FlexPod エクスプレスの略

FlexPod

NetApp

October 30, 2025

目次

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：[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

"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.
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。

[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

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

[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

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。

[エラー：グラフィックイメージがありません]

"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。

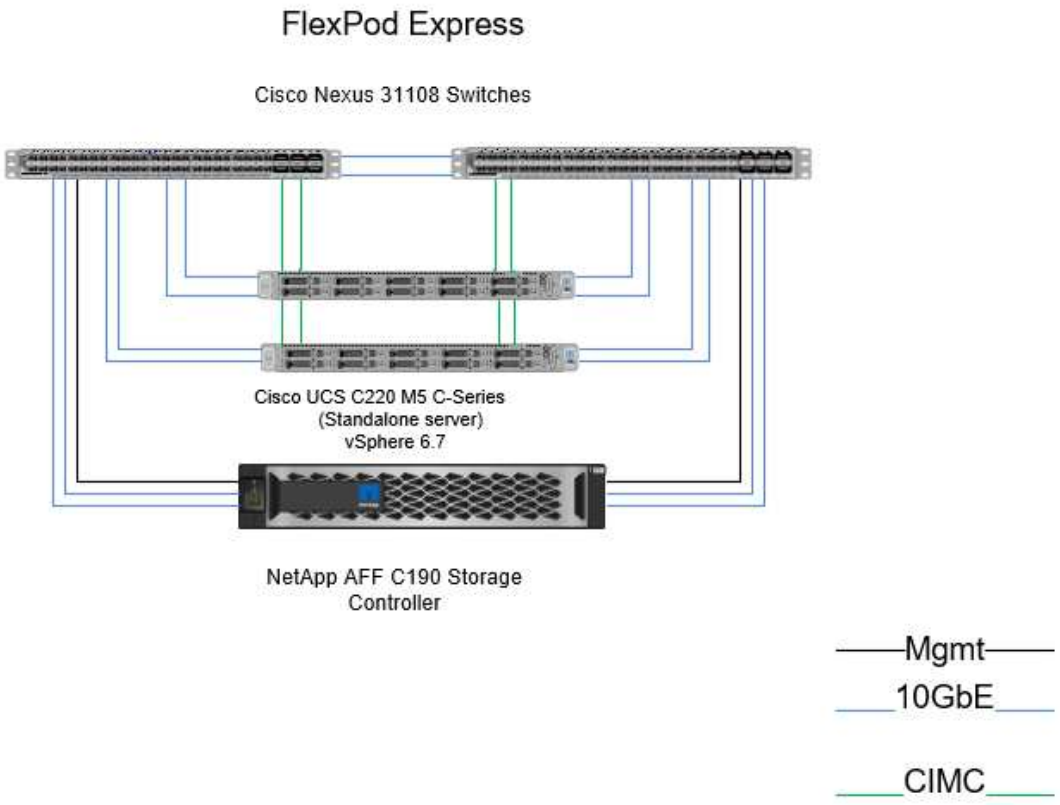
- 徹底的なテスト
- あらかじめ規定されている
- 導入リスクを最小限に抑制
- 運用開始までの時間を短縮

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

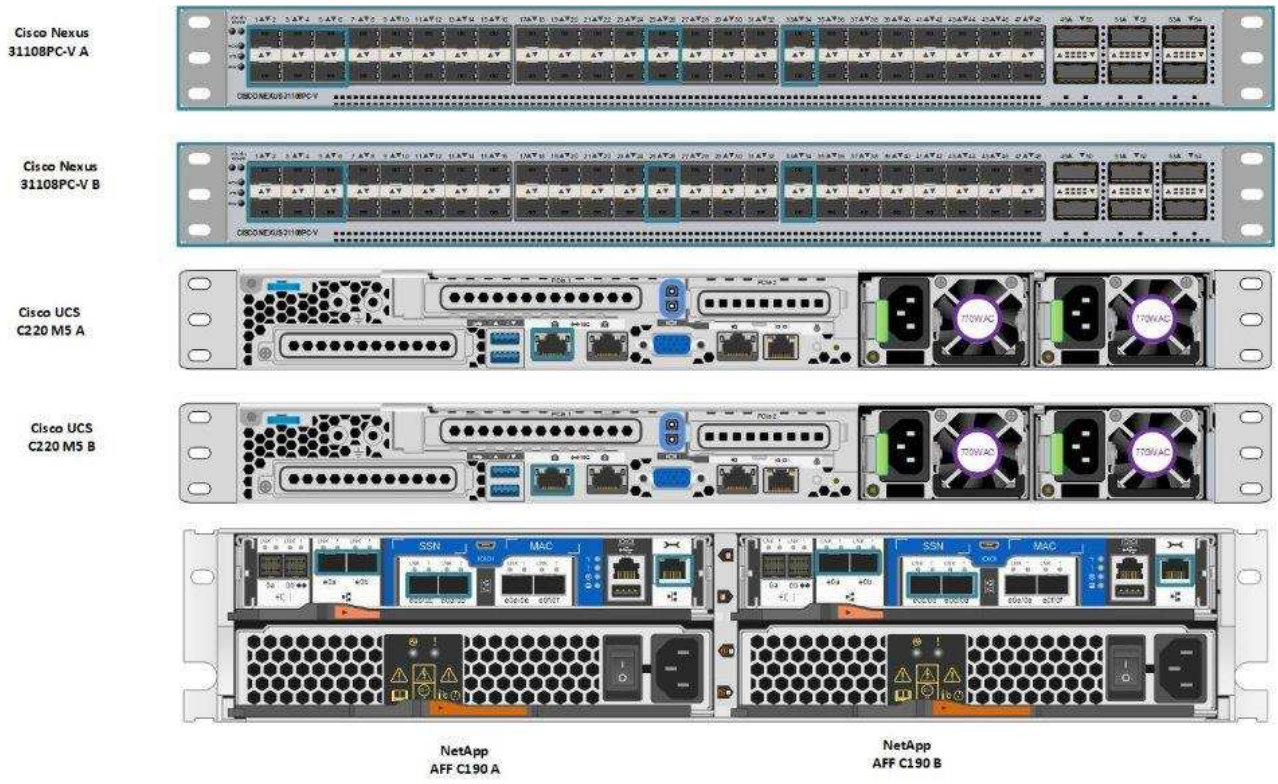
次の表に、 FlexPod Express でのすべての VMware vSphere 環境に必要なソフトウェアを示します。

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。

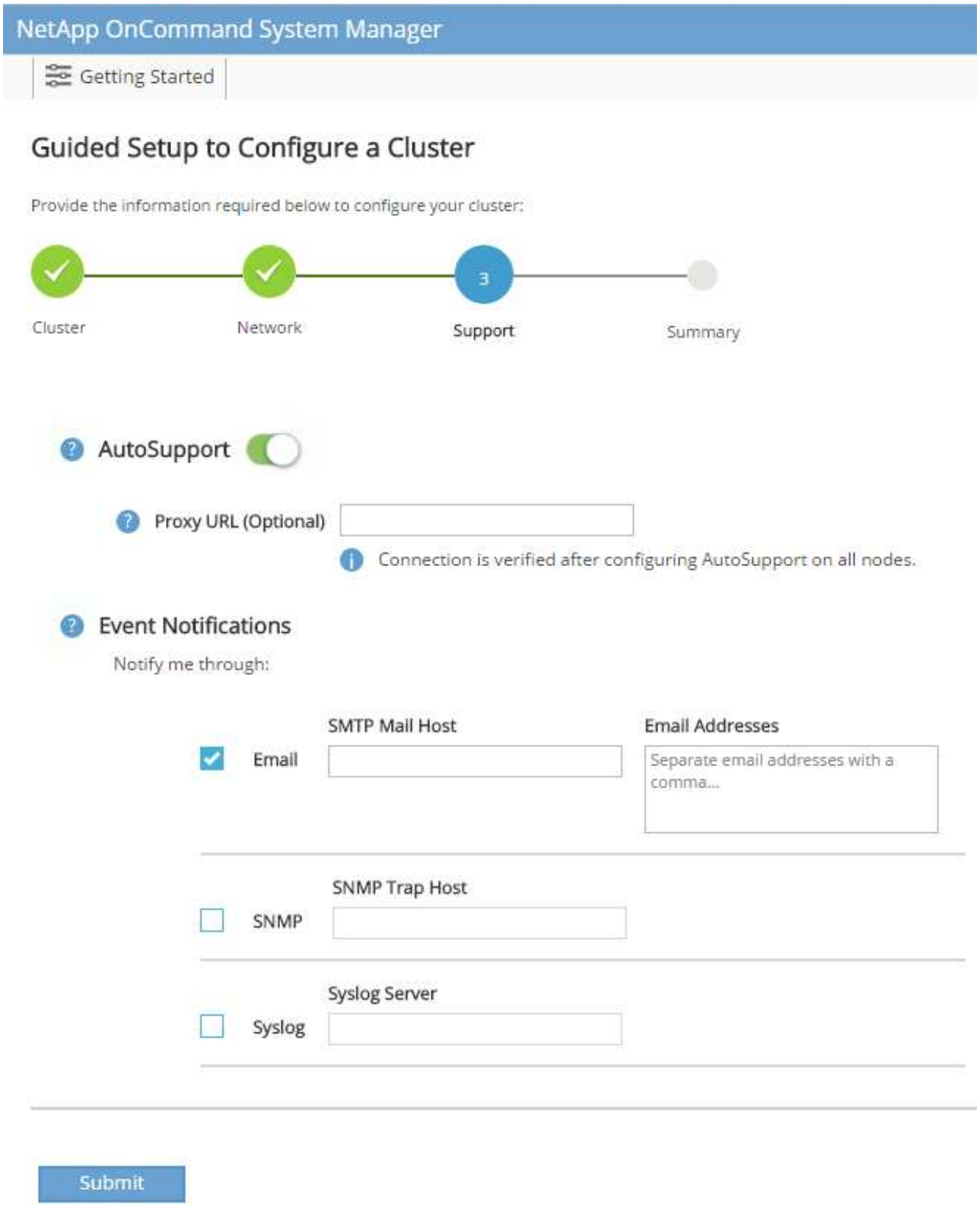
代替 NTP サーバを入力することもできます。「 \<<var_ntp_server_ip>> 」の IP アドレス「 10.63.172.16.2 」は、 Nexus Mgmt IP です。

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>`

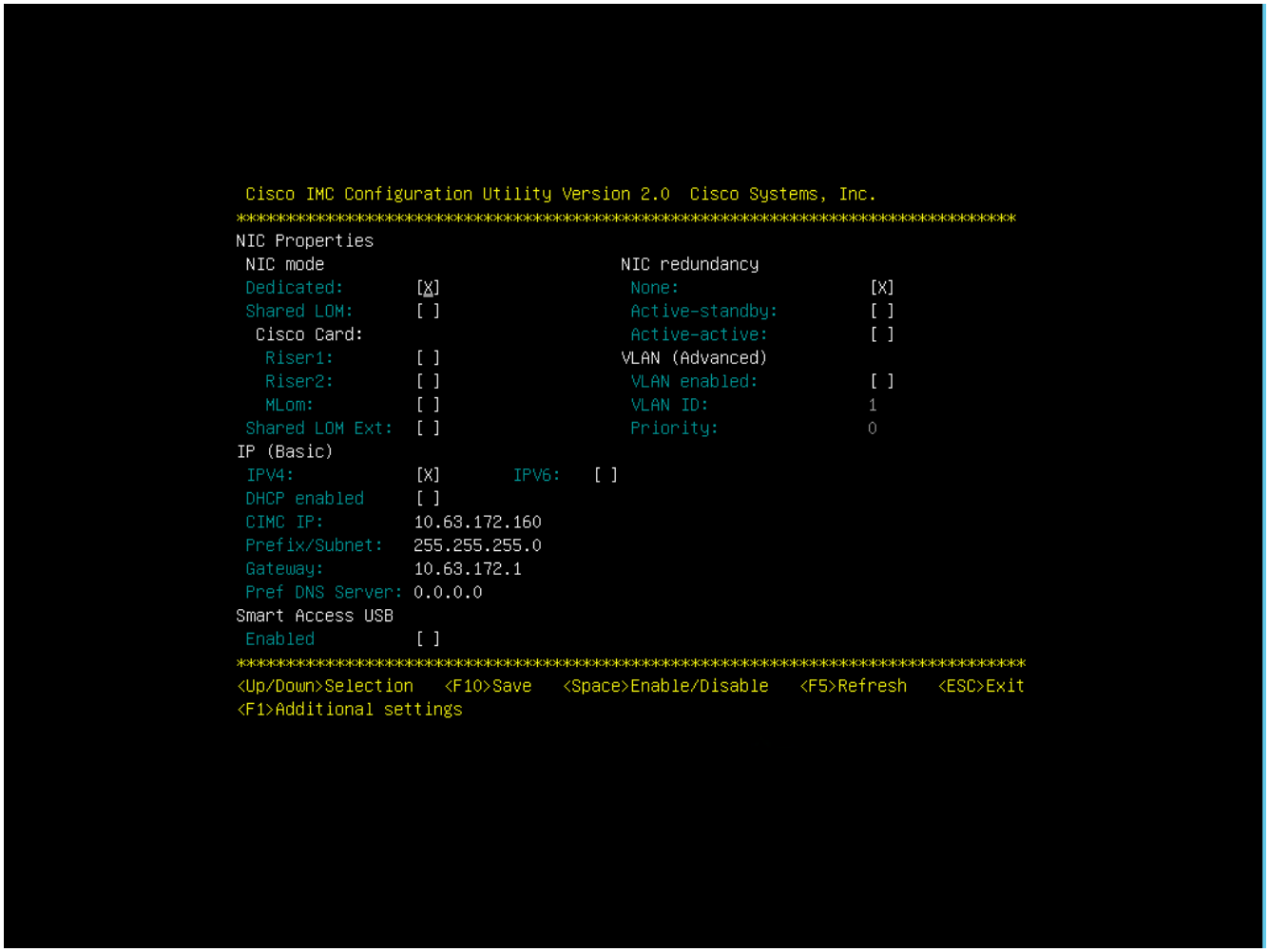
      プレフィックス / サブネット： `\<CIMC_netmask>`

      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。

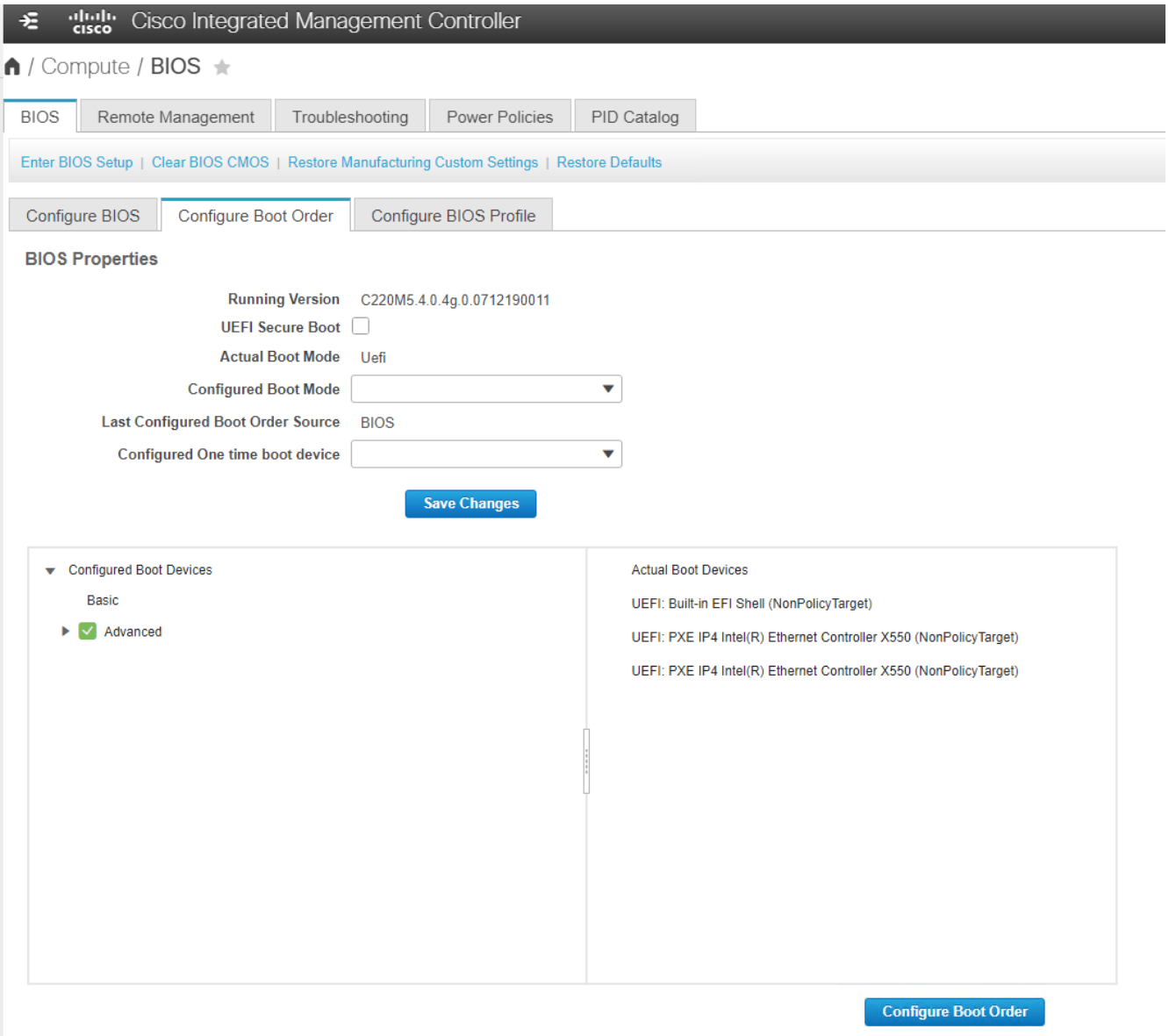
斜体のフォントは、 ESXi ホストごとに一意の変数を示します。

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

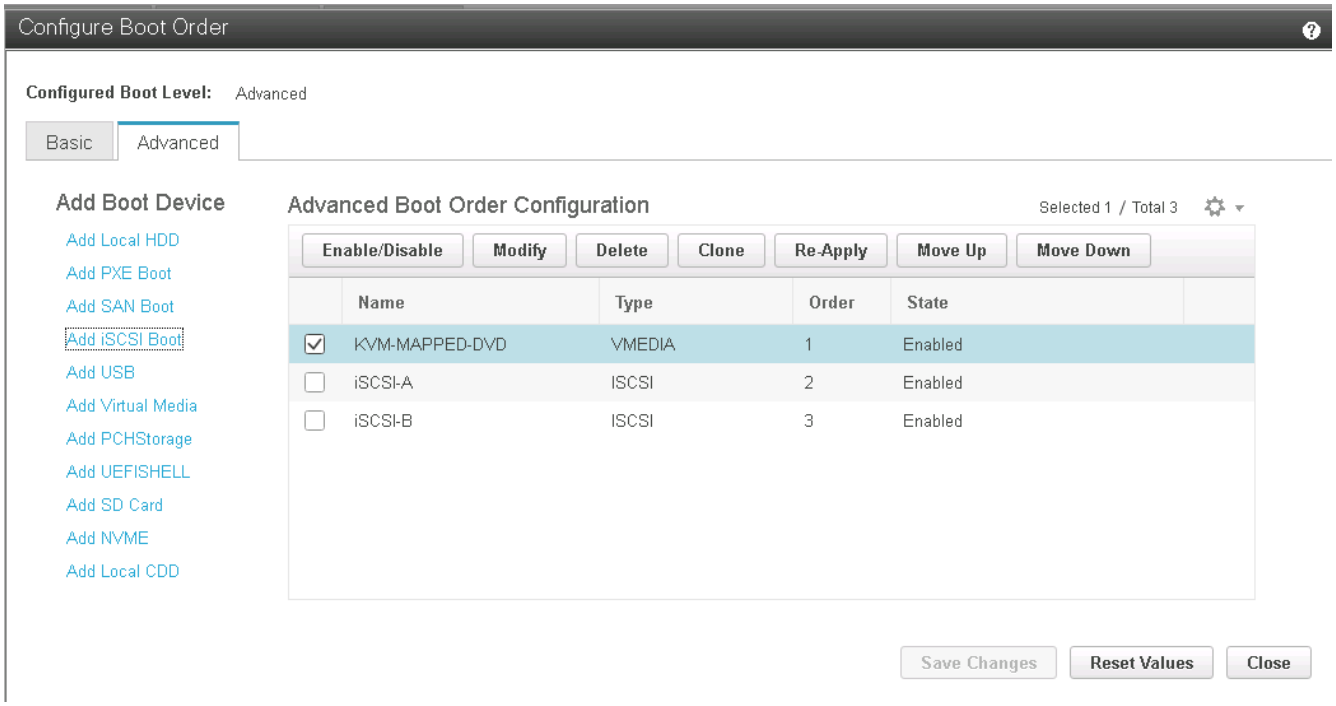
状態：有効

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。



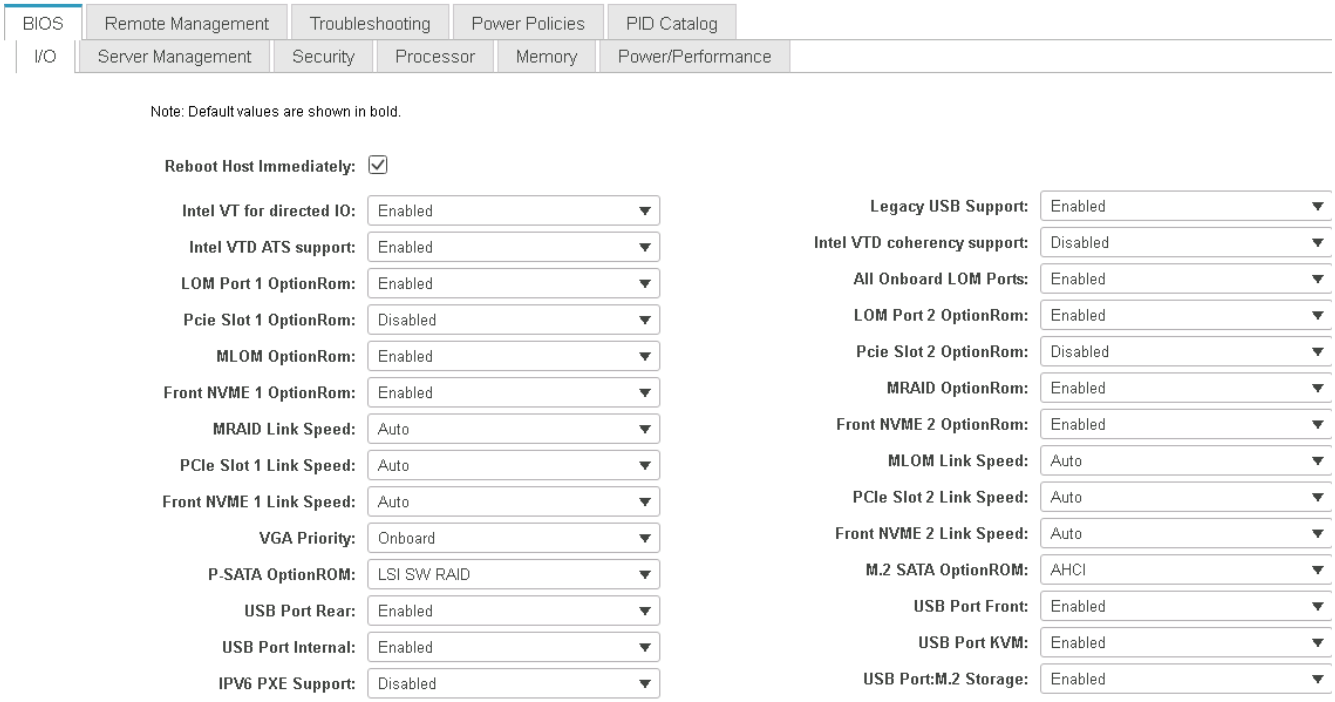
6. サーバをリブートして、新しいブート順序でブートします。

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。

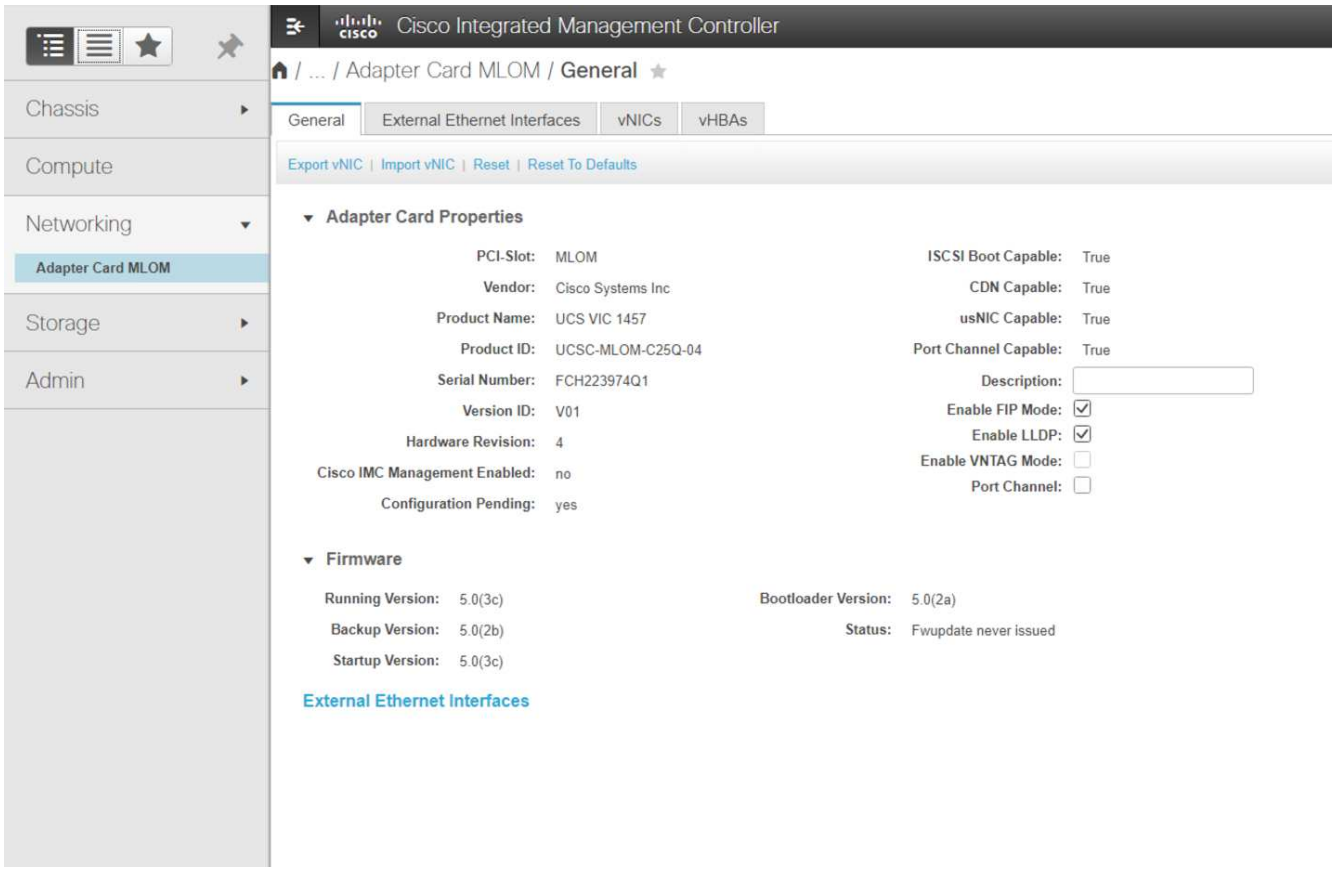


iSCSI ブート用に **Cisco VIC1457** を設定します

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。

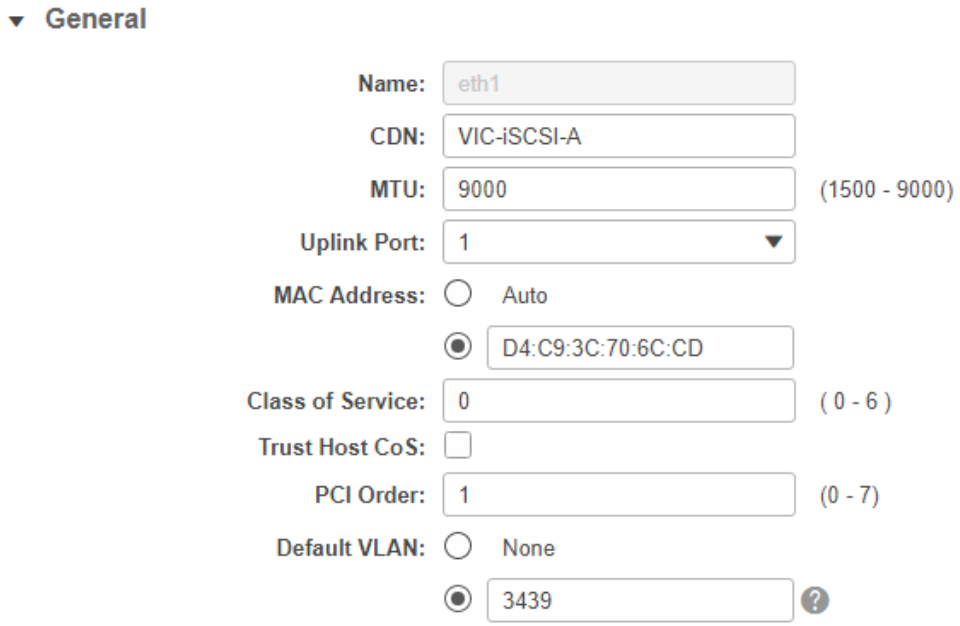
1. [ネットワーク] タブで、 [Adapter Card mLOM] をクリックします。
2. General タブで、ポートチャネルのチェックを外します。
3. 変更を保存し、 CIMC をリブートします。



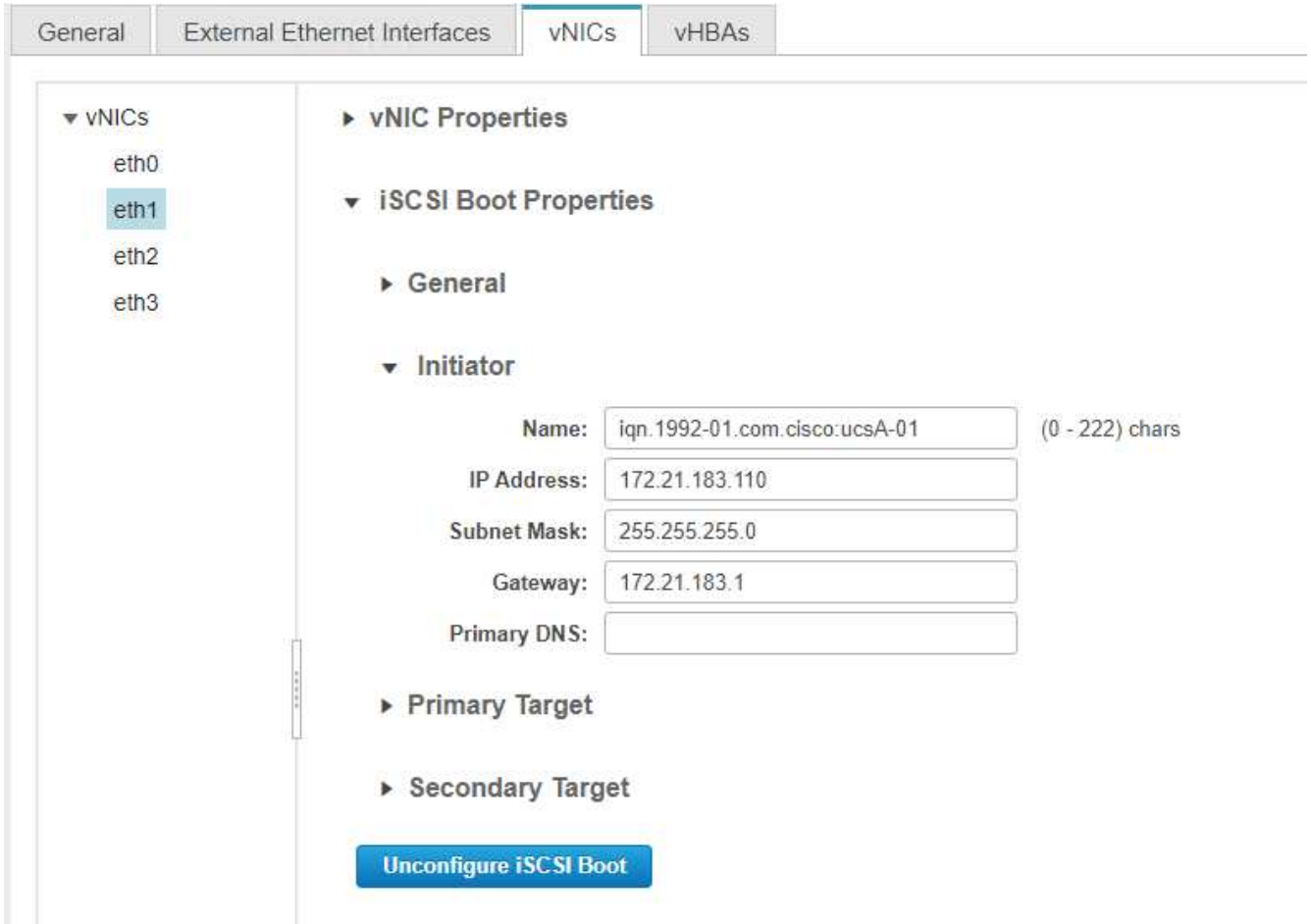
iSCSI vNIC を作成します

iSCSI vNIC を作成するには、次の手順を実行します。

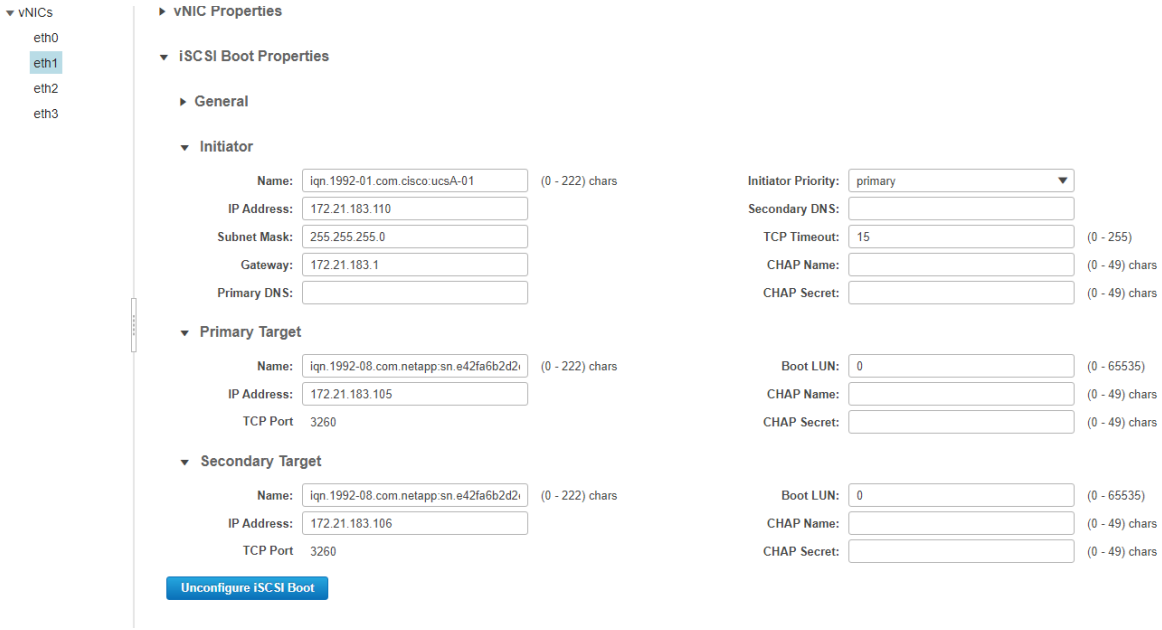
1. [ネットワーク] タブで、 [Adapter Card mLOM] をクリックします。
2. [Add vNIC] をクリックして vNIC を作成します。
3. [Add vNIC] セクションで、次の設定を入力します。
   - 名前： eth1
   - CDN 名： iscsi-vNIC-A
   - MTU ： 9000
   - デフォルト VLAN ： `\<<var_iscsi_vlan_a>`
   - VLAN モード：トランク
   - Enable PXE boot: チェック
4. [Add vNIC] をクリックし、 [OK] をクリックします。
5. このプ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>>



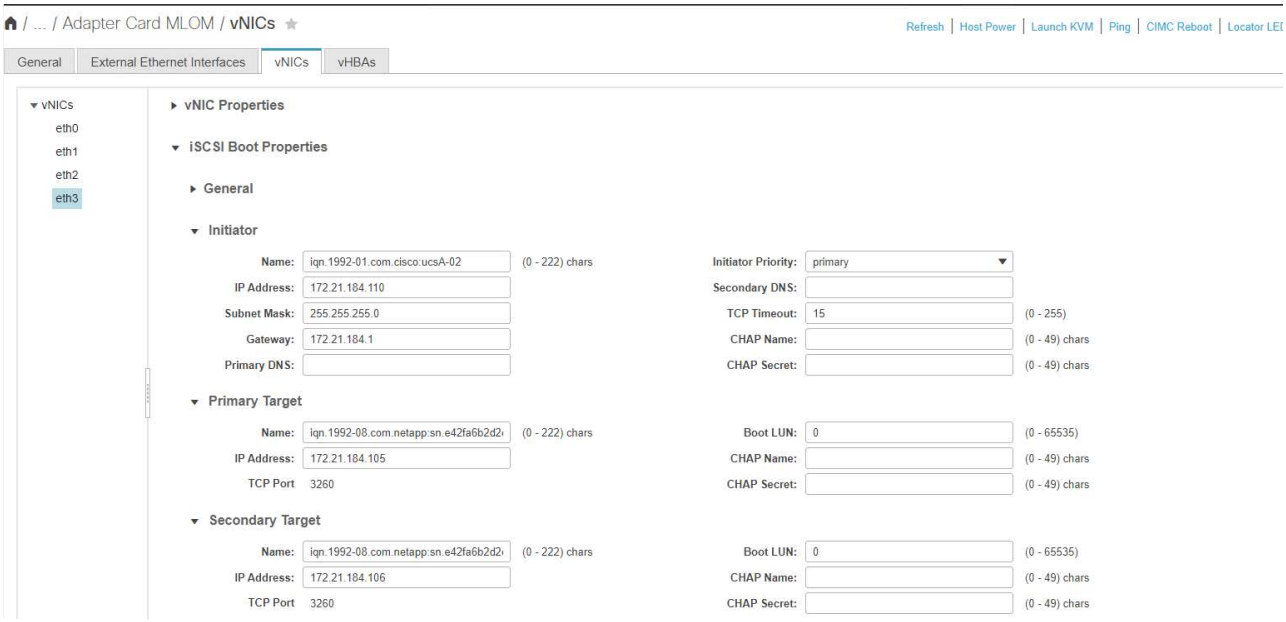
8. プライマリターゲットの詳細を入力します。
   - name ：インフラ SVM の IQN 番号
   - IP アドレス： iscsi_dlif01a の IP アドレス
   - ブート LUN ： 0
9. セカンダリターゲットの詳細を入力します。
   - name ：インフラ SVM の IQN 番号
   - IP アドレス： iSCSI_lif02a の IP アドレス
   - ブート LUN ： 0

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。

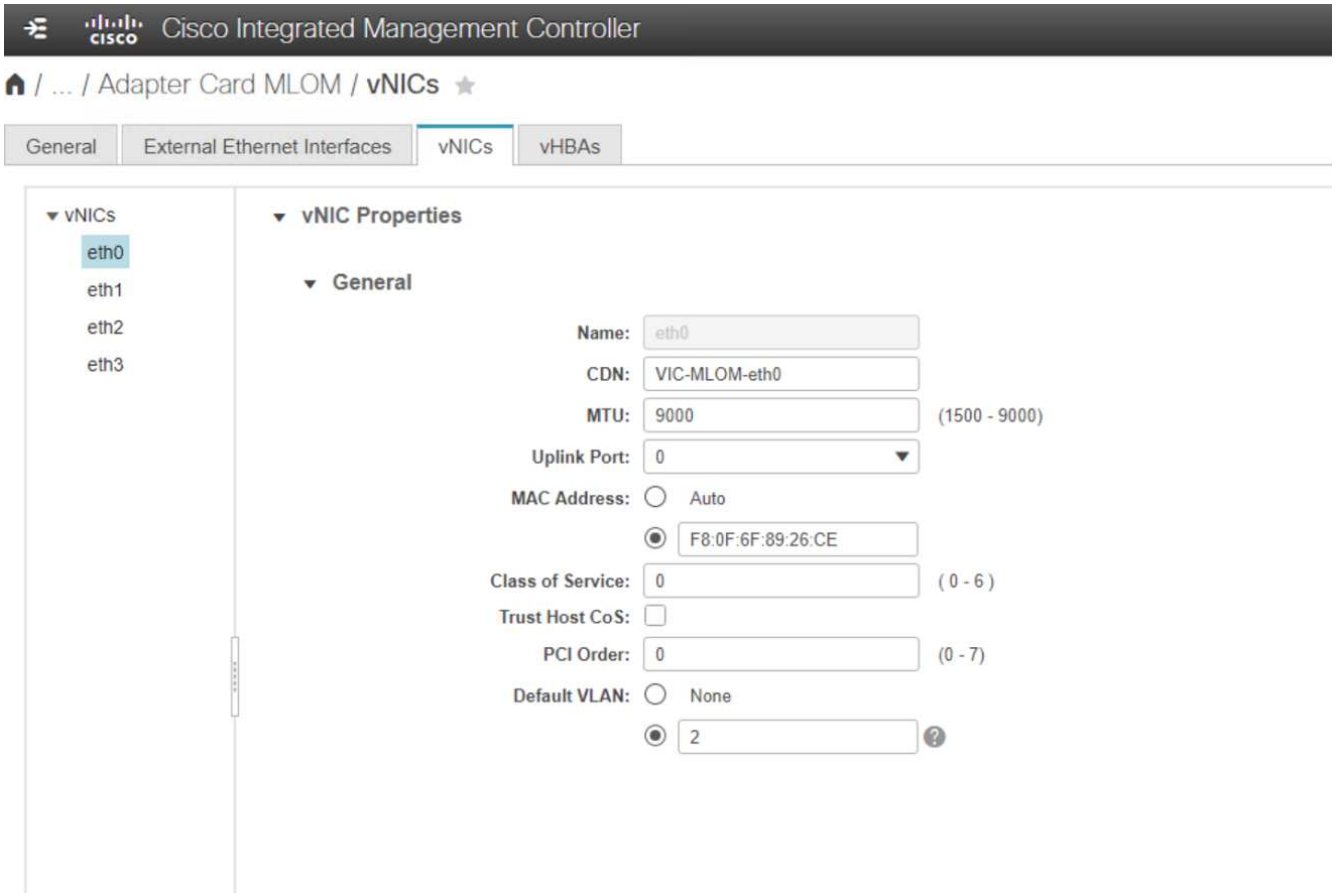
各 vNIC の IQN 名を必ず記録してください。これらのファイルはあとで必要になります。

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

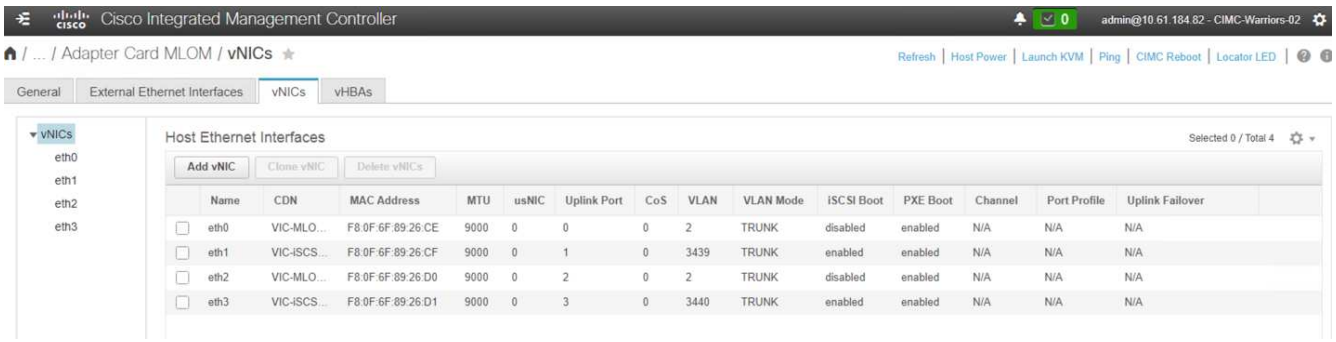
ESXi の **vNIC** を設定します

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。

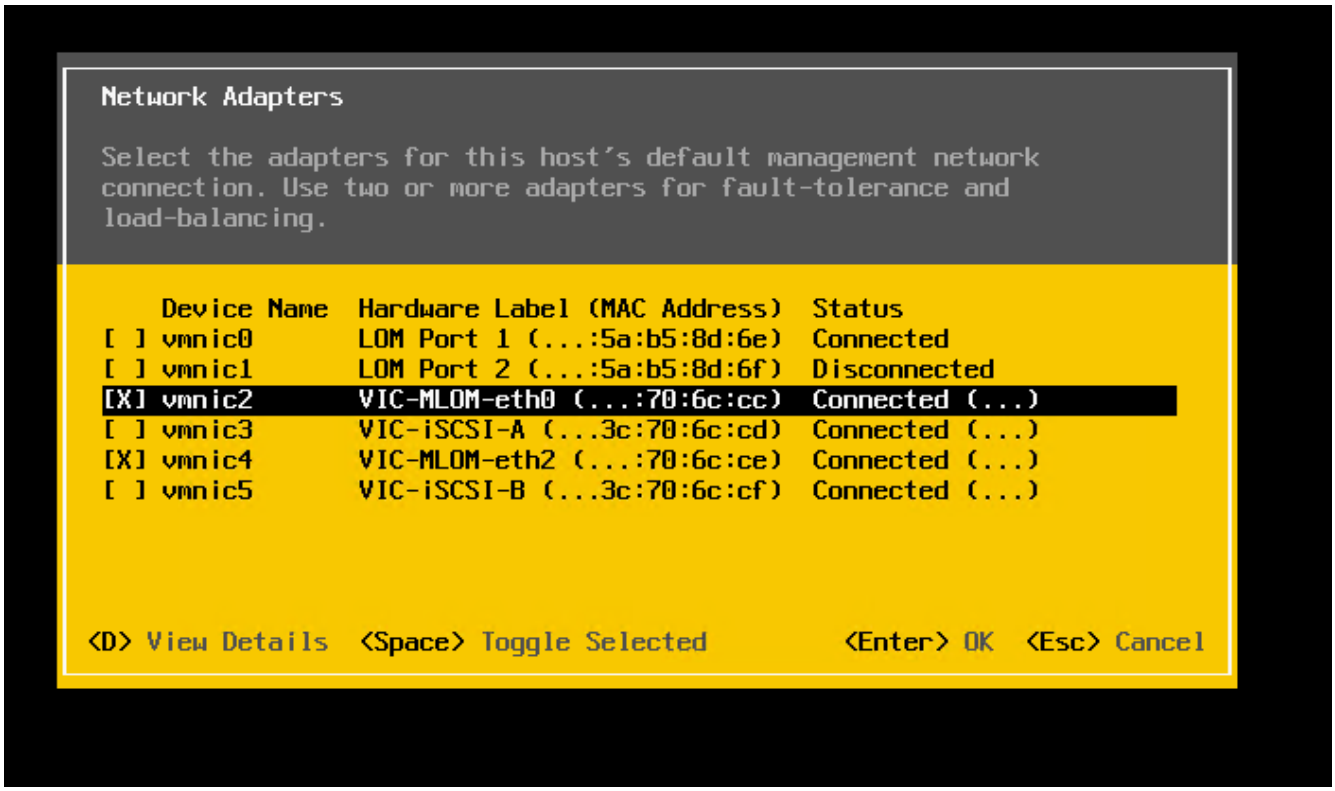
9. 適切なキーボードレイアウトを選択し、 Enter キーを押します。
10. ルートパスワードを入力して確定し、 Enter キーを押します。
11. 既存のパーティションがボリュームから削除されていることを示す警告が表示されます。F11 キーを押してインストールを続行します。ESXi のインストール後にサーバがリブートします。

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

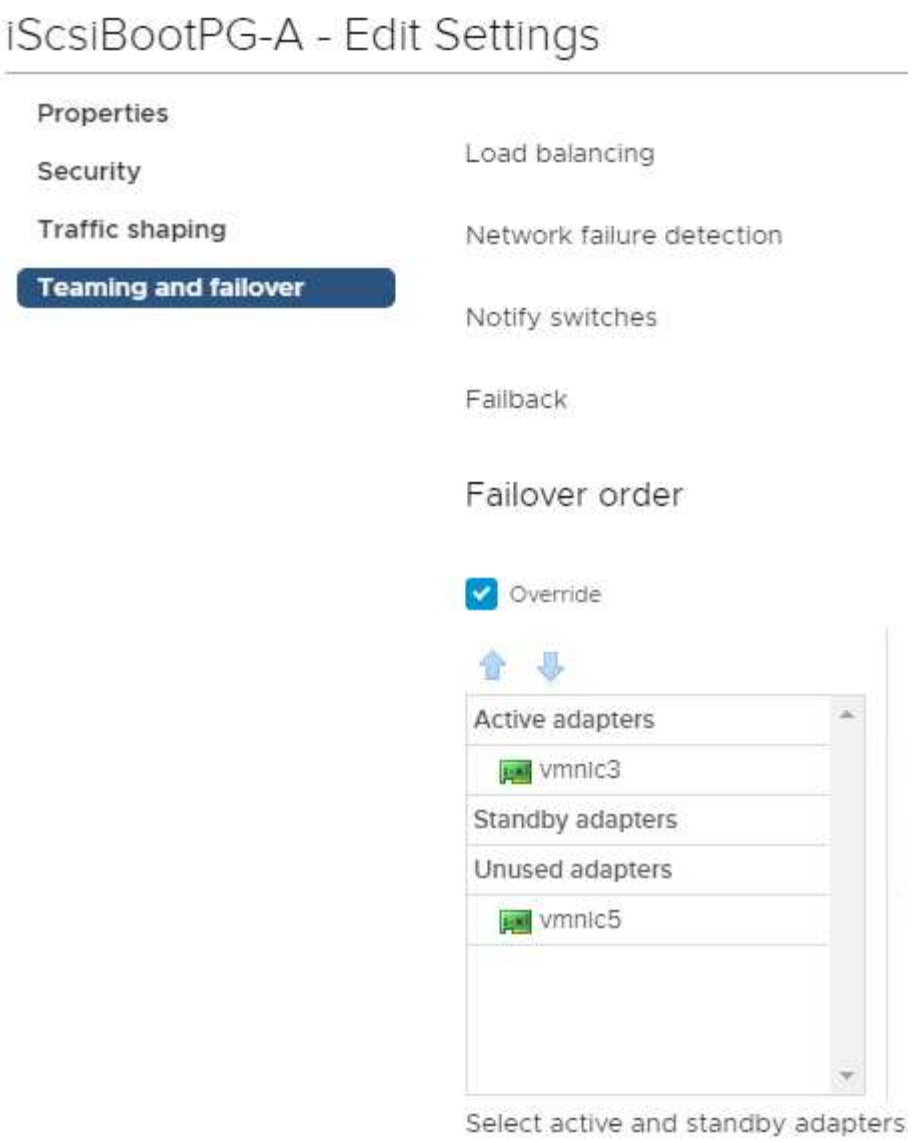
> この構成では、 vmnic3 と vmnic5 が iSCSI ブートに使用されます。ESXi ホストに NIC がほかにもある場合は、 vmnic 番号が異なることがあります。iSCSI ブートに使用されている NIC を確認するには、 CIMC の iSCSI vNIC 上の MAC アドレスを ESXi の vmnic に照合します。

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

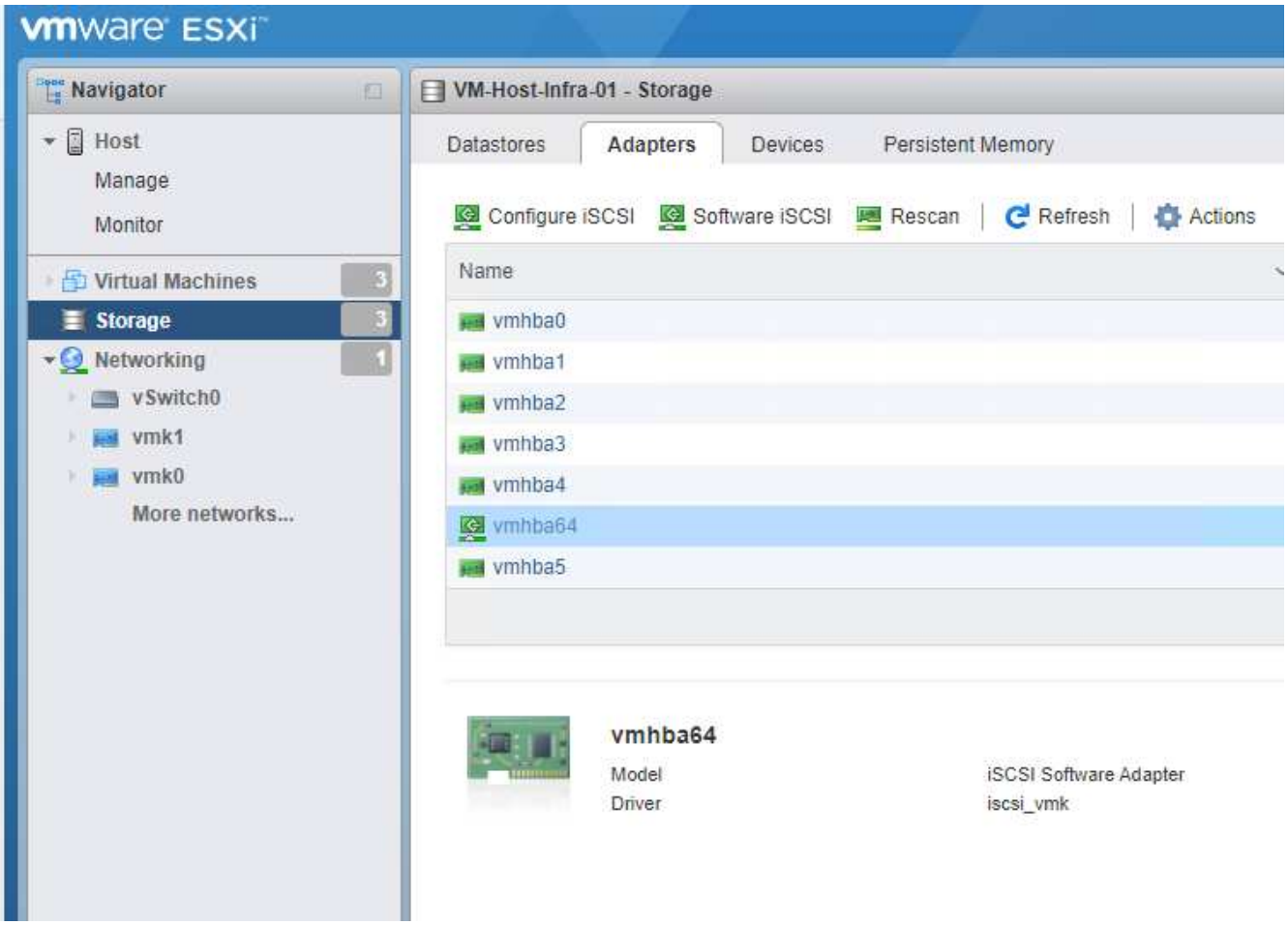
9. フェイルオーバーを設定するには、次の手順を実行します。
a. iSCSIBootPG の設定の編集 - A > 階層化とフェイルオーバー > フェイルオーバー順序 > vmnic3 をクリックします。vmnic3 がアクティブで、 vmnic5 が未使用である。
b. iSCSIBootPG-B で設定の編集 > チーム化とフェイルオーバー > フェイルオーバー順序 > vmnic5 をクリックします。vmnic5 がアクティブで、 vmnic3 が未使用である。



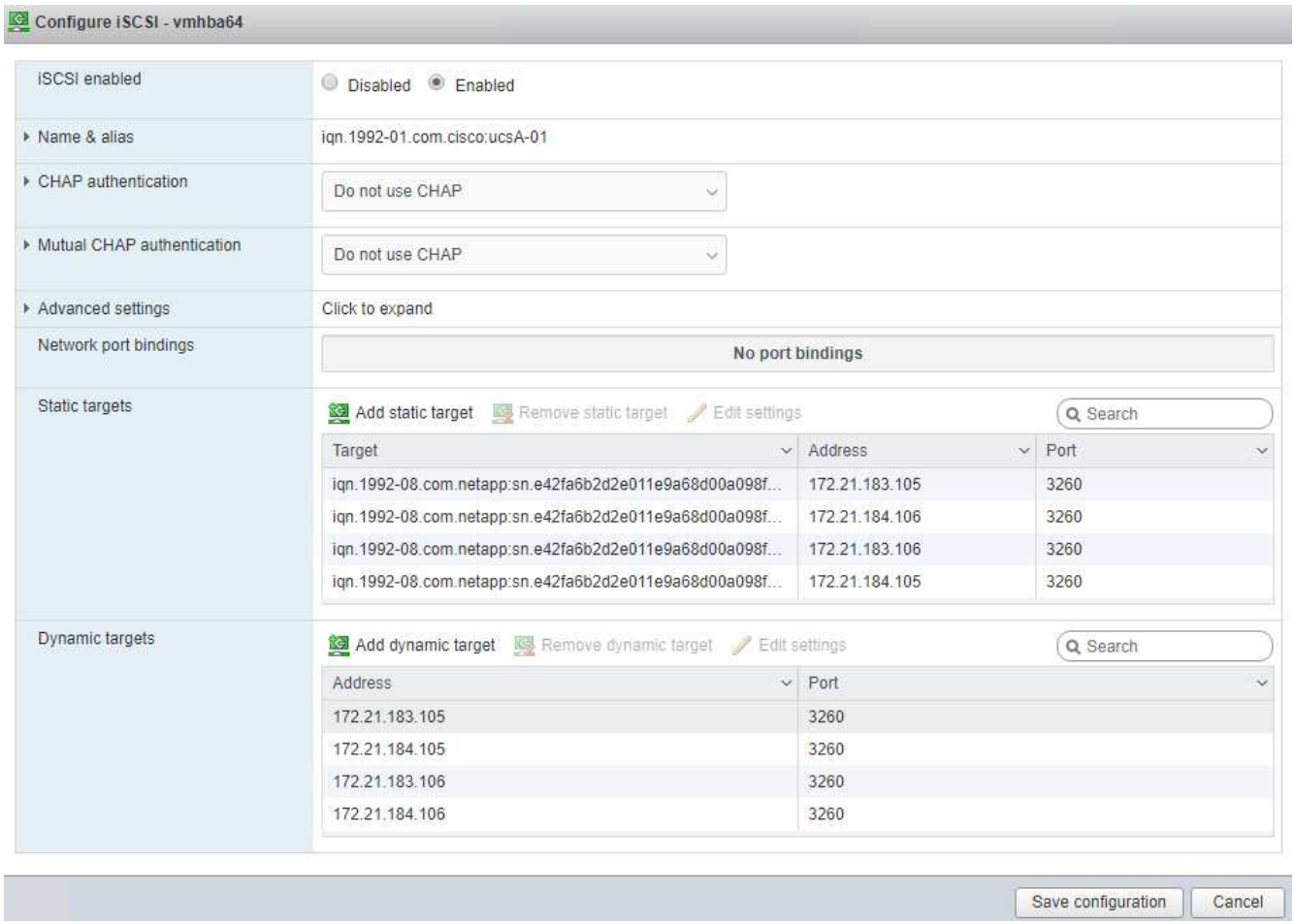
iSCSI マルチパスを設定します

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。

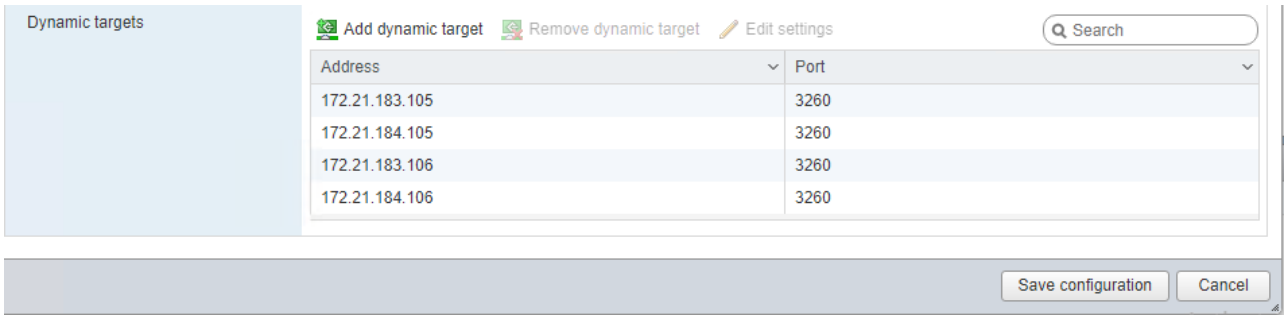
1. 左側のナビゲーションペインで Storage （ストレージ）を選択します。アダプタをクリックします。
2. iSCSI ソフトウェアアダプタを選択し、 Configure iSCSI （ iSCSI の設定）をクリックします。



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。



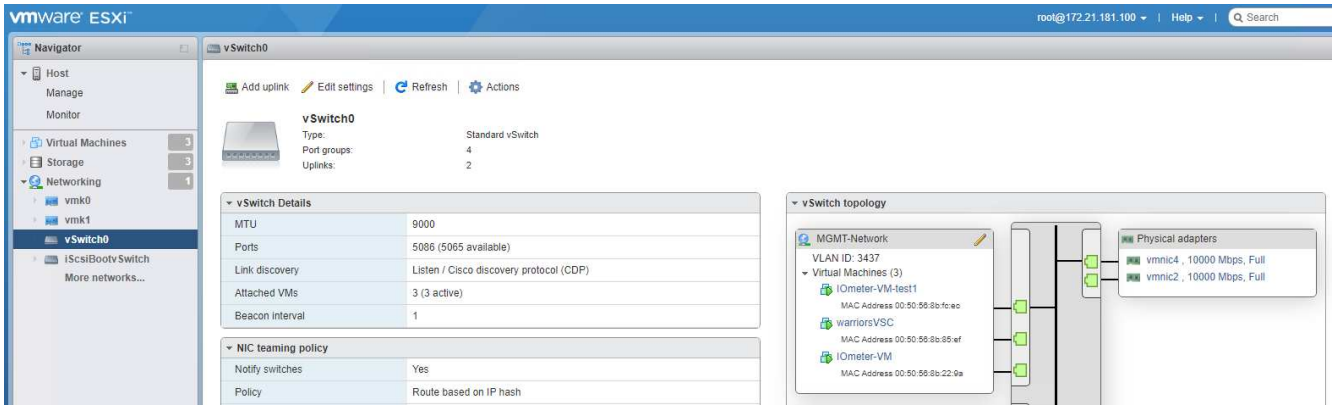
iSCSI LIF の IP アドレスは、ネットアップクラスタで network interface show コマンドを実行するか、 System Manager の Network Interfaces タブで確認できます。

