み物理容量の代わりに使用済み容量をレポートします。

2023年6月

> 最新リリースとの互換性とフル機能を確保するには、NetApp Active IQ Unified Manager 9.13RC1へのアップグレードが必要です。

- NetAppストレージタスクの名前が更新されました。を参照してください "使用例 3 デザイナフリーフォームを使用したカスタムワークフロー" は、名前を変更したタスクの完全なリストです。

2023年4月

- ユーザインターフェイスの[Inventory]セクションの[Policies]ページに、[Protection Policies（SnapMirror）]タブと[Snapshot Policies]タブが追加されました。
- ユーザインターフェイスの[Inventory]セクションに[NFS Clients]ページが追加されました。
- ユーザインターフェイスの[Inventory]セクションに、[Storage VMs]ページに[Protected]列が追加されました。
- データ削減情報のレポートおよび表示方法が変更されました。
- ユーザインターフェイスの[インベントリ]セクションの[階層]ページに[ローカル階層]タブと[クラウド階層]タブが追加されました。
- ユーザインターフェイスの[Inventory]セクションの[Ports]ページの[Name]列のあとに[Node]列が表示されるようになりました。

2023年1月

> 最新リリースとの互換性を確保し、すべての機能を利用するには、NetApp Active IQ Unified Manager 9.12 GAへのアップグレードが必要です。このリリースに関連する既知の問題のリストについては、を参照してください [既知の問題]。

- 互換性チェックを実行するときに、相互接続性チェックでUCSMモードとIMMファームウェアモードを区別できるようになりました。
- ONTAP 9.7の場合、保護関係はサイト間に表示されません。この問題 はONTAP 9.8RC1で修正されました。

2022年8月

> 最新リリースとの互換性を確保し、すべての機能を利用するには、NetApp Active IQ Unified Manager 9.11 GAへのアップグレードが必要です。このリリースに関連する既知の問題のリストについては、を参照してください [既知の問題]。

- クラスタの使用可能容量の計算方法がSystem Managerに合わせて更新されました
- クラスタの全般ページが更新され、パフォーマンスデータが表示されるまでパフォーマンス指標の概要が非表示になりました
- クラスタの全般ページUI問題 が修正され、ページがハングする場合がある
- CIFS共有、CIFSサービス、qtree、およびSVM SnapMirrorポリシーがバックエンドインベントリに追加されました。
- Logical inventoryセクションのUIナビゲーションメニューに共有およびqtreeを追加しました

- 選択したStorage VMから共有をタブとして追加しました
- Storage VMでCIFSが有効になっている場合に、Storage VMのGeneralタブにCIFSサービス情報が追加されました
- ネットアップストレージシステムの構成の検証に使用するクラスタチェックページがベストプラクティスに準拠していることを確認できるようになりました

2022年7月

- Capacityウィジェットでクラスタデータ削減比率のビジュアルが向上しました
- [Network Interfaces]ページにFCインターフェイスタブを追加しました
- 汎用の「新しいストレージボリューム」タスクを使用して新しいボリュームを作成すると、ボリュームのスペースギャランティがnoneに設定され、Snapshotリザーブの割合が0%に設定されるようになりました
- Edit Snapshot PolicyタスクのCommentフィールドは省略可能になり、必須ではなくなりました
- UIインベントリとオーケストレーションの一貫性が向上
- Cluster Capacityのサイト間の容量情報がSystem Managerと同じになりました
- 操作性を向上させるために新しい管理インターフェイスを作成する際にすべてのパラメータを表示するチェックボックスをStorage Virtual Machineタスクの下に追加しました
- クライアント一致より下にプロトコルを移動しましたが、System Managerと同じ結果が得られました
- エクスポートポリシーの一般ページにアクセスプロトコルが表示されるようになりました
- igroupの削除は、条件付きでログに記録される
- 新しいストレージNASデータインタフェースと新しいストレージiSCSIデータインタフェースの下に、NASの「フェールオーバーポリシー」および「自動設定」パラメータを追加
- 新規ストレージNASスマートボリュームのロールバックタスクで、他のボリュームが関連付けられていない場合にエクスポートポリシーが削除されるようになりました
- Smart VolumeとSmart LUNタスクの機能強化

2022 年 4 月

> 今後のリリースとの互換性を確保し、すべての機能を利用できるように、 NetApp Active IQ Unified Manager をバージョン 9.10P1 にアップグレードすることを推奨します。

- Ethernet Port Detail ページにブロードキャストドメインを追加
- ユーザインターフェイス内のアグリゲートおよび SVM の「集約」を「階層」に変更しました
- 「クラスタステータス」を「アレイステータス」に変更
- MTU フィルタが、 < 、 > 、 = 、 ⇐ 、 >= 文字に対応できるようになりました
- クラスタのインベントリにネットワークインターフェイスページが追加されました
- クラスタインベントリに AutoSupport を追加
- ノードに cdpd .enable オプションを追加
- CDP ネイバーのオブジェクトを追加しました

- Cisco Intersight にネットアップワークフローのストレージタスクが追加されました。を参照してください "使用例 3 デザイナフリーフォームを使用したカスタムワークフロー" NetApp ストレージ・タスクの一覧を表示します。

2022 年 1 月

- NetApp Active IQ Unified Manager 9.10 以降のイベントベースのサイト間アラームが追加されました。

> 今後のリリースとの互換性を確保し、すべての機能を利用できるようにするために、 NetApp Active IQ Unified Manager をバージョン 9.10 にアップグレードすることを推奨します。

- Storage Virtual Machine に対して各プロトコルを明示的に有効（ true または false ）に設定します
- clusterHealthStatus 状態を正常にマッピングしました。 -suppressed を OK に設定します
- クラスタリストページで Health 列の名前が Cluster Status 列に変更されました
- クラスタが停止しているか到達不能である場合に、ストレージアレイ「 Unreachable 」を表示します
- クラスタの全般ページで Health 列の名前が Array Status 列に変更されました
- SVM に「 Volumes 」タブが追加され、 SVM のすべてのボリュームが表示されます
- ボリュームに Snapshot 容量セクションがあります
- ライセンスが正しく表示されるようになりました

2021年10月

- Cisco Intersight に含まれるネットアップストレージのタスクの最新リストを追加しました。を参照してください "使用例 3 デザイナフリーフォームを使用したカスタムワークフロー" NetApp ストレージ・タスクの一覧を表示します。
- クラスタリストページに Health 列が追加されました。
- 選択したクラスタの全般ページで詳細が表示されるようになりました。
- ナビゲーションペインから NTP サーバテーブルにアクセスできるようになりました。
- Storage Virtual Machine の General ページを含む新しい Sensors タブが追加されました。
- VLAN およびリンクアグリゲーショングループの概要が、 Port General ページで使用できるようになりました。
- ボリューム合計容量テーブルに追加された合計データ容量列。
- Average Volume Statistics テーブル、 Average LUN Statistics テーブル、 Average Aggregate Statistics テーブル、 Average Storage VM Statistics テーブル、および Average Node Statistics テーブルに追加されたレイテンシ、 IOPS 、およびスループットの列

> 上記のパフォーマンス指標は、 NetApp Active IQ Unified Manager 9.9 以降で監視されるストレージアレイでのみ使用できます。

既知の問題

- AIQUM 9.11以前のバージョンを使用している場合は、ストレージリストページに表示される値とストレージ全般ページの容量バーグラフの値が一致しません。この問題 を解決するには、AIQUM 9.12以降にア

ップグレードして、表示される容量値が正確であることを確認します。

- AIQUM 9.11以前を使用している場合、[Integrated Systems]ページの[Interoperability（相互運用性）]タブで実行されたチェックでは、IMMとUCSMのCiscoコンポーネントを正確に区別できません。この問題 を解決するには、AIQUM 9.12にアップグレードして、すべてのコンポーネントが正しく識別されるようにします。
- データ収集プロセス中にサイト間ストレージのインベントリデータに影響がないようにするには、サポートされていないONTAP クラスタ（ONTAP 9.7P1より前のバージョン）をActive IQ Unified Manager（AIQUM）から削除する必要があります。
- 要求されているすべてのターゲットで、FlexPod 統合システム相互運用性クエリーを正常に完了するには、9.11以上のAIQUMバージョンが必要です。
- FQDNを使用してONTAP クラスタをAIQUMに追加すると、[Storage Inventory Checks]ページが表示されません。IPアドレスを使用してONTAP クラスタをAIQUMに追加する必要があります。

要件

NetApp ONTAPストレージとCisco Intersightを統合するためのハードウェア、ソフトウェア、ライセンスの要件を満たしていることを確認します。

ハードウェアとソフトウェアの要件

解決策の実装に必要な最小限のハードウェアコンポーネントとソフトウェアコンポーネントを以下に示します。解決策の特定の実装で使用されるコンポーネントは、お客様の要件に応じて異なる場合があります。

コンポーネント	要件の詳細
NetApp ONTAP	ONTAP 9.7P1 以降
NetApp Active IQ Unified Manager の略	最新バージョンのNetApp Active IQ Unified Manager が必要（現在は9.14RC1）
ネットアップストレージアレイ	ONTAP 9.7P1以降でサポートされるすべてのONTAP ASA、AFF、FASストレージアレイ
仮想化ハイパーバイザー	vSphere 7.0以降

を参照してください "Cisco Intersightでサポートされるシステム" Cisco UCS Compute Components と UCSM バージョンの最小要件については、を参照してください。

Cisco Intersight のライセンス要件

Cisco Intersightは、物理ストレージ（NetAppストレージ）の管理、自動化、最適化を行うインフラサービスやクラウドオーケストレーションサービスなどのサービスを提供しています。これらのサービスを使用して、Cisco UCSサーバとCisco HyperFlexシステムを管理できます。インフラサービスとCloud Orchestratorサービスでは、複数の階層を含むサブスクリプションベースのライセンスモデルが使用されます。選択したサブスクリプション期間に必要なCisco UCSサーバボリューム階層を選択できます。

ライセンスモデル

Cisco Intersightインフラサービスのライセンスモデルが簡易化され、次の2つのティアが提供されるようになりました。

- * Cisco Intersight Infrastructure Services Essentials *- Essentialsライセンスレベルは、グローバルヘルスモニタリング機能、インベントリ、Cisco TAC統合によるプロアクティブなサポート、多要素認証、SDKおよびAPIアクセスなどのサーバ管理を提供します。
- * Cisco Intersight Infrastructure Services Advantage *- Advantageライセンスレベルでは、高度なサーバ管理と拡張された可視性、エコシステムの統合、シスコおよびサードパーティ製ハードウェアとソフトウェアの自動化、マルチドメインソリューションを提供します。

さまざまなライセンスレベルでサポートされる機能の詳細については、を参照してください "Infrastructure Servicesライセンス"。

作業を開始する前に

ネットアップストレージの監視とオーケストレーションを Cisco Intersight から行うには、 NetApp Active IQ Unified Manager と Cisco Intersight Assist 仮想アプライアンスが vCenter 環境にインストールされている必要があります。

