



# 『 FlexPod Express with Cisco UCS C Series and AFF A220 Series Deployment Guide 』

FlexPod

NetApp  
March 25, 2024

This PDF was generated from [https://docs.netapp.com/ja-jp/flexpod/express/express-c-series-aff220-deploy\\_program\\_summary.html](https://docs.netapp.com/ja-jp/flexpod/express/express-c-series-aff220-deploy_program_summary.html) on March 25, 2024. Always check docs.netapp.com for the latest.

# 目次

『 FlexPod Express with Cisco UCS C Series and AFF A220 Series Deployment Guide 』	1
NVA-1123-deploy : FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 deployment guide 』	1
解決策の概要	1
テクノロジー要件	4
FlexPod エクスプレスクーブル接続情報	5
導入手順	8
まとめ	83
追加情報の参照先	83

# 『 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:[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、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ー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ーを基盤とした、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

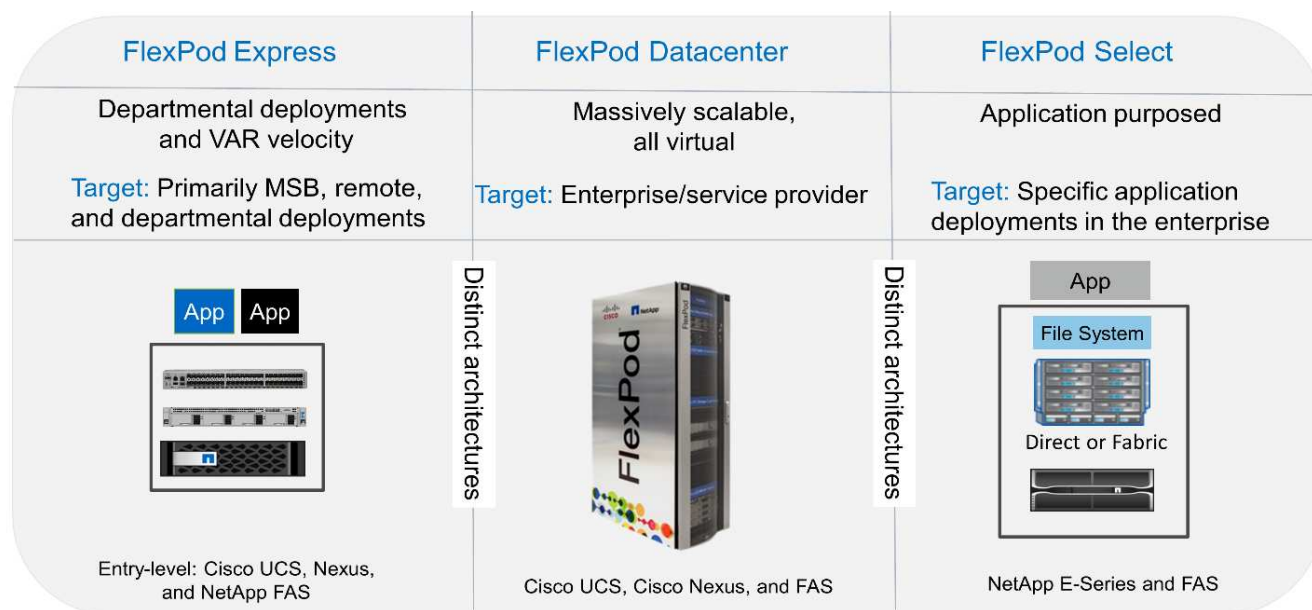
この FlexPod Express 解決策は、FlexPod コンバージドインフラプログラムの一部です。

### 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ー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

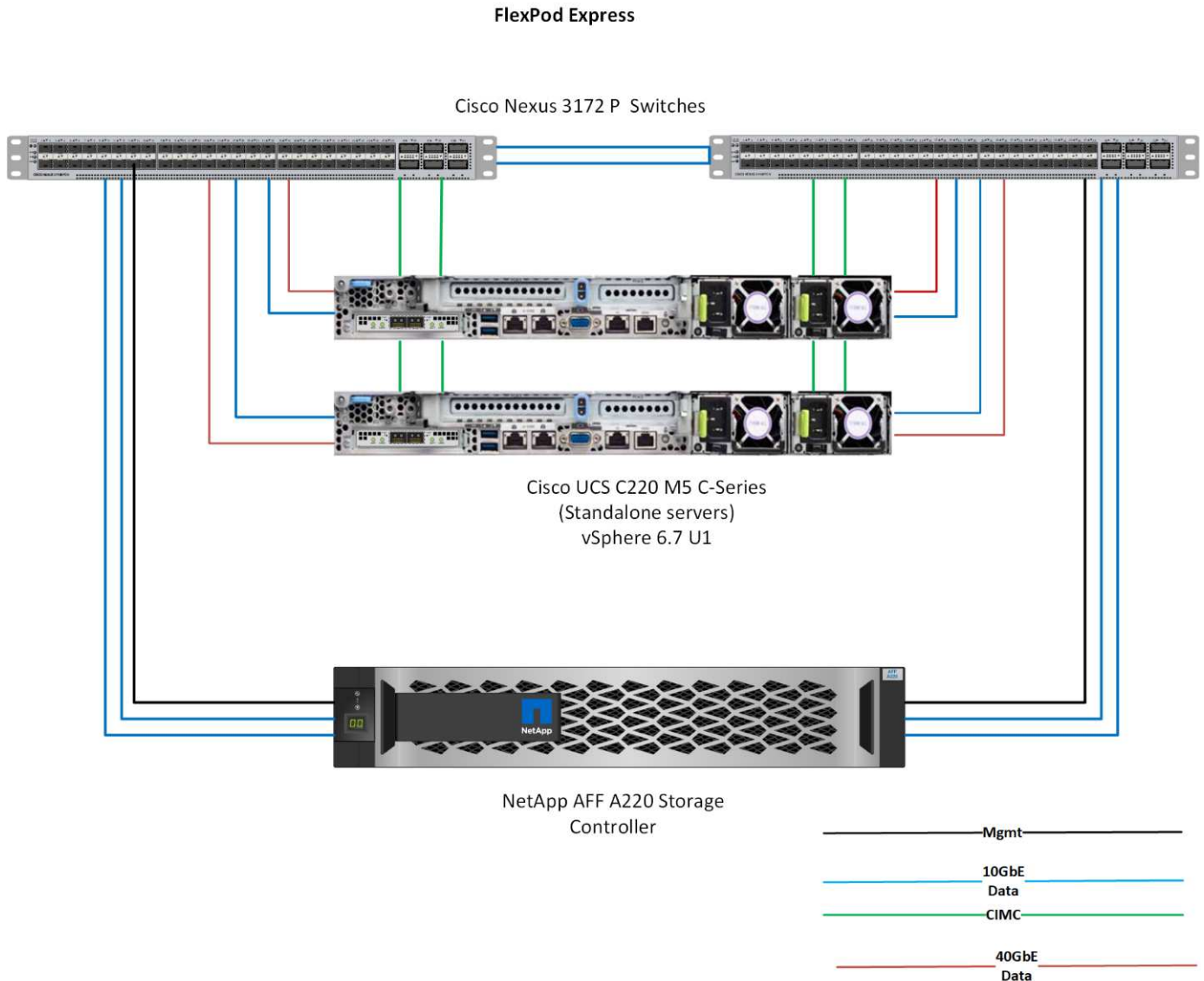
このガイドでは、VMware vSphere を使用した FlexPod Express の設計について詳しく説明します。また、この設計では、NetApp ONTAP 9.4、Cisco Nexus 3172P、Cisco UCS C シリーズ C220 M5 サーバをハイパーバイザーノードとして実行する、まったく新しい AFF A220 システムを使用します。

## 解決策テクノロジー

この解決策は、ネットアップ、Cisco、VMware の最新テクノロジーを活用しています。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 テクノロジーを使用しています。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"](#)。

