



FlexPod Express と VMware vSphere 6.7U1 、および直接接続型の IP ベースストレージを搭載した NetApp AFF A220

FlexPod

NetApp
March 25, 2024

目次

FlexPod Express と VMware vSphere 6.7U1、および直接接続型の IP ベースストレージを搭載した NetApp AFF A220	1
NVA-1131 - 導入：VMware vSphere 6.7U1 搭載の FlexPod Express と、直接接続型の IP ベースのストレージを搭載した NetApp AFF A220	1
解決策の概要	1
テクノロジー要件	5
FlexPod エクスプレスケーブル接続情報	6
導入手順	7
まとめ	114
追加情報	115

FlexPod Express と VMware vSphere 6.7U1、および直接接続型の IP ベースストレージを搭載した NetApp AFF A220

NVA-1131 - 導入：VMware vSphere 6.7U1 搭載の FlexPod Express と、直接接続型の IP ベースのストレージを搭載した NetApp AFF A220

ネットアップ、Sree Lakshmi Lanka です

業界のトレンドは、共有インフラとクラウドコンピューティングへの大規模なデータセンターの移行を示しています。さらに、リモートオフィスやブランチオフィスにもシンプルで効果的な解決策を導入し、データセンターでよく使用されているテクノロジーを活用することができます。

FlexPod Express は、Cisco Unified Computing System（Cisco UCS）、Cisco Nexus ファミリースイッチ、およびネットアップストレージテクノロジーを基盤とした、事前設計されたベストプラクティスアーキテクチャです。FlexPod Express システムのコンポーネントは、FlexPod Datacenter と同様に、小規模な IT インフラ環境全体での管理面の相乗効果を実現します。FlexPod Datacenter と FlexPod Express は、仮想化、ベアメタル OS、エンタープライズワークロードに最適なプラットフォームです。

FlexPod Datacenter と FlexPod Express は、ベースライン構成が可能で、多種多様なユースケースや要件に対応できるよう、サイジングと最適化が可能な汎用性を備えています。FlexPod データセンターを利用している既存のお客様は、使い慣れたツールを使用して FlexPod Express システムを管理できます。FlexPod Express の新規のお客様は、環境の拡大に合わせて FlexPod データセンターの管理を容易に行うことができます。

FlexPod Express は、リモートオフィスやブランチオフィス（ROBO）、中堅企業向けの最適なインフラ基盤です。また、専用のワークロードにインフラを提供したいお客様にも最適な解決策です。

FlexPod Express は、ほぼすべてのワークロードに適した、管理しやすいインフラを提供します。

解決策の概要

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

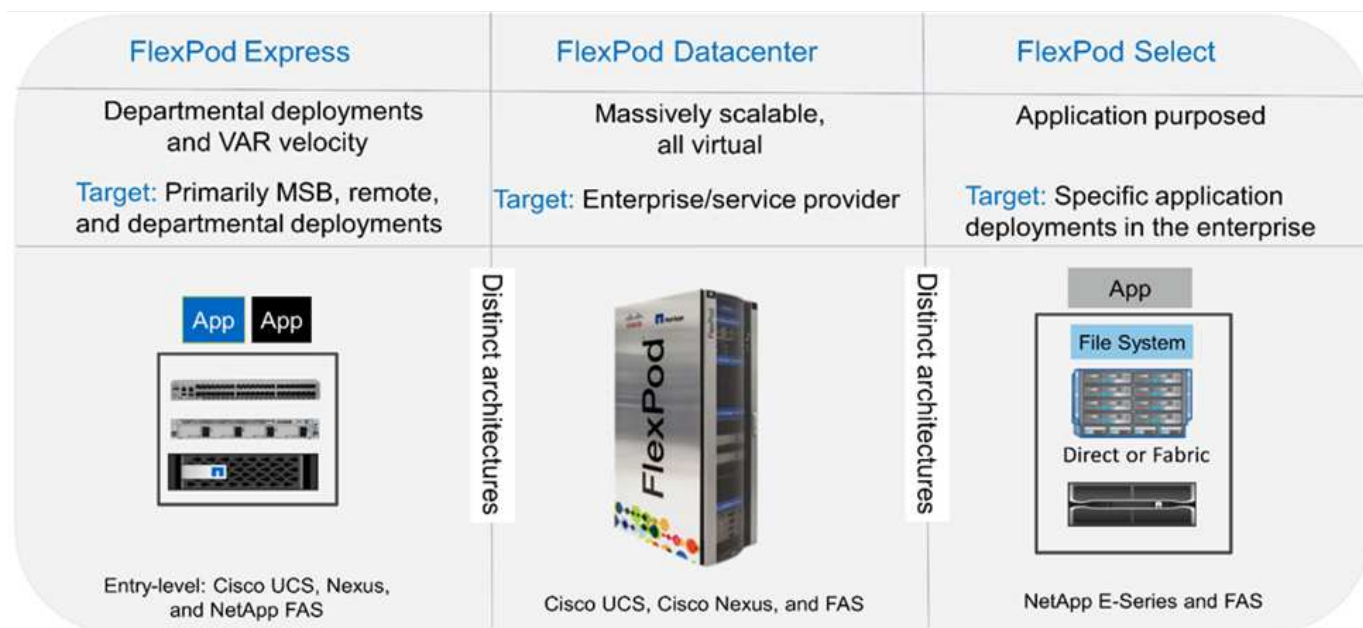
FlexPod 統合インフラプログラム

FlexPod リファレンスアーキテクチャは、Cisco Validated Design（CVD；シスコ検証済み設計）または NetApp Verified Architectures（NVA；ネットアップ検証済みアーキテクチャ）として提供されます。これらのバリエーションでサポートされない構成が作成されない場合、特定の CVD または NVA からのお客様の要件に基づく差異は認められます。

次の図に示すように、FlexPod プログラムには、FlexPod Express、FlexPod Datacenter、FlexPod Select の 3 つのソリューションが含まれています。

- * FlexPod Express * は、Cisco とネットアップが提供するテクノロジーを搭載したエントリレベルの解決策をお客様に提供します。
- * FlexPod Datacenter * は、さまざまなワークロードやアプリケーションに最適な多目的基盤を提供します。
- * FlexPod Select * は、FlexPod データセンターの最良の側面を組み込み、特定のアプリケーションにインフラストラクチャを調整します。

次の図に、解決策の技術コンポーネントを示します。



NetApp Verified Architecture プログラム

NVA プログラムは、ネットアップソリューションの検証済みアーキテクチャをお客様に提供します。NVA は、次の品質を持つ NetApp 解決策アーキテクチャを示しています。

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

このガイドでは、ネットアップストレージが直接接続された FlexPod Express の設計について詳しく説明します。次のセクションでは、この解決策の設計に使用されるコンポーネントについて説明します。