NetApp Active IQ Unified Manager をインストールまたはアップグレードします

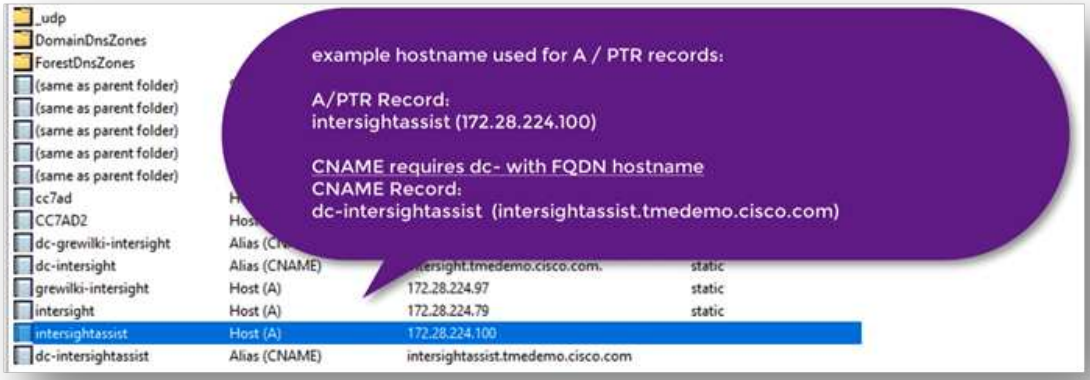
Active IQ Unified Manager（最新バージョンが必要、現在は9.14RC1）をインストールまたはアップグレードしていない場合はインストールします。手順については、を参照してください "NetApp Active IQ Unified Manager のドキュメント"。

Cisco Intersight Assist Virtual Appliance をインストールします

がを満たしていることを確認します "Cisco Intersight Virtual Appliance のライセンス、システム、ネットワークの要件"。

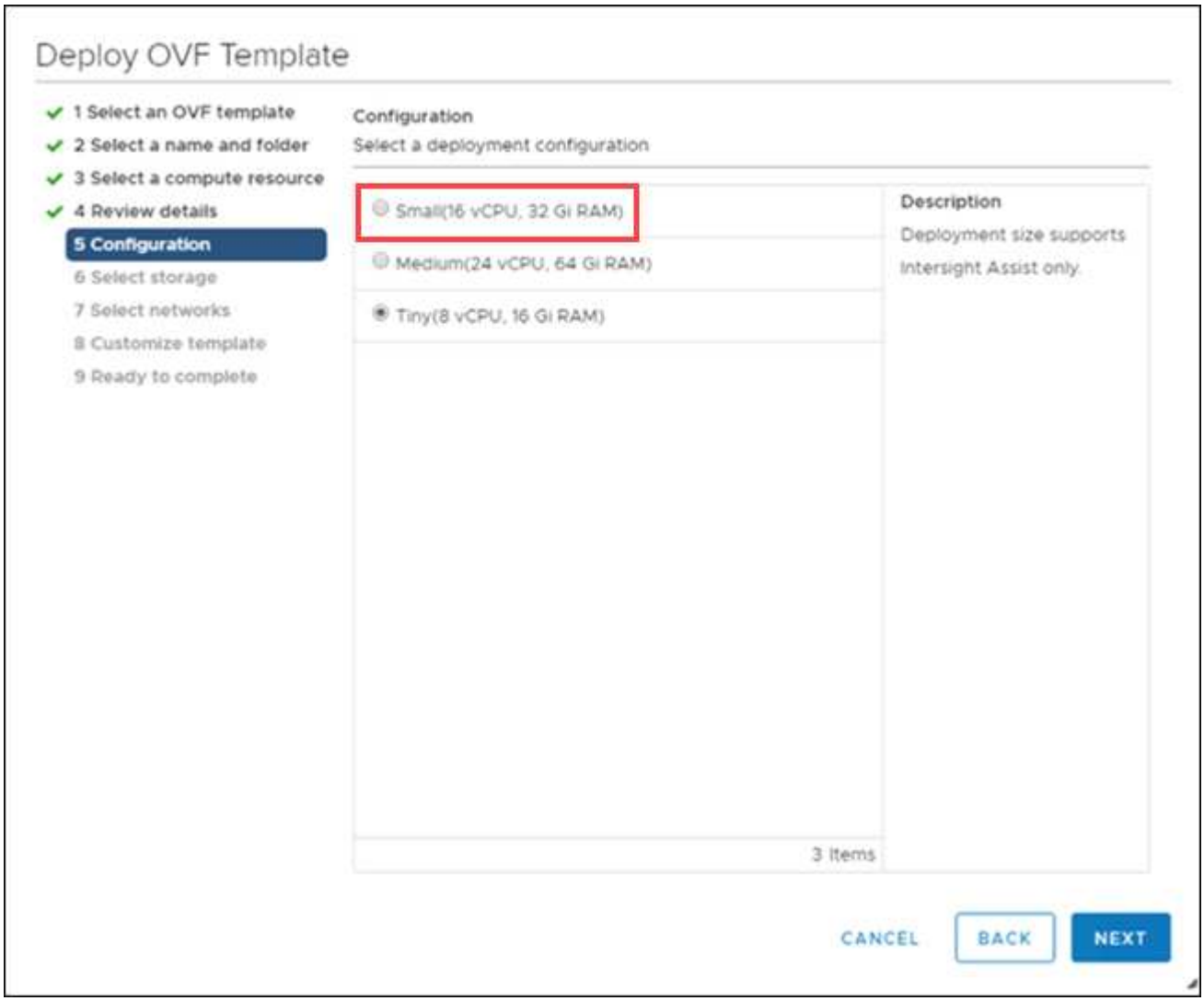
- 手順 *

1. Cisco Intersight アカウントを作成します。にアクセスします "https://intersight.com/" サイト間アカウントを作成します。Cisco Intersight アカウントを作成するには、有効な Cisco ID が必要です。
2. サイト間仮想アプライアンスは、からダウンロードできます "software.cisco.com"。詳細については、を参照してください "『 Intersight Appliance Install and Upgrade Guide 』を参照してください"。
3. OVA を導入します。OVA を導入するには、 DNS と NTP が必要です。
   a. OVA を導入する前に、 A / PTR レコードと CNAME エイリアスレコードを使用して DNS を設定します。以下の例を参照してください。

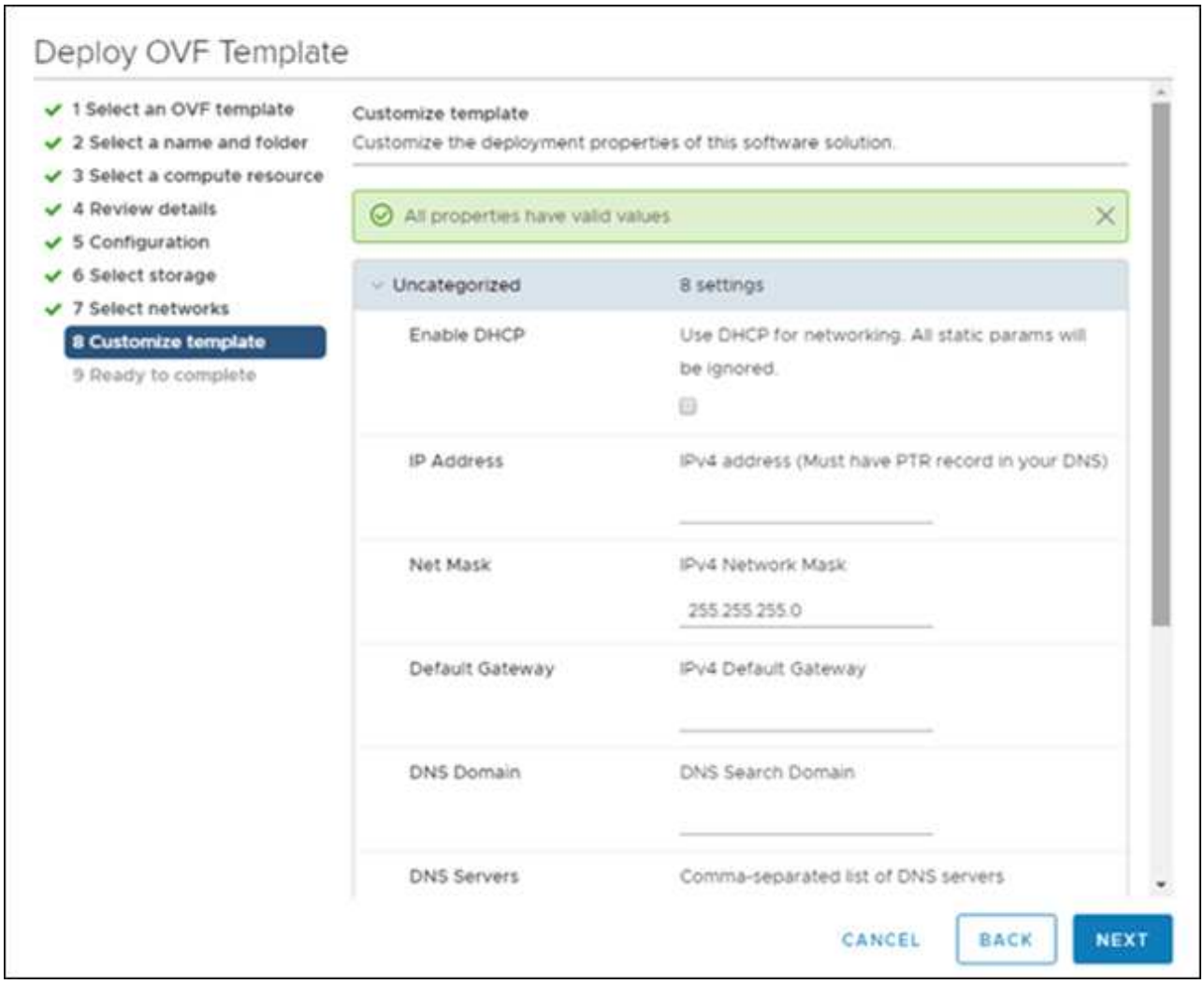


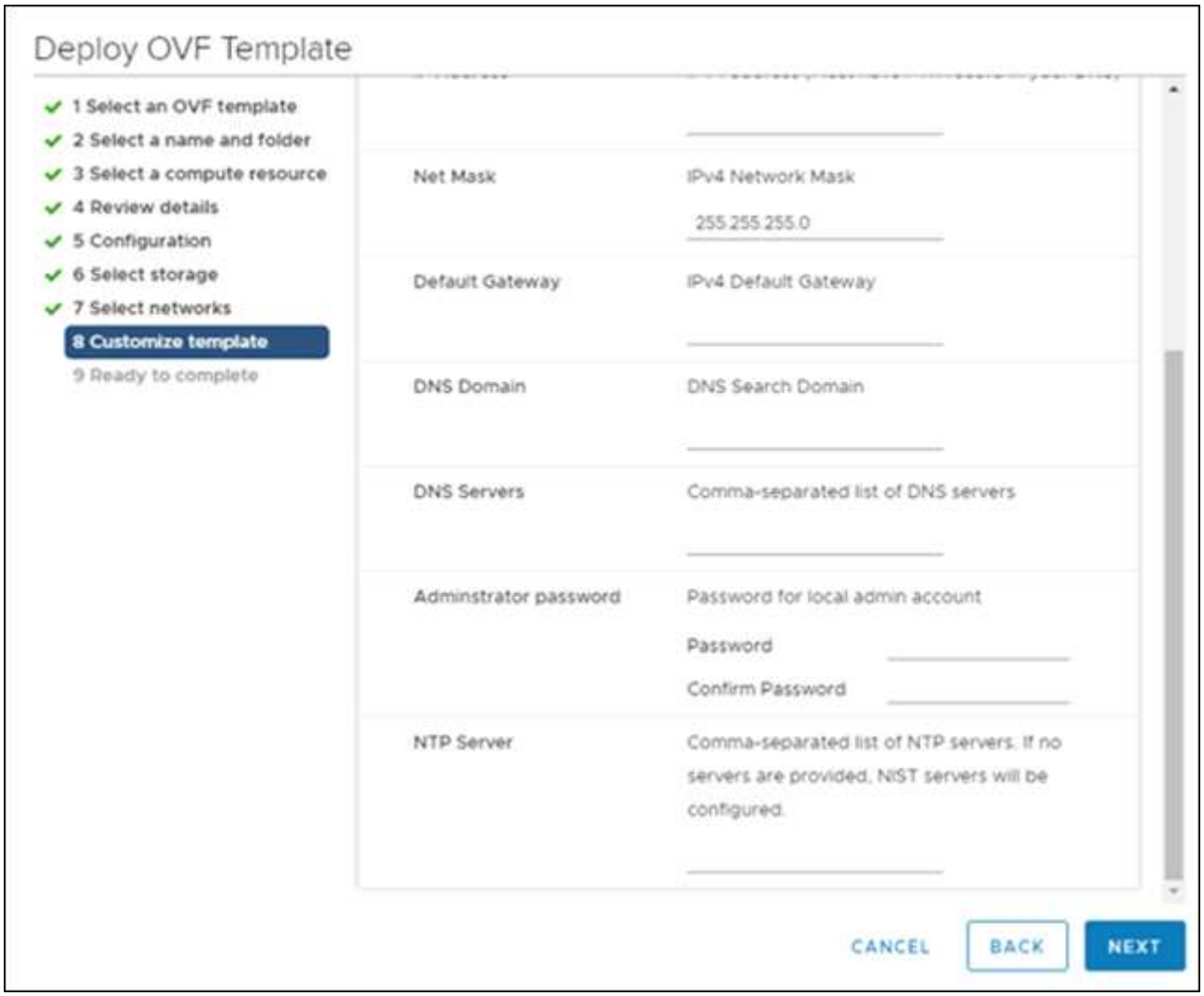
b. サイト間仮想アプライアンスの OVA 導入の要件に基づいて、適切な構成サイズ（小、小、中規模）を選択します。

