



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 FlexPod

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/flexpod/express/express-c-series-c190-deploy_program_summary_overview.html on March 25, 2024. Always check docs.netapp.com for the latest.

目次

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	1
NVA-1142-deploy : FlexPod Express with Cisco UCS C シリーズ and NetApp AFF C190 Series - NVA	
Deployment (英語)	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	98
謝辞	99
追加情報の参照先	99
バージョン履歴	99

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ー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 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。

The FlexPod Portfolio

A prevalidated, flexible platform that features



FlexPod® Express

Remote office or branch office, retail, small and midsize business, and edge



FlexPod Datacenter

Enterprise apps, unified infrastructure, and virtualization

11

NetApp Verified Architecture プログラム

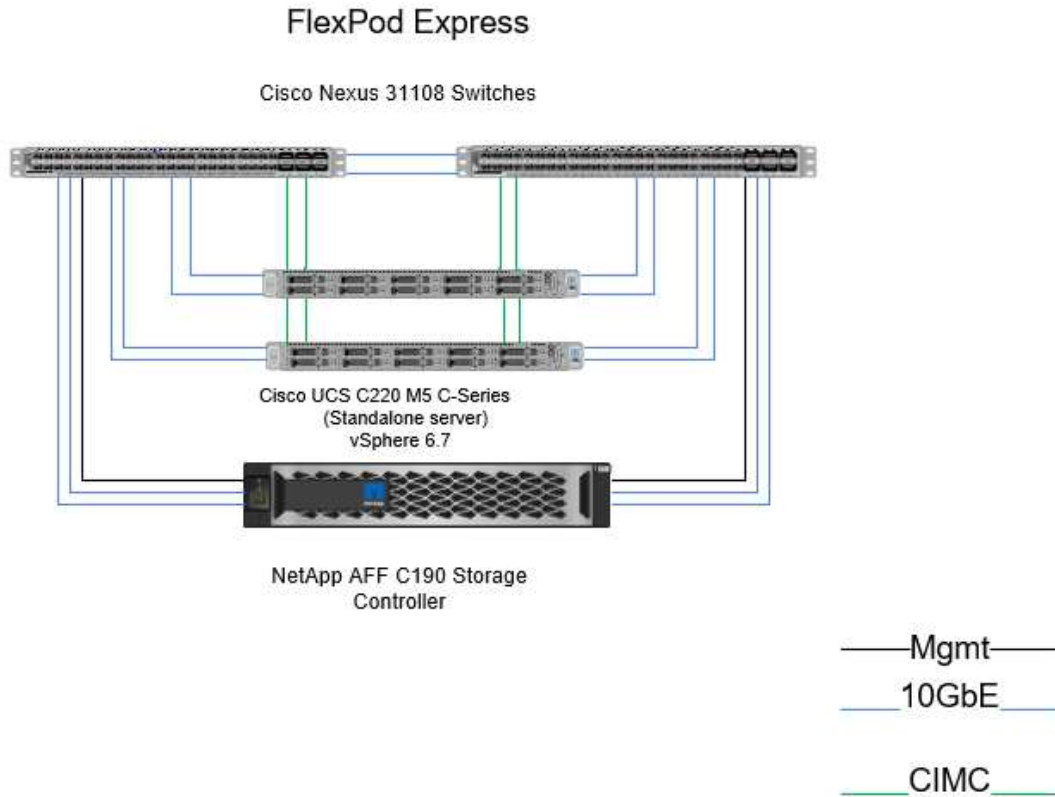
NetApp Verified Architecture プログラムは、ネットアップソリューションの検証済みアーキテクチャを提供するものです。NetApp Verified Architecture は、NetApp 解決策アーキテクチャに次の品質を提供します。

- 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 9.6 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。



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。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 ノードクラスターです	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

ーネットを示します。

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

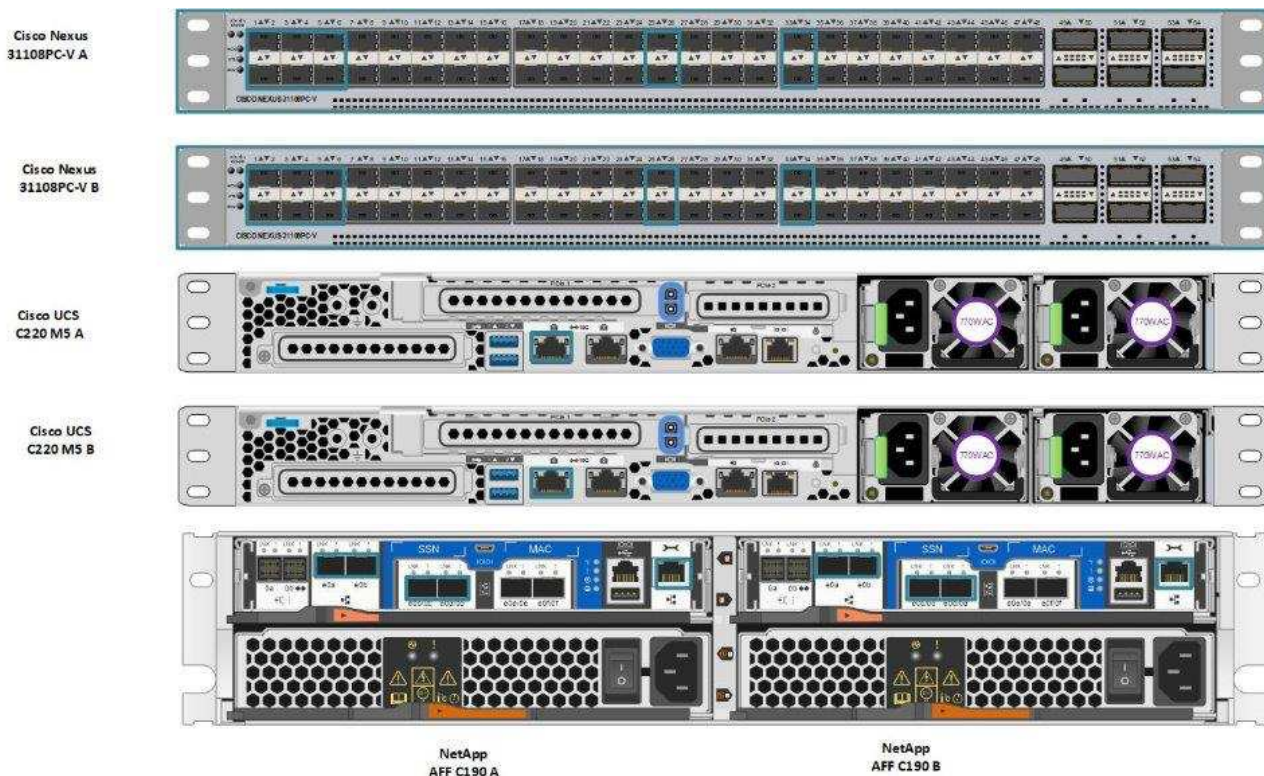
次の表に、 FlexPod Express でのすべての VMware vSphere 環境に必要なソフトウェアを示します。

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 エクスプレスクーブル接続情報

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 31108PC-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? (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。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
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 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

```

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。



ルータ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 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「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。

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

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。

ストレージクラス構成を継続します

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
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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. vservers 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
```



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。

- 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。
- 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
```

- 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 -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 権限レベルにリポ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） 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。

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。



Copyright (c) 2019 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics
Press <F8> CIMC Setup : <F12> Network Boot
Bios Version : C220M5.4.0.4g.0.0712190011
Platform ID : C220M5

Processor(s) Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
Total Memory = 64 GB Effective Memory = 64 GB
Memory Operating Speed 2400 Mhz
M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 10.63.172.160
Cisco IMC MAC Address : 70:69:5A:B5:8D:68

Entering CIMC Configuration Utility ...

92

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: `\

プレフィックス / サブネット： `\

ゲートウェイ： `\

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]