ハードウェアコンポーネント

- NetApp AFF A220
- Cisco UCS Mini
- Cisco UCS B200 M5
- Cisco UCS VIC 140/1480

- Cisco Nexus 3000 シリーズスイッチ

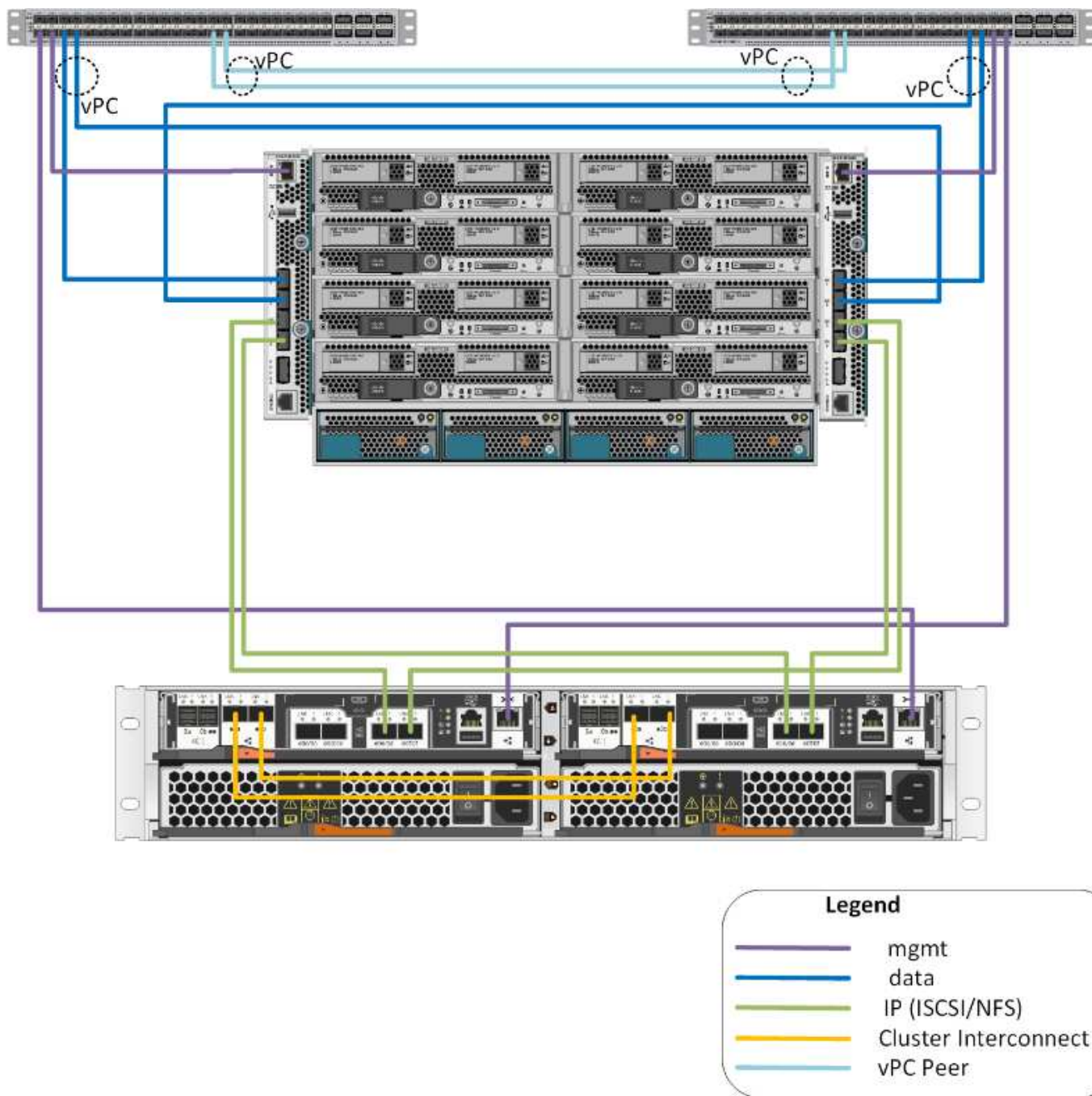
ソフトウェアコンポーネント

- NetApp ONTAP 9.5.
- VMWare vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Cisco NXOS ファームウェア 7.0(3) I6(1)

解決策テクノロジー

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。ONTAP 9.5 を実行する新しい NetApp AFF A220、Cisco Nexus 31108PCV スイッチが 2 台、VMware vSphere 6.7U1 を実行する Cisco UCS B200 M5 サーバが搭載されています。検証済みのこの解決策では、10GbE テクノロジー経由で Direct Connect IP ストレージを使用します。

次の図は、FlexPod Express と VMware vSphere 6.7U1 IP ベースの Direct Connect アーキテクチャを示しています。



ユースケースの概要

FlexPod Express 解決策は、次のようないくつかのユースケースに適用できます。

- ROBOs
- 中堅・中小企業向け
- コスト効率に優れた専用の解決策が必要な環境

FlexPod Express は、仮想ワークロードと混在ワークロードに最適です。

テクノロジー要件

FlexPod Express システムには、ハードウェアコンポーネントとソフトウェアコンポーネントを組み合わせる必要があります。FlexPod Express では、システムにハイパーバイザーノードを追加するために必要なハードウェアコンポーネントについても、2つのユニット単位で説明します。

ハードウェア要件

選択したハイパーバイザーに関係なく、すべての FlexPod Express 構成で同じハードウェアが使用されます。そのため、ビジネス要件が変わっても、どちらのハイパーバイザーも同じ FlexPod Express ハードウェア上で実行できます。

次の表に、すべての FlexPod 構成に必要なハードウェアコンポーネントを示します。

ハードウェア	数量
AFF A220 HA ペア	1.
Cisco UCS B200 M5 サーバ	2.
Cisco Nexus 31108PCV スイッチ	2.
Cisco UCS B200 M5 サーバの Cisco UCS Virtual Interface Card (VIC ; 仮想インターフェイスカード) 1440	2.
2つの統合 UCS-fi-M6324 ファブリックインターコネクトを備えた Cisco UCS Mini	1.

ソフトウェア要件

次の表に、FlexPod Express ソリューションのアーキテクチャを実装するために必要なソフトウェアコンポーネントを示します。

ソフトウェア	バージョン	詳細
Cisco UCS Manager の略	4.0 (1b)	Cisco UCS Fabric Interconnect FI_6324UP の場合
Cisco Blade ソフトウェア	4.0 (1b)	Cisco UCS B200 M5 サーバの場合
Cisco nenic ドライバ	1.0.25.0	Cisco VIC 1440 インターフェイスカードの場合
Cisco NX-OS	7.0 (3) I6 (1)	Cisco Nexus 31108PCV スイッチの場合
NetApp ONTAP	9.5	AFF A220 コントローラの場合

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

ソフトウェア	バージョン
VMware vCenter Server Appliance の略	6.7U1

ソフトウェア	バージョン
VMware vSphere ESXi ハイパーバイザー	6.7U1

FlexPod エクスプレスケーブル接続情報

リファレンス検証のケーブル接続については、次の表で説明します。

次の表に、Cisco Nexus スイッチ 31108PCV A のケーブル接続情報を示します

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
Cisco Nexus スイッチ 31108PCV A	Eth1/1	NetApp AFF A220 ストレージコントローラ A	e0M
	Eth1/2	Cisco UCS-mini FIA	mgmt0 (管理)
	Eth1/3	Cisco UCS-mini FIA	Eth1/1
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/1
	ETH 1/13	Cisco NX 31108PCV B	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV B	ETH 1/14

次の表に、Cisco Nexus スイッチ 31108PCV B のケーブル接続情報を示します

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
Cisco Nexus スイッチ 31108PCV B	Eth1/1	NetApp AFF A220 ストレージコントローラ B	e0M
	Eth1/2	Cisco UCS-mini FI-B	mgmt0 (管理)
	Eth1/3	Cisco UCS-mini FIA	Eth1/2
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/2
	ETH 1/13	Cisco NX 31108PCV A	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV A	ETH 1/14