- ヒント：ストレージオブジェクトの数が多い 2 ノード ONTAP クラスタの場合、小規模（ vCPU 16 、 Gi RAM ）オプションを使用することを推奨します。



a. [* テンプレートのカスタマイズ * （ Customize Template ）] ページで、 OVF テンプレートの展開プロパティをカスタマイズします。管理者パスワードはローカル・ユーザに使用されます admin （ WebUI / CLI / ssh ）





b. 「 * 次へ * 」をクリックします。

   1. Intersight Assist アプライアンスの導入後。

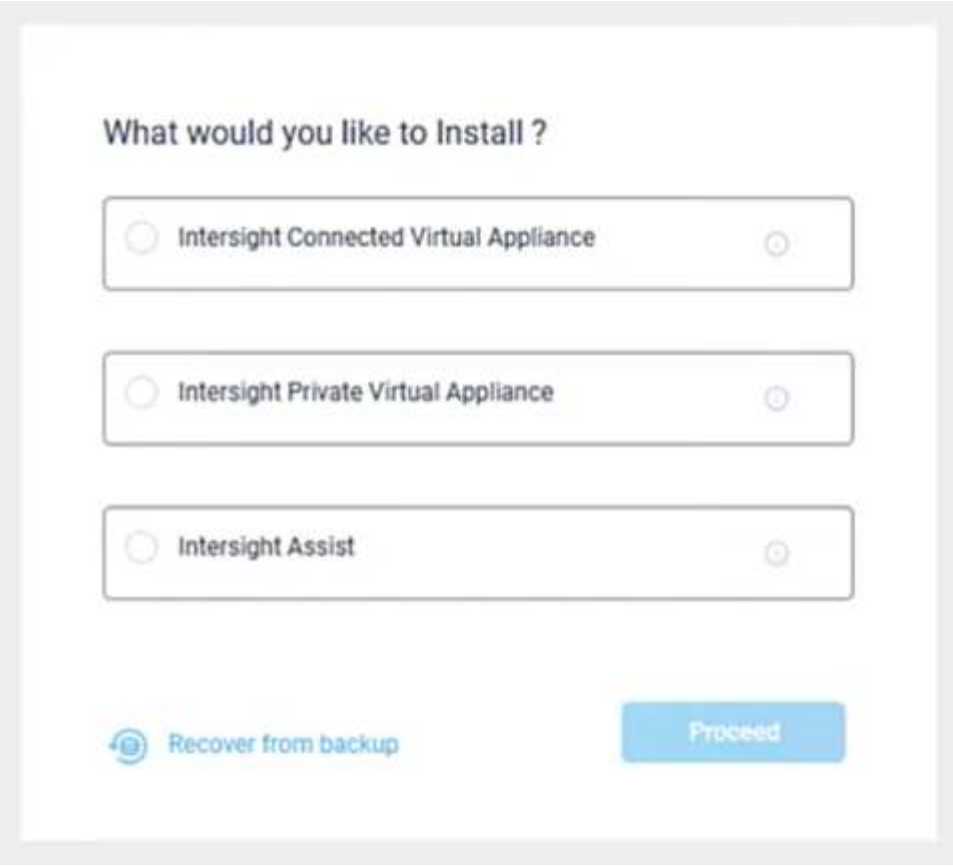
c. に移動します https://FQDN-of-your-appliance アプライアンスの設置後のセットアップを完了するには、次の手順を実行します。

   インストールプロセスが自動的に開始されます。Intersight.com への帯域幅によっては、インストールに最大 1 時間かかる場合があります。また、 VM の電源がオンになったあとでセキュアなサイトが稼働するまでに数秒かかることもあります。

d. 導入後のプロセスで、次のオプションを選択します。

   - * Intersight Assist 。 * この導入により、 SaaS モデルを Cisco Intersight に接続できるようになりました。

   「Intersight Assist」を選択する場合は、続行する前にデバイスIDと請求コードをメモしておきます。



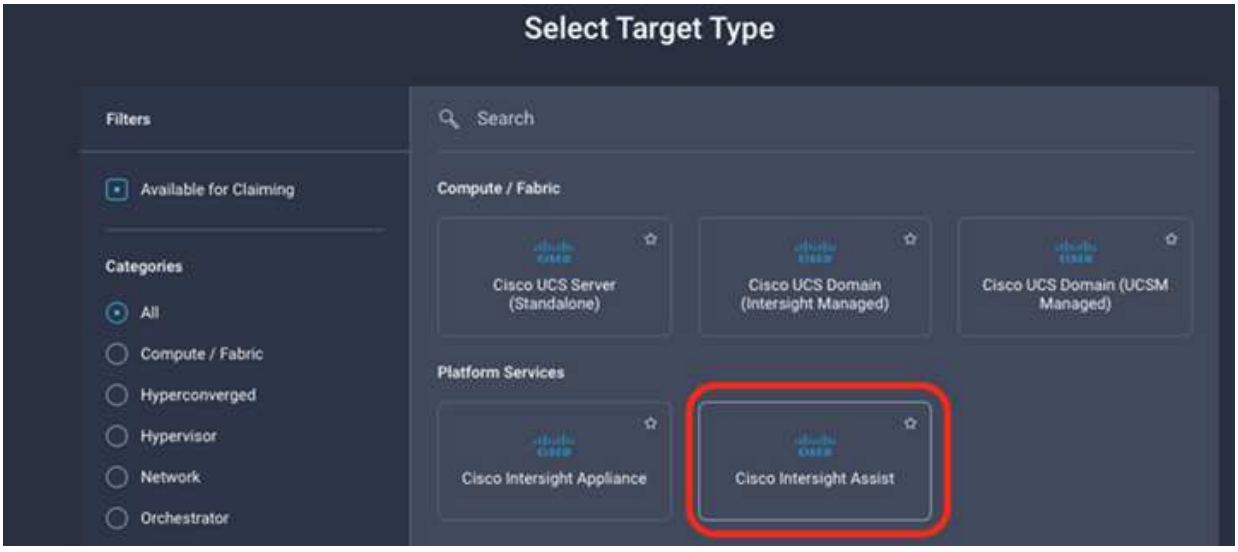
a. [* Proceed] をクリックします。

b. 「* Intersight Assist *」を選択し、次の手順を実行します。

   i. SaaS Intersight のアカウントに移動します "https://intersight.com"。

   ii. [**Targets**,**Cisco Intersight Assist**] 、 [**Start**] の順にクリックします。

   iii. 新しく導入した Intersight Assist 仮想アプライアンスからデバイス ID と請求コードをコピーして貼り付けることで、 * Cisco Intersight Assist * アプライアンスを要求します。



   iv. Cisco Intersight Assist * アプライアンスに戻り、 [* Continue] をクリックします。 * ブラウザの更新が必要になる場合があります。

ダウンロードとインストールのプロセスが開始されます。バイナリは、 Intersight Cloud からオンプレミスアプライアンスに転送されます。完了時間は、 Intersight Cloud への帯域幅によって異なります。

IMT サービス用にAIQ UMプロキシサーバを設定

NetApp ONTAP ストレージでAIQ UM for Cisco Intersightのプロキシサーバを使用している場合は、Interoperability Matrix Toolサービス（IMT ）を利用するためにコマンドラインインターフェイス（CLI）を使用してセットアップを設定する必要があります。IMT サービスは、[Integrated Systems]ページの[*Interoperability *]タブで使用できます。Active IQ Unified Manager UMプロキシサーバの設定には、仮想マシン（OVA）診断シェルを使用する必要があります。

> AIQ UM Diagシェルへのアクセス方法については、を参照してください "Active IQ Unified Manager 仮想マシン（OVA）のDIAGシェルへのアクセス方法"

- 手順 *

1. AIQ UMターミナルにログインし、次のコマンドを実行してUMにログインします。

```
um cli login -u <um maintenance user name>
```

- 例 *

```
um cli login -u admin
```

1. 次のコマンドを実行して'imm_proxy_host'およびimm_proxy_port'を設定します

> IMT プロキシは、AutoSupport （ASUP）プロキシ設定とは別の設定です。

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

- 例 *

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

> IMT プロキシサーバ構成では、認証はサポートされていません。

1. 次のコマンドを使用してIMT プロキシの詳細を表示し'proxy_host'およびproxy_port'の設定を確認します

```
um option list |grep imt
```

クレームの目標

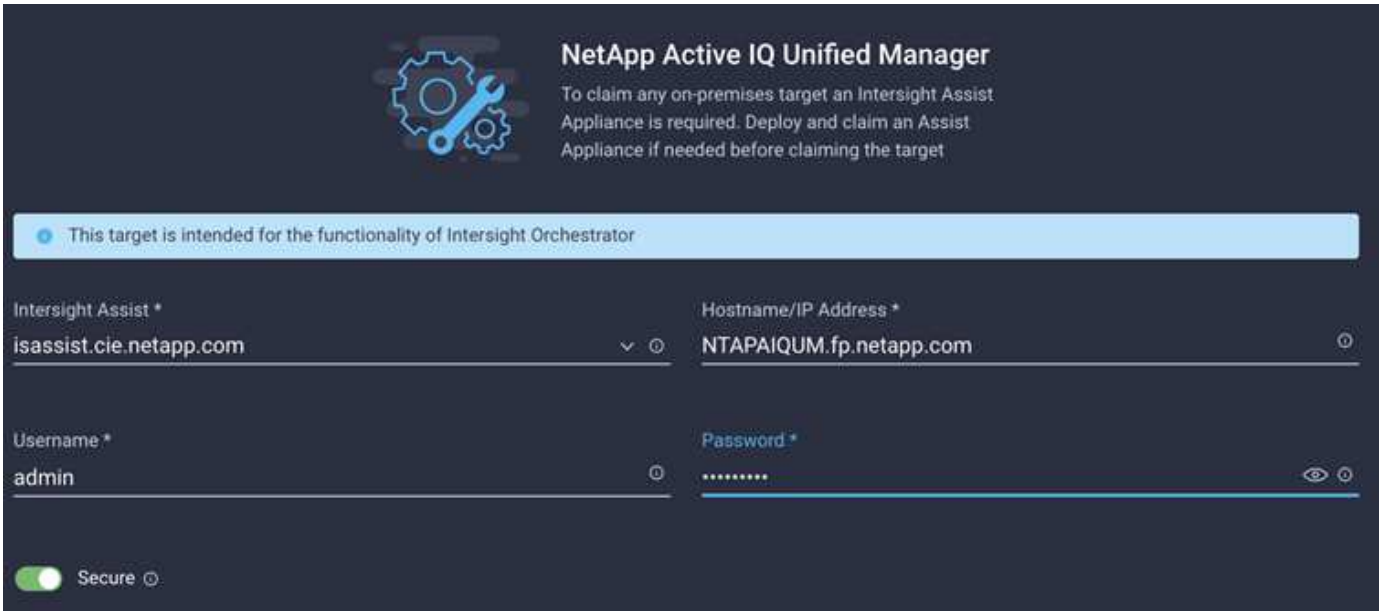
Cisco Intersight Assist をインストールすると、ネットアップのストレージデバイスと仮想化デバイスを請求できます。「 * Intersight Targets * 」ページに戻り、 vCenter と NetApp Active IQ Unified Manager のターゲットを追加します。請求プロセスの詳細については、ビデオをご覧ください "Cisco Intersight Assist を使用してターゲットを請求します。"