```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                   None:          [X]
Shared LOM:     [ ]                   Active-standby: [ ]
Cisco Card:     [ ]                   Active-active:  [ ]
  Riser1:       [ ]                   VLAN (Advanced)
  Riser2:       [ ]                   VLAN enabled:   [ ]
  MLom:         [ ]                   VLAN ID:       1
  Shared LOM Ext: [ ]                   Priority:      0
IP (Basic)
IPv4:           [X]                   IPv6:          [ ]
DHCP enabled    [ ]
CIMC IP:        10.63.172.160
Prefix/Subnet:  255.255.255.0
Gateway:        10.63.172.1
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

```

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。

 Cisco Integrated Management Controller

[Home](#) / [Compute](#) / [BIOS](#) ★

[BIOS](#)
[Remote Management](#)
[Troubleshooting](#)
[Power Policies](#)
[PID Catalog](#)

[Enter BIOS Setup](#) | [Clear BIOS CMOS](#) | [Restore Manufacturing Custom Settings](#) | [Restore Defaults](#)

[Configure BIOS](#)
[Configure Boot Order](#)
[Configure BIOS Profile](#)

BIOS Properties

Running Version

C220M5.4.0.4g.0.0712190011

UEFI Secure Boot

☐

Actual Boot Mode

Uefi

Configured Boot Mode

Last Configured Boot Order Source

BIOS

Configured One time boot device

Save Changes

▼ Configured Boot Devices

Basic

▶

☒ Advanced

Actual Boot Devices

UEFI: Built-in EFI Shell (NonPolicyTarget)

UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)

UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)

Configure Boot Order

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。

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

Enable/Disable Modify Delete Clone Re-Apply Move Up Move Down

	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. 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。

- 下にスクロールして [PCIe Slot:HBA Option ROM] を表示します。
- 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 ▼	Legacy USB Support:	Enabled ▼
Intel VTD ATS support:	Enabled ▼	Intel VTD coherency support:	Disabled ▼
LOM Port 1 OptionRom:	Enabled ▼	All Onboard LOM Ports:	Enabled ▼
Pcie Slot 1 OptionRom:	Disabled ▼	LOM Port 2 OptionRom:	Enabled ▼
MLOM OptionRom:	Enabled ▼	Pcie Slot 2 OptionRom:	Disabled ▼
Front NVME 1 OptionRom:	Enabled ▼	MRAID OptionRom:	Enabled ▼
MRAID Link Speed:	Auto ▼	Front NVME 2 OptionRom:	Enabled ▼
PCle Slot 1 Link Speed:	Auto ▼	MLOM Link Speed:	Auto ▼
Front NVME 1 Link Speed:	Auto ▼	PCle Slot 2 Link Speed:	Auto ▼
VGA Priority:	Onboard ▼	Front NVME 2 Link Speed:	Auto ▼