## テクノロジー要件

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。

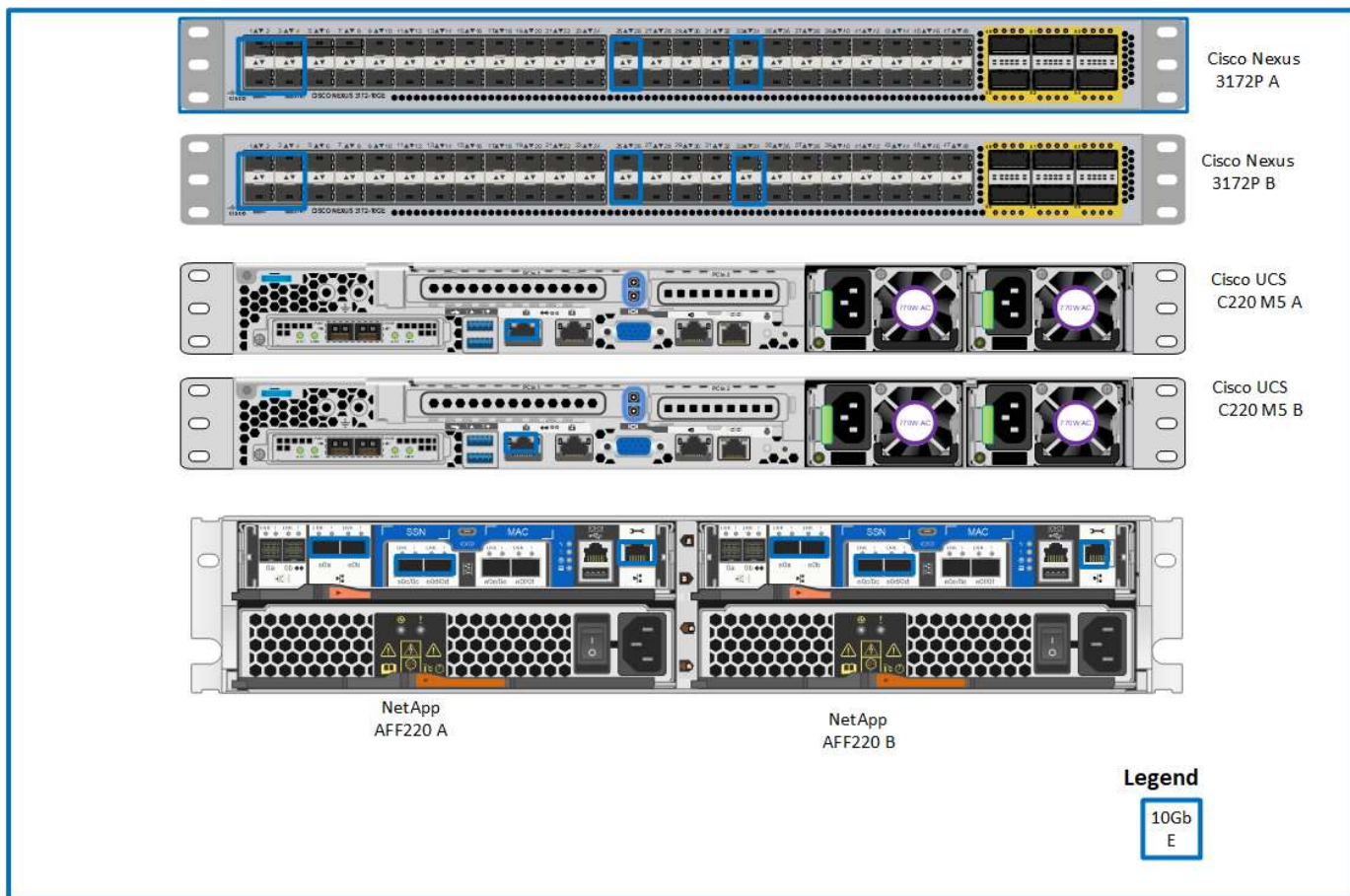
ソフトウェア	バージョン	詳細
Cisco Integrated Management Controller (CIMC)	3.1 (3G)	Cisco UCS C220 M5 ラックサーバの場合
Cisco nenic ドライバ	1.0.25.0	VIC 1387 インターフェイスカード用
Cisco NX-OS	nxos.7.0.3.17.5.bin	Cisco Nexus 3172P スイッチの場合
NetApp ONTAP	9.4	AFF A220 コントローラの場合

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



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
	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.

AN 名	VLAN の目的	このドキュメントの検証で使用された ID
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すべての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 Pol1
  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 Pol2
  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

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
  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 eth1/3-4
  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。



## ノード A の設定およびクラスタ設定の継続

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、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。

NetApp OnCommand System Manager
Getting Started

### Guided Setup to Configure a Cluster

Provide the information required below to configure your cluster:

1

2

3

Cluster

Network

Support

Summary

Cluster Name

Nodes

Not sure all nodes have been discovered? Refresh

FAS2650
62163000092

HA-PAGE

FAS2650
62163000093

Cluster Configuration:

☐ Switched Cluster
☒ Switchless Cluster

Username admin

Password

Confirm Password

Cluster Base License (Optional)

For any queries related to licenses, contact [mysupport.netapp.com](https://mysupport.netapp.com)

Feature Licenses (Optional)
Enter comma separated license keys...

Cluster Base License is mandatory to add Feature Licenses.

Submit

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 Method 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。

## Guided Setup to Configure a Cluster

Provide the information required below to configure your cluster:



### AutoSupport ☒

☐ Proxy URL (Optional)

**i** Connection is verified after configuring AutoSupport on all nodes.

### Event Notifications

Notify me through:

☒ Email

SMTP Mail Host

Email Addresses

Separate email addresses with a comma...

☐ SNMP

SNMP Trap Host

☐ Syslog

Syslog Server

Submit

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。

```
AFF A220::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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,fc
```

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 -ssl3-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。

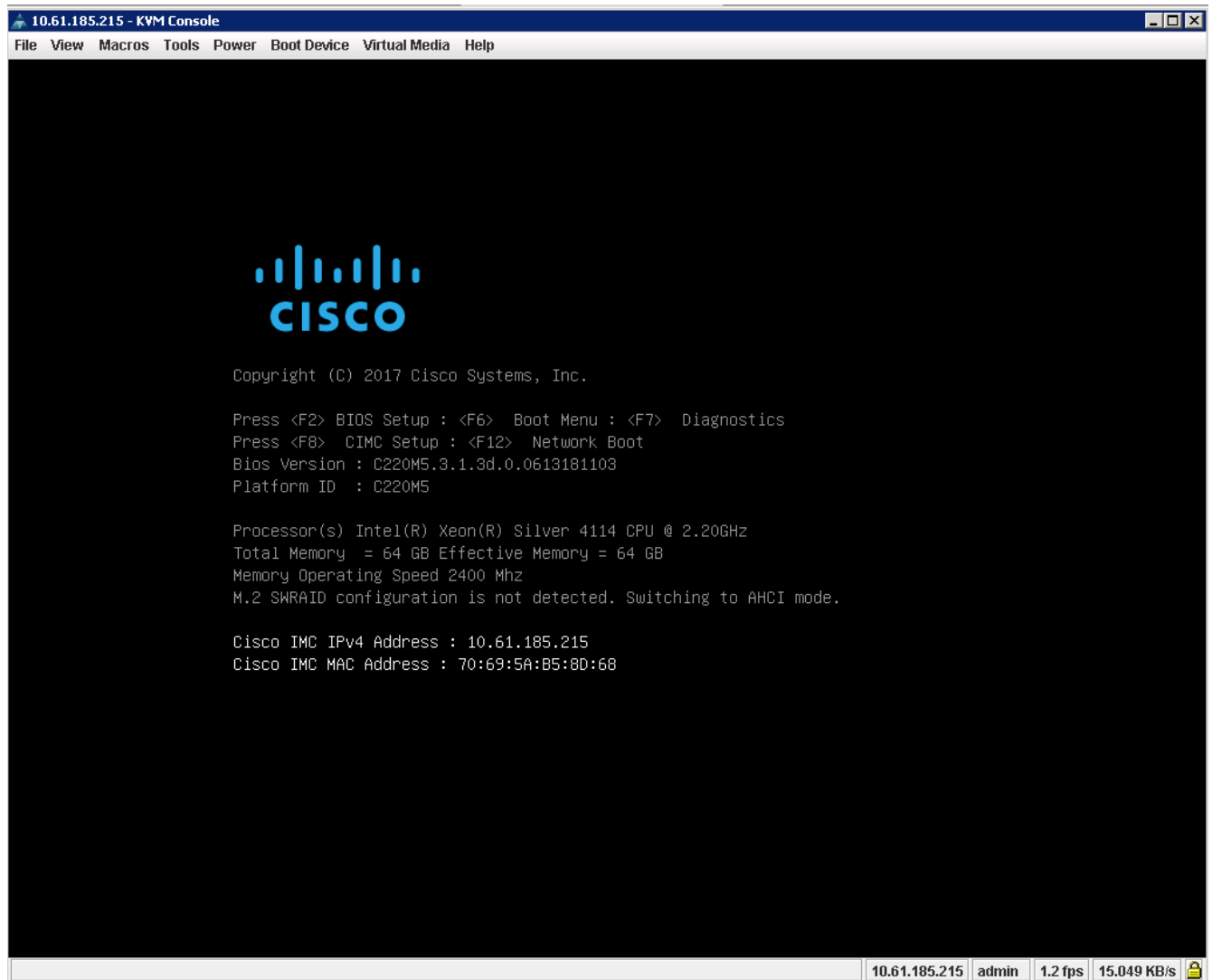
詳細（Detail）	詳細値
CIMC IP アドレス	\<CIMC_IP>>
CIMC サブネットマスク	\<CIMC_netmask>>
CIMC デフォルトゲートウェイ	\<CIMC_Gateway>> のようになります



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） dongle（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 dongle 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]

```
Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode
Dedicated:      [X]          NIC redundancy
Shared LOM:     [ ]          None: [X]
Cisco Card:     [ ]          Active-standby: [ ]
Riser1:         [ ]          Active-active: [ ]
Riser2:         [ ]          VLAN (Advanced)
MLom:           [ ]          VLAN enabled: [ ]
Shared LOM Ext: [ ]          VLAN ID: 1
Priority: 0
IP (Basic)
IPv4: [X]          IPv6: [ ]
DHCP enabled [ ]
CIMC IP: 10.61.185.215
Prefix/Subnet: 255.255.255.0
Gateway: 10.61.185.1
Pref DNS Server: 0.0.0.0
Smart Access USB
Enabled [ ]
*****
<Up/Down>Selection <F10>Save <Space>Enable/Disable <F5>Refresh <ESC>Exit
<F1>Additional settings
```