> NetApp Active IQ Unified Manager （ AIQ UM ） API ゲートウェイが有効になっていることを確認します。

NetApp IQ Unified Managerで、* Settings > General > Feature Settings *の順に選択します。

次の例は、 Cisco Intersight の NetApp AIQ UM ターゲットを請求する方法を示しています。

> NetApp AIQ UM ターゲットを要求すると、 Active IQ Unified Manager で管理されるすべてのクラスタが自動的にサイト間に追加されます。

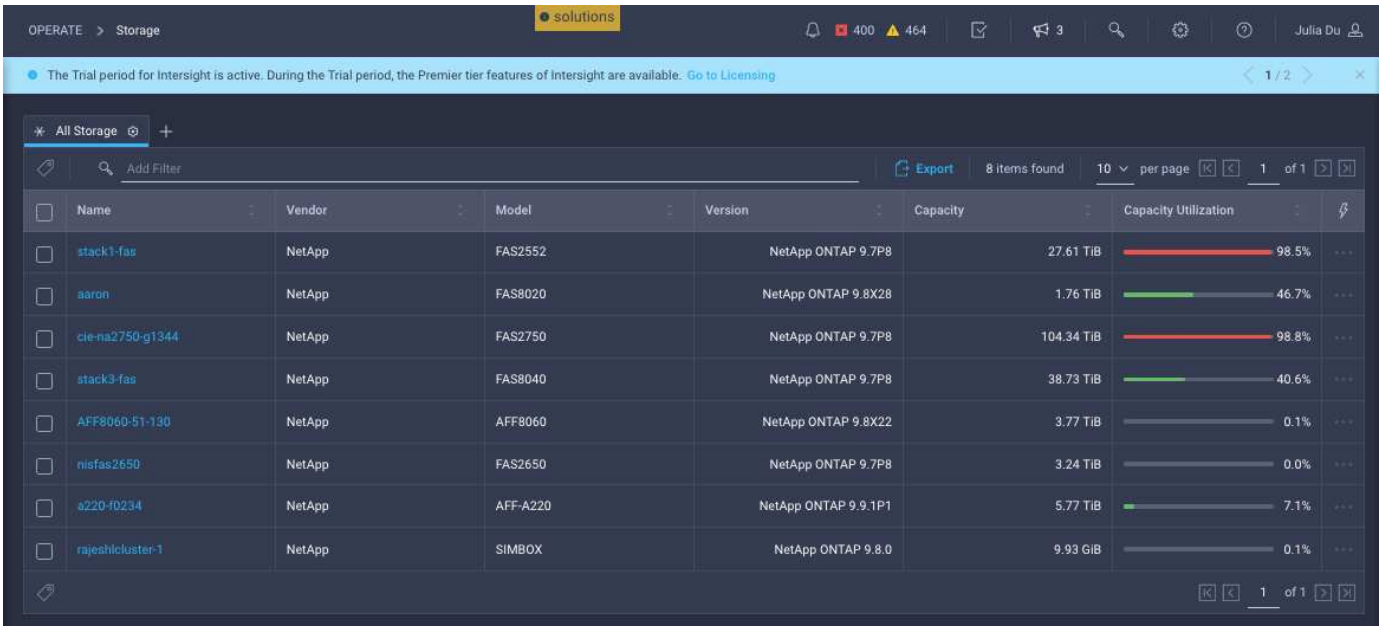


Cisco Intersight からネットアップストレージを監視

ターゲットへの請求が完了すると、 Advantage Tier ライセンスがある場合は、ネットアップストレージウィジェット、ストレージインベントリ、および仮想化の各タブを使用できるようになります。Premier Tier ライセンスがある場合は、オーケストレーションタブを使用できます。

ストレージインベントリの概要

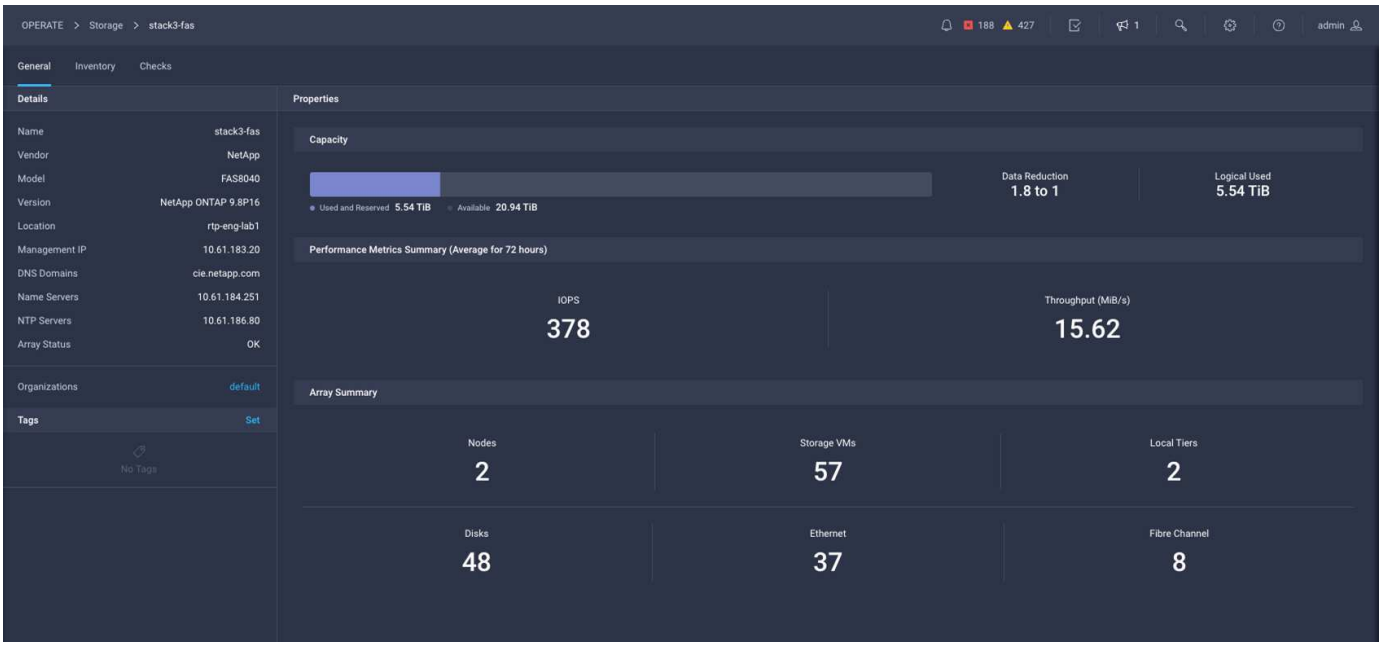
次のスクリーンショットは、 * Operate > Storage * 画面を示しています。



画面を示しています"]

次のスクリーンショットは、ストレージクラスタの概要を示しています。

以下のパフォーマンス指標の概要情報は、ストレージアレイが NetApp Active IQ Unified Manager 9.9 以上を介して監視されている場合にのみ表示されます。



ストレージウィジェット

ストレージウィジェットを表示するには、 * Monitoring > Dashboards > View NetApp Storage widgets * に移動します。

- 次のスクリーンショットは、ストレージバージョンサマリウィジェットを示しています。

- このスクリーンショットは、容量利用率別の上位 5 つのストレージアレイを示しています。

Top 5 Storage Arrays by Capacity Utilization

#	Name	Vendor	Capacity	Utilization
1	Warriors_Controller	NetApp	13.83 TiB	89.4%
2	stack3-fas	NetApp	8.95 TiB	66.2%
3	aaron	NetApp	4.71 TiB	44.1%
4	aff-a400	NetApp	40.62 TiB	0.2%

- このスクリーンショットは、容量利用率別の上位 5 つのストレージボリュームを示しています。

Top 5 Storage Volumes by Capacity Utilization

#	Name	Vendor	Capacity	Utilization
1	test_1_vol	NetApp	10.31 GiB	98.6%
2	test_lun_vol	NetApp	10.31 GiB	97.9%
3	vmware_server_1	NetApp	50.00 GiB	95.0%
4	vmware_server_2	NetApp	50.00 GiB	82.3%
5	VM_Datastore_vol	NetApp	150.00 GiB	67.0%

ユースケース

これらは、 Cisco Intersight のネットアップストレージの監視とオーケストレーションのユースケース例です。

ユースケース 1 ：ネットアップストレージのインベントリとウィジェットを監視する

ネットアップストレージ環境が Cisco Intersight に存在する場合は、ネットアップストレージオブジェクトをストレージインベントリから詳細に監視し、ストレージウィジェットの概要を確認できます。

1. Intersight Assist OVA を導入（ vCenter 環境ではオンプレミスのタスク）
2. Intersight Assist に NetApp AIQ UM デバイスを追加します。
3. 「 * Storage * 」に移動して、ネットアップストレージインベントリをナビゲートします。
4. ネットアップストレージのウィジェット * を監視ダッシュボード * に追加します。

   はです "リンク" からビデオに、 ONTAP ストレージ監視機能を Cisco Intersight から紹介しています。

ユースケース2：リファレンスワークフローを使用した**NetApp**ストレージオーケストレーション

Cisco IntersightでNetAppストレージ環境とvCenter環境を利用できる場合は、次のURLからGitHubで提供されているエンドツーエンドのリファレンスワークフローを使用できます。 "FlexPod Intersightワークフローリポジトリ"。

リファレンスワークフローには、ストレージと仮想化のタスクが含まれています。リポジトリのREADMEファイルには、ワークフローの実行に必要な前提条件、役立つリソースへのリンク(ワークフローのインポート方法に関するドキュメントを含む)、および各参照ワークフローのドキュメントリンクが含まれています。

各ワークフローには'リポジトリ内に次の2つのファイルを含むフォルダがあります

- ダウンロードしてIntersightにインポートするJSONファイル
- ワークフロー内のタスクのビュー、ワークフロー入力、およびワークフローの実行例を提供するドキュメントファイル。

参照ワークフローをインポートして使用するには、次の手順を実行します。

1. Intersight Assist OVA を導入（ vCenter 環境ではオンプレミスのタスク）
2. Intersight Assist に NetApp AIQ UM デバイスを追加します。
3. Intersight Assist を介して vCenter ターゲットを Intersight に追加します。
4. 参照ワークフロー用のJSONファイルをFlexPod - Intersight - Workflowリポジトリからダウンロードします。
5. ワークフローをIntersightにインポートし、ワークフローを実行します。