P-SATA OptionROM:	LSI SW RAID ▼	M.2 SATA OptionROM:	AHCI ▼
USB Port Rear:	Enabled ▼	USB Port Front:	Enabled ▼
USB Port Internal:	Enabled ▼	USB Port KVM:	Enabled ▼
IPv6 PXE Support:	Disabled ▼	USB Port:M.2 Storage:	Enabled ▼

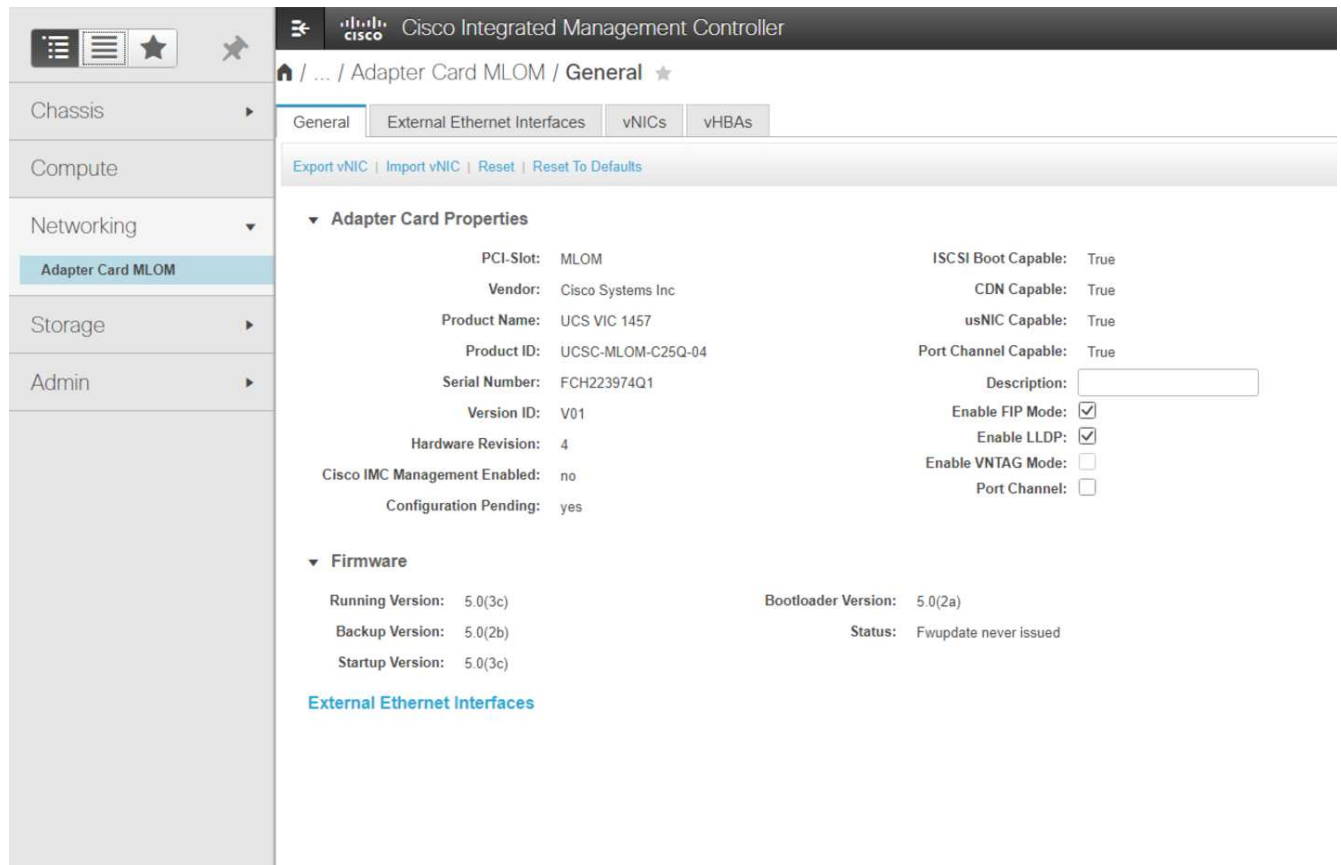
iSCSI ブート用に Cisco VIC1457 を設定します

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。

- [ネットワーク] タブで、[Adapter Card mLOM] をクリックします。
- General タブで、ポートチャネルのチェックを外します。
- 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。

▼ General

Name:

CDN:

MTU: (1500 - 9000)

Uplink Port: ▼

MAC Address: ☐ Auto
☒

Class of Service: (0 - 6)

Trust Host CoS: ☐

PCI Order: (0 - 7)

Default VLAN: ☐ None
☒ ?

6. 左側の vNIC eth1 を選択します。

General External Ethernet Interfaces **vNICs** vHBAs

▼ vNICs

- eth0
- eth1**
- eth2
- eth3

▶ vNIC Properties

▼ iSCSI Boot Properties

▶ General

▼ Initiator

Name: (0 - 222) chars

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

▶ Primary Target

▶ Secondary Target

[Unconfigure iSCSI Boot](#)

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>>

▼ vNICs
eth0
eth1
eth2
eth3

▶ vNIC Properties

▼ iSCSI Boot Properties

▶ General

▼ Initiator

Name: iqn.1992-01.com.cisco.ucsa-A-01 (0 - 222) chars

IP Address: 172.21.183.110

Subnet Mask: 255.255.255.0

Gateway: 172.21.183.1

Primary DNS:

Initiator Priority: primary

Secondary DNS:

TCP Timeout: 15 (0 - 255)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

▼ Primary Target

Name: iqn.1992-08.com.netapp:sn.e42fa6b2d2 (0 - 222) chars

IP Address: 172.21.183.105

TCP Port: 3260

Boot LUN: 0 (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

▼ Secondary Target

Name: iqn.1992-08.com.netapp:sn.e42fa6b2d2 (0 - 222) chars

IP Address: 172.21.183.106

TCP Port: 3260

Boot LUN: 0 (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

Unconfigure iSCSI Boot

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>>

Adapter Card MLOM / vNICs

General External Ethernet Interfaces vNICs vHBAs

vNICs

eth0 eth1 eth2 eth3

vNIC Properties

iSCSI Boot Properties

General

Initiator

Name: iqn.1992-01.com.cisco.ucsa-02 (0 - 222) chars

IP Address: 172.21.184.110

Subnet Mask: 255.255.255.0

Gateway: 172.21.184.1

Primary DNS:

Initiator Priority: primary

Secondary DNS:

TCP Timeout: 15 (0 - 255)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

Primary Target

Name: iqn.1992-08.com.netapp.sn.e42fa6b2d2v (0 - 222) chars

IP Address: 172.21.184.105

TCP Port: 3260

Secondary Target