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。

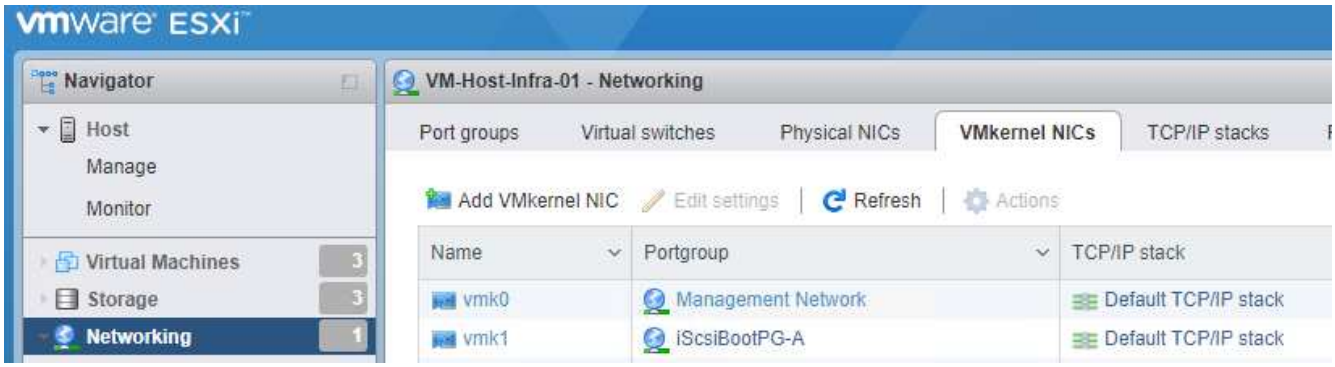
> ロードバランシングの IP ハッシュ方式では、スタティック（モードオン）ポートチャネルで SRC-DST-IP EtherChannel を使用して、基盤となる物理スイッチを適切に設定する必要があります。スイッチの設定ミスが原因で接続が断続的に発生する可能性があります。その場合は、ポートチャネル設定のトラブルシューティング中に、 Cisco スイッチに関連付けられている 2 つのアップリンクポートのいずれかを一時的にシャットダウンして ESXi 管理 vmkernel ポートへの通信をリストアします。

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。

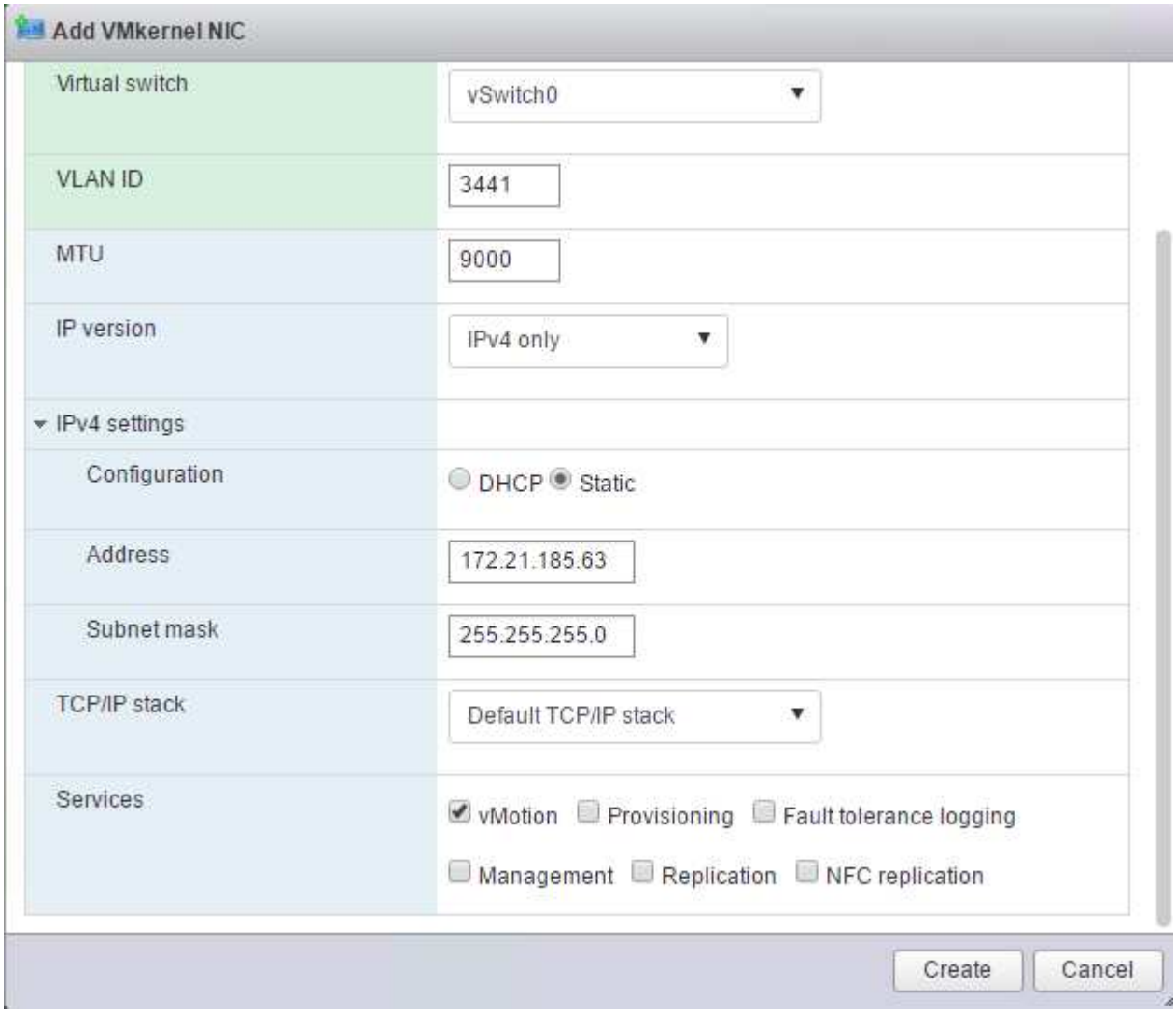
3. [VM Network] を右クリックし、 [Edit] を選択します。VLAN ID を「 <<var_vm_traffic_vlan>> 」に変更します。
4. [Add Port Group] をクリックします。
   a. ポートグループに MGMT-Network という名前を付けます。
   b. VLAN ID に「 \ <mgmt_vlan>> 」と入力します。
   c. vSwitch0 が選択されていることを確認してください。
   d. [保存] をクリックします .
5. [VMkernel NICs] タブをクリックします。



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。

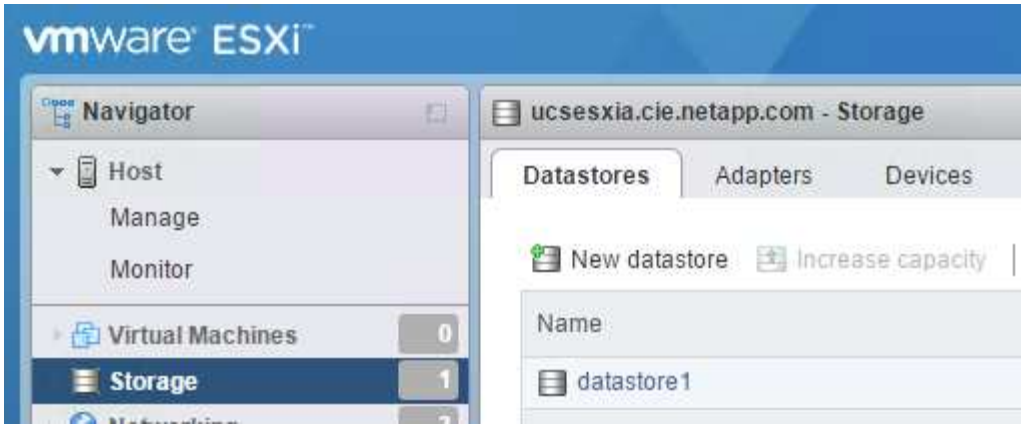


ESXi ネットワークの設定には、ライセンスで許可されている場合に VMware vSphere Distributed Switch を使用するなどの方法が多数あります。ビジネス要件を満たす必要がある場合は、 FlexPod Express で代替ネットワーク構成がサポートされます。

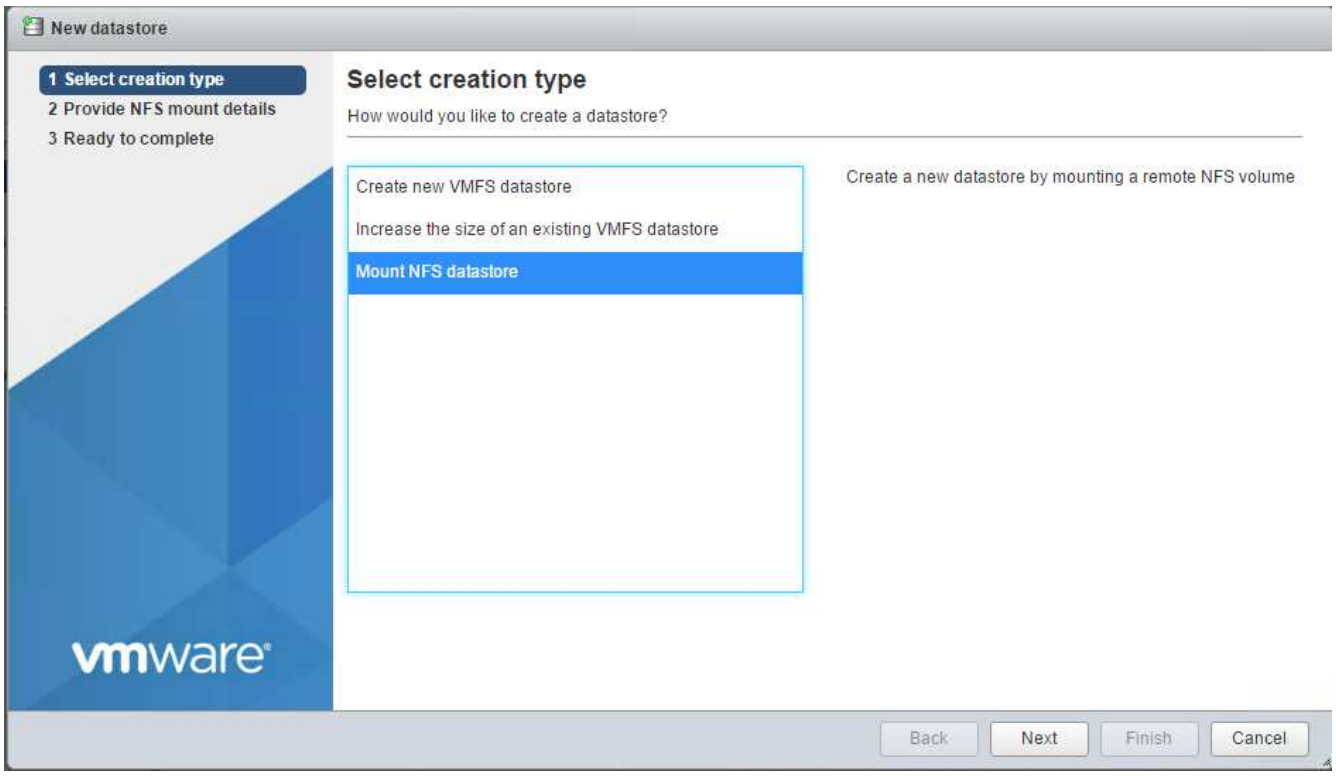
最初のデータストアをマウント

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。



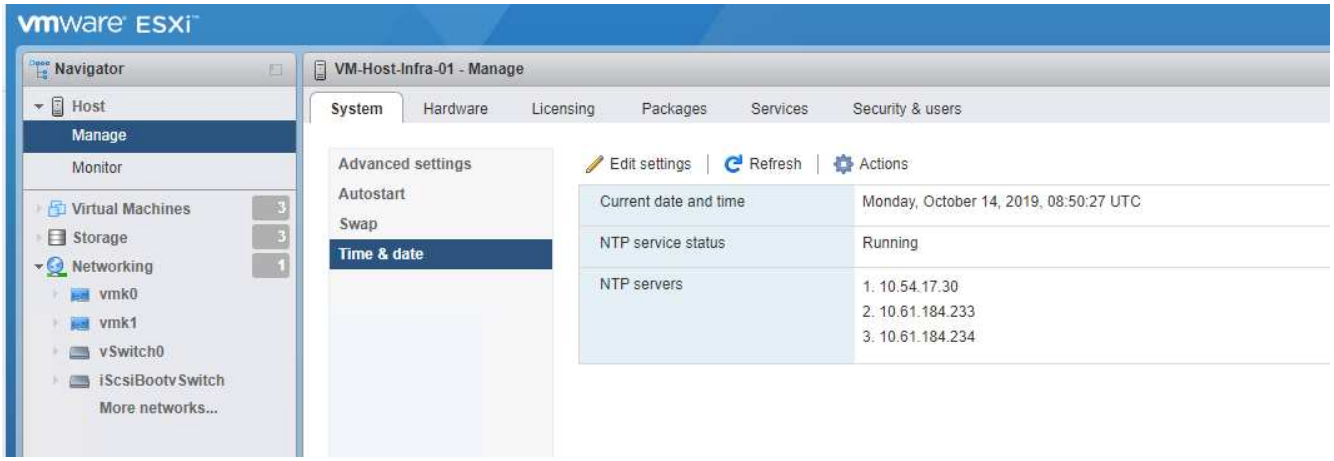
3. Provide NFS Mount Details （ NFS マウントの詳細の提供）ページに次の情報を入力します。
   - 名前： 'infra_datastore.
   - NFS サーバ : `\<<var_nodeA_nfs_lif>`
   - 共有 : 「 /infra_datastore 」
   - NFS 3 が選択されていることを確認します。
4. 完了をクリックします。[最近のタスク] ペインにタスクの完了が表示されます。
5. この手順を繰り返して 'infra_swap' データストアをマウントします
   - 名前： infra_swap
   - NFS 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。

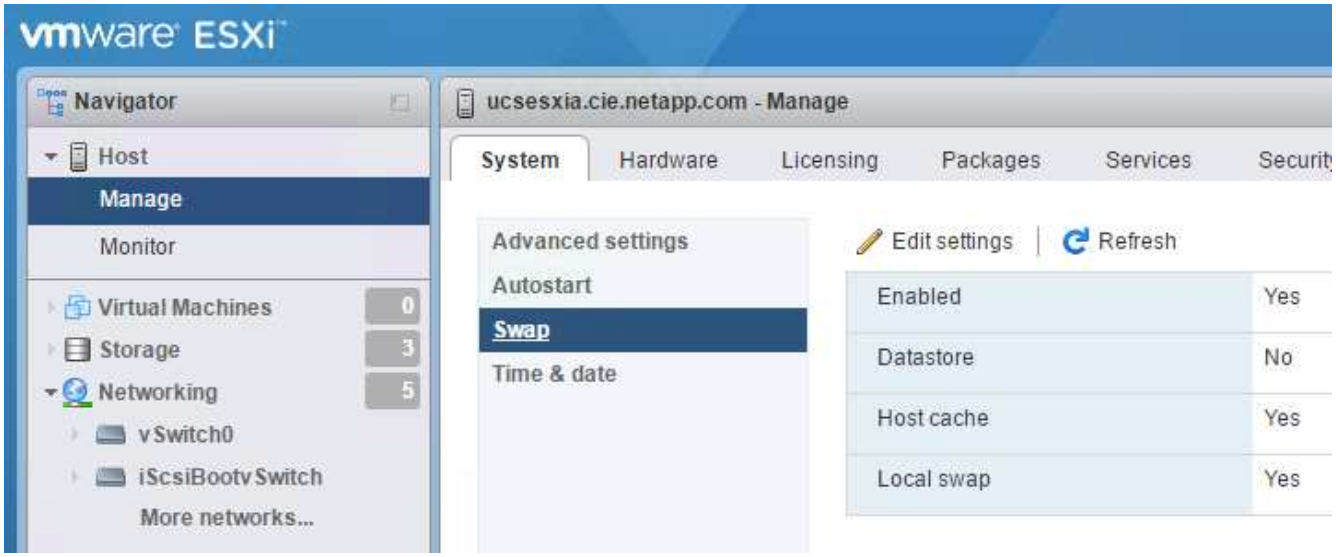
1. 左側のナビゲーションペインで、 [管理] をクリックします。右側のペインで [システム] を選択し、 [時刻と日付] をクリックします。
2. Use Network Time Protocol （ NTP クライアントを有効にする）を選択します。
3. NTP サービスのスタートアップポリシーとして、 Start and Stop With Host を選択します。
4. NTP サーバとして「 <<var_ntp>> 」と入力します。複数の NTP サーバを設定できます。
5. [保存] をクリックします .



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

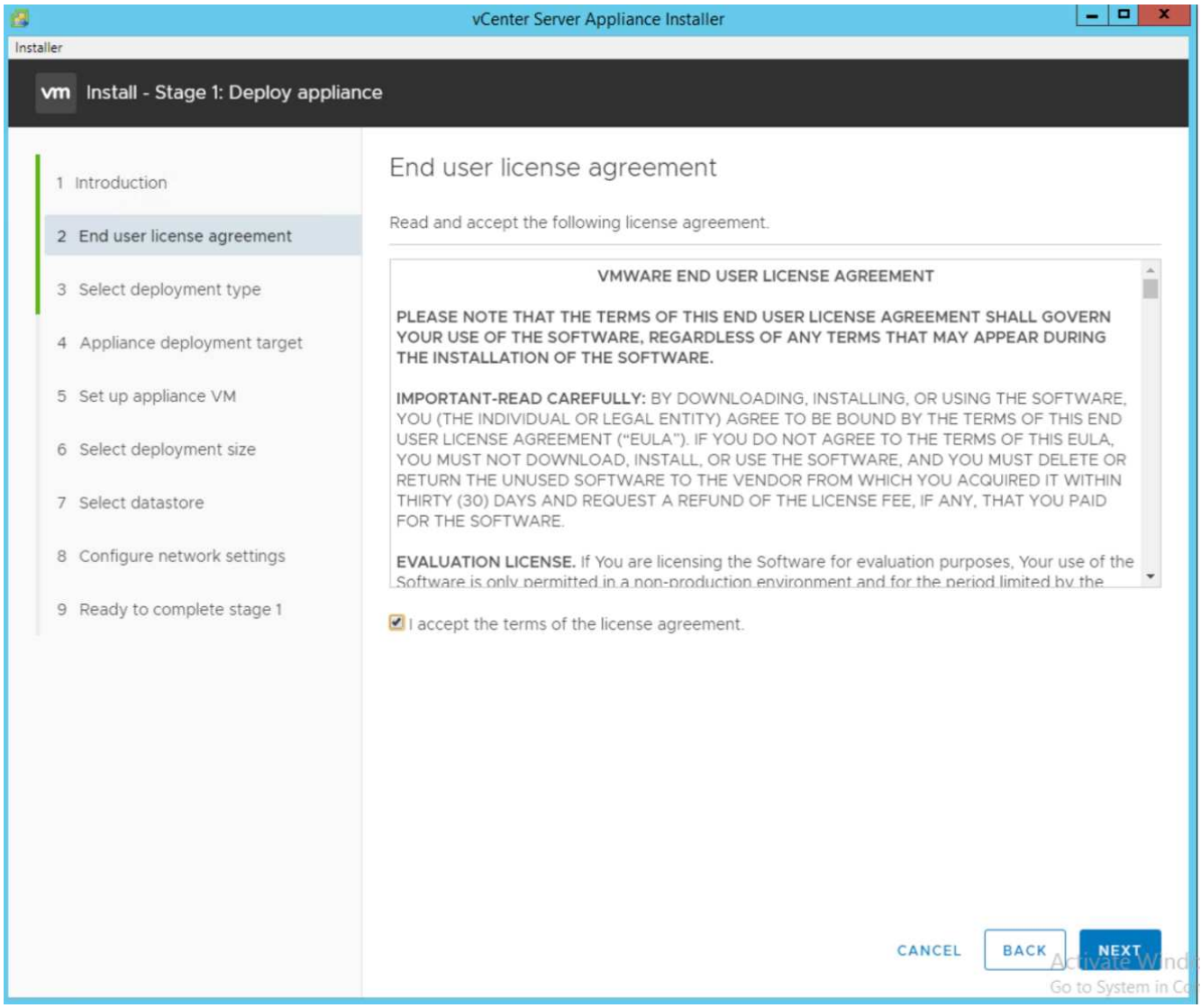
このセクションでは、 FlexPod 構成に VMware vCenter Server 6.7 をインストールする詳細な手順について説明します。

FlexPod Express では、 VMware vCenter Server Appliance （ VCSA ）を使用します。

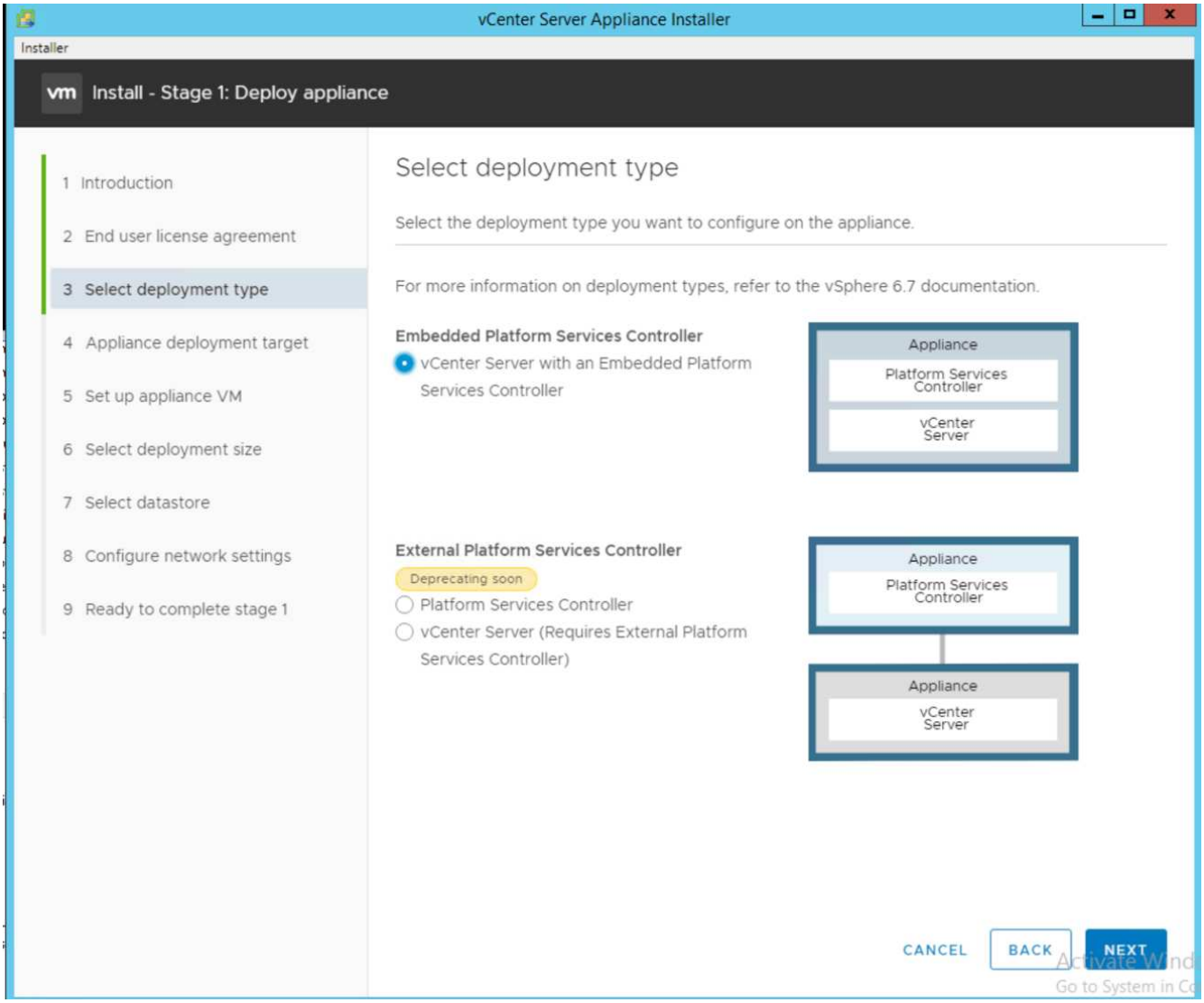
VMware vCenter Server Appliance をダウンロードします

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。

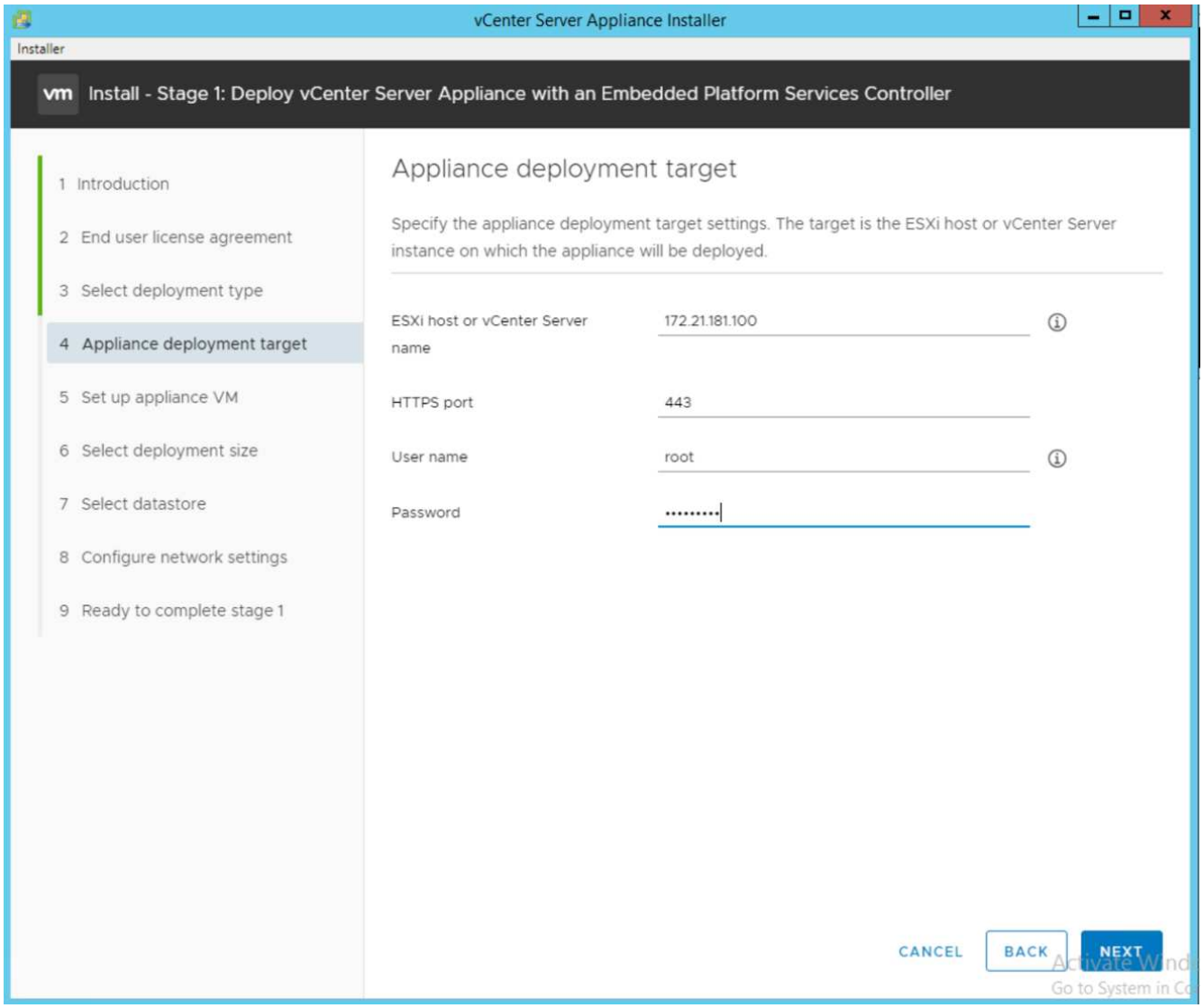


8. 展開タイプとして、 Embedded Platform Services Controller を選択します。

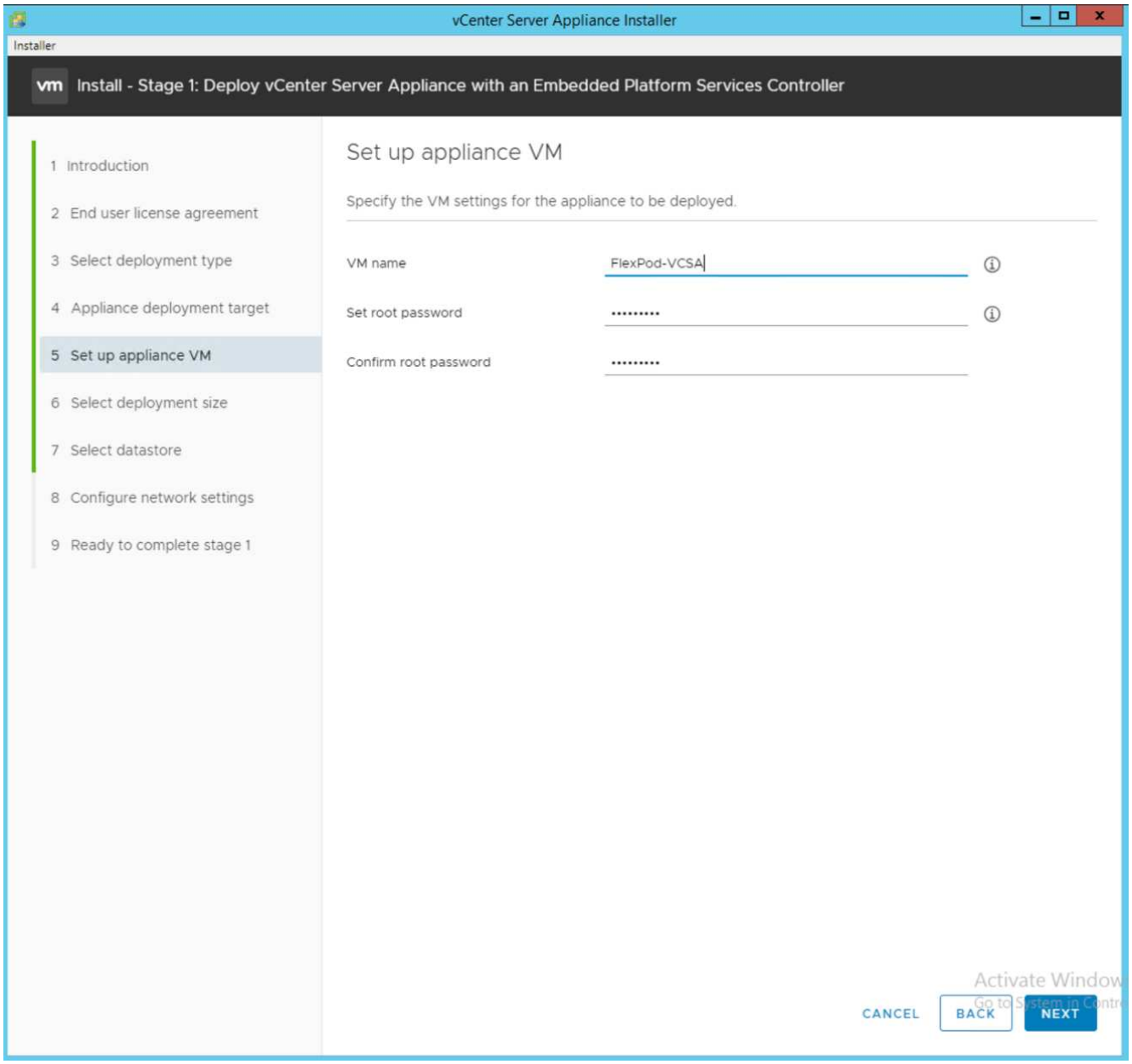


必要に応じて、 FlexPod Express 解決策の一部として、外部プラットフォームサービスコントローラの導入もサポートされます。

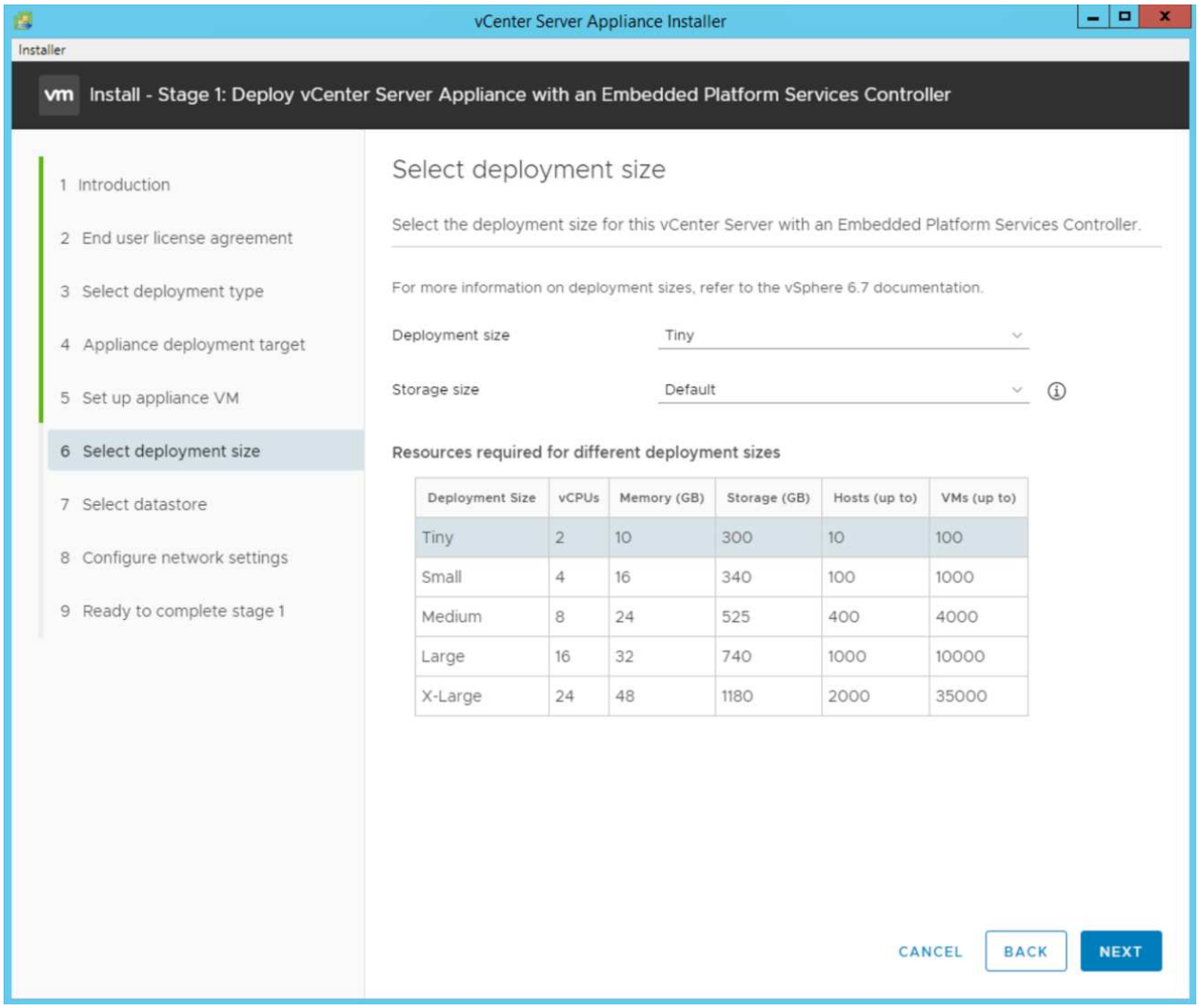
9. アプライアンス導入ターゲットで、導入した ESXi ホストの IP アドレス、ルートユーザ名、および root パスワードを入力します。



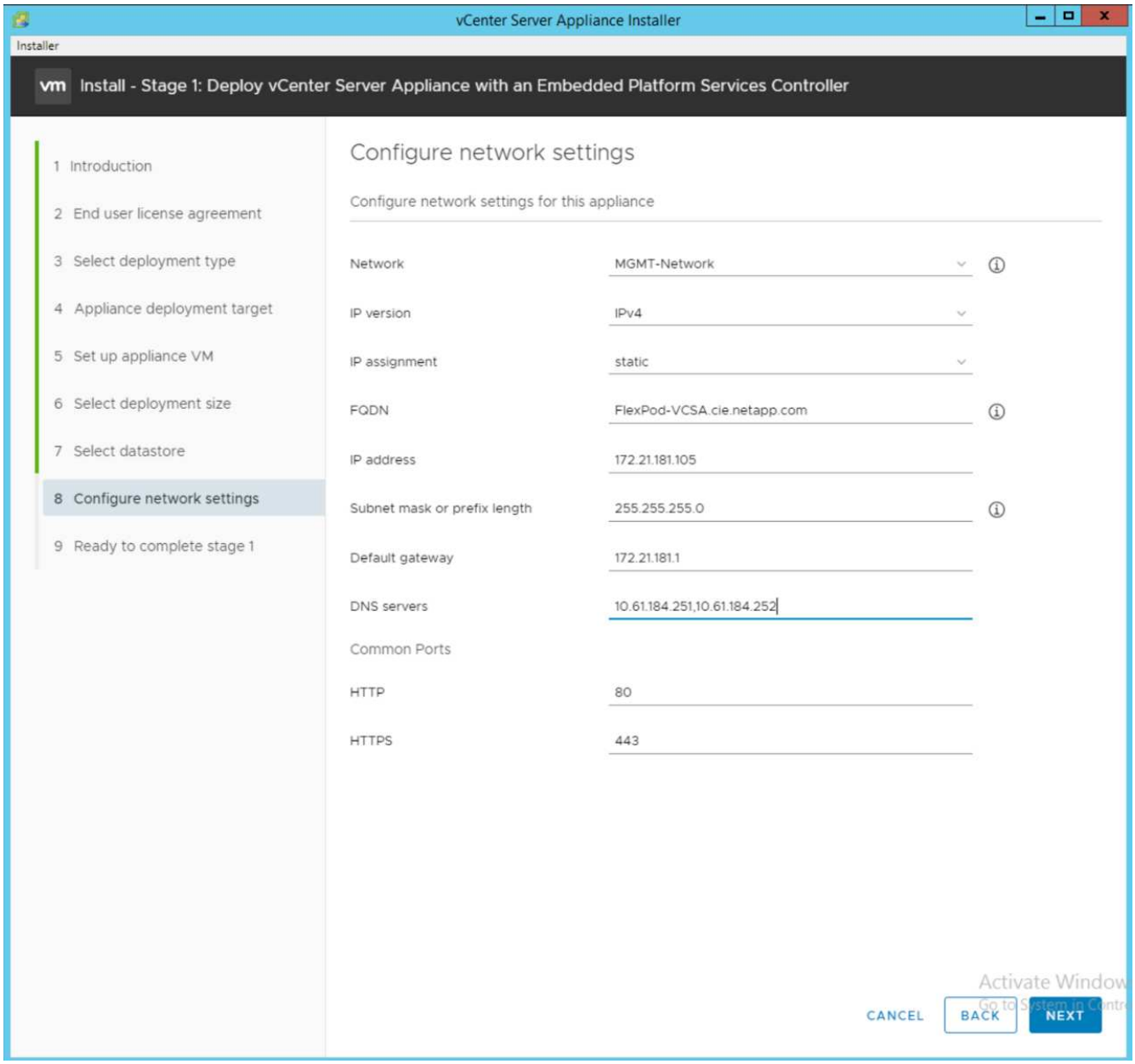
10. vCSA に VM 名および root パスワードとして入力し、 vCSA に使用するアプライアンス VM を設定します。



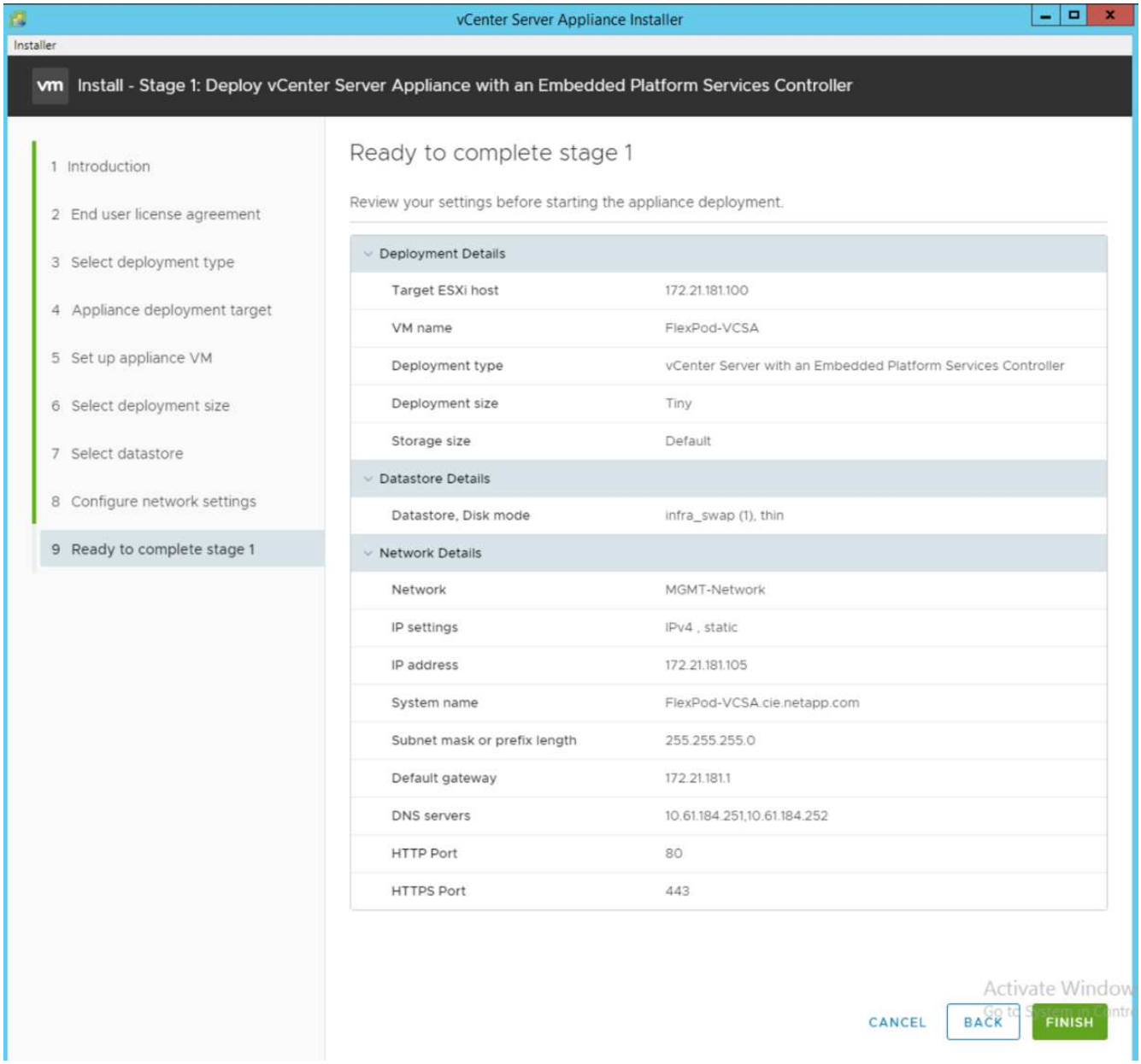
11. 環境に最も適した導入サイズを選択してください。次へをクリックします。



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。

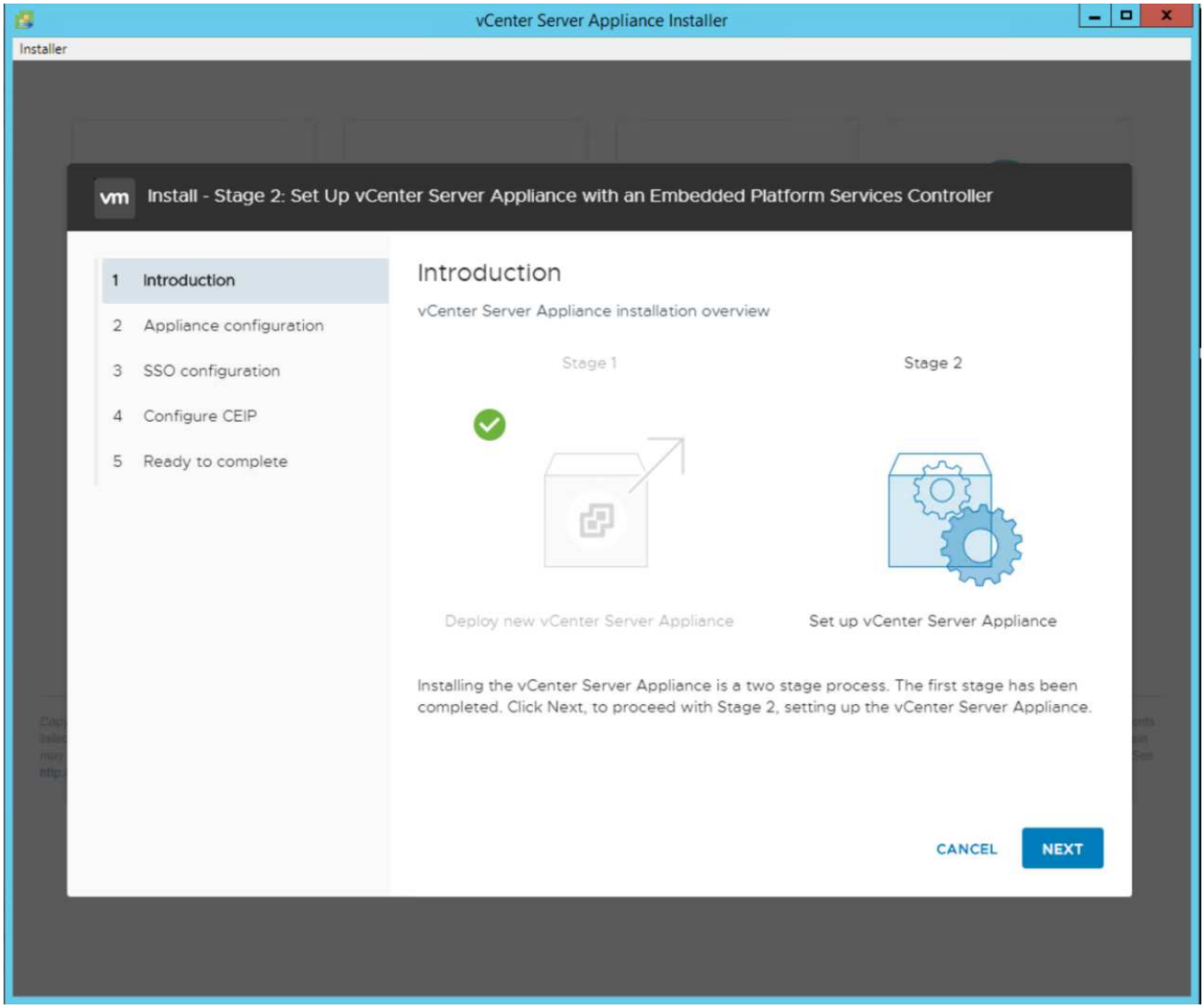


15. アプライアンスの導入を開始する前に、第 1 段階の設定を確認してください。

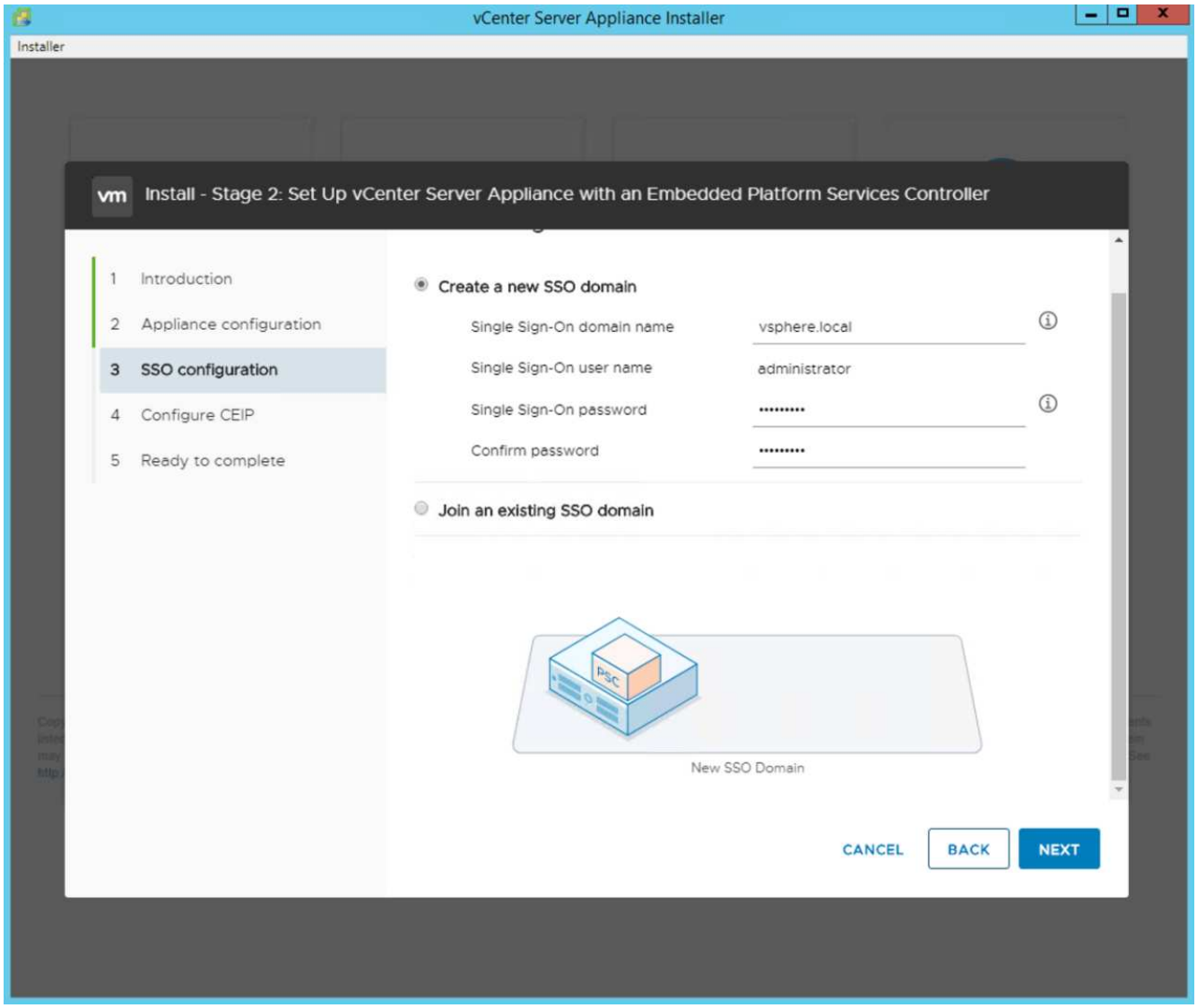


vCSA がインストールされます。このプロセスには数分かかります。

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。

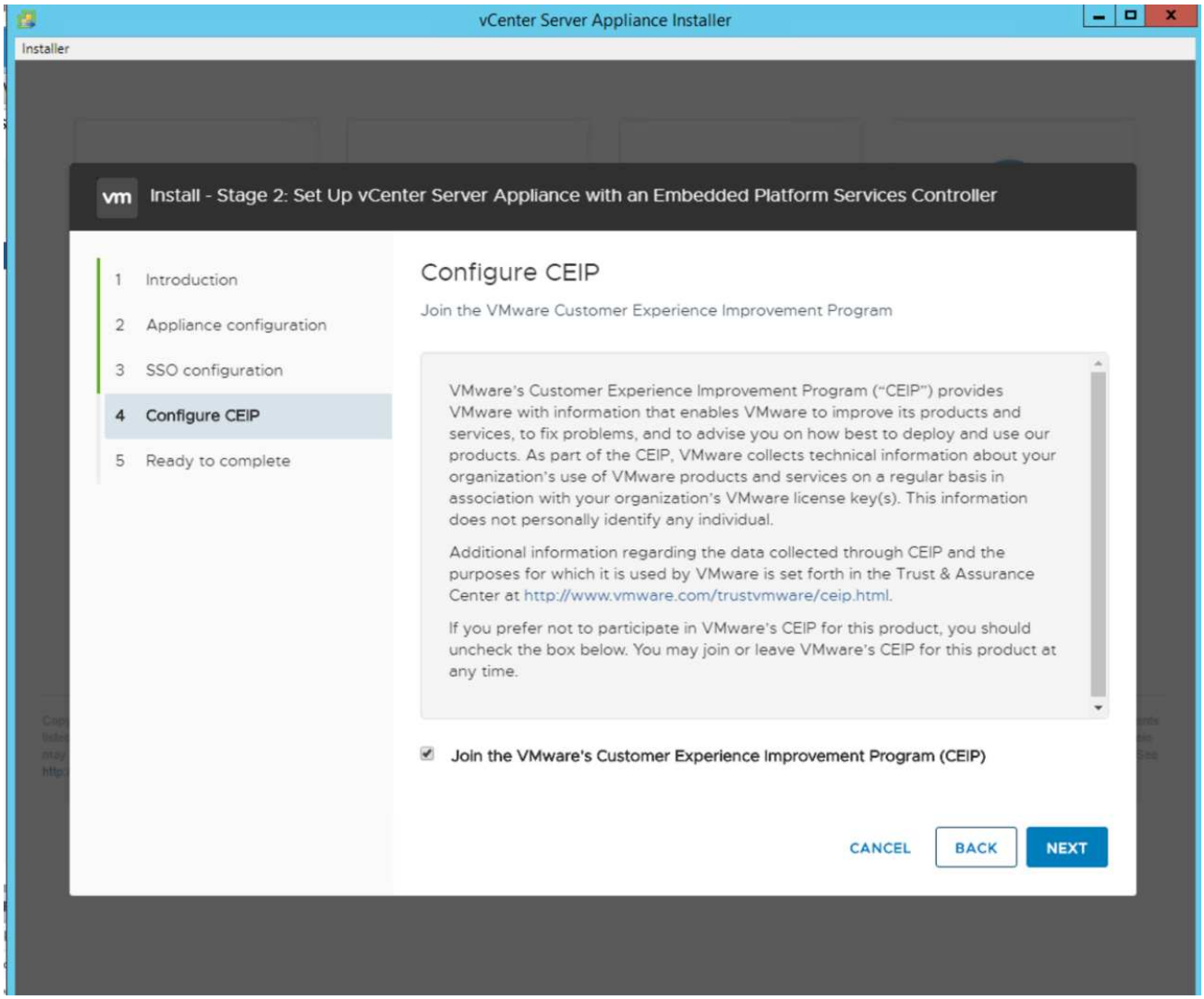


18. NTP サーバのアドレスとして「 \<<var_ntp_id>> 」と入力します。複数の NTP IP アドレスを入力できます。
19. vCenter Server High Availability （ HA ；高可用性）を使用する場合は、 SSH アクセスが有効になっていることを確認してください。
20. SSO ドメイン名、パスワード、およびサイト名を設定します。次へをクリックします。

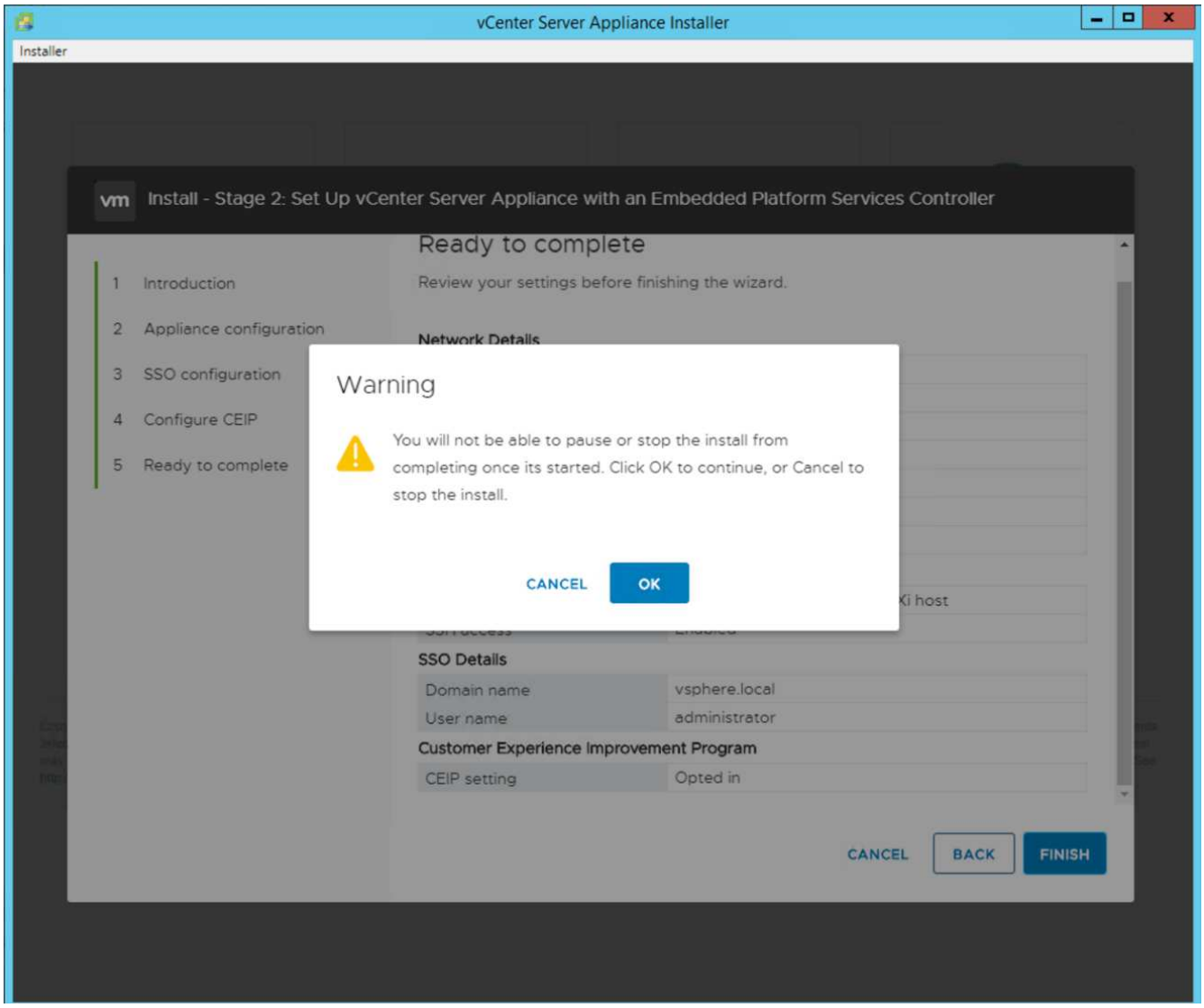


特に 'vSpher.local' ドメイン名から外れる場合は ' これらの値を参考にしてください

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。

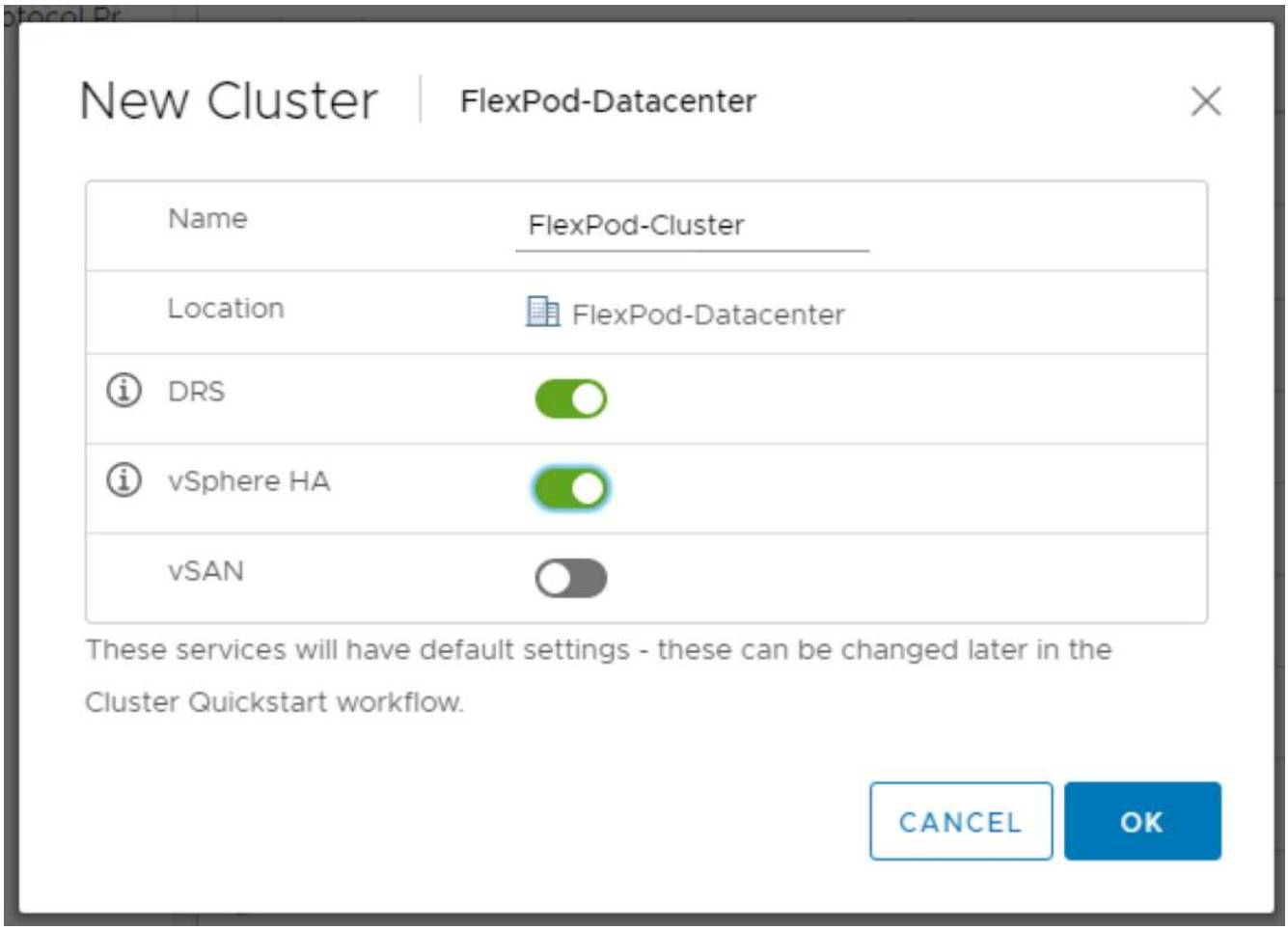
1. 「 \ https://\<<FQDN 」または「 vCenter の IP >>/vsphere-client/` 」に移動します。
2. vSphere Client の起動をクリックします。
3. vCSA のセットアッププロセスで入力したユーザ名 mailto ： administrator@vspehre.loca l [administrator^] @vsphere.local および SSO パスワードを使用してログインします。
4. vCenter 名を右クリックし、 New Datacenter を選択します。