GitHub FlexPod - Intersight - Workflowリポジトリで利用可能なワークフローのリストを次に示します。

- NetAppイニシエータグループにイニシエータを追加します

- NetAppボリュームの新しいエクスポートポリシー
- NetAppスマートボリュームを使用した新しいNASデータストア
- 新しいNetApp FCデータインターフェイス
- 新しいNetAppイニシエータグループ
- 新しいNetApp iSCSIデータインターフェイス
- 新しいNetApp NASデータインターフェイス
- 新しいNetApp Storage Virtual Machineの略
- NetAppスマートLUNを使用した新しいVMFSデータストア
- NetAppイニシエータグループからイニシエータを削除
- NetAppスマートボリュームを使用したNASデータストアの削除
- NetAppエクスポートポリシーを削除します
- NetAppイニシエータグループを削除します
- NetAppスマートLUNを使用したVMFSデータストアの削除
- NetAppスマートボリュームを使用したNASデータストアの更新
- NetAppスマートLUNを使用したVMFSデータストアの更新

使用事例 3 ：デザイナー不要のフォームを使用したカスタムワークフロー

ネットアップストレージ環境と vCenter 環境が Cisco Intersight に存在する場合は、ネットアップのストレージと仮想化タスクを使用してカスタムワークフローを構築できます。

1. サイト間アシスト OVA の導入（ vCenter 環境ではオンプレミスのタスク）
2. Intersight Assist に NetApp AIQ UM デバイスを追加します。
3. Intersight Assist を介して vCenter ターゲットを Intersight に追加します。
4. Intersight の「 * Orchestration 」タブに移動します。
5. [ワークフローの作成 *] を選択します。
6. ストレージと仮想化のタスクをワークフローに追加できます。

   Cisco Intersight には、次のネットアップストレージタスクが用意されています。

   - NetApp CIFS共有へのACLの追加
   - NetAppエクスポートポリシールールへのクライアント一致の追加
   - NetAppボリュームにエクスポートポリシーを追加してください
   - NetAppイニシエータグループにイニシエータを追加します
   - NetAppエクスポートポリシーにルールを追加します
   - NetApp Snapshotポリシーにスケジュールを追加します
   - NetAppライセンスステータスの確認
   - NetApp Storage Virtual MachineのFCPプロトコルステータスの確認

- Storage Virtual MachineのNetAppアグリゲートを編集します
- NetApp非同期SnapMirrorポリシーの編集
- NetApp CIFS共有ACL権限の編集
- NetAppエクスポートポリシールールの編集
- NetApp Snapshotポリシーを編集します
- NetApp Snapshotポリシーのスケジュールを編集します
- NetAppボリュームのセキュリティ形式の編集
- NetAppボリュームのSnapshotポリシーの編集
- NetApp CIFSサービスの有効化
- NetApp LUNを展開します
- 新しいNetApp非同期SnapMirrorポリシー
- 新しいNetApp CIFSサーバ
- 新しいNetApp CIFS共有
- NetAppイニシエータグループのLUNマップを検索します
- IDでNetApp LUNを検索します
- IDでNetAppボリュームを検索します
- 新しいNetAppエクスポートポリシー
- 新しいNetApp FCデータインターフェイス
- 新しいNetAppイニシエータグループ
- 新しいNetApp iSCSIデータインターフェイス
- SVMルートボリュームの新しいNetApp負荷共有ミラー
- 新しいNetApp LUN
- 新しいNetApp LUNマップ
- 新しいNetApp NASデータインターフェイス
- 新しいNetApp NASスマートボリューム
- 新しいNetAppスマートLUN
- ボリュームの新しいNetApp SnapMirror関係
- 新しいNetApp Snapshotポリシー
- 新しいNetApp Storage Virtual Machineの略
- 新しいNetAppボリューム
- 新しいNetAppボリュームSnapshot
- NetApp Storage Virtual MachineのDNSの登録
- NetApp CIFS共有からACLを削除する
- NetAppエクスポートポリシールールからクライアント一致を削除

- NetAppボリュームからエクスポートポリシーを削除します
- NetAppイニシエータグループからイニシエータを削除
- NetApp CIFSサーバの削除
- NetApp CIFS共有の削除
- NetAppエクスポートポリシーを削除します
- NetApp FCデータインターフェイスを削除
- NetAppイニシエータグループを削除します
- NetApp IPインターフェイスを削除します
- SVMルートボリュームのNetApp負荷共有ミラーの削除
- NetApp LUNを削除します
- NetApp LUNマップを削除します
- NetApp NASスマートボリュームを削除します
- NetAppスマートLUNを削除します
- ボリュームのNetApp SnapMirror関係の削除
- NetApp SnapMirrorポリシーを削除
- NetApp Snapshotポリシーを削除します
- NetApp Storage Virtual Machineを削除します
- NetAppボリュームを削除します
- NetAppボリュームSnapshotを削除します
- NetAppエクスポートポリシーからルールを削除します
- NetApp Snapshotポリシーからスケジュールを削除します
- NetAppボリュームSnapshotの名前を変更します
- SVMルートボリュームのNetApp負荷共有ミラーの更新
- NetAppボリュームの容量を更新します

ネットアップのストレージと仮想化タスクを使用したワークフローのカスタマイズの詳細については、ビデオをご覧ください "Cisco Intersight の NetApp ONTAP ストレージオーケストレーション"。

インフラ

Cisco UCSM 、 VMware vSphere 7.0 、および NetApp ONTAP 9 を使用した FlexPod 向けのエンドツーエンド NVMe

TR-4914 ：『 End-to-End NVMe for FlexPod with Cisco UCSM 、 VMware vSphere 7.0 、 and NetApp ONTAP 9 』

ネットアップ Chris Schmitt と Kamini Singh

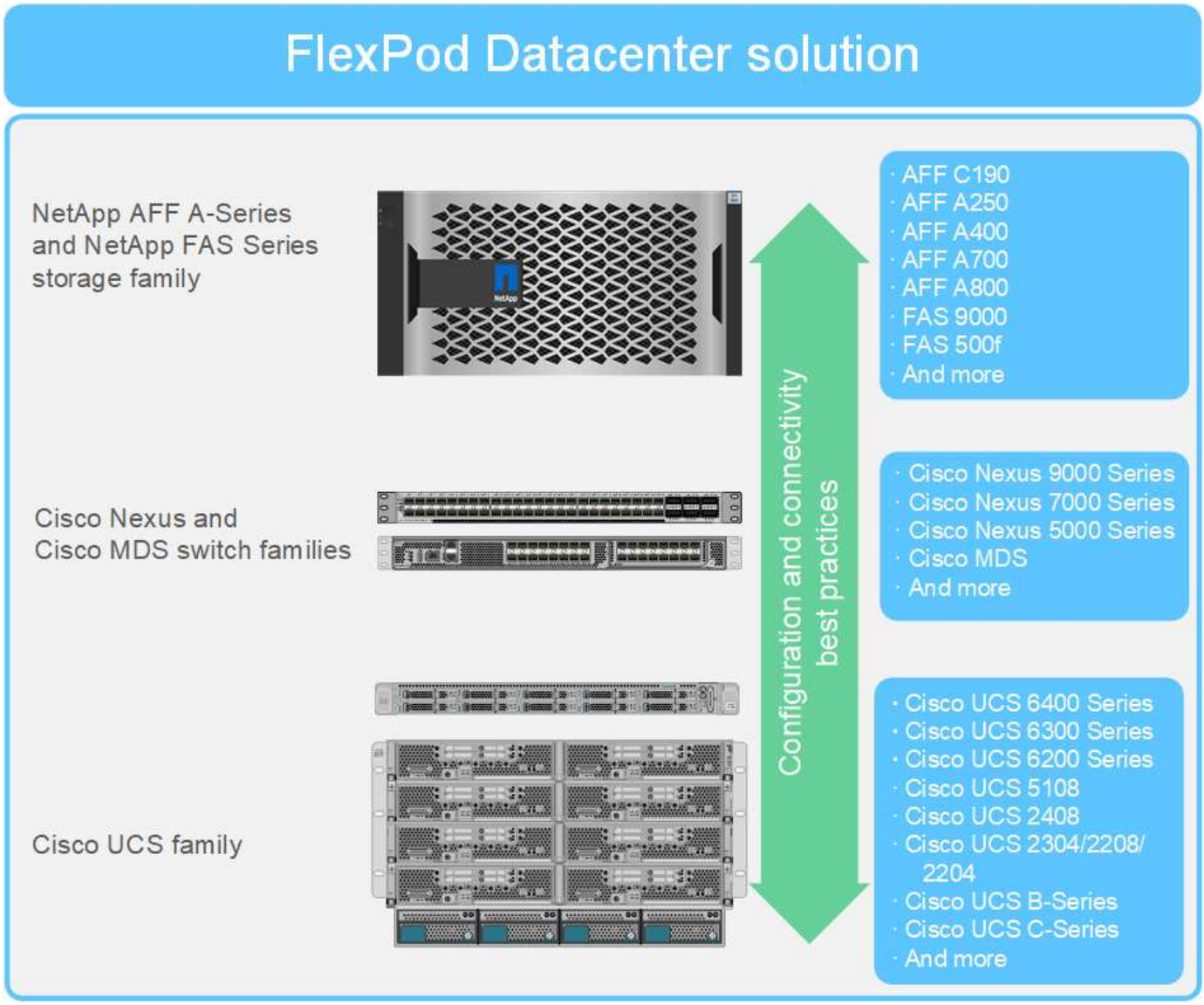
協力：

最先端のコアテクノロジである NVMe データストレージ標準は、現在および将来のメモリテクノロジに非常に広帯域で超低レイテンシのストレージアクセスを提供することで、エンタープライズデータストレージのアクセスと転送を変革しています。NVMe は、 SCSI コマンドセットを NVMe コマンドセットに置き換えます。

NVMe は、不揮発性フラッシュドライブ、マルチコア CPU 、ギガバイト単位のメモリを搭載するように設計されています。また、 1970 年代からコンピュータサイエンスの大きな進歩を活かし、より効率的にデータを解析して操作できる合理化されたコマンドセットを実現しています。エンドツーエンドの NVMe アーキテクチャを採用することで、データセンター管理者は、仮想環境とコンテナ化環境をどの程度まで拡張できるか、またトランザクション指向データベースでサポートできる拡張性の程度を再考することができます。

FlexPod は、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus スイッチ、 Cisco MDS スイッチ、 NetApp AFF システムを含む、ベストプラクティスのデータセンターアーキテクチャです。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優れたプラットフォームを提供します。FlexPod はスケールアップとスケールアウトに対応しており、パフォーマンスと容量の向上（コンピューティング、ネットワーク、またはストレージのリソースを必要に応じて個別に追加）が可能です。また、複数の一貫した導入が必要な環境（ FlexPod スタックの追加ロールアウトなど）ではスケールアウトすることもできます。

次の図に、 FlexPod コンポーネントファミリーを示します。



FlexPod は FC-NVMe を導入するための理想的なプラットフォームです。既存の Cisco UCS B200 M5 サーバまたは M6 サーバ、または Cisco UCS C シリーズ M5 または M6 ラックサーバに Cisco UCS VIC 1400 シリーズおよびポートエクスパンダを追加し、 Cisco UCS システム、 Cisco MDS 32Gbps スイッチへの無停止でのシンプルなソフトウェアアップグレードをサポートします。 および NetApp AFF ストレージアレイで使用できます。サポート対象のハードウェアとソフトウェアを導入したあとの FC-NVMe 設定は、 FCP の設定と似ています。