#### 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。

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
  Hostname:      CIMC-Tiger-02
  Dynamic DNS:   [X]
  DDNS Domain:
FactoryDefaults
  Factory Default:      [ ]
Default User(Basic)
  Default password:      -
  Reenter password:
Port Properties
  Auto Negotiation:      [X]
                                Admin Mode      Operation Mode
  Speed[1000/100/10Mbps]:      Auto              1000
  Duplex mode[half/full]:      Auto              full
Port Profiles
  Reset:                  [ ]
  Name:
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F2>PreviousPageettings

```

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 ( <b>Detail</b> )	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

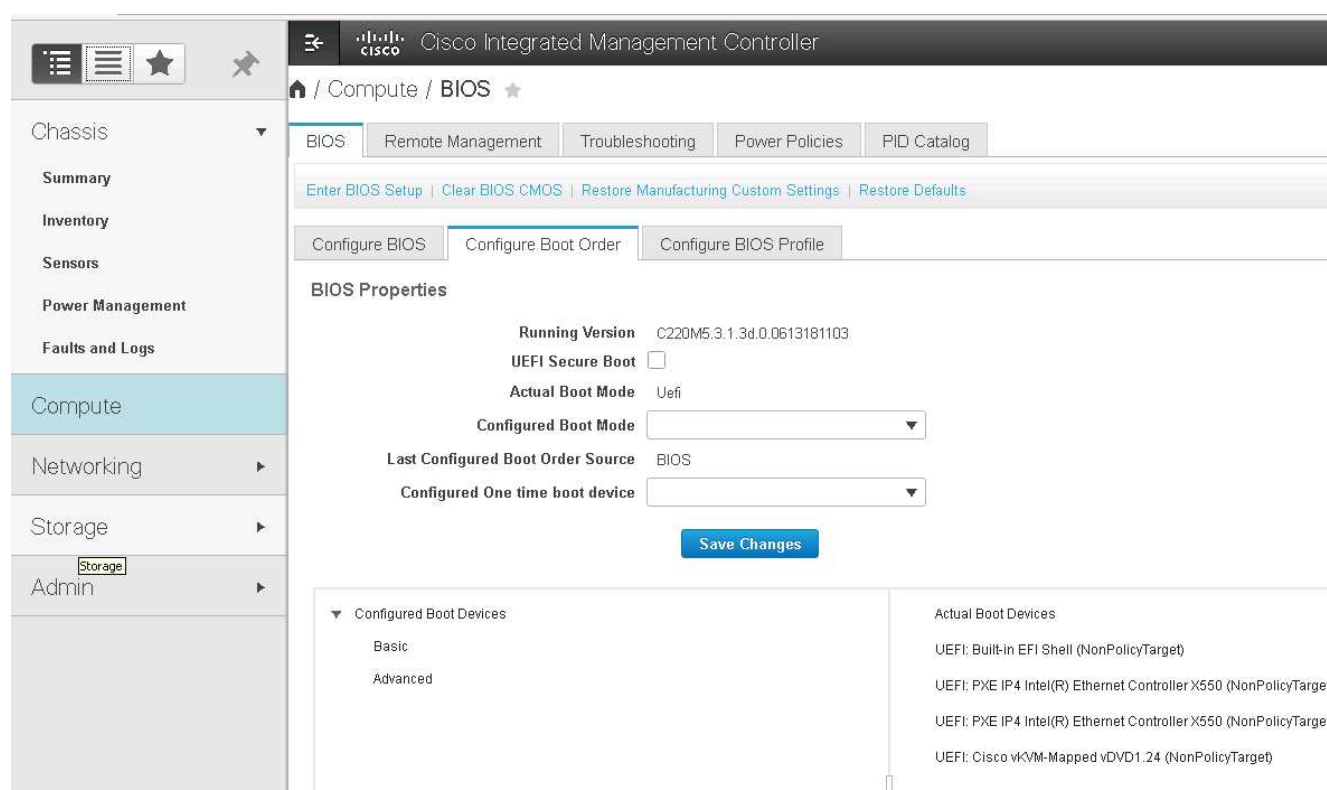


詳細（Detail）	詳細値
IP アドレス iSCSI_lif01a	
IP アドレス iSCSI_lif02a	
IP アドレス iSCSI_lif01b	
IP アドレス iSCSI_lif02b	
インフラ SVM IQN	

## 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。

Configure Boot Order

Configured Boot Level: Advanced

Basic Advanced

Add Boot Device

- Add Local HDD
- Add PXE Boot
- Add SAN Boot
- Add iSCSI Boot
- Add USB
- Add Virtual Media
- Add PCHStorage
- Add UEFISHELL
- Add SD Card
- Add NVME
- Add Local CDD

Advanced Boot Order Configuration

Selected 1 / Total 3

	Name	Type	Order	State
<input checked="" type="checkbox"/>	KVM-MAPPED-DVD	VMEDIA	1	Enabled
<input type="checkbox"/>	iSCSI-A	ISCSI	2	Enabled
<input type="checkbox"/>	iSCSI-B	ISCSI	3	Enabled

Save Changes Reset Values Close

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。

BIOS	Remote Management	Troubleshooting	Power Policies	PID Catalog
I/O	Server Management	Security	Processor	Memory
				Power/Performance

Note: Default values are shown in bold.

Reboot Host Immediately: ☒

Intel VT for directed IO: Enabled ▼

Intel VTD ATS support: Enabled ▼

LOM Port 1 OptionRom: Enabled ▼

Pcie Slot 1 OptionRom: Disabled ▼

MLOM OptionRom: Enabled ▼

Front NVME 1 OptionRom: Enabled ▼

MRAID Link Speed: Auto ▼

PCIe Slot 1 Link Speed: Auto ▼

Front NVME 1 Link Speed: Auto ▼

VGA Priority: Onboard ▼

P-SATA OptionROM: LSI SW RAID ▼

USB Port Rear: Enabled ▼

USB Port Internal: Enabled ▼

IPV6 PXE Support: Disabled ▼

Legacy USB Support: Enabled ▼

Intel VTD coherency support: Disabled ▼

All Onboard LOM Ports: Enabled ▼

LOM Port 2 OptionRom: Enabled ▼

Pcie Slot 2 OptionRom: Disabled ▼

MRAID OptionRom: Enabled ▼

Front NVME 2 OptionRom: Enabled ▼

MLOM Link Speed: Auto ▼

PCIe Slot 2 Link Speed: Auto ▼

Front NVME 2 Link Speed: Auto ▼

M.2 SATA OptionROM: AHCI ▼

USB Port Front: Enabled ▼

USB Port KVM: Enabled ▼

USB Port:M.2 Storage: Enabled ▼