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。

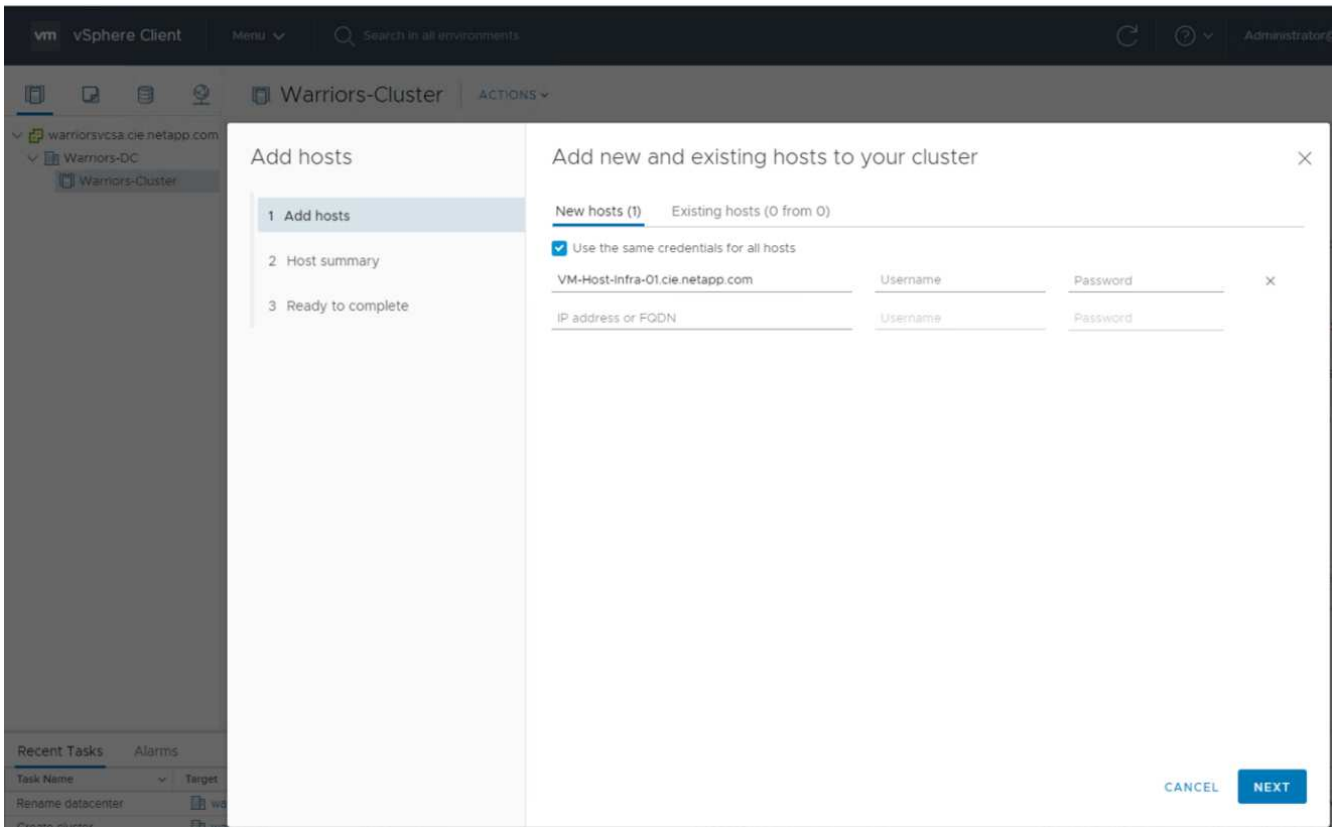
1. 新しく作成したデータセンターを右クリックし、 [New Cluster] を選択します。
2. クラスタの名前を入力します。
3. チェックボックスをオンにして DR と vSphere HA を有効にします。
4. [OK] をクリックします。



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

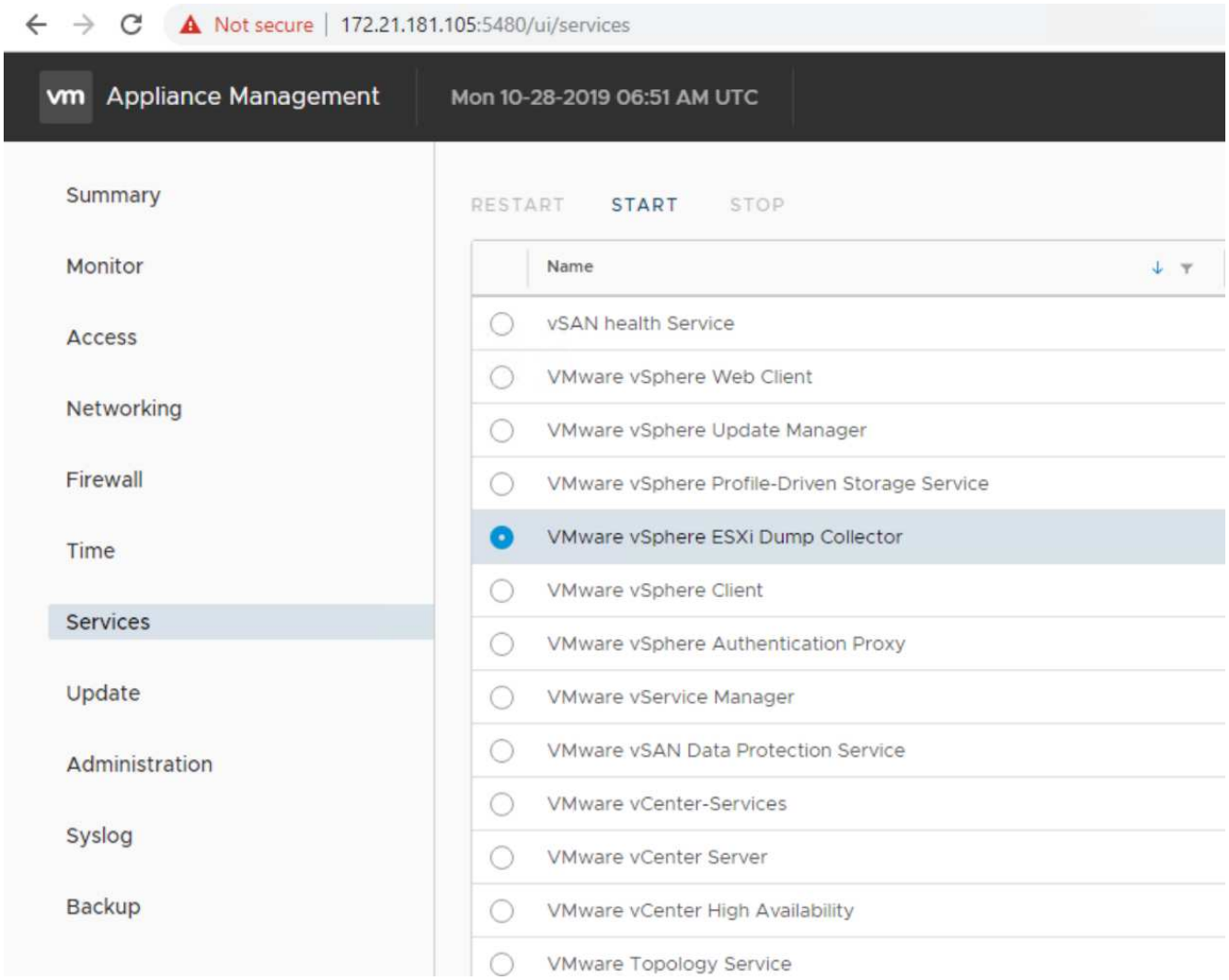
FlexPod 構成にホストを追加する場合は、この手順を実行する必要があります。

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"

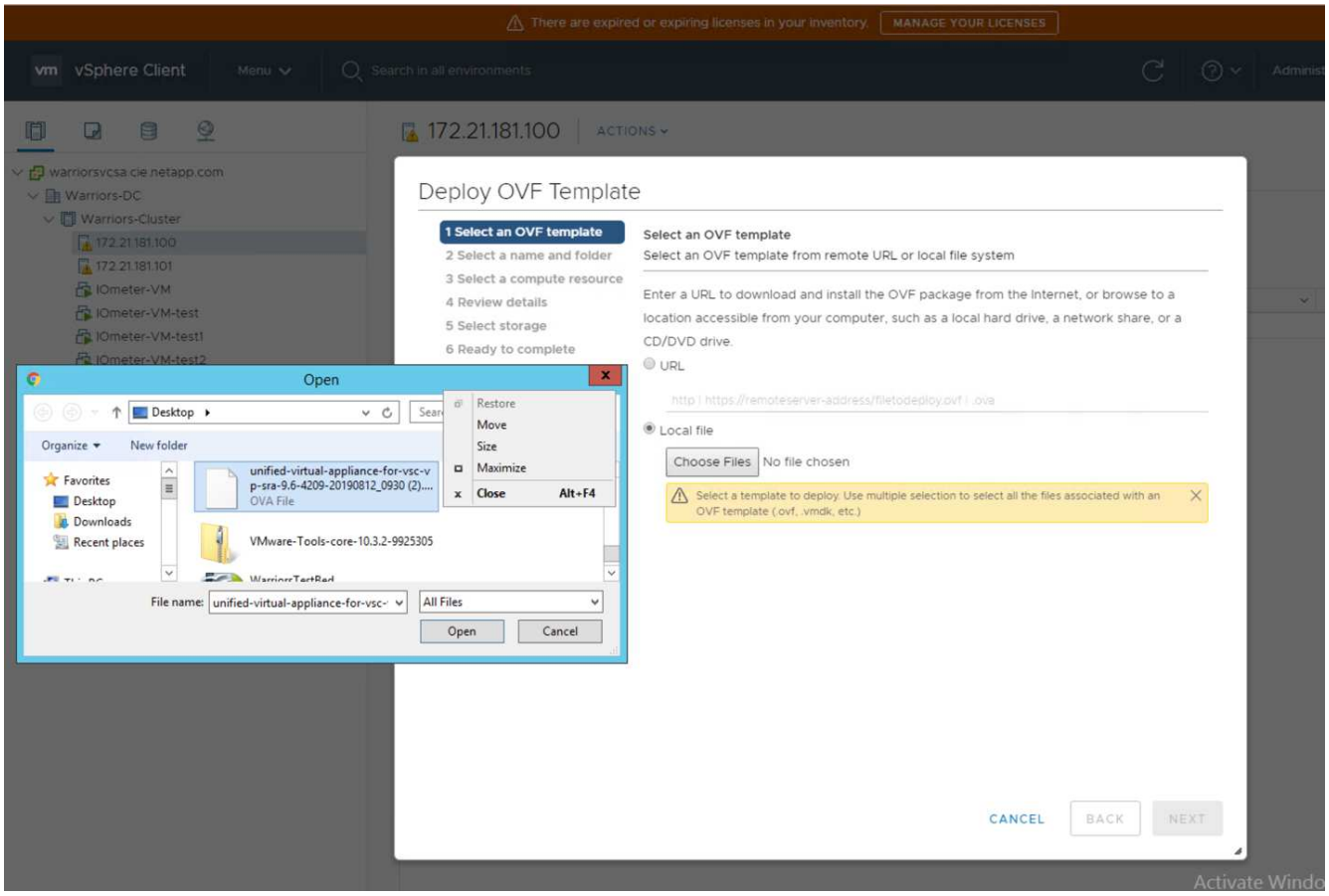
NetApp Virtual Storage Console 9.6 の導入手順

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

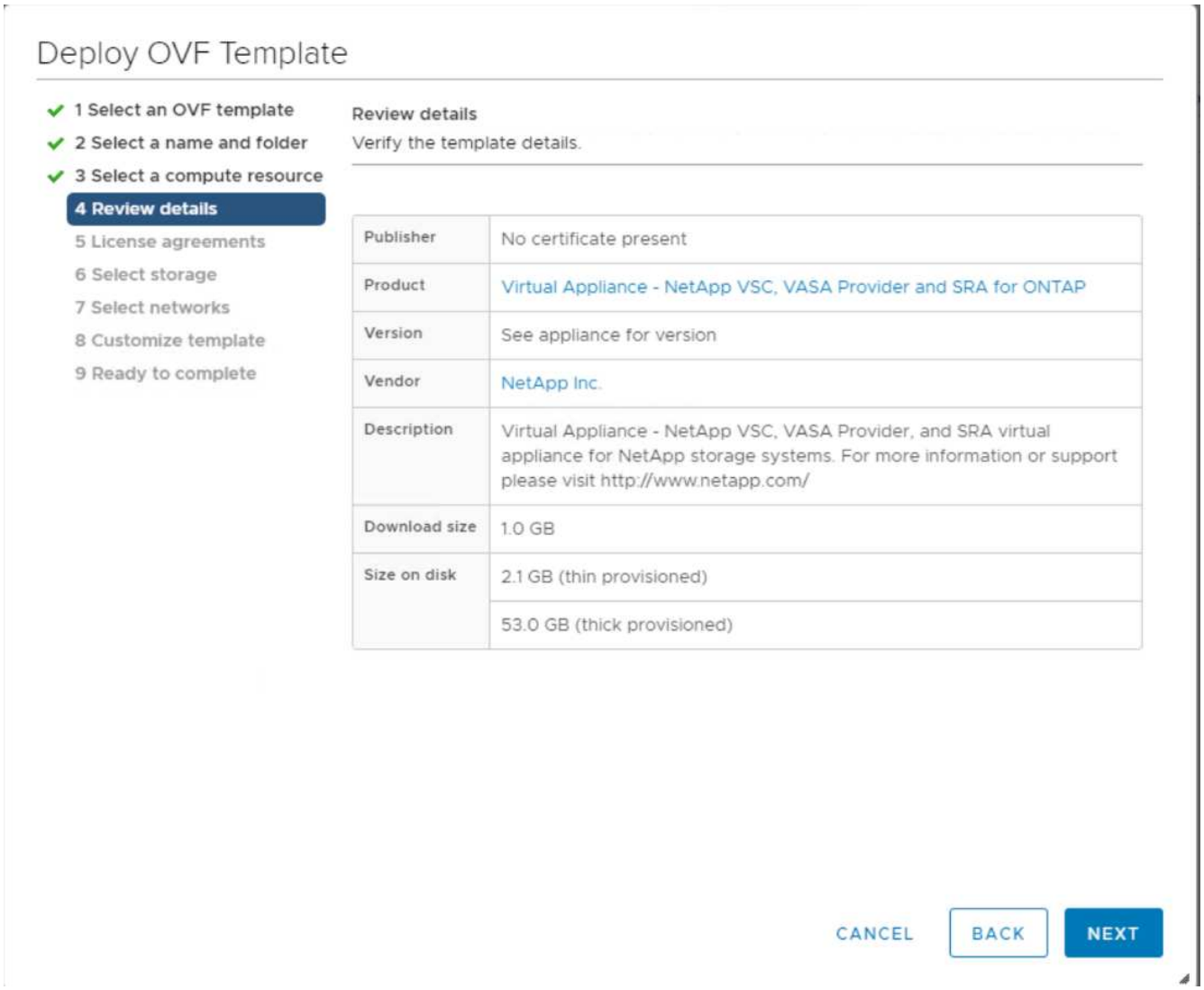
Open Virtualization Format （ OVF ）導入を使用して VSC 9.6 ソフトウェアをインストールする手順は、次のとおりです。

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。

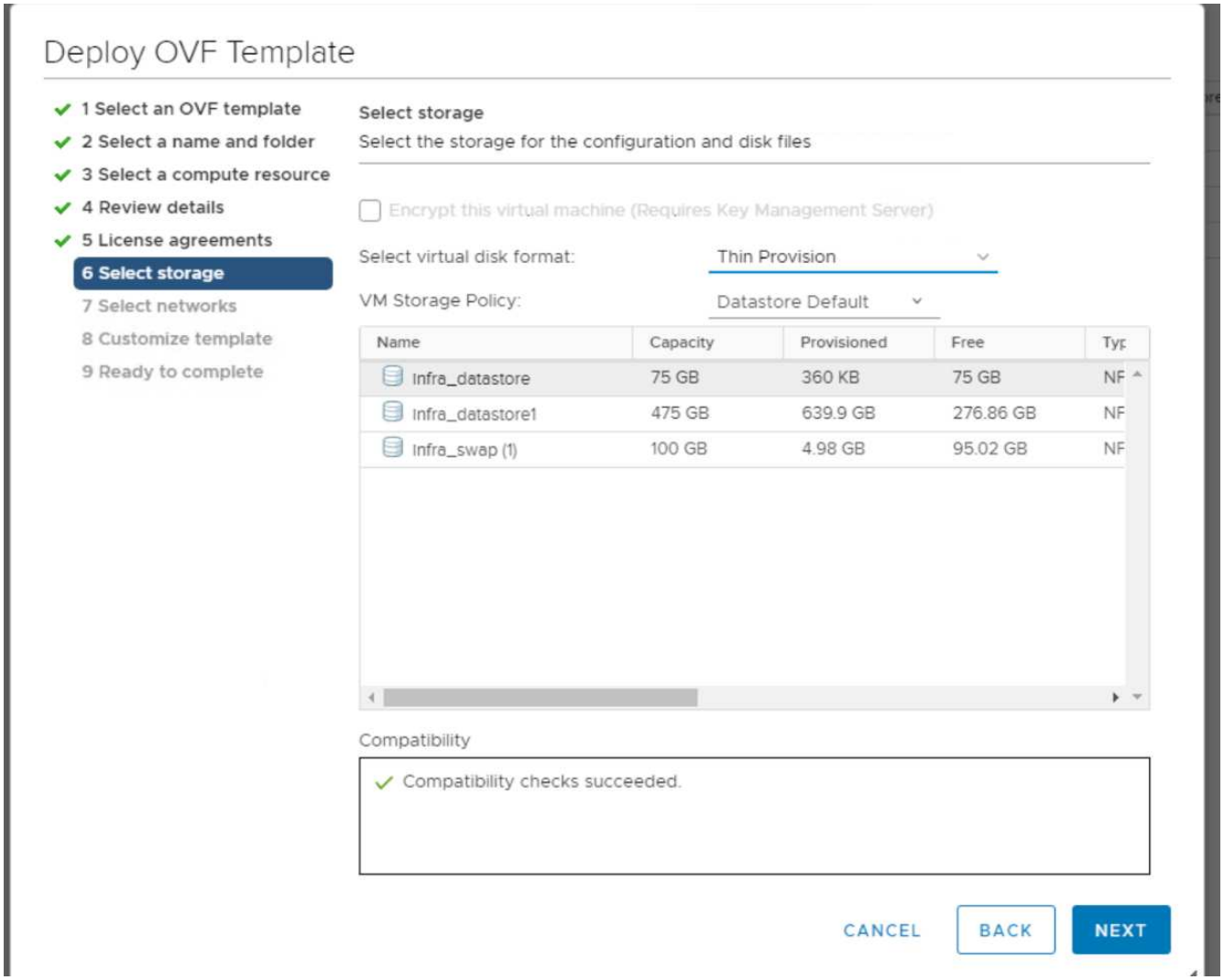


3. VM 名を入力し、導入先のデータセンターまたはフォルダを選択します。次へをクリックします。

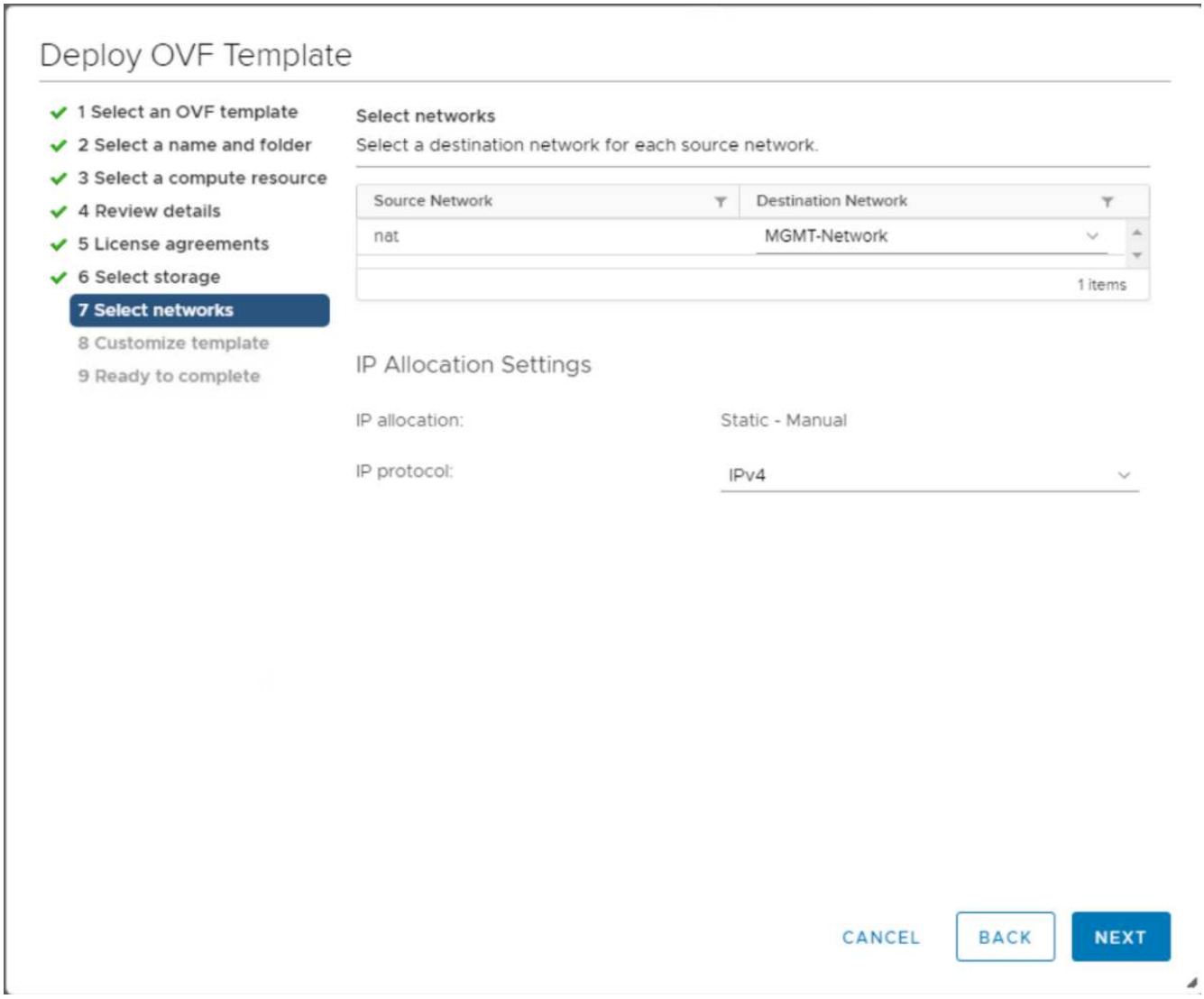
4. 「 FlexPod - Cluster ESXi 」クラスタを選択し、「 Next 」をクリックします。
5. 詳細を確認し、 [次へ] をクリックします。



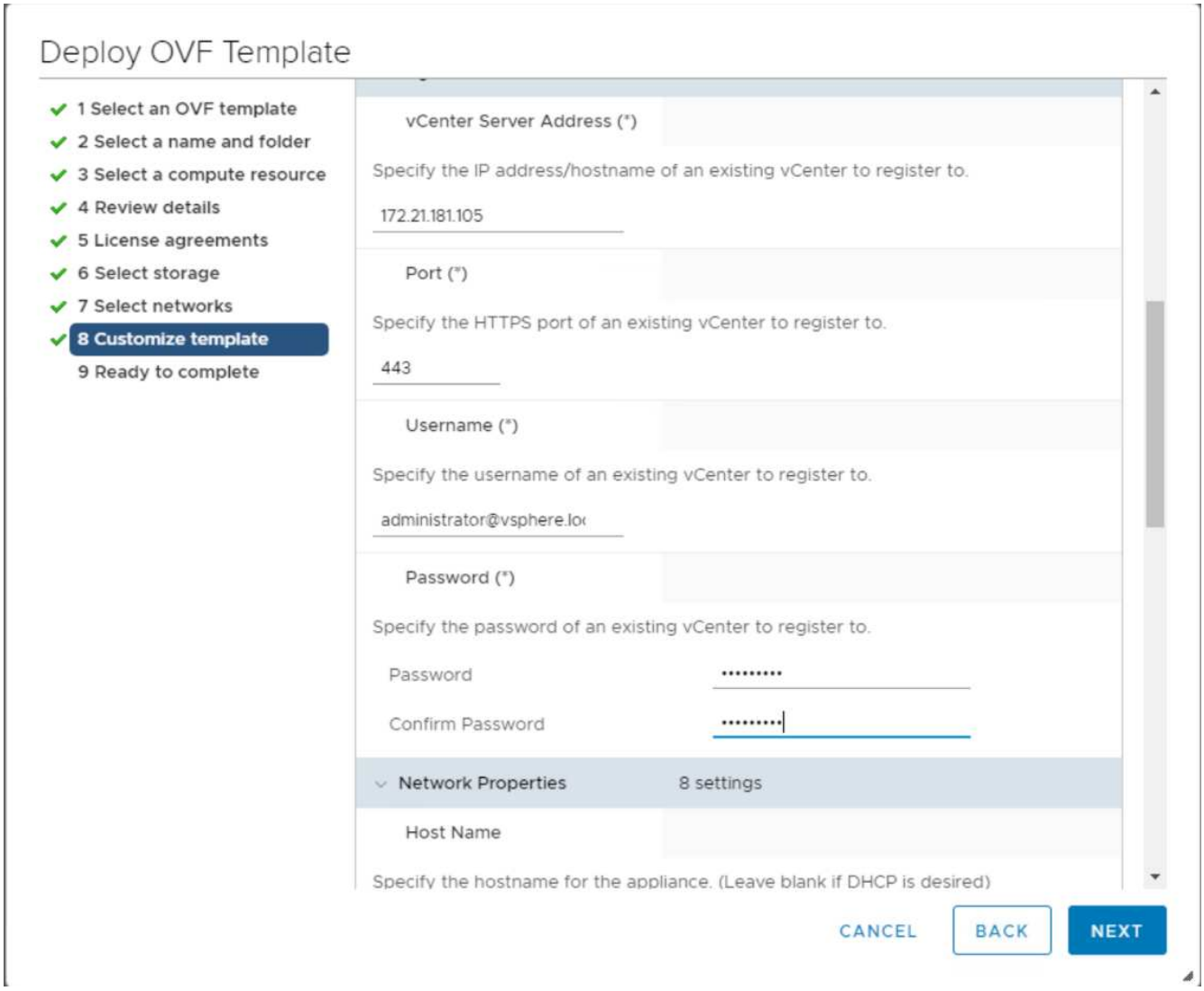
6. [Accept （同意）] をクリックしてライセンスを受け入れ、 [Next] をクリックします。
7. シンプロビジョニング仮想ディスク形式と NFS データストアの 1 つを選択します。次へをクリックします。



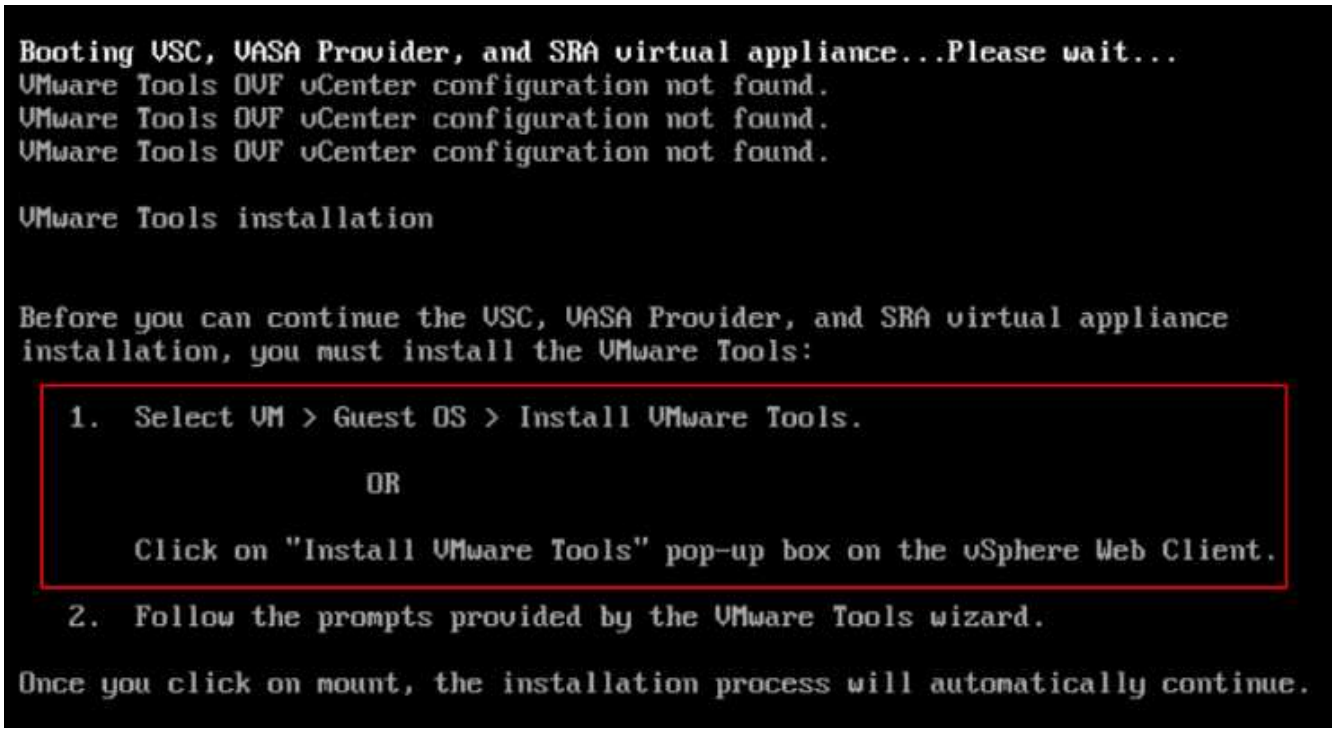
8. [Select Networks] (ネットワークの選択) から宛先ネットワークを選択し、 [Next] (次へ) をクリックします。



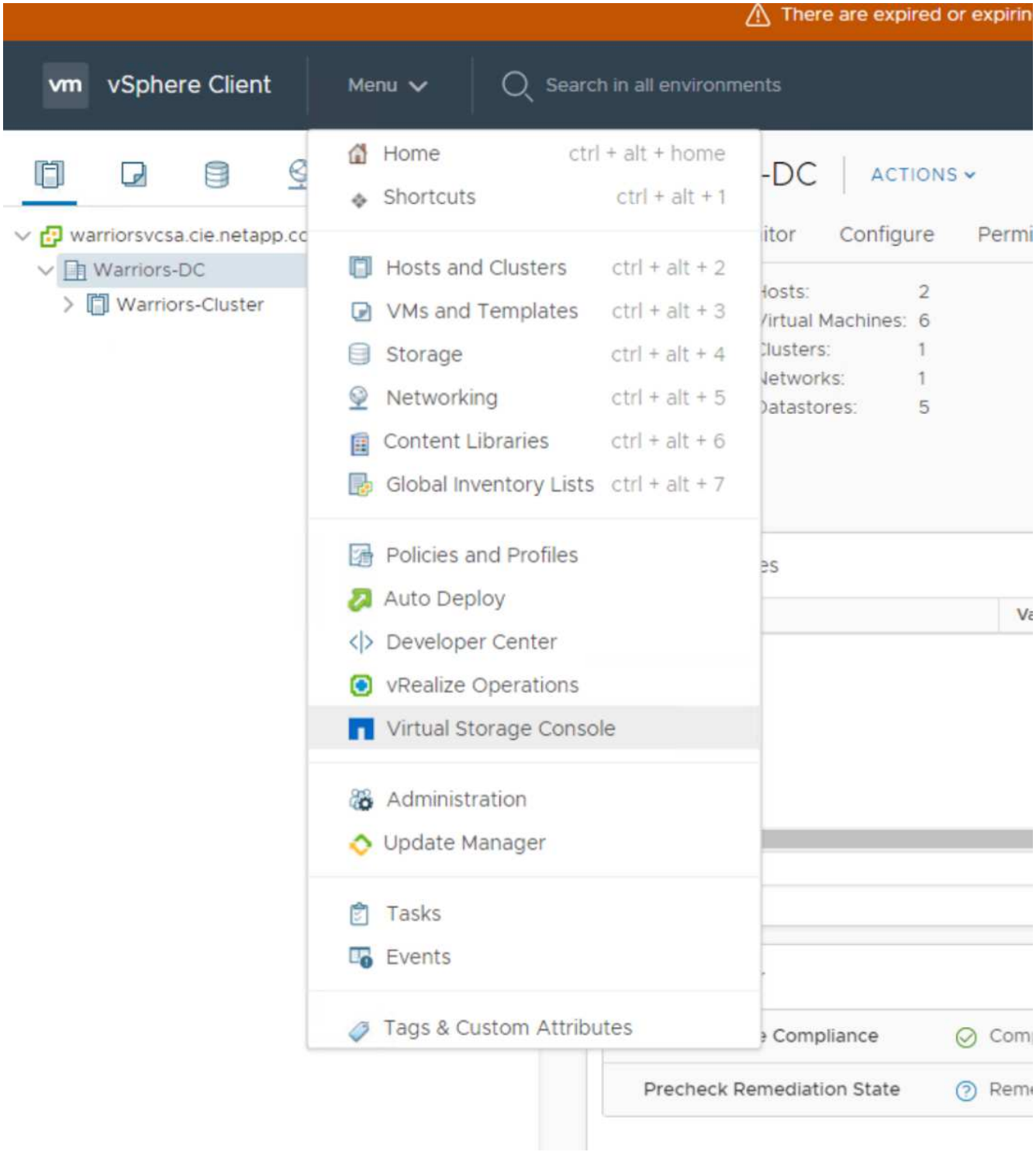
9. テンプレートのカスタマイズで、 VSC 管理者パスワード、 vCenter 名または IP アドレス、およびその他の設定の詳細を入力し、次へをクリックします。



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。



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

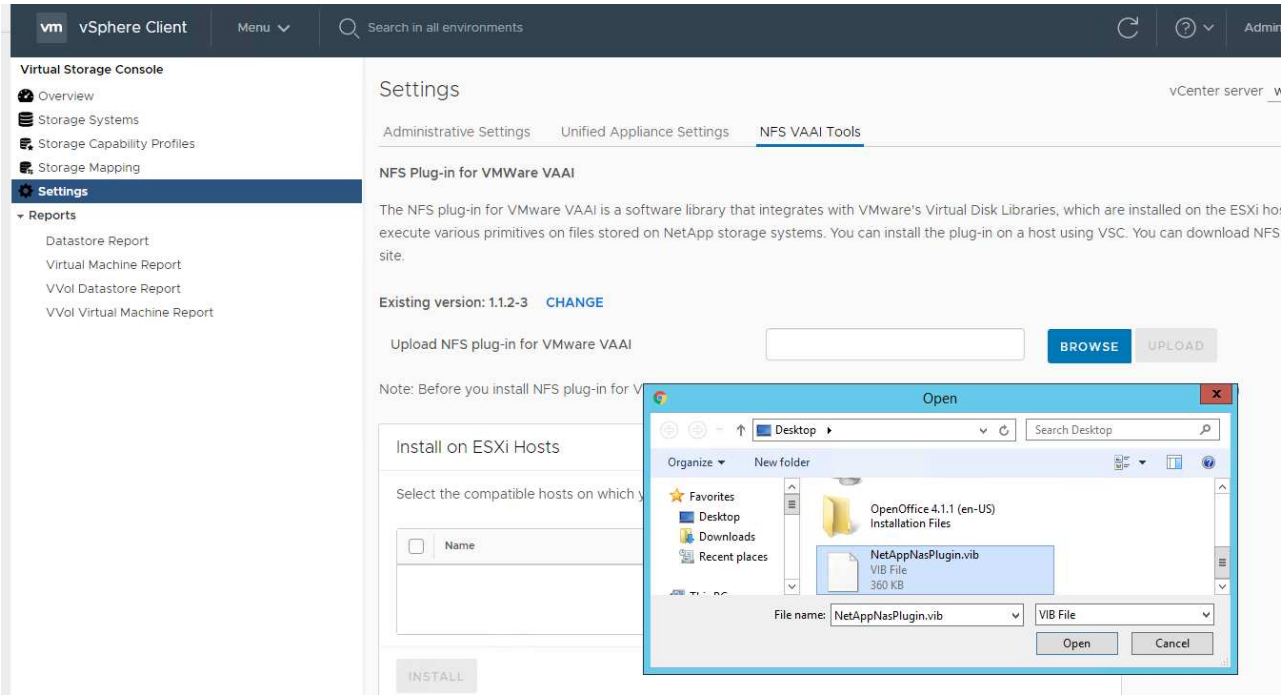
NetApp NFS VAAI Plug-in をダウンロードしてインストールするには、次の手順を実行します。

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。

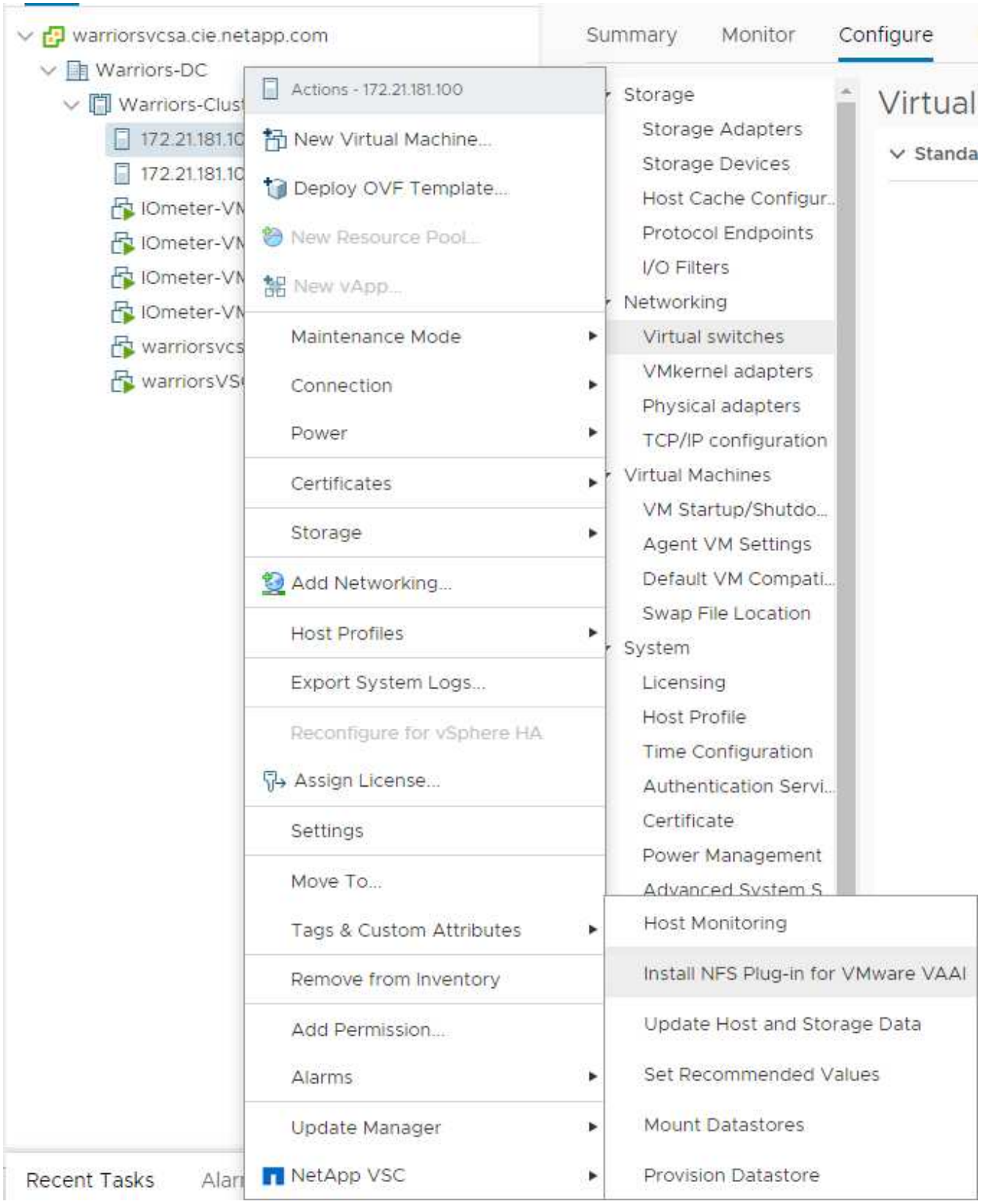
c. vSphere Web Client のホーム画面で、 Virtual Storage Console を選択します。

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。

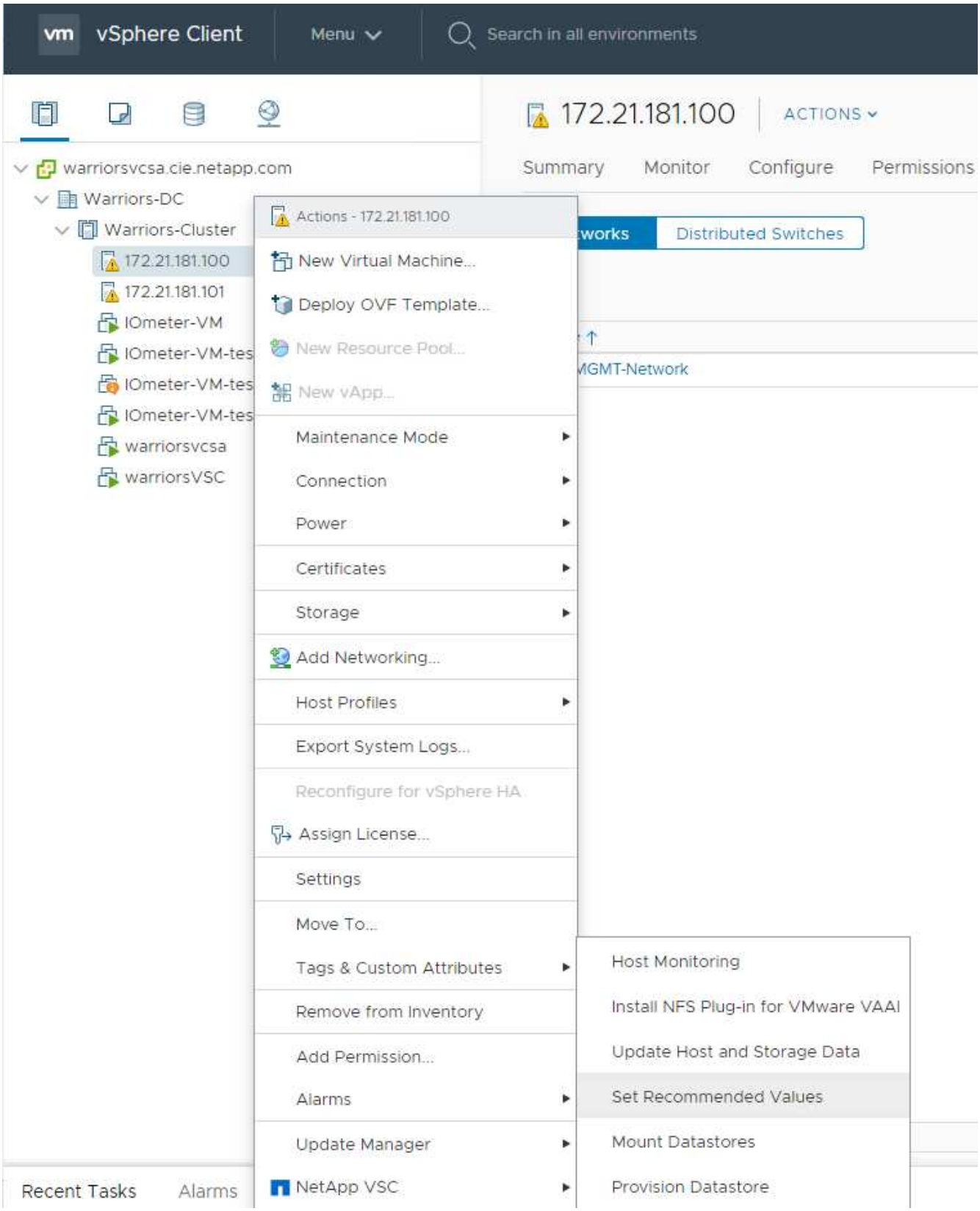
4. ホストを選択し、 NetApp VSC > Install NFS Plug-in for VMware VAAI の順に選択します。



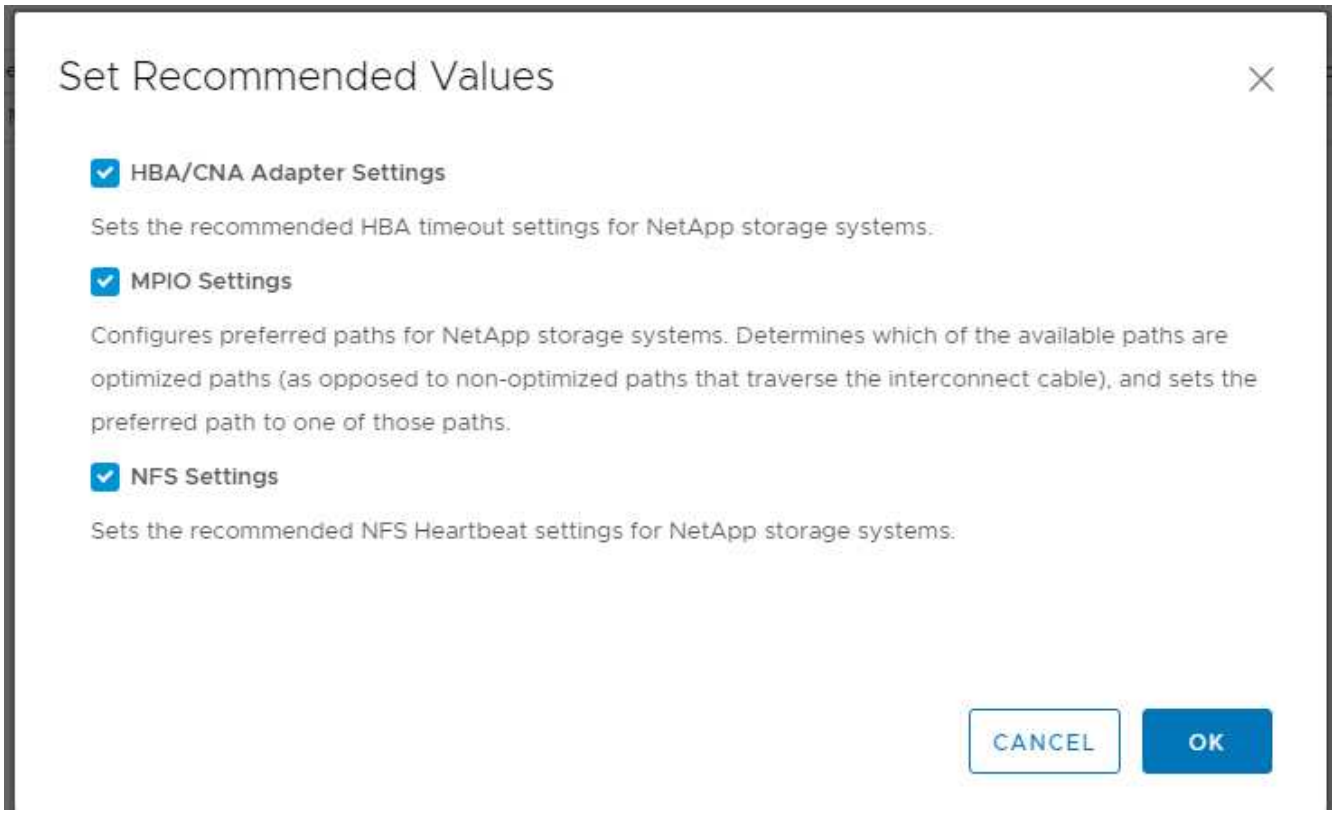
ESXi ホストのストレージ設定を最適化します

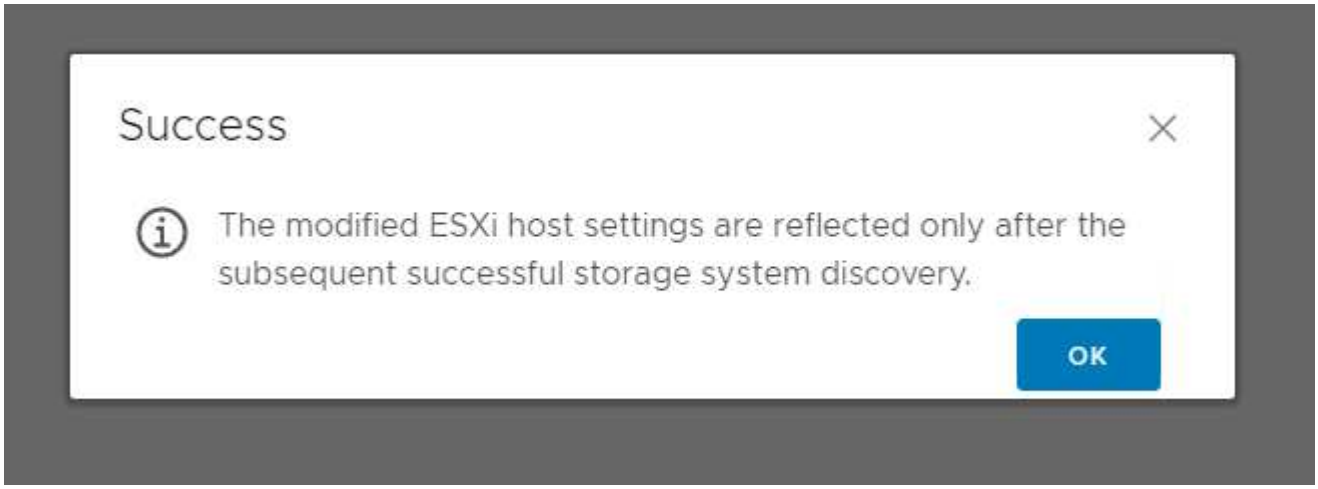
VSC を使用すると、ネットアップストレージコントローラに接続されているすべての ESXi ホストに対して、ストレージ関連の設定を自動的に構成できます。これらの設定を使用するには、次の手順を実行します。

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"

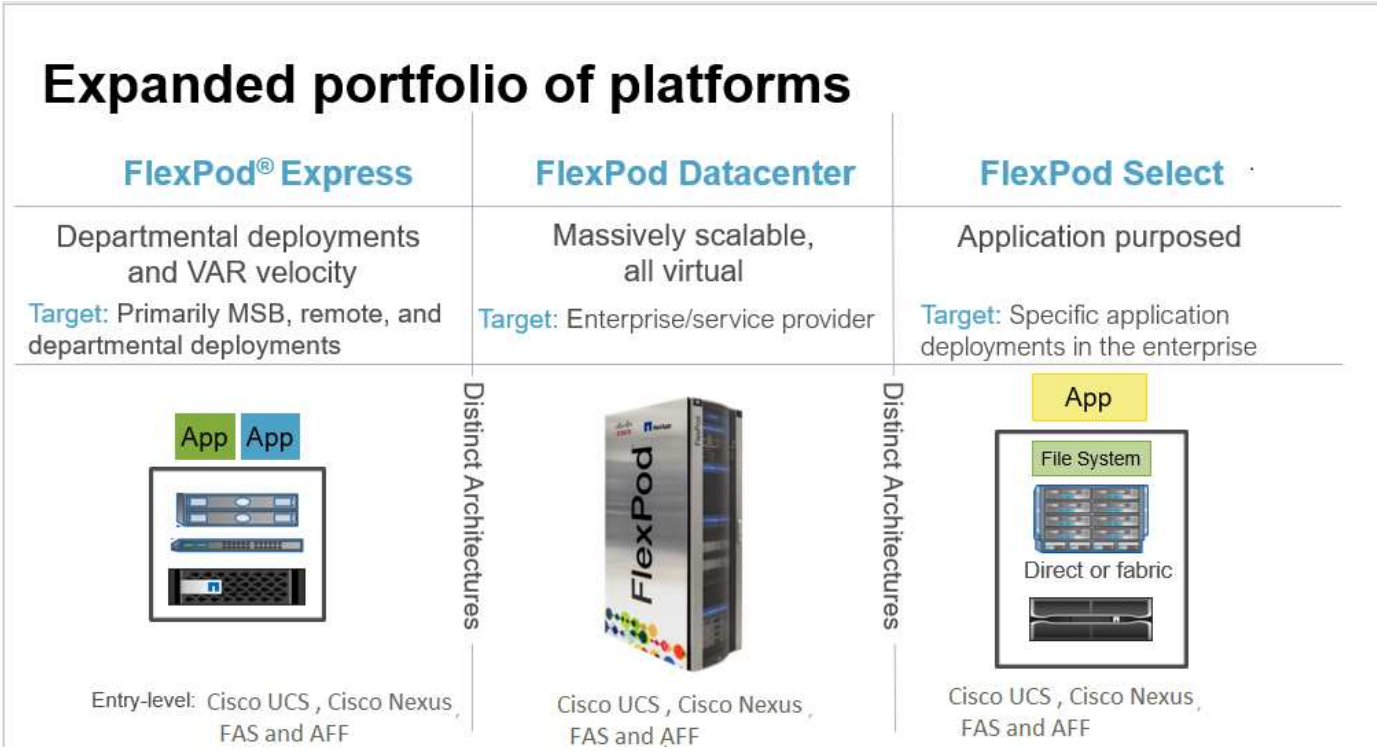
プログラムの概要

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。

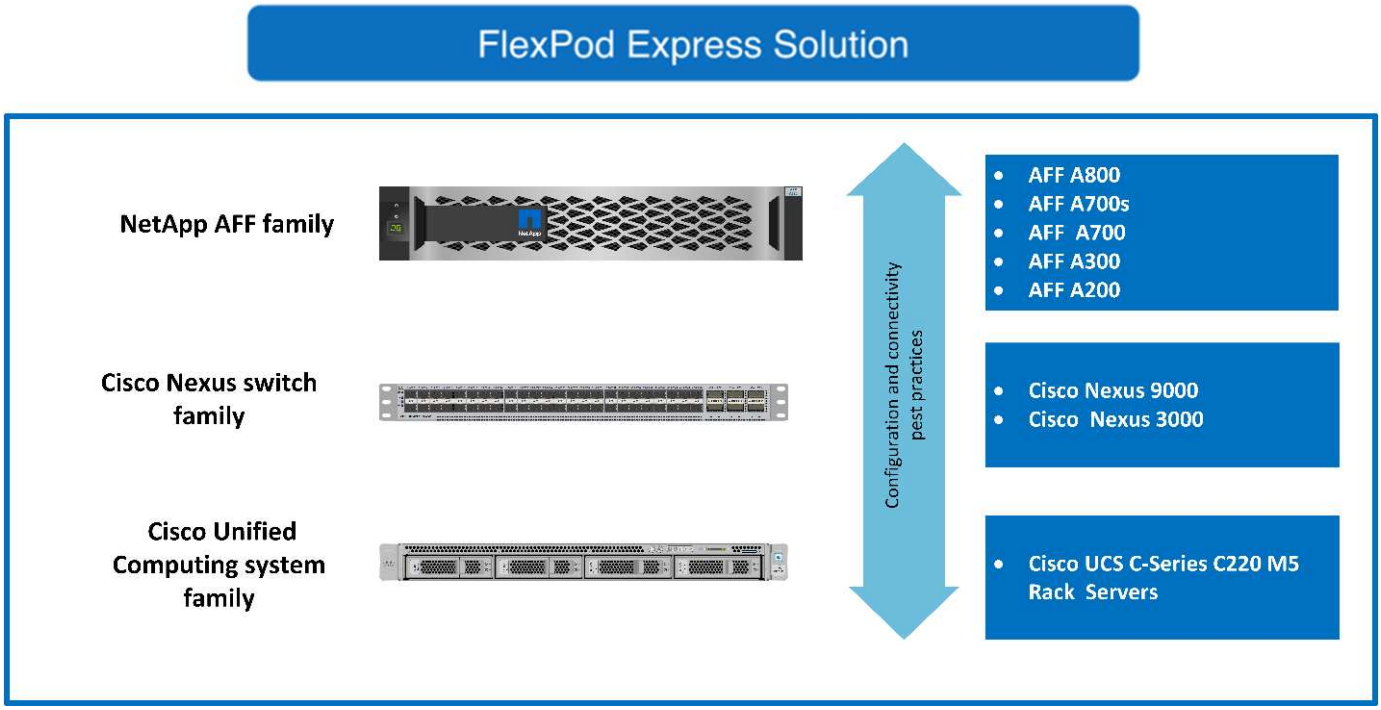
このドキュメントは AFF A220 で検証済みですが、この解決策は FAS2700 もサポートしています。

"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。



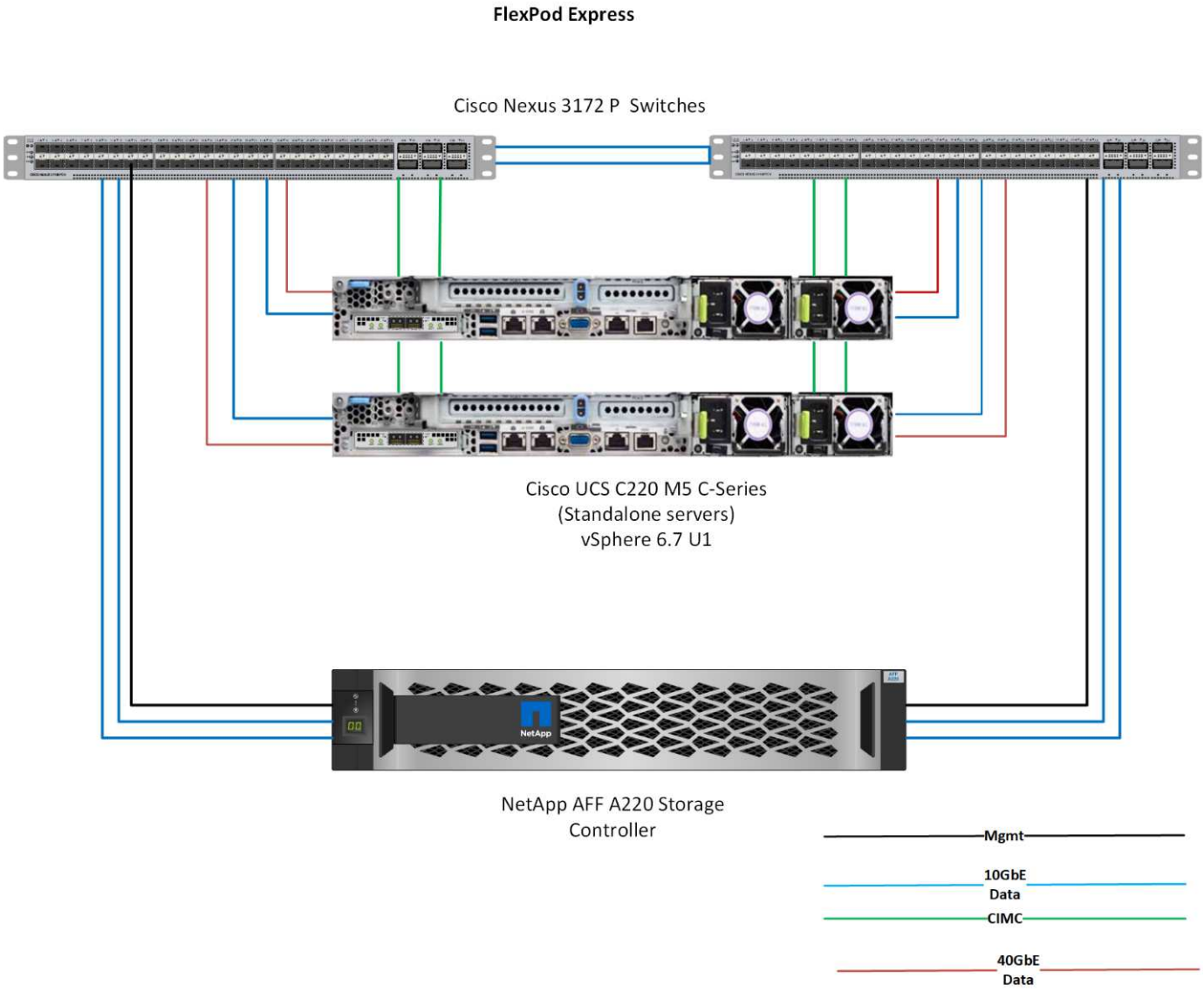
対象読者

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。

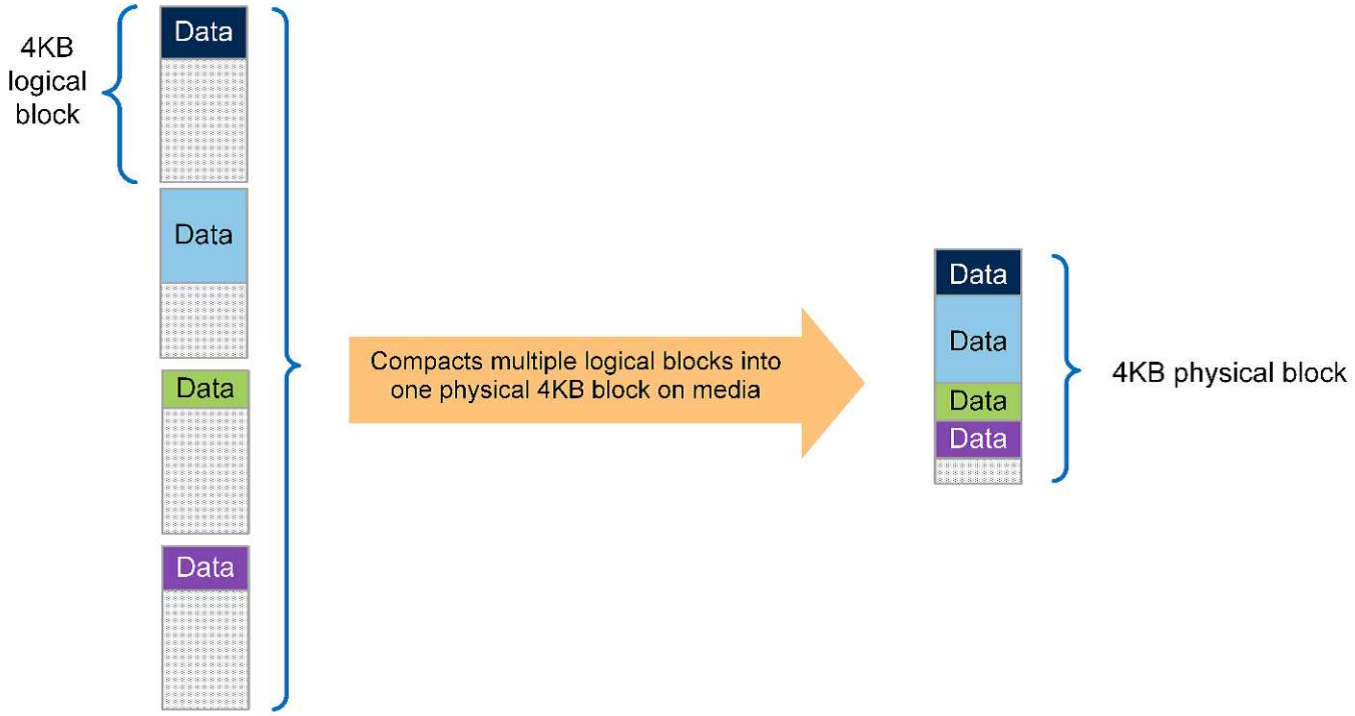
AFF A220 システム

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"。

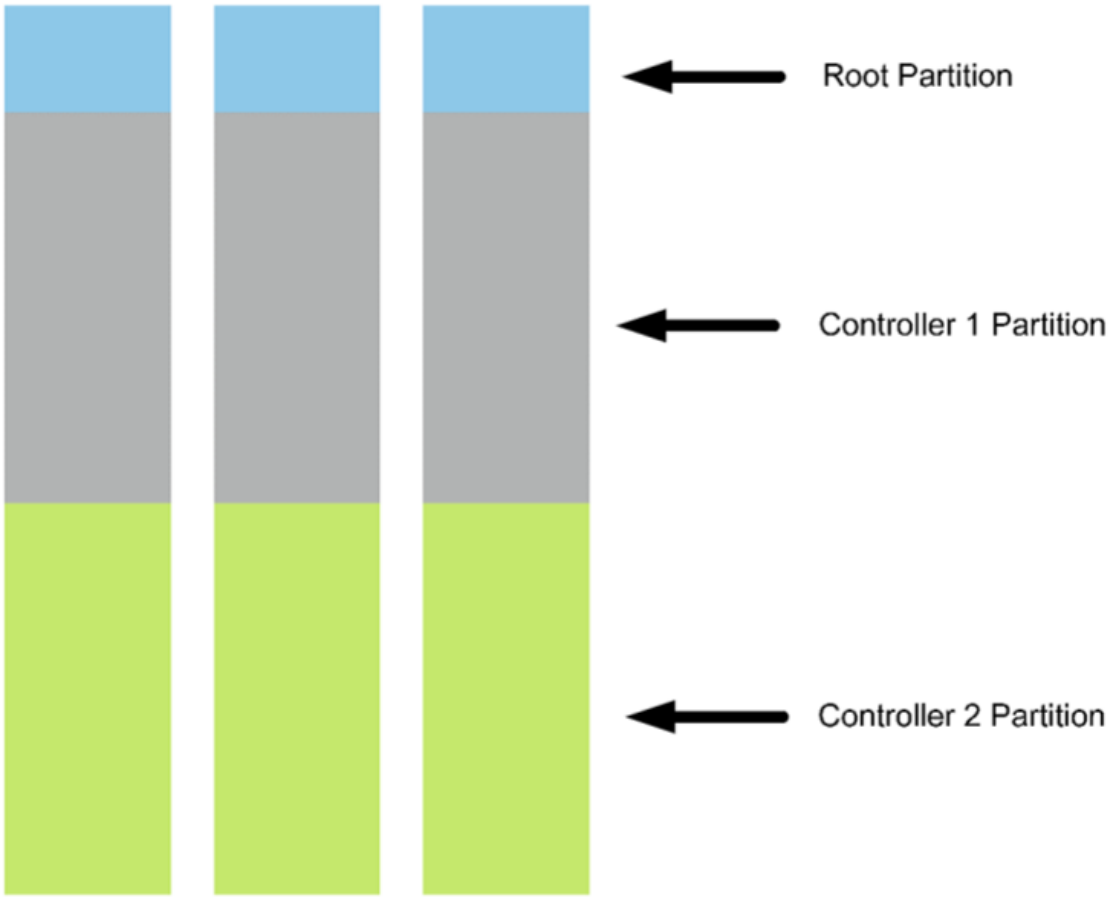
ONTAP 9.4 ソフトウェア

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の追加機能の詳細については、を参照してください。4 "ONTAP 9 データ管理ソフトウェアのデータシート"また、 "ONTAP 9 ドキュメンテーション・センター"ONTAP 9を含むように更新されたNetAppも参照してください。4.