次の表に、NetApp AFF A220 ストレージコントローラ A のケーブル接続情報を示します

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
NetApp AFF A220 ストレージコントローラ A	e0a	NetApp AFF A220 ストレージコントローラ B	e0a
	e0b	NetApp AFF A220 ストレージコントローラ B	e0b
	e0e	Cisco UCS-mini FIA	Eth1/3
	e0f	Cisco UCS-mini FI-B	Eth1/3
	e0M	Cisco NX 31108PCV A	Eth1/1

次の表に、NetApp AFF A220 ストレージコントローラ B のケーブル接続情報を示します

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
NetApp AFF A220 ストレージコントローラ B	e0a	NetApp AFF A220 ストレージコントローラ B	e0a
	e0b	NetApp AFF A220 ストレージコントローラ B	e0b
	e0e	Cisco UCS-mini FIA	Eth1/4
	e0f	Cisco UCS-mini FI-B	Eth1/4
	e0M	Cisco NX 31108PCV B	Eth1/1

次の表に、Cisco UCS Fabric Interconnect A のケーブル接続情報を示します

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
Cisco UCS ファブリックインターコネクト A	Eth1/1	Cisco NX 31108PCV A	Eth1/3
	Eth1/2	Cisco NX 31108PCV B	Eth1/3
	Eth1/3	NetApp AFF A220 ストレージコントローラ A	e0e
	Eth1/4	NetApp AFF A220 ストレージコントローラ B	e0e
	mgmt0 (管理)	Cisco NX 31108PCV A	Eth1/2

次の表に、Cisco UCS ファブリックインターコネクト B のケーブル接続情報を示します

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
Cisco UCS ファブリックインターコネクト B	Eth1/1	Cisco NX 31108PCV A	Eth1/4
	Eth1/2	Cisco NX 31108PCV B	Eth1/4
	Eth1/3	NetApp AFF A220 ストレージコントローラ A	e0f
	Eth1/4	NetApp AFF A220 ストレージコントローラ B	e0f
	mgmt0 (管理)	Cisco NX 31108PCV B	Eth1/2

導入手順

このドキュメントでは、完全な冗長性と高可用性を備えた FlexPod Express システムの構成について詳しく説明します。この冗長性を反映するために、各手順で設定するコンポーネントをコンポーネント A またはコンポーネント B と呼びますたとえば、このドキュメントでプロビジョニングされている 2 台のネットアップストレージコントローラは、コントローラ A とコントローラ B で識別されます。スイッチ A とスイッチ B は Cisco Nexus スイッチのペアを表します。ファブリックインターコネクト A とファブリックインターコネクト B は、2 つの統合 Nexus ファブリックインターコネクトです。

また、このドキュメントでは、複数の Cisco UCS ホストをプロビジョニングする手順についても説明します。これらのホストは、サーバ A、サーバ B などとして順次識別されます。

環境に関連する情報をステップに含める必要があることを示すために、コマンド構造の一部として「\<text>>」が表示されます。「vlan create」コマンドについては、次の例を参照してください。

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

本ドキュメントでは、FlexPod Express 環境を完全に構成する方法について説明します。このプロセスでは、さまざまな手順で、お客様固有の命名規則、IP アドレス、および VLAN（仮想 LAN）スキームを入力する必要があります。次の表に、このガイドで説明する導入に必要な VLAN を示します。このテーブルは、特定のサイト変数に基づいて作成し、ドキュメントの設定手順を実装するために使用できます。



別々のインバンド管理 VLAN とアウトオブバンド管理 VLAN を使用する場合は、それらの間にレイヤ 3 ルートを作成する必要があります。この検証では、共通の管理 VLAN を使用しました。

VLAN 名	VLAN の目的	このドキュメントの検証に使用する ID
管理 VLAN	管理インターフェイス用の VLAN	18
ネイティブ VLAN	タグなしフレームが割り当てられている VLAN	2.
NFS VLAN	NFS トラフィック用の VLAN	104
VMware vMotion VLAN	ある物理ホストから別の物理ホストへの仮想マシン（VM）の移動用に指定された VLAN	103
VM トラフィック VLAN	VM アプリケーショントラフィック用の VLAN	102
iSCSI-A VLAN	ファブリック A の iSCSI トラフィック用 VLAN	124
iSCSI-B VLAN	ファブリック B の iSCSI トラフィック用 VLAN	125

VLAN 番号は、FlexPod Express の設定全体で必要になります。VLAN は「<<var_xxxx_vlan>>」と呼ばれます。「xxxx」は VLAN の目的（iSCSI-A など）です。

次の表は、作成された VMware VM を示しています。

VM 概要の略	ホスト名
VMware vCenter Server の各機能を使用し	Seahawks-vcsa.cie.netapp.com

Cisco Nexus 31108PCV 導入手順

このセクションでは、FlexPod Express 環境で使用される Cisco Nexus 31308PCV スイッチ構成について詳しく説明します。

Cisco Nexus 31108PCV スイッチの初期設定

ここでは、FlexPod Express の基本環境で使用する Cisco Nexus スイッチの設定方法について説明します。



この手順は、NX-OS ソフトウェアリリース 7.0(3) I6(1) を実行する Cisco Nexus 31108PCV を使用していることを前提としています。

1. スイッチのコンソールポートを最初にブートして接続すると、Cisco NX-OS セットアップが自動的に開始されます。この初期構成では、スイッチ名、mgmt0 インターフェイス構成、および Secure Shell (SSH) セットアップなどの基本的な設定を行います。
2. FlexPod Express 管理ネットワークは、さまざまな方法で構成できます。31108PCV スイッチの mgmt0 インターフェイスは、既存の管理ネットワークに接続することも、31108PCV スイッチの mgmt0 インターフェイスをバックツーバック構成で接続することもできる。ただし、このリンクは、SSH トラフィックなどの外部管理アクセスには使用できません。

この導入ガイドでは、FlexPod Express Cisco Nexus 31108PCV スイッチが既存の管理ネットワークに接続されています。

3. Cisco Nexus 31108PCV スイッチを設定するには、スイッチの電源をオンにし、画面に表示される指示に従って両方のスイッチの初期セットアップを行い、スイッチ固有の情報に適切な値を置き換えます。

```
This setup utility will guide you through the basic configuration of the
system. Setup configures only enough connectivity for management of the
system.
```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. 設定の概要が表示され、設定を編集するかどうかを確認するメッセージが表示されます。設定が正しい場合は、「n」と入力します。

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. その後、この設定を使用するかどうかを確認するメッセージが表示され、保存します。その場合は、「y」と入力します。

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus スイッチ B について、手順 1~5 を繰り返します

高度な機能を有効にします

追加の設定オプションを提供するには、Cisco NX-OS で特定の高度な機能をイネーブルにする必要があります。

1. Cisco Nexus スイッチ A およびスイッチ B で適切な機能をイネーブルにするには、コンフィギュレーションモードを開始するには、コマンド「(config t)」を使用し、次のコマンドを実行します。

```
feature interface-vlan
feature lacp
feature vpc
```