## 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

▼ vNIC Properties

▼ General

Name:

CDN:

MTU:  (1500 - 9000)

Uplink Port:

MAC Address: ☐ Auto  
☒

Class of Service:  (0 - 6)

Trust Host CoS: ☒

PCI Order:  (0 - 5)

Default VLAN: ☐ None  
☒

VLAN Mode:

Rate Limit: ☒ OFF  
☐

Channel Number:  (1 - 1000)

PCI Link:  (0 - 1)

Enable NVGRE: ☐

Enable VXLAN: ☐

Advanced Filter: ☐

Port Profile:

Enable PXE Boot: ☒

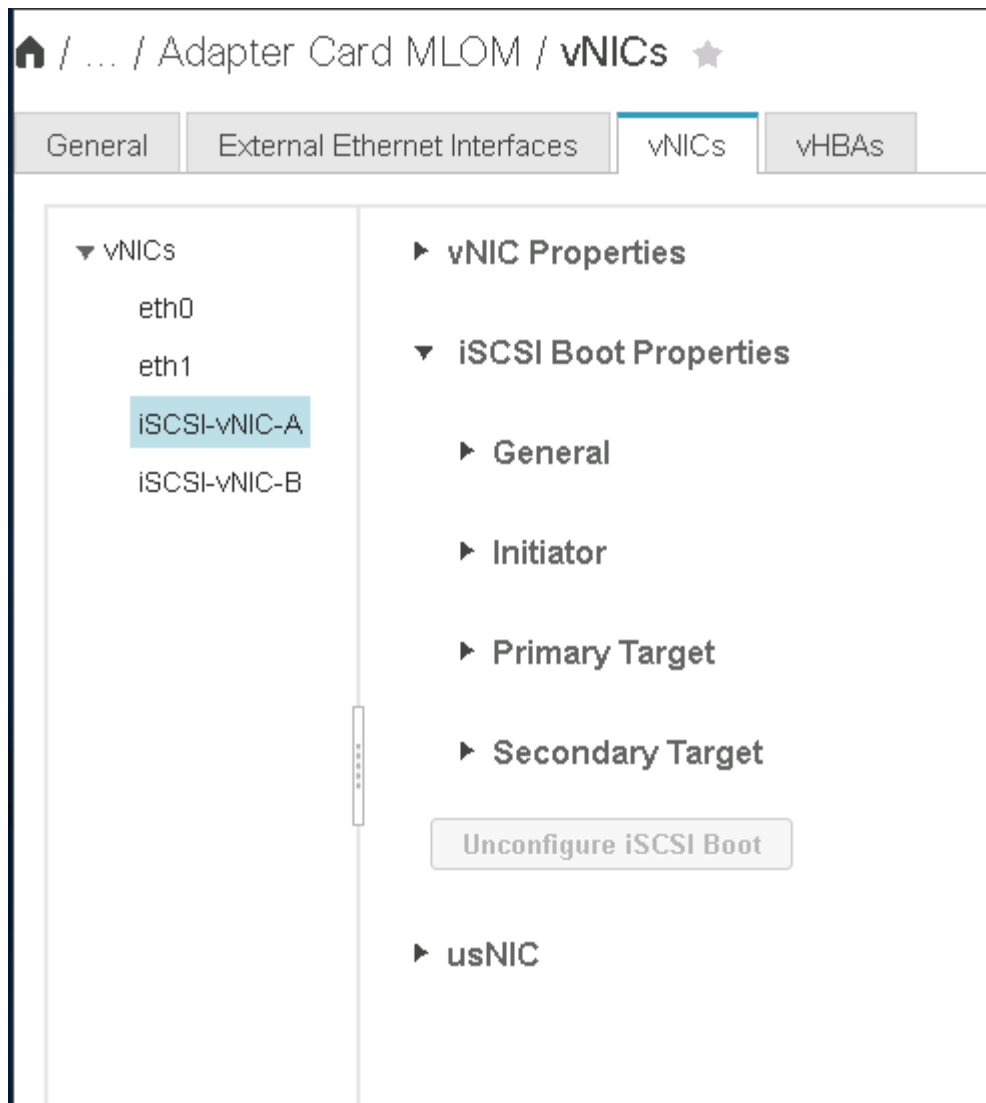
Enable VMQ: ☐

Enable aRFS: ☐

Enable Uplink Failover: ☐

Failback Timeout:  (0 - 600)

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>>

vNICs

eth0
eth1
iSCSI-v
iSCSI-v

iSCSI Boot Properties

General

Initiator

Name:  (0 - 233) chars
Initiator Priority:

IP Address: 
Secondary DNS:

Subnet Mask: 
TCP Timeout:

Gateway: 
CHAP Name:

Primary DNS: 
CHAP Secret:

Primary Target

Secondary Target

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。

General
External Ethernet Interfaces
vNICs
vHBAs

▼ vNICs

eth0
eth1
iSCSI-v
iSCSI-v

▶ Initiator

▼ Primary Target

Name: iqn.1992-08.com.netapp:sn.7e560f73a51 (0 - 233) chars
IP Address: 172.21.246.16
TCP Port: 3260

Name: iqn.1992-08.com.netapp:sn.7e560f73a51 (0 - 233) chars
IP Address: 172.21.246.18
TCP Port: 3260

Boot LUN: 0
CHAP Name:
CHAP Secret:

Boot LUN: 0
CHAP Name:
CHAP Secret:

Unconfigure iSCSI Boot

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。

🏠 / ... / Adapter Card  
MLOM / vNICs ★

[Refresh](#) | [Host Power](#) | [Launch KVM](#) | [Ping](#) | [CIMC Reboot](#) | [Locat](#)

General External Ethernet Interfaces **vNICs** vHBAs

▼ vNICs  
eth0  
eth1  
iSCSI-v  
iSCSI-v

### Host Ethernet Interfaces

Selected 0

[Add vNIC](#) [Clone vNIC](#) [Delete vNICs](#)

	Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode
<input type="checkbox"/>	eth0	VIC-MLO...	70:69:5A:C0:98:49	1500	0	0	0	NONE	TRUNK
<input type="checkbox"/>	eth1	VIC-MLO...	70:69:5A:C0:98:4A	1500	0	1	0	NONE	TRUNK
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4D	9000	0	0	0	3439	TRUNK
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4E	9000	0	1	0	3440	TRUNK

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。



General
External Ethernet Interfaces
vNICs
vHBAs

▼ vNICs

eth0

eth1

ISCSI-v

ISCSI-v

**Name:** eth0  
**CDN:** VIC-MLOM-eth0  
**MTU:** 9000 (1500 - 9000)  
**Uplink Port:** 0 ▼  
**MAC Address:** ☐ Auto  
☒ 70:69:5A:C0:98:49  
**Class of Service:** 0 (0 - 6)  
**Trust Host CoS:** ☐  
**PCI Order:** 0 (0 - 5)  
**Default VLAN:** ☒ None  
☐ ?

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。

Home / ... / Adapter Card MLOM / vNICs ★

General
External Ethernet Interfaces