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

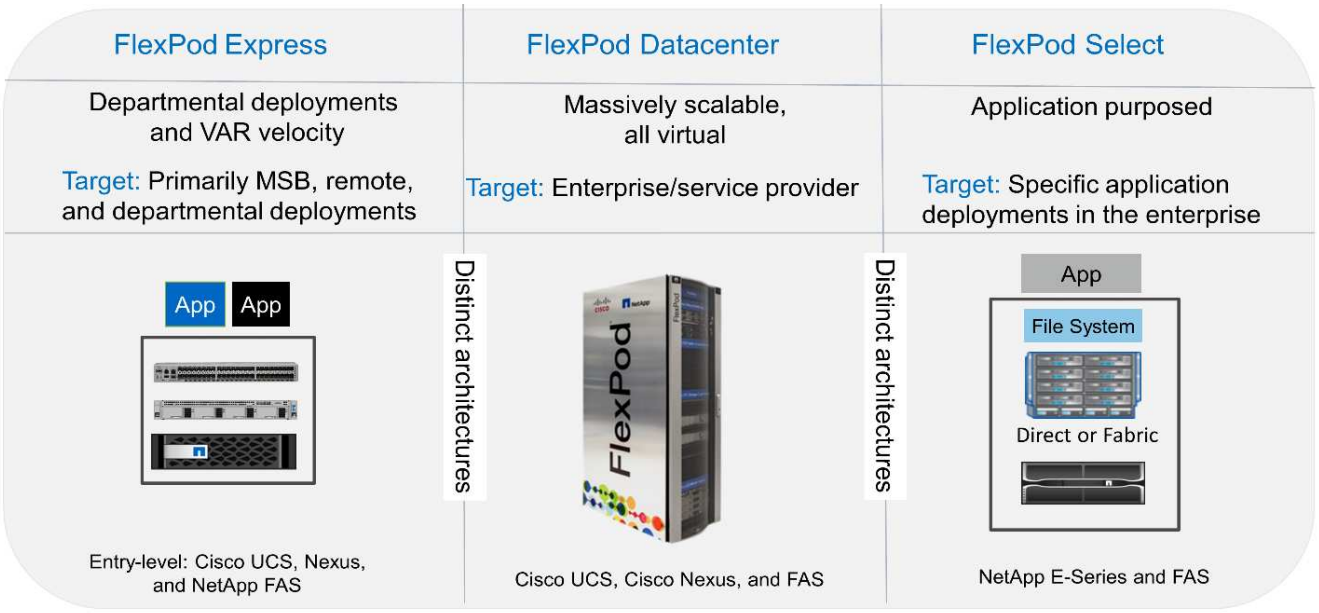
この FlexPod Express 解決策は、 FlexPod コンバージドインフラプログラムの一部です。

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。

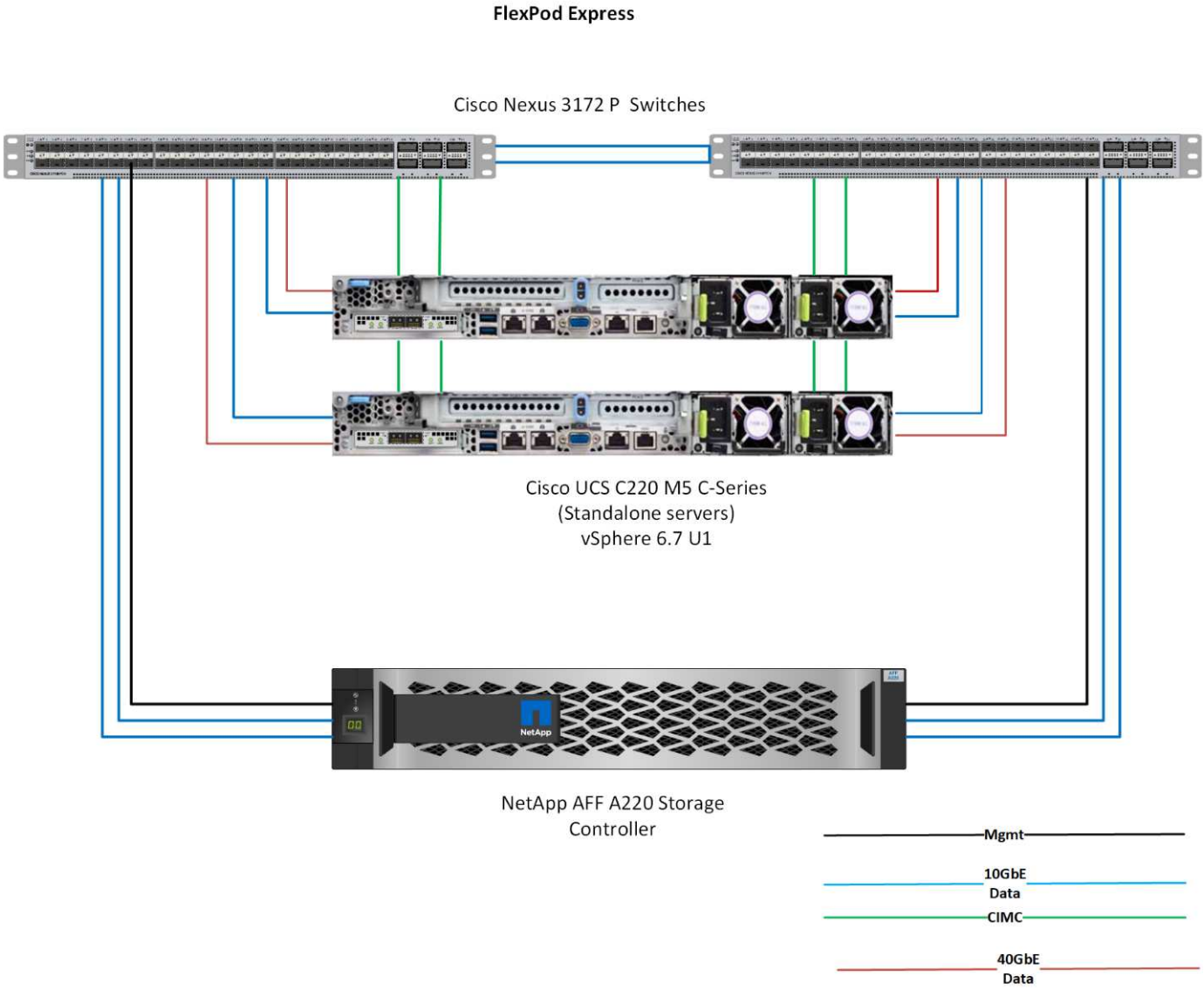
- 入念にテストされています
- あらかじめ規定されている
- 導入リスクを最小限に抑えます
- 運用開始までの時間を短縮

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。

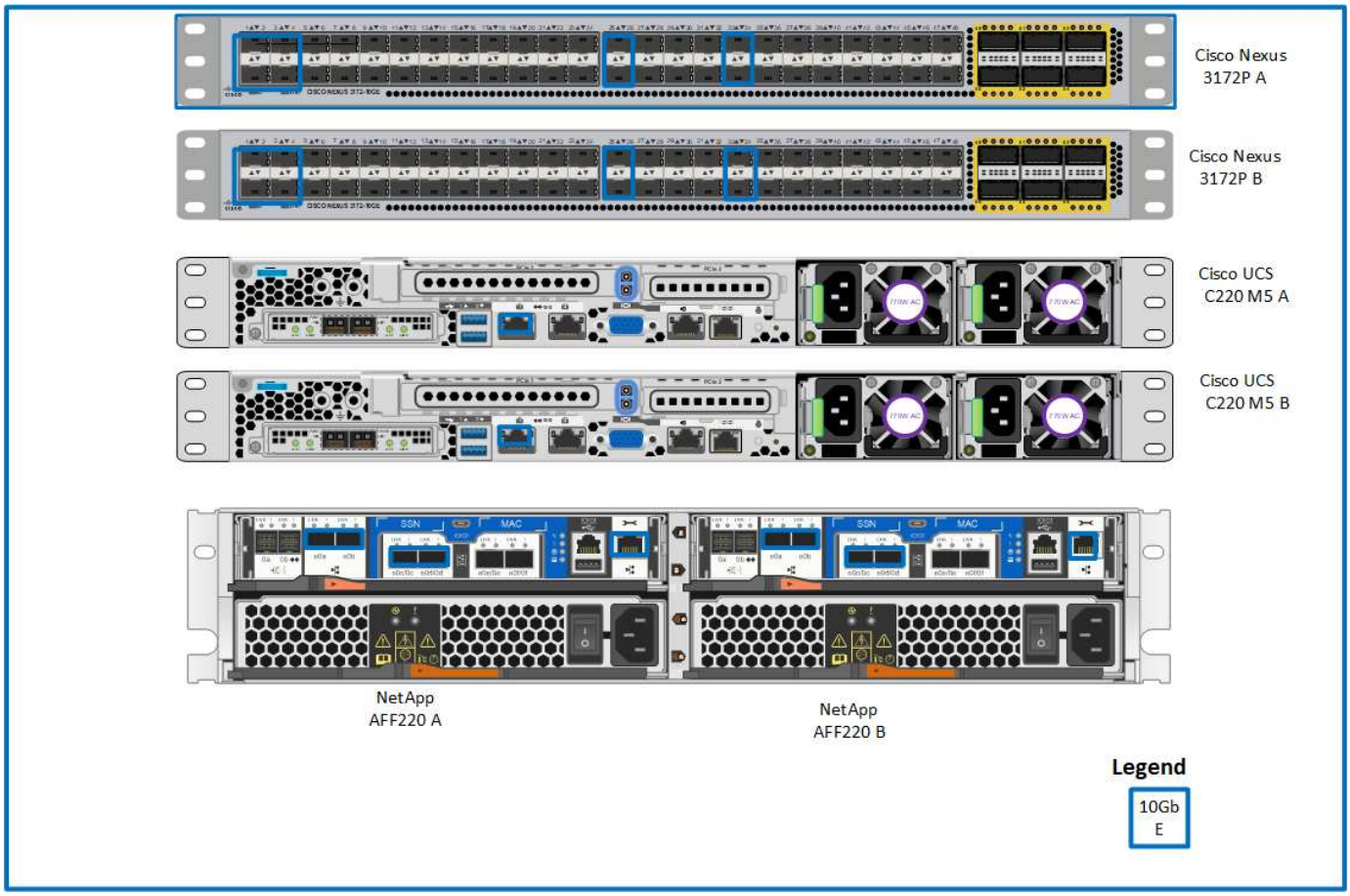
ソフトウェア	バージョン	詳細
Cisco Integrated Management Controller （ CIMC ）	3.1 （ 3G ）	Cisco UCS C220 M5 ラックサーバの場合
Cisco nenic ドライバ	1.0.25.0	VIC 1387 インターフェイスカード用
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Cisco Nexus 3172P スイッチの場合
NetApp ONTAP	9.4	AFF A220 コントローラの場合