ポートチャネルのデフォルトのロードバランシングハッシュでは、ソースおよびデスティネーションの IP アドレスを使用して、ポートチャネルのインターフェイス全体のロードバランシングアルゴリズムを決定します。ハッシュアルゴリズムにソースおよびデスティネーションの IP アドレス以外にもデータを提供することで、ポートチャネルのメンバー全体へのより均等なロードバランシングを実現できます。同じ理由から、ソースおよびデスティネーションの TCP ポートをハッシュアルゴリズムに追加することを推奨します。

2. 構成モード (config t) から次のコマンドを実行し、Cisco Nexus スイッチ A およびスイッチ B のグローバルポートチャネルロードバランシング構成を設定します。

```
port-channel load-balance src-dst ip-l4port
```

グローバルスパニングツリーコンフィギュレーションを実行します。

Cisco Nexus プラットフォームでは、ブリッジアシュアランスと呼ばれる新しい保護機能を使用します。ブリッジアシュアランスは、スパニングツリーアルゴリズムを実行していないデバイスでデータトラフィックの転送を継続する単方向リンクやその他のソフトウェア障害から保護するのに役立ちます。ポートは、プラットフォームに応じて、ネットワークやエッジなどのいくつかの状態のいずれかに配置できます。

すべてのポートがデフォルトでネットワークポートとみなされるように、ブリッジアシュアランスを設定することを推奨します。この設定により、ネットワーク管理者は各ポートの設定を確認することになります。また、未識別のエッジポートや、ブリッジアシュアランス機能が有効になっていないネイバーなど、最も一般的な構成エラーも表示されます。また、スパニングツリーでブロックするポートの数が少なすぎない方が、多くのポートをブロックする方が安全で、デフォルトのポートの状態ですべてのネットワーク全体の安定性を高めることができます。

サーバ、ストレージ、アップリンクスイッチを追加するときは、スパニングツリーの状態に細心の注意を払ってください。追加する構成がブリッジアシュアランスをサポートしていない場合は特に注意が必要です。このような場合は、ポートをアクティブにするためにポートタイプの変更が必要になることがあります。

Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット) ガードは、別の保護レイヤとしてデフォルトでエッジポートでイネーブルになっています。ネットワーク内のループを防止するために、このインターフェイス上で BPDU が別のスイッチから受信された場合、この機能はポートをシャットダウンします。

Cisco Nexus スイッチ A およびスイッチ B で、構成モード (「 config t 」) から次のコマンドを実行し、デフォルトのポートタイプや BPDU ガードなどのデフォルトのスパニングツリーオプションを設定します。

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

VLAN を定義します

VLAN の異なるポートを個別に設定する前に、レイヤ 2 VLAN をスイッチ上に定義する必要があります。また、VLAN に名前を付けておくと、今後のトラブルシューティングを簡単に行うことができます。

コンフィギュレーションモード（`config t`）から次のコマンドを実行して、Cisco Nexus スイッチ A および スイッチ B 上のレイヤ 2 VLAN を定義し、説明します。

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

アクセスポートと管理ポートの説明を設定します

レイヤ 2 VLAN に名前を割り当てる場合と同様に、すべてのインターフェイスに説明を設定すると、プロビジョニングとトラブルシューティングの両方に役立ちます。

各スイッチの構成モード（`config t`）から、FlexPod Express の大規模構成の次のポート説明を入力します。

Cisco Nexus スイッチ A

```

int eth1/1
    description AFF A220-A e0M
int eth1/2
    description Cisco UCS FI-A mgmt0
int eth1/3
    description Cisco UCS FI-A eth1/1
int eth1/4
    description Cisco UCS FI-B eth1/1
int eth1/13
    description vPC peer-link 31108PVC-B 1/13
int eth1/14
    description vPC peer-link 31108PVC-B 1/14

```

Cisco Nexus スイッチ B

```

int eth1/1
    description AFF A220-B e0M
int eth1/2
    description Cisco UCS FI-B mgmt0
int eth1/3
    description Cisco UCS FI-A eth1/2
int eth1/4
    description Cisco UCS FI-B eth1/2
int eth1/13
    description vPC peer-link 31108PVC-B 1/13
int eth1/14
    description vPC peer-link 31108PVC-B 1/14

```

サーバおよびストレージの管理インターフェイスを設定します

サーバとストレージの管理インターフェイスで使用する VLAN は、通常、どちらも 1 つだけです。そのため、管理インターフェイスポートをアクセスポートとして設定します。各スイッチの管理 VLAN を定義し、スパニングツリーポートタイプをエッジに変更します。

構成モード (config t) から次のコマンドを実行して 'サーバとストレージの両方の管理インタフェースのポート設定を構成します

Cisco Nexus スイッチ A

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus スイッチ B

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

NTP 配信インターフェイスを追加します

Cisco Nexus スイッチ A

グローバルコンフィギュレーションモードから、次のコマンドを実行します。

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Cisco Nexus スイッチ B

グローバルコンフィギュレーションモードから、次のコマンドを実行します。

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

仮想ポートチャネルのグローバル設定を実行します

仮想ポートチャネル（vPC）を使用すると、2つの異なる Cisco Nexus スイッチに物理的に接続されたリンクを、3番目のデバイスに対する単一のポートチャネルとして認識できます。3番目のデバイスには、スイッチ、サーバ、またはその他のネットワークデバイスを使用できます。vPC はレイヤ 2 マルチパスを提供します。これにより、帯域幅を増やし、ノード間で複数のパラレルパスを有効にし、代替パスが存在する場合はトラフィックをロードバランシングすることで、冗長性を確保できます。

vPC には次の利点があります。

- 1つのデバイスが2つのアップストリームデバイス間でポートチャネルを使用できるようにする
- スパニングツリープロトコルのブロックポートの排除
- ループフリートポロジを提供する
- 使用可能なすべてのアップリンク帯域幅を使用する
- リンクまたはデバイスのいずれかに障害が発生した場合に、高速コンバージェンスを提供します
- リンクレベルの耐障害性を提供します
- 高可用性の実現を支援します

vPC 機能を正しく機能させるには、2つの Cisco Nexus スイッチ間でいくつかの初期セットアップを行う必要があります。バックツーバックの mgmt0 構成を使用する場合は、インターフェイスに定義されたアドレスを使用し、`ping <switch_a/B_mgmt0_ip_addr> vrf management` コマンドを使用してそれらのアドレスで通信が可能であることを確認します。

構成モード（`config t`）から次のコマンドを実行し、両方のスイッチの vPC グローバル構成を設定します。

Cisco Nexus スイッチ A

```

vpc domain 1
  role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start