Name: iqn.1992-08.com.netapp.sn.e42fa6b2d2v (0 - 222) chars

IP Address: 172.21.184.106

TCP Port: 3260

Boot LUN: 0 (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

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。

Cisco Integrated Management Controller

Home / ... / Adapter Card MLOM / vNICs

General External Ethernet Interfaces **vNICs** vHBAs

vNIC Properties

General

Name: eth0

CDN: VIC-MLOM-eth0

MTU: 9000 (1500 - 9000)

Uplink Port: 0

MAC Address: ☐ Auto ☒ F8:0F:6F:89:26:CE

Class of Service: 0 (0 - 6)

Trust Host CoS: ☐

PCI Order: 0 (0 - 7)

Default VLAN: ☐ None ☒ 2

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。

Cisco Integrated Management Controller

Home / ... / Adapter Card MLOM / vNICs

General External Ethernet Interfaces **vNICs** vHBAs

Host Ethernet Interfaces

Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	iSCSI Boot	PXE Boot	Channel	Port Profile	Uplink Failover
<input type="checkbox"/> eth0	VIC-MLO...	F8:0F:6F:89:26:CE	9000	0	0	0	2	TRUNK	disabled	enabled	N/A	N/A	N/A
<input type="checkbox"/> eth1	VIC-iSCS...	F8:0F:6F:89:26:CF	9000	0	1	0	3439	TRUNK	enabled	enabled	N/A	N/A	N/A
<input type="checkbox"/> eth2	VIC-MLO...	F8:0F:6F:89:26:D0	9000	0	2	0	2	TRUNK	disabled	enabled	N/A	N/A	N/A
<input type="checkbox"/> eth3	VIC-iSCS...	F8:0F:6F:89:26:D1	9000	0	3	0	3440	TRUNK	enabled	enabled	N/A	N/A	N/A



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



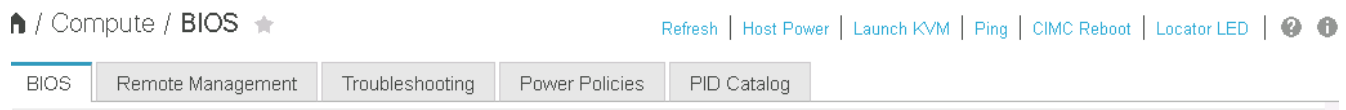
クラスタに追加するノードに対してこの手順を完了しておく必要があります。

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。

Network Adapters

Select the adapters for this host's default management network connection. Use two or more adapters for fault-tolerance and load-balancing.

Device Name	Hardware Label (MAC Address)	Status
<input type="checkbox"/> vmnic0	LOM Port 1 (...:5a:b5:8d:6e)	Connected
<input type="checkbox"/> vmnic1	LOM Port 2 (...:5a:b5:8d:6f)	Disconnected
<input checked="" type="checkbox"/> vmnic2	VIC-MLOM-eth0 (...:70:6c:cc)	Connected (...)
<input type="checkbox"/> vmnic3	VIC-iSCSI-A (...:3c:70:6c:cd)	Connected (...)
<input checked="" type="checkbox"/> vmnic4	VIC-MLOM-eth2 (...:70:6c:ce)	Connected (...)
<input type="checkbox"/> vmnic5	VIC-iSCSI-B (...:3c:70:6c:cf)	Connected (...)

<D> View Details <Space> Toggle Selected

<Enter> OK <Esc> Cancel

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。

iScsiBootPG-A - Edit Settings

Properties

Security

Traffic shaping

Teaming and failover

Load balancing

Network failure detection

Notify switches

Failback