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。

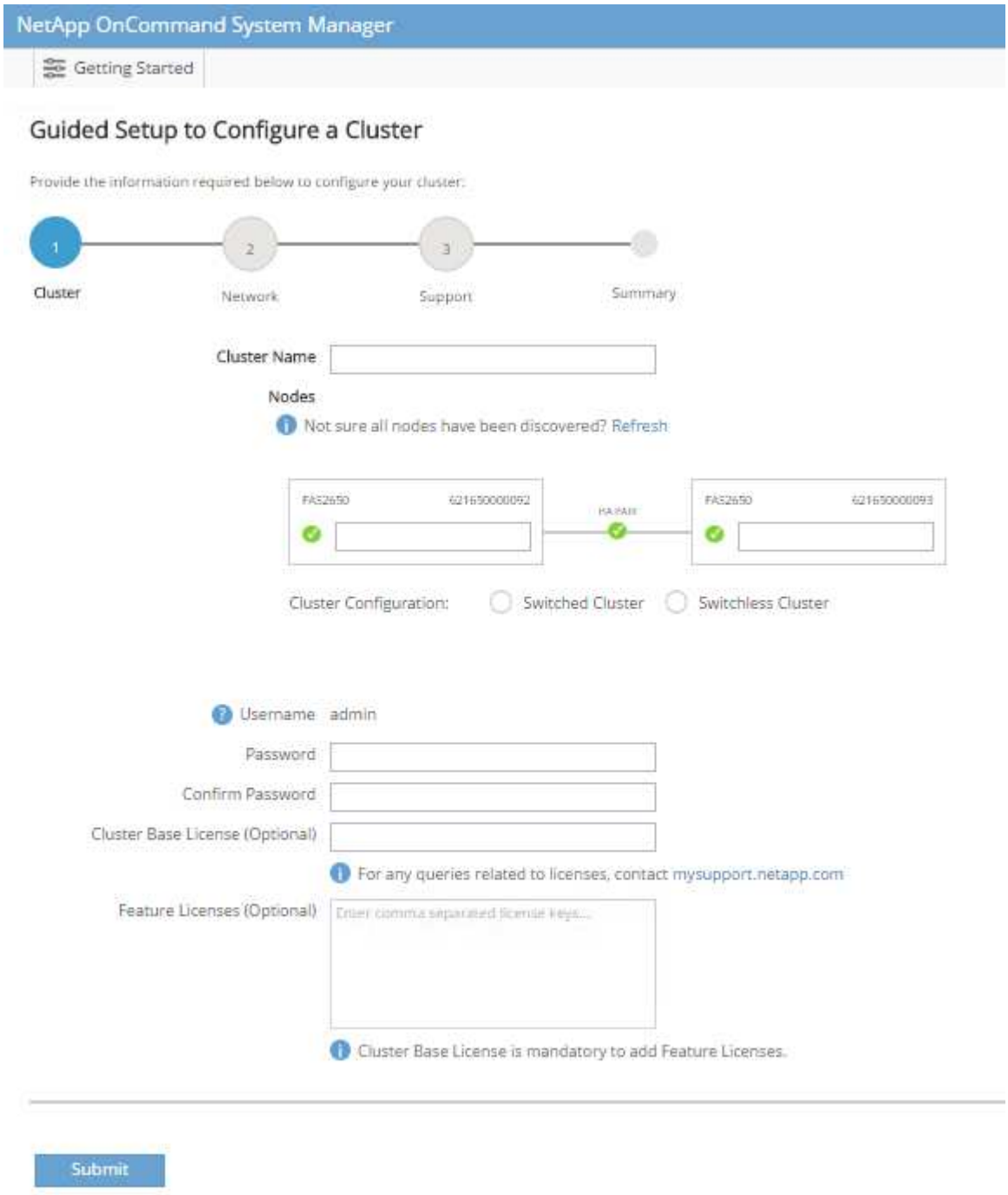
1. プロンプトに従ってノード A をセットアップします

```
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。

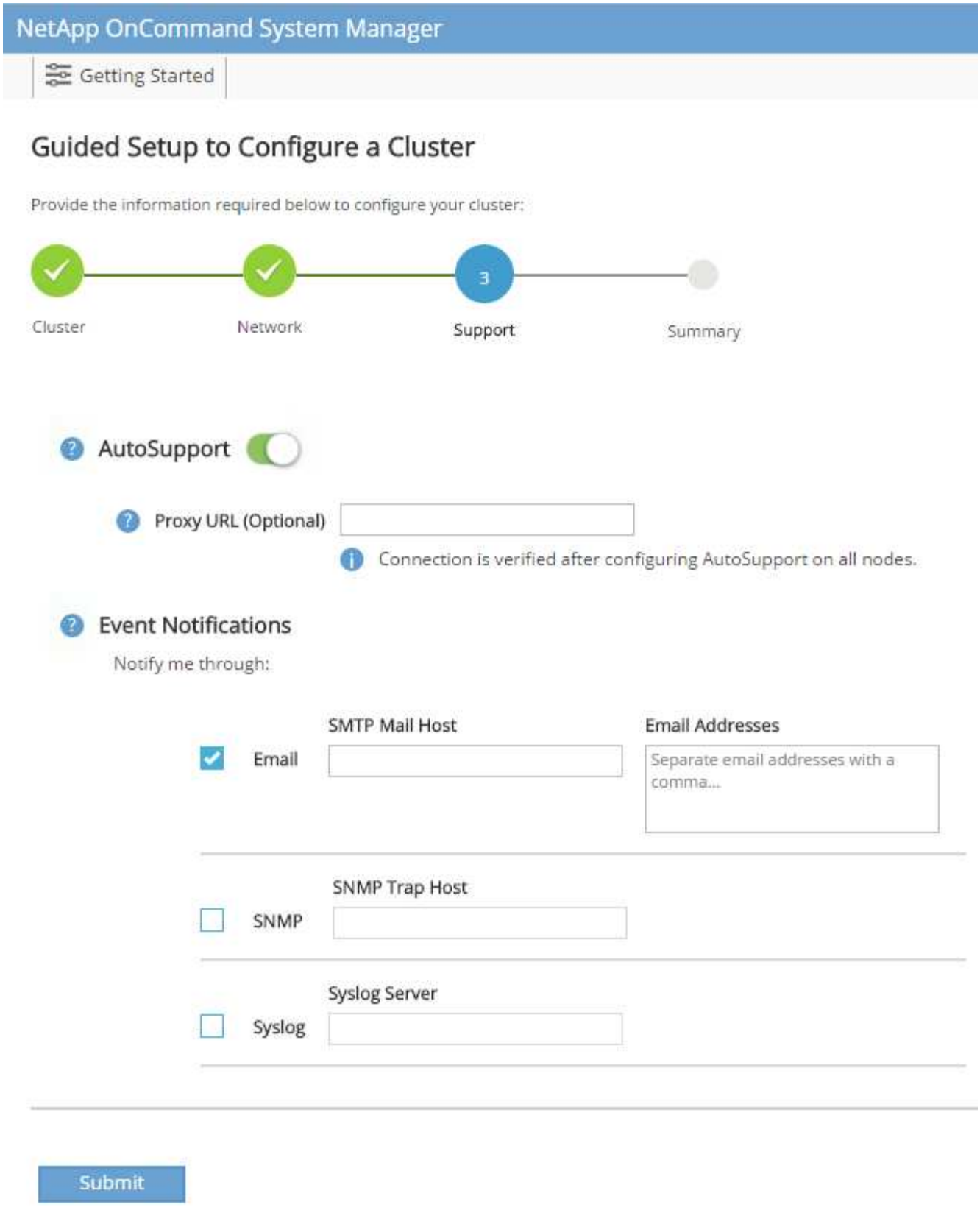
   代替 NTP サーバを入力することもできます。

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。

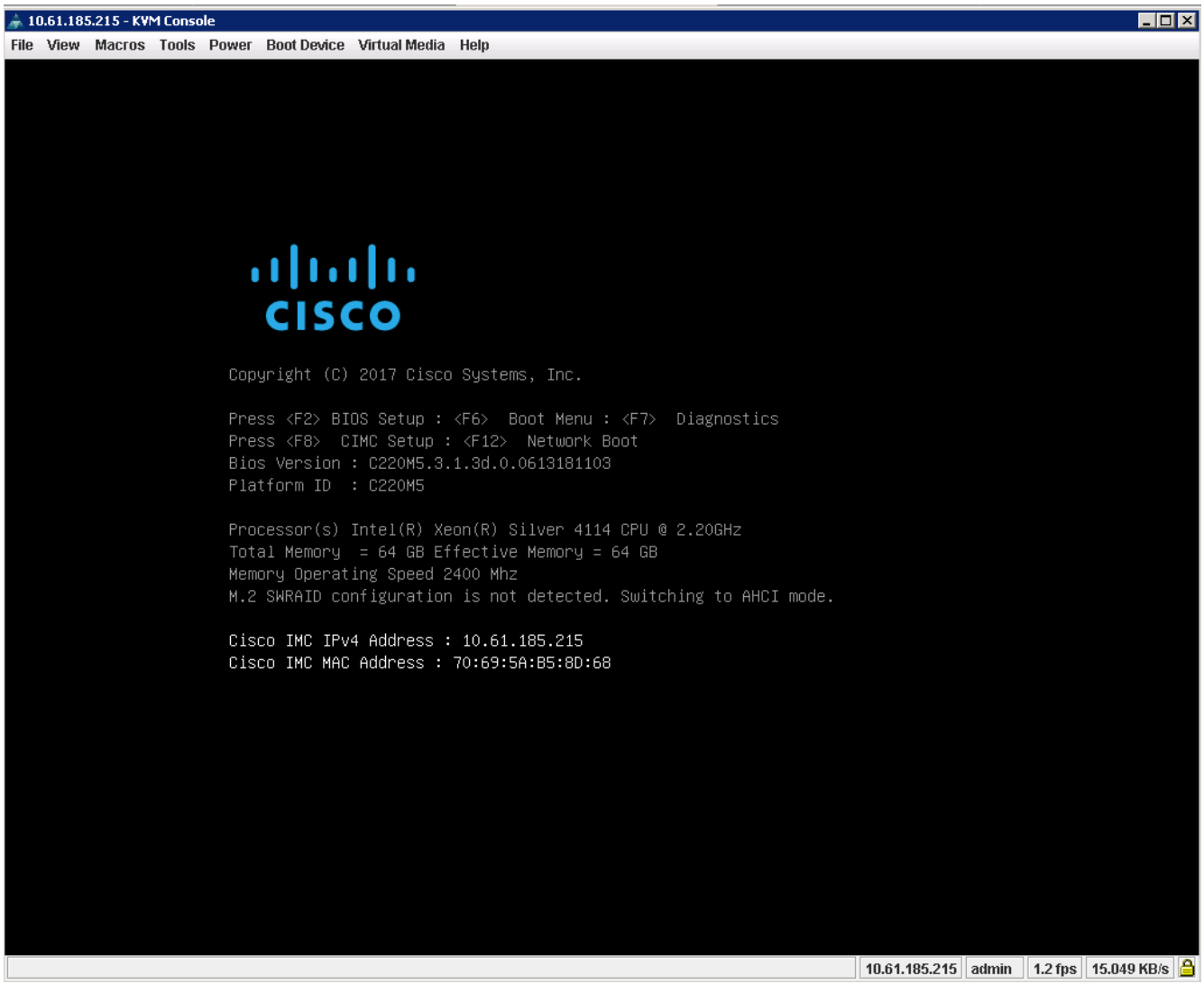
次の表に、 Cisco UCS C シリーズスタンドアロンサーバごとに CIMC を設定するために必要な情報を示します。

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

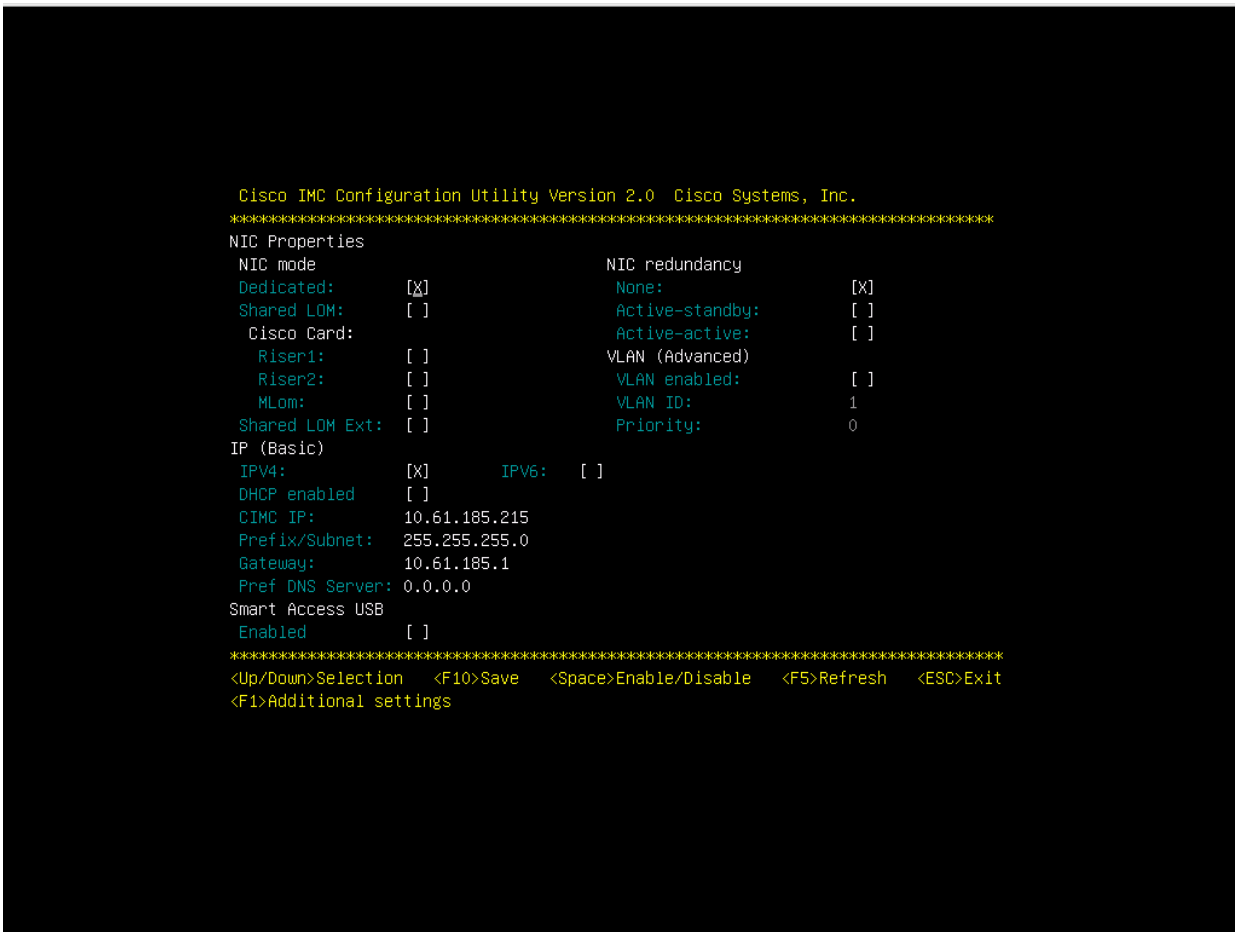
この検証で使用されている CIMC バージョンは、 CIMC 3.1.3 （ g ）です。

すべてのサーバ

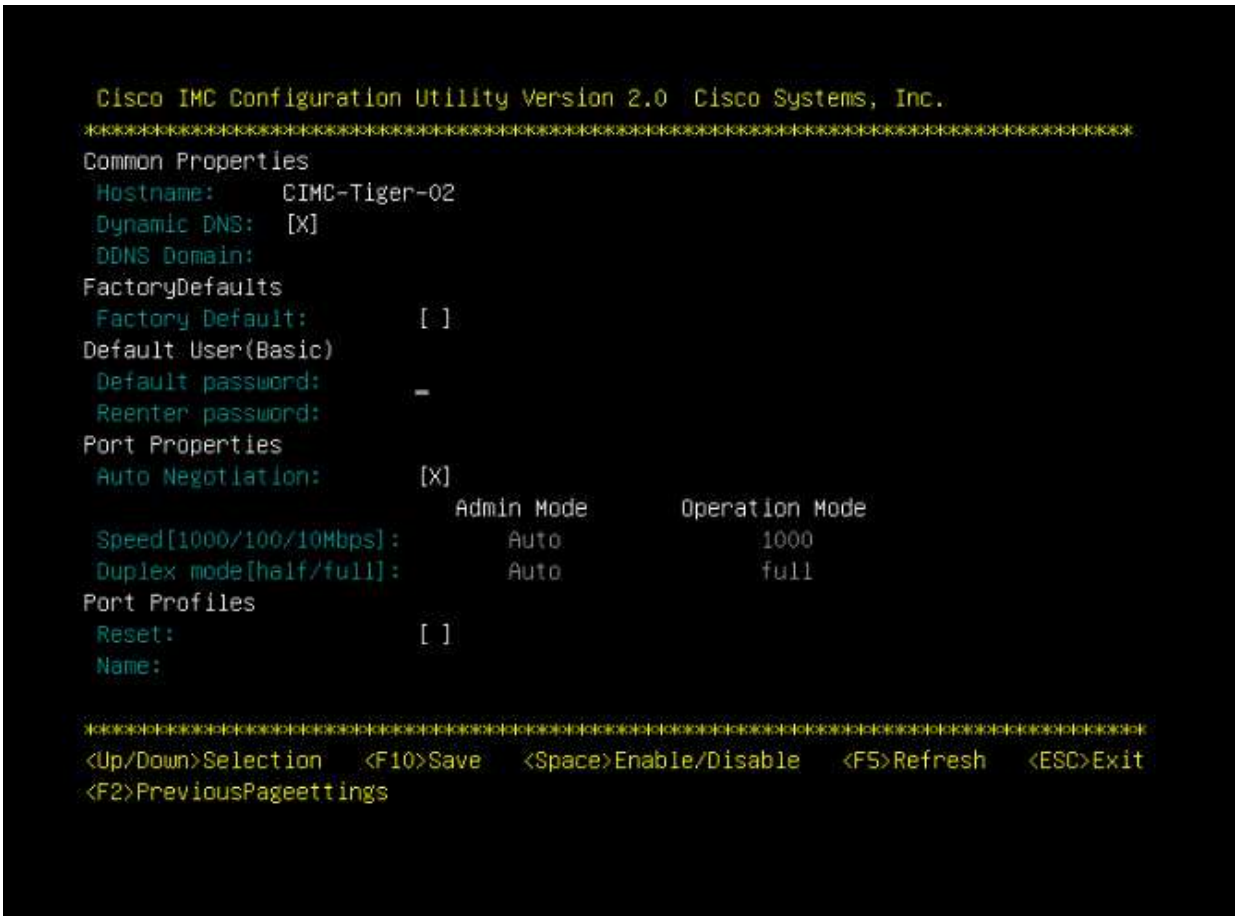
1. Cisco KVM （キーボード、ビデオ、およびマウス）ドングル（サーバに付属）を、サーバ前面の KVM ポートに取り付けます。VGA モニタと USB キーボードを、 KVM ドングルの対応するポートに接続します。
2. サーバの電源を入れ、 CIMC 設定を開始するかどうか確認するプロンプトが表示されたら F8 キーを押します。



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。

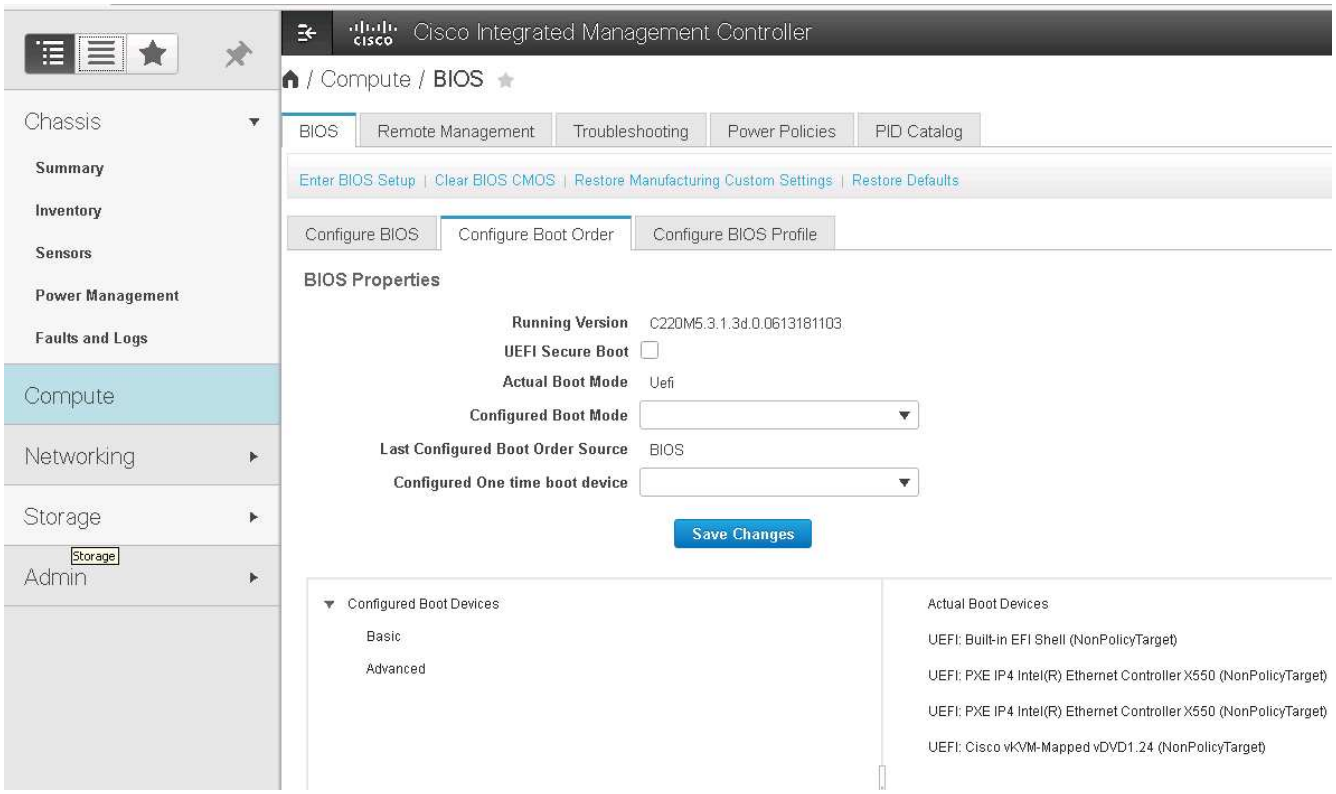
詳細（ **Detail** ）	詳細値
ESXi ホストイニシエータの名前	<<var_UCS_initiator_name_a>> を参照してください
ESXi ホスト iSCSI-A IP	<<var_esxi_host_iscsia_ip>>
ESXi ホスト iSCSI - ネットワークマスク	<<var_esxi_host_iscsia_mask>> を指定します
ESXi ホスト iSCSI A のデフォルトゲートウェイ	<<var_esxi_host_iscsia_gateway>> を指定します
ESXi ホストイニシエータ B の名前	<<var_UCS_initiator_name_b>> 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。

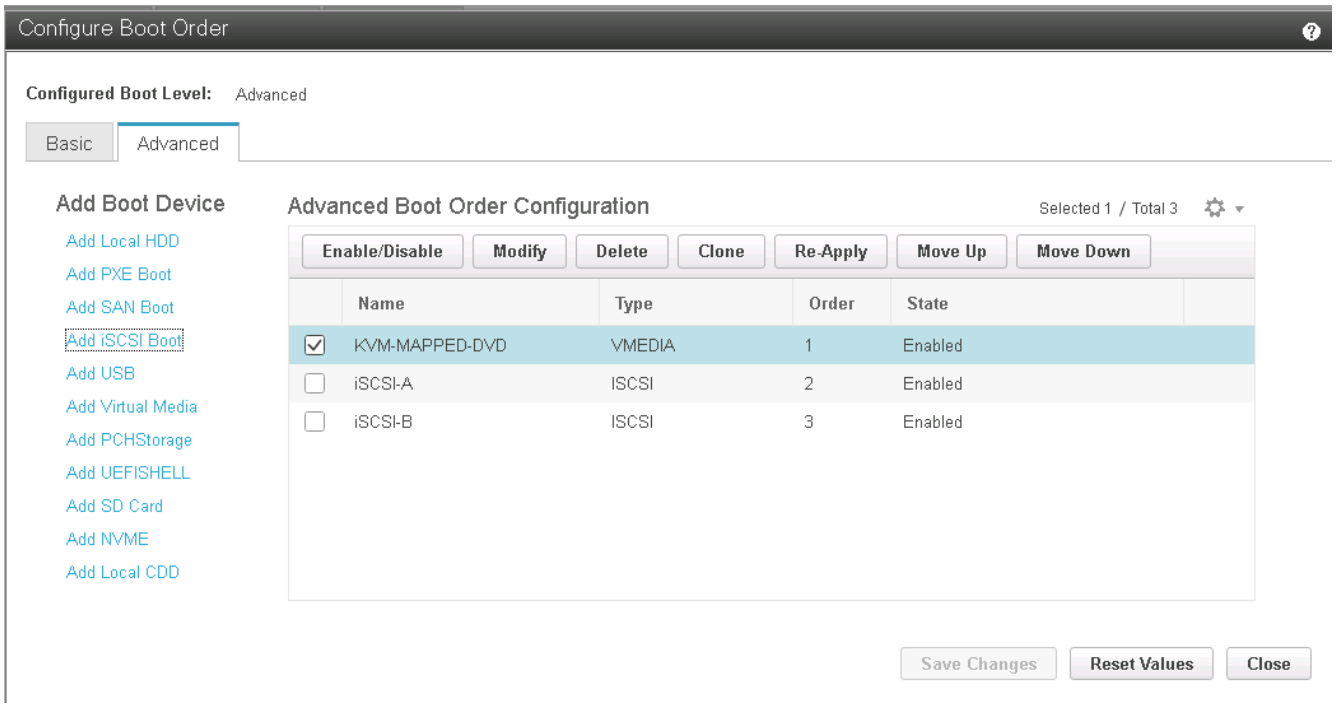
1. CIMC インターフェイスのブラウザウィンドウで、 [Server （サーバ）] タブをクリックし、 [BIOS （ BIOS ）] を選択します。
2. Configure Boot Order （起動順序の設定）をクリックし、 OK をクリックします。



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。



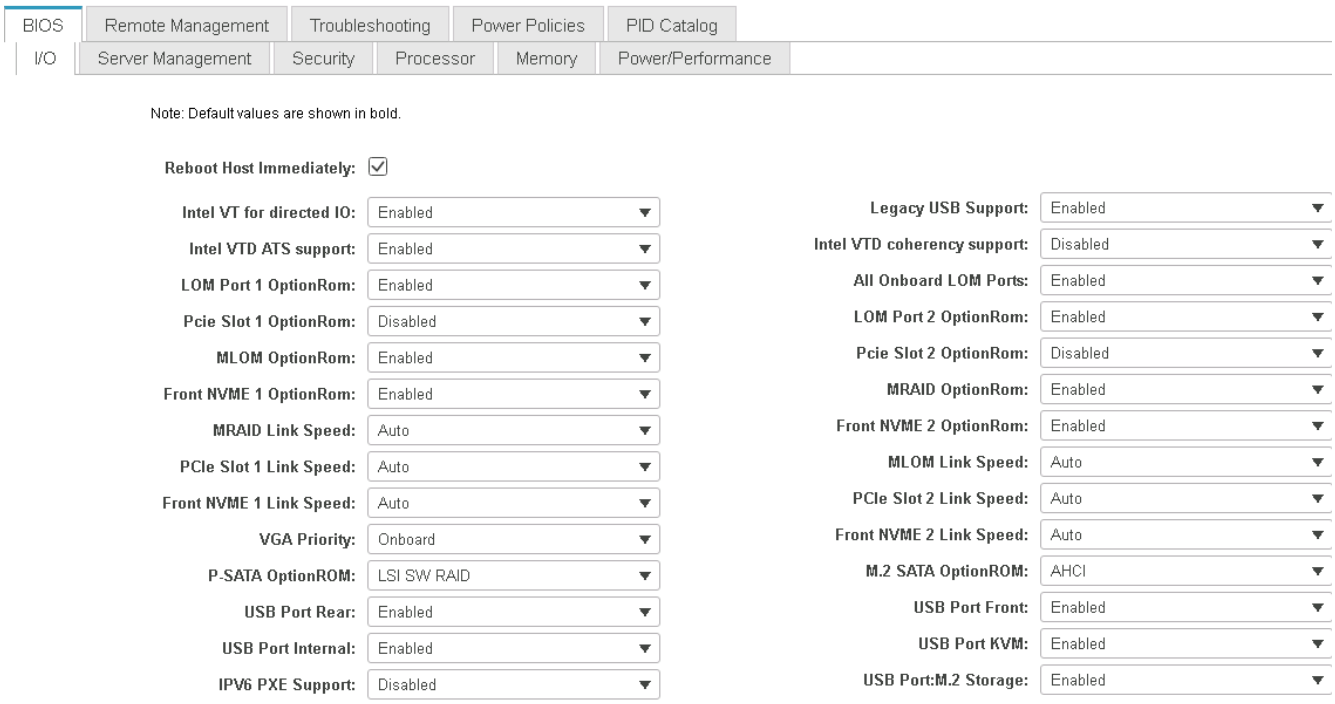
6. サーバをリブートして、新しいブート順序でブートします。

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。



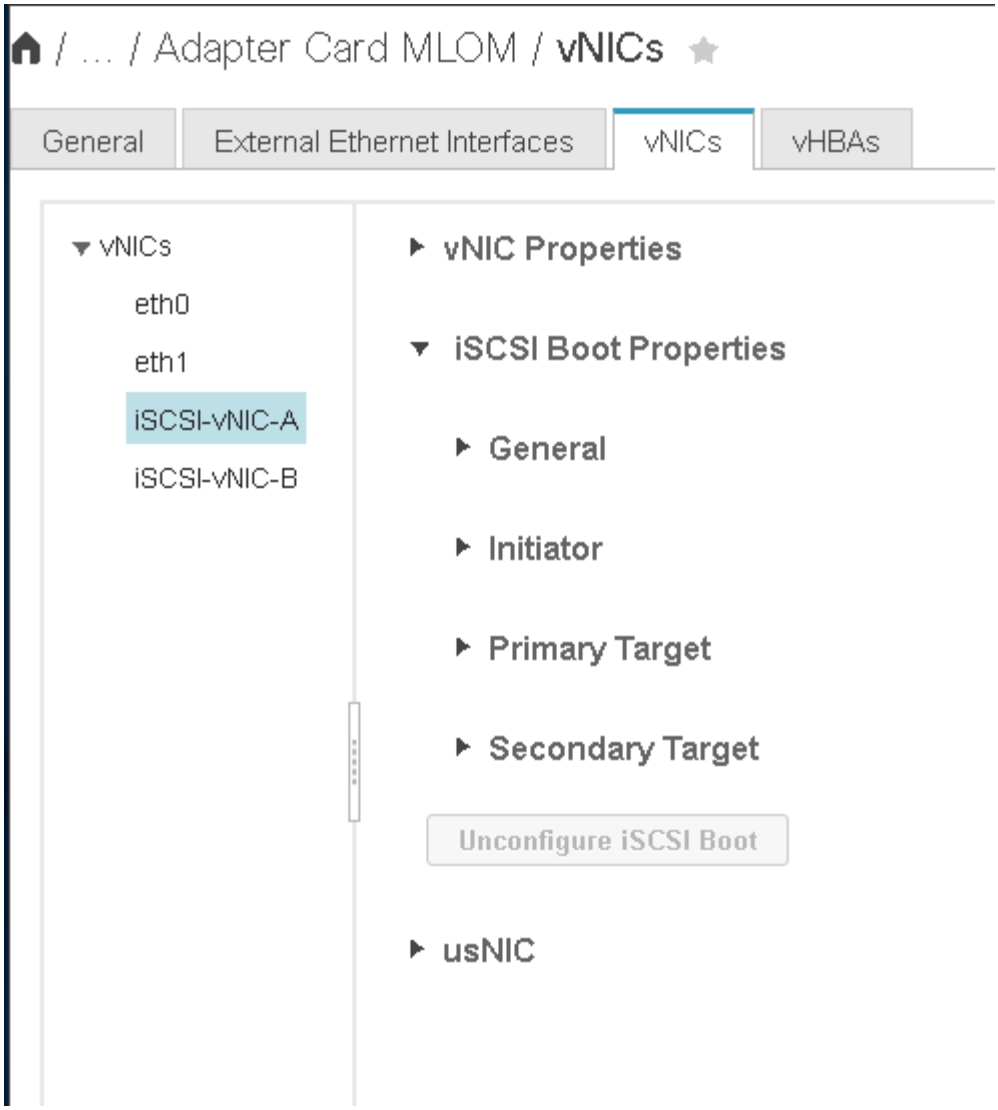
iSCSI ブート用に Cisco VIC1387 を設定します

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。

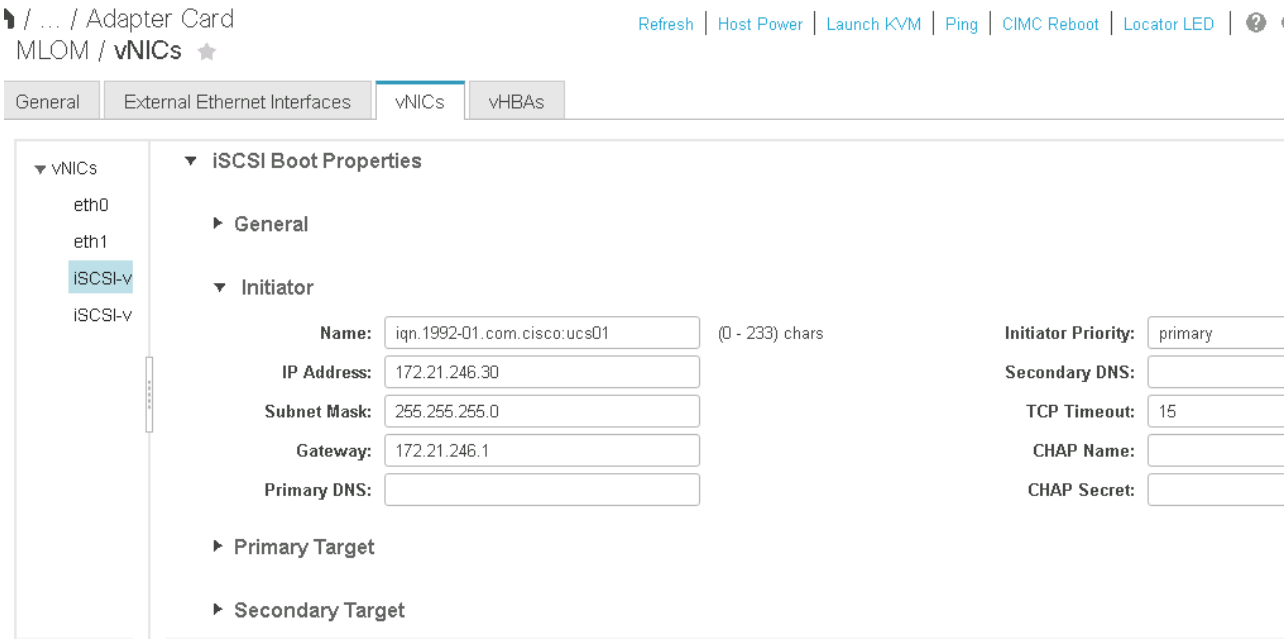
iSCSI vNIC を作成します

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。



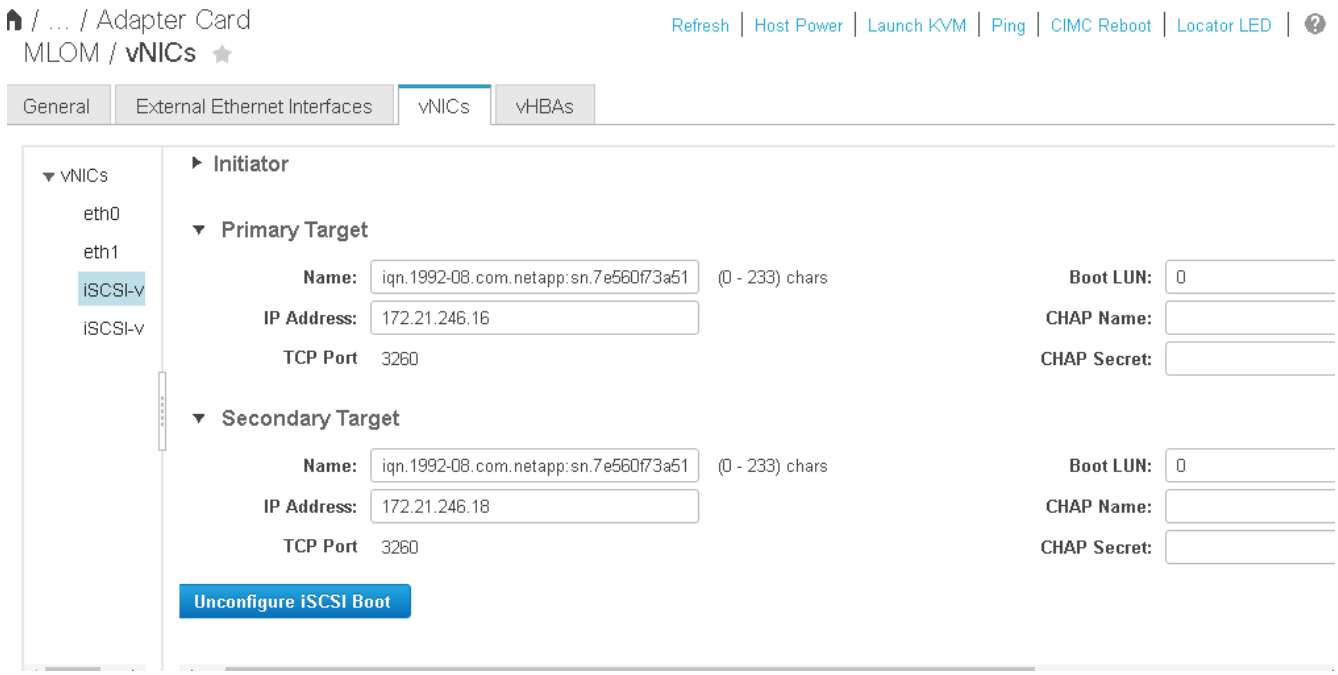
6. iSCSI Boot Properties （iSCSI 起動プロパティ）で、イニシエータの詳細を入力します。
   - 名前： <<var_ucsa_initiator_name_a>>
   - IP アドレス： <<var_esxi_hosta_iscsia_ip>>
   - サブネットマスク： <<var_esxi_hosta_iscsia_mask>>
   - ゲートウェイ： <<var_esxi_hosta_iscsia_gateway>>



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

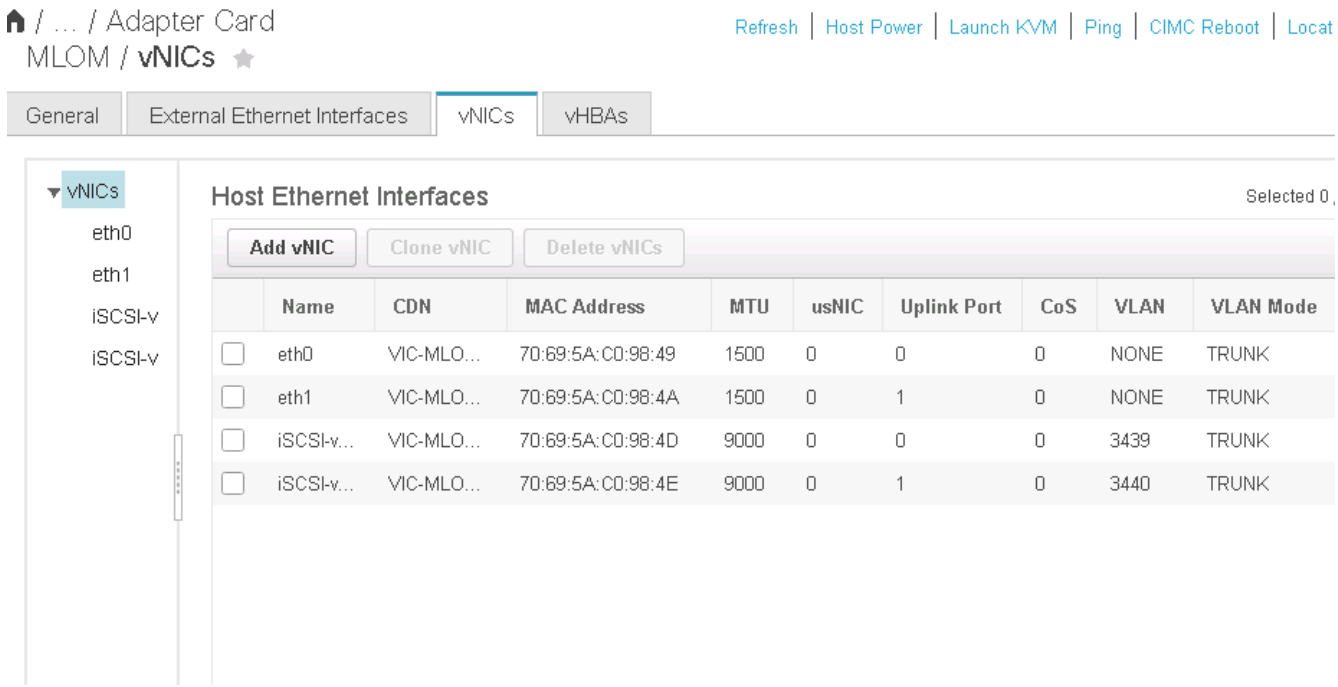
    ストレージ IQN 番号は、「 vserver iscsi show 」コマンドを使用して取得できます。

    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。

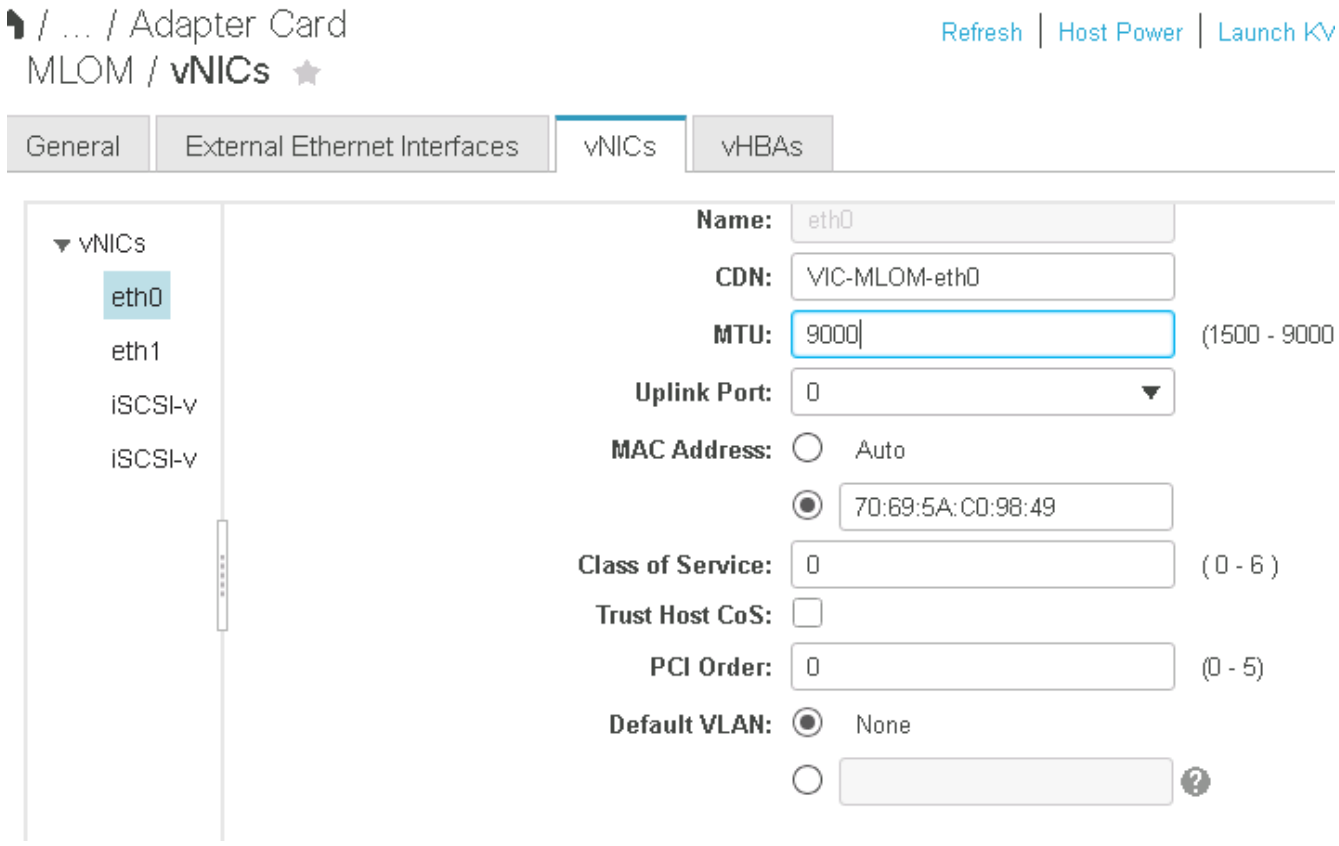
16. このプロセスを繰り返して、 Cisco UCS サーバ B の iSCSI ブートを設定します

ESXi の **vNIC** を設定します

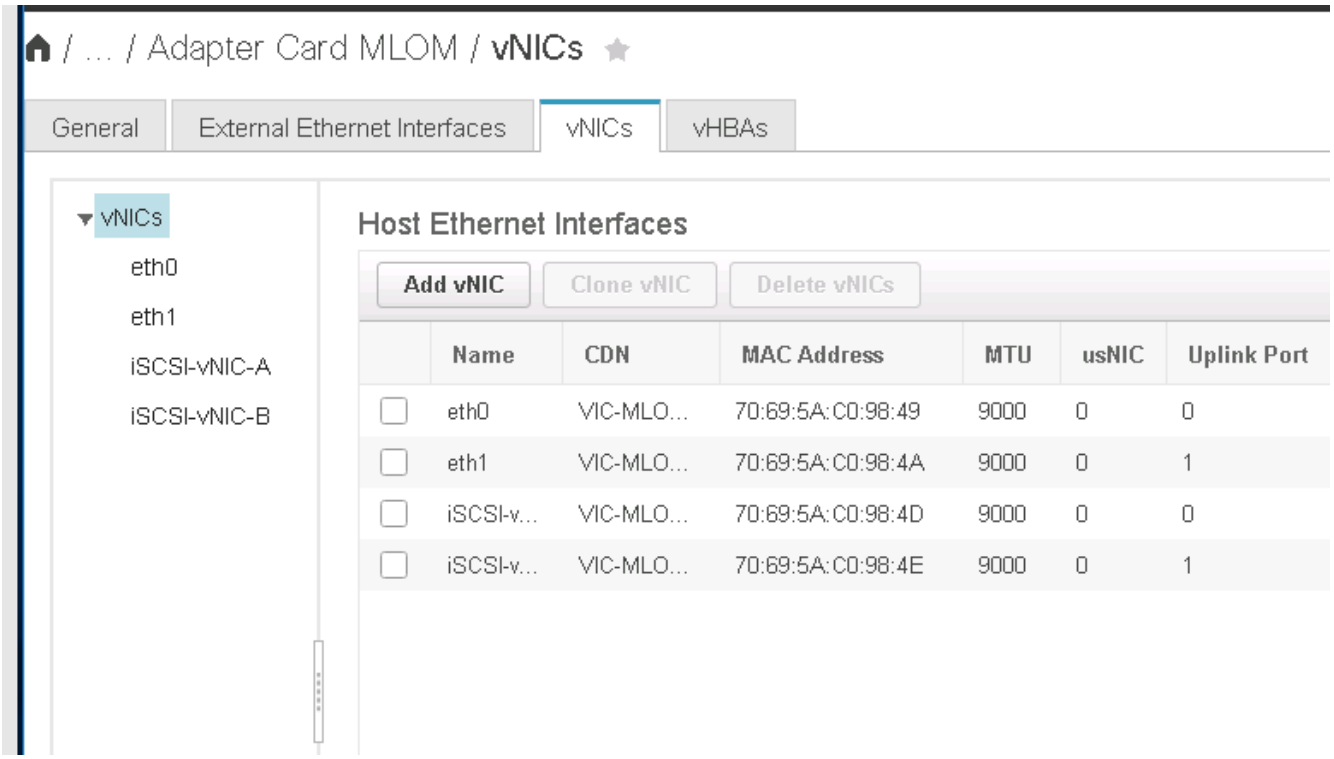
1. CIMC インターフェイスブラウザウィンドウで、 [Inventory] をクリックし、右側のペインで [Cisco VIC adapters] をクリックします。
2. [アダプタカード] で、 [Cisco UCS VIC 1387] を選択し、その下の vNIC を選択します。



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

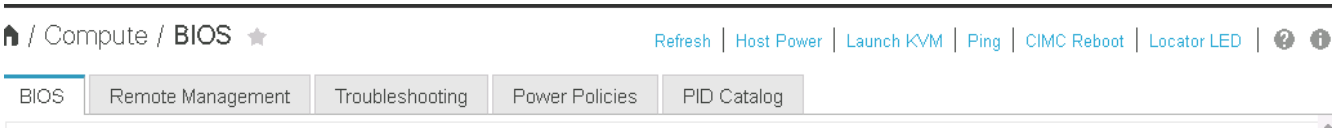
クラスタに追加するノードに対してこの手順を完了しておく必要があります。

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。

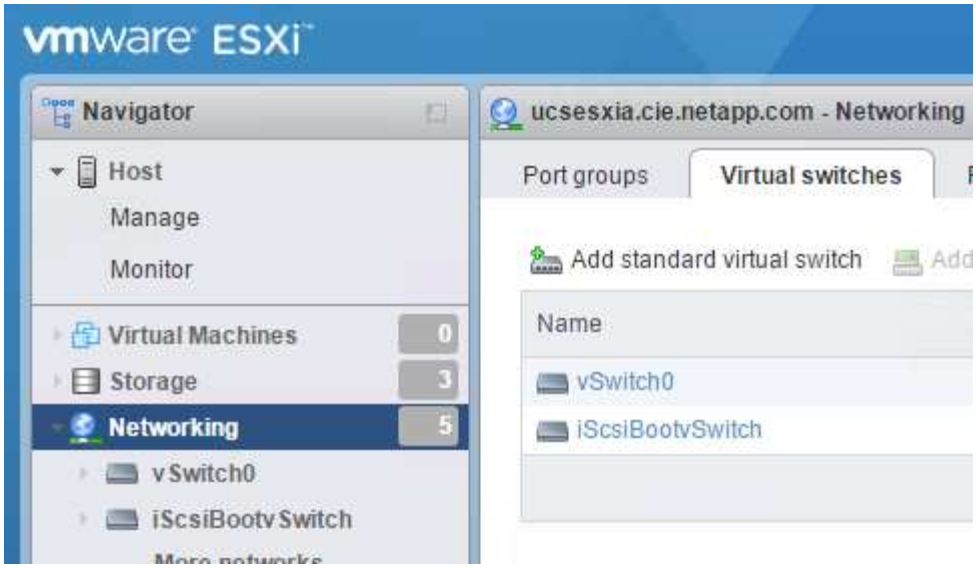
詳細（ **Detail** ）	価値
ESXi ホスト名	
ESXi ホスト管理 IP	
ESXi ホスト管理マスク	
ESXi ホスト管理ゲートウェイ	
ESXi ホストの NFS IP	
ESXi ホストの NFS マスク	
ESXi ホストの NFS ゲートウェイ	
ESXi ホスト vMotion IP	
ESXi ホストの vMotion マスク	
ESXi ホストの vMotion ゲートウェイ	
ESXi ホスト iSCSI-A IP	
ESXi ホスト iSCSI-A マスク	
ESXi ホスト iSCSI-A ゲートウェイ	
ESXi ホスト iSCSI-B IP	
ESXi 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。

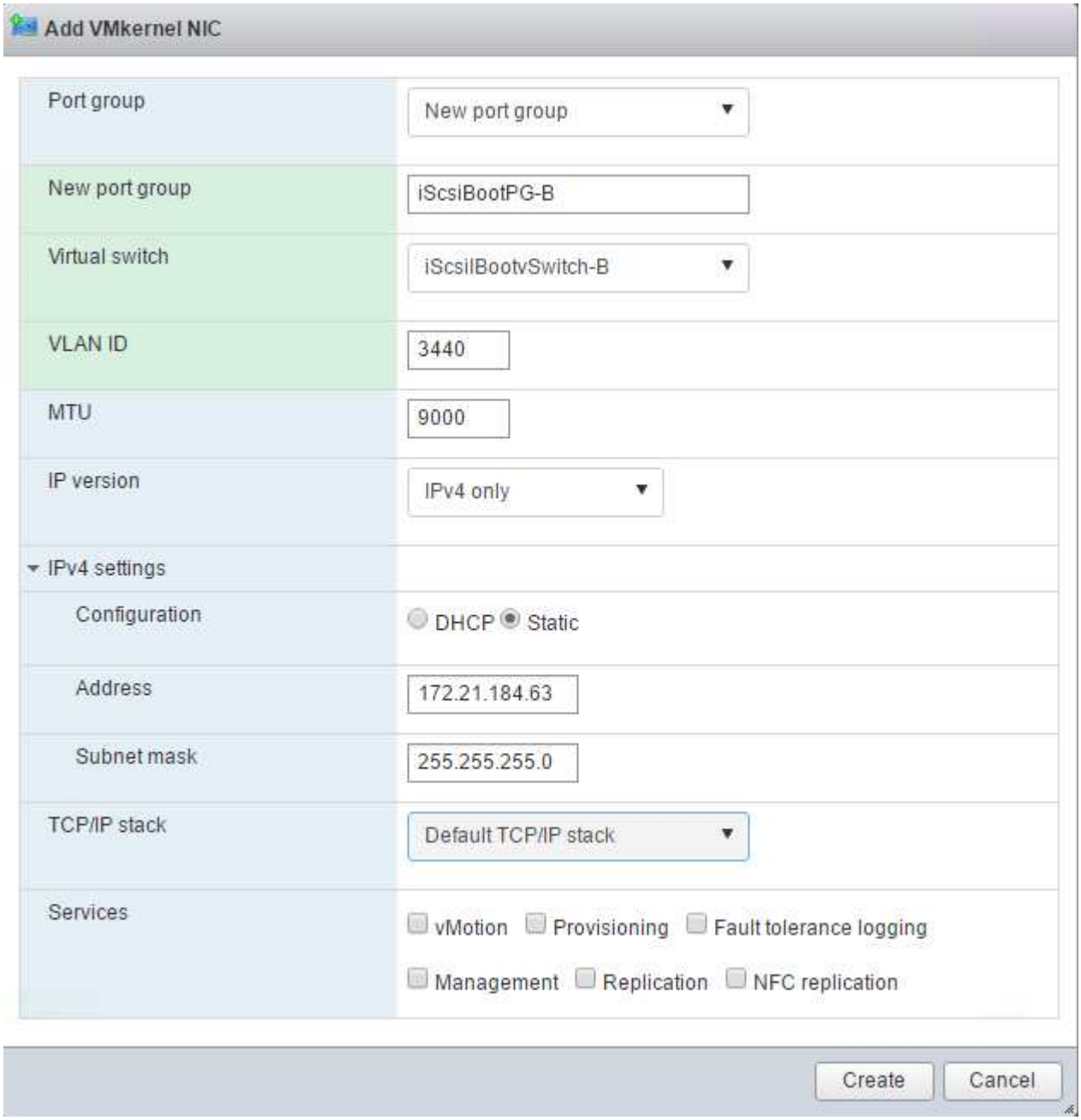


3. iScsiBootvSwitch をクリックします。
4. [設定の編集] を選択します
5. MTU を 9000 に変更し、 [保存] をクリックします。
6. 左側のナビゲーションペインで Networking （ネットワーク）をクリックして、 Virtual Switches （仮想スイッチ）タブに戻ります。
7. Add Standard Virtual Switch をクリックします。
8. vSwitch 名に「 iScsiBootvSwitch -B 」という名前を付けます。
   - MTU を 9000 に設定します。
   - アップリンク 1 のオプションから vmnic3 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。 .

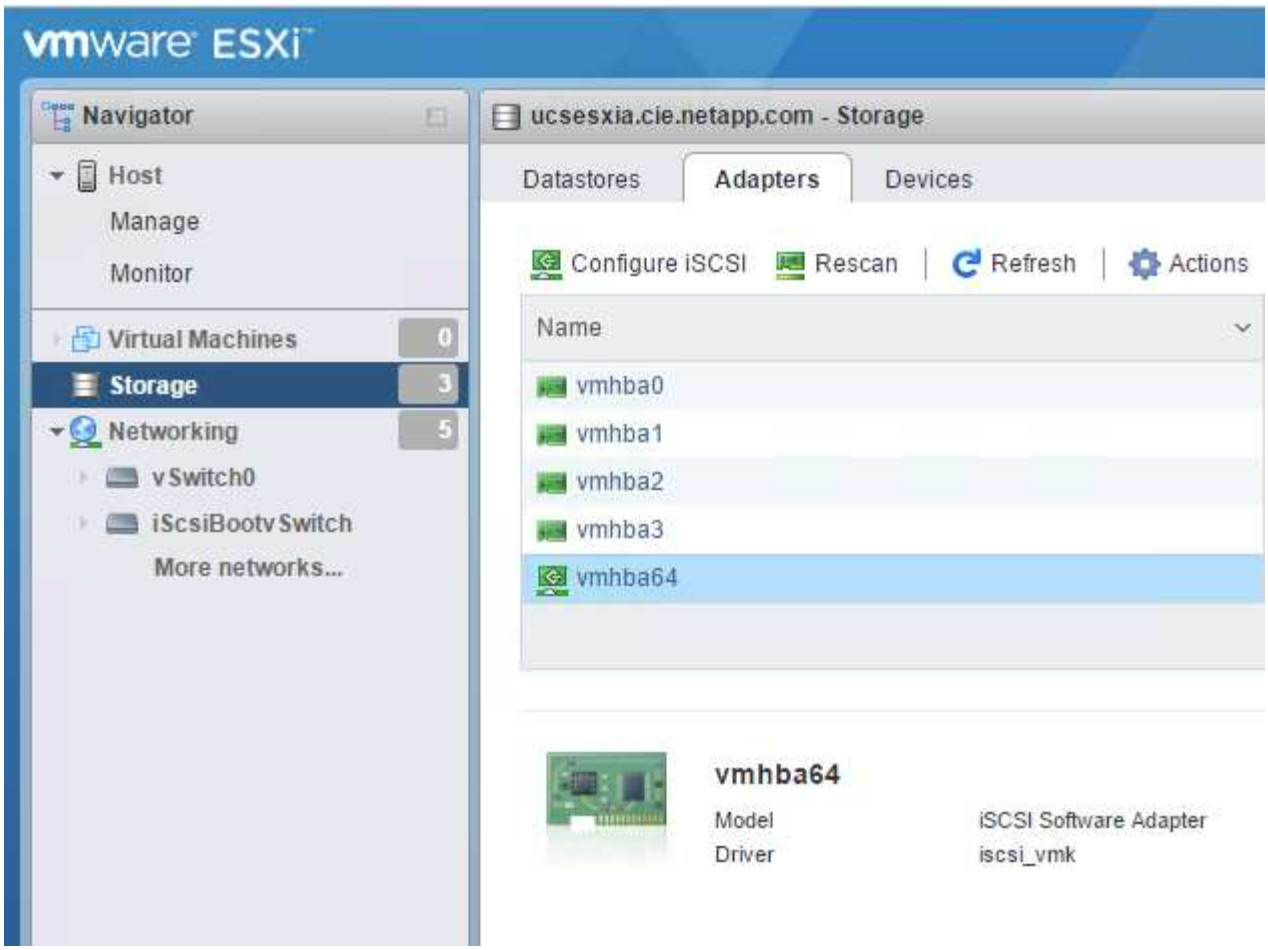


「 iScsiBootPG-A 」で MTU を 9000 に設定します

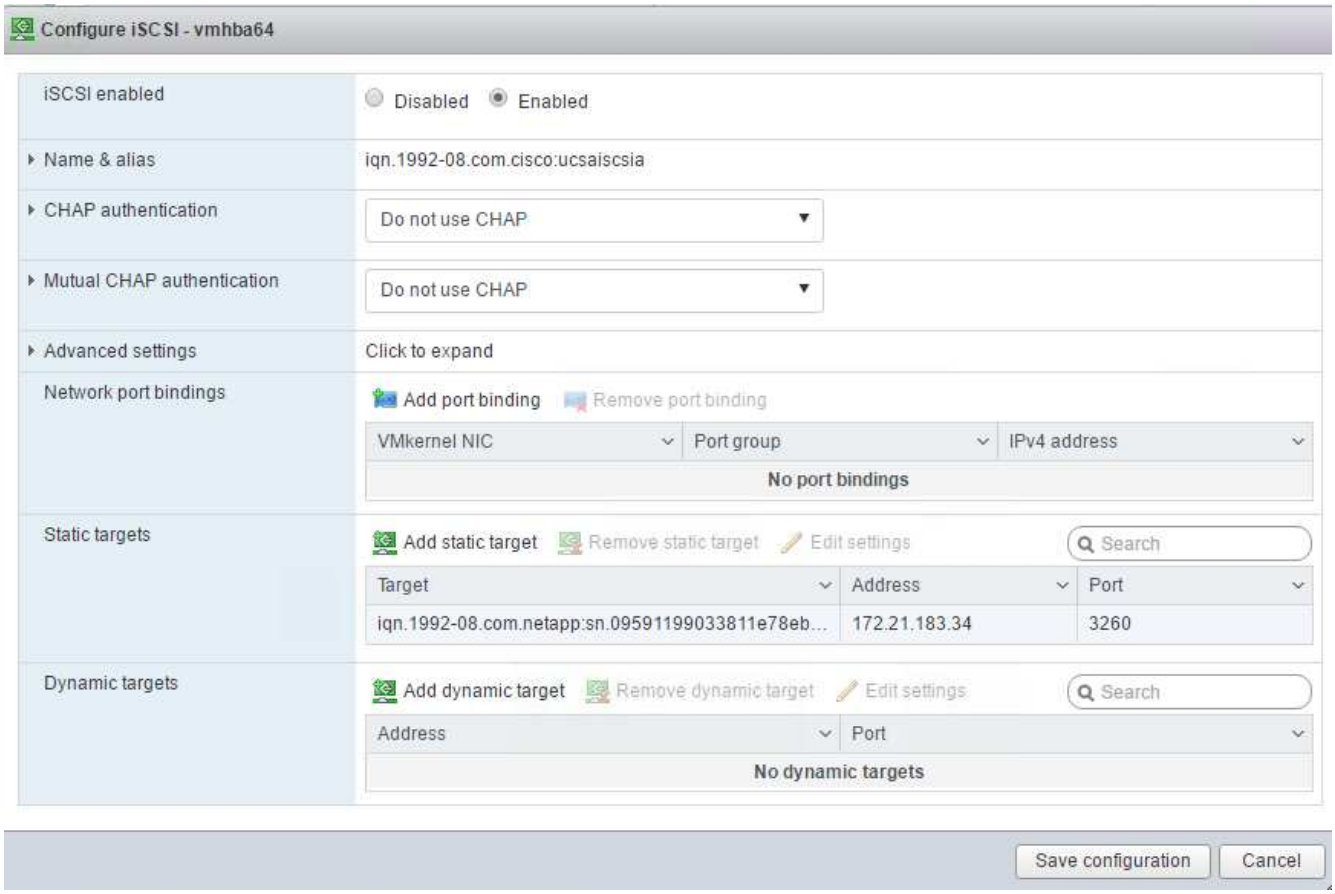
iSCSI マルチパスを設定します

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。

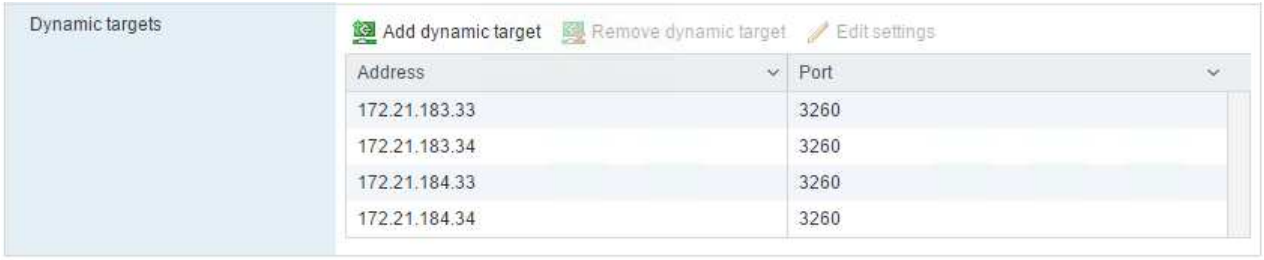
1. 左側のナビゲーションペインで Storage （ストレージ）を選択します。アダプタをクリックします。
2. iSCSI ソフトウェアアダプタを選択し、 Configure iSCSI （ iSCSI の設定）をクリックします。



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。



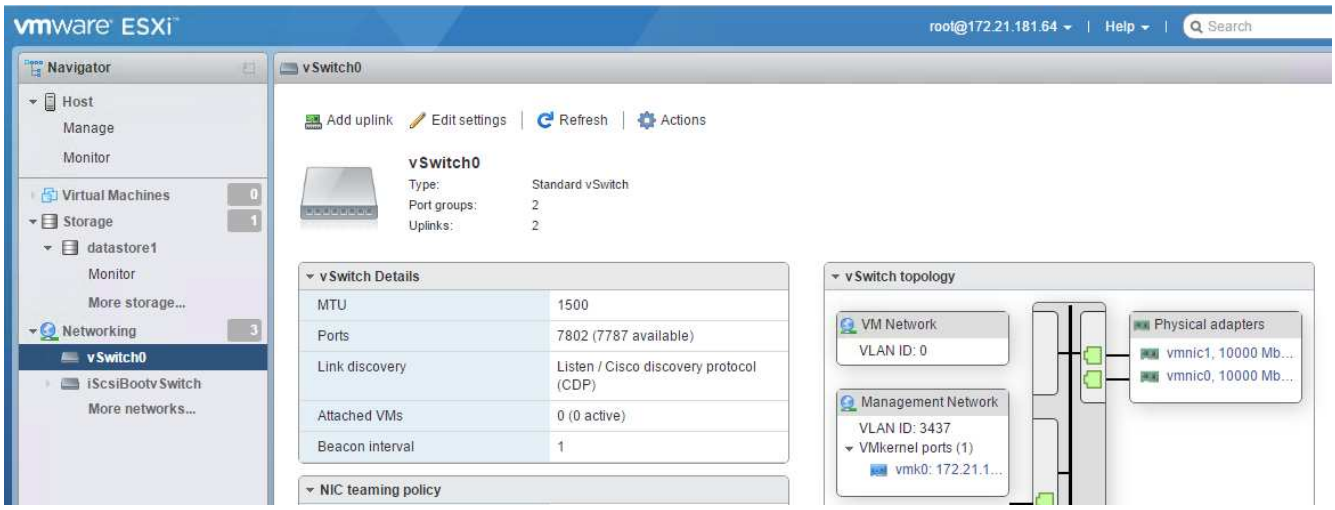
4. IP アドレス「 iscsi_dlif01a 」を入力します。
   - IP アドレス 'iSCSI_lif01b’iSCSI_lif02a’iSCSI_lif02b' で繰り返します
   - [Save Configuration] をクリックします。



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。

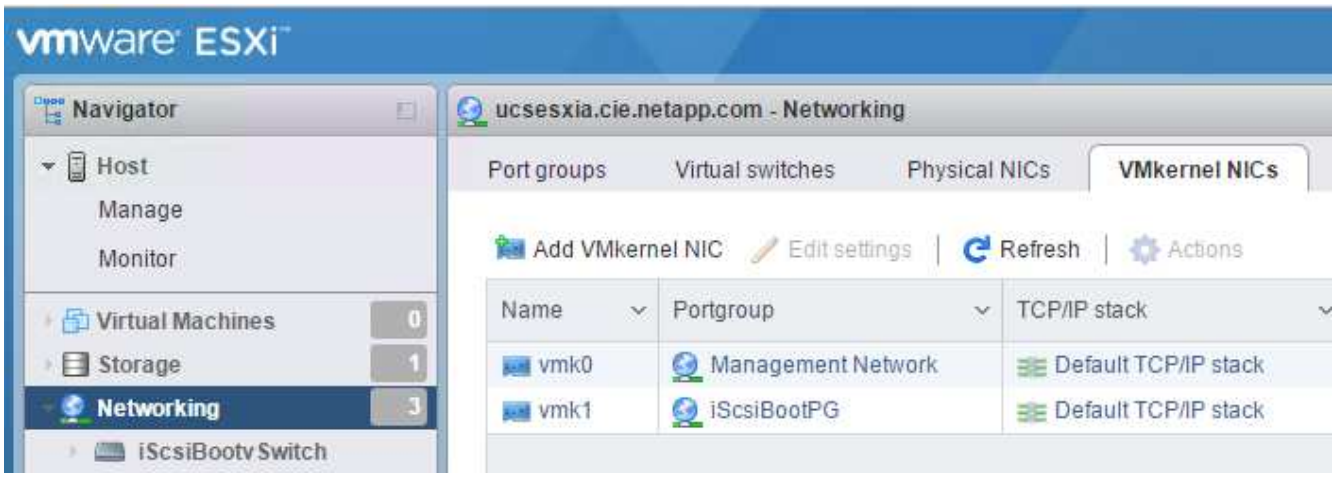
ポートグループと **VMkernel NIC** を設定します

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。

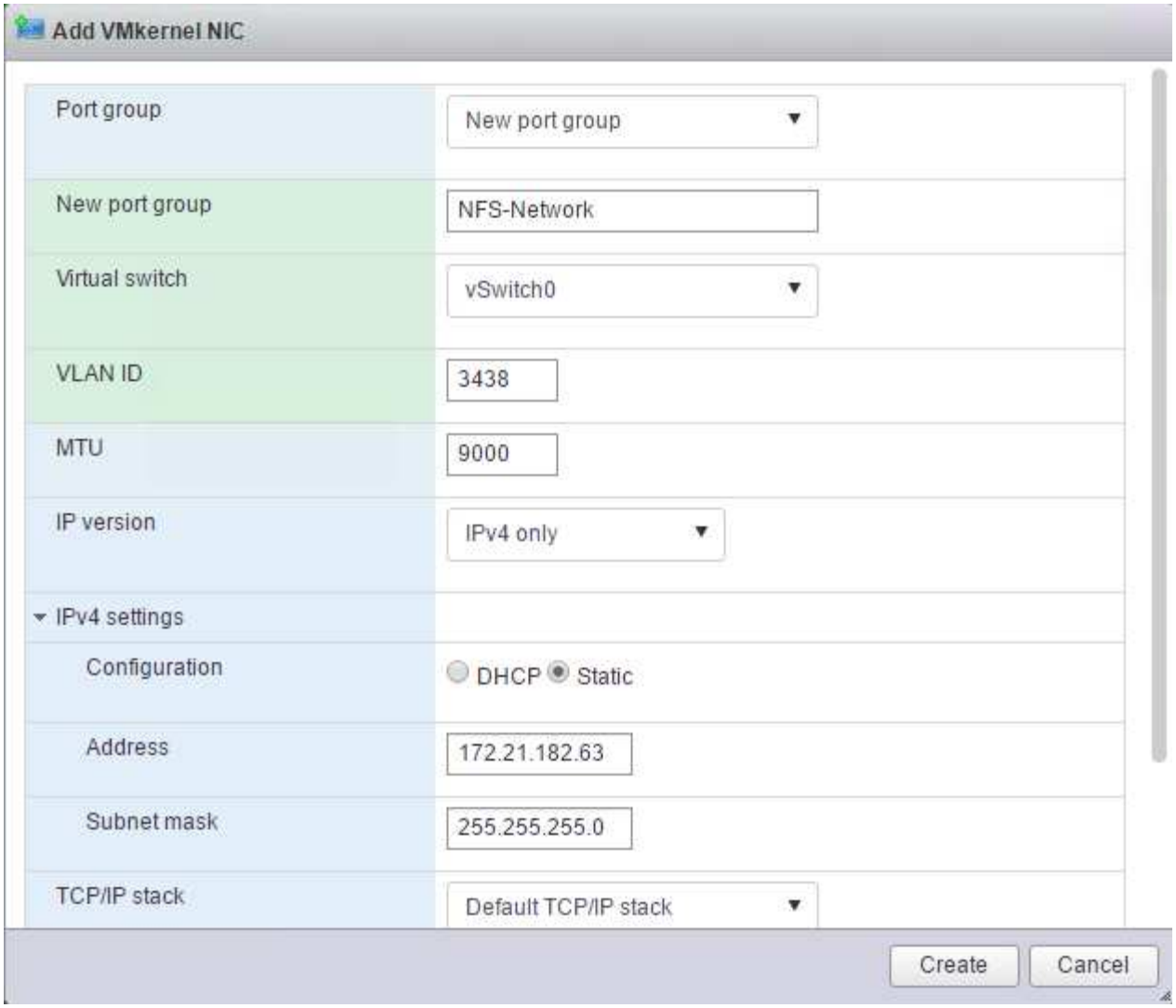
3. [VM Network] を右クリックし、 [Edit] を選択します。VLAN ID を「 <<var_vm_traffic_vlan>> 」に変更します。
4. [Add Port Group] をクリックします。
   - ポートグループに「 MGMT-Network 」という名前を付けます。
   - VLAN ID に「 \ <mgmt_vlan>> 」と入力します。
   - vSwitch0 が選択されていることを確認してください。

◦ 追加をクリックします。

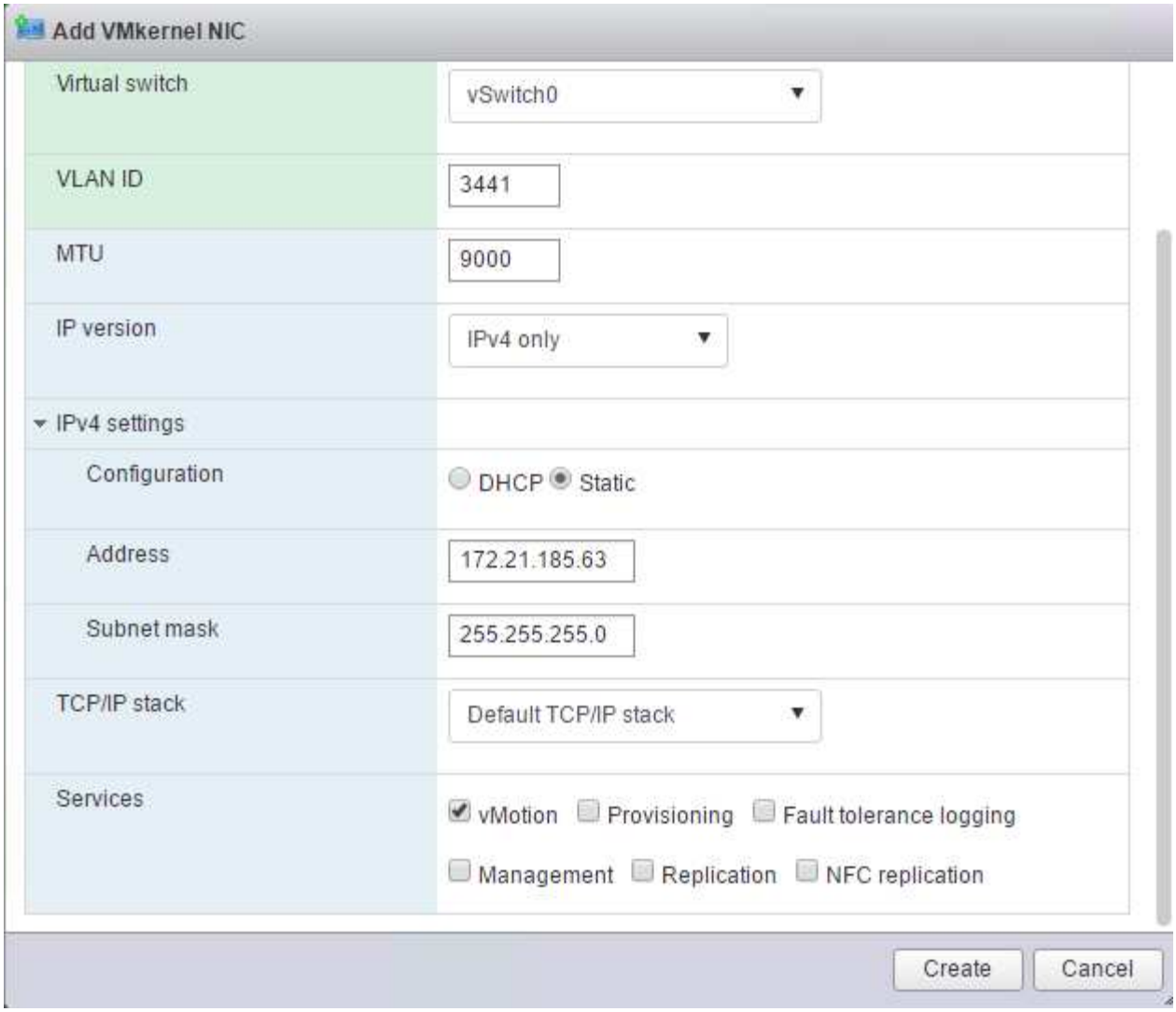
5. [VMkernel NICs] タブをクリックします。



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。

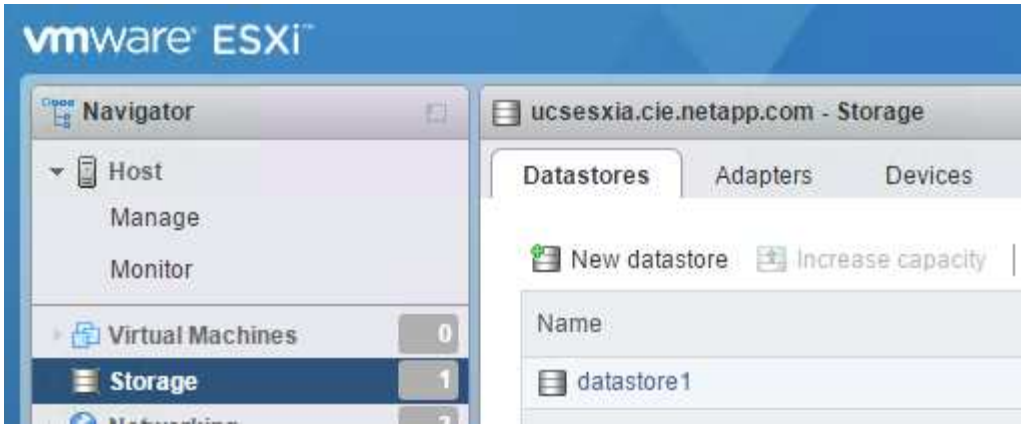