```

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
    peer-gateway
    auto-recovery
    ip arp synchronize
    int eth1/13-14
    channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
    channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
channel-group 14 mode active
copy run start
```



この解決策検証では、最大伝送ユニット（MTU）9、000 が使用されました。ただし、アプリケーションの要件に基づいて、適切な MTU 値を設定できます。FlexPod 解決策全体で同じ MTU 値を設定することが重要です。コンポーネント間の MTU 設定が正しくないと、パケットが破棄されます。

既存のネットワークインフラへのアップリンク

使用可能なネットワークインフラに応じて、FlexPod 環境をアップリンクするためのいくつかの方法や機能があります。既存の Cisco Nexus 環境がある場合は、vPC を使用して、FlexPod 環境に含まれる Cisco Nexus 31108PVC スイッチをインフラにアップリンクすることを推奨します。必要に応じて、10GbE インフラ解決策の場合は 10GbE アップリンク、1GbE インフラ解決策の場合は 1GbE アップリンクがサポートされます。前述の手順を使用して、既存の環境へのアップリンク vPC を作成できます。設定が完了したら、必ず copy run start を実行して各スイッチに設定を保存してください。

ネットアップストレージ導入手順（パート 1）

このセクションでは、NetApp AFF ストレージ導入手順について説明します。

NetApp ストレージコントローラ AFF2xx シリーズインストールガイド

NetApp Hardware Universe の略

。"NetApp Hardware Universe の略"（HWU）アプリケーションは、特定の ONTAP バージョンでサポートされているハードウェアコンポーネントとソフトウェアコンポーネントを提供します。ONTAP ソフトウェアで現在サポートされているネットアップのすべてのストレージアプライアンスに関する構成情報を提供します。また、コンポーネントの互換性の表も示します。

使用するハードウェアコンポーネントとソフトウェアコンポーネントが、インストールする ONTAP のバージョンでサポートされていることを確認します。

1. にアクセスします ["HWU" システム設定ガイド](#)を表示するアプリケーション。ストレージシステムの比較タブを選択して、ONTAP ソフトウェアのバージョンとネットアップストレージアプライアンスの互換性を必要な仕様で確認します。
2. または、ストレージアプライアンス別にコンポーネントを比較するには、ストレージシステムの比較をクリックします。

コントローラ AFF2XX シリーズの前提条件

ストレージシステムの物理的な場所を計画するには、次のセクションを参照してください。電力要件サポートされる電源コードオンボードポートとケーブル

ストレージコントローラ

のコントローラの物理的な設置手順に従います ["AFF A220 のドキュメント"](#)。

NetApp ONTAP 9.5

設定ワークシート

セットアップスクリプトを実行する前に、製品マニュアルから構成ワークシートに情報を記入してください。設定ワークシートは、で使用できます ["ONTAP 9.5 ソフトウェアセットアップガイド"](#)（で使用できます ["ONTAP 9 ドキュメンテーション・センター"](#)）。次の表は、ONTAP 9.5 のインストールと設定の情報を示しています。



このシステムは、2 ノードスイッチレスクラスタ構成でセットアップされます。

クラスタの詳細	クラスタの値
クラスタノード A の IP アドレス	<<var_nodeA_mgmt_ip>>
クラスタノード A のネットマスク	<<var_nodeA_mgmt_mask>> を使用します
クラスタノード A のゲートウェイ	<<var_nodeA_mgmt_gateway>> を使用します
クラスタノードの名前	<<var_nodeA>> を使用します
クラスタノード B の IP アドレス	<<var_nodeB_mgmt_ip>>
クラスタノード B のネットマスク	<<var_nodeB_mgmt_mask>> を使用します
クラスタノード B のゲートウェイ	<<var_nodeB_mgmt_gateway>> を使用します
クラスタノード B の名前	<<var_nodeB>> を使用します
ONTAP 9.5 の URL	<<var_url_boot_software>> を参照してください
クラスタの名前	\<<var_clustername> を使用します
クラスタ管理 IP アドレス	<<var_clustermgmt_ip>>
クラスタ B ゲートウェイ	<<var_clustermgmt_gateway>> を使用します
クラスタ B のネットマスク	<<var_clustermgmt_mask>> を使用します
ドメイン名	<<var_domain_name>> を参照してください
DNS サーバ IP（複数入力できます）	<<var_dns_server_ip>>
NTP サーバ A の IP	<switch-A-ntp-ip>>
NTP サーバ B の IP	<switch-b-ntp-ip>>

ノード A を設定

ノード A を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. システムをブートできるようにします。

autoboot

3. Ctrl+C キーを押してブートメニューを表示します。

ONTAP 9 の場合：5 は起動しているソフトウェアのバージョンではありません。次の手順に進んで新しいソフトウェアをインストールしてください。ONTAP 9 の場合：5 はブートしているバージョンです。オプション 8 と y を選択してノードをリブートします。その後、手順 14 に進みます。

4. 新しいソフトウェアをインストールするには 'オプション 7' を選択します
5. アップグレードを実行するには 'y' を入力します
6. ダウンロードに使用するネットワーク・ポートに e0M を選択します
7. 今すぐ再起動するには 'y' を入力します
8. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. ソフトウェアを検索できる URL を入力します。



ping 可能な Web サーバを指定する必要があります。

10. ユーザ名が入力されていない場合は、Enter キーを押します。
11. 新しくインストールしたソフトウェアを '次回の再起動に使用するデフォルトとして設定するには 'y' を入力します
12. ノードを再起動するには 'y' を入力します

新しいソフトウェアをインストールするときに、BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

13. Ctrl+C キーを押してブートメニューを表示します。
14. [Clean Configuration] で [4] を選択し、[Initialize All Disks] を選択します。
15. ディスクをゼロにするには 'y' を入力し '構成をリセットして' 新しいファイル・システムをインストールします
16. ディスク上のすべてのデータを消去するには 'y' を入力します

ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。ノード A のディスクの初期化中も、ノード B の設定を続行できます。

17. ノード A を初期化している間に、ノード B の設定を開始します

ノード B を設定

ノード B を設定するには、次の手順を実行します。

1. ストレージ・システムのコンソール・ポートに接続します。ローダー A のプロンプトが表示されます。ただし、ストレージシステムがリブートループに入っている場合は、このメッセージが表示されたら Ctrl-C キーを押して自動ブートループを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Ctrl+C キーを押してブートメニューを表示します。

```
autoboot
```

3. プロンプトが表示されたら、Ctrl-C キーを押します。

ONTAP 9 の場合：5 は起動しているソフトウェアのバージョンではありません。次の手順に進んで新しいソフトウェアをインストールしてください。ブートしているバージョンが ONTAP 9.4 の場合は、オプション 8 と y を選択してノードをリブートします。その後、手順 14 に進みます。

4. 新しいソフトウェアをインストールするには、オプション 7 を選択します。
5. アップグレードを実行するには 'y' を入力します
6. ダウンロードに使用するネットワーク・ポートに e0M を選択します
7. 今すぐ再起動するには 'y' を入力します
8. e0M の IP アドレス、ネットマスク、およびデフォルトゲートウェイをそれぞれの場所に入力します。

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. ソフトウェアを検索できる URL を入力します。



ping 可能な Web サーバを指定する必要があります。

```
<<var_url_boot_software>>
```

10. ユーザ名が入力されていない場合は、Enter キーを押します
11. 新しくインストールしたソフトウェアを ' 次回の再起動に使用するデフォルトとして設定するには 'y' を入力します
12. ノードを再起動するには 'y' を入力します

新しいソフトウェアをインストールするときに、BIOS およびアダプタカードのファームウェアアップグレードが実行され、リブートが発生してローダー A プロンプトで停止する可能性があります。これらの操作が行われた場合、システムがこの手順と異なることがあります。

13. Ctrl+C キーを押してブートメニューを表示します。
14. Clean Configuration および Initialize All Disks のオプション 4 を選択します。

15. ディスクをゼロにするには 'y' を入力し '構成をリセットして '新しいファイル・システムをインストールします
16. ディスク上のすべてのデータを消去するには 'y' を入力します

ルートアグリゲートの初期化と作成には、接続されているディスクの数とタイプに応じて 90 分以上かかる場合があります。初期化が完了すると、ストレージシステムがリブートします。SSD の初期化にかかる時間は大幅に短縮されます。

ノード **A** の設定およびクラスタ構成を継続します

ストレージコントローラ A（ノード A）のコンソールポートに接続されているコンソールポートプログラムから、ノードセットアップスクリプトを実行します。このスクリプトは、ONTAP 9.5 をノードで初めてブートしたときに表示されます。

ONTAP 9.5 では、ノードとクラスタのセットアップ手順が少し変更されています。クラスタセットアップウィザードを使用してクラスタの最初のノードを設定できるようになりました。System Manager を使用してクラスタを設定します。

1. プロンプトに従ってノード A をセットアップします