NetApp ONTAP 9.5 以降には、包括的な FC-NVMe 解決策が搭載されています。AFF A300 、 AFF A400 、 AFF A700 、 AFF A700s 、および AFF A800 アレイの ONTAP ソフトウェアを無停止で更新することで、これらのデバイスでエンドツーエンドの NVMe ストレージスタックがサポートされます。そのため、第 6 世代の Host Bus Adapter （ HBA ；ホストバスアダプタ）と NVMe ドライバがサポートされているサーバは、ネイティブの NVMe を使用してこれらのアレイと通信できます。

目的

この解決策は、 FlexPod 上の VMware vSphere 7 における FC-NVMe パフォーマンスの概要を示しています。解決策は、 FC-NVMe トラフィックを正常に通過できることが確認され、さまざまなデータブロックサイズの FC-NVMe に対してパフォーマンスメ米はキャプチャされた。

解決策のメリット

FlexPod 向けエンドツーエンド NVMe は、解決策がもたらす次のメリットを通じて、お客様に卓越した価値を提供します。

- NVMe は、高速で広帯域のハードウェアプロトコルである PCIe を利用しています。これは、 SCSI 、 SAS 、 SATA などの従来の標準規格に比べてはるかに高速です。Cisco UCS サーバとネットアップストレージアレイ間の広帯域幅、超低レイテンシ接続により、要件の厳しいアプリケーションの大部分に対応します。
- FC-NVMe 解決策はロスレスであり、次世代アプリケーションの拡張性要件に対応できます。こうした新しいテクノロジには、人工知能（ AI ）、機械学習（ ML ）、ディープラーニング（ DL ）、リアルタイム分析、その他ミッションクリティカルなアプリケーションなどがあります。
- スタック全体のすべてのリソースを効率的に使用することで、 IT コストを削減します。
- 応答時間を大幅に短縮し、アプリケーションのパフォーマンスを大幅に向上させます。これは、 IOPS とスループットの向上に対応し、レイテンシを低減します。解決策は、パフォーマンスを最大 60% 向上し、既存のワークロードのレイテンシを最大 50% 低減します。
- FC-NVMe は効率的なプロトコルで、優れたキューイング機能を備えています。特に、 1 秒あたりの I/O 処理数（ IOPS 、トランザクション数）が増え、アクティビティが並列に処理される場合に適しています。
- Cisco UCS 、 Cisco MDS 、 NetApp AFF ストレージアレイなどの FlexPod コンポーネントのソフトウェアを無停止でアップグレードできます。アプリケーションを変更する必要はありません。

"次のステップ：テストアプローチ"

テストアプローチ

"前へ：はじめに。"

ここでは、 FC-NVMe on FlexPod の検証テストの概要を示します。また、 VMware vSphere 7 を使用した FC-NVMe for FlexPod に関してワークロードのテストを実行するために採用したテスト環境とテスト計画の両方が含まれます。

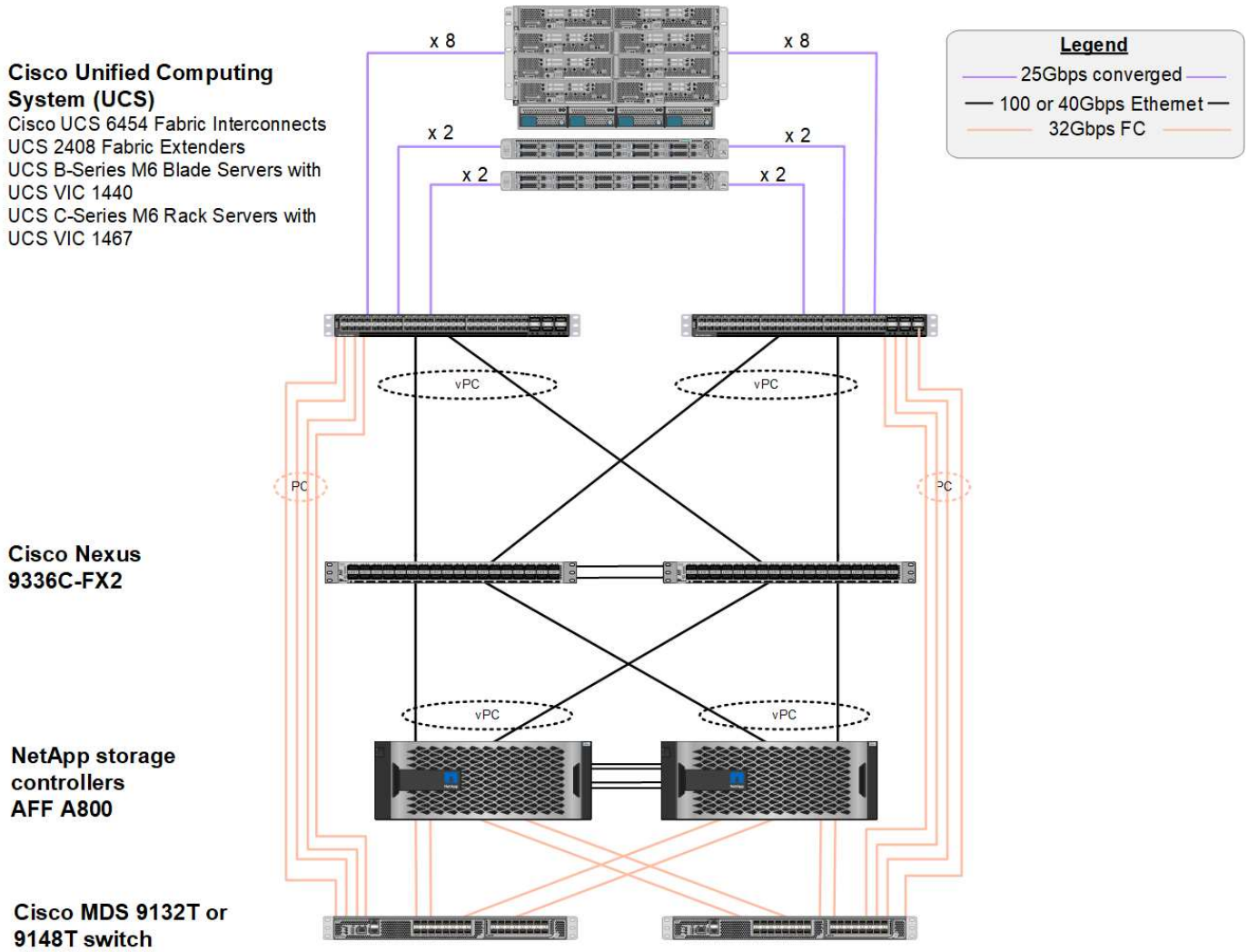
テスト環境

Cisco Nexus 9000 シリーズスイッチは、次の 2 つの動作モードをサポートします。

- NX-OS スタンドアロンモード、 Cisco NX-OS ソフトウェアを使用
- Cisco Application Centric Infrastructure （ Cisco ACI ）プラットフォームを使用する ACI ファブリックモード

スタンドアロンモードでは、スイッチは一般的な Cisco Nexus スイッチのように機能し、ポート密度、低レイテンシ、 40GbE および 100GbE 接続を向上させます。

NX-OS を搭載した FlexPod は、コンピューティング、ネットワーク、ストレージの各レイヤで完全な冗長性を実現するように設計されています。デバイスまたはトラフィックパスの観点からは、単一点障害はありません。次の図は、この FC-NVMe の検証で使用した最新の FlexPod 設計のさまざまな要素の接続を示しています。



この設計では、 FC SAN の観点から、最新の第 4 世代 Cisco UCS 6454 ファブリックインターコネクトと、サーバにポートエクスパンダを備えた Cisco UCS VIC 1400 プラットフォームを使用しています。Cisco UCS シャーシ内の Cisco UCS B200 M6 ブレードサーバは、 Cisco UCS 2408 ファブリックエクステンダ IOM に接続されたポートエクスパンダ付き Cisco UCS VIC 1440 を使用し、各 Fibre Channel over Ethernet （ FCoE ）仮想ホストバスアダプタ（ vHBA ）の速度は 40Gbps です。Cisco UCS C220 M5 ラックサーバは、 Cisco UCS VIC 1457 を使用し、各ファブリックインターコネクトに 25Gbps インターフェイスを 2 つ搭載しています。各 C220 M5 FCoE vHBA の速度は 50 Gbps です。

ファブリックインターコネクトは、 32Gbps SAN ポートチャネルを介して、最新世代の Cisco MDS 9148T または 9132T FC スイッチに接続します。Cisco MDS スイッチと NetApp AFF A800 ストレージクラスタ間の接続も 32Gbps FC です。この構成では、ストレージクラスタと Cisco UCS の間で 32Gbps FC 、 FCP 、 FC-NVMe ストレージがサポートされます。この検証では、各ストレージコントローラへの FC 接続が 4 つ使用されます。各ストレージコントローラでは、 FCP と FC-NVMe の両方のプロトコルに 4 つの FC ポートが使用されます。

Cisco Nexus スイッチと最新世代の NetApp AFF A800 ストレージクラスタ間の接続も 100Gbps で、ストレージコントローラのポートチャネルとスイッチの vPC もあります。NetApp AFF A800 ストレージコントローラには、高速の Peripheral Connect Interface Express （ PCIe ）バス上に NVMe ディスクが搭載されています。

この検証で使用する FlexPod の実装方法は、に基づいています "UCS 管理モードの FlexPod データセンター（ Cisco UCS 4.2(1) 、 VMware vSphere 7.0U2 、および NetApp ONTAP 9.9 ）"。

検証済みのハードウェアとソフトウェア

次の表に、解決策の検証プロセスで使用したハードウェアとソフトウェアのバージョンを示します。Cisco とネットアップは、相互運用性マトリックスを用意しています。これらのマトリックスは、 FlexPod の具体的な実装についてサポートが必要かどうかを確認するために参照してください。詳細については、次のリソースを参照してください。

- "NetApp Interoperability Matrix Tool で確認できます"
- "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"

レイヤー（ **Layer** ）	デバイス	イメージ（ **Image** ）	コメント
コンピューティング	• Cisco UCS 6454 ファブリックインターコネクト × 2 • Cisco UCS 5108 ブレードシャーシ × 1 （ Cisco UCS 2408 I/O モジュール × 2 • Cisco UCS B200 M6 ブレード × 4 （各 Cisco UCS VIC 1440 アダプタおよびポートエキスパンダカード × 1	リリース 4.2 （ 1f ）	Cisco UCS Manager 、 Cisco UCS VIC 1440 、およびポートエクスパンダが含まれます
CPU	2.0 GHz の Intel Xeon Gold 6330 CPU × 2 、 42 MB のレイヤ 3 キャッシュ、 CPU あたり 28 コア	–	–
メモリ	1 、 024GB （ 3200 MHz で動作する 64 GB DIMM × 16 ）	–	–
ネットワーク	NX-OS スタンドアロンモードの 2 台の Cisco Nexus 9336C-FX2 スイッチ	リリース 9.3(8)	–
ストレージネットワーク	Cisco MDS 9132T 32Gbps 32 ポート FC スイッチ × 2	リリース 8.4 （ 2c ）	FC-NVMe SAN 分析をサポートします
ストレージ	1.8TB NVMe SSD × 24 搭載の NetApp AFF A800 ストレージコントローラ × 2	NetApp ONTAP 9.9.3.1P1	–
ソフトウェア	Cisco UCS Manager の略	リリース 4.2 （ 1f ）	–
	VMware vSphere の場合	7.0U2	–
	VMware ESXi	7.0.2 の場合	–