vNICs
vHBAs

▼ vNICs

eth0

eth1

ISCSI-vNIC-A

ISCSI-vNIC-B

**Host Ethernet Interfaces**

Add vNIC
Clone vNIC
Delete vNICs

	Name	CDN	MAC Address	MTU	usNIC	Uplink Port
<input type="checkbox"/>	eth0	VIC-MLO...	70:69:5A:C0:98:49	9000	0	0
<input type="checkbox"/>	eth1	VIC-MLO...	70:69:5A:C0:98:4A	9000	0	1
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4D	9000	0	0
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4E	9000	0	1



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。

## 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

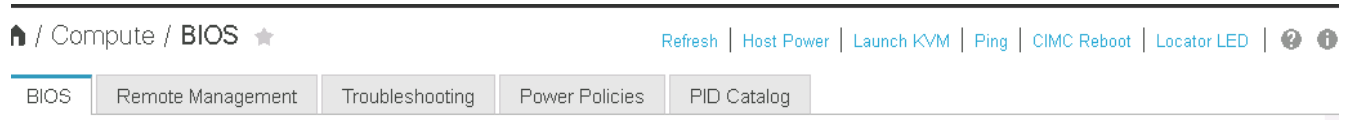
クラスタに追加するノードに対してこの手順を完了しておく必要があります。

### 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

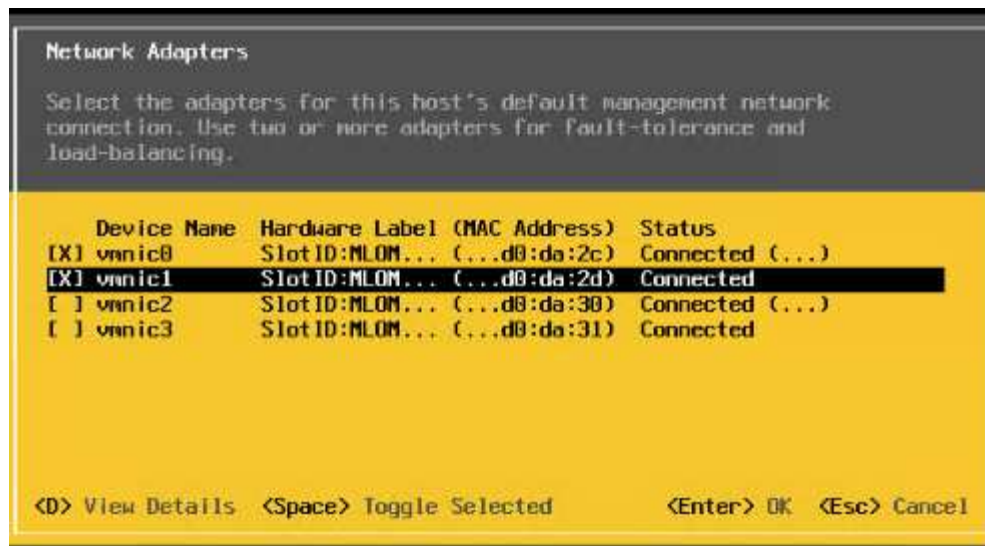
以下に、VMware ESXi ホストごとに管理ネットワークを追加する手順について説明します。

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、次の表の情報がが必要です。

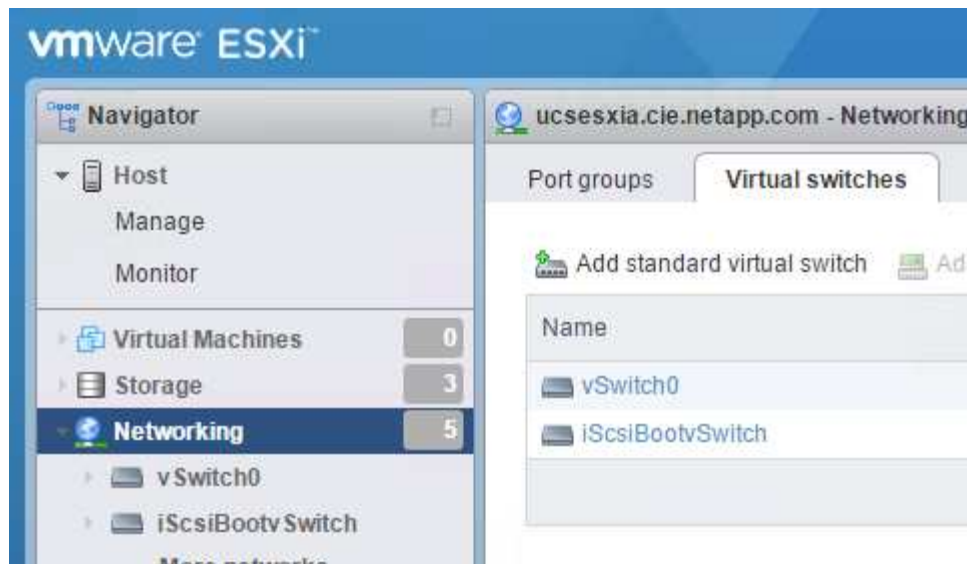
詳細（ <b>Detail</b> ）	価値
ESXi ホスト名	
ESXi ホスト管理 IP	
ESXi ホスト管理マスク	
ESXi ホスト管理ゲートウェイ	
ESXi ホストの NFS IP	
ESXi ホストの NFS マスク	
ESXi ホストの NFS ゲートウェイ	
ESXi ホスト vMotion IP	
ESXi ホストの vMotion マスク	
ESXi ホストの vMotion ゲートウェイ	
ESXi ホスト iSCSI-A IP	
ESXi ホスト iSCSI-A マスク	
ESXi ホスト iSCSI-A ゲートウェイ	
ESXi ホスト iSCSI-B IP	
ESXi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

Port group	New port group ▼
New port group	iScsiBootPG-B
Virtual switch	iScsiBootvSwitch-B ▼
VLAN ID	3440
MTU	9000
IP version	IPv4 only ▼
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.184.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack ▼
Services	<input type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging <input type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication

Create Cancel



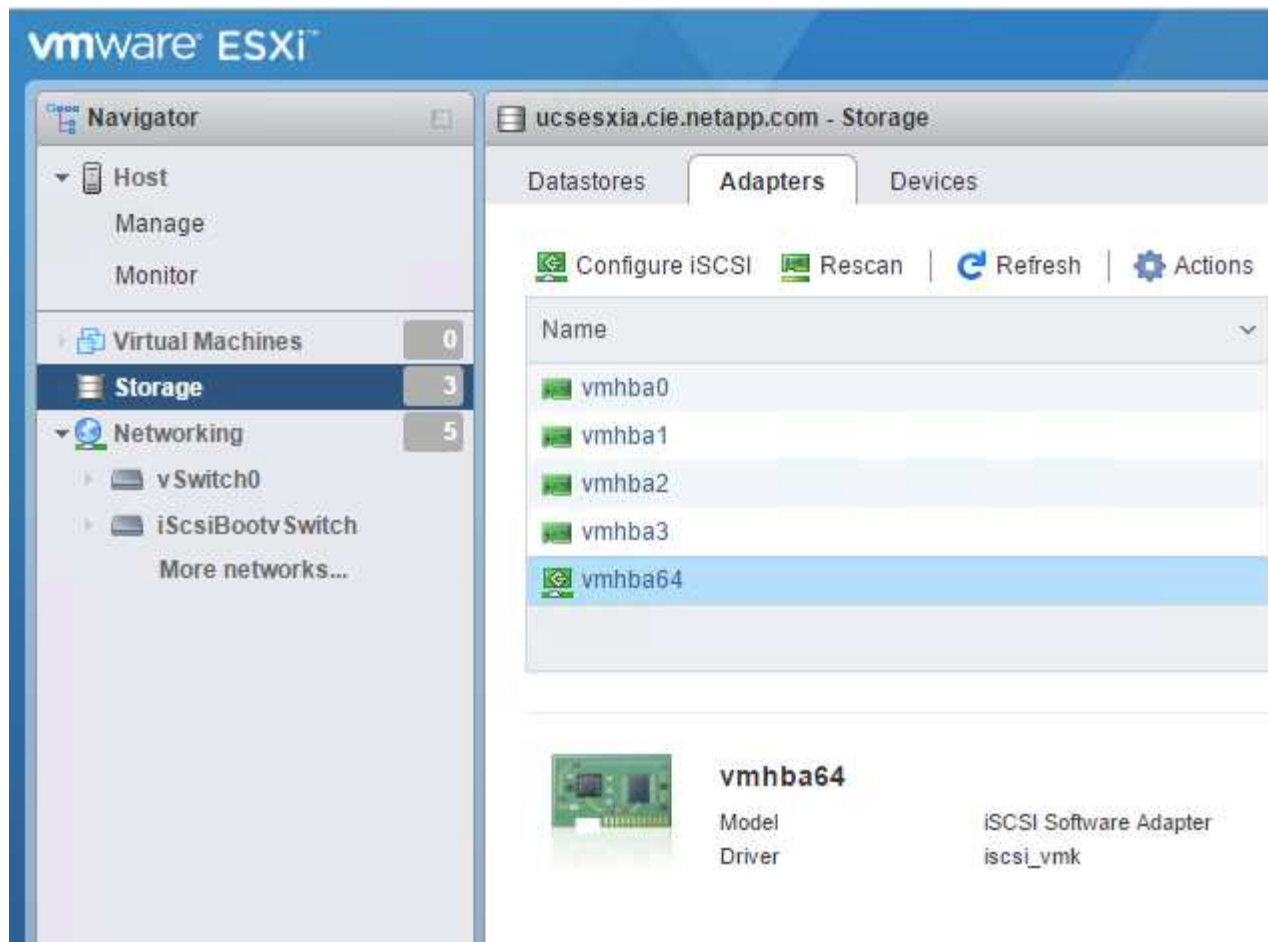
「iScsiBootPG-A」で MTU を 9000 に設定します

#### 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。

**Configure iSCSI - vmhba64**

iSCSI enabled	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled								
▶ Name & alias	iqn.1992-08.com.cisco:ucsaiscsia								
▶ CHAP authentication	Do not use CHAP ▼								
▶ Mutual CHAP authentication	Do not use CHAP ▼								
▶ Advanced settings	Click to expand								
Network port bindings	<div>  Add port binding            Remove port binding         </div> <table border="1"> <thead> <tr> <th>VMkernel NIC</th> <th>Port group</th> <th>IPv4 address</th> </tr> </thead> <tbody> <tr> <td colspan="3">No port bindings</td> </tr> </tbody> </table>			VMkernel NIC	Port group	IPv4 address	No port bindings		
VMkernel NIC	Port group	IPv4 address							
No port bindings									