Failover order

☒ Override



Active adapters

 vmnic3

Standby adapters

Unused adapters

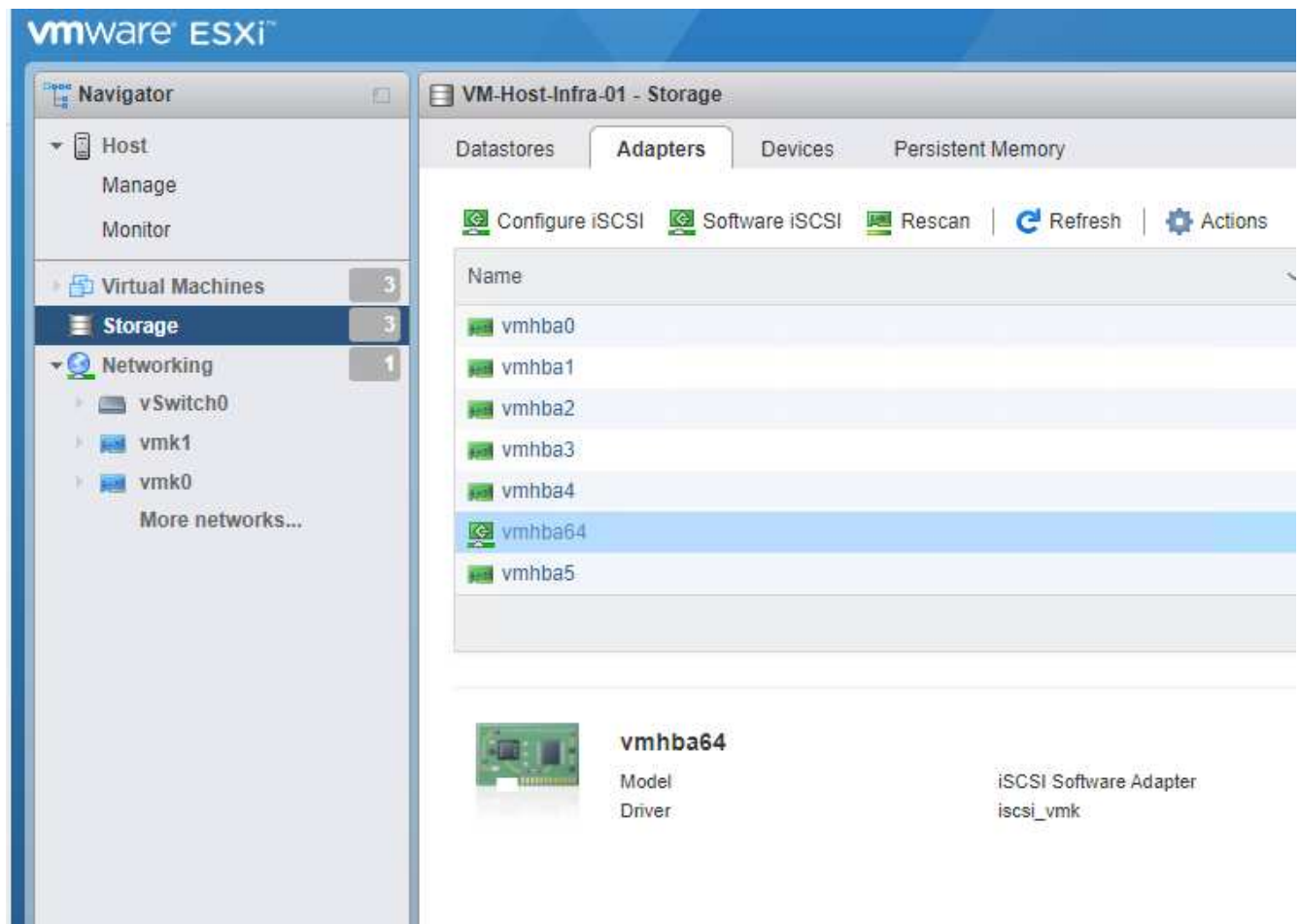
 vmnic5

Select active and standby adapters

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 ☐ Disabled ☒ Enabled

▶ Name & alias iqn.1992-01.com.cisco:ucsA-01

▶ CHAP authentication Do not use CHAP

▶ Mutual CHAP authentication Do not use CHAP

▶ Advanced settings Click to expand

Network port bindings No port bindings

Static targets

Add static target Remove static target Edit settings

Target	Address	Port
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.183.105	3260
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.184.106	3260
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.183.106	3260
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.184.105	3260

Dynamic targets

Add dynamic target Remove dynamic target Edit settings

Address	Port
172.21.183.105	3260
172.21.184.105	3260
172.21.183.106	3260
172.21.184.106	3260

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
172.21.183.105	3260
172.21.184.105	3260
172.21.183.106	3260
172.21.184.106	3260



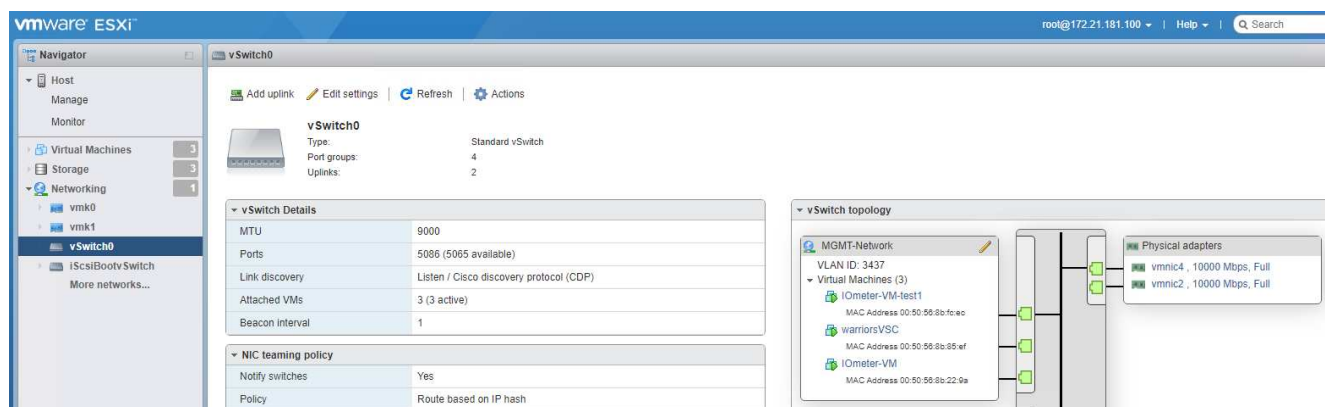
iSCSI LIF の IP アドレスは、ネットアップクラスタで network interface show コマンドを実行するか、System Manager の Network Interfaces タブで確認できます。

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。

- 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。

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

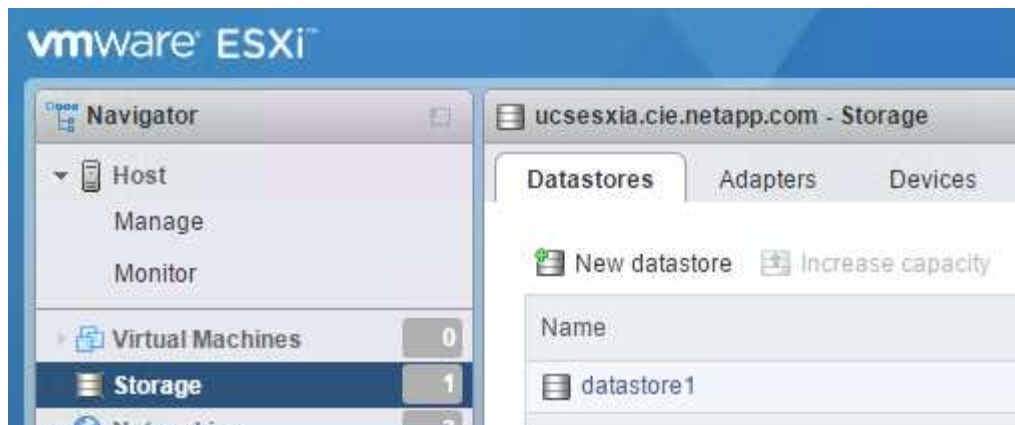


ESXi ネットワークの設定には、ライセンスで許可されている場合に VMware vSphere Distributed Switch を使用するなどの方法が多数あります。ビジネス要件を満たす必要がある場合は、FlexPod Express で代替ネットワーク構成がサポートされます。

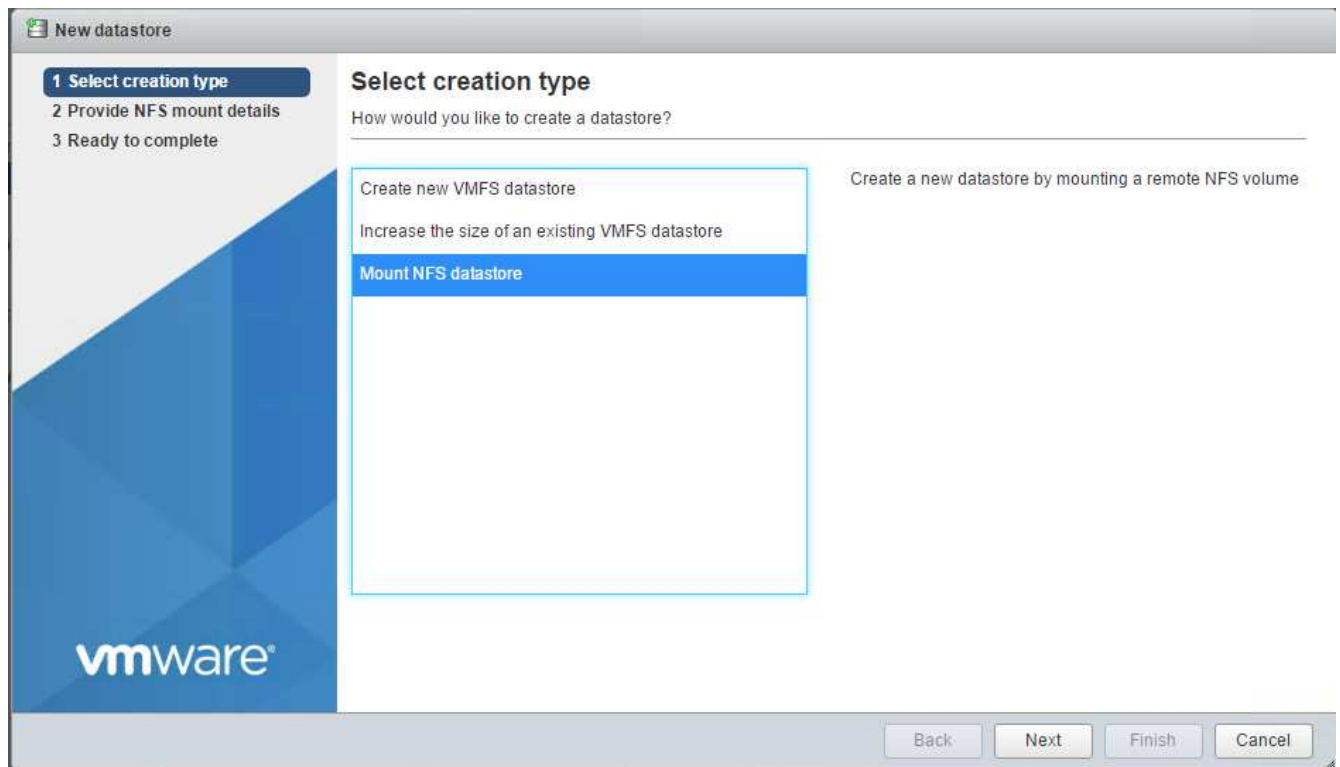
最初のデータストアをマウント

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

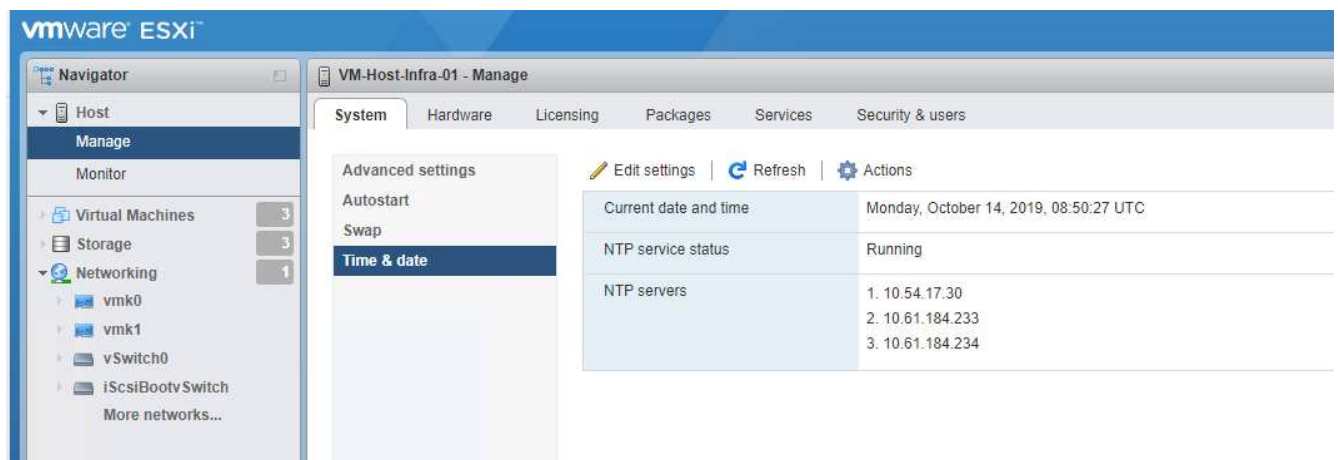
- 名前： infra_swap
- NFS サーバ： \<<var_nodeA_nfs_lif>
- 共有： /infra_swap

- 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。

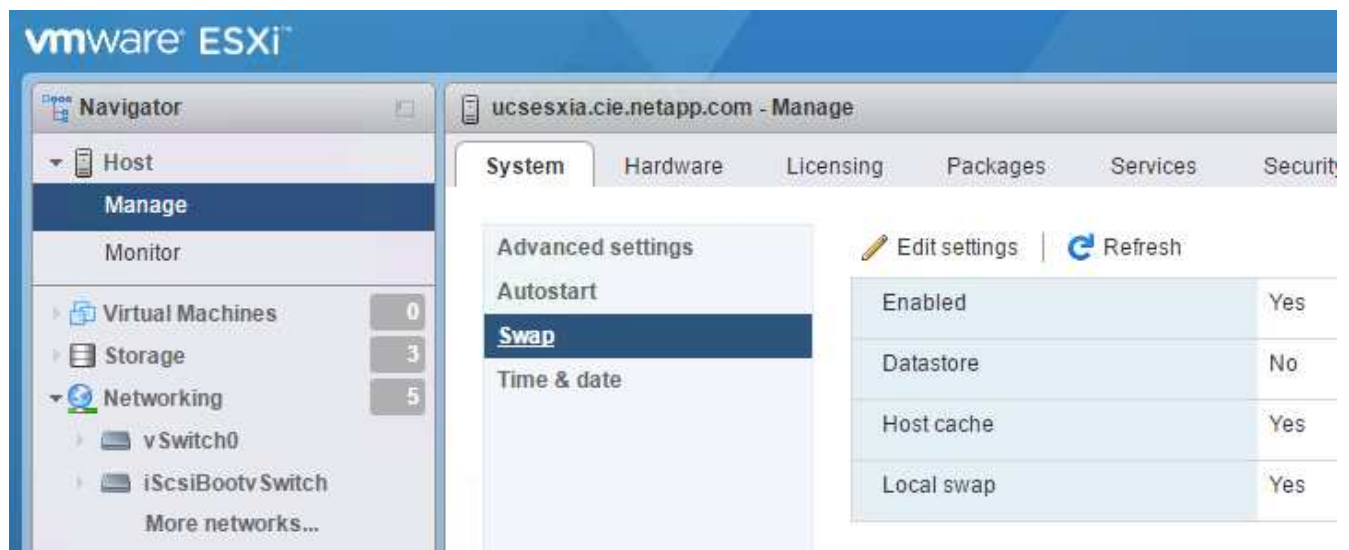
1. 左側のナビゲーションペインで、[管理] をクリックします。右側のペインで [システム] を選択し、[時刻と日付] をクリックします。
2. Use Network Time Protocol （NTP クライアントを有効にする）を選択します。
3. NTP サービスのスタートアップポリシーとして、Start and Stop With Host を選択します。
4. NTP サーバとして「<<var_ntp>>」と入力します。複数の NTP サーバを設定できます。
5. [保存] をクリックします。



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。

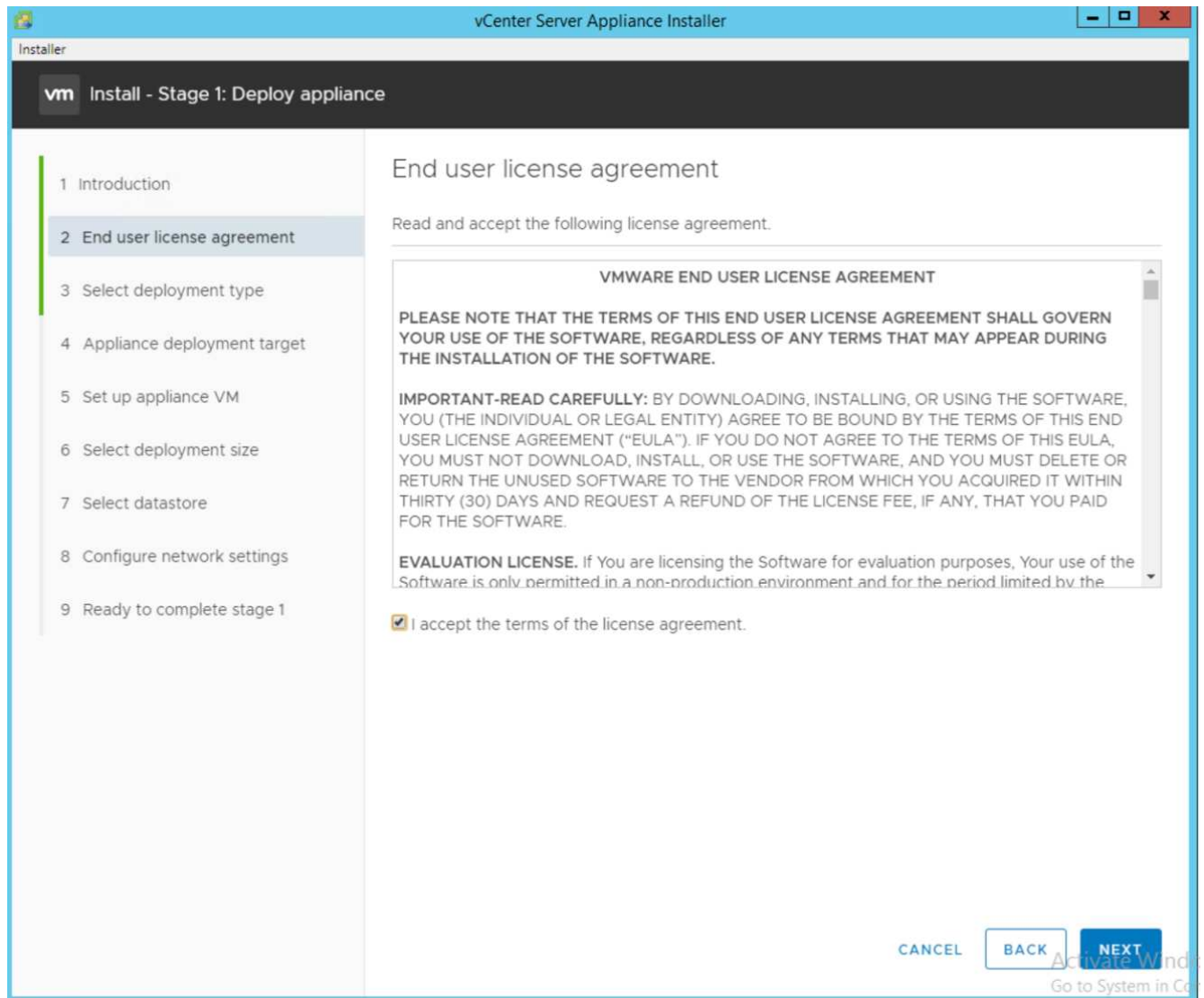


FlexPod Express では、VMware vCenter Server Appliance （VCSA）を使用します。

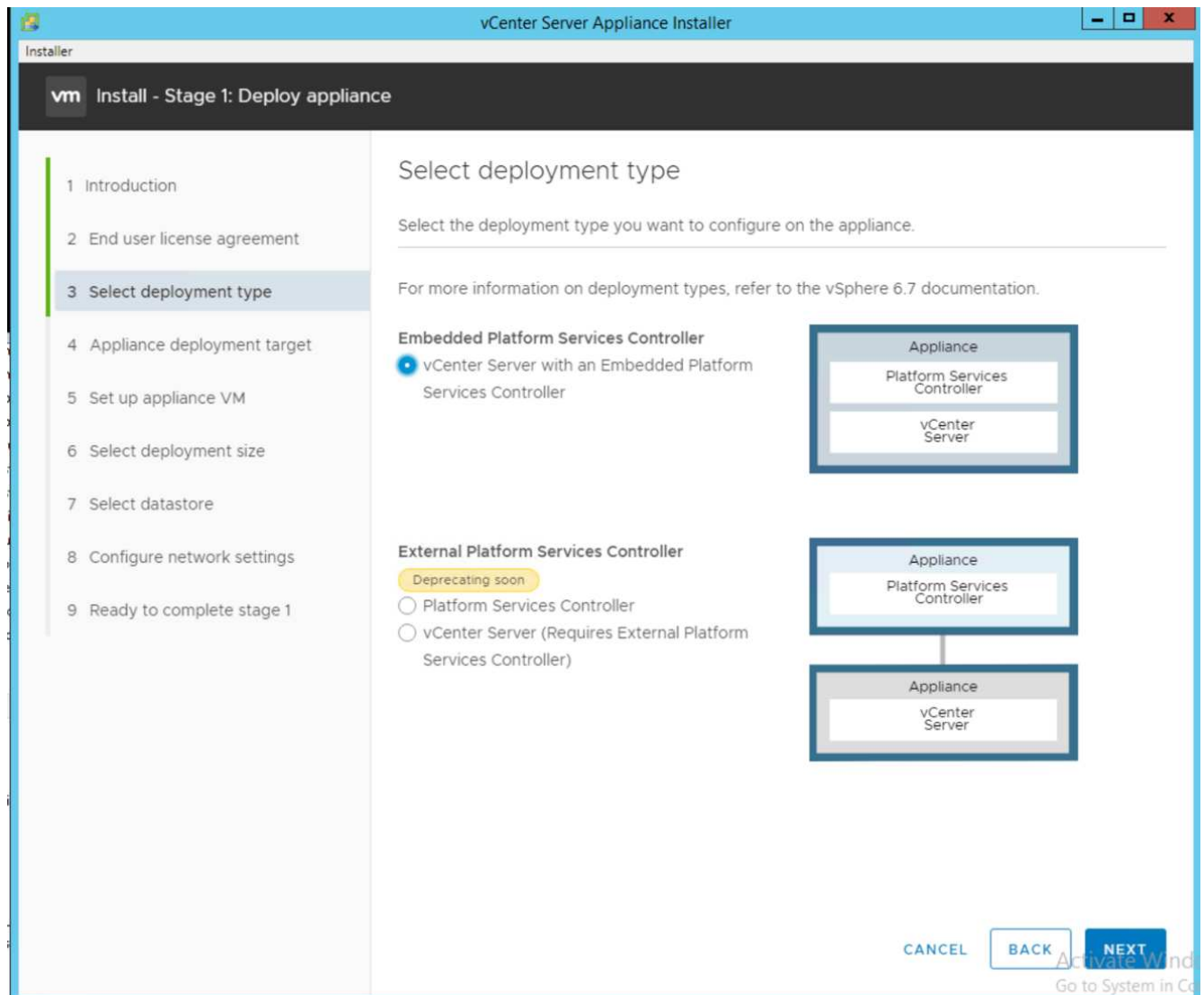
VMware vCenter Server Appliance をダウンロードします

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。