レイヤー（ **Layer** ）	デバイス	イメージ（ **Image** ）	コメント
	VMware ESXi ネイティブファイバチャネル NIC ドライバ（ NFNIC ）	5.0.0.12	VMware で FC-NVMe をサポートします
	VMware ESXi ネイティブイーサネット NIC ドライバ（ NENIC ）	1.0.35.0	–
テストツール	fio	3.19	–

テスト計画

また、統合型ワークロードを使用して FlexPod 上の NVMe を検証するパフォーマンステスト計画を作成しました。このワークロードにより、 8KB のランダムリードおよびライト、および 64KB の読み取りと書き込みを実行できました。AFF A800 ストレージに対して、 VMware ESXi ホストを使用してテストケースを実行しました。

パフォーマンス測定に使用できるオープンソースの合成 I/O ツールである fio を使用して、合成ワークロードを生成しました。

パフォーマンステストを完了するために、ストレージとサーバの両方でいくつかの設定手順を実行しました。実装の詳細な手順は次のとおりです。

1. ストレージ側で、 4 つの Storage Virtual Machine （ SVM 、旧 Vserver ）、 1 つの SVM に 8 つのボリューム、 1 つのボリュームに 1 つのネームスペースを作成しました。1TB のボリュームと 960GB のネームスペースを作成しました。SVM ごとに 4 つの LIF と、 SVM ごとに 1 つのサブシステムを作成しました。SVM LIF は、クラスタ上の使用可能な 8 つの FC ポートに均等に分散されました。
2. サーバ側で、 ESXi ホストごとに 1 つの仮想マシン（ VM ）を作成し、合計 4 台の VM を構築しました。統合型ワークロードを実行するために、サーバに fio をインストールしました。
3. ストレージと VM の構成が完了すると、 ESXi ホストからストレージネームスペースに接続できるようになります。そのため、ネームスペースに基づいてデータストアを作成し、それらのデータストアに基づいて仮想マシンディスク（ VMDK ）を作成することができました。

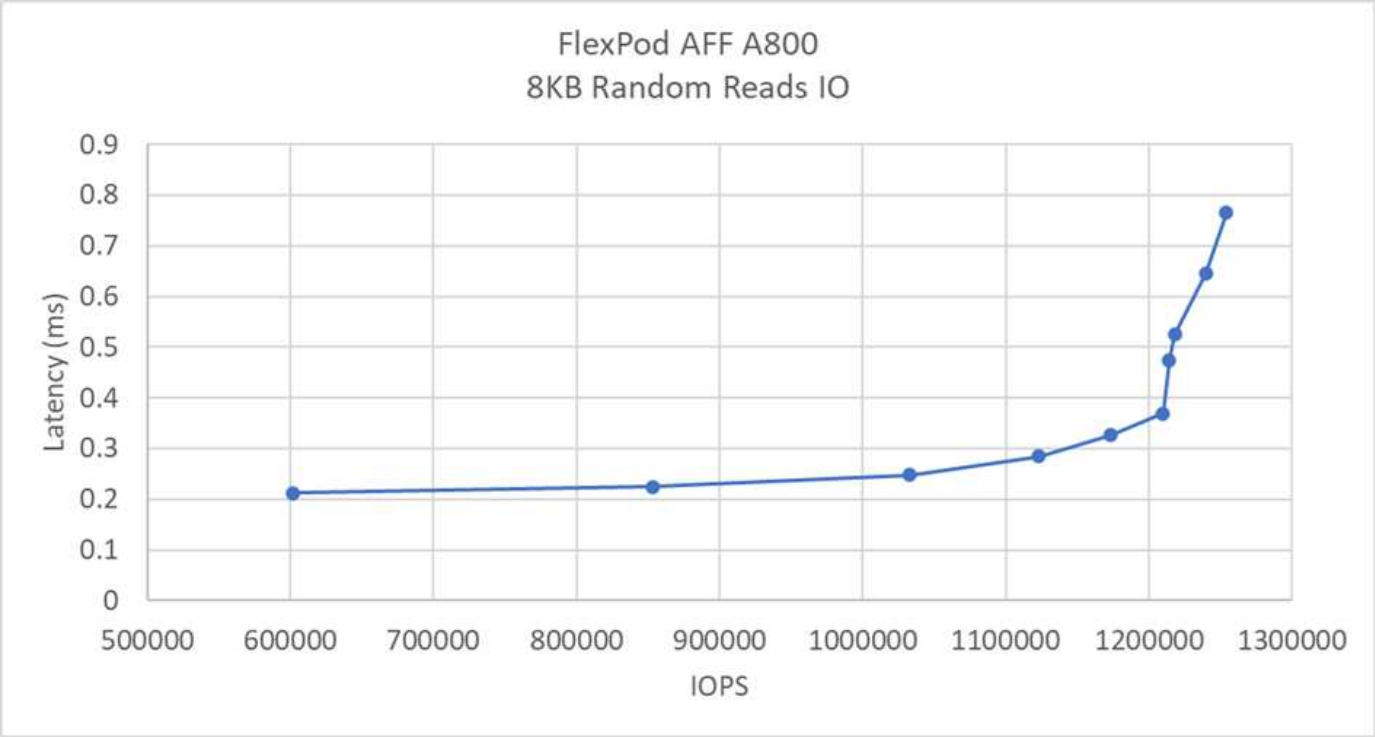
"次の手順：テスト結果"

テスト結果

"従来のテストアプローチ："

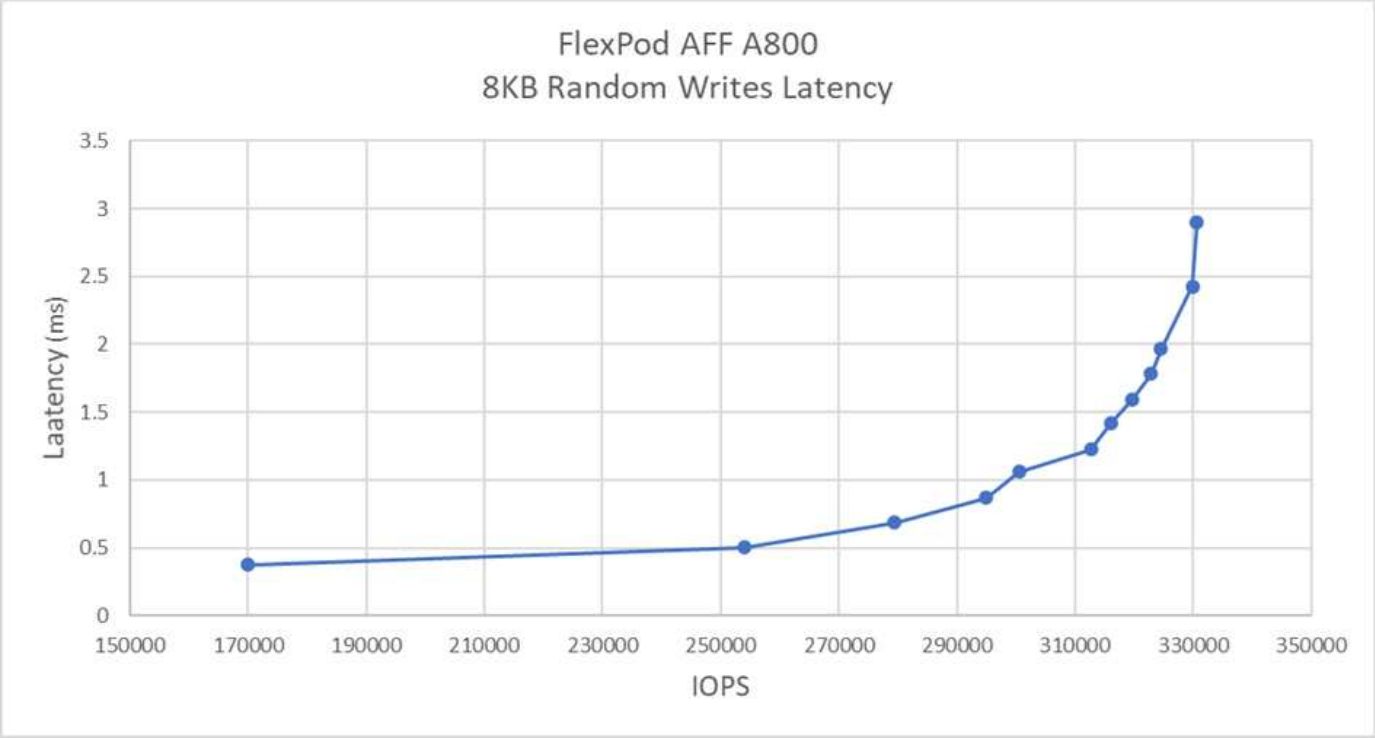
テストでは、 FC / NVMe のパフォーマンスを IOPS とレイテンシの観点から測定する fio ワークロードを実行しました。

次のグラフは、ブロックサイズ 8KB を使用して 100% ランダムリードワークロードを実行した場合の結果を示しています。



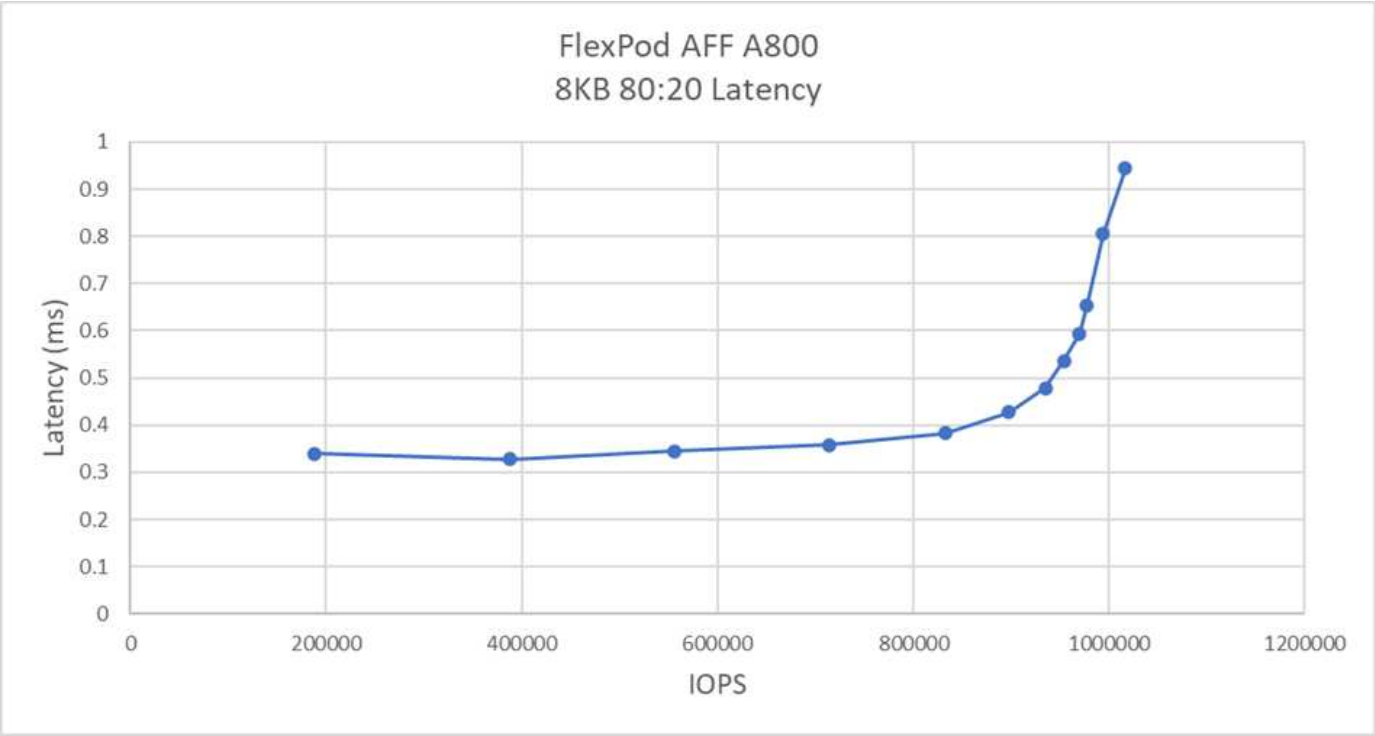
このテストでは、サーバ側のレイテンシを 0.35 ミリ秒未満に抑えながら、 120 万 IOPS を超えるパフォーマンスが得られたことがわかりました。