ESXi ネットワークの設定には、ライセンスで許可されている場合に VMware vSphere Distributed Switch を使用するなどの方法が多数あります。ビジネス要件を満たす必要がある場合は、 FlexPod Express で代替ネットワーク構成がサポートされます。

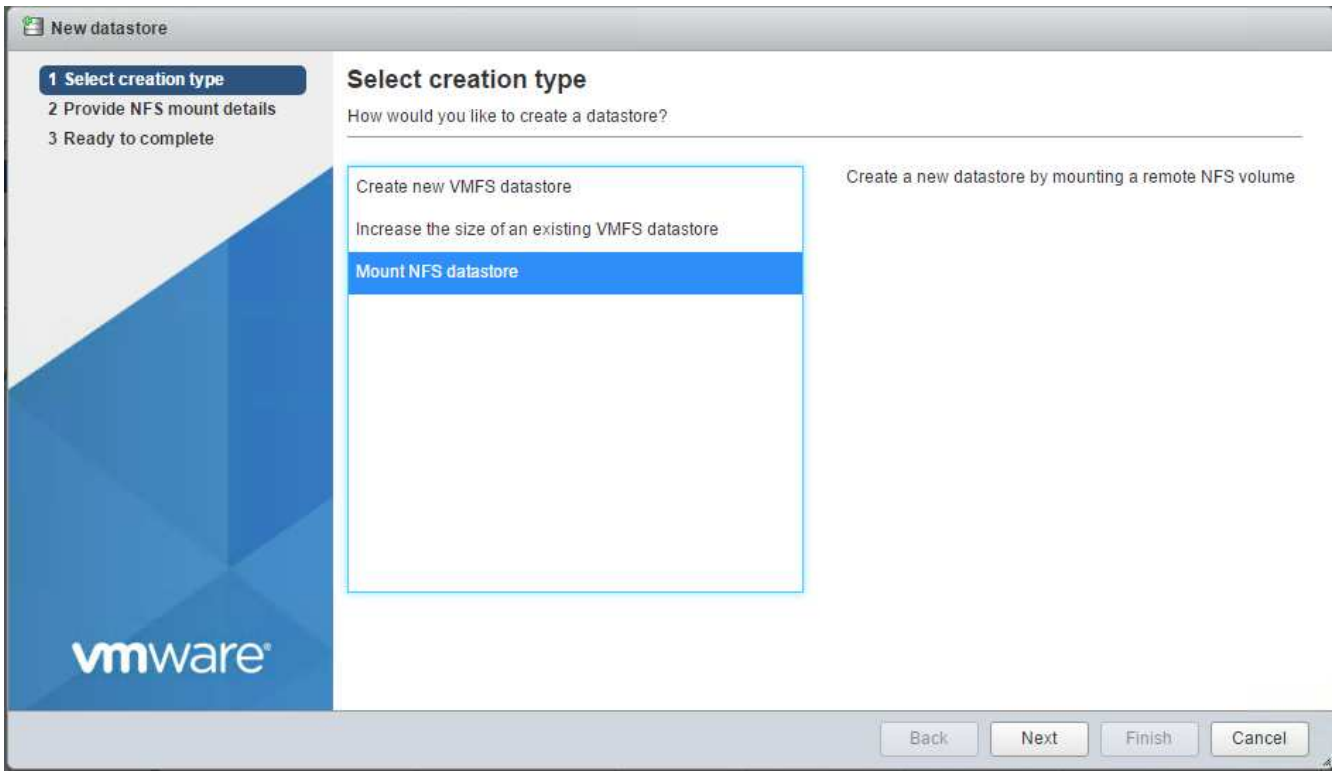
最初のデータストアをマウント

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。



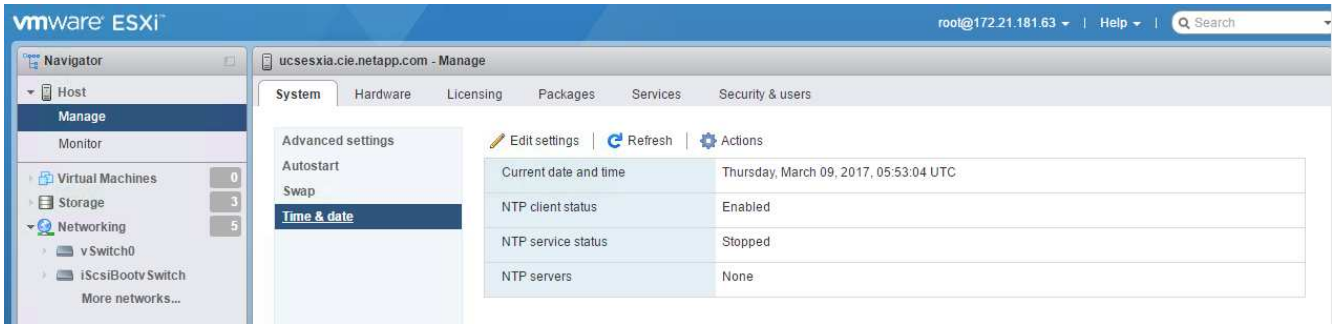
3. 次に、 Provide NFS Mount Details （ NFS マウントの詳細の提供）ページに次の情報を入力します。
   - 名前： 'infra_datastore_1'
   - NFS サーバ : `\<<var_nodeA_nfs_lif>`
   - 共有： /infra_datastor_1
   - NFS 3 が選択されていることを確認します。
4. 完了をクリックします。[最近のタスク] ペインにタスクの完了が表示されます。
5. 同じ手順で infra_swap データストアをマウントします。
   - 名前： infra_swap
   - NFS サーバ : `\<<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。

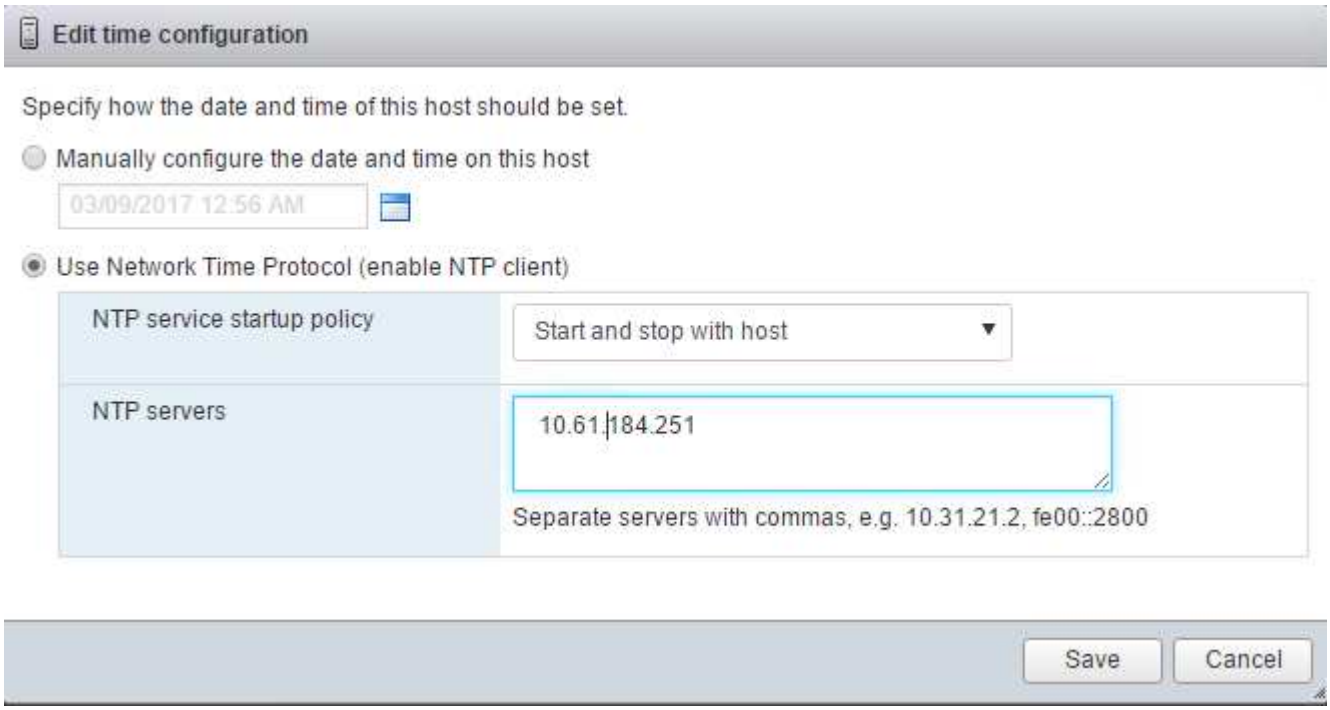
NTP を設定します

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 .

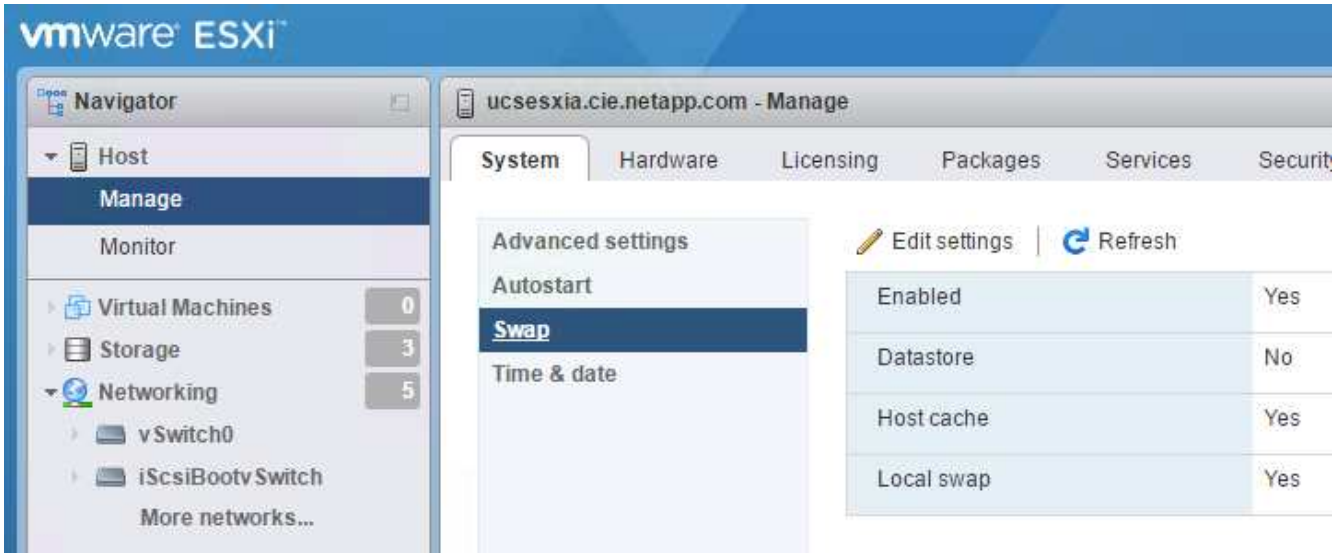


仮想マシンのスワップファイルの場所を移動します

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"

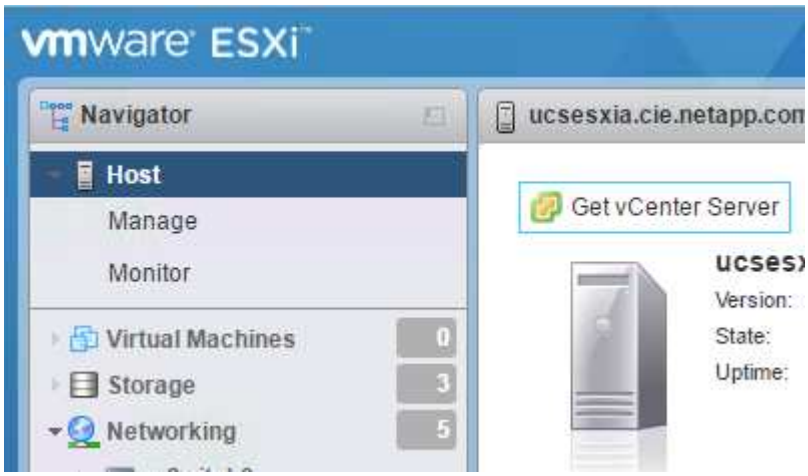
VMware vCenter Server 6.7 をインストールする

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

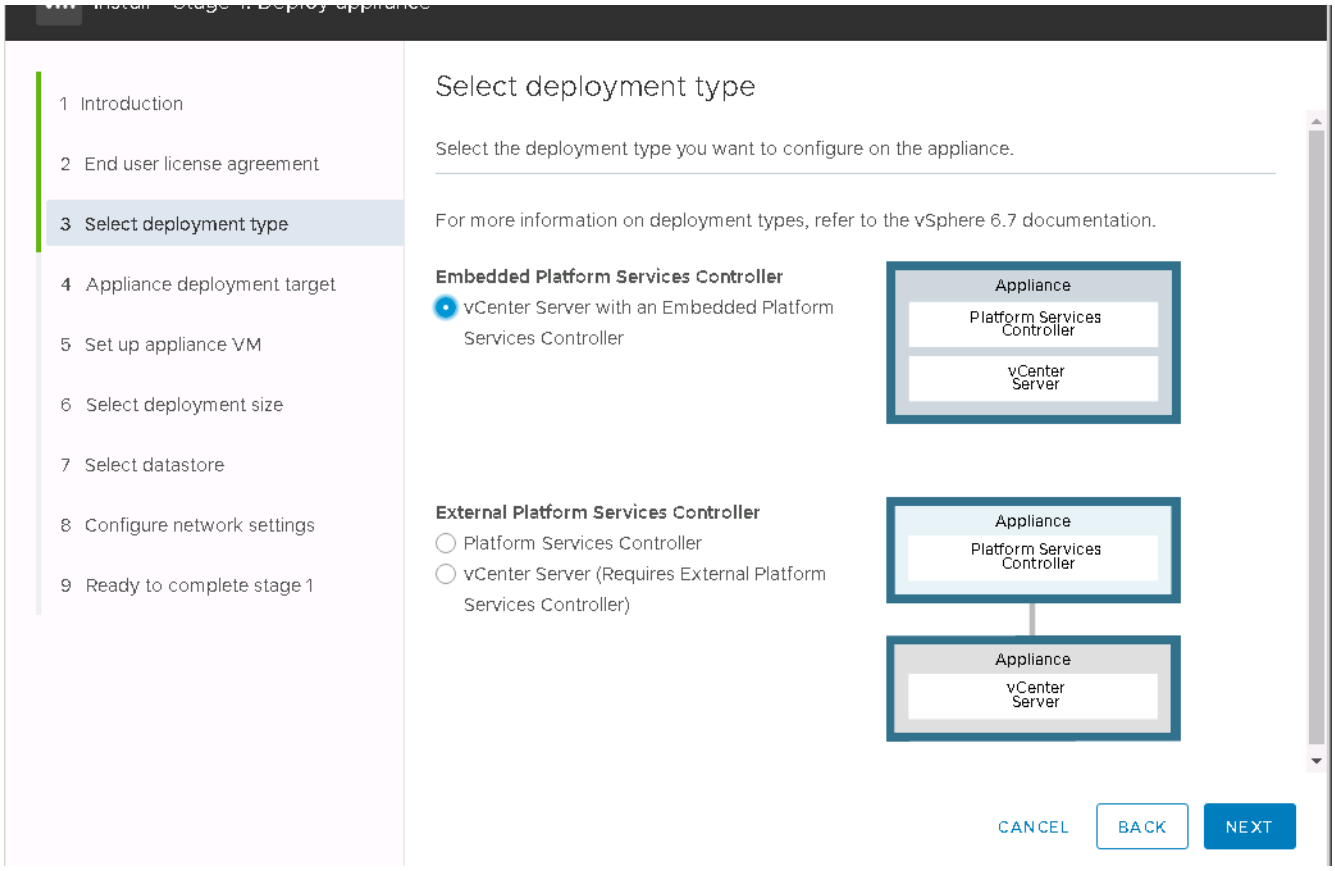
1. vCSA をダウンロードします。ESXi ホストの管理時に Get vCenter Server アイコンをクリックして、ダウンロードリンクにアクセスします。



2. vCSA を VMware サイトからダウンロードします。

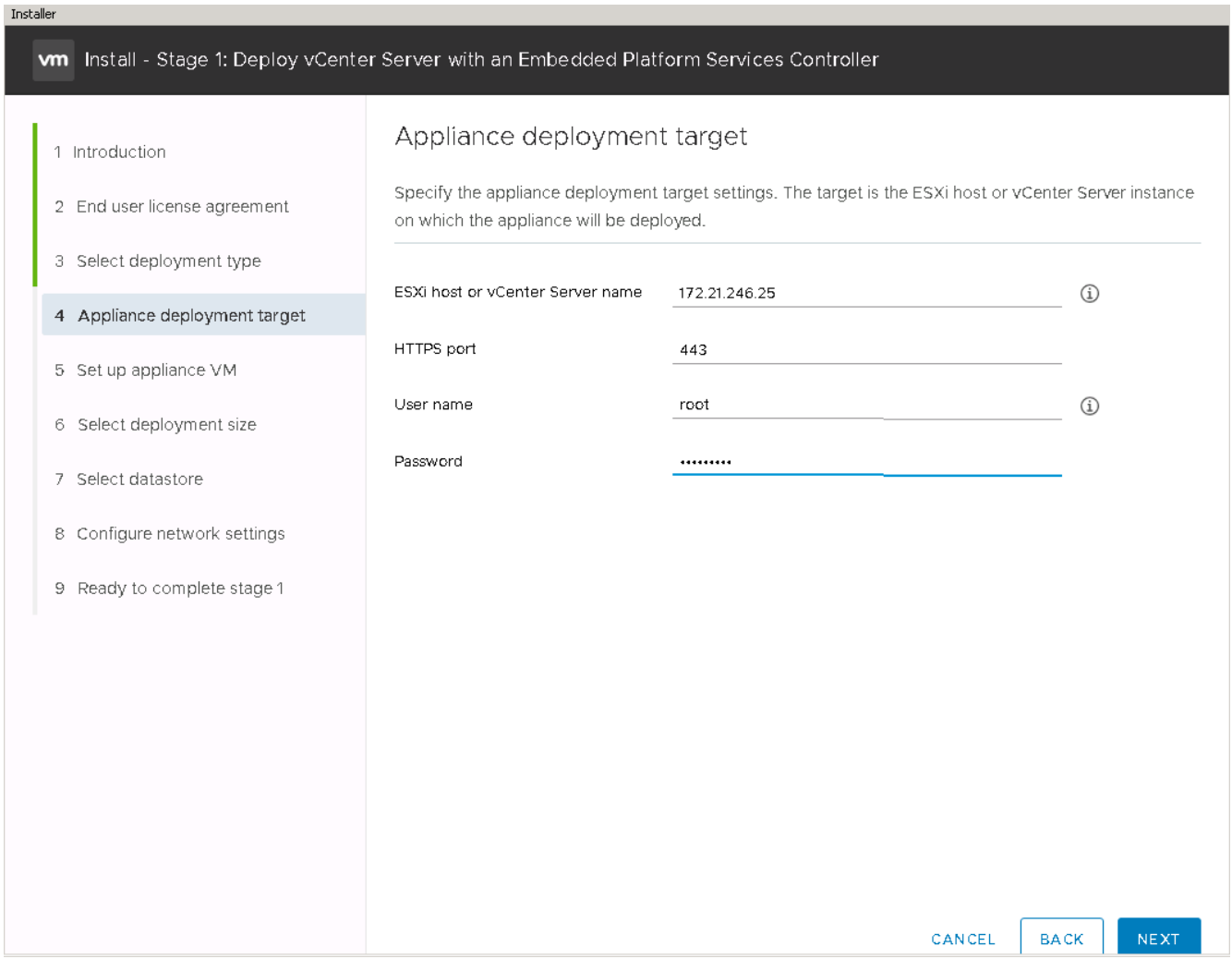
インストール可能な Microsoft Windows vCenter Server がサポートされますが、 VMware では新しい導入に vCSA を推奨します。

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。

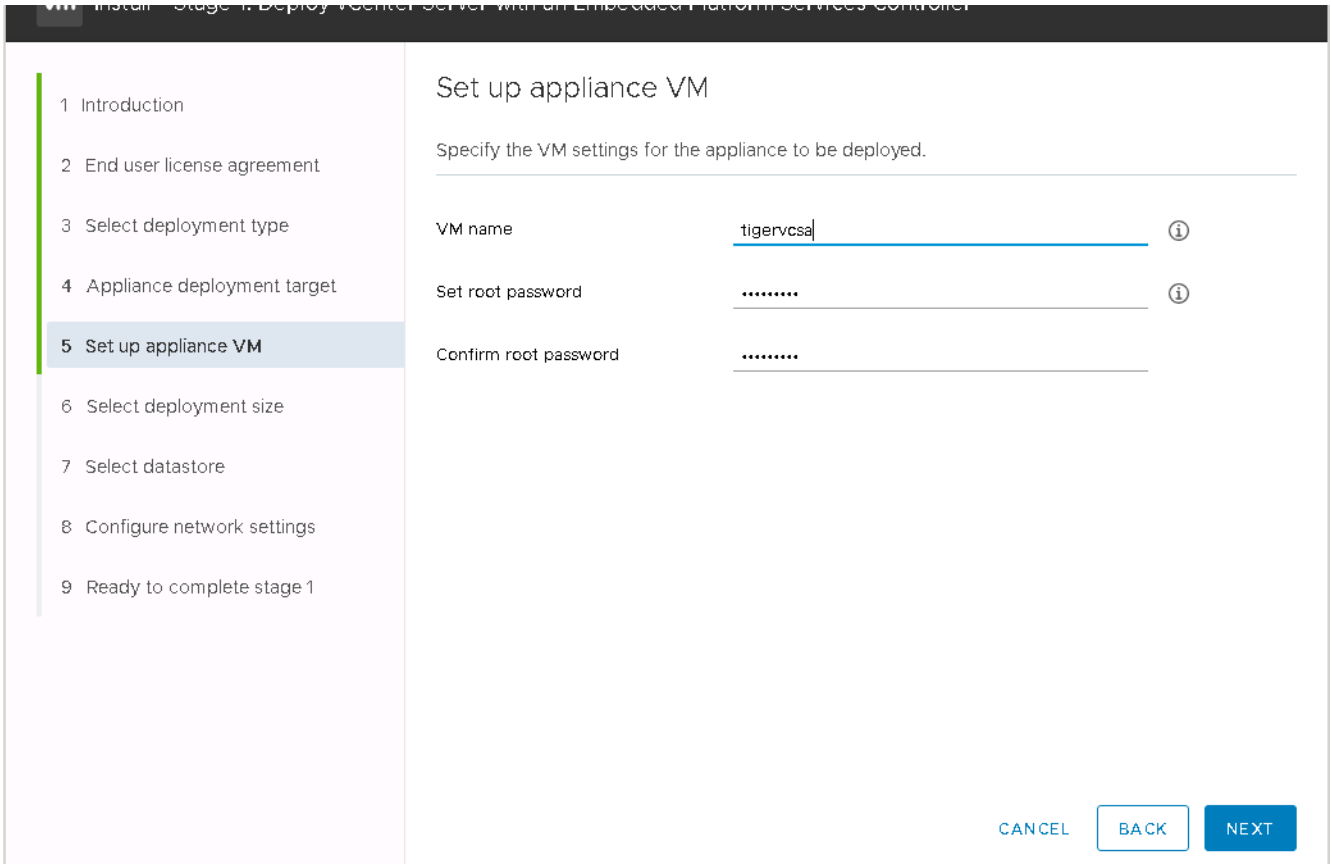


必要に応じて、 FlexPod Express 解決策の一部として、外部プラットフォームサービスコントローラの導入もサポートされます。

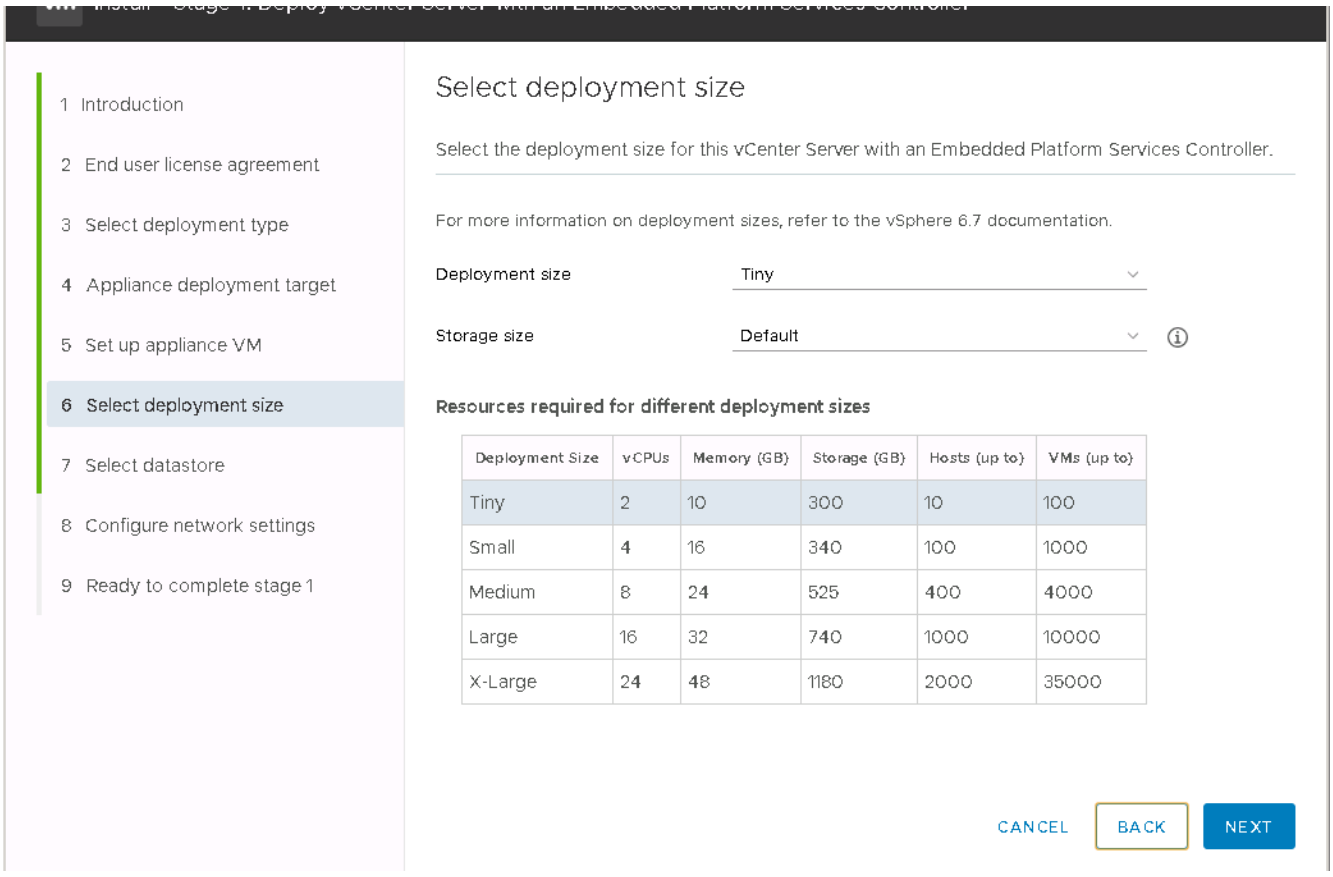
9. アプライアンス導入ターゲットで、導入した ESXi ホストの IP アドレス、および root ユーザ名と root パスワードを入力します。



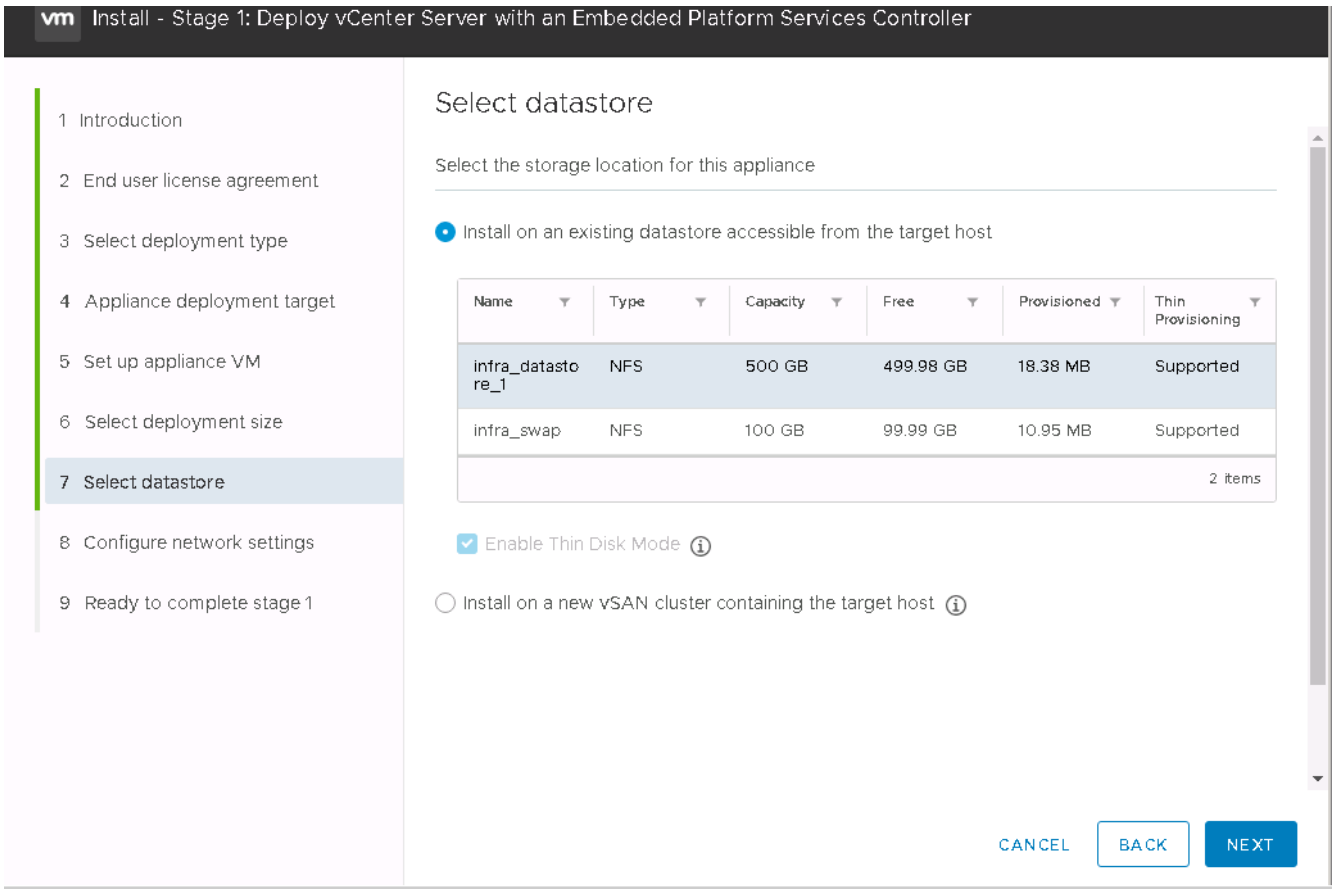
10. VCSA を VM 名として「 VCSA 」に入力し、 VCSA に使用するルート・パスワードを設定します。



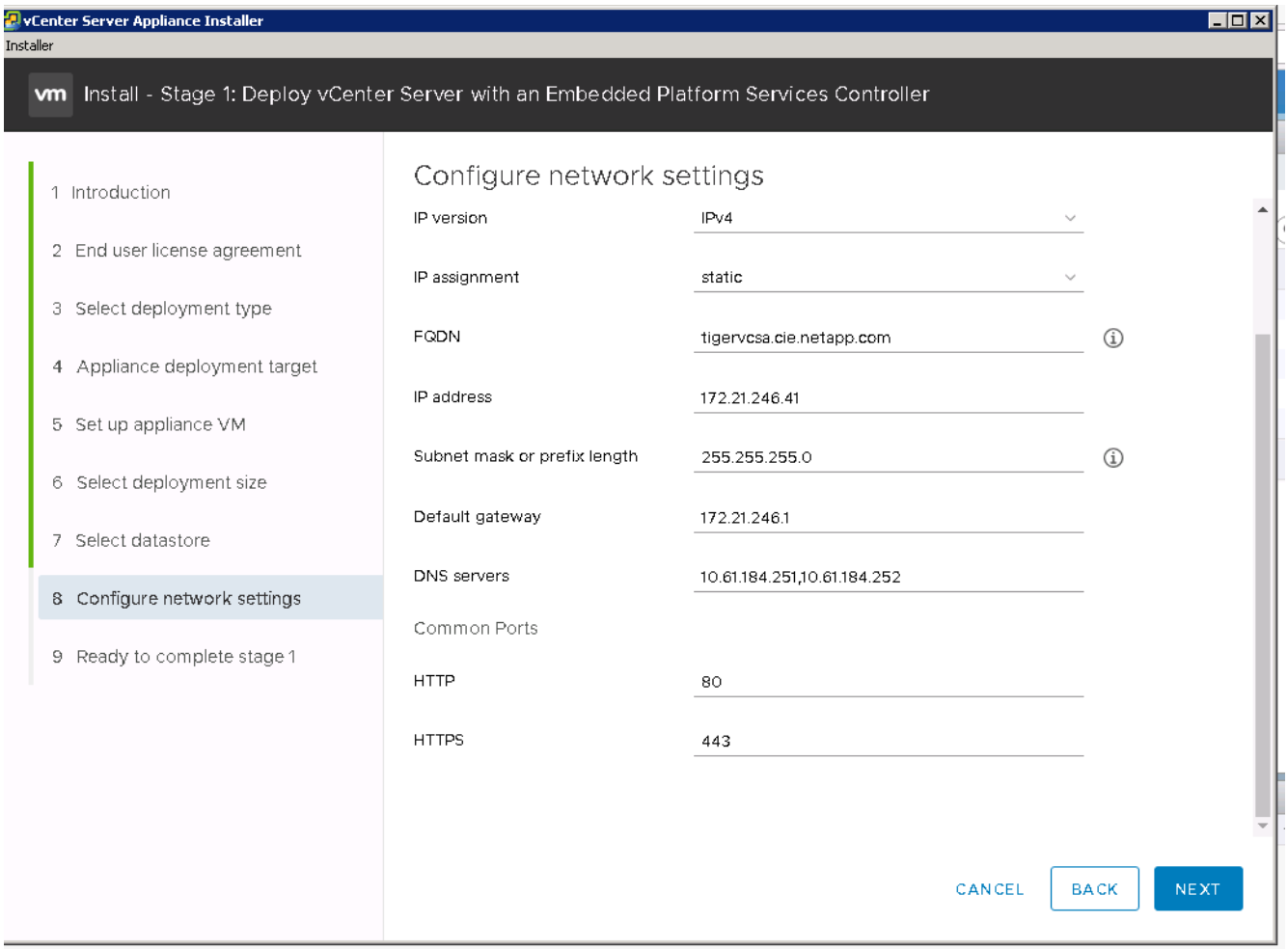
11. 環境に最も適した導入サイズを選択してください。次へをクリックします。



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。

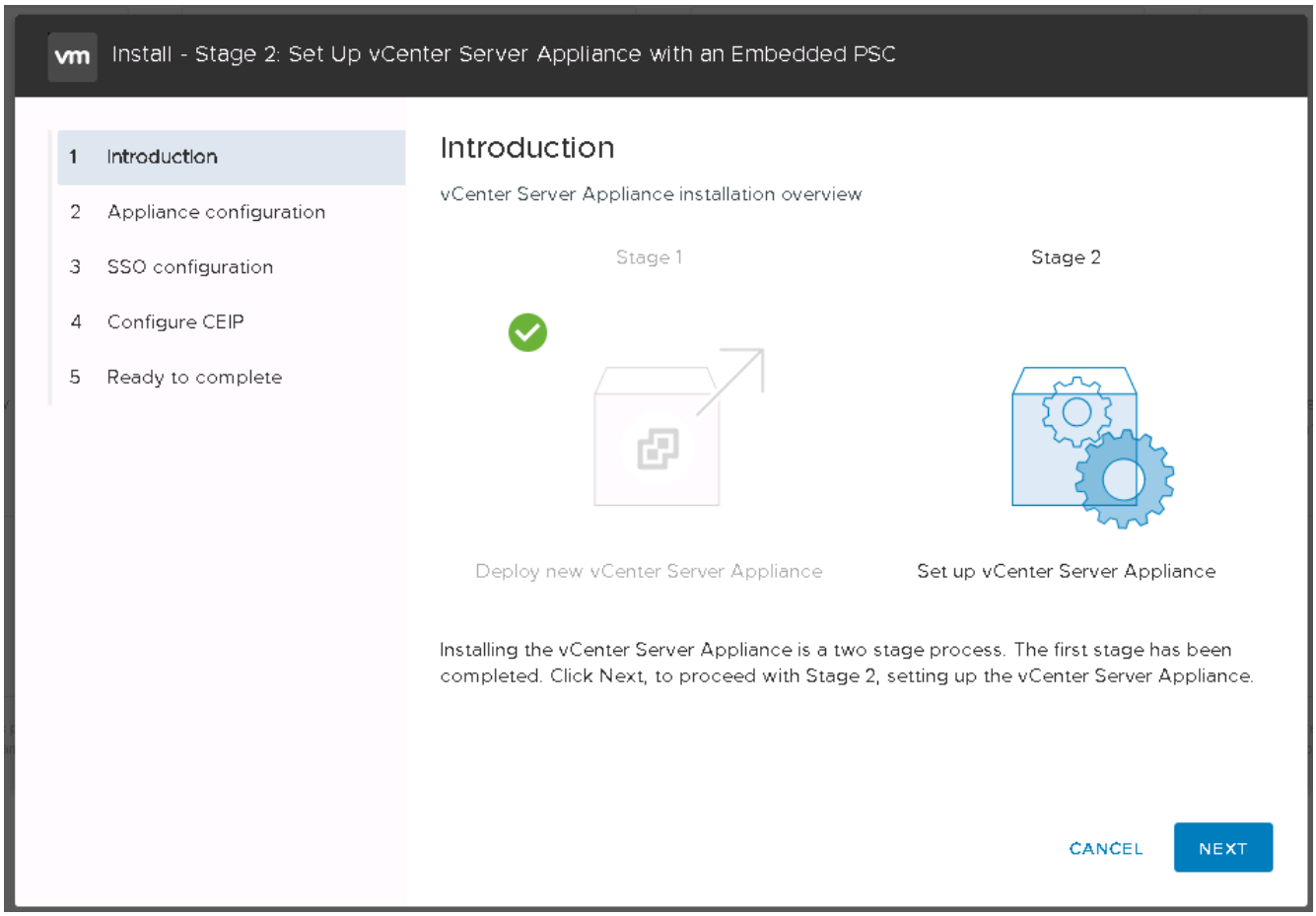


13. Configure network settings （ネットワーク設定の設定）ページで次の情報を入力し、 Next （次へ）をクリックします。
    a. MGMT - Network （ネットワーク）を選択します。
    b. vCSA に使用する FQDN または IP を入力します。
    c. 使用する IP アドレスを入力します。
    d. 使用するサブネットマスクを入力します。
    e. デフォルトゲートウェイを入力します。
    f. DNS サーバを入力します。
14. 「ステージ 1 を完了する準備ができました」ページで、入力した設定が正しいことを確認します。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

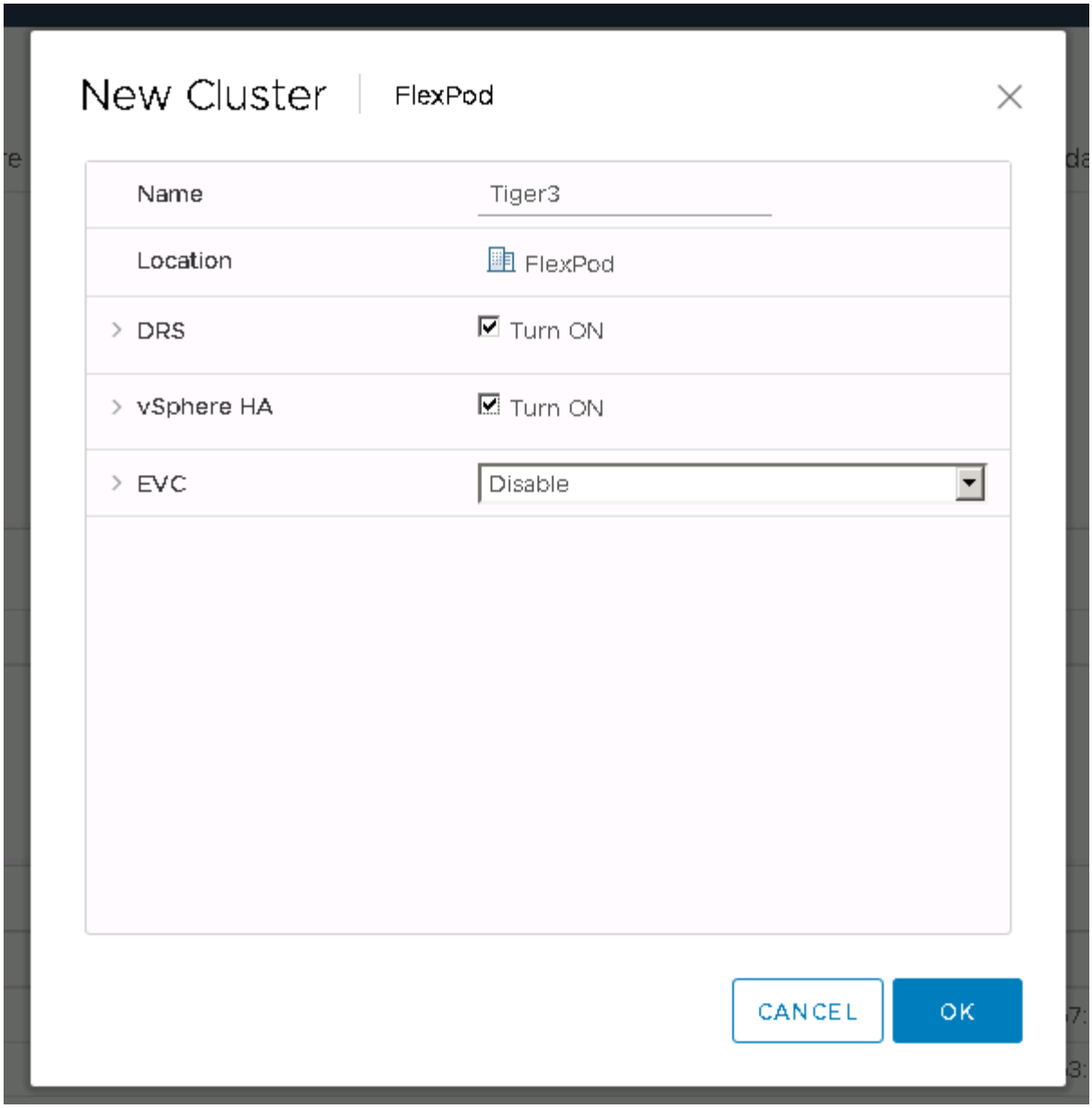
VMware vCenter Server 6.7 および vSphere クラスタリングを設定するには、次の手順を実行します。

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

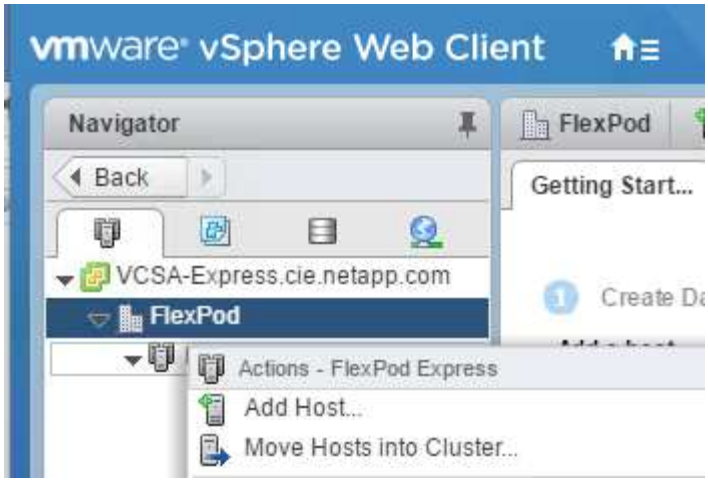
vSphere クラスタを作成するには、次の手順を実行します。

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。

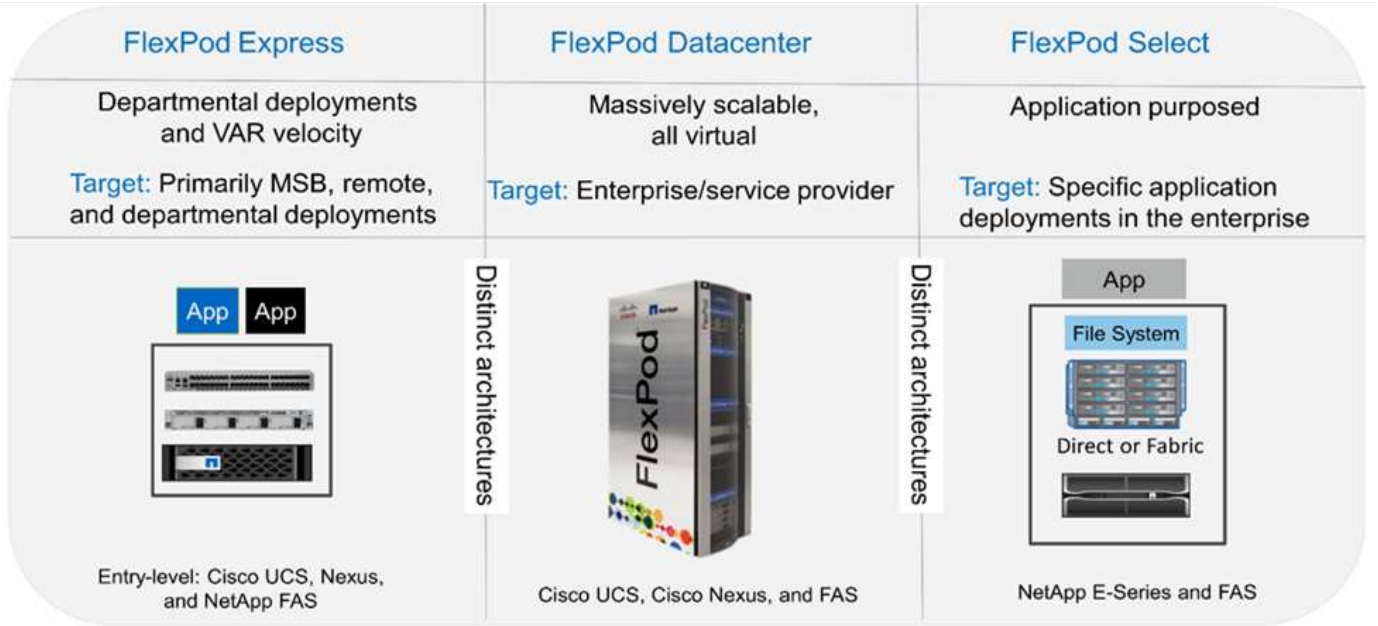
FlexPod 統合インフラプログラム

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

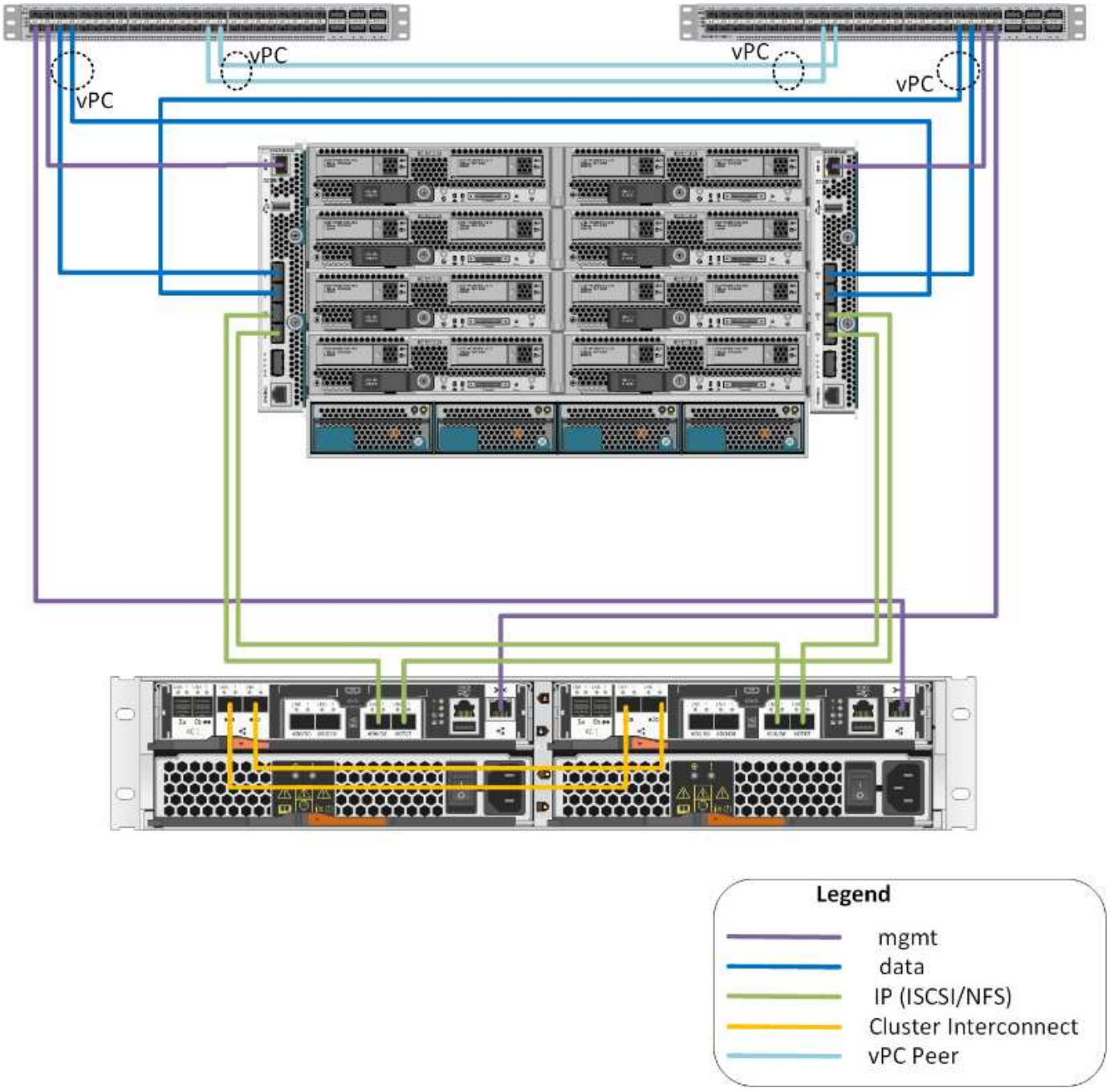
ソフトウェアコンポーネント

- 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。

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

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。

   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

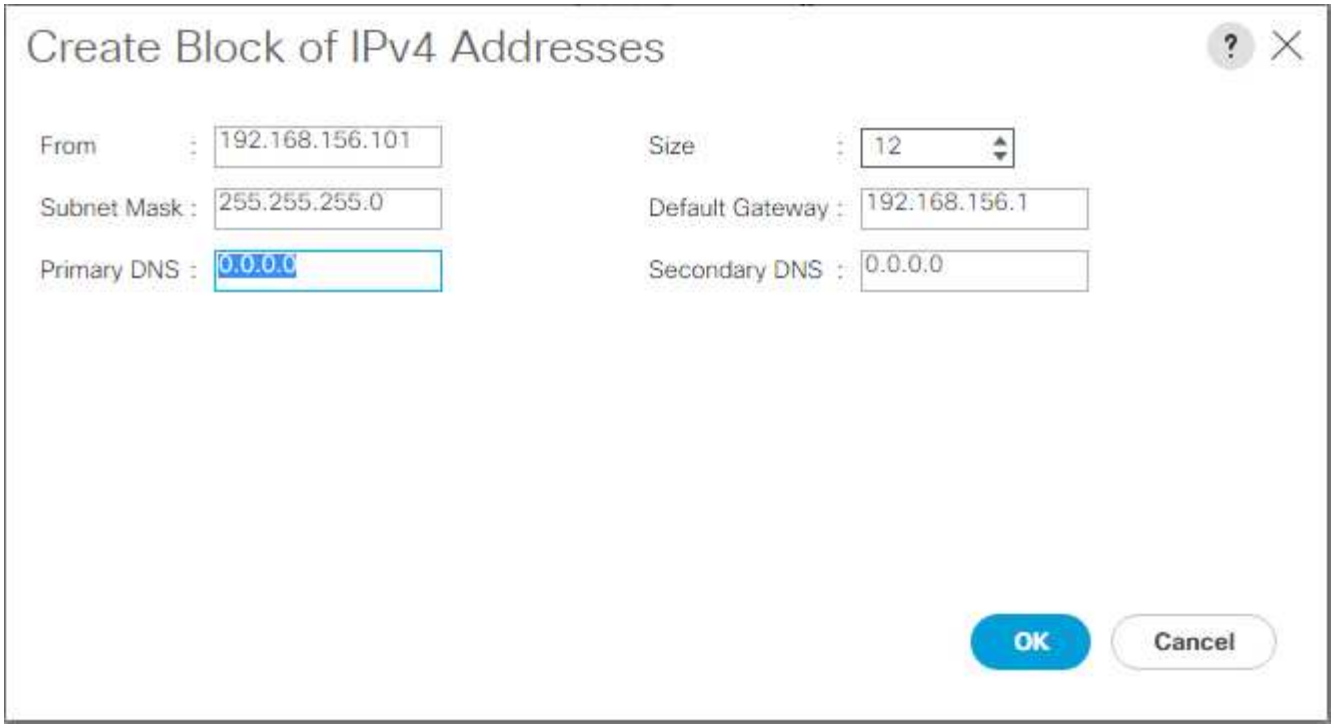
Cisco UCS Manager で Call Home を設定することを強く推奨します。Call Home を設定すると、サポートケースの解決が迅速になります。Call Home を設定するには、次の手順を実行します。

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。



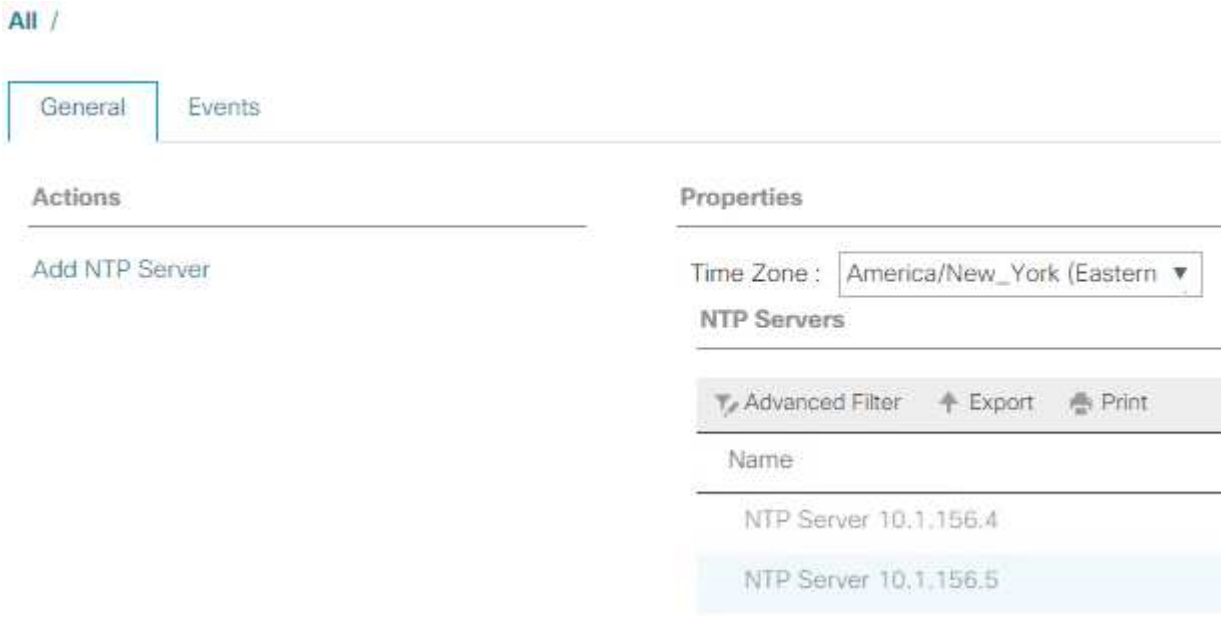
5. [OK] をクリックして、ブロックを作成する。
6. 確認メッセージで [OK] をクリックします。

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

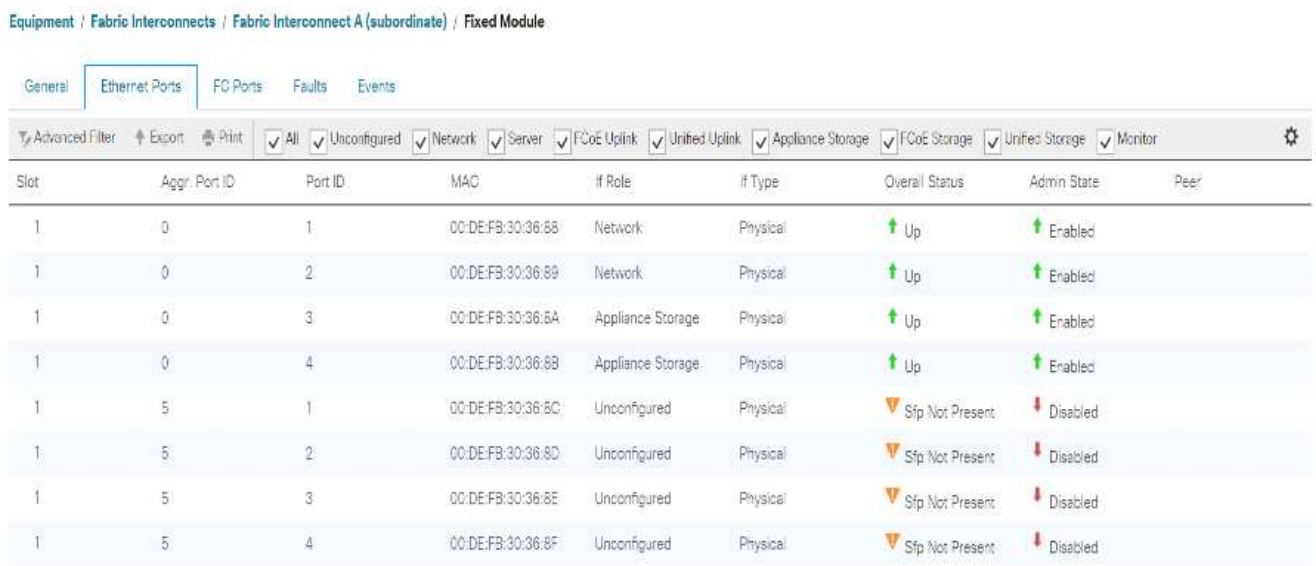
Enabled （有効）に設定します。

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

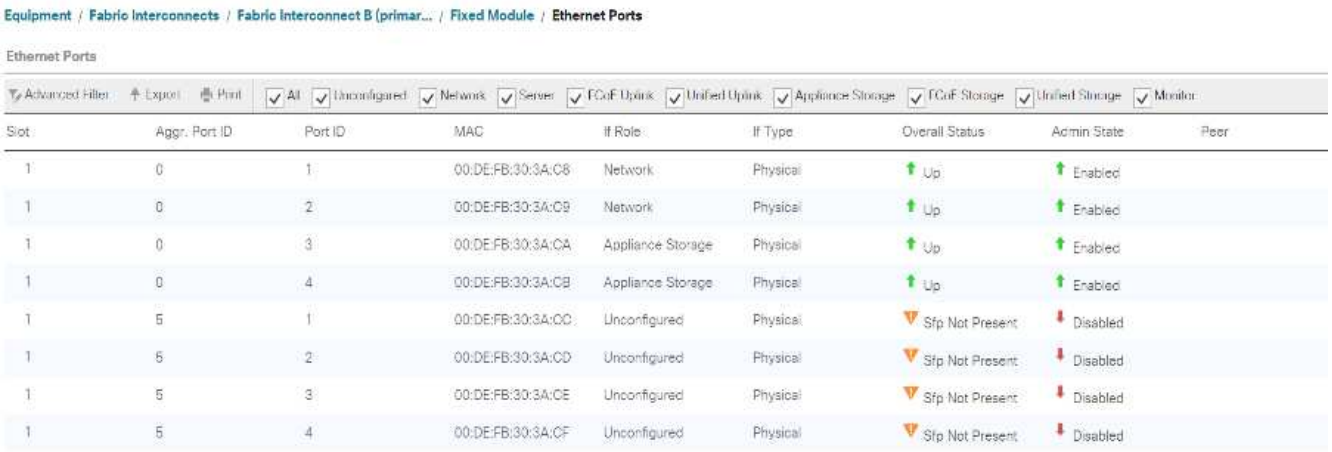
サーバポートとアップリンクポートをイネーブルにするには、次の手順を実行します。

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。



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。



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

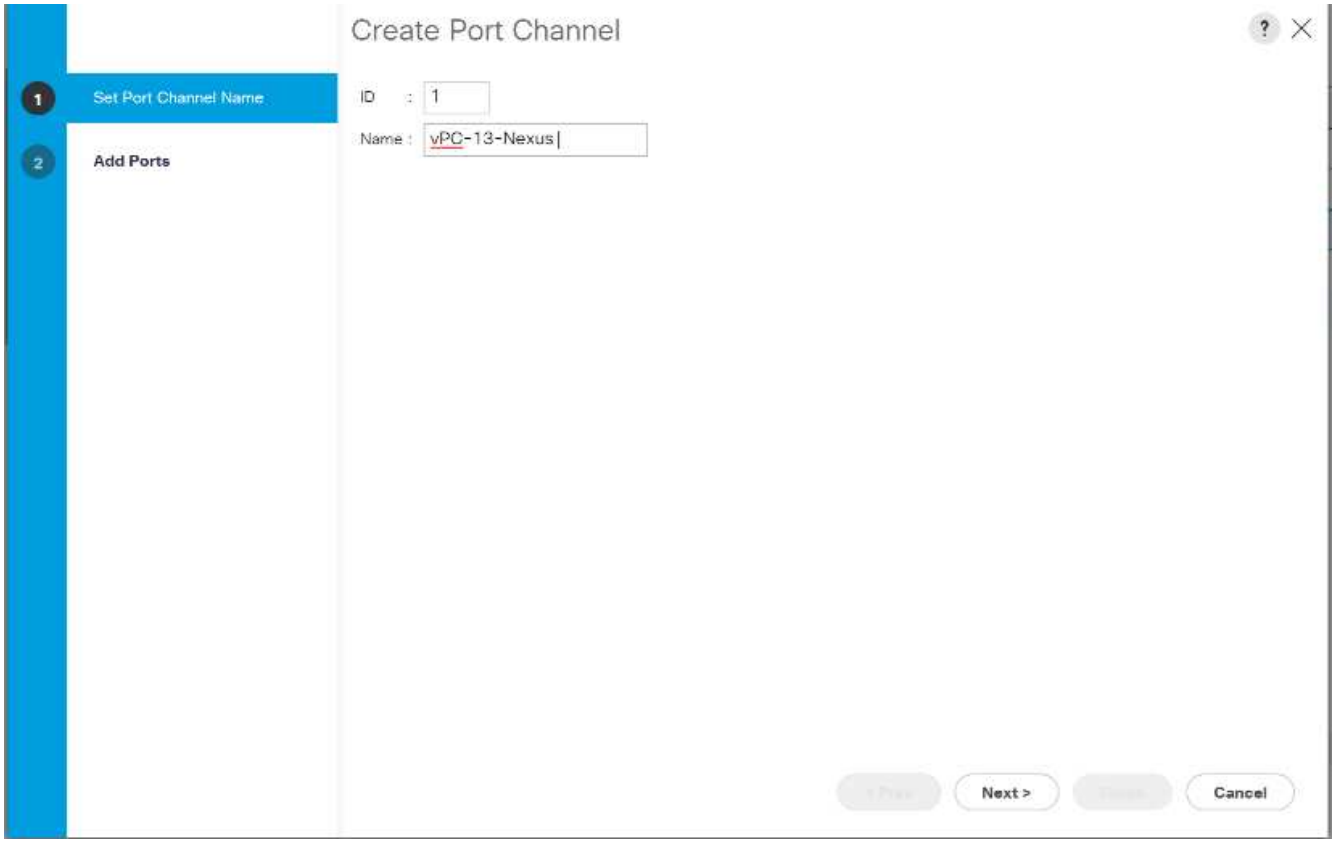
Cisco UCS 環境で必要なポートチャネルを設定するには、次の手順を実行します。

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。

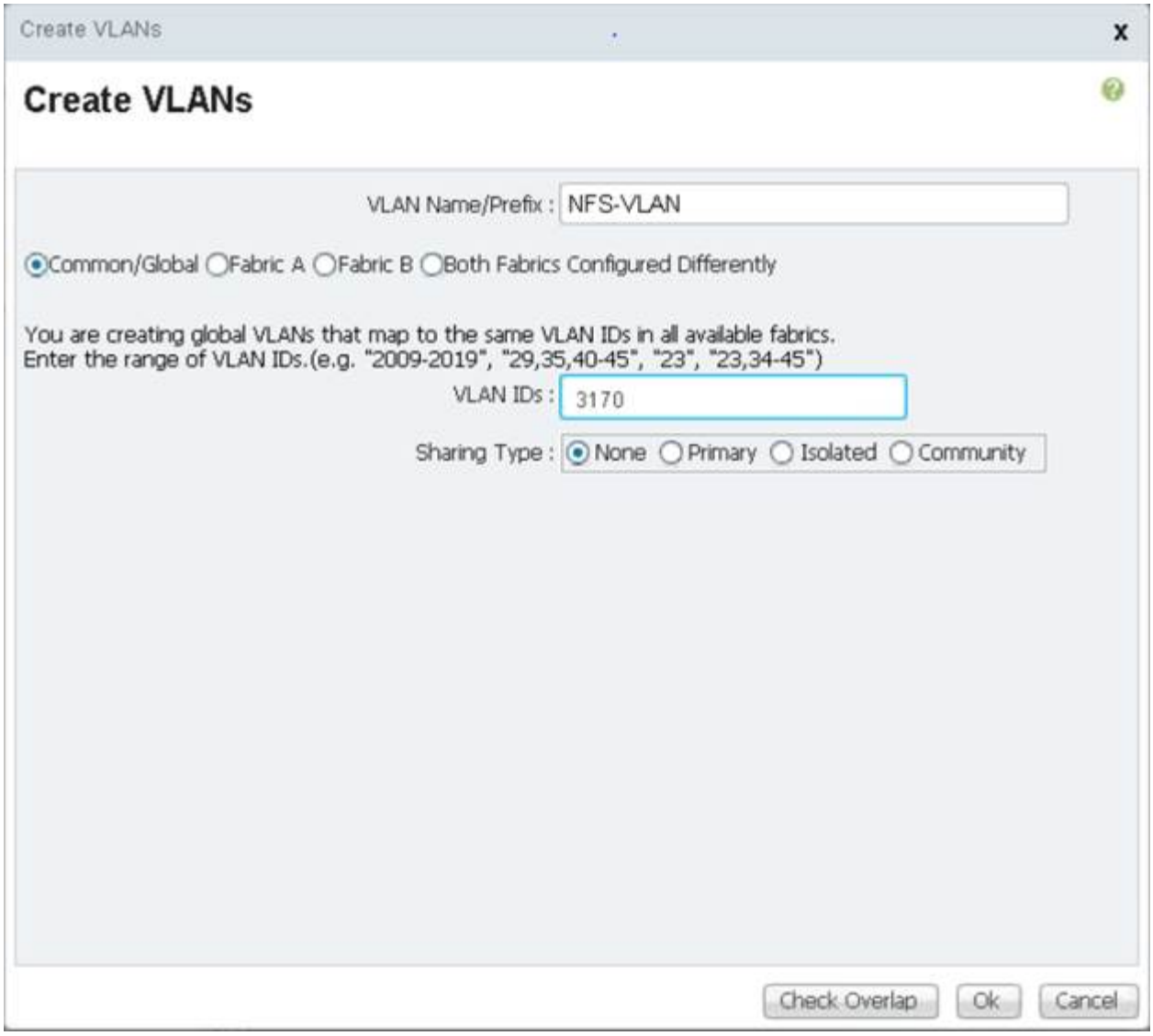
Cisco UCS 環境で組織を設定するには、次の手順を実行します。

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

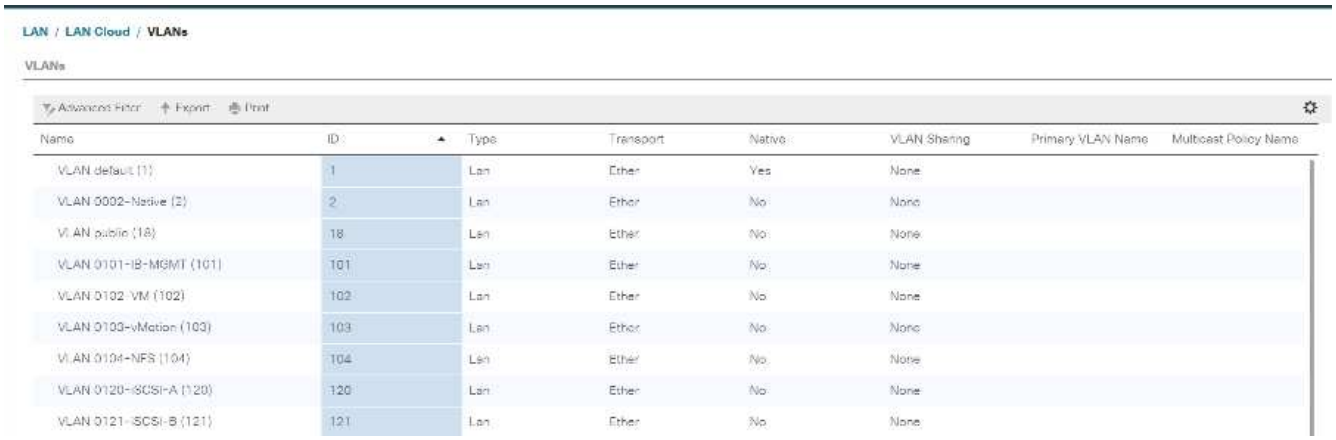
ストレージアプライアンスのポートとストレージ VLAN を設定するには、次の手順を実行します。

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。

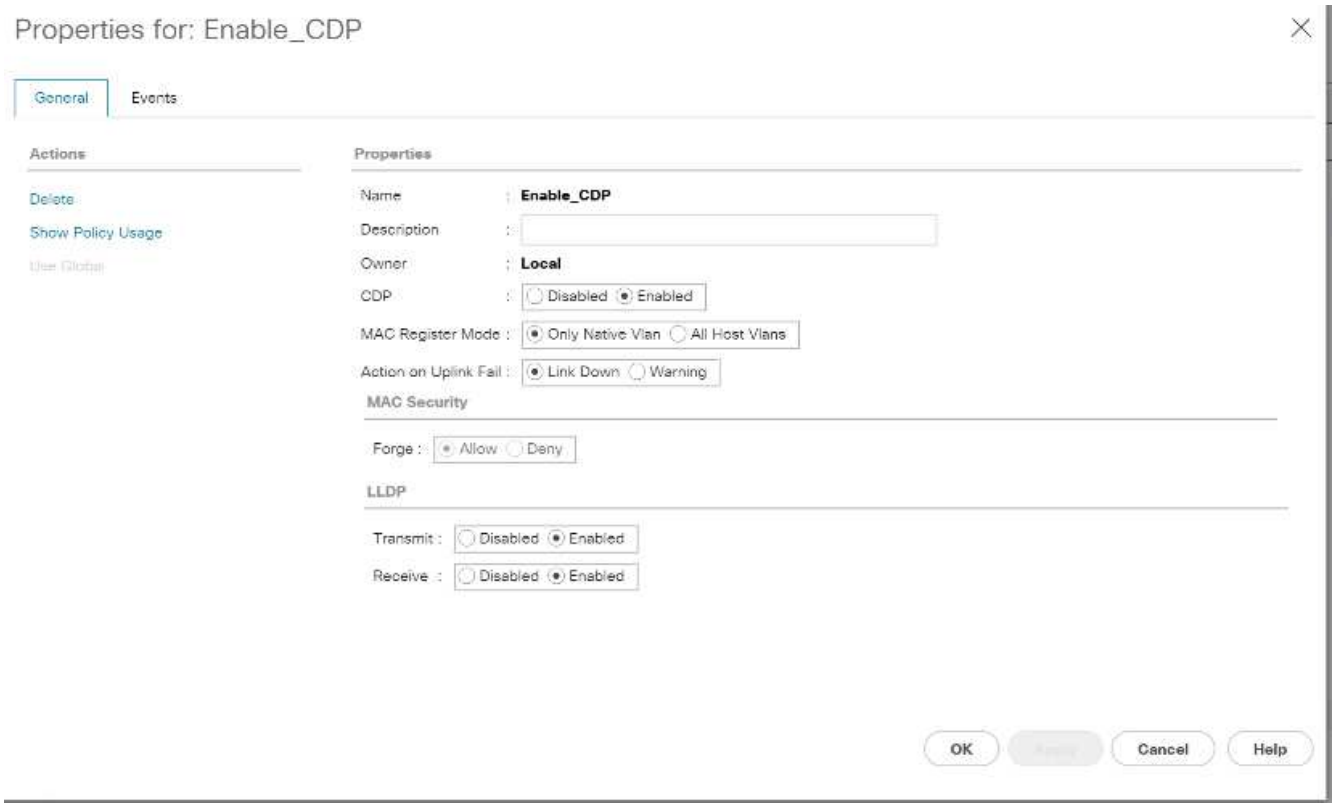


9. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。
10. アプライアンスクラウドの下の VLAN を右クリックします。
11. [Create VLANs] を選択します。
12. Infrastructure iSCSI Fabric A VLAN の名前として「 iSCSI-A-VLAN 」と入力します。
13. 共通 / グローバルを選択したままにします。
14. VLAN ID として「 <<var_iscsi-a_vlan_id>> 」と入力します。
15. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。
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。

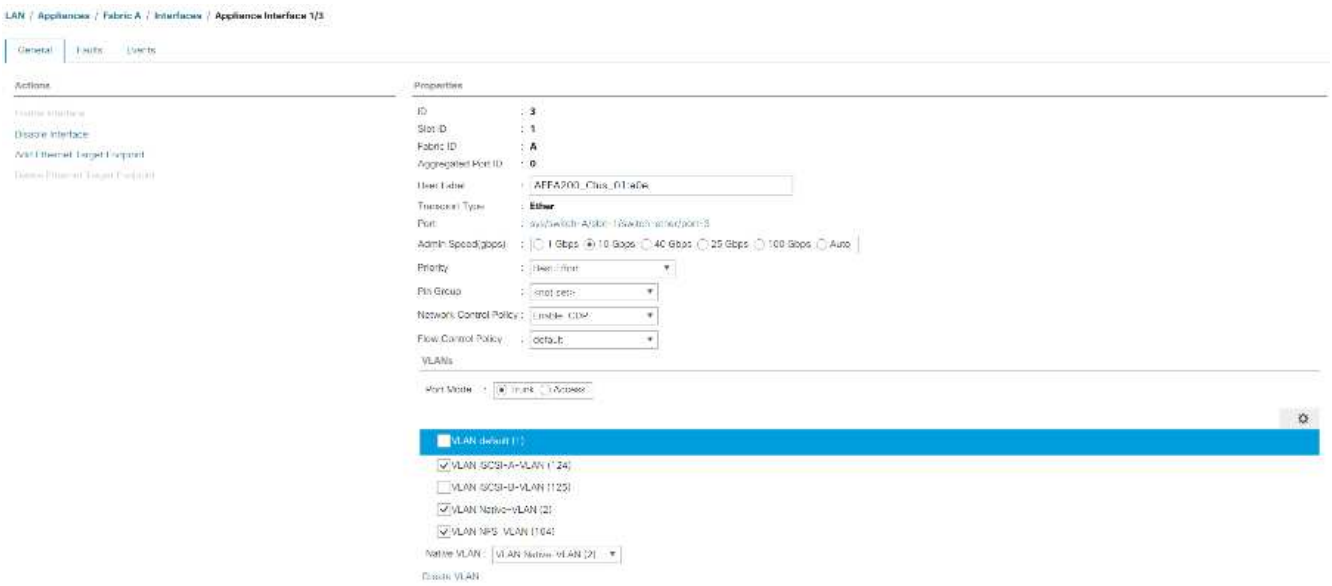
22. アプライアンスクラウドの下の VLAN を右クリックします。
23. [Create VLANs] を選択します。
24. ネイティブ VLAN の名前として「 Native - VLAN 」と入力します。
25. 共通 / グローバルを選択したままにします。
26. VLAN ID として「 <<var_native_vlan_id>> 」と入力します。
27. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。



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。

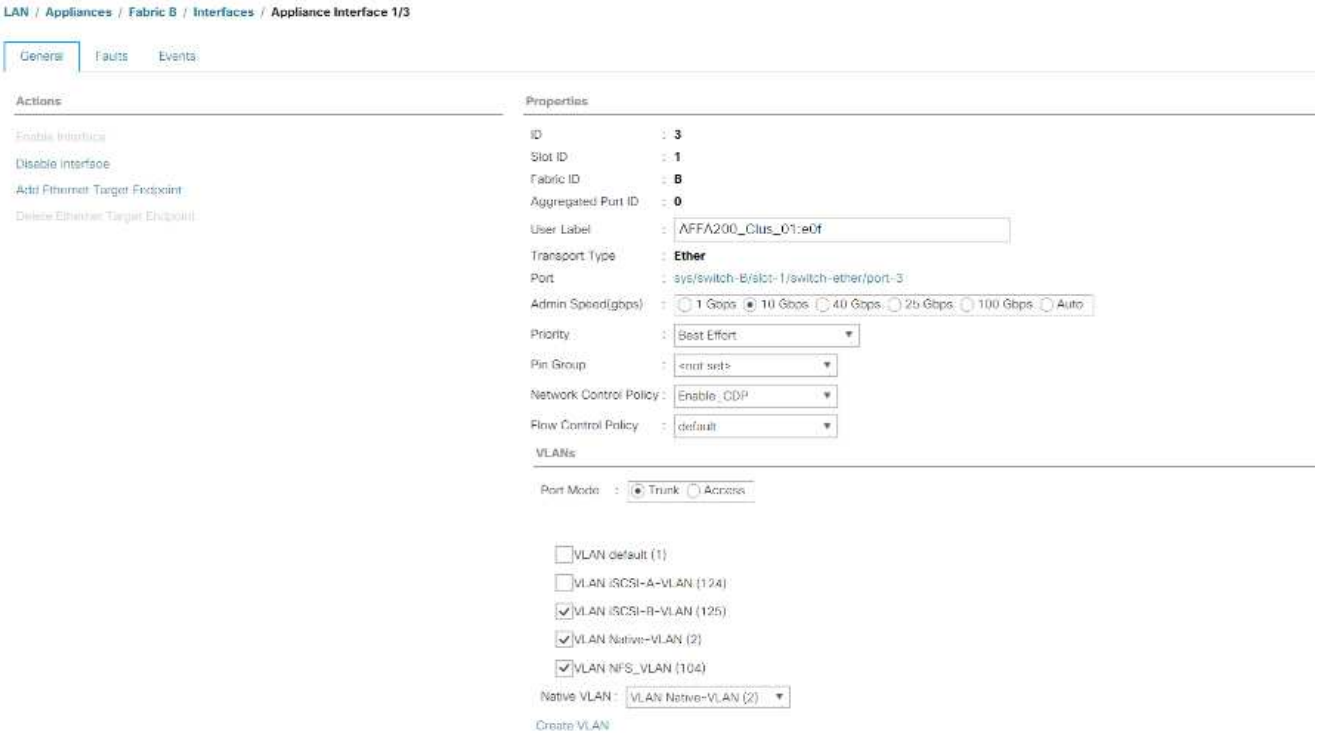


32. [OK] をクリックし、もう一度 [OK] をクリックしてポリシーを作成します。