```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
    "help" or "?" - if you want to have a question clarified,
    "back" - if you want to change previously answered questions, and
    "exit" or "quit" - if you want to quit the cluster setup wizard.
    Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. ノードの管理インターフェイスの IP アドレスに移動します。



クラスタのセットアップは、CLI を使用して実行することもできます。このドキュメントでは、NetApp System Manager のセットアップガイドを使用したクラスタセットアップについて説明します。

3. クラスタを設定するには、セットアップガイドをクリックします。
4. クラスタ名には「\<<var_clusternam>>」を、設定する各ノードには「<<var_nodeA>」と「\<<var_nodeB>>」を入力します。ストレージシステムに使用するパスワードを入力します。クラスタタイプに「スイッチレスクラスタ」を選択します。クラスタベースライセンスを入力します。
5. クラスタ、NFS、および iSCSI の機能ライセンスを入力することもできます。
6. クラスタの作成中を示すステータスメッセージが表示されます。このステータスメッセージは、複数のステータスを切り替えます。このプロセスには数分かかります。
7. ネットワークを設定します
 - a. [IP Address Range] オプションを選択解除します。

- b. Cluster Management IP Address フィールドに「<<var_clustermgmt_ip>>」、Netmask フィールドに「\var_clustermgmt_mask>>」と入力します。また、Gateway フィールドに「<<var_clustermgmt_gateway>>」と入力します。Port フィールドの ... セレクタを使用して、ノード A の e0M を選択します
- c. ノード A のノード管理 IP がすでに入力されています。ノード B には「\<<var_nodeA_mgmt_ip>>」を入力します
- d. [DNS Domain Name] フィールドに「<<var_domain_name>`」と入力します。[DNS Server IP Address] フィールドに「\<<var_dns_server_ip>>」と入力します。

DNS サーバの IP アドレスは複数入力できます。

- e. Primary NTP Server フィールドに「\<switch-a-ntp-ip>>」と入力します。

代替 NTP サーバを「\<switch-b-ntp-ip>>」として入力することもできます。

- 8. サポート情報を設定します。
 - a. AutoSupport へのアクセスにプロキシが必要な環境の場合は、プロキシの URL をプロキシの URL に入力します。
 - b. イベント通知に使用する SMTP メールホストと E メールアドレスを入力します。

続行するには、少なくともイベント通知方式を設定する必要があります。いずれかの方法を選択できます。

- 9. クラスタ構成が完了したことが示されたら、Manage Your Cluster（クラスタの管理）をクリックしてストレージを構成します。

ストレージクラスタ構成を継続

ストレージノードとベースクラスタの設定が完了したら、ストレージクラスタの設定に進むことができます。

すべてのスベアディスクを初期化します

クラスタ内のすべてのスベアディスクを初期化するには、次のコマンドを実行します。

```
disk zerospares
```

オンボード **UTA2** ポートパーソナリティを設定します

- 1. ucadmin show コマンドを実行して、現在のモードとポートの現在のタイプを確認します。

```
AFFA220-Clus:> ucdadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
AFFA220-Clus-01	0c	cna	target	-	-	offline
AFFA220-Clus-01	0d	cna	target	-	-	offline
AFFA220-Clus-01	0e	cna	target	-	-	offline
AFFA220-Clus-01	0f	cna	target	-	-	offline
AFFA220-Clus-02	0c	cna	target	-	-	offline
AFFA220-Clus-02	0d	cna	target	-	-	offline
AFFA220-Clus-02	0e	cna	target	-	-	offline
AFFA220-Clus-02	0f	cna	target	-	-	offline

8 entries were displayed.

2. 使用中のポートの現在のモードが「cna」であり、現在のタイプが「target」に設定されていることを確認します。設定されていない場合は、次のコマンドを実行してポートパーソナリティを変更します。

```
ucdadmin modify -node <home node of the port> -adapter <port name> -mode  
cna -type target
```

前のコマンドを実行するには、ポートをオフラインにする必要があります。ポートをオフラインにするには、次のコマンドを実行します。

```
network fcp adapter modify -node <home node of the port> -adapter <port  
name> -state down
```



ポートパーソナリティを変更した場合、変更を有効にするには、各ノードをリブートする必要があります。

Cisco Discovery Protocol を有効にします

ネットアップストレージコントローラで Cisco Discovery Protocol（CDP）を有効にするには、次のコマンドを実行します。

```
node run -node * options cdpd.enable on
```

すべてのイーサネットポートでリンクレイヤ検出プロトコルを有効にします

次のコマンドを実行して、ストレージスイッチとネットワークスイッチ間のリンクレイヤ検出プロトコル（LLDP）ネイバー情報の交換を有効にします。このコマンドは、クラスタ内のすべてのノードのすべてのポートで LLDP を有効にします。

```
node run * options lldp.enable on
```

管理論理インターフェイスの名前を変更します

管理論理インターフェイス（LIF）の名前を変更するには、次の手順を実行します。

1. 現在の管理 LIF の名前を表示します。

```
network interface show -vserver <<clustername>>
```

2. クラスタ管理 LIF の名前を変更します。

```
network interface rename -vserver <<clustername>> -lif  
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. ノード B の管理 LIF の名前を変更します。

```
network interface rename -vserver <<clustername>> -lif  
cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
```

クラスタ管理で自動リバートを設定する

クラスタ管理インターフェイスで 'auto-revert' パラメータを設定します

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-  
revert true
```

サービスプロセッサのネットワークインターフェイスをセットアップする

各ノードのサービスプロセッサに静的 IPv4 アドレスを割り当てるには、次のコマンドを実行します。

```
system service-processor network modify -node <<var_nodeA>> -address  
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>  
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>  
system service-processor network modify -node <<var_nodeB>> -address  
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>  
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```



サービスプロセッサの IP アドレスは、ノード管理 IP アドレスと同じサブネット内にある必要があります。

ONTAP でストレージフェイルオーバーを有効にします

ストレージフェイルオーバーが有効になっていることを確認するには、フェイルオーバーペアで次のコマンドを実行します。

1. ストレージフェイルオーバーのステータスを確認

```
storage failover show
```

\<<var_nodeA>>` と \<<var_nodeB>> の両方がテイクオーバーを実行できる必要があります。ノードでテイクオーバーを実行できる場合は、ステップ 3 に進みます。

2. 2 つのノードのどちらかでフェイルオーバーを有効にします。

```
storage failover modify -node <<var_nodeA>> -enabled true
```