Static targets	<div>  Add static target            Remove static target            Edit settings           <input type="text" value="Search"/> </div> <table border="1"> <thead> <tr> <th>Target</th> <th>Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td>iqn.1992-08.com.netapp:sn.09591199033811e78eb...</td> <td>172.21.183.34</td> <td>3260</td> </tr> </tbody> </table>			Target	Address	Port	iqn.1992-08.com.netapp:sn.09591199033811e78eb...	172.21.183.34	3260
Target	Address	Port							
iqn.1992-08.com.netapp:sn.09591199033811e78eb...	172.21.183.34	3260							
Dynamic targets	<div>  Add dynamic target            Remove dynamic target            Edit settings           <input type="text" value="Search"/> </div> <table border="1"> <thead> <tr> <th>Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td colspan="2">No dynamic targets</td> </tr> </tbody> </table>			Address	Port	No dynamic targets			
Address	Port								
No dynamic targets									

#### 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。

Dynamic targets

Add dynamic target
 Remove dynamic target
 Edit settings

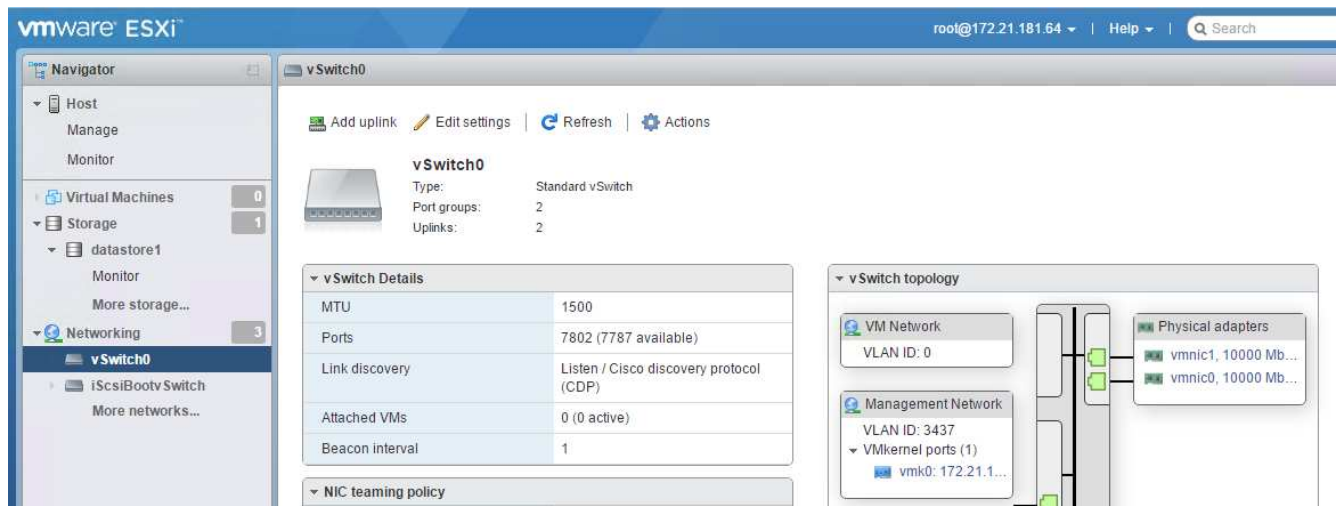
Address	Port
172.21.183.33	3260
172.21.183.34	3260
172.21.184.33	3260
172.21.184.34	3260



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

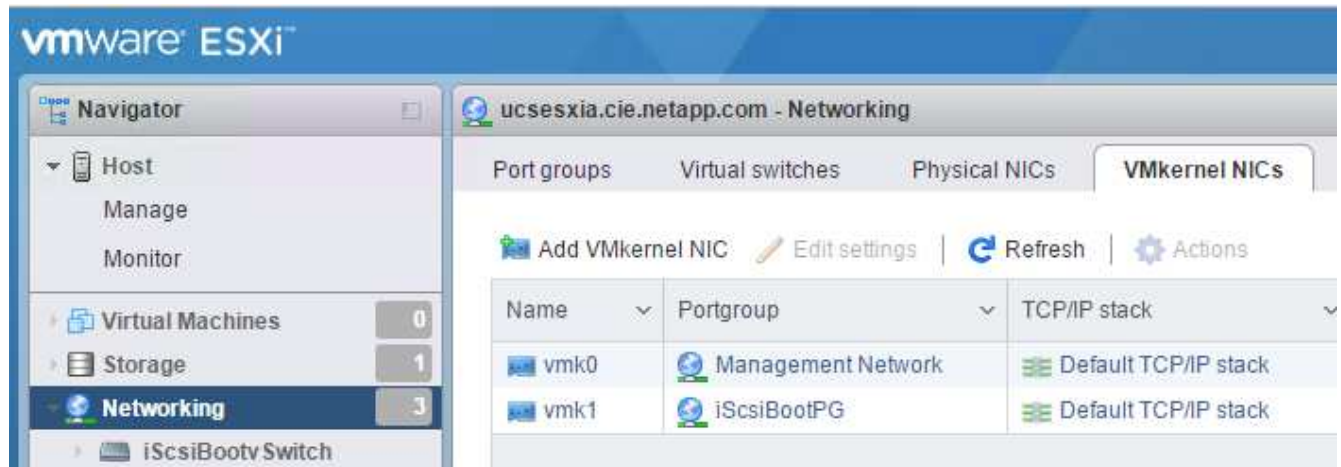
1. 左側のナビゲーションペインで、[ネットワーク]を選択します。
2. Port Groups タブを右クリックします。



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。 .

Port group	New port group ▼
New port group	NFS-Network
Virtual switch	vSwitch0 ▼
VLAN ID	3438
MTU	9000
IP version	IPv4 only ▼
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.182.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack ▼

Create Cancel

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。

Virtual switch	vSwitch0
VLAN ID	3441
MTU	9000
IP version	IPv4 only
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.185.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack
Services	<input checked="" type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging <input type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication

Create Cancel



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。

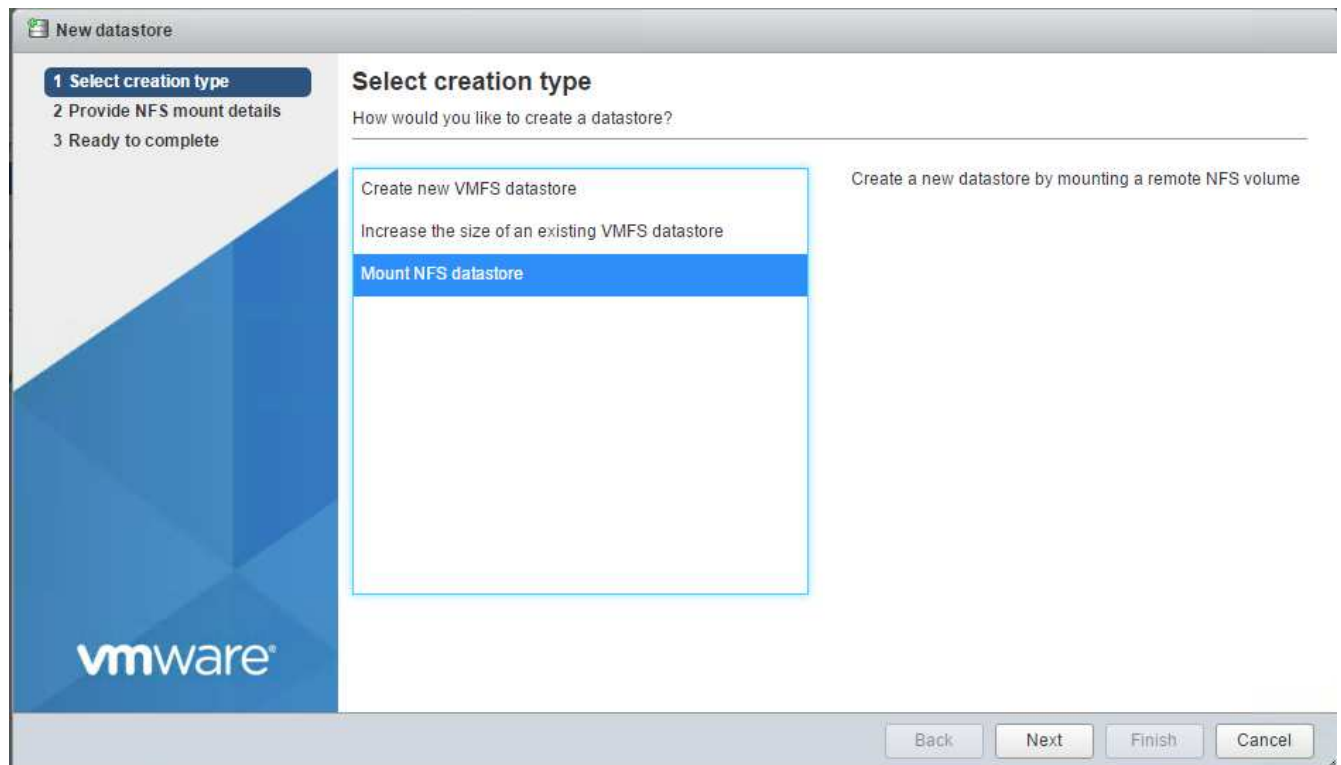
## 最初のデータストアをマウント

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

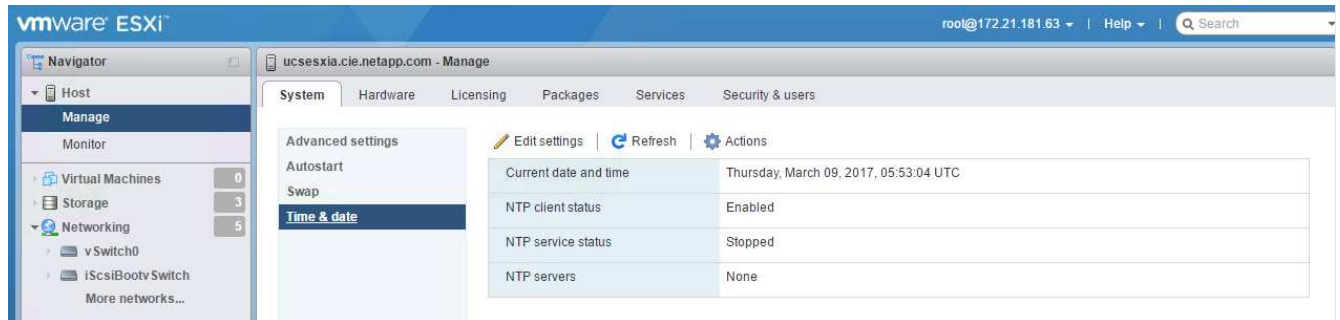


- NFS 3 が選択されていることを確認します。

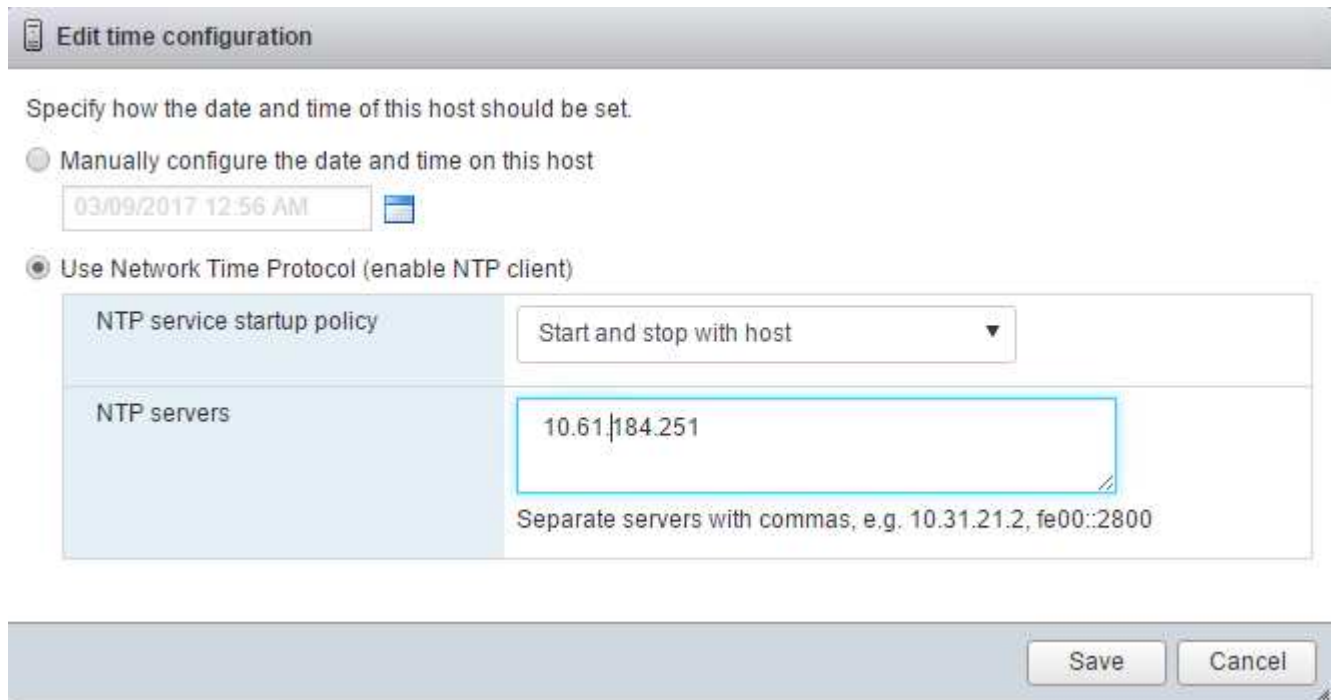
## NTP を設定します

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。

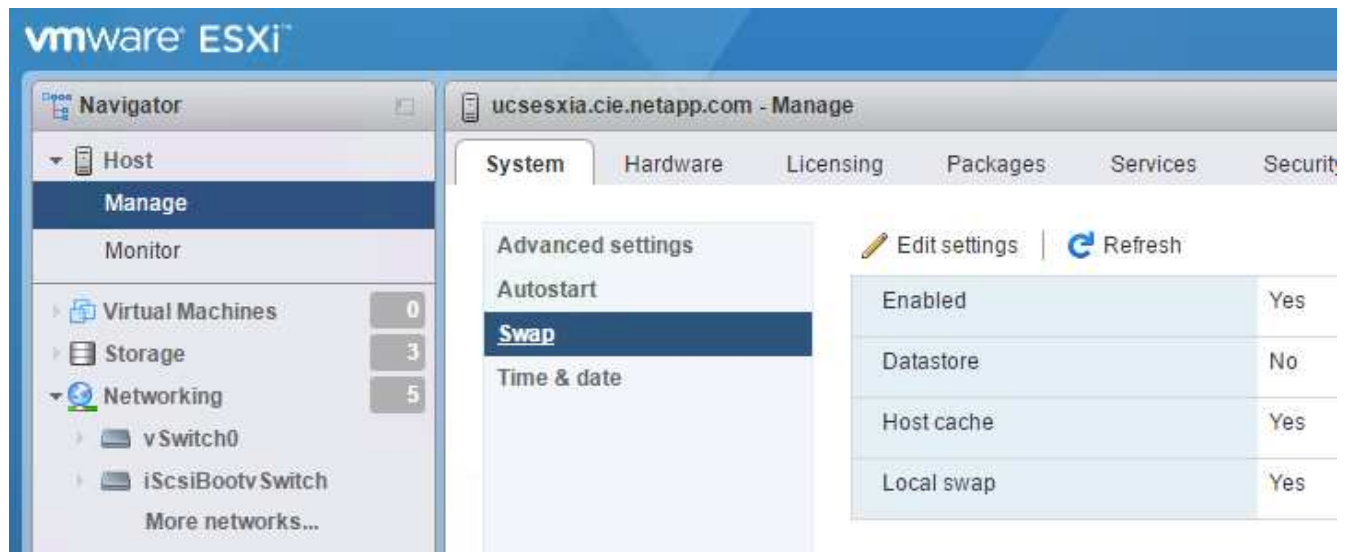


## 仮想マシンのスワップファイルの場所を移動します

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。
- にアクセスします ["ソフトウェアダウンロードページ"](#)。
  - 下にスクロールして、NetApp NFS Plug-in for VMware VAAI をクリックします。
  - ESXi プラットフォームを選択します。
  - 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:
```