vCenter Server Appliance Installer

Installer

vm Install - Stage 1: Deploy vCenter Server Appliance 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	172.21.181.100	?
HTTPS port	443	
User name	root	?
Password	

CANCEL BACK NEXT

Activate Windows
Go to System in Settings

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。

vCenter Server Appliance Installer

Installer

vm Install - Stage 1: Deploy vCenter Server Appliance 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 ⓘ

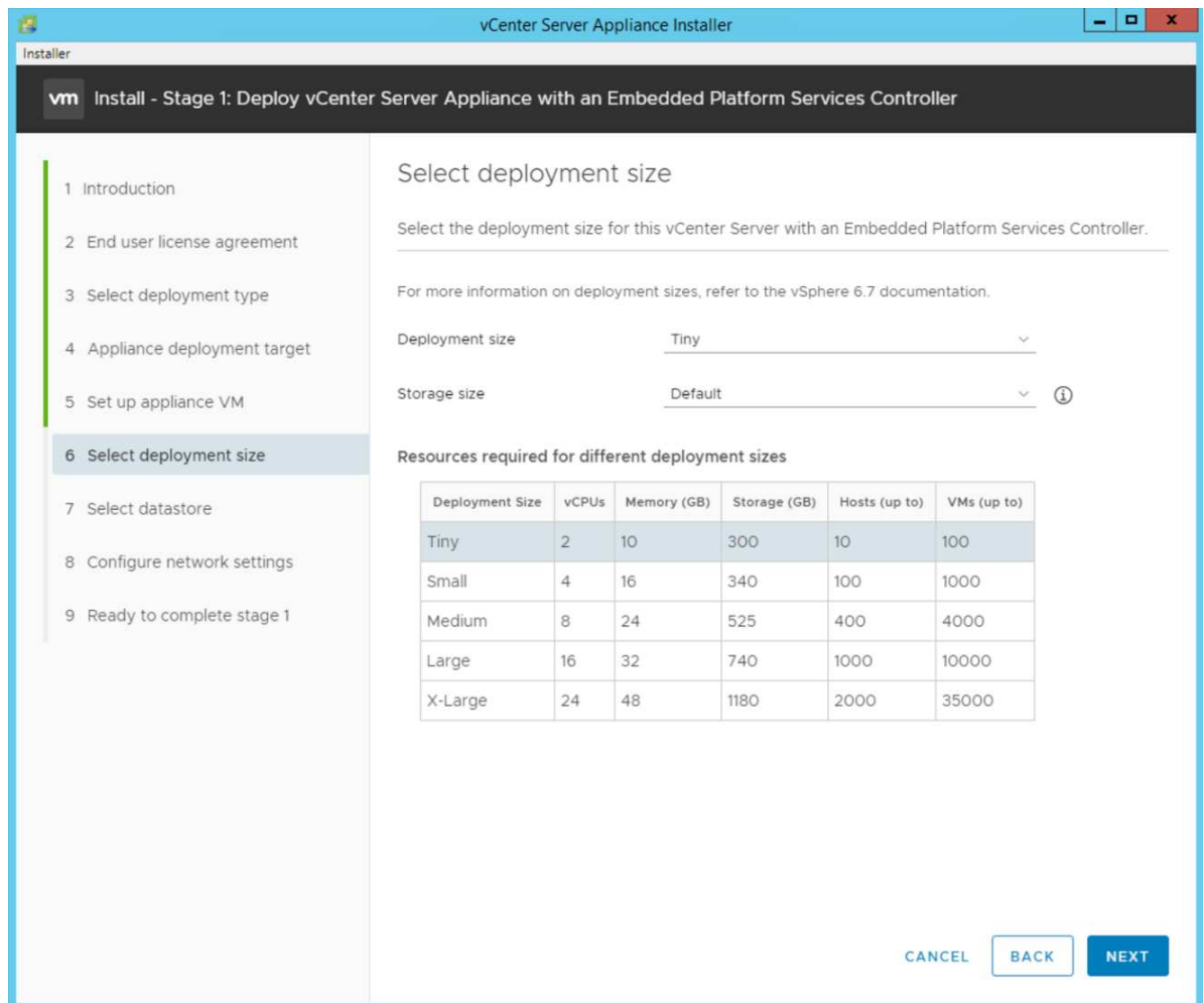
Set root password ⓘ

Confirm root password

CANCEL BACK NEXT

Activate Windows
Go to System in Centre

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。

Installer

vCenter Server Appliance Installer

vm Install - Stage 1: Deploy vCenter Server Appliance 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

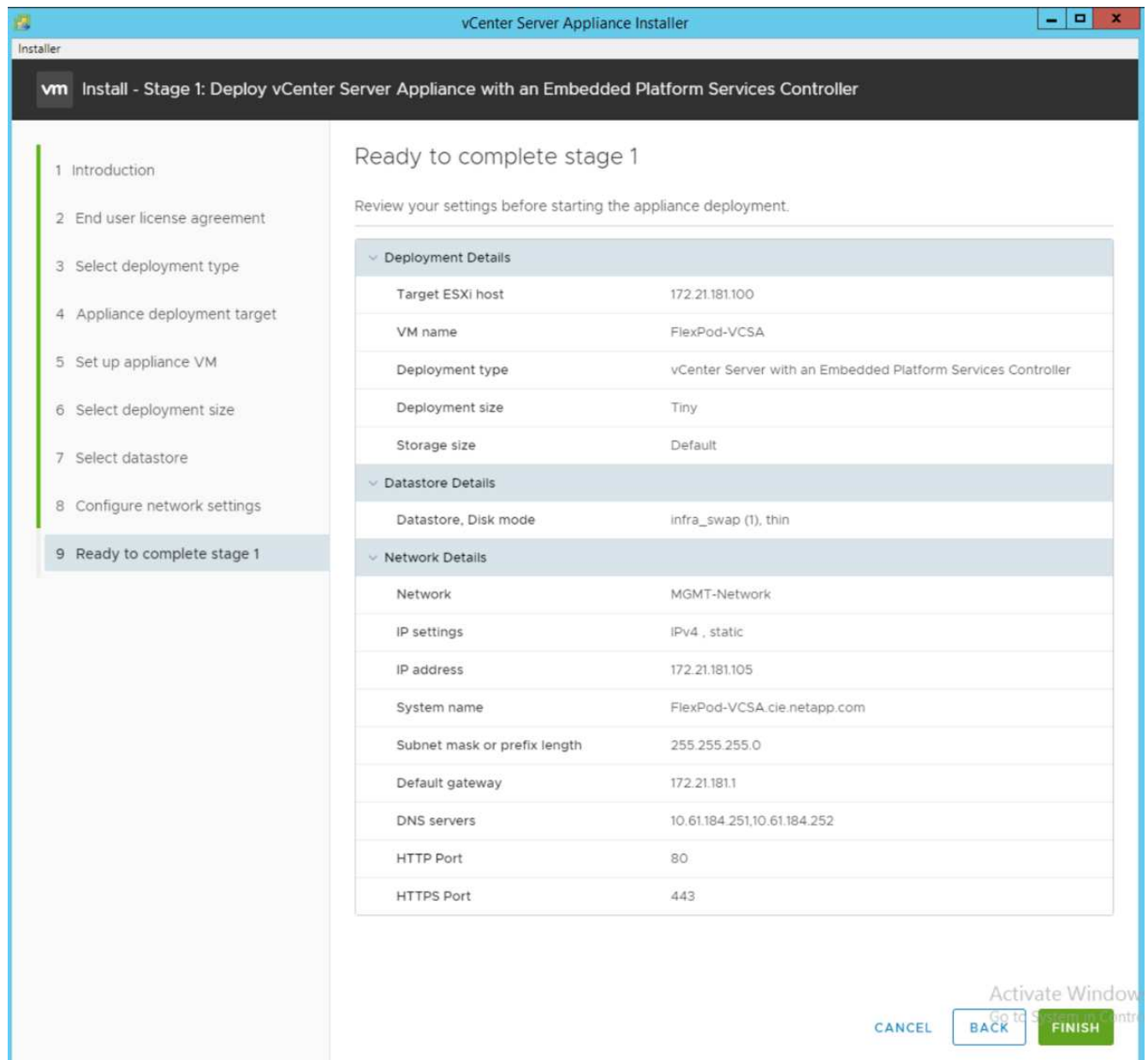
Configure network settings for this appliance

Network	MGMT-Network	①
IP version	IPv4	
IP assignment	static	
FQDN	FlexPod-VCSA.cie.netapp.com	①
IP address	172.21.181.105	
Subnet mask or prefix length	255.255.255.0	①
Default gateway	172.21.181.1	
DNS servers	10.61.184.251,10.61.184.252	
Common Ports		
HTTP	80	
HTTPS	443	

CANCEL BACK NEXT

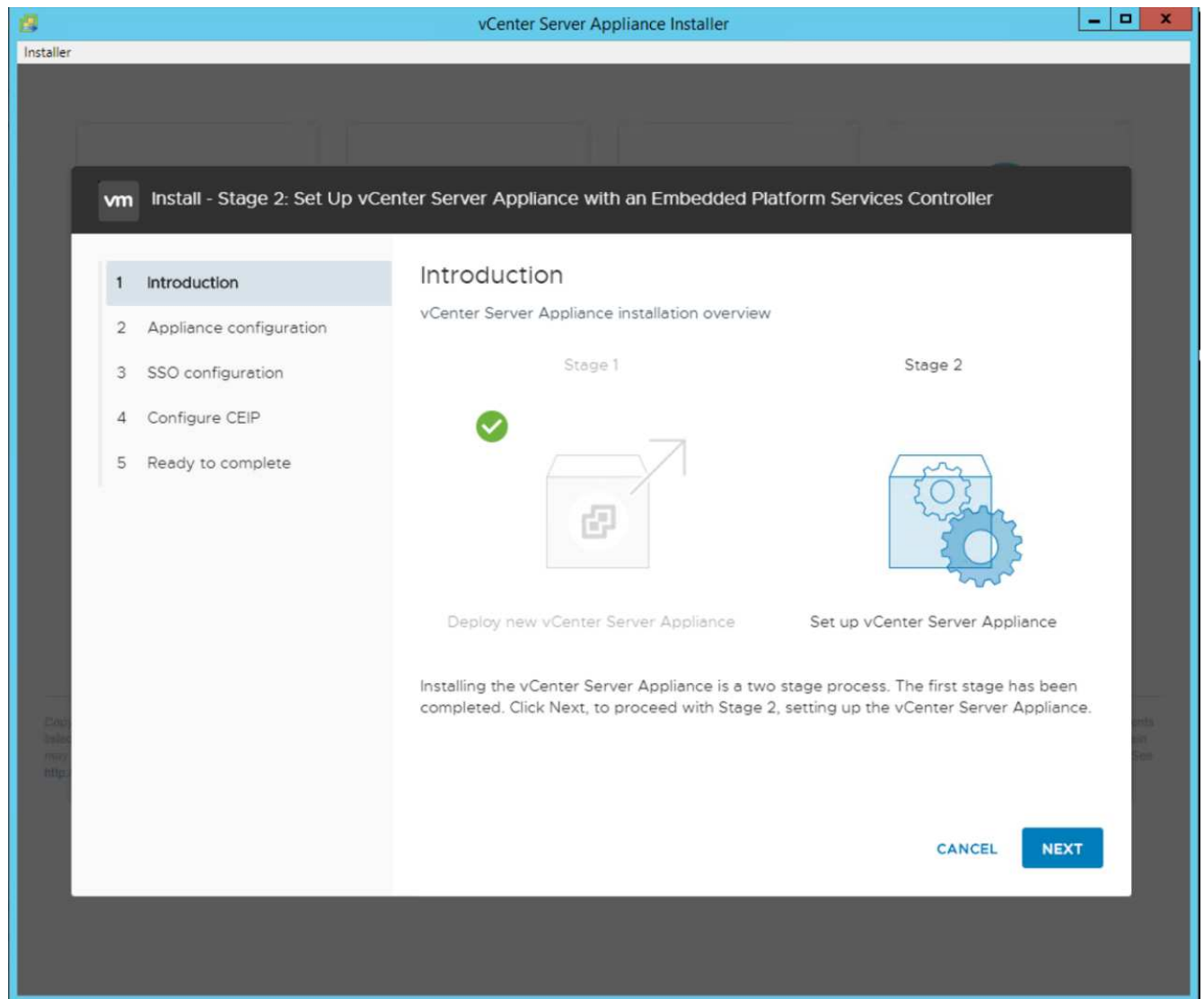
Activate Windows
Go to System in Control

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。

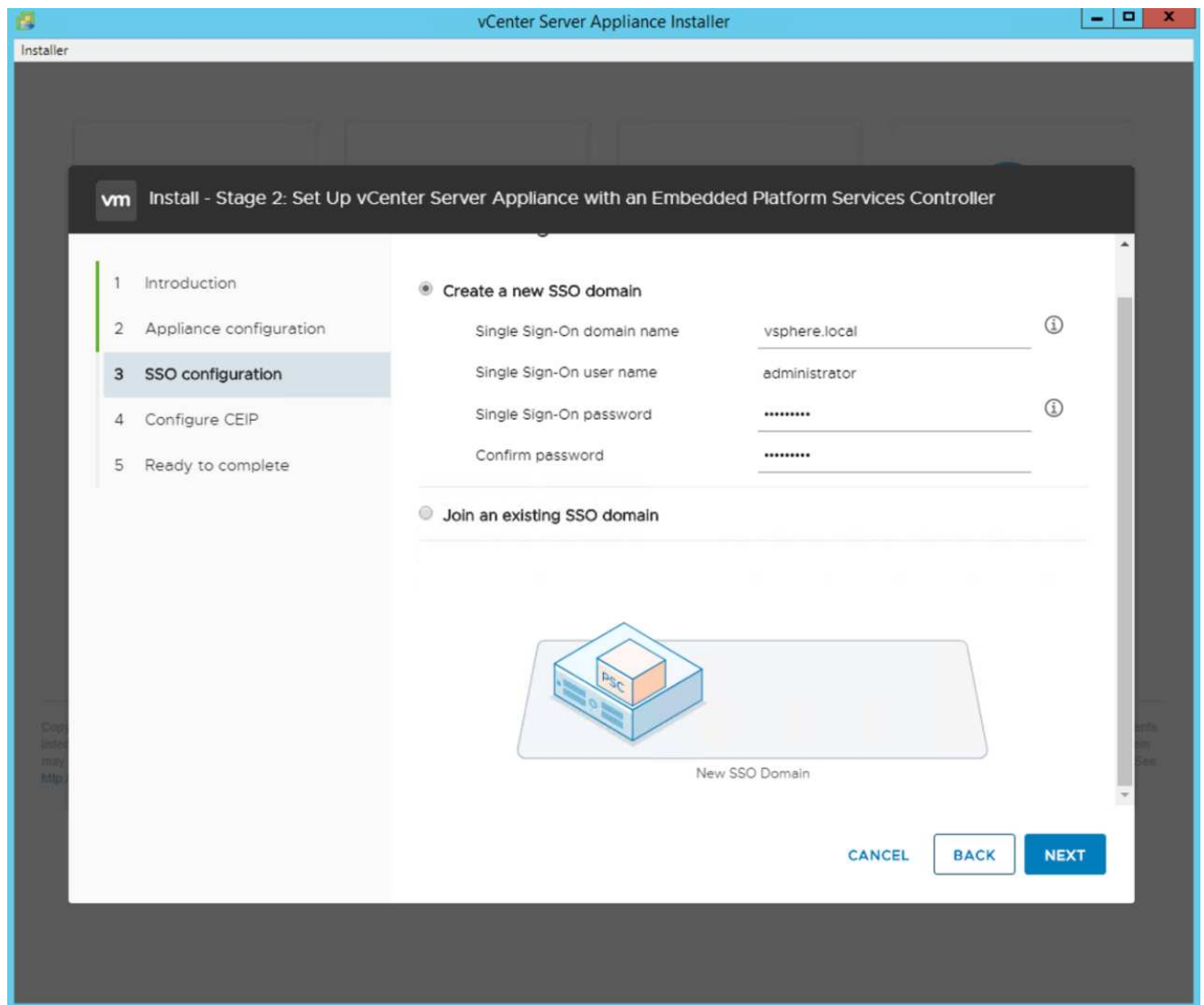


vCSA がインストールされます。このプロセスには数分かかります。

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。

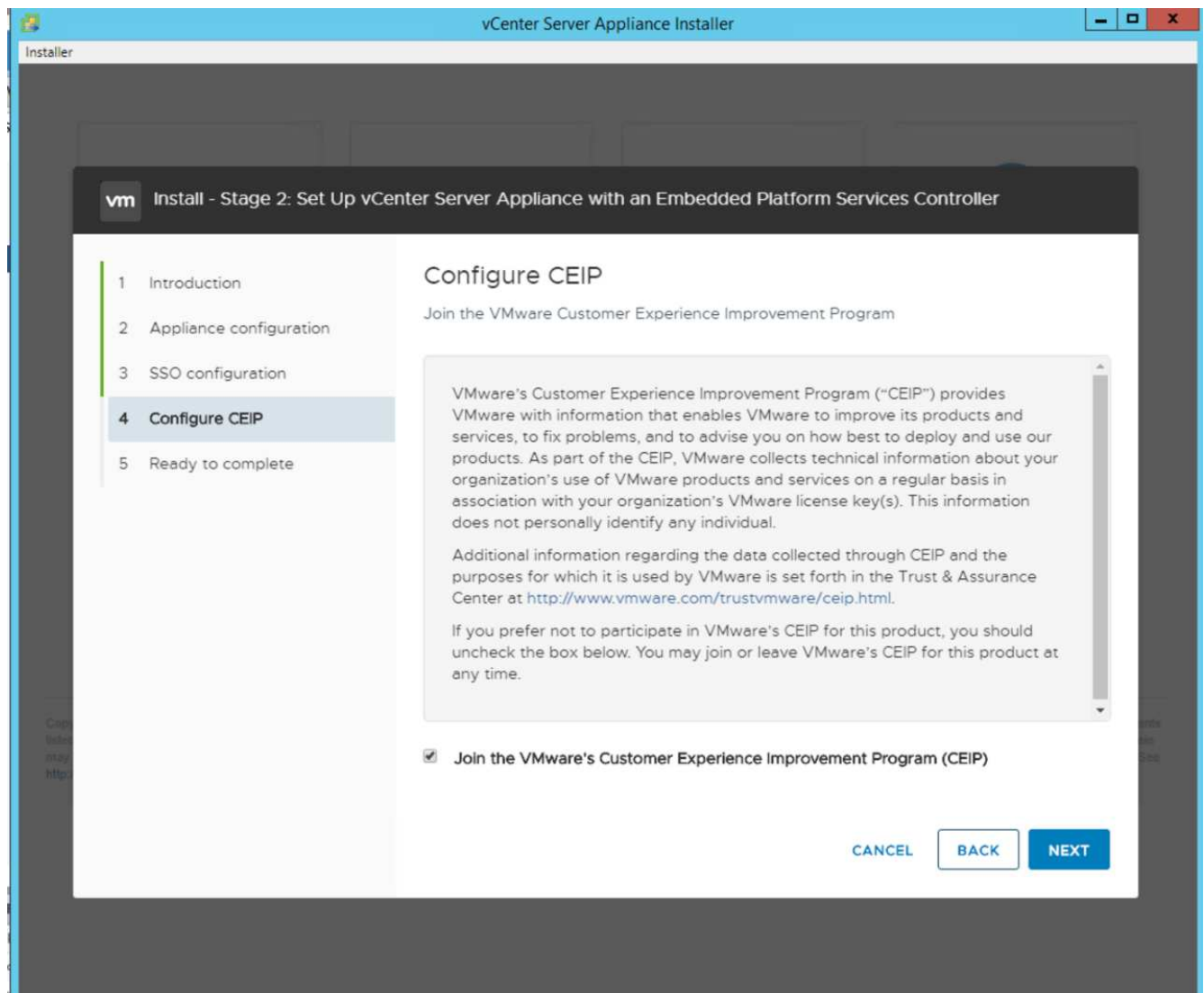


18. NTP サーバのアドレスとして「\<<var_ntp_id>>」と入力します。複数の NTP IP アドレスを入力できます。
19. vCenter Server High Availability （ HA ；高可用性）を使用する場合は、SSH アクセスが有効になっていることを確認してください。
20. SSO ドメイン名、パスワード、およびサイト名を設定します。次へをクリックします。

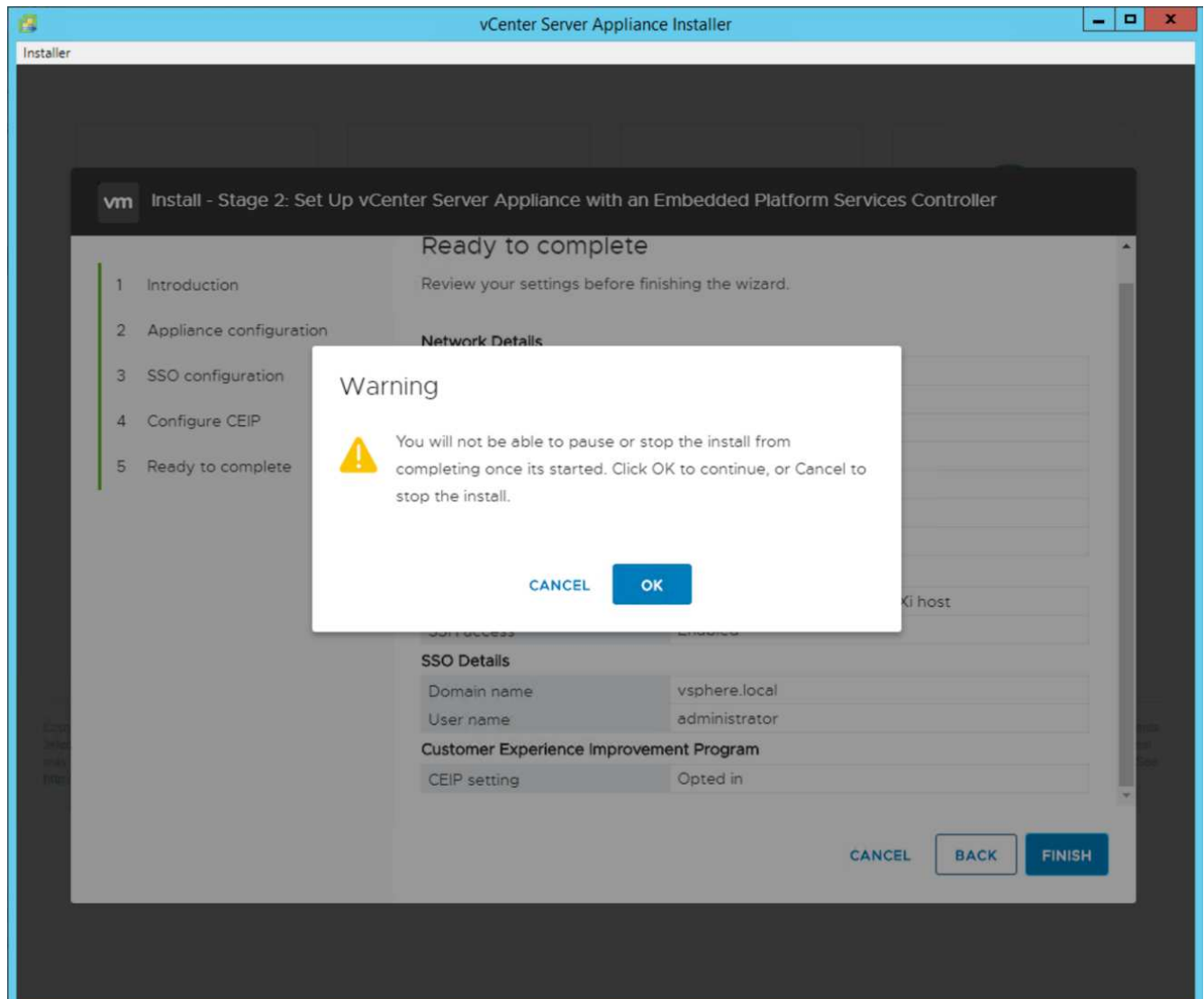


特に 'vspher.local' ドメイン名から外れる場合は 'これらの値を参考にしてください

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@vsphere.local` [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。

New Cluster | FlexPod-Datacenter

Name	FlexPod-Cluster
Location	FlexPod-Datacenter
DRS	<input checked="" type="checkbox"/>
vSphere HA	<input checked="" type="checkbox"/>
vSAN	<input type="checkbox"/>

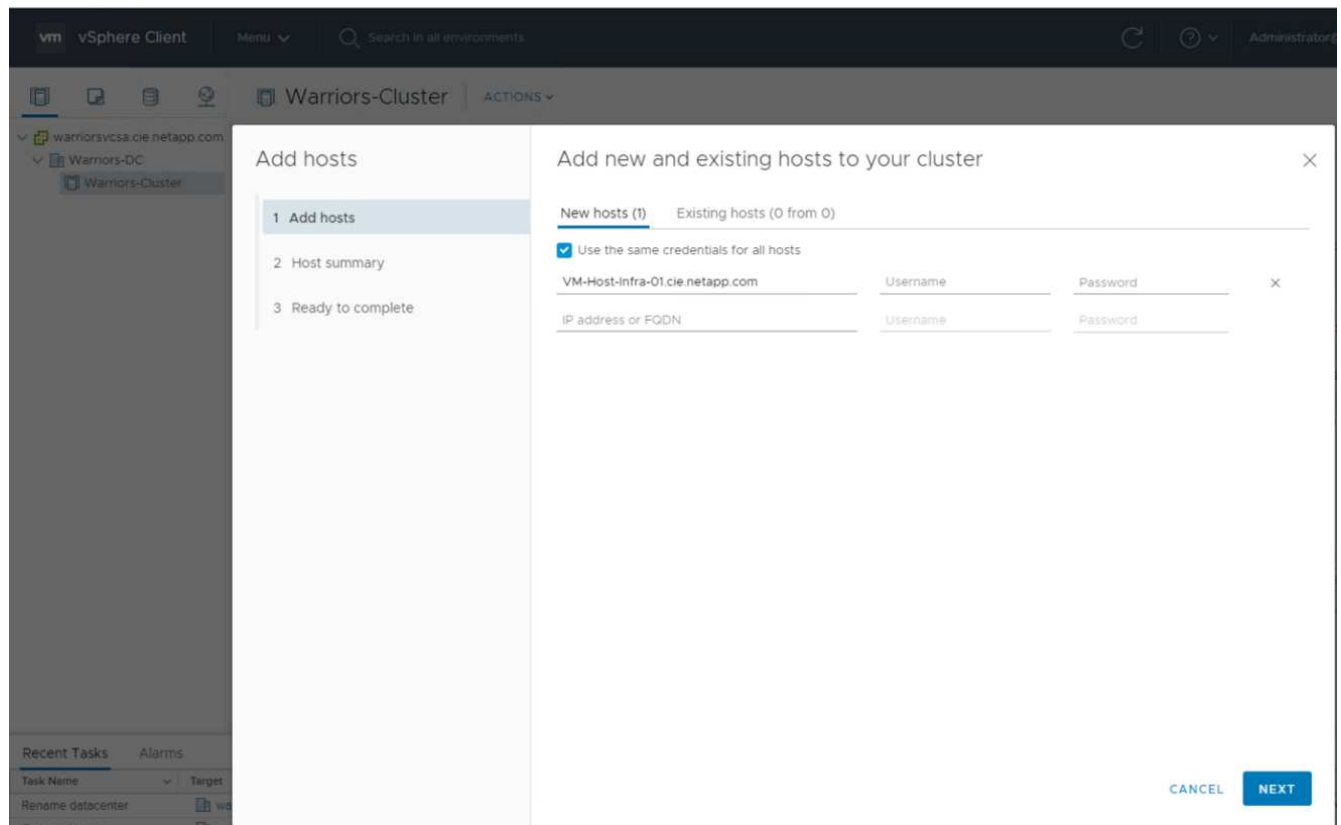
These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

CANCEL **OK**

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



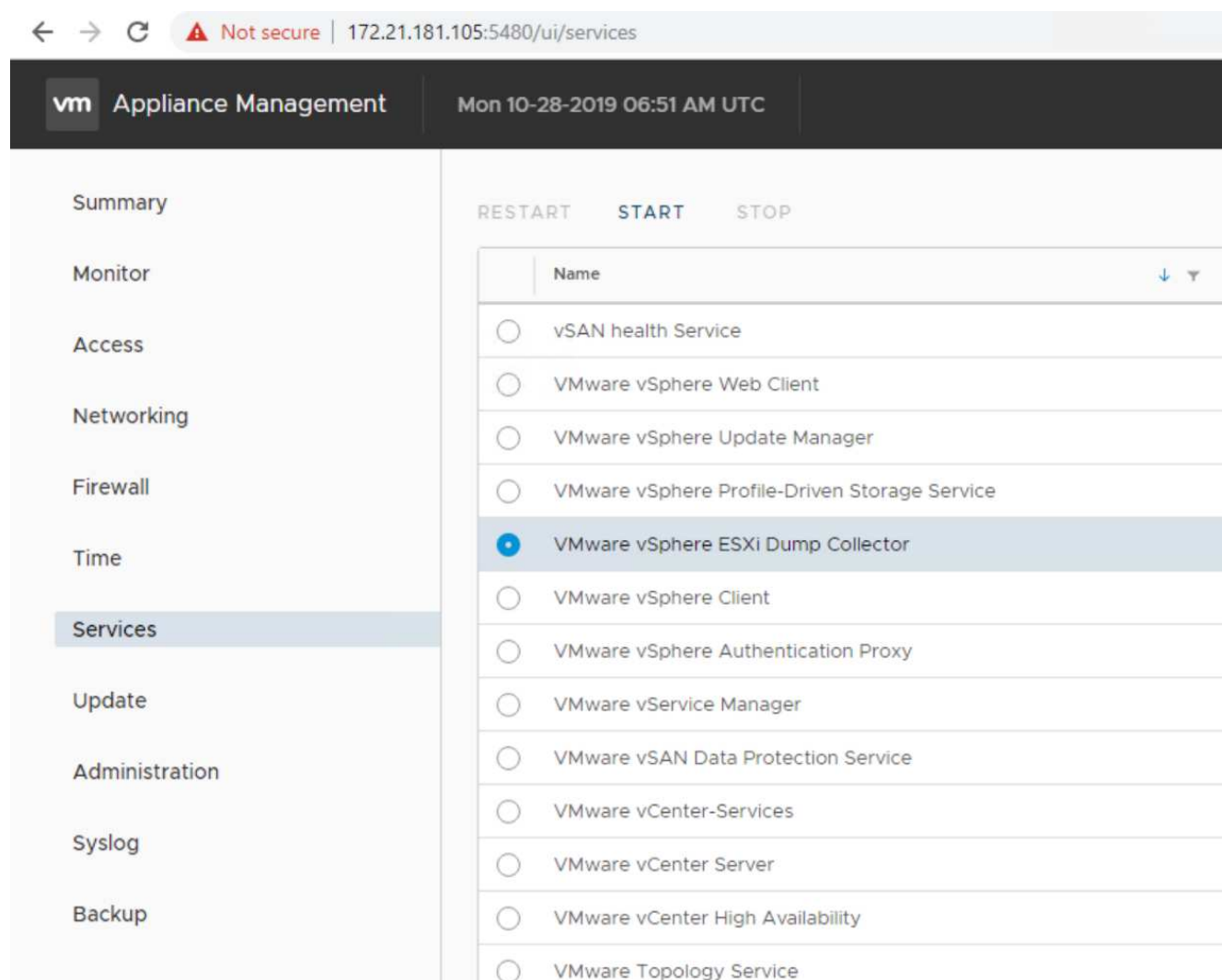
FlexPod 構成にホストを追加する場合は、この手順を実行する必要があります。

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  