3. 2 ノードクラスタの HA ステータスを確認



この手順は、ノードが 3 つ以上のクラスタには適用されません。

```
cluster ha show
```

4. ハイアベイラビリティが構成されている場合は、ステップ 6 に進みます。ハイアベイラビリティが設定されている場合は、コマンドの実行時に次のメッセージが表示されます。

```
High Availability Configured: true
```

5. HA モードは 2 ノードクラスタでのみ有効にします。

ノードが 3 つ以上のクラスタの場合は、このコマンドを実行しないでください。フェイルオーバーで問題が発生します。

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. ハードウェアアシストが正しく設定されていることを確認し、必要に応じてパートナーの IP アドレスを変更

```
storage failover hwassist show
```

「Keep Alive Status: Error: Did not receive hwassist keep alive alerts from partner」というメッセージは、ハードウェアアシストが設定されていないことを示します。ハードウェアアシストを設定するには、次のコマンドを実行します。

```
storage failover modify -hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node <<var_nodeA>>
storage failover modify -hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node <<var_nodeB>>
```

ONTAP でジャンボフレーム **MTU** ブroadcastドメインを作成します

MTU が 9000 のデータブroadcast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roadcast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roadcastドメインからポートを削除するには、次のコマンドを実行します。

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 ポートではフロー制御を無効にします

ネットアップでは、外部デバイスに接続されているすべての UTA2 ポートでフロー制御を無効にすることをベストプラクティスとして推奨します。フロー制御を無効にするには、次のコマンドを実行します。

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```



ONTAP への Cisco UCS Mini の直接接続は、LACP をサポートしていません。

NetApp ONTAP でジャンボフレームを設定します

ジャンボフレーム（一般に MTU サイズが 9、000 バイトのフレーム）を使用するように ONTAP ネットワークポートを設定するには、クラスタシェルから次のコマンドを実行します。

```

AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y

```

ONTAP で VLAN を作成します

ONTAP で VLAN を作成するには、次の手順を実行します。

1. NFS VLAN ポートを作成し、データブロードキャストドメインに追加します。

```

network port vlan create -node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>

```

2. iSCSI VLAN ポートを作成し、データブロードキャストドメインに追加します。


```

network port vlan create -node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>

```

3. MGMT-VLAN ポートを作成します。

```

network port vlan create -node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>

```

ONTAP でアグリゲートを作成する

ONTAP のセットアッププロセスで、ルートボリュームを含むアグリゲートが作成されます。追加のアグリゲートを作成するには、アグリゲート名、アグリゲートを作成するノード、アグリゲートに含まれるディスク数を確認します。

アグリゲートを作成するには、次のコマンドを実行します。

```

aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>

```

構成内で少なくとも 1 つのディスクをスペアとして保持します（最も大きいディスクを選択してください）。ディスクのタイプとサイズごとに少なくとも 1 つのスペアを用意しておくことを推奨します。

ディスクは 5 本から始めて、追加のストレージが必要になったときにアグリゲートにディスクを追加できます。

ディスクの初期化が完了するまで、アグリゲートを作成することはできません。aggr show コマンドを実行して、アグリゲートの作成ステータスを表示します。「aggr1_nodeA」がオンラインになるまで、次の手順に進まないでください。

ONTAP でタイムゾーンを設定します

時刻の同期を設定し、クラスタのタイムゾーンを設定するには、次のコマンドを実行します。

```
timezone <<var_timezone>>
```



たとえば、米国東部では、タイムゾーンは「アメリカ/ニューヨーク」です。タイムゾーン名の入力を開始したら、Tab キーを押して使用可能なオプションを表示します。

ONTAP で SNMP を設定します

SNMP を設定するには、次の手順を実行します。

1. 場所や連絡先などの SNMP 基本情報を設定します。ポーリング時に 'この情報は 'sysLocation' 変数と SNMP の sysContact' 変数として表示されます

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. リモートホストに送信する SNMP トラップを設定します。

```
snmp traphost add <<var_snmp_server_fqdn>>
```

ONTAP で SNMPv1 を設定します

SNMPv1 を設定するには、コミュニティと呼ばれる共有シークレットのプレーンテキストパスワードを設定します。

```
snmp community add ro <<var_snmp_community>>
```



「snmp community delete all」コマンドは慎重に使用してください。他の監視製品にコミュニティストリングが使用されている場合、このコマンドはそれらを削除します。

ONTAP で SNMPv3 を設定します

SNMPv3 では、認証用のユーザを定義および設定する必要があります。SNMPv3 を設定するには、次の手順を実行します。

1. 「securitysnmpusers」コマンドを実行して、エンジン ID を表示します。
2. 「mpv3user」という名前のユーザを作成します。

```
security login create -username snmpv3user -authmethod usm -application snmp
```

3. 信頼できるエンティティのエンジン ID を入力し、認証プロトコルとして「mD5」を選択します。
4. プロンプトが表示されたら、認証プロトコルのパスワードとして最低 8 文字のパスワードを入力します。
5. プライバシープロトコルとして「es」を選択します。
6. プロンプトが表示されたら、プライバシープロトコルのパスワードとして最低 8 文字のパスワードを入力します。

ONTAP で AutoSupport HTTPS を設定します

NetApp AutoSupport ツールは、サポート概要情報を HTTPS 経由でネットアップに送信します。AutoSupport を設定するには、次のコマンドを実行します。

```
system node autosupport modify -node * -state enable -mail-hosts  
<<var_mailhost>> -transport https -support enable -noteto  
<<var_storage_admin_email>>
```

Storage Virtual Machine を作成

インフラ Storage Virtual Machine （SVM）を作成するには、次の手順を実行します。

1. vserver create コマンドを実行します

```
vserver create -vserver Infra-SVM -rootvolume rootvol -aggregate  
aggr1_nodeA -rootvolume- security-style unix
```

2. NetApp VSC のインフラ SVM アグリゲートリストにデータアグリゲートを追加します。

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS と iSCSI を残して、未使用のストレージプロトコルを SVM から削除します。

```
vserver remove-protocols -vserver Infra-SVM -protocols cifs,ndmp,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 は以前はサーバと呼ばれていたため、コマンドラインでは「vserver」の前にコマンドが配置されます

ONTAP で NFSv3 を設定します

次の表に、この設定を完了するために必要な情報を示します。

詳細 (Detail)	詳細値
ESXi ホスト A の NFS IP アドレス	<<var_esxi_hostA_nfs_ip>>
ESXi ホスト B の NFS IP アドレス	<<var_esxi_hostB_nfs_ip>> を追加します

SVM に NFS を設定するには、次のコマンドを実行します。

- 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 B シリーズサーバを追加するときにエクスポートポリシールールを作成する必要があります。

ONTAP で iSCSI サービスを作成します

iSCSI サービスを作成するには、次の手順を実行します。

1. SVM で iSCSI サービスを作成します。また、このコマンドでは iSCSI サービスが開始され、SVM に iSCSI Qualified Name (IQN) が設定されます。iSCSI が設定されていることを確認します。

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP で SVM ルートボリュームの負荷共有ミラーを作成

ONTAP で SVM ルートボリュームの負荷共有ミラーを作成するには、次の手順を実行します。

1. インフラ SVM ルートボリュームの負荷共有ミラーとなるボリュームを各ノードに作成します。

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate
aggr1_nodeA -size 1GB -type DPvolume create -vserver Infra_Vserver
-volume rootvol_m02 -aggregate aggr1_nodeB -size 1GB -type DP
```