"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

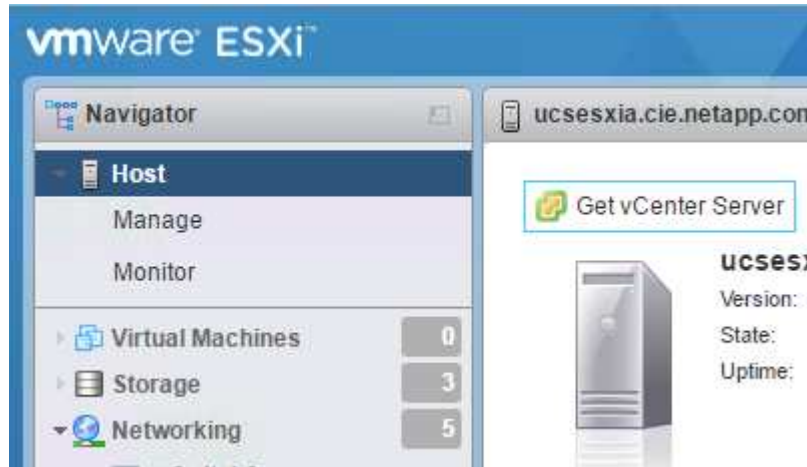
このセクションでは、FlexPod 構成に VMware vCenter Server 6.7 をインストールする詳細な手順について説明します。



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。

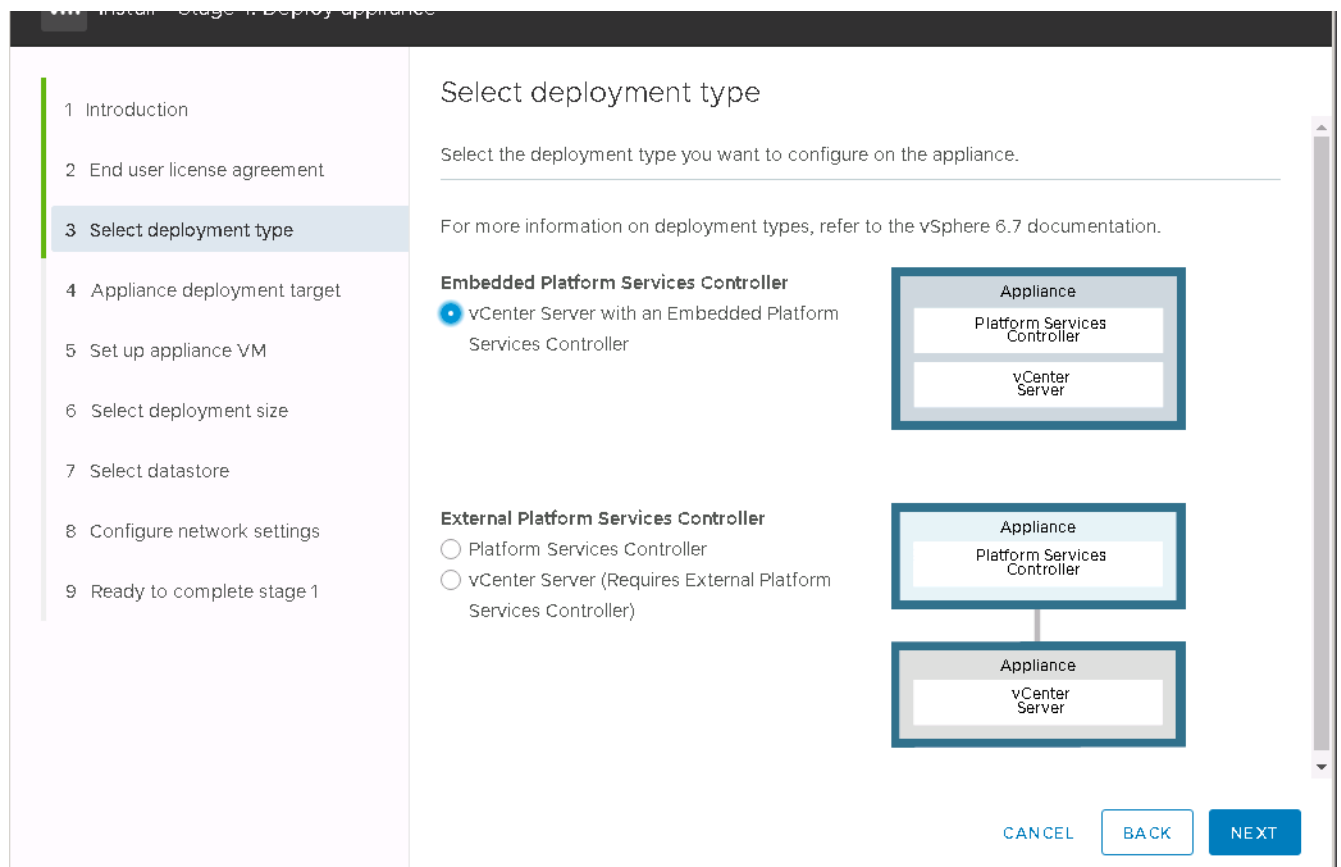


2. vCSA を VMware サイトからダウンロードします。



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。

Installer

vm Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction

2 End user license agreement

3 Select deployment type

4 Appliance deployment target

5 Set up appliance VM

6 Select deployment size

7 Select datastore

8 Configure network settings

9 Ready to complete stage 1

### Appliance deployment target

Specify the appliance deployment target settings. The target is the ESXi host or vCenter Server instance on which the appliance will be deployed.