Verified 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"](#)

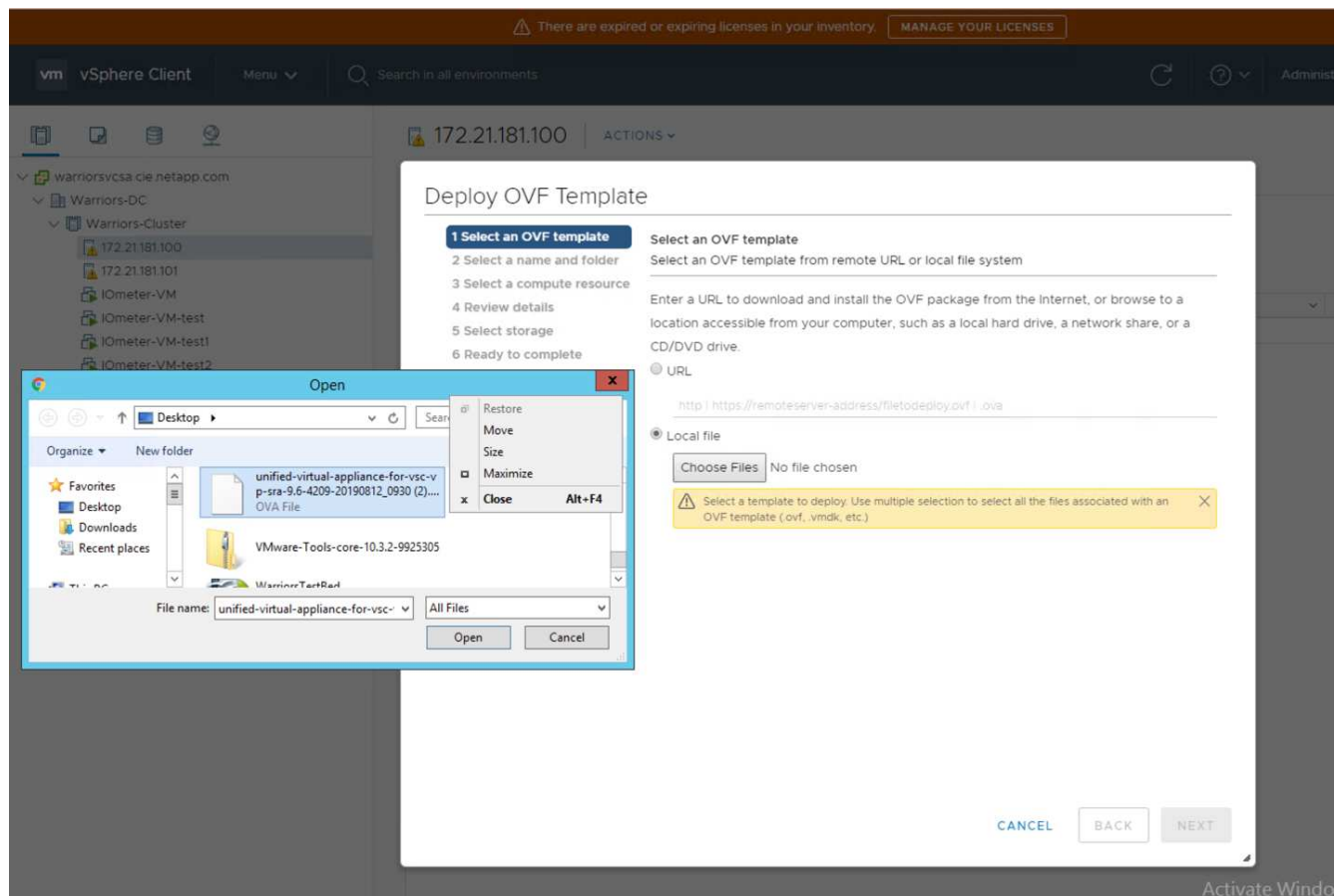
NetApp Virtual Storage Console 9.6 の導入手順

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。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource

4 Review details

- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Review details

Verify the template details.

Publisher	No certificate present
Product	Virtual Appliance - NetApp VSC, VASA Provider and SRA for ONTAP
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp VSC, VASA Provider, and SRA virtual appliance for NetApp storage systems. For more information or support please visit http://www.netapp.com/
Download size	1.0 GB
Size on disk	2.1 GB (thin provisioned)
	53.0 GB (thick provisioned)

CANCEL

BACK

NEXT

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。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- 6 Select storage**
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type
infra_datastore	75 GB	360 KB	75 GB	NF
infra_datastore1	475 GB	639.9 GB	276.86 GB	NF
infra_swap (1)	100 GB	4.98 GB	95.02 GB	NF

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

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。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- 7 Select networks**
- 8 Customize template
- 9 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	MGMT-Network
1 items	

IP Allocation Settings

IP allocation:

Static - Manual

IP protocol:

IPv4

CANCEL

BACK

NEXT

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。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- ✓ 8 Customize template**
- 9 Ready to complete

vCenter Server Address (*)

Specify the IP address/hostname of an existing vCenter to register to.

172.21.181.105

Port (*)

Specify the HTTPS port of an existing vCenter to register to.

443

Username (*)

Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*)

Specify the password of an existing vCenter to register to.

Password:

Confirm Password:

✓ **Network Properties** 8 settings

Host Name

Specify the hostname for the appliance. (Leave blank if DHCP is desired)

CANCEL

BACK

NEXT

10. 入力した設定の詳細を確認し、Finish をクリックして NetApp-VSC VM の導入を完了します。
11. NetApp-VSC VM の電源をオンにして、VM コンソールを開きます。
12. NetApp - VSC VM のブートプロセス中に、VMware Tools のインストールを求めるプロンプトが表示されます。vCenter で、[NetApp-VSC VM] -[ゲスト OS] -[VMware Tools のインストール] を選択します。

Booting VSC, VASA Provider, and SRA virtual appliance...Please wait...

VMware Tools OVF vCenter configuration not found.