次のグラフは、ブロックサイズ 8KB を使用して 100% のランダムライトワークロードを実行した場合の結果を示しています。



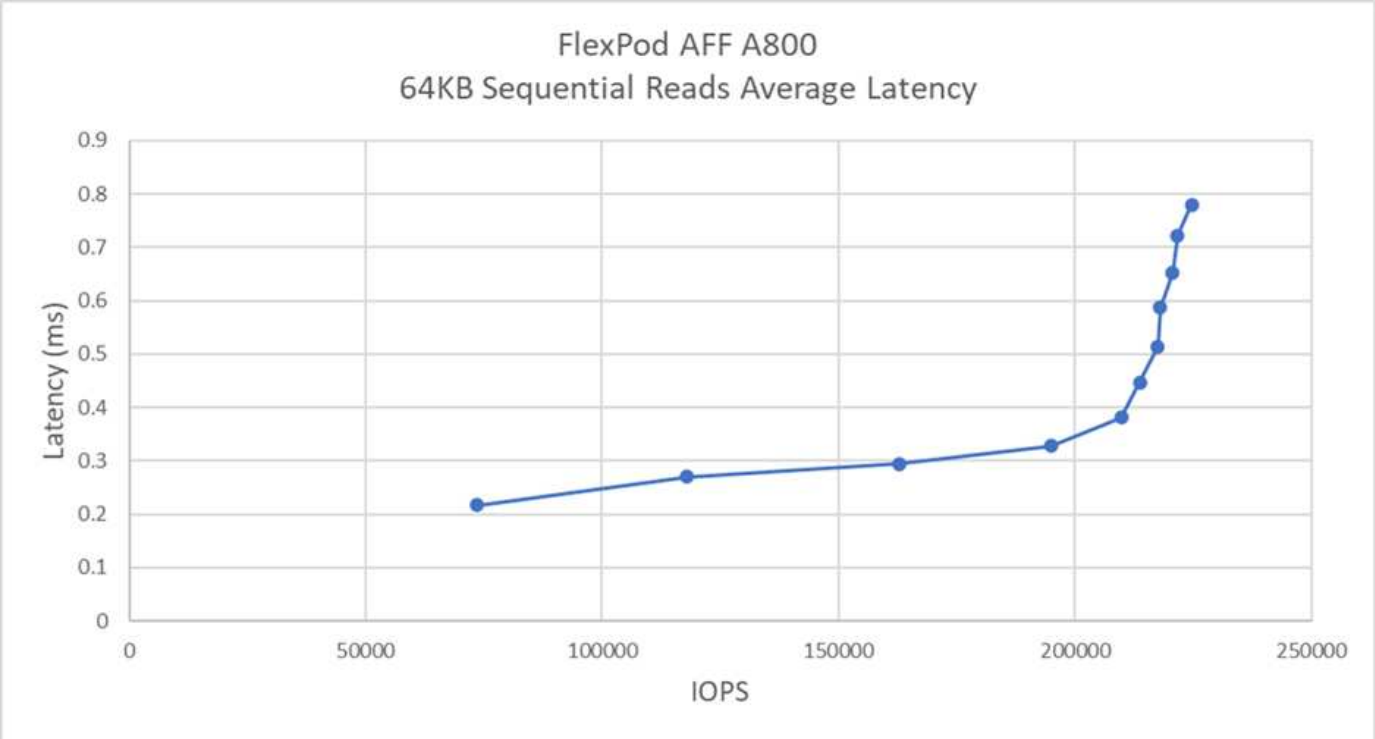
テストでは、システムの IOPS は 300k に近く、サーバ側でのレイテンシは 1 ミリ秒未満に抑えられていることがわかりました。

8KB のブロックサイズでランダムリードの 80% と書き込みの 20% を処理したところ、以下の結果が得られました。



テストでは、 100 万 IOPS を超えるシステムを達成し、サーバ側のレイテンシを 1 ミリ秒未満に抑えていることがわかりました。

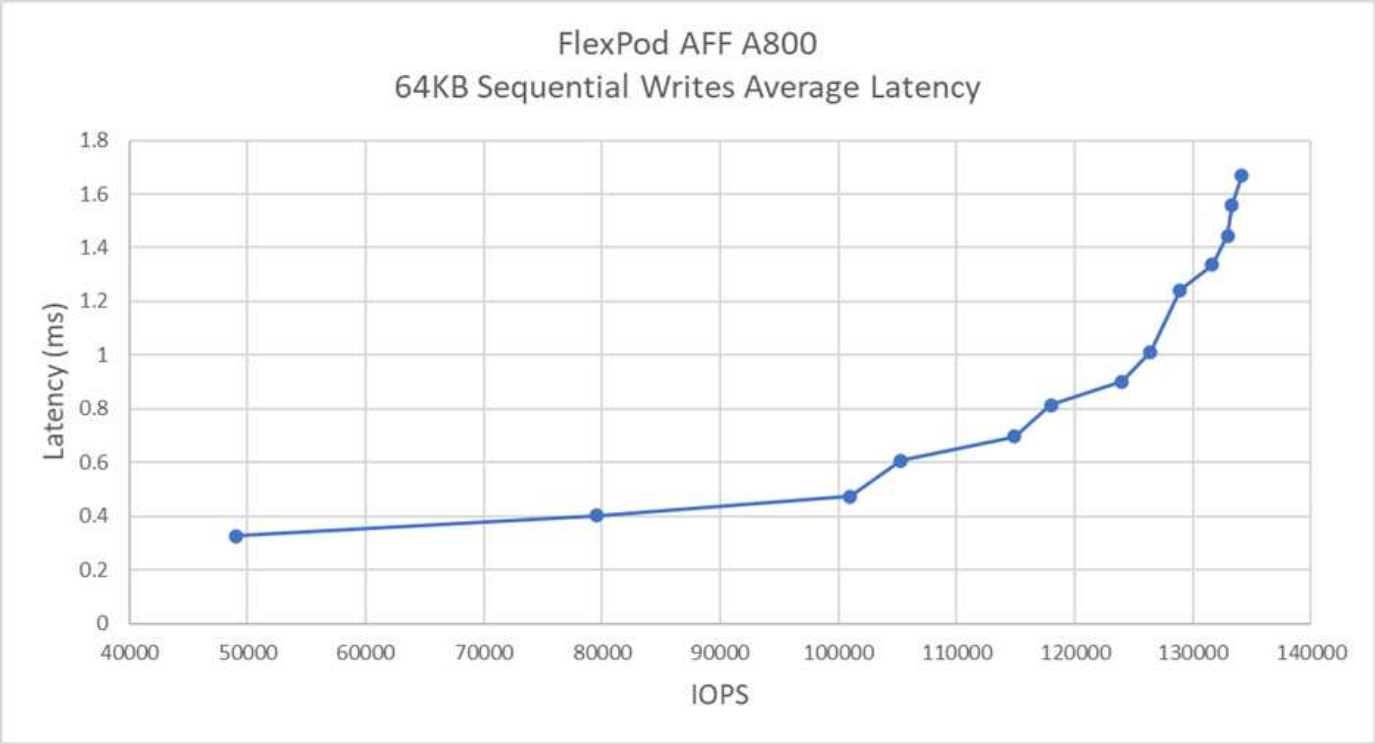
ブロックサイズ 64KB 、シーケンシャルリード 100% の場合、以下の結果が得られました。



テストでは、サーバ側のレイテンシを 1 ミリ秒未満に抑えながら約 25 万 IOPS を達成したことがわかりまし

た。

ブロックサイズ 64KB とシーケンシャルライト 100% の場合、結果は次のようになりました。



テストでは、サーバ側のレイテンシを 1 ミリ秒未満に抑えながら約 120k IOPS を達成したことがわかりました。

"次は終わりです"

まとめ

"前へ：テスト結果。"

この解決策の測定されたスループットは、 14GBps であり、 1 ミリ秒未満のレイテンシでシーケンシャルリードワークロードを処理する場合は 220 万 IOPS です。ランダムリードワークロードのスループットは 9.5GBps で 1.25M IOPS です。FlexPod を使用して FC-NVMe でこのパフォーマンスを提供できれば、ミッションクリティカルなアプリケーションのニーズに対応することができます。

VMware vSphere 7.0 U2 を搭載した FlexPod データセンターは、さまざまな IT ワークロードに FC-NVMe を導入するための最適な共有インフラ基盤です。これにより、 FC-NVMe を必要とするアプリケーションにハイパフォーマンスなストレージアクセスを提供できます。FC-NVMe は進化し、高可用性、マルチパス、およびオペレーティングシステムの追加サポートが組み込まれています。 FlexPod は、このような機能をサポートするために必要な拡張性と信頼性を備えたプラットフォームに最適です。

シスコとネットアップは、 FlexPod を使用して、さまざまなユースケースやアプリケーションに対応できる柔軟性と拡張性に優れたプラットフォームを開発しました。FC-NVMe を使用すると、同じ共有インフラで同時に実行されているビジネスクリティカルなアプリケーションを効率的かつ効果的にサポートするための機能が FlexPod に追加されています。FlexPod は柔軟性と拡張性に優れているため、進化するビジネス要件に合わせて拡張できる適切なサイズのインフラから利用を開始できます。

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。

- Cisco Unified Computing System （ UCS ）

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Cisco UCS 6400 シリーズファブリックインターコネクトデータシート

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Cisco UCS 5100 シリーズブレードサーバシャーシ

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Cisco UCS B シリーズブレードサーバ

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Cisco UCS C シリーズラックサーバ

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Cisco Unified Computing System アダプタ

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Cisco UCS Manager の略

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Cisco Nexus 9000 シリーズスイッチ

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Cisco MDS 9000 マルチレイヤファブリックスイッチ

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Cisco MDS 9132T 32 Gbps 32 ポートファイバチャネルスイッチ

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- NetApp ONTAP 9.

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- NetApp AFF A シリーズ

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VMware vSphere の場合

  "https://www.vmware.com/products/vsphere"

- VMware vCenter Server の各機能を使用し

  "http://www.vmware.com/products/vcenter-server/overview.html"

- 最新 SAN のベストプラクティス

  "https://www.netapp.com/us/media/tr-4080.pdf"

- FlexPod 向けエンドツーエンド NVMe の導入

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

相互運用性マトリックス

- NetApp Interoperability Matrix Tool で確認できます

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

- Cisco UCS ハードウェア互換性マトリックス

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

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

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

謝辞

本プロジェクトの実施にあたって、 Cisco と Scott Lane 、 Bobby Oommen から協力して得た支援とガイダンスに感謝の意を表します。

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

http://www.netapp.com/us/legal/copyright.aspx

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

http://www.netapp.com/us/legal/netapptmlist.aspx

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/us/media/patents-page.pdf

プライバシーポリシー

https://www.netapp.com/us/legal/privacypolicy/index.aspx