ESXi host or vCenter Server name	172.21.246.25	i
HTTPS port	443	
User name	root	i
Password	*****	

CANCEL

BACK

NEXT

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。

VM Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction  
2 End user license agreement  
3 Select deployment type  
4 Appliance deployment target  
**5 Set up appliance VM**  
6 Select deployment size  
7 Select datastore  
8 Configure network settings  
9 Ready to complete stage 1

### Set up appliance VM

Specify the VM settings for the appliance to be deployed.

VM name
 ⓘ

Set root password
 ⓘ

Confirm root password

CANCEL
BACK
NEXT

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。

VM Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction  
2 End user license agreement  
3 Select deployment type  
4 Appliance deployment target  
5 Set up appliance VM  
**6 Select deployment size**  
7 Select datastore  
8 Configure network settings  
9 Ready to complete stage 1

### Select deployment size

Select the deployment size for this vCenter Server with an Embedded Platform Services Controller.

For more information on deployment sizes, refer to the vSphere 6.7 documentation.

Deployment size

Storage size
 ⓘ

**Resources required for different deployment sizes**

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	10	300	10	100
Small	4	16	340	100	1000
Medium	8	24	525	400	4000
Large	16	32	740	1000	10000
X-Large	24	48	1180	2000	35000

CANCEL
BACK
NEXT

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。

vm Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction  
2 End user license agreement  
3 Select deployment type  
4 Appliance deployment target  
5 Set up appliance VM  
6 Select deployment size  
7 Select datastore  
8 Configure network settings  
9 Ready to complete stage 1

### Select datastore

Select the storage location for this appliance

☒ Install on an existing datastore accessible from the target host

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
infra_datastore_1	NFS	500 GB	499.98 GB	18.38 MB	Supported
infra_swap	NFS	100 GB	99.99 GB	10.95 MB	Supported

2 items

☒ Enable Thin Disk Mode ⓘ

☐ Install on a new vSAN cluster containing the target host ⓘ

CANCEL BACK NEXT

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。
- MGMT - Network（ネットワーク）を選択します。
  - vCSA に使用する FQDN または IP を入力します。
  - 使用する IP アドレスを入力します。
  - 使用するサブネットマスクを入力します。
  - デフォルトゲートウェイを入力します。
  - 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。

vCenter Server Appliance Installer

Installer

vm Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction

2 End user license agreement

3 Select deployment type

4 Appliance deployment target

5 Set up appliance VM

6 Select deployment size

7 Select datastore

8 Configure network settings

9 Ready to complete stage 1

### Configure network settings

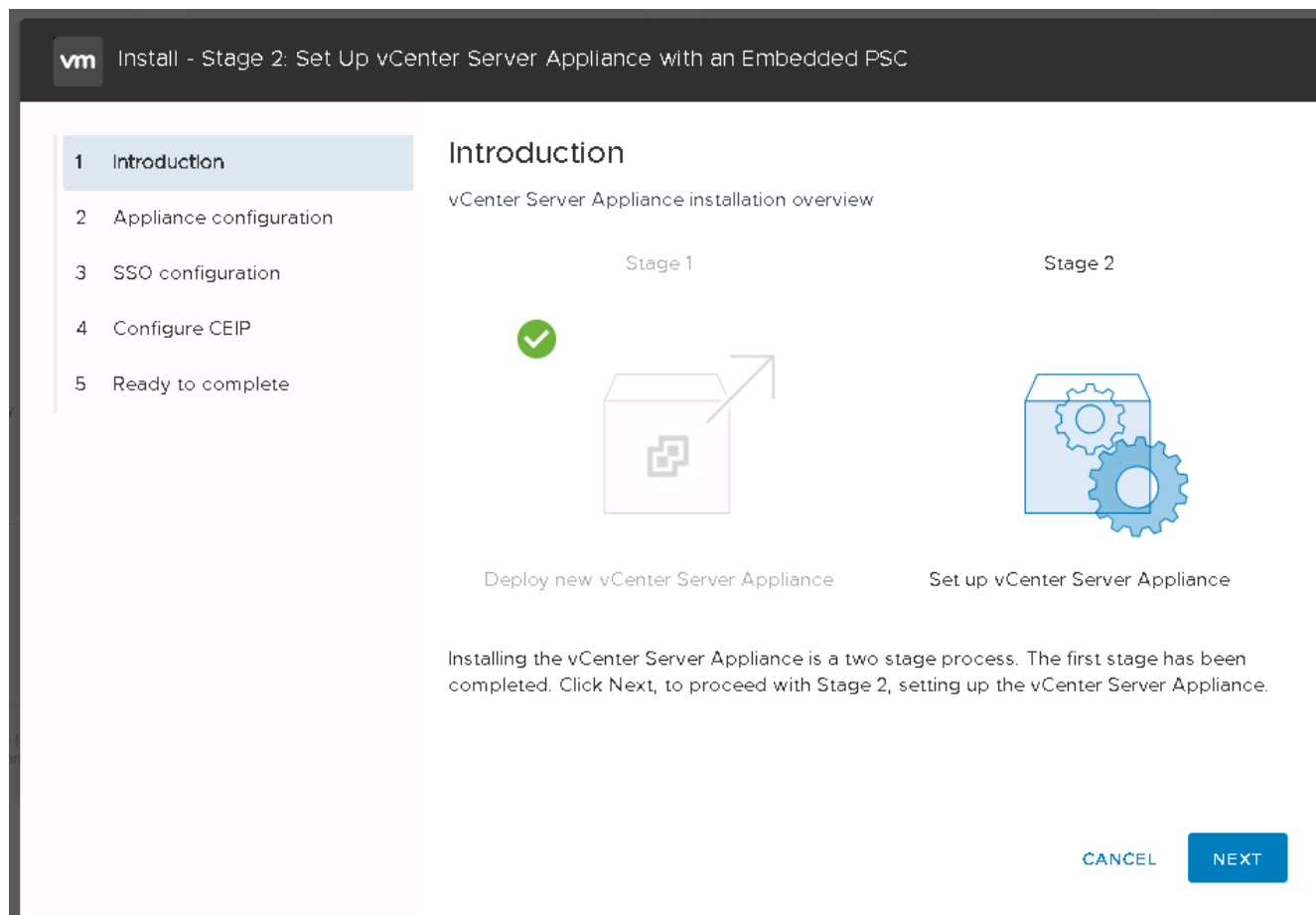
IP version	IPv4	▼
IP assignment	static	▼
FQDN	tigervcsa.cle.netapp.com	ⓘ
IP address	172.21.246.41	
Subnet mask or prefix length	255.255.255.0	ⓘ
Default gateway	172.21.246.1	
DNS servers	10.61.184.251,10.61.184.252	
Common Ports		
HTTP	80	
HTTPS	443	

[CANCEL](#) [BACK](#) [NEXT](#)

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 クラスターリングを設定する

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

1. <https://<FQDN> /vsphere-client/> 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@vsphere.local` [administrator@vsphere.local] 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。

New Cluster | FlexPod

Name

Tiger3

Location

FlexPod

> DRS

☒ Turn ON

> vSphere HA

☒ Turn ON

> EVC

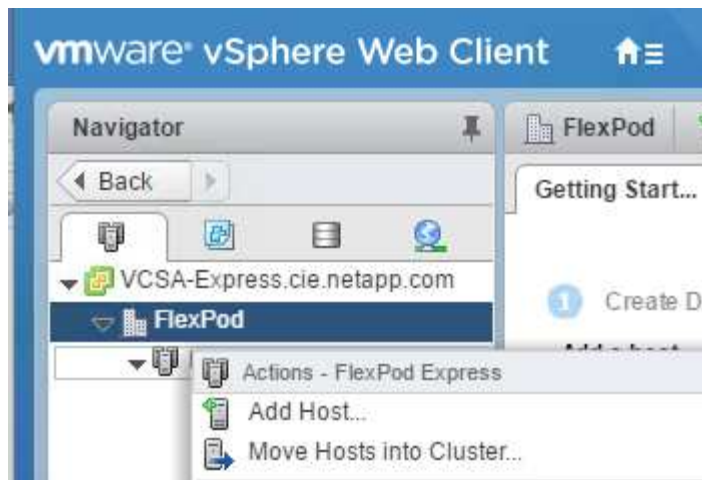
Disable

CANCEL

OK

## 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"](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"](https://www.netapp.com/us/media/nva-1125-design.pdf)

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。