33. ナビゲーションペインの [LAN] > [Appliances Cloud] で、 [Fabric A tree] を展開します。
34. [Interfaces] を展開します。
35. アプライアンス・インターフェイス 1/3 を選択します。
36. [User Label] フィールドに、「 <storage_controller_01_name> ： e0e 」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。
37. Enable_CDP 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。

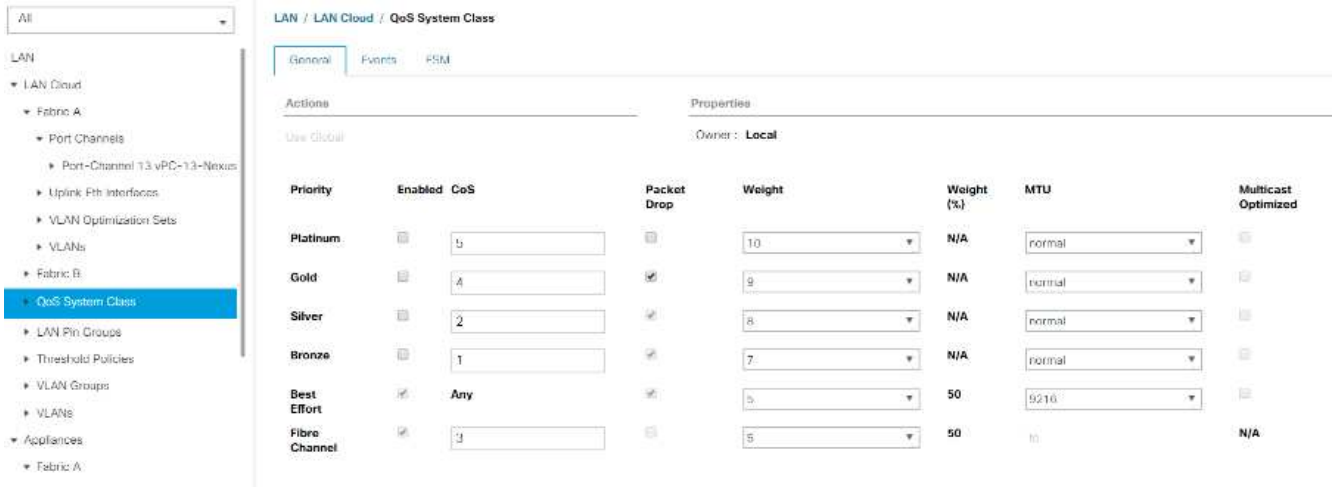


53. [変更を保存して OK] をクリックします。
54. [Fabric B] の下にある [Appliance Interface] 1/4 を選択します
55. [User Label] フィールドに、「 <storage_controller_02_name> ： e0f 」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。
56. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
57. [VLANs] で、 [iSCSI-B-VLAN] 、 [NFS 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"。

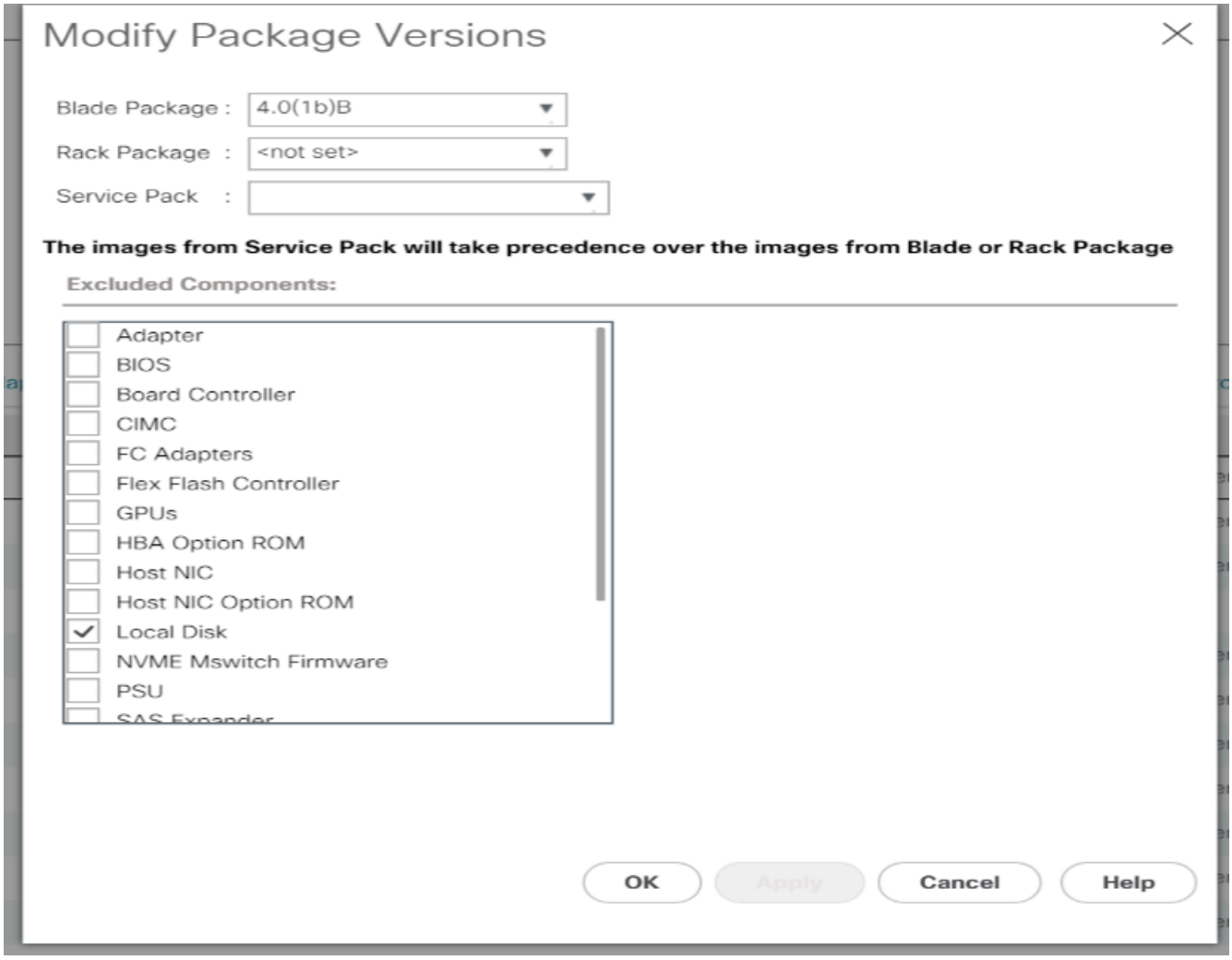
ホストファームウェアパッケージを作成する

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。

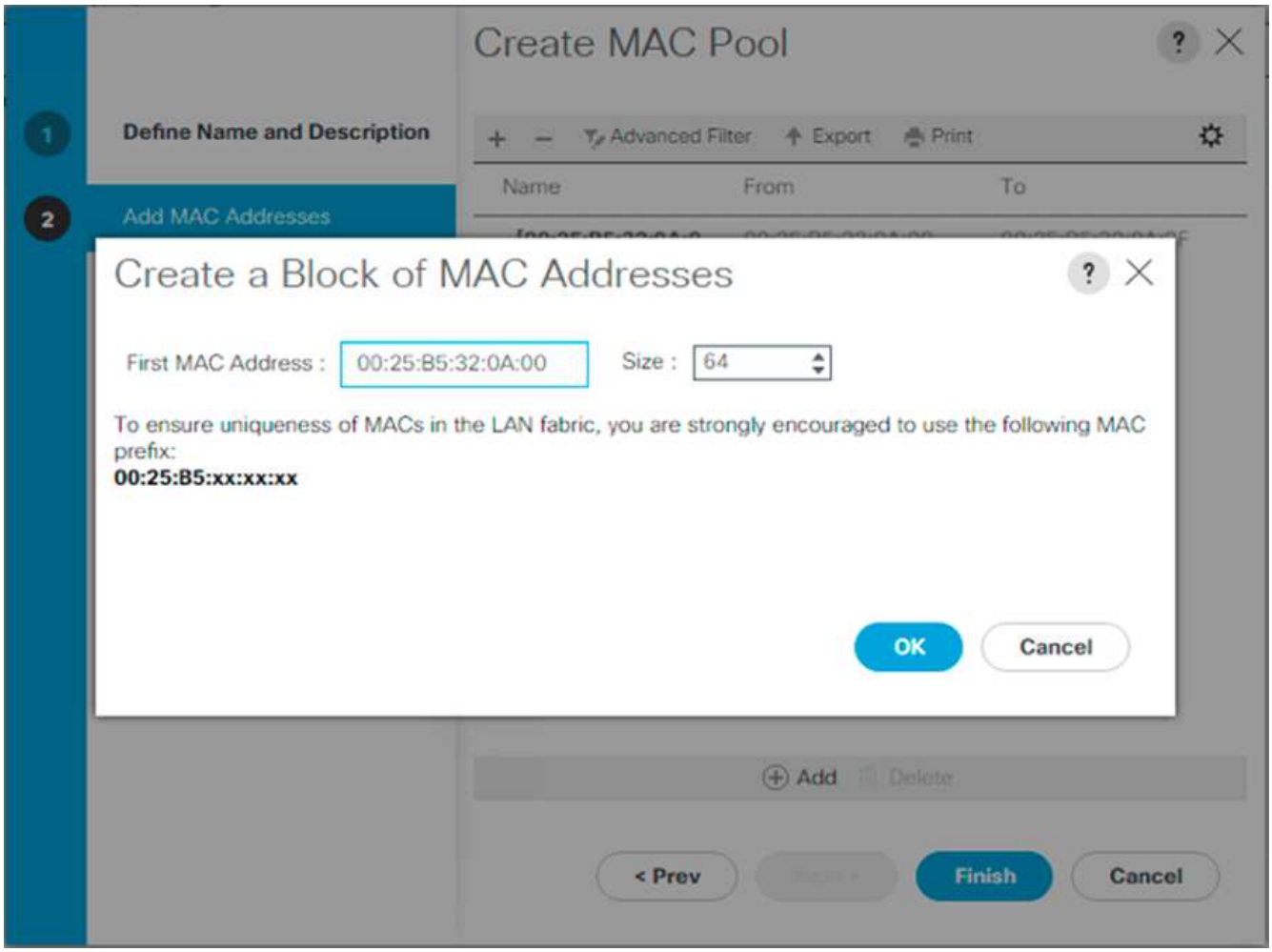
   この手順では、スイッチングファブリックごとに 1 つずつ、 2 つの MAC アドレスプールが作成されます。

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。

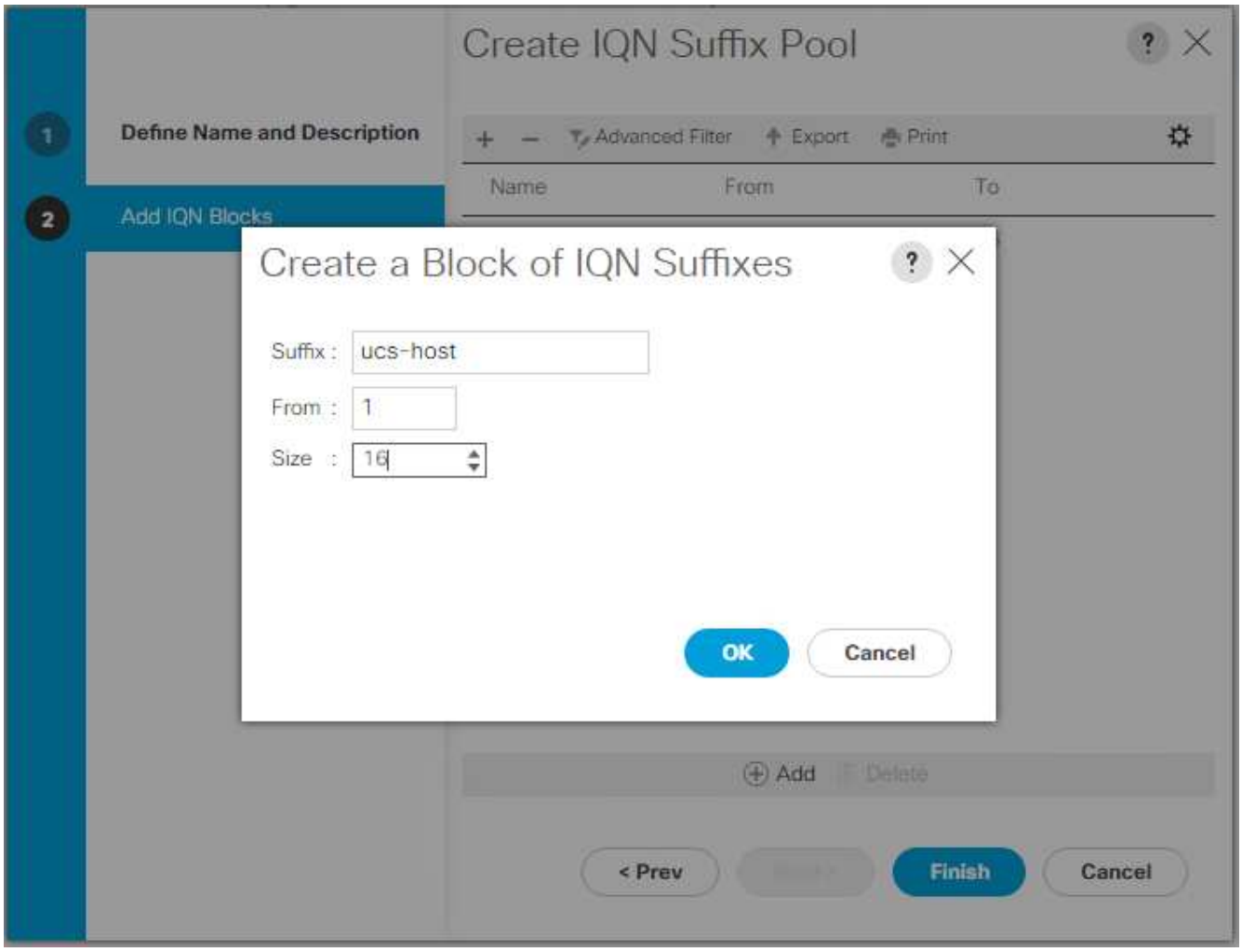
iSCSI IQN プールを作成します

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。

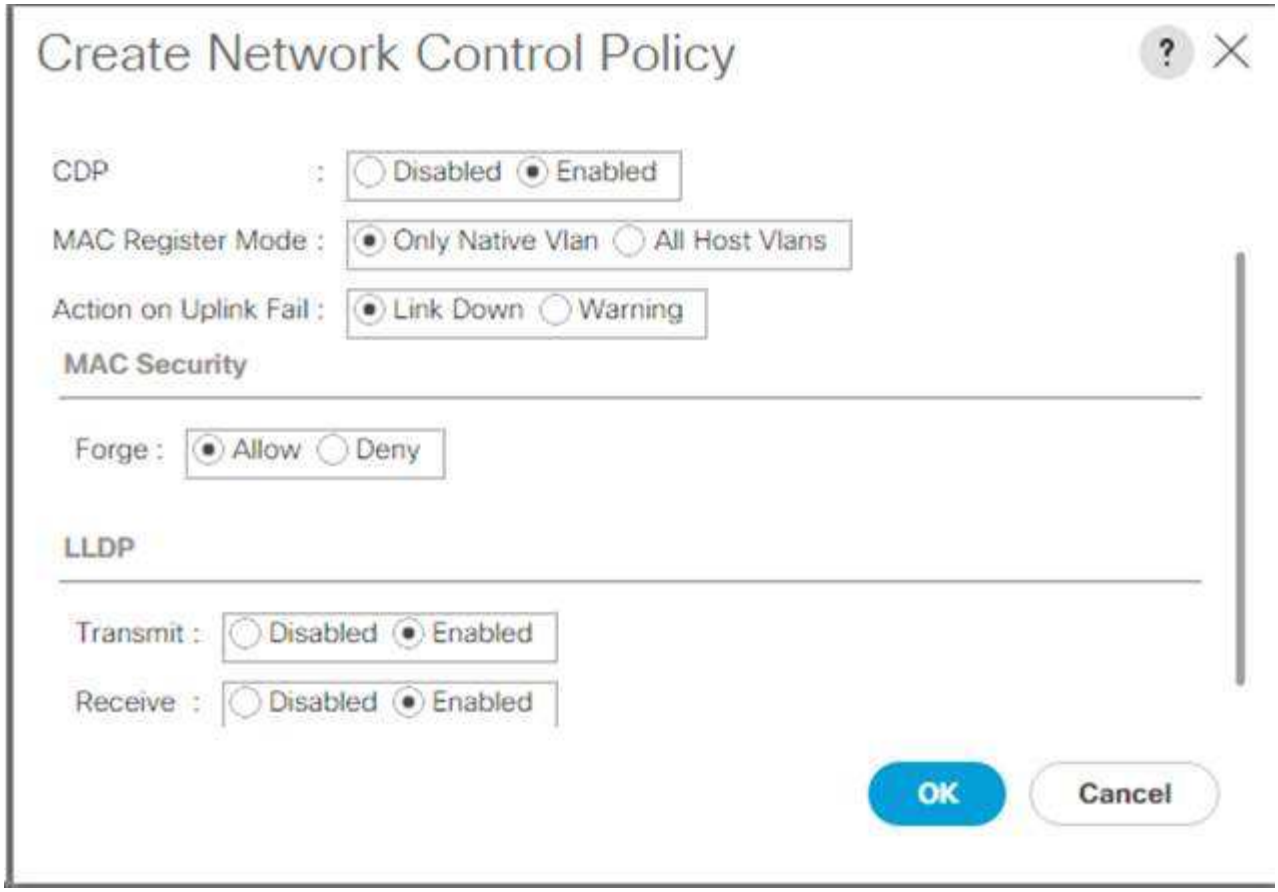
環境で必要とされる細分性を実現するために、固有のサーバプールを作成することを検討してください。

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。

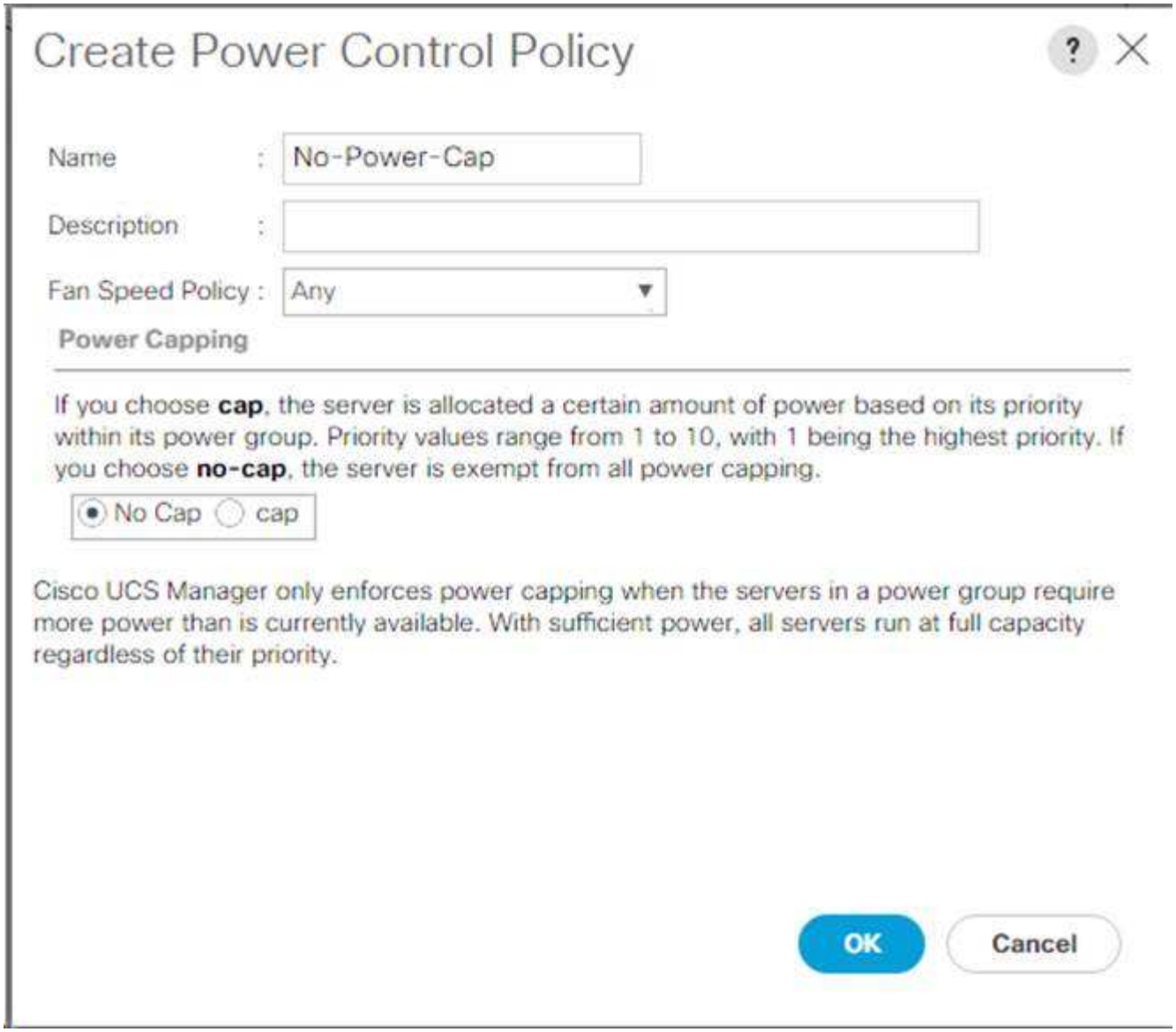
1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [ネットワーク制御ポリシー] を右クリックします。
4. Create Network Control Policy を選択します。
5. Enable-CDP-LLDP ポリシー名を入力します。
6. CDP の場合は、 Enabled オプションを選択します。
7. LLDP の場合は、下にスクロールして、送信と受信の両方で有効を選択します。
8. [OK] をクリックして、ネットワーク制御ポリシーを作成します。[OK] をクリックします。



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。



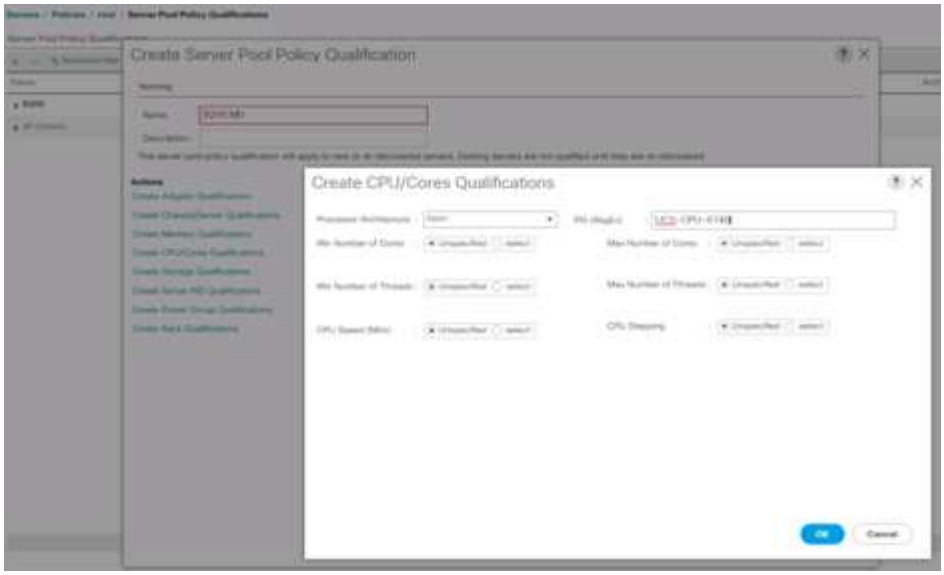
サーバプール認定ポリシーの作成（オプション）

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。

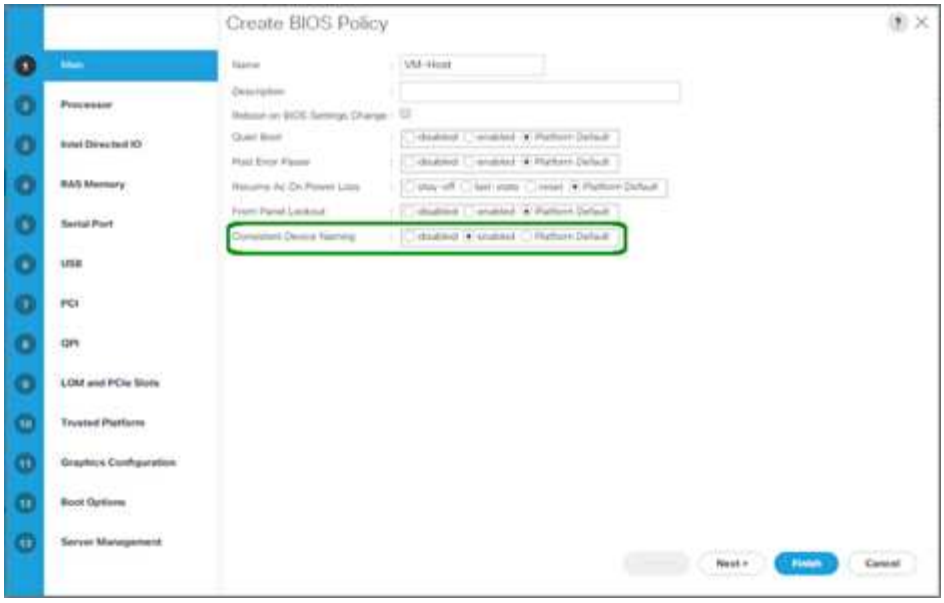
8. プロセス ID （ PID ）として「 <UCS-CPU-PID>` 」と入力します。
9. [OK] をクリックして、 CPU/ コアの資格情報を作成します。
10. [OK] をクリックしてポリシーを作成し、 [OK] をクリックして確認します。



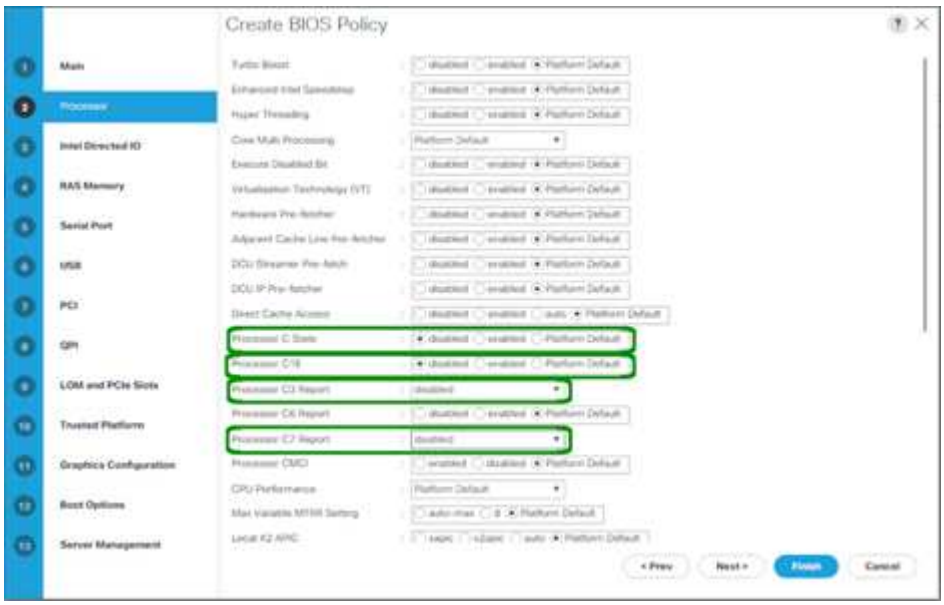
サーバ **BIOS** ポリシーを作成します

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。

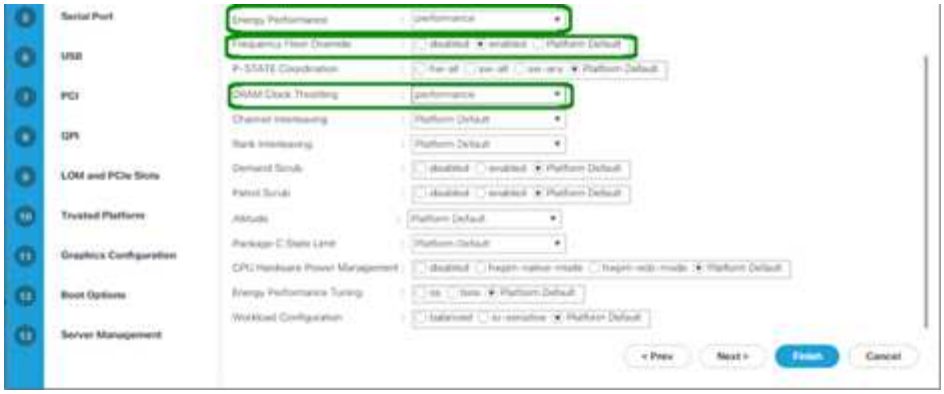
1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. BIOS Policies （ BIOS ポリシー）を右クリックします。
4. [Create BIOS Policy] を選択します。
5. BIOS ポリシー名として「 VM-Host 」と入力します。
6. Quiet Boot 設定を disabled に変更します。
7. 一貫したデバイス名を有効に変更します。



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



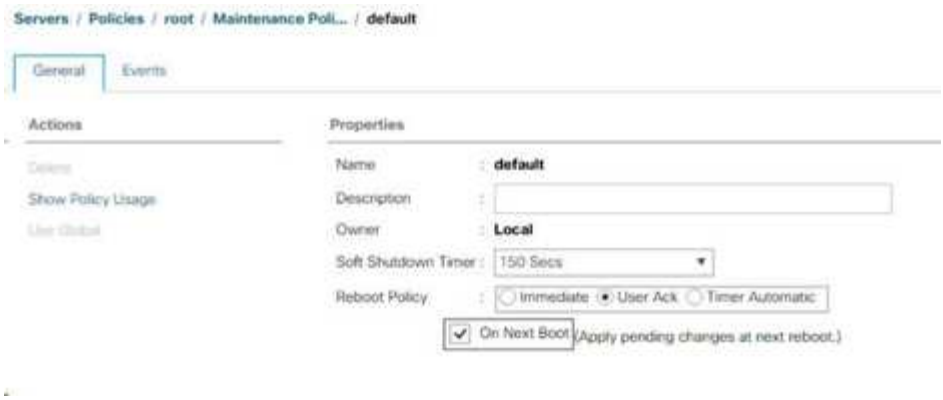
10. [RAS メモリ] をクリックして、次のパラメータを設定します。
    - LV DDR モード：パフォーマンスモード

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。

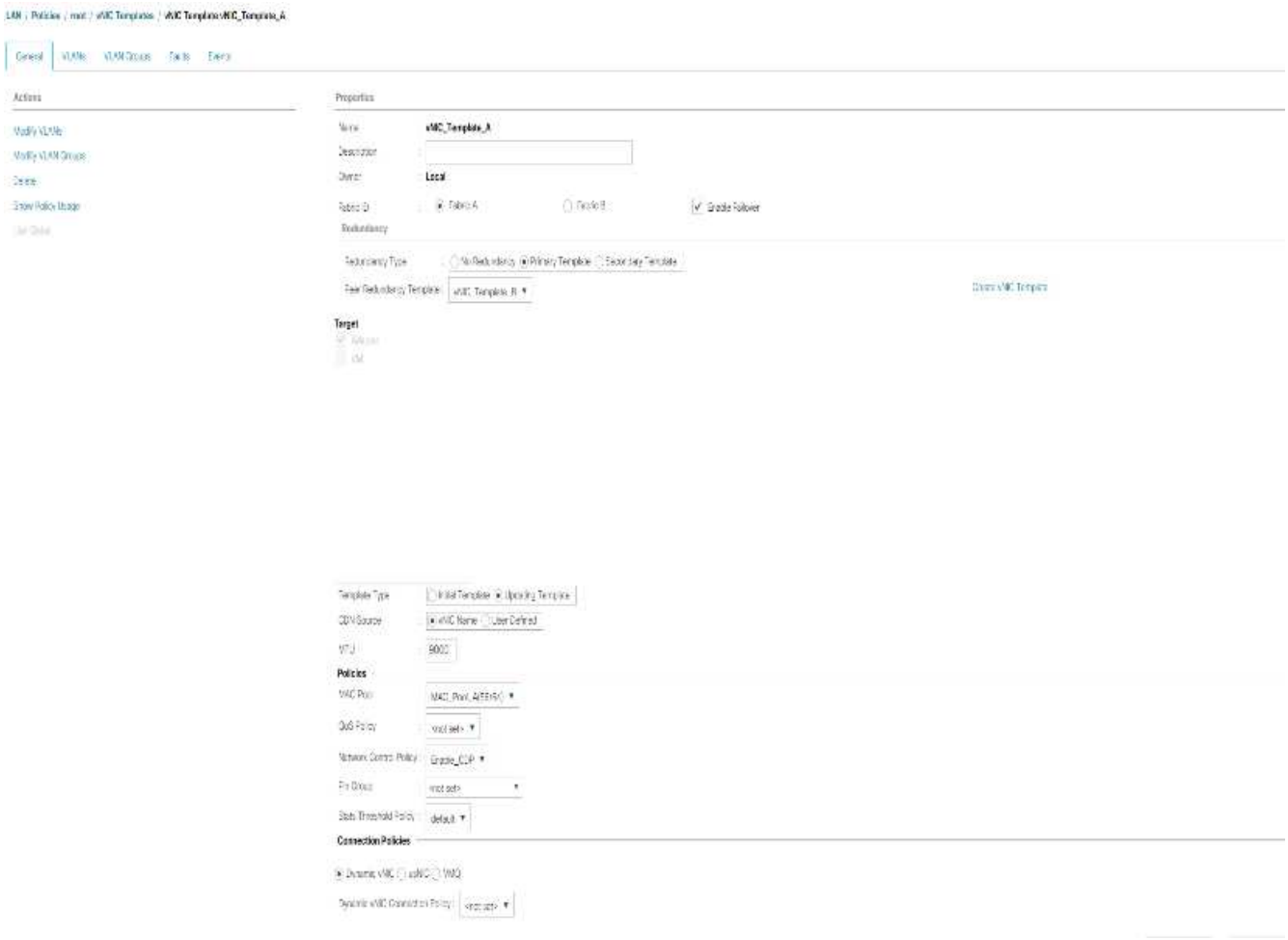
合計 4 つの vNIC テンプレートが作成されます。

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。

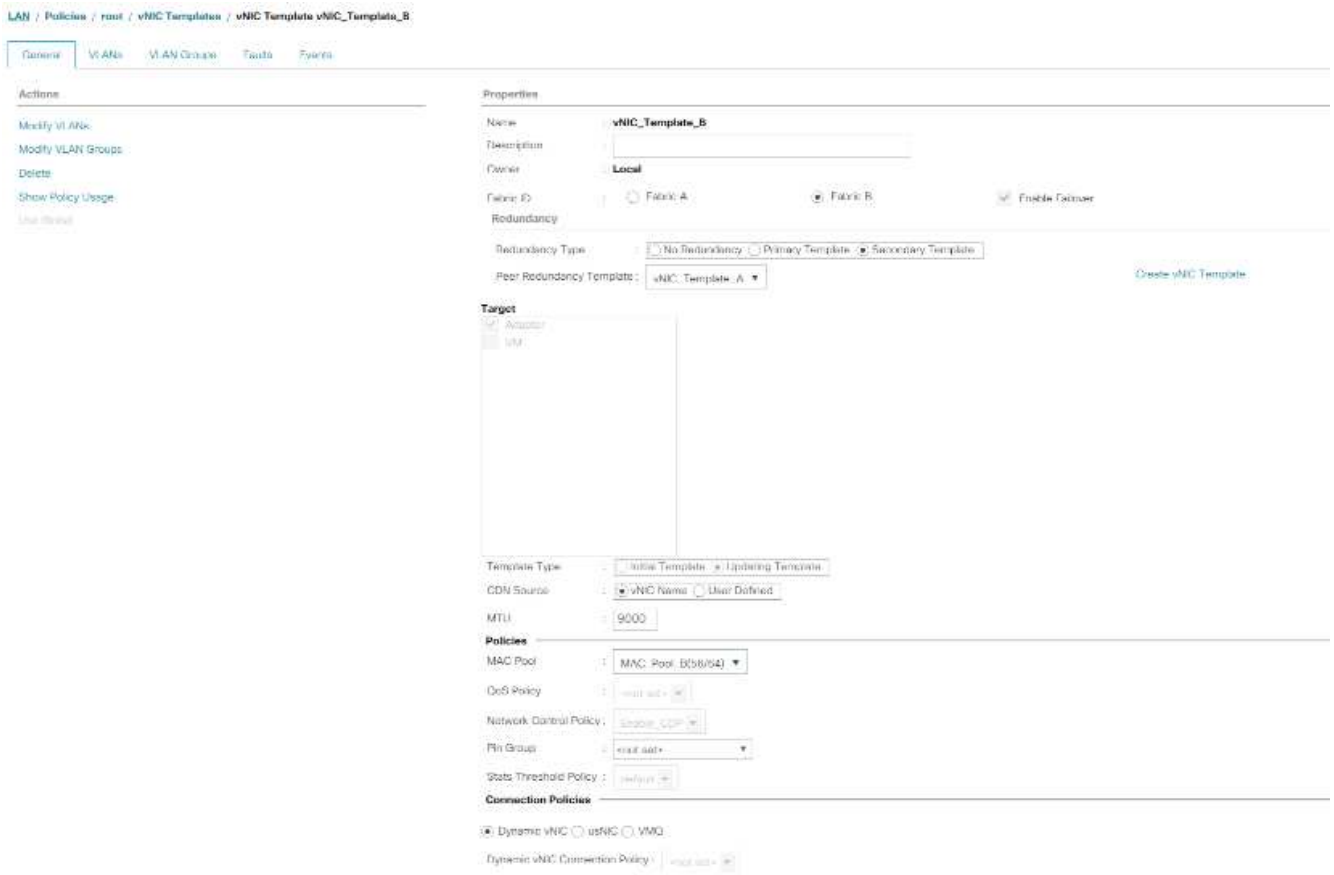


セカンダリ冗長テンプレート Infra-B を作成するには、次の手順を実行します。

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。

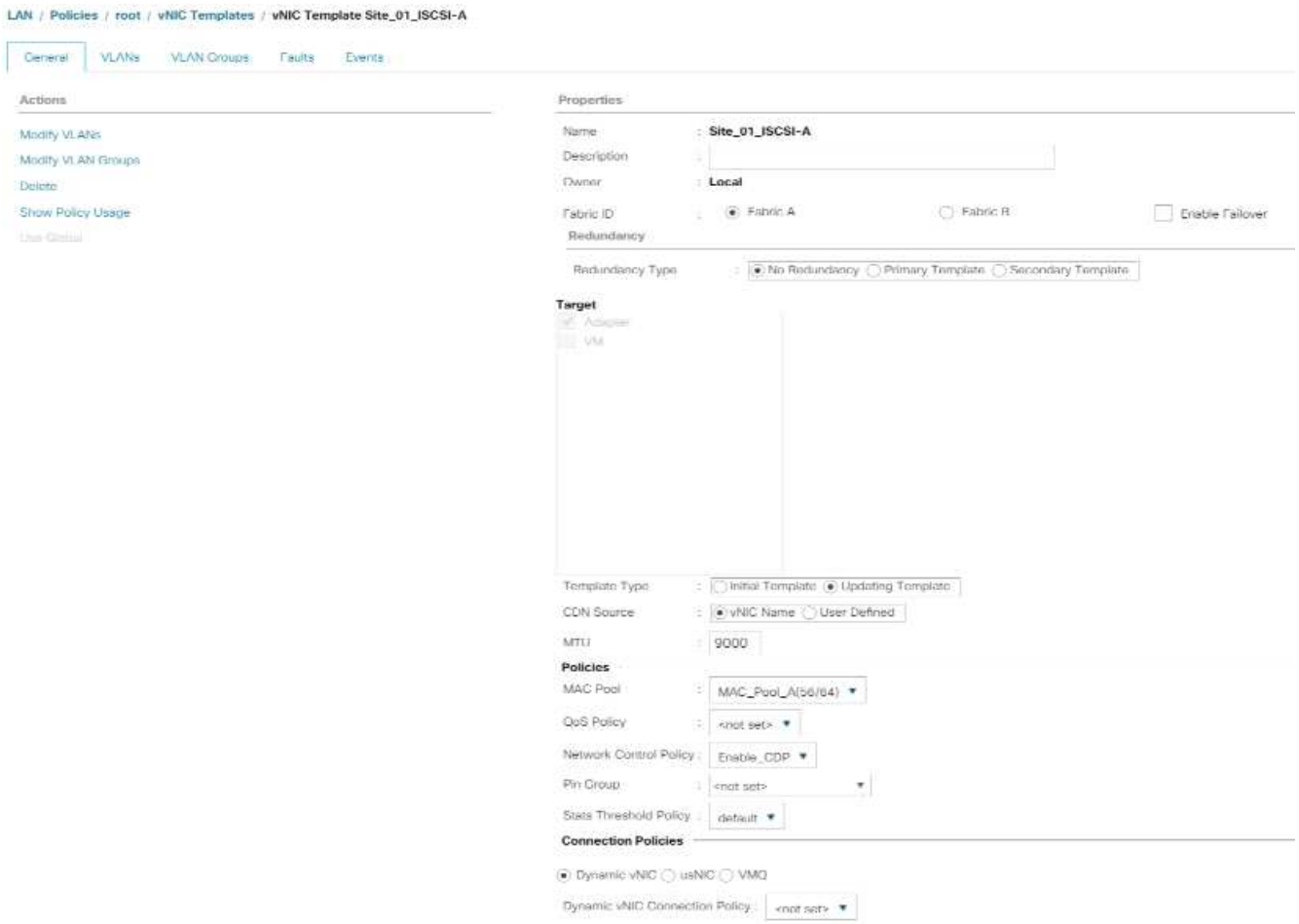
9. [冗長性タイプ] の [プライマリテンプレート] を選択します。
10. ピア冗長性テンプレートは 'vNIC_Template_A' のままにします
11. [ターゲット] で、 [アダプタ] オプションのみが選択されていることを確認します。
12. ネイティブ VLAN として 'Native - VLAN' を設定します
13. CDN ソースの vNIC 名を選択します。
14. MTU には '9000' と入力します
15. [Permitted VLANs] で、 [Native - VLAN] 、 [Site-XX-IB-MGMT] 、 [Site-XX-NFS] 、 [Site-XX-VM-Traffic] 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

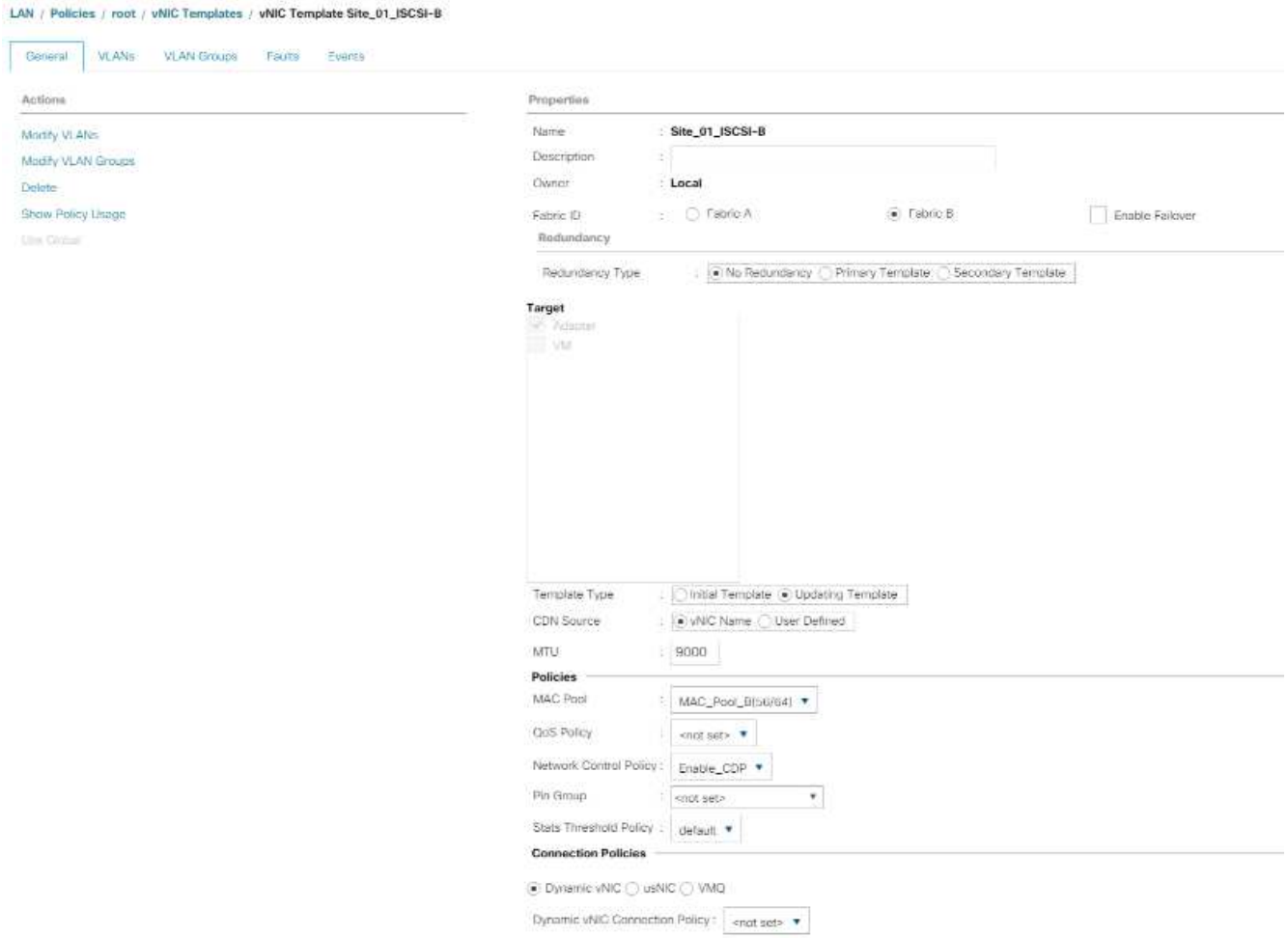
iSCSI vNIC を作成するには、次の手順を実行します。

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。



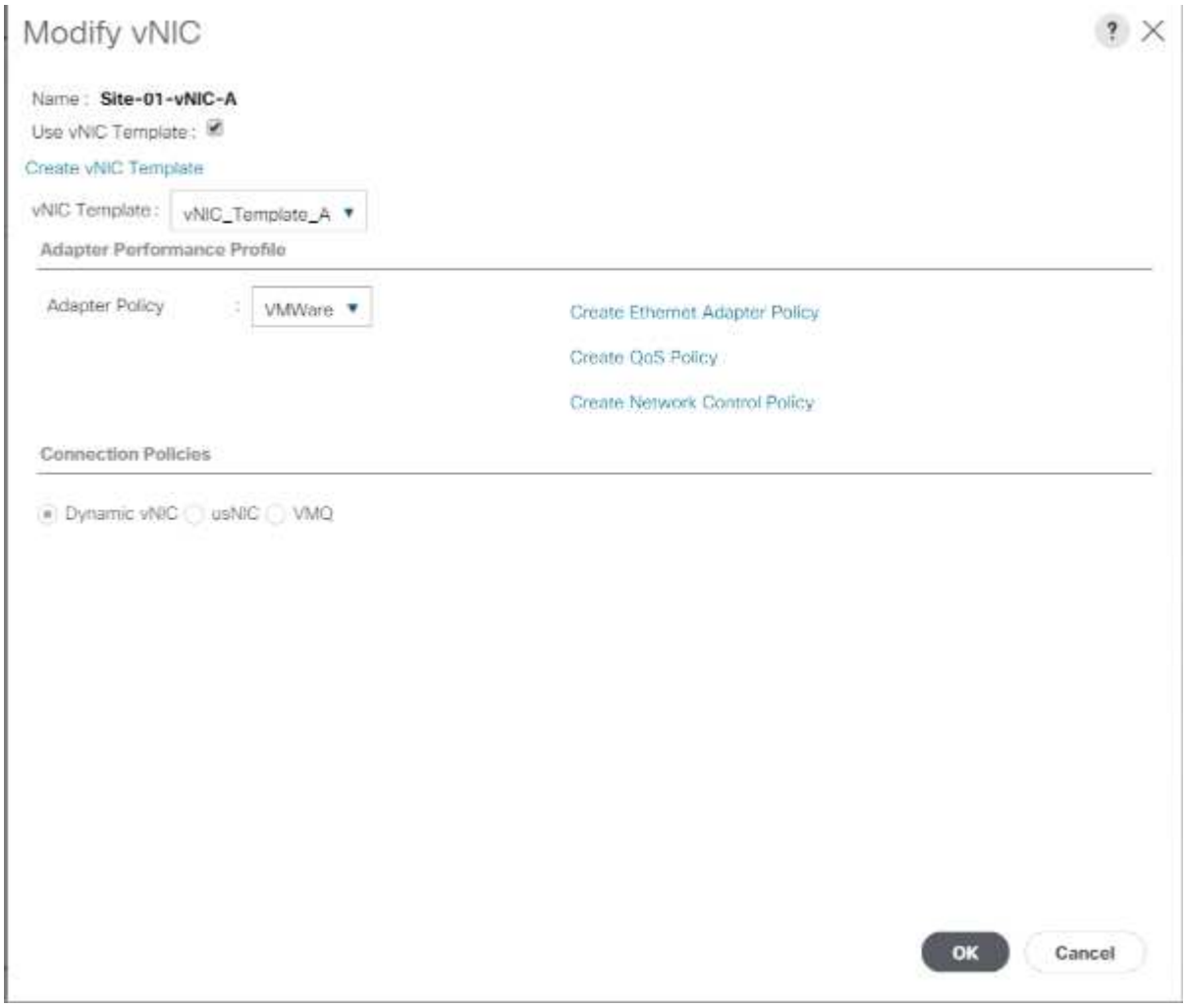
iSCSI ブート用の **LAN** 接続ポリシーを作成します

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。

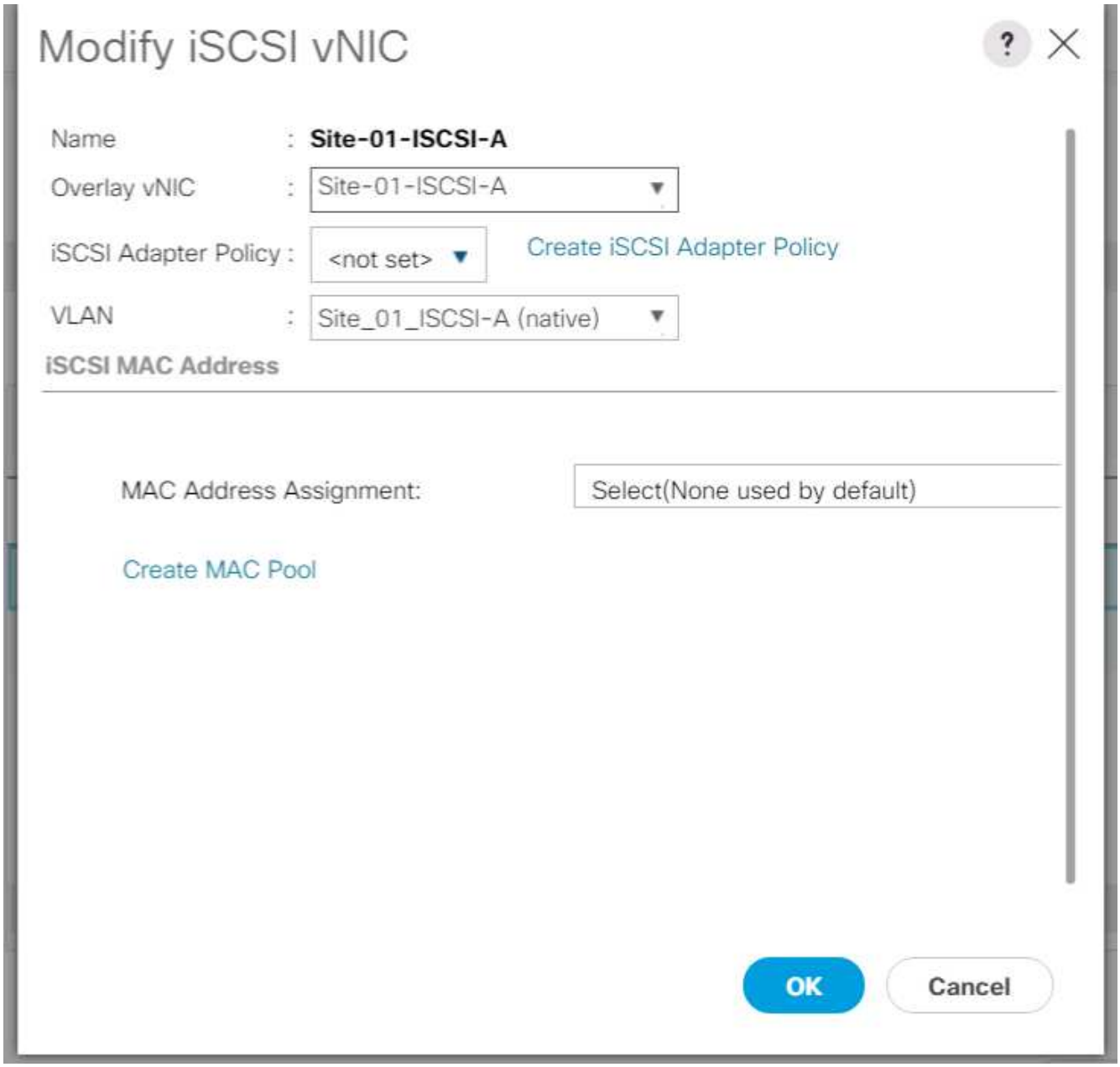
1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [LAN] > [Policies] > [root] を選択します。
3. [LAN 接続ポリシー] を右クリックします。
4. [Create LAN Connectivity Policy] を選択します。
5. ポリシー名として「 ite-XX-fFabric-a」 と入力します。
6. vNIC を追加するには、上部の Add オプションをクリックします。
7. [Create vNIC] ダイアログボックスで、 vNIC の名前として「 S`ite-01-vNIC-A` 」と入力します。

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。

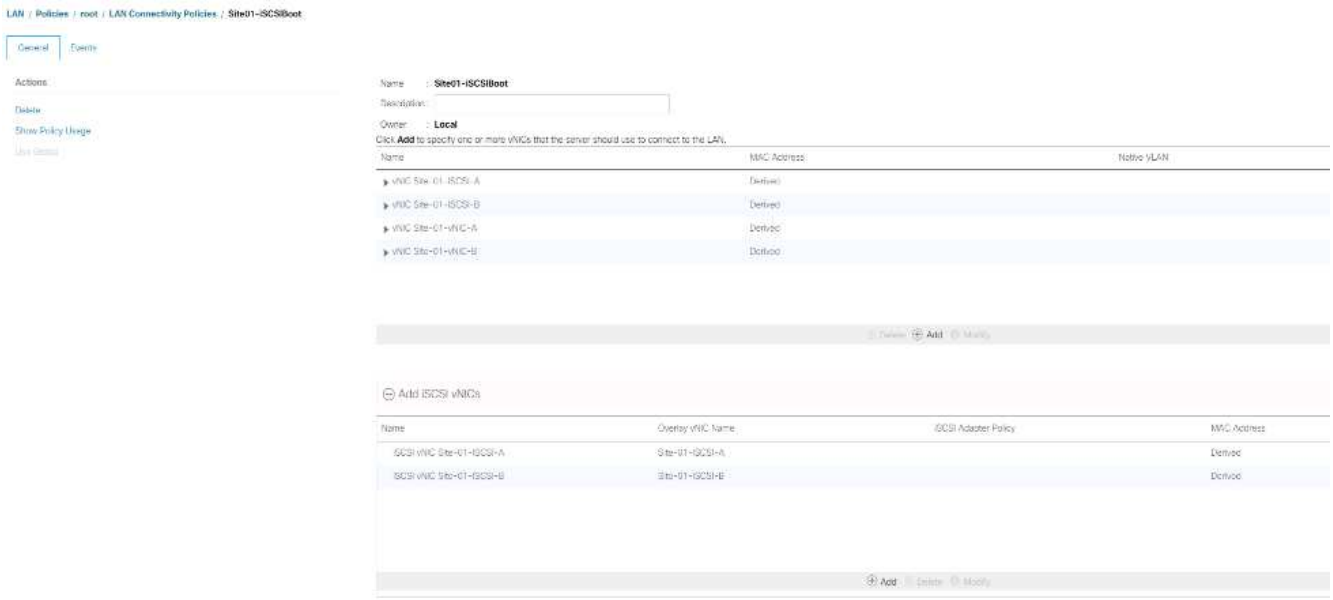


12. vNIC を追加するには、上部の Add オプションをクリックします。
13. [Create vNIC] ダイアログボックスで、 vNIC の名前として「 S`it-01-vNIC-B` 」と入力します。
14. [Use vNIC Template] オプションを選択します。
15. [vNIC Template] リストで、 [vNIC_Template_B] を選択します。
16. [Adapter Policy] ドロップダウンリストから [VMware] を選択します。
17. [OK] をクリックして、この vNIC をポリシーに追加します。
18. vNIC を追加するには、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。

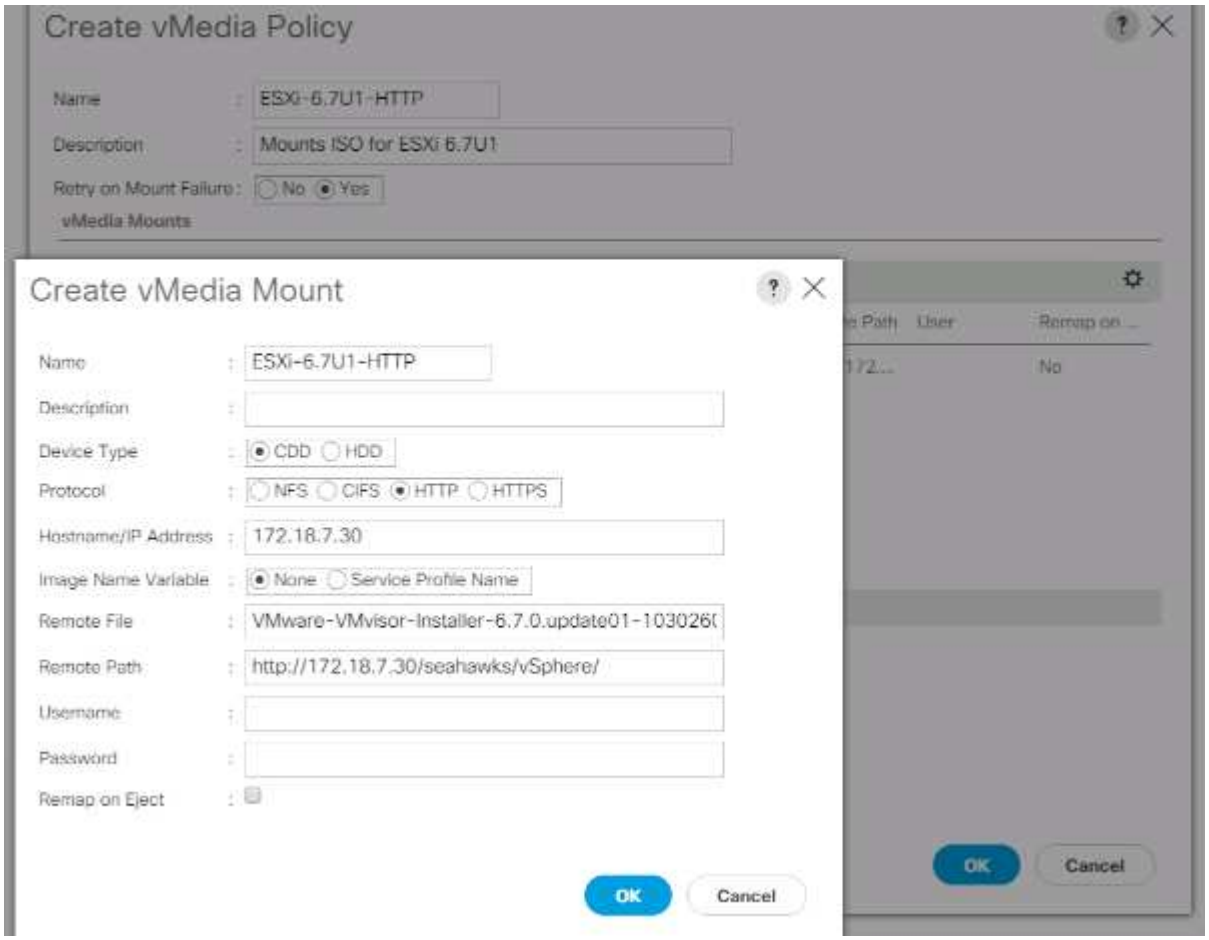
> DNS サーバの IP は KVM IP に入力されていなかったため、ホスト名ではなく Web サーバの IP を入力する必要があります。

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

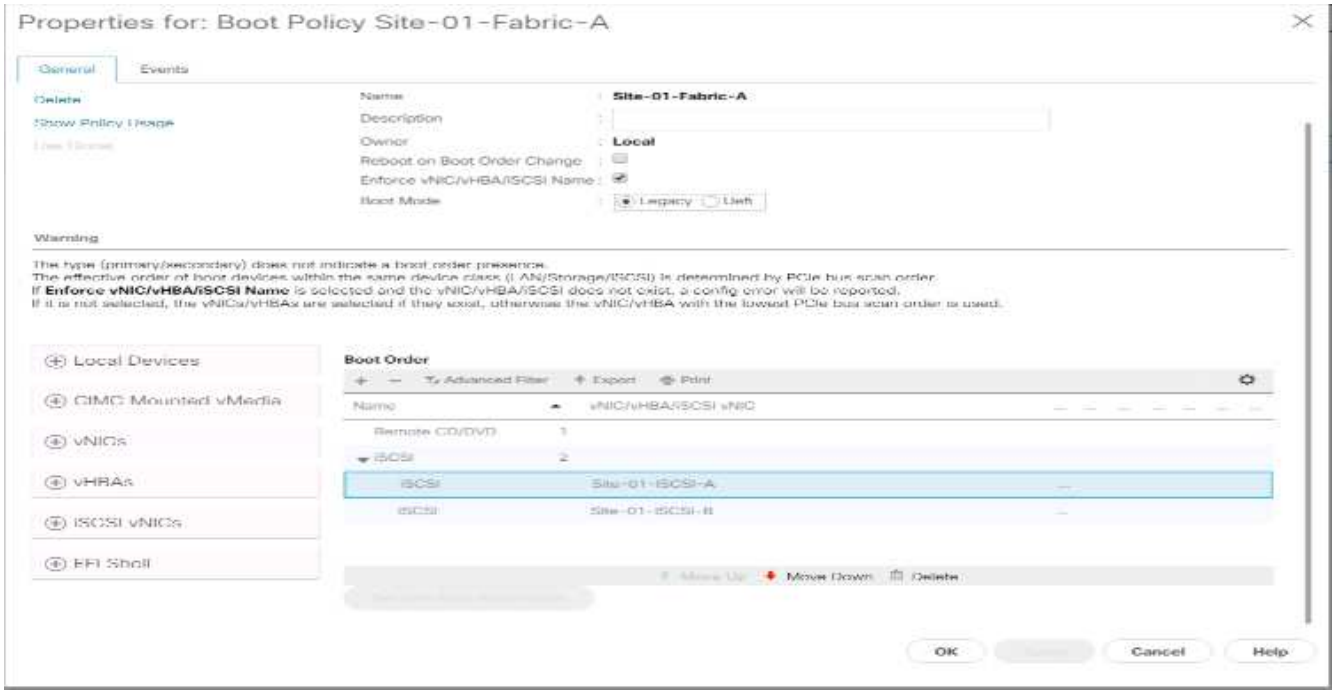
ここで説明する環境の手順は、 2 つの iSCSI 論理インターフェイス（ LIF ）がクラスタノード 1 （「 iscsi_dlif01a 」および「 iscsi_dlif01b 」）にあり、 2 つの iSCSI LIF がクラスタノード 2 （「 iscsi_dlif02a 」および「 iscsi_dlif02b 」）にある Cisco UCS 環境です。また、 A LIF がファブリック A （ Cisco UCS ファブリックインターコネクト A ）に接続され、 B LIF がファブリック B （ Cisco UCS ファブリックインターコネクト B ）に接続されていることも前提となります。

> 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。



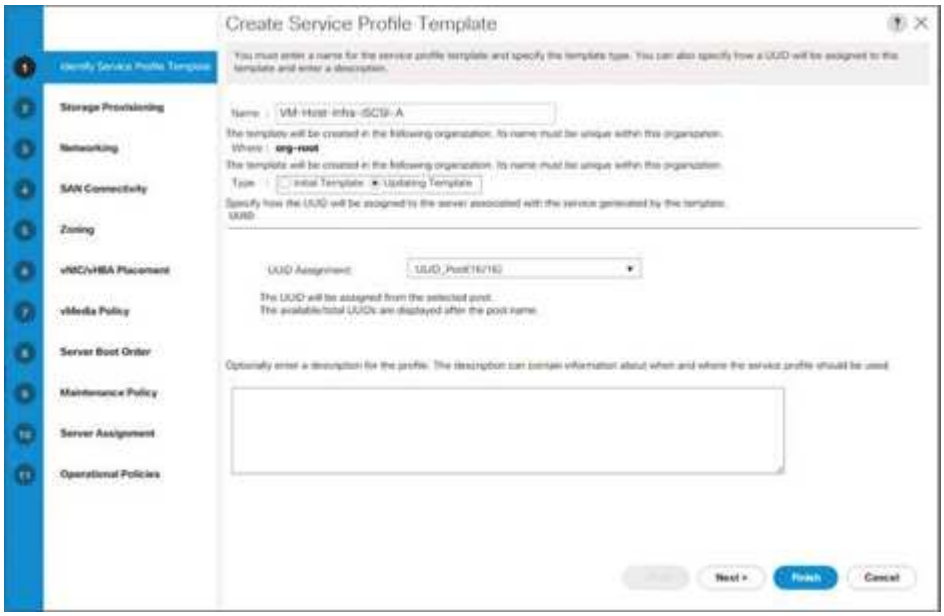
サービスプロファイルテンプレートを作成します