VMware Tools OVF vCenter configuration not found.

VMware Tools OVF vCenter configuration not found.

VMware Tools installation

Before you can continue the VSC, VASA Provider, and SRA virtual appliance installation, you must install the VMware Tools:

1. Select VM > Guest OS > Install VMware Tools.

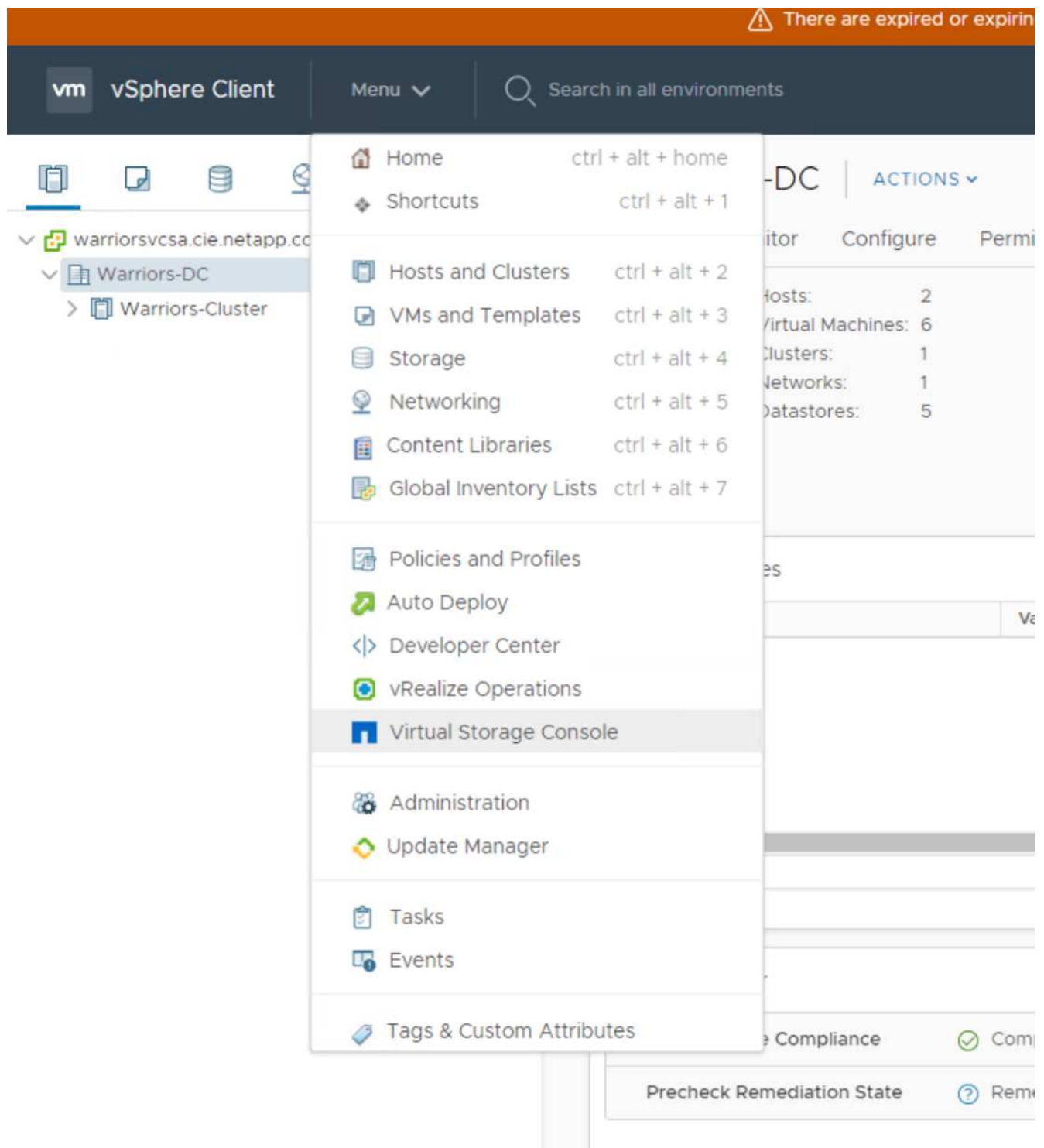
OR

Click on "Install VMware Tools" pop-up box on the vSphere Web Client.

2. Follow the prompts provided by the VMware Tools wizard.

Once you click on mount, the installation process will automatically continue.

13. OVF テンプレートのカスタマイズ時に、ネットワーク設定と vCenter の登録情報が提供されました。そのため、NetApp-VSC VM の実行後、VSC、vSphere API for Storage Awareness（VASA）、および VMware Storage Replication Adapter（SRA）が vCenter に登録されます。
14. vCenter Client からログアウトし、再度ログインします。ホームメニューから、NetApp VSC がインストールされていることを確認します。

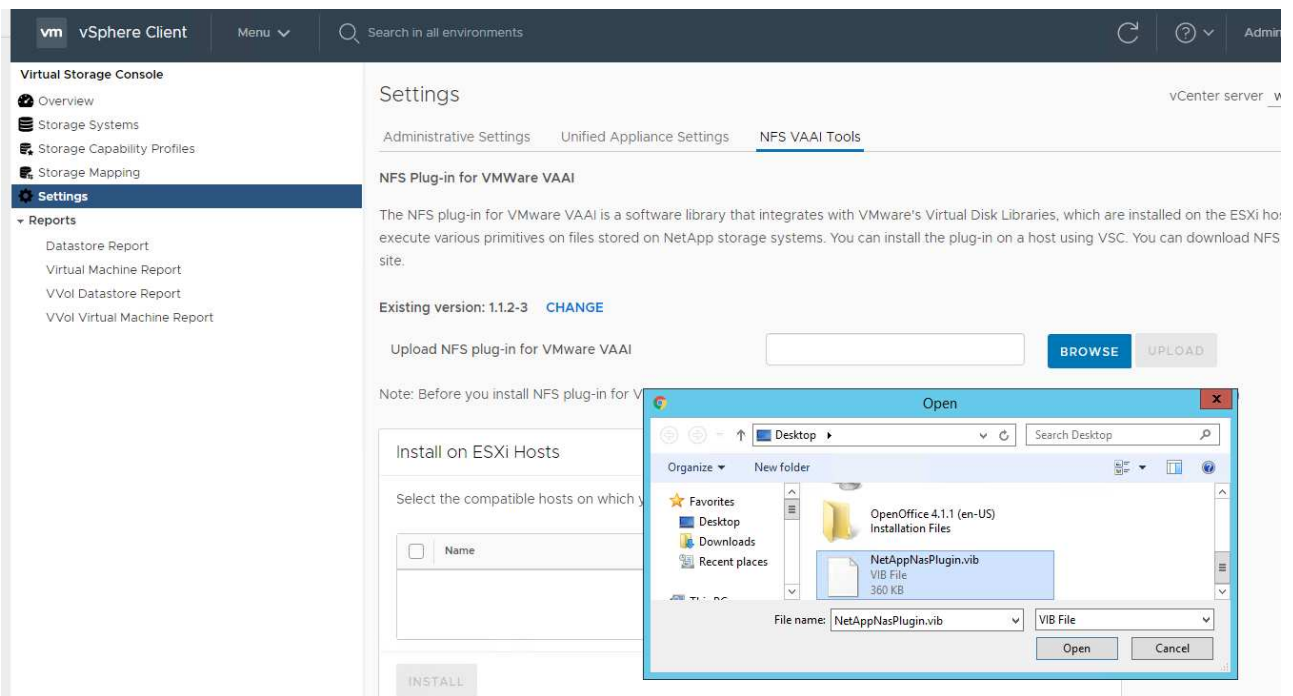


NetApp NFS VAAI Plug-in をダウンロードしてインストールします

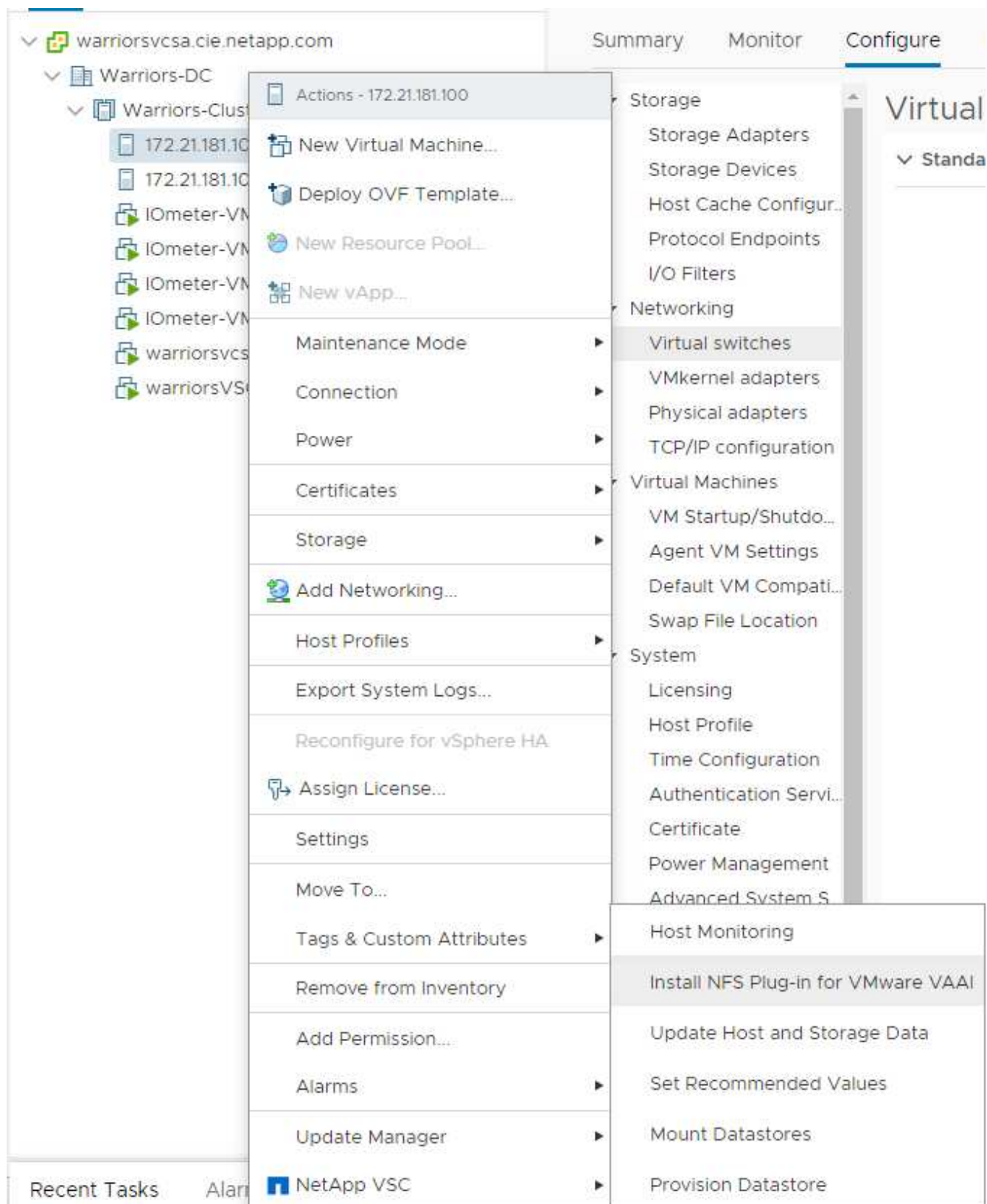
NetApp NFS VAAI Plug-in をダウンロードしてインストールするには、次の手順を実行します。

1. NetApp NFS Plug-in 1.1.2 for VMware' をダウンロードしますNFS プラグインのダウンロードページから VIB ファイルをダウンロードし、ローカルマシンまたは管理ホストに保存します。
2. NetApp NFS Plug-in for VMware VAAI をダウンロードします。
 - a. にアクセスします ["ソフトウェアダウンロードページ"](#)。

- b. 下にスクロールして、 NetApp NFS Plug-in for VMware VAAI をクリックします。
- c. vSphere Web Client のホーム画面で、 Virtual Storage Console を選択します。
- d. Virtual Storage Console > Settings > NFS VAAI Tools で、 ファイルを選択し、ダウンロードしたプラグインが格納されている場所を参照して、 NFS Plug-in をアップロードします。



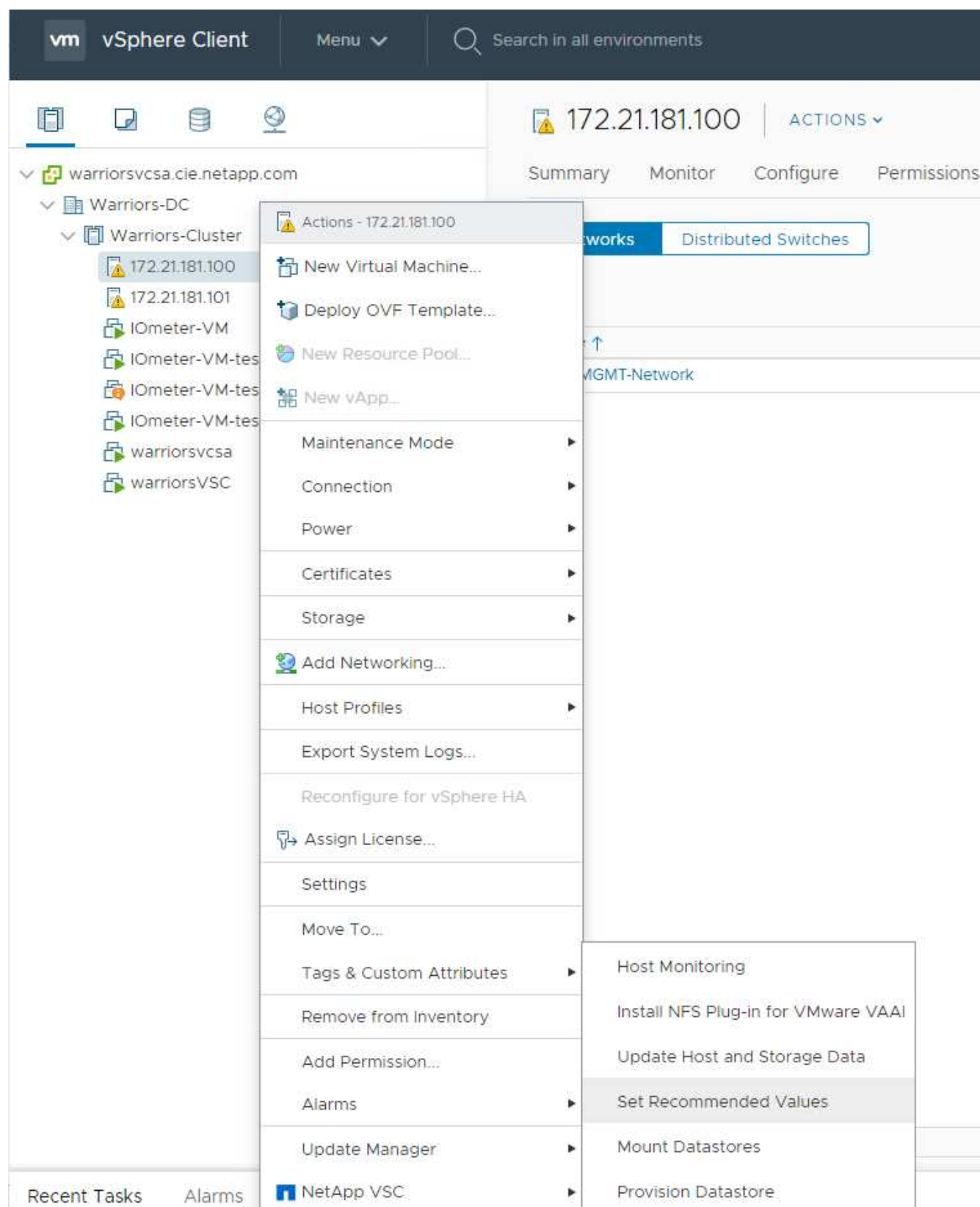
- 3. アップロードをクリックして、プラグインを vCenter に転送します。
- 4. ホストを選択し、 NetApp VSC > Install NFS Plug-in for VMware VAAI の順に選択します。



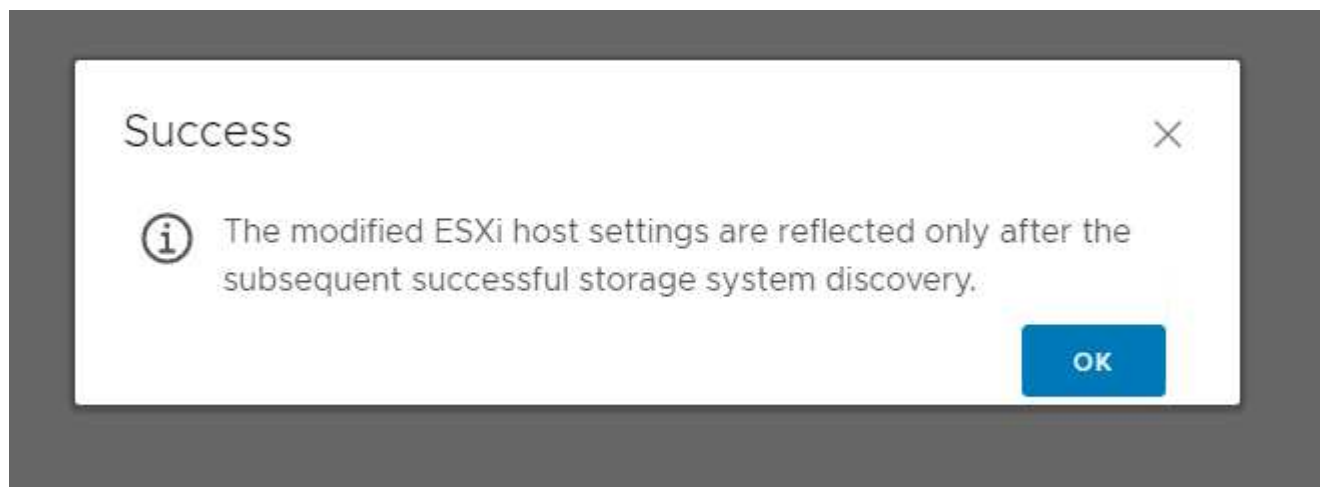
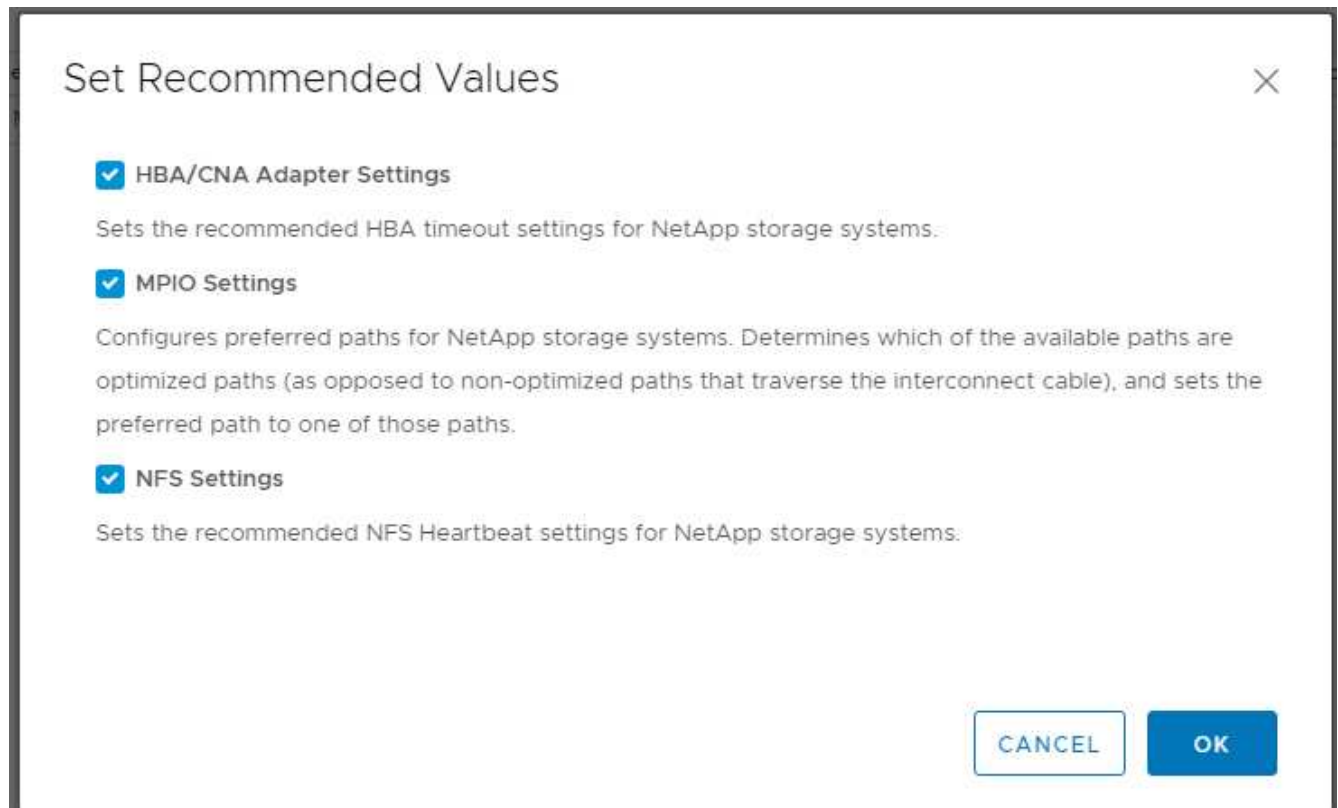
ESXi ホストのストレージ設定を最適化します

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

1. ホーム画面で、vCenter > Hosts and Clusters を選択します。各 ESXi ホストを右クリックし、NetApp VSC > Set Recommended Values を選択します。



2. 選択した vSphere ホストに適用する設定を確認してください。[OK] をクリックして設定を適用します。



3. これらの設定を適用したら、ESXi ホストをリブートします。

まとめ

FlexPod Express は、業界をリードするコンポーネントを使用した検証済みの設計を提供することで、シンプルで効果的な解決策を実現します。コンポーネントの追加による拡張により、FlexPod Express は特定のビジネスニーズに合わせて調整できます。FlexPod Express は、中小規模の企業や、特定用途向けのソリューションを必要とする企業向けに設計されています。

謝辞

著者はジョンジョージをこの設計への彼のサポートそして貢献のために認めたいと思う。

追加情報の参照先

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

ネットアップの製品マニュアル

[http://docs. "ネットアップ".com](http://docs.netapp.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"](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

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。