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

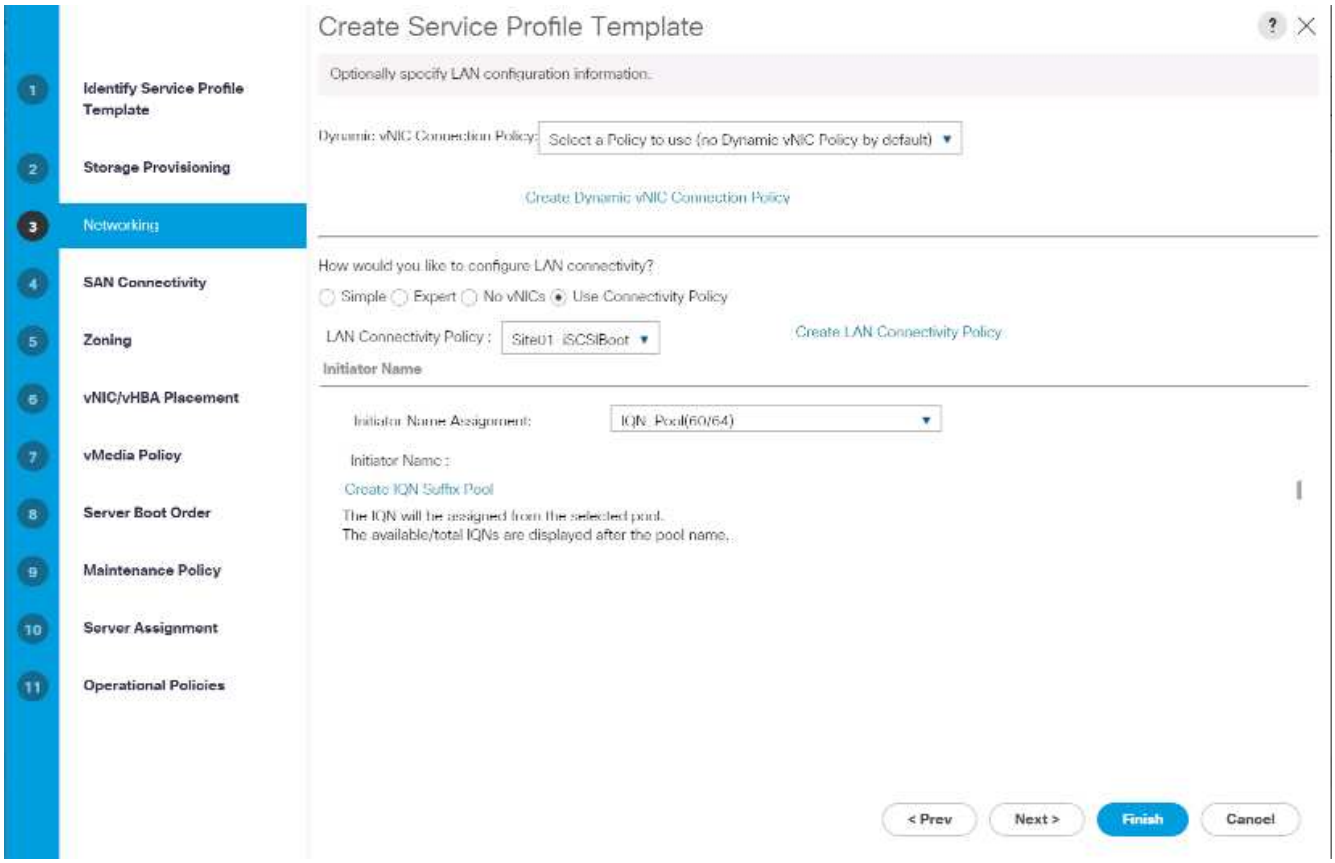
ストレージプロビジョニングを設定するには、次の手順を実行します。

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

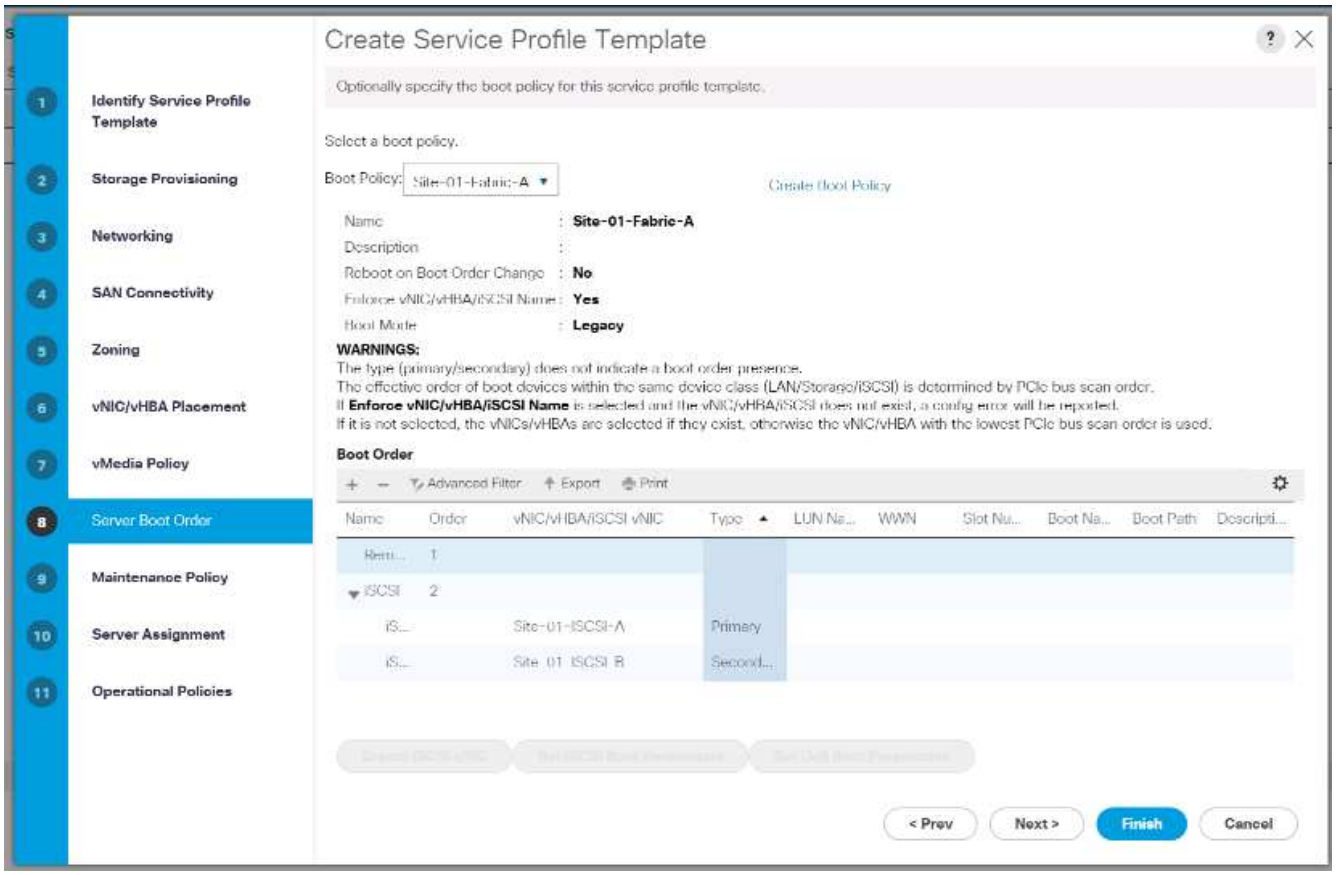
vMedia ポリシーを設定するには、次の手順を実行します。

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



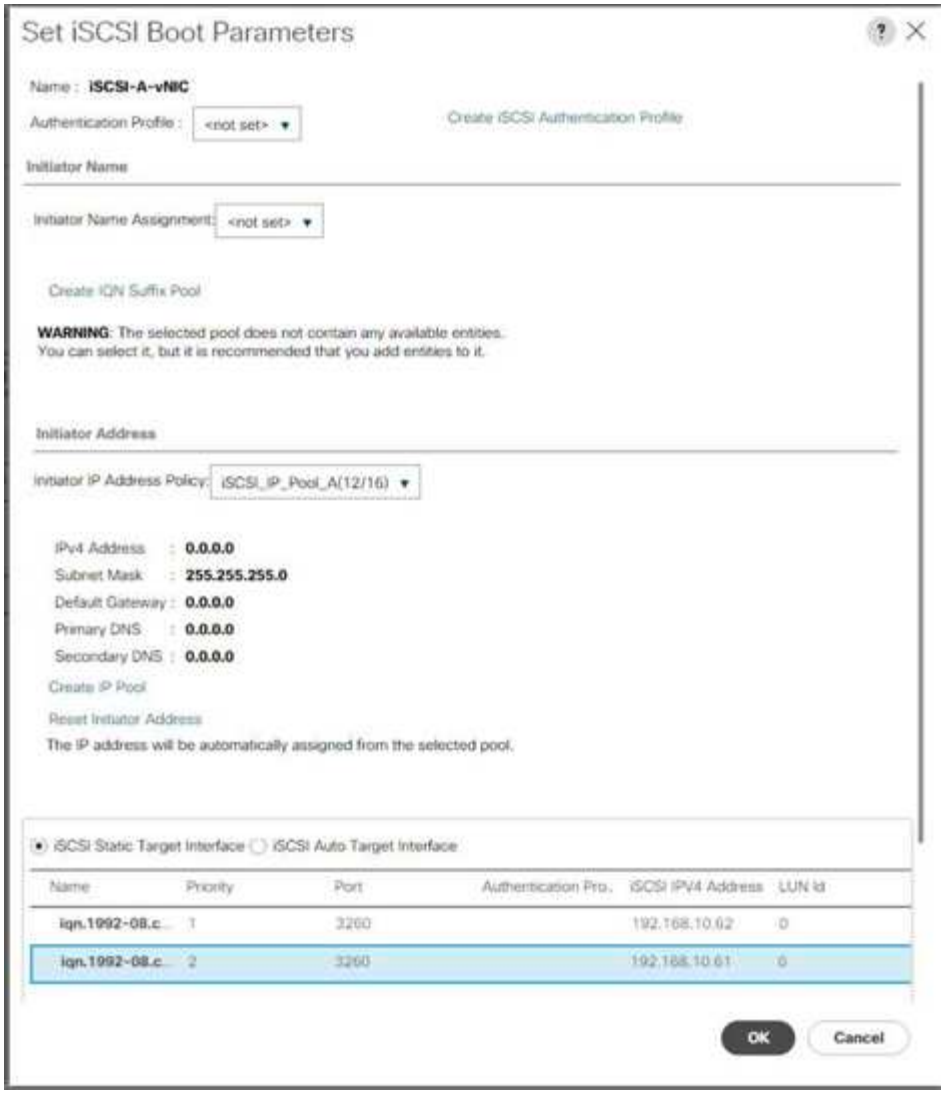
2. Boor 注文で、「ライト -01-iSCSI-A 」を選択します。
3. iSCSI 起動パラメータの設定をクリックします。
4. iSCSI ブートパラメータの設定ダイアログボックスで、環境に適した認証プロファイルを個別に作成していない限り、認証プロファイルオプションを Not Set のままにします。
5. [イニシエータ名の割り当て] ダイアログボックスは、前の手順で定義した単一のサービスプロファイルのイニシエータ名を使用するように設定されていないままにします。
6. 「 iSCSI_IP_Pool_A 」をイニシエータ IP アドレス・ポリシーとして設定します。
7. iSCSI 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。

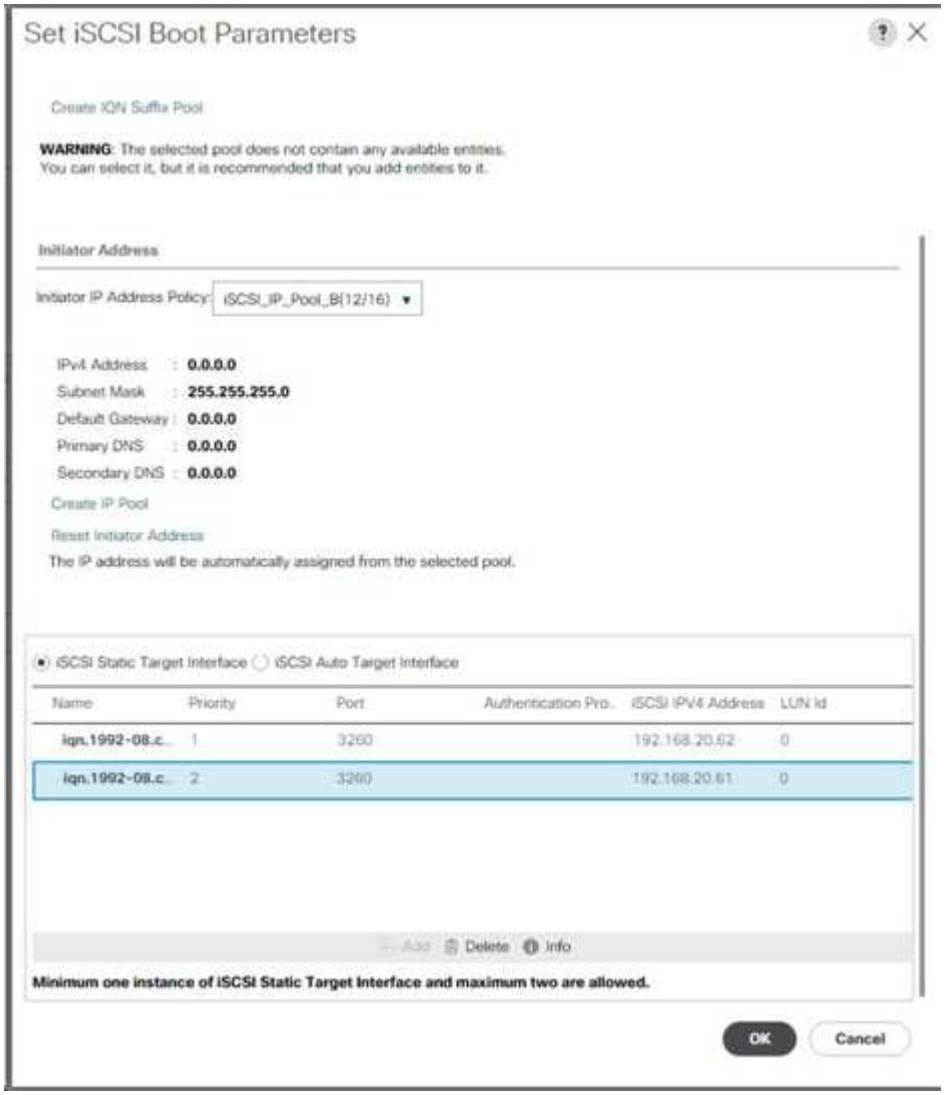
16. 起動順序で、 [iSCSI-B-vNIC] を選択します。
17. iSCSI 起動パラメータの設定をクリックします。
18. iSCSI ブートパラメータの設定ダイアログボックスで、環境に適した認証プロファイルを個別に作成していない限り、認証プロファイルオプションは Not Set のままにします。
19. [イニシエータ名の割り当て] ダイアログボックスは、前の手順で定義した単一のサービスプロファイルのイニシエータ名を使用するように設定されていないままにします。
20. イニシエータの IP アドレス・ポリシーとして 'iSCSI_IP_Pool_B' を設定します
21. iSCSI 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。

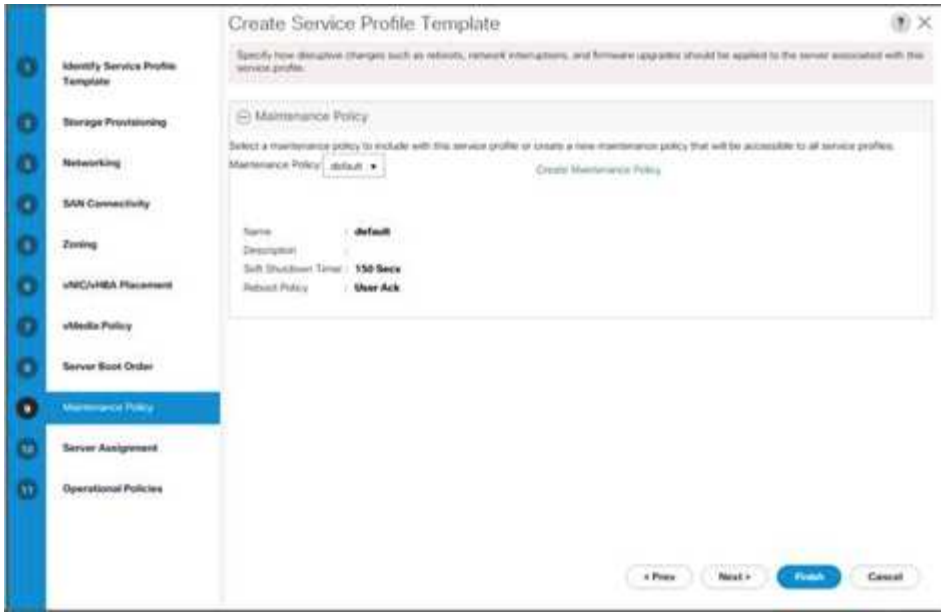


30. 次へをクリックします。

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。

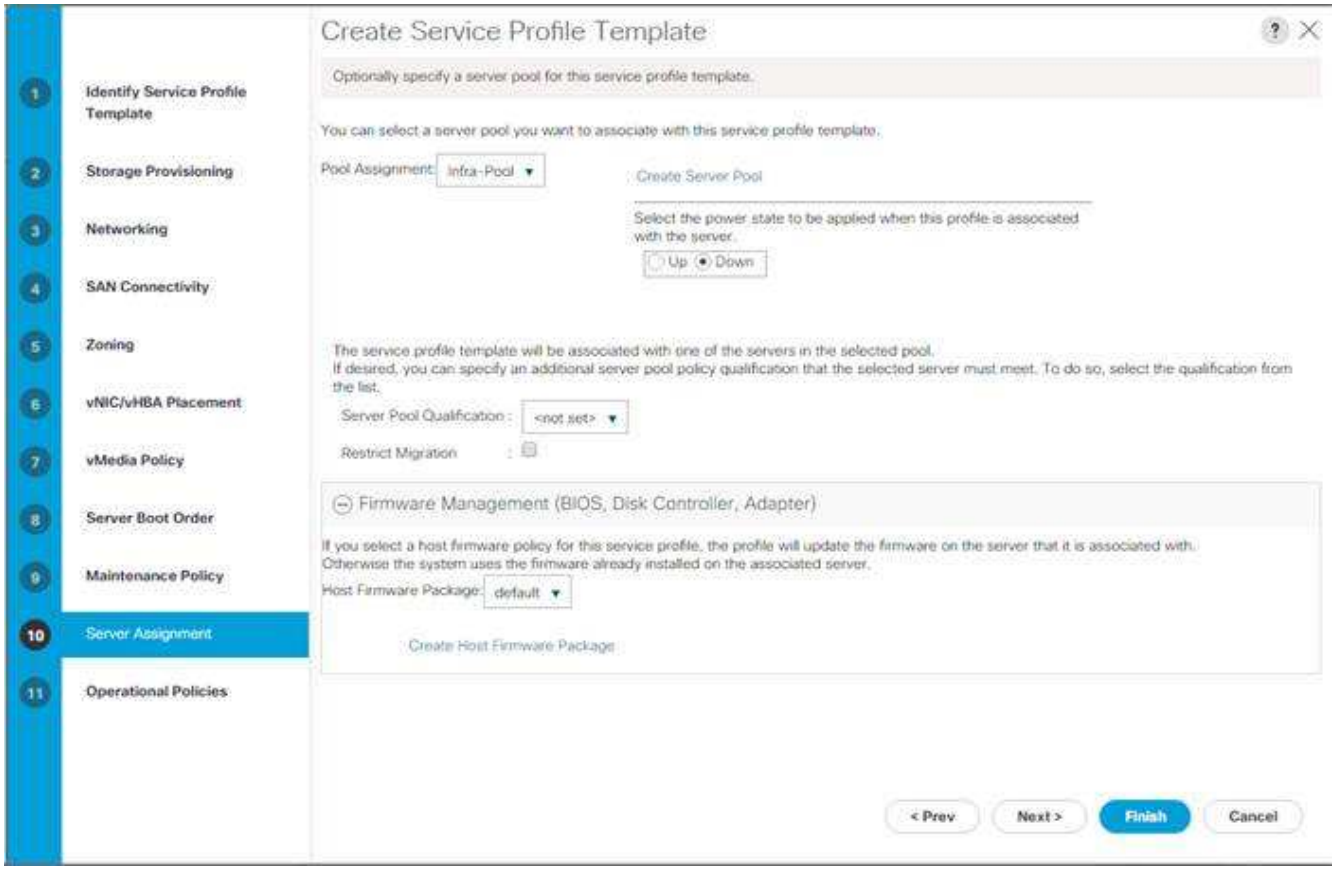


2. 次へをクリックします。

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。

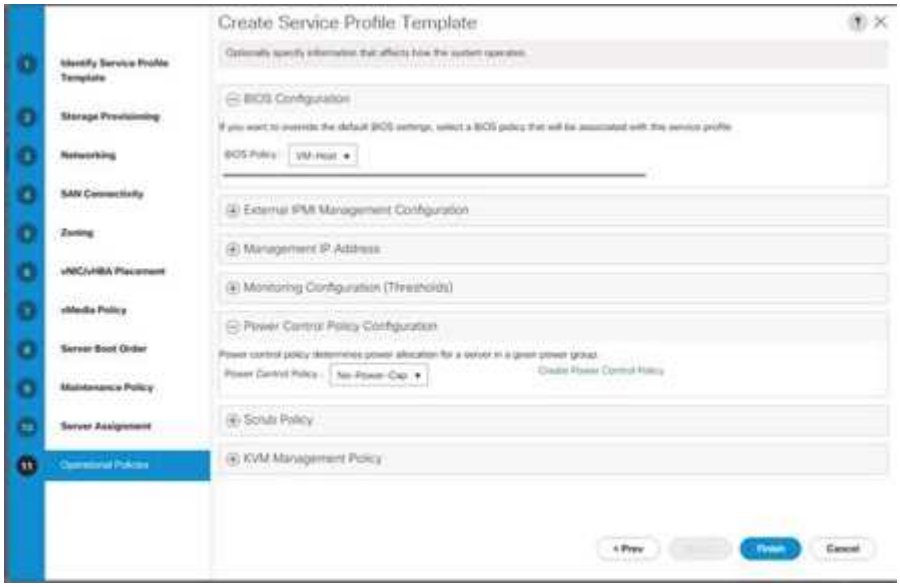


4. 次へをクリックします。

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

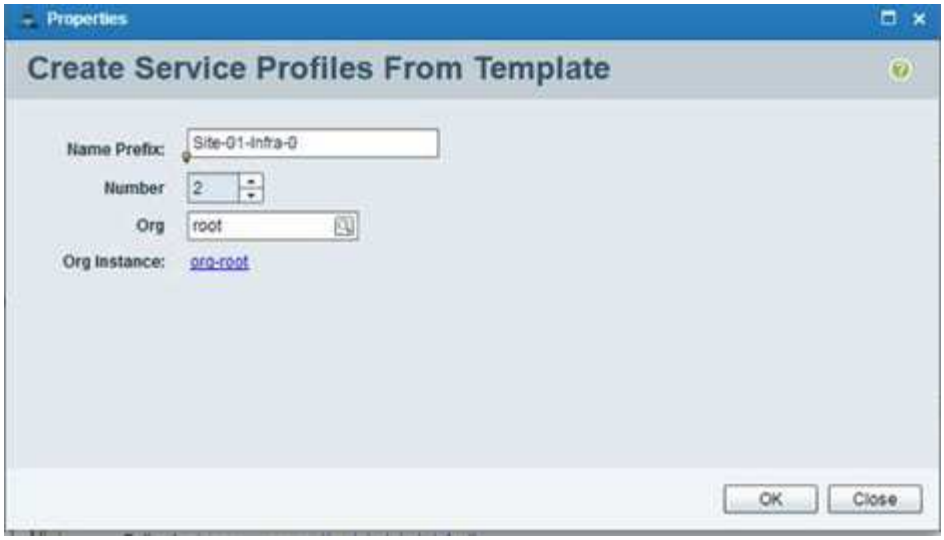
vMedia を有効にしてサービスプロファイルテンプレートを作成するには、次の手順を実行します。

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。

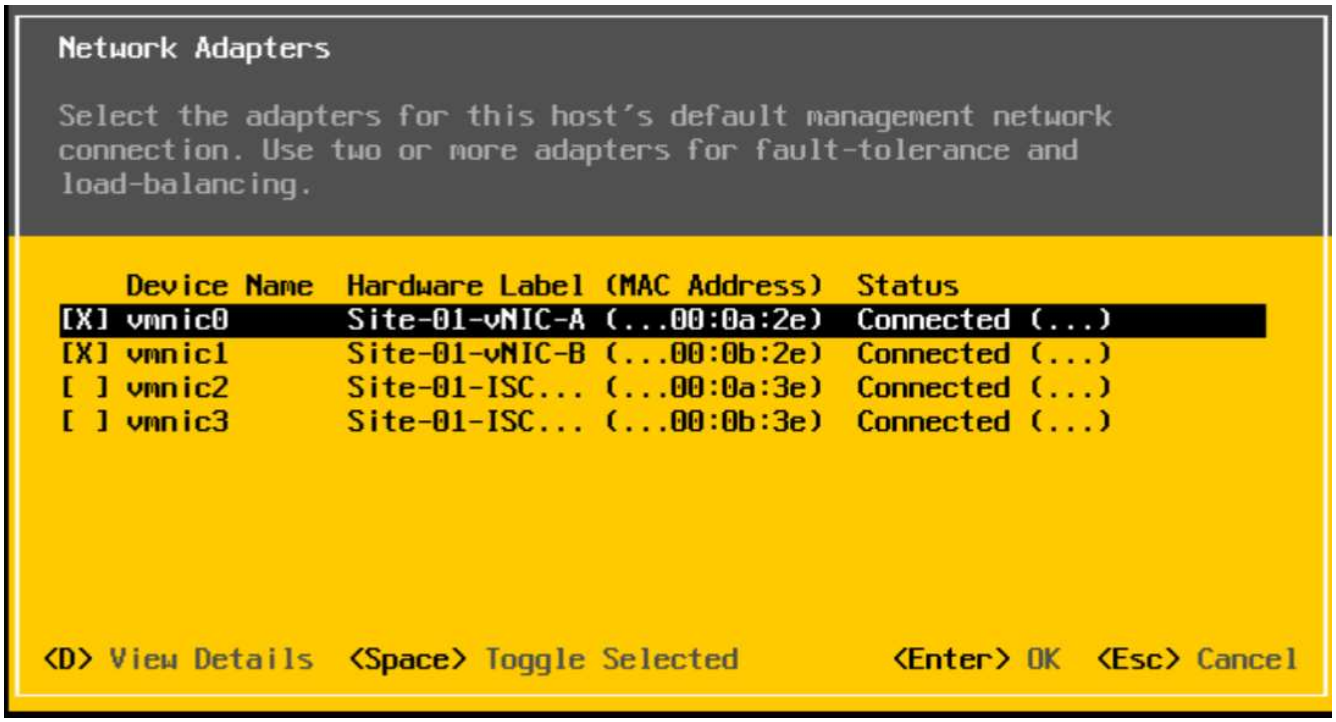
ESXi ホストの管理ネットワークをセットアップします

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

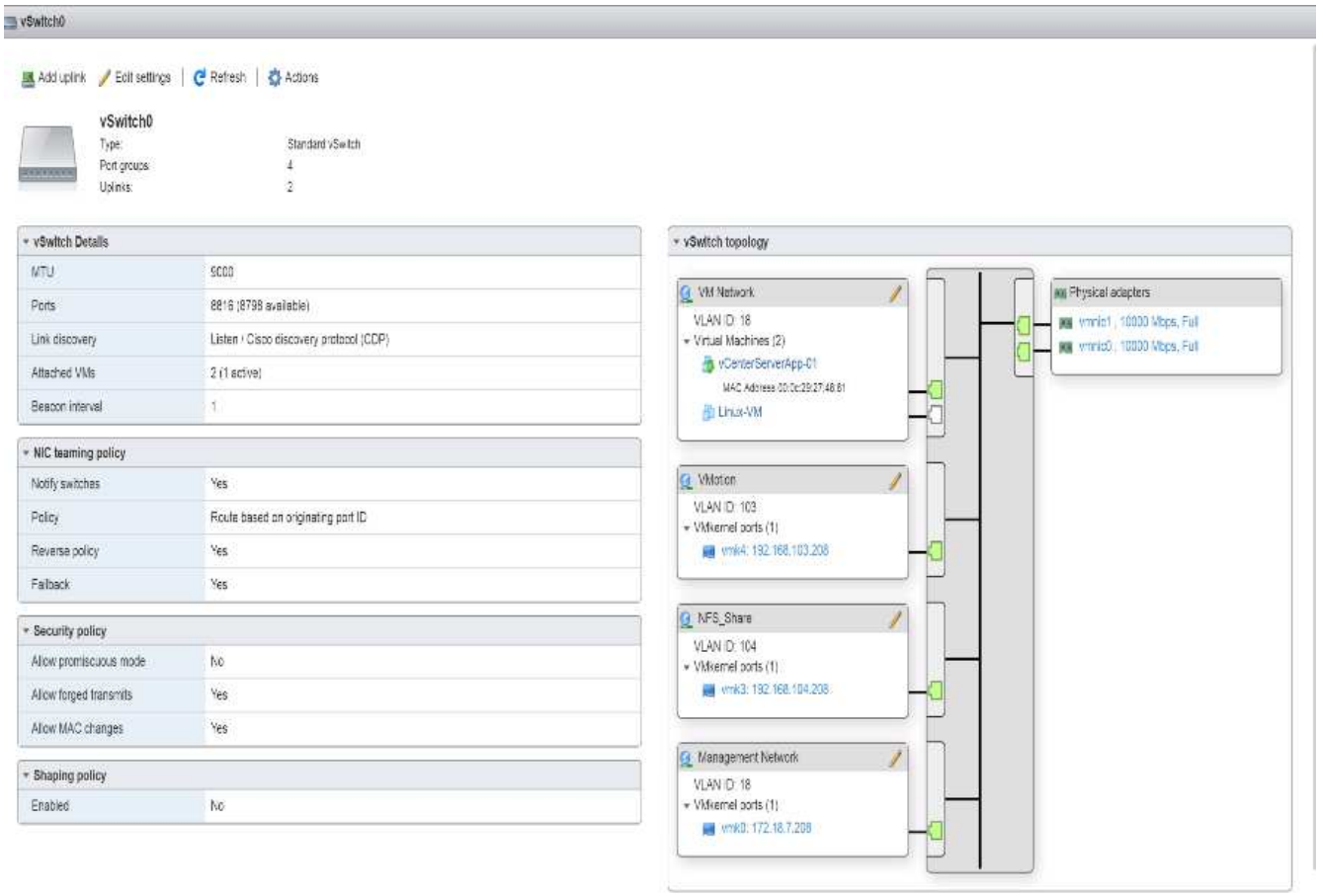
> Cisco UCS iSCSI IP プールアドレスを再割り当てする必要がある場合に IP アドレスの競合を回避するには、 iSCSI VMkernel ポートに対して同じサブネット内の異なる IP アドレスを使用することを推奨します。

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。

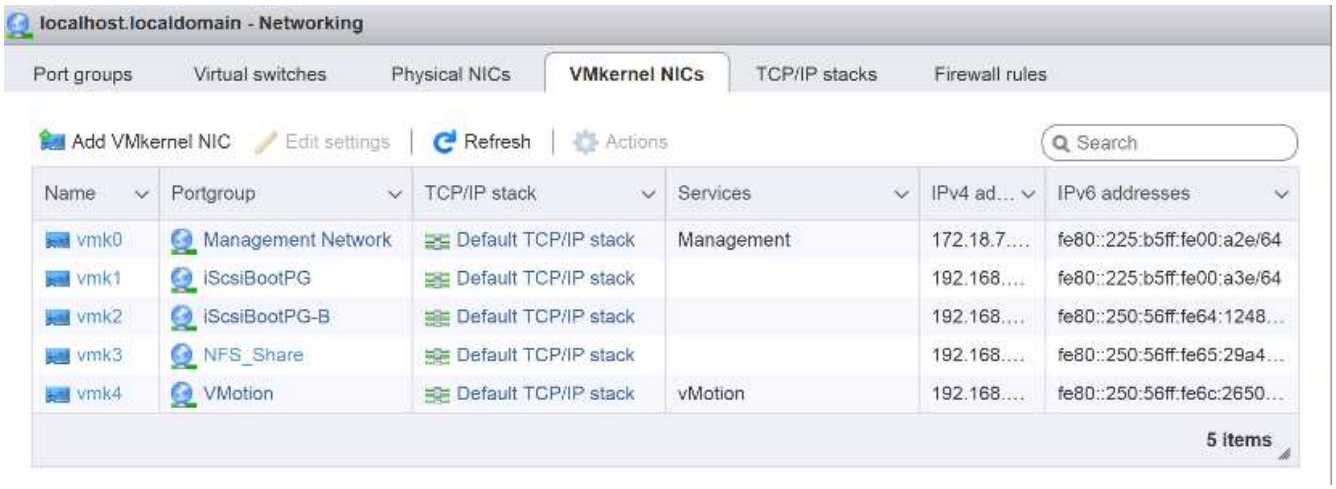
> IP アドレスの競合を避けるため、 Cisco UCS iSCSI IP プールアドレスを再割り当てする必要がある場合は、 iSCSI VMkernel ポートに対して同じサブネット内の異なる IP アドレスを使用することを推奨します。

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。



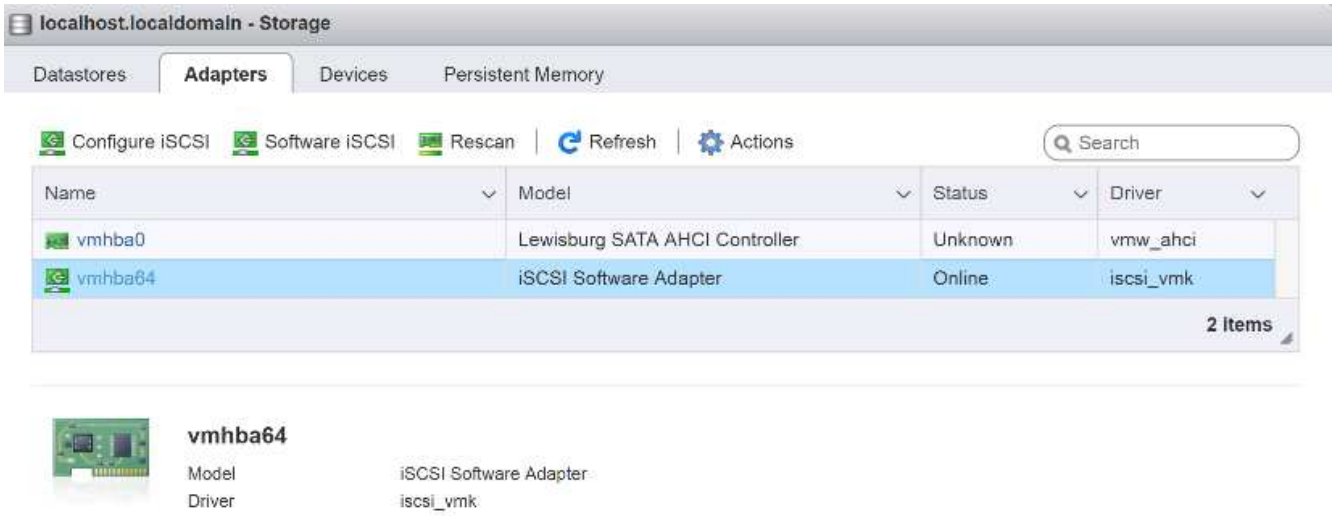
iSCSI マルチパスをセットアップします

ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

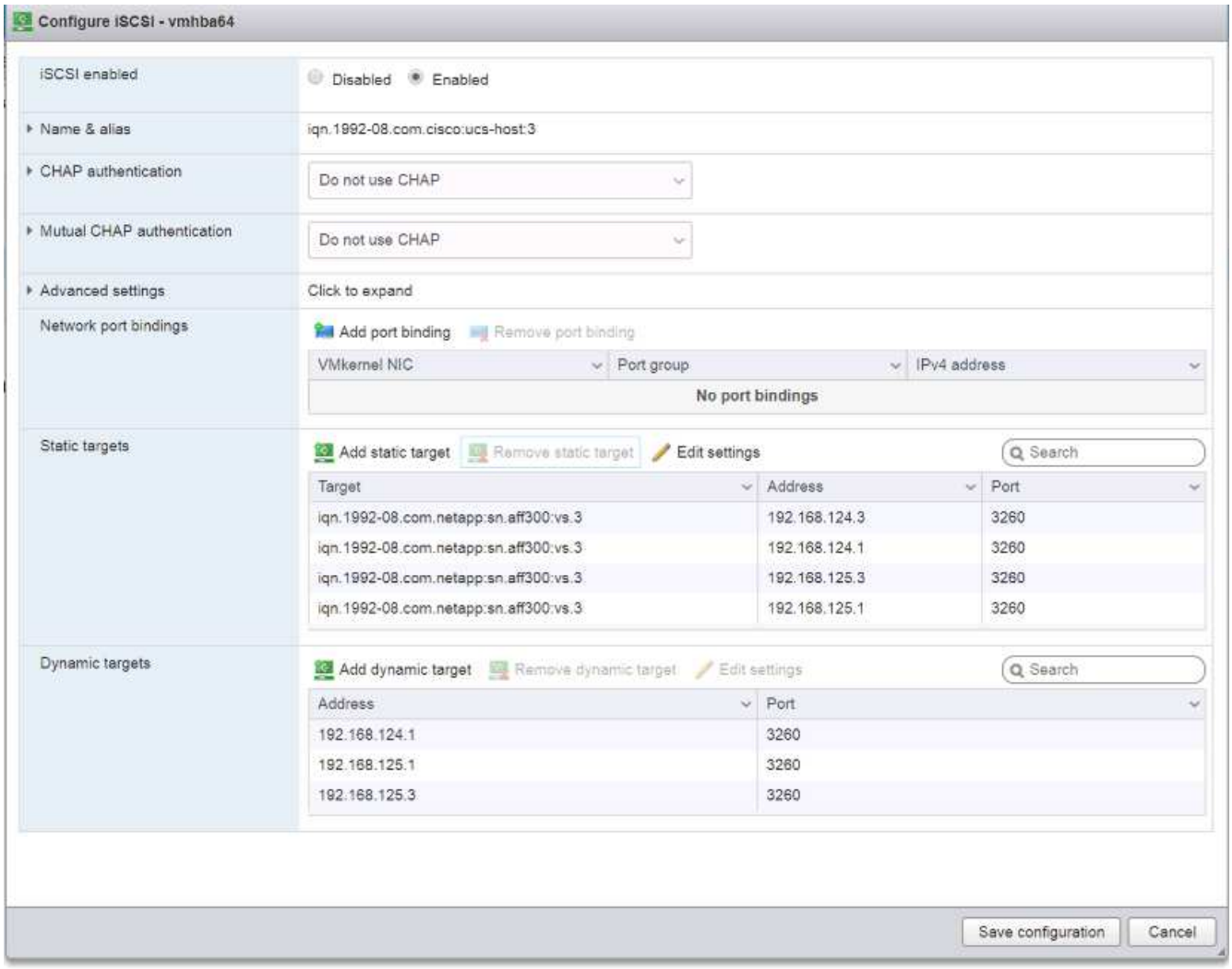
ESXi ホスト VM-Host-Infra-01 および VM-Host-Infra-02 で iSCSI マルチパスを設定するには、次の手順を実行します。

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。

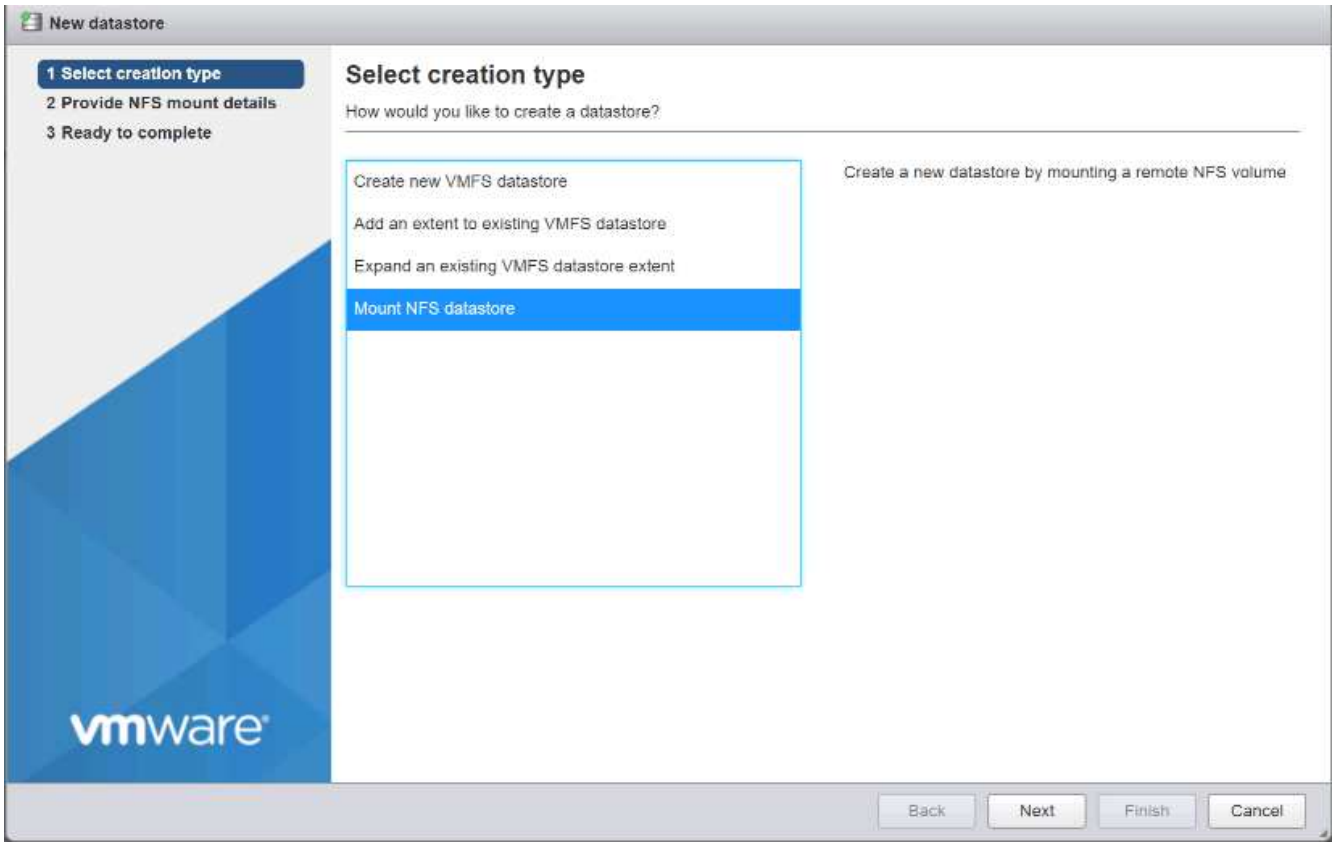
ホストが自動的にストレージアダプタとターゲットを再スキャンし、静的ターゲットに追加します。

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。

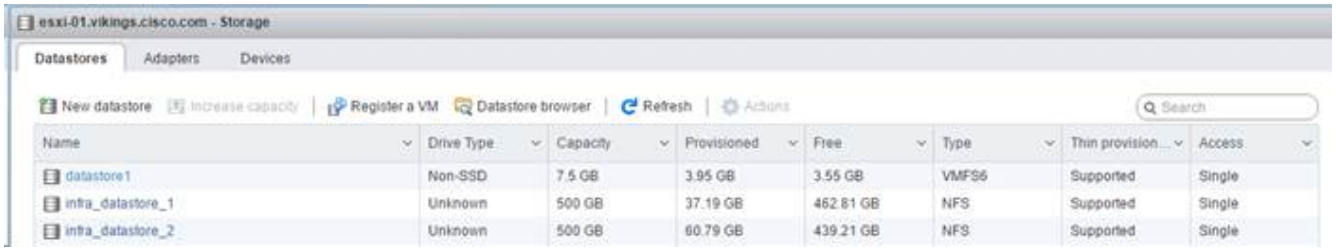
1. ホスト・クライアントで ' 左側の Storage を選択します
2. 中央のペインで、 [Datastores] を選択します。
3. 中央のペインで、 New Datastore （新規データストア）を選択して新しいデータストアを追加します。
4. [新規データストア] ダイアログボックスで、 [NFS データストアのマウント] を選択し、 [次へ] をクリックします。



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。



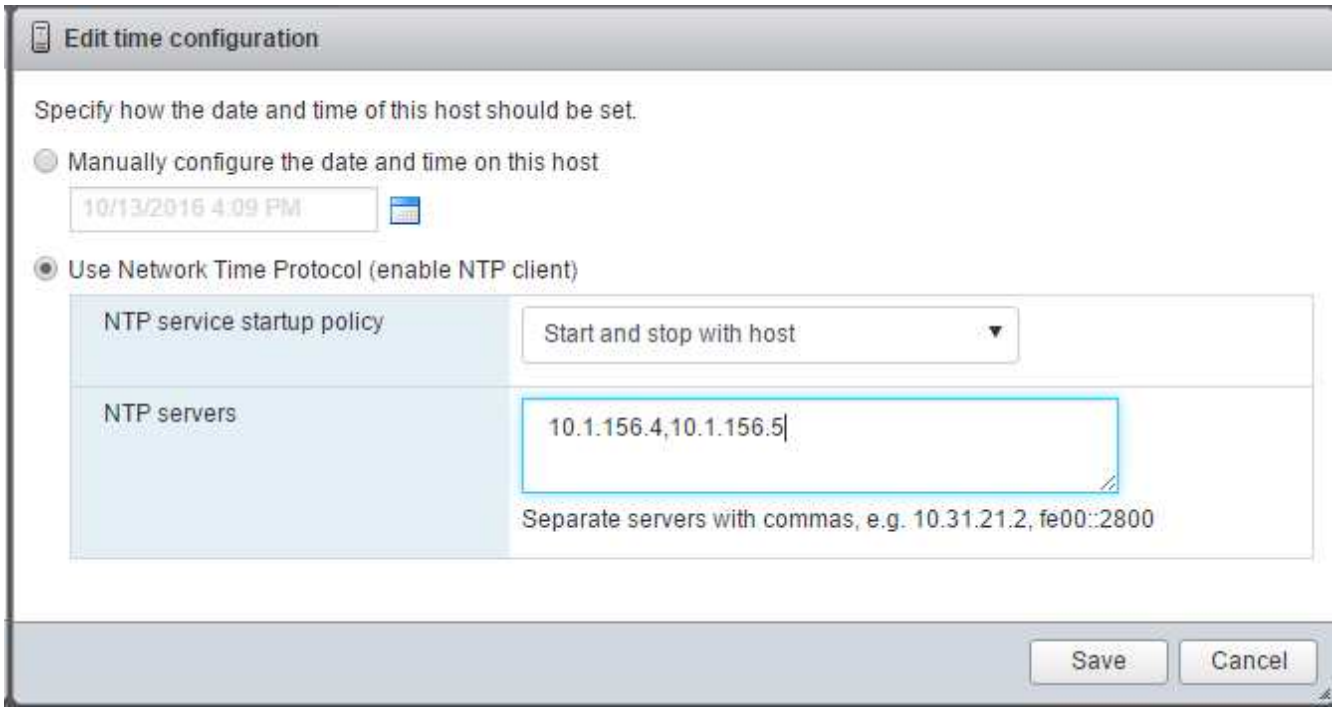
11. 両方の ESXi ホストに両方のデータストアをマウントします。

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

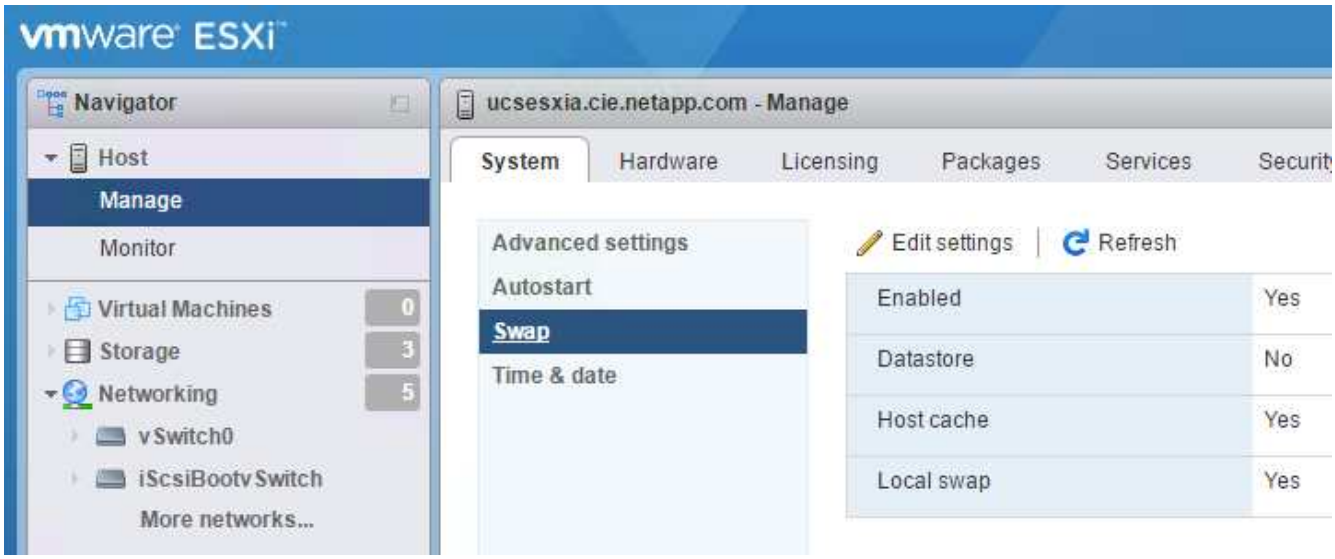
NTP サーバの時間はホストの時間とは多少異なる場合があります。

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

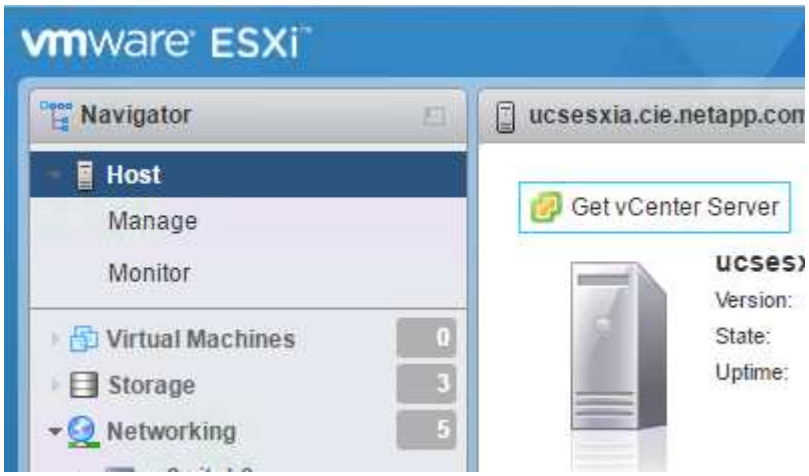
このセクションでは、 FlexPod 構成に VMware vCenter Server 6.7 をインストールする詳細な手順について説明します。

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。

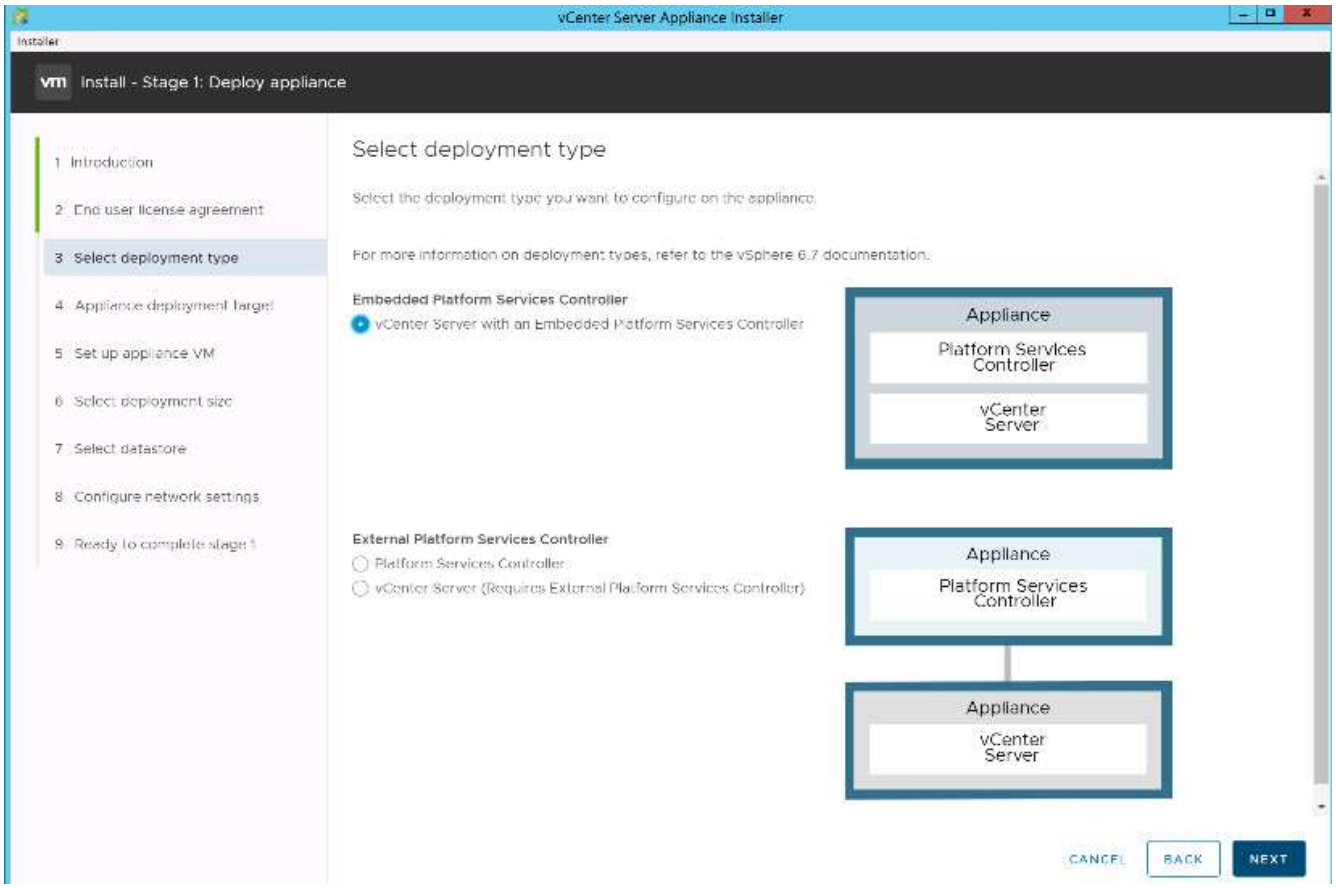
1. vCSA をダウンロードします。ESXi ホストの管理時に Get vCenter Server アイコンをクリックして、ダウンロードリンクにアクセスします。



2. vCSA を VMware サイトからダウンロードします。

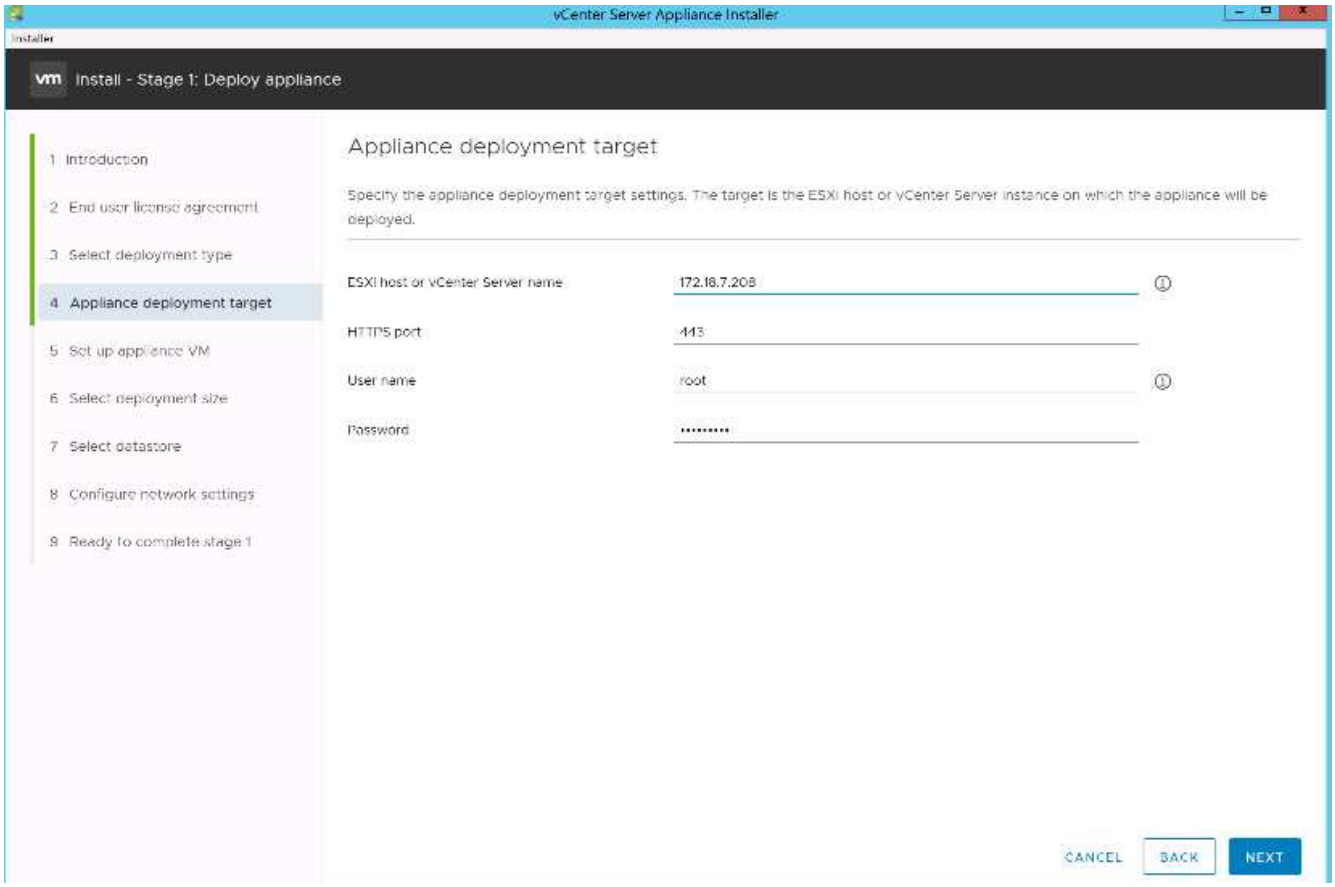
インストール可能な Microsoft Windows vCenter Server がサポートされますが、 VMware では新しい導入に vCSA を推奨します。

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。

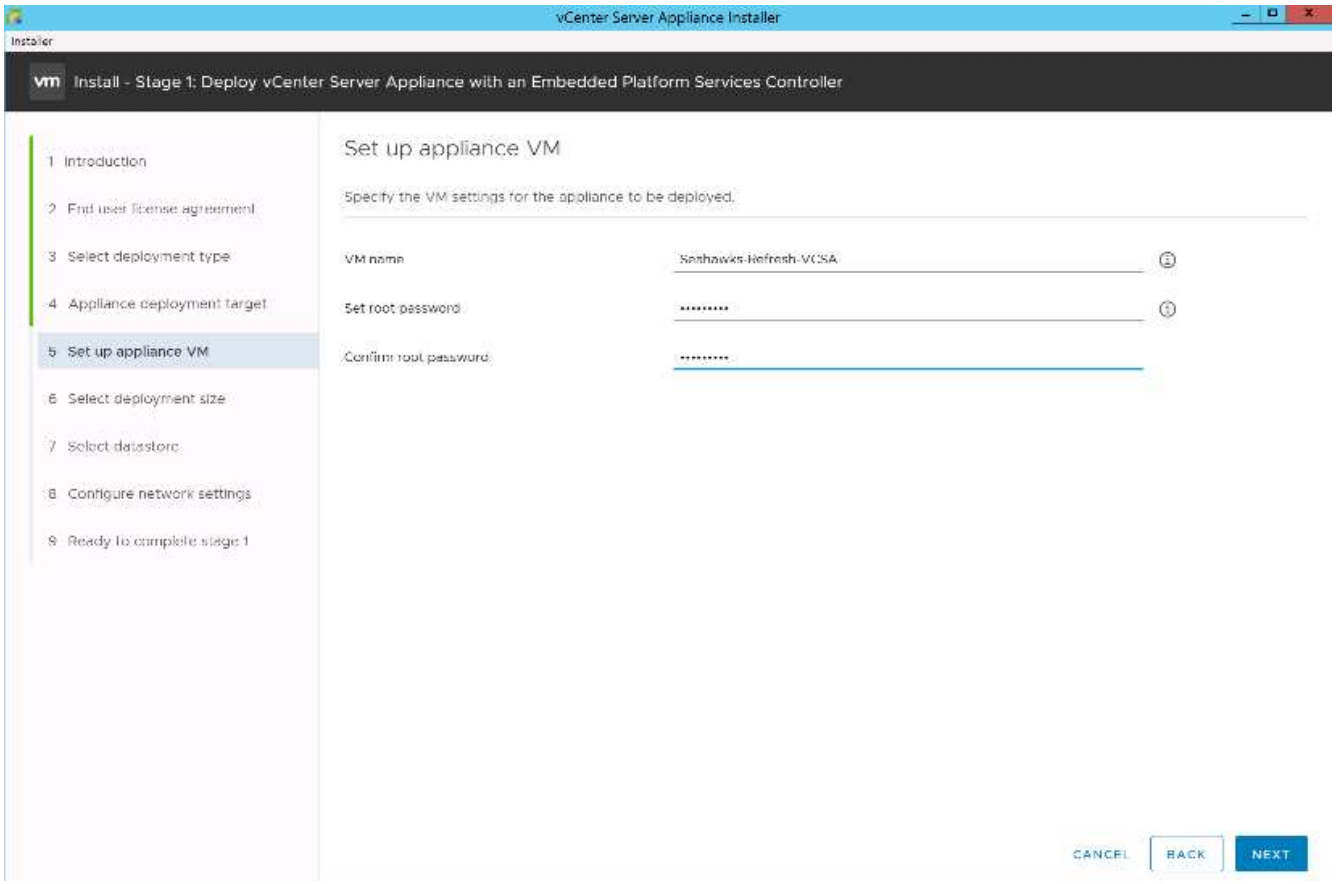


必要に応じて、 FlexPod Express 解決策の一部として、外部プラットフォームサービスコントローラの導入もサポートされます。

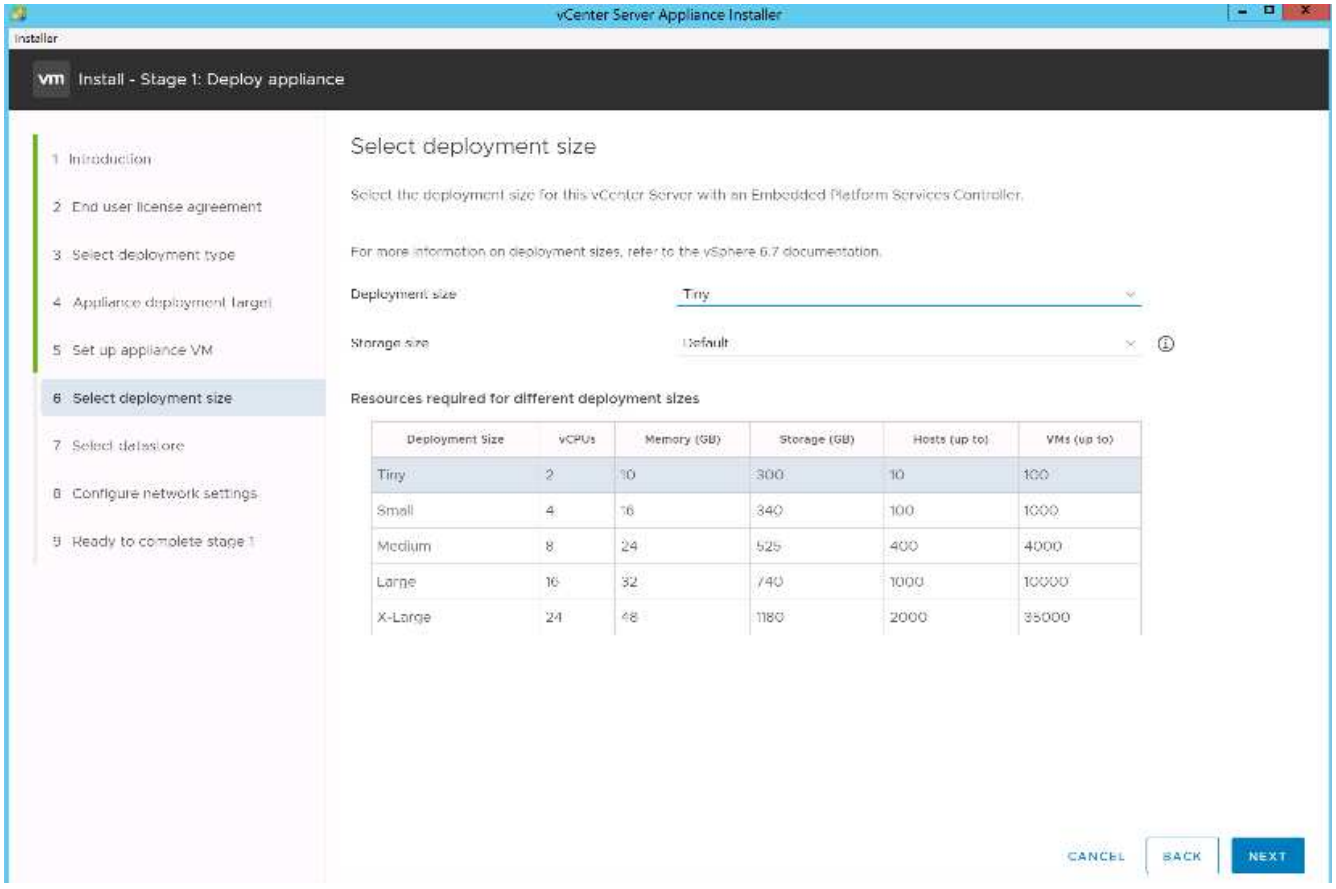
9. アプライアンス導入ターゲットページで、導入した ESXi ホストの IP アドレス、ルートユーザ名、および root パスワードを入力します。次へをクリックします。



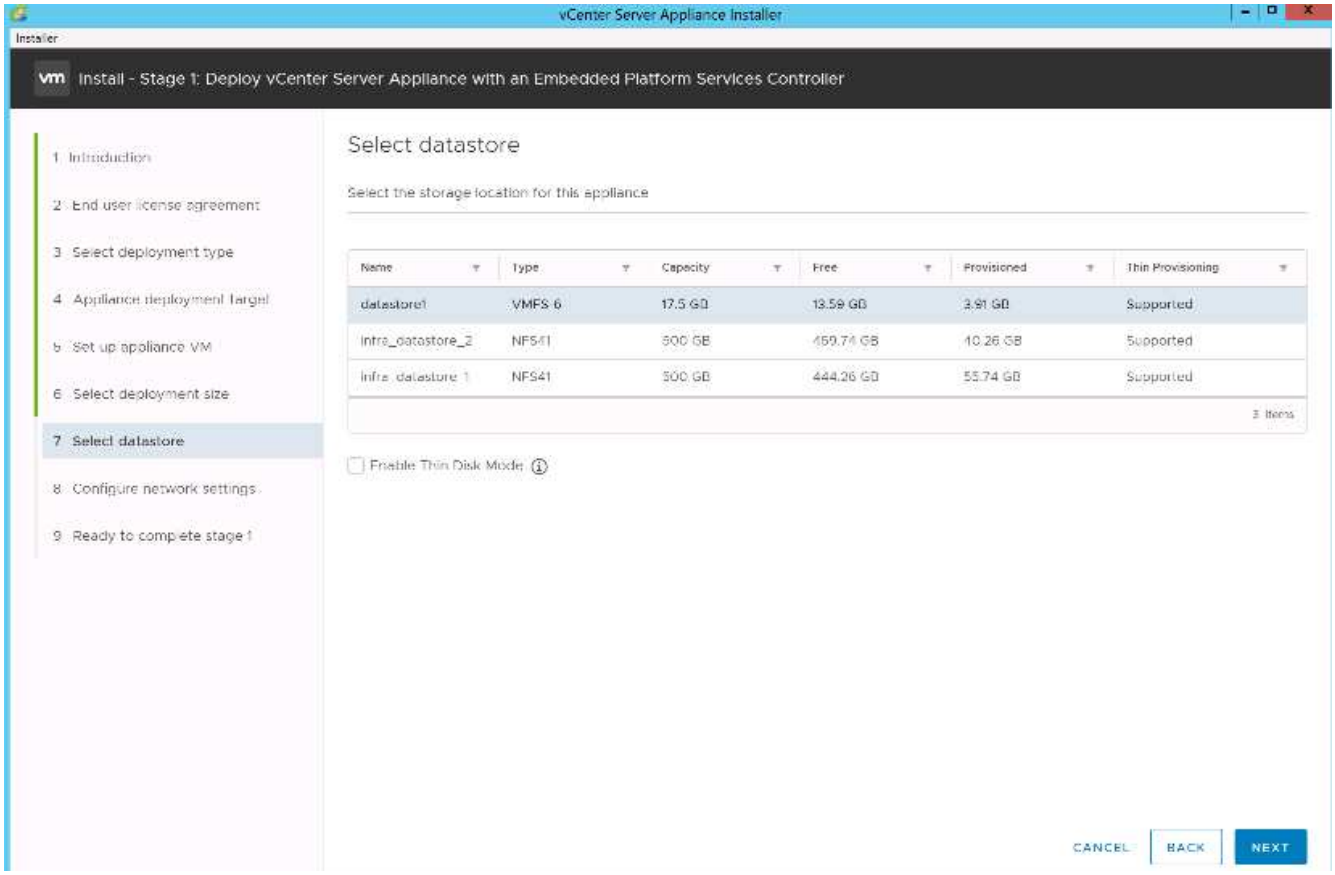
10. vCSA に VM 名および vCSA に使用するルートパスワードとして VCSA を入力して、アプライアンス VM を設定します。次へをクリックします。



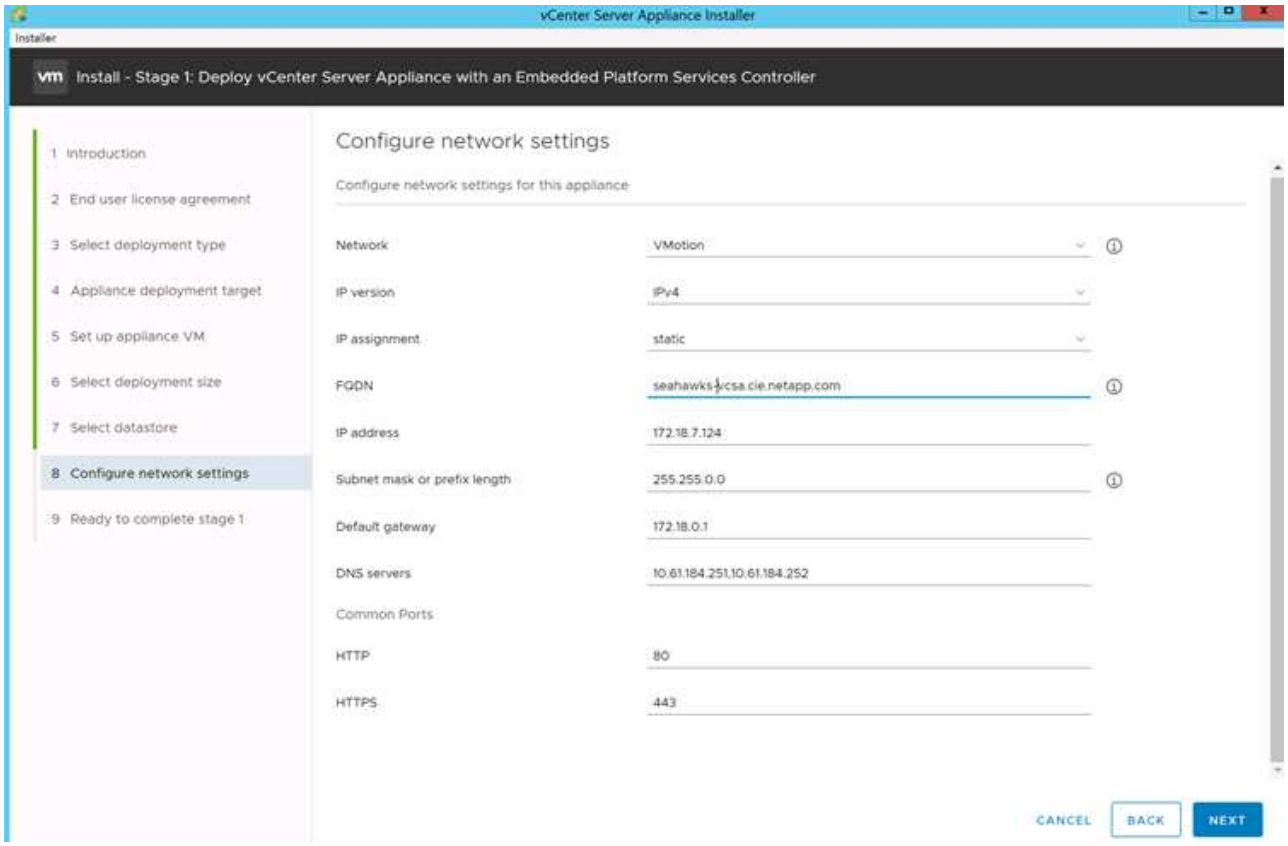
11. 環境に最も適した導入サイズを選択してください。次へをクリックします。



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。



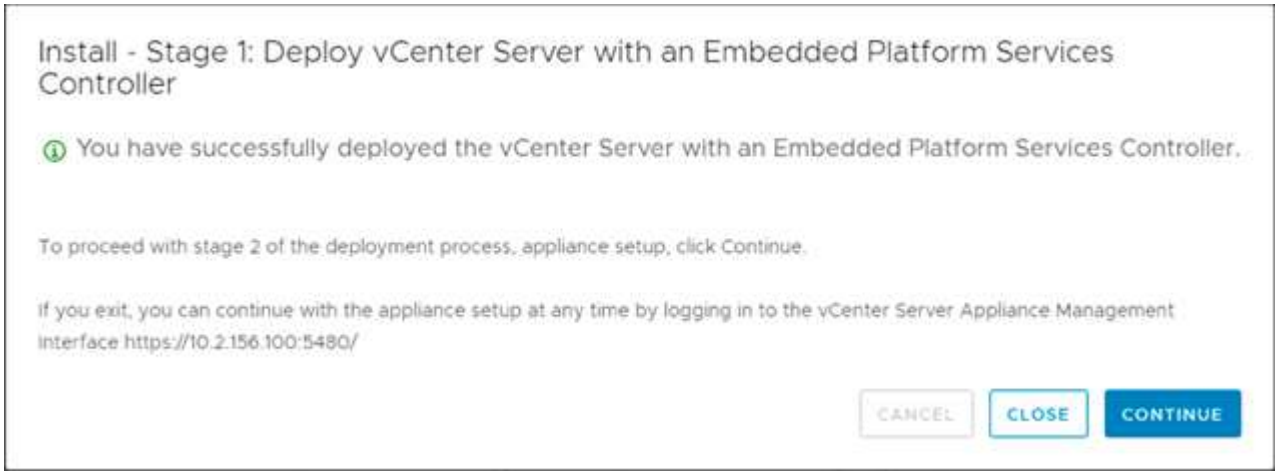
13. [Configure Network Settings] ページで次の情報を入力し、 [Next] をクリックします。
    a. ネットワークとして MGMT-Network を選択します。
    b. vCSA に使用する FQDN または IP を入力します。
    c. 使用する IP アドレスを入力します。
    d. 使用するサブネットマスクを入力します。
    e. デフォルトゲートウェイを入力します。
    f. DNS サーバを入力します。



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。

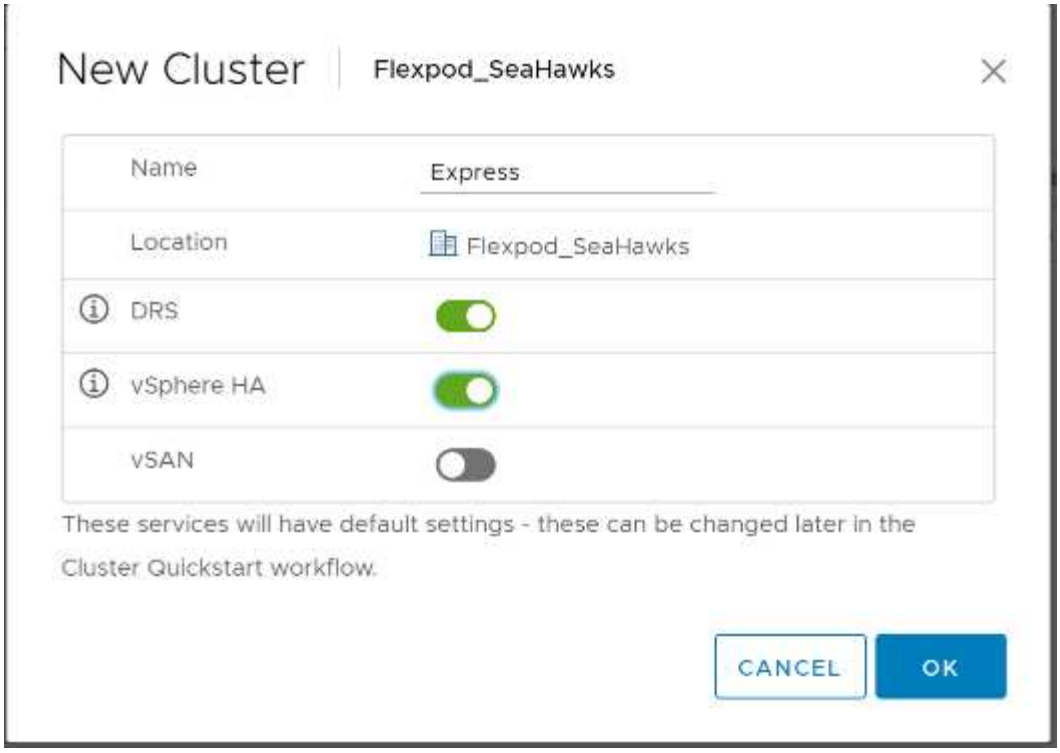
VMware vCenter Server 6.7 および **vSphere** クラスタリングを設定する

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。

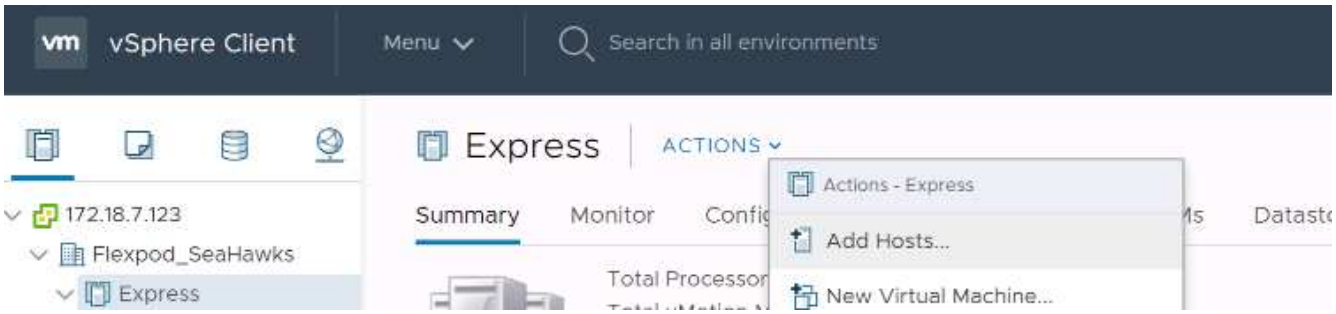
1. 新しく作成したデータセンターを右クリックし、 [New Cluster] を選択します。
2. クラスタの名前を入力します。
3. DRS と vSphere HA のオプションを選択して有効にします。
4. [OK] をクリックします。



◦ 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"