2. ルートボリュームのミラー関係を 15 分ごとに更新するジョブスケジュールを作成します。

```
job schedule interval create -name 15min -minutes 15
```

3. ミラーリング関係を作成

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. ミラーリング関係を初期化し、作成されたことを確認します。

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

ONTAP で HTTPS アクセスを設定する

ストレージコントローラへのセキュアなアクセスを設定するには、次の手順を実行します。

1. 証明書コマンドにアクセスするには、権限レベルを上げてください。

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 通常は、自己署名証明書がすでに存在します。次のコマンドを実行して証明書を確認します。

```
security certificate show
```

3. 表示されている各 SVM の証明書の共通名は、SVM の DNS 完全修飾ドメイン名（FQDN）と一致している必要があります。4 つのデフォルト証明書を削除して、認証局の自己署名証明書または証明書に置き換える必要があります。

証明書を作成する前に期限切れになった証明書を削除することを推奨します。「securitycertificate delete」コマンドを実行して、期限切れの証明書を削除します。次のコマンドでは、タブ補完を使用して、デフォルトの証明書を選択して削除します。

```
security certificate delete [TAB] ...  
Example: security certificate delete -vserver Infra-SVM -common-name  
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. 自己署名証明書を生成してインストールするには、次のコマンドを 1 回限りのコマンドとして実行します。インフラ SVM とクラスタ SVM のサーバ証明書を生成します。これらのコマンドの実行に役立つように、タブ補完を使用してください。

```
security certificate create [TAB] ...  
Example: security certificate create -common-name infra-svm.netapp.com  
-type server -size 2048 - country US -state "North Carolina" -locality  
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr  
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256  
-vserver Infra-SVM
```

5. 次の手順で必要なパラメータの値を取得するには、「securitycertificate show」コマンドを実行します。
6. 作成した各証明書を '-server-enabled true' および '-client-enabled false' パラメータを使用して有効にしますタブ補完を使用してください。

```
security ssl modify [TAB] ...  
Example: security ssl modify -vserver Infra-SVM -server-enabled true  
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common  
-name infra-svm.netapp.com
```

7. SSL と HTTPS アクセスを設定して有効にし、HTTP アクセスを無効にします。

```
system services web modify -external true -ssl3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```



これらのコマンドの一部で、エントリが存在しないことを示すエラーメッセージが返されますが、これは通常の動作であり問題ありません。

8. admin 権限レベルにリバートしてセットアップを作成し、SVM を Web で使用できるようにします。

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

ONTAP で NetApp FlexVol ボリュームを作成します

NetApp FlexVol® ボリュームを作成するには、ボリューム名、サイズ、およびボリュームが存在するアグリゲートを入力します。2 つの VMware データストアボリュームと 1 つのサーバブートボリュームを作成します。

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent-snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP で重複排除を有効にします

適切なボリュームで 1 日に 1 回重複排除を有効にするには、次のコマンドを実行します。

```

volume efficiency modify -vserver Infra-SVM -volume esxi_boot -schedule
sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_1
-schedule sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_2
-schedule sun-sat@0

```

ONTAP で LUN を作成します

2 つのブート論理ユニット番号（LUN）を作成するには、次のコマンドを実行します。

```

lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled

```



Cisco UCS C シリーズサーバを追加する場合は、追加のブート LUN を作成する必要があります。

ONTAP に iSCSI LIF を作成

次の表に、この設定を完了するために必要な情報を示します。

詳細（Detail）	詳細値
ストレージノード A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
ストレージノード A の iSCSI LIF01A ネットワークマスク	<<var_nodeA_iscsi_lif01a_mask>> をクリックします
ストレージノード A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
ストレージノード A の iSCSI LIF01B ネットワークマスク	<<var_nodeA_iscsi_lif01b_mask>> をクリックします
ストレージノード B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
ストレージノード B iSCSI LIF01A ネットワークマスク	<<var_nodeB_iscsi_lif01a_mask>> を選択します
ストレージノード B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
ストレージノード B iSCSI LIF01B ネットワークマスク	<<var_nodeB_iscsi_lif01b_mask>> をクリックします

1. 各ノードに 2 つずつ、4 つの iSCSI LIF を作成します。


```

network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface show

```

ONTAP に NFS LIF を作成します

次の表に、この設定を完了するために必要な情報を示します。

詳細（Detail）	詳細値
ストレージノード A NFS LIF 01 A IP	<<var_nodeA_nfs_lif_01_a_ip>>
ストレージノード A NFS LIF 01 のネットワークマスク	<<var_nodeA_nfs_lif_01_a_mask>> を参照してください
ストレージノード A NFS LIF 01 b IP	<<var_nodeA_nfs_lif_01_b_ip>>
ストレージノード A NFS LIF 01 b ネットワークマスク	<<var_nodeA_nfs_lif_01_b_mask>> を参照してください
ストレージノード B の NFS LIF 02 A IP	<<var_nodeB_nfs_lif_02_a_ip>>
ストレージノード B の NFS LIF 02 A ネットワークマスク	<<var_nodeB_nfs_lif_02.a_mask>> を参照してください
ストレージノード B の NFS LIF 02 b IP	<<var_nodeB_nfs_lif_02_b_ip>>
ストレージノード B の NFS LIF 02 b ネットワークマスク	<<var_nodeB_nfs_lif_02_b_mask>> を参照してください

1. NFS LIF を作成します。

```

network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface show

```

インフラ **SVM** 管理者を追加

次の表に、この設定を完了するために必要な情報を示します。

詳細 (Detail)	詳細値
vsmgmt IP	<<var_svm_mgmt_ip>> を追加します
vsmgmt ネットワークマスク	<<var_SVM_mgmt_mask>> を使用します
vsmgmt デフォルトゲートウェイ	<<var_SVM_mgmt_gateway>> を使用します

インフラ SVM 管理者および SVM 管理 LIF を管理ネットワークに追加するには、次の手順を実行します。

1. 次のコマンドを実行します。

```

network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true

```



ここで指定する SVM 管理 IP は、ストレージクラス管理 IP と同じサブネット内にある必要があります。

2. SVM 管理インターフェイスの外部へのアクセスを許可するデフォルトルートを作成します。

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway  
<<var_svm_mgmt_gateway>> network route show
```

3. SVM 「vsadmin」 ユーザのパスワードを設定し、ユーザのロックを解除します。

```
security login password -username vsadmin -vserver Infra-SVM  
Enter a new password: <<var_password>>  
Enter it again: <<var_password>>  
security login unlock -username vsadmin -vserver
```

Cisco UCS サーバの構成

FlexPod の Cisco UCS ベース

FlexPod 環境で Cisco UCS 6324 ファブリックインターコネクトの初期セットアップを実行します。

このセクションでは、Cisco UCS Manager を使用して、FlexPod ROBO 環境で使用する Cisco UCS を設定する手順について詳しく説明します。

Cisco UCS ファブリックインターコネクト 6324 A

Cisco UCS は、アクセスレイネットワークとサーバを使用します。この高性能な次世代サーバシステムは、データセンターにワークロードの即応性と拡張性をもたらします。

Cisco UCS Manager 4.0(1b) は、ファブリックインターコネクトを Cisco UCS シャーシに統合する 6324 ファブリックインターコネクトをサポートし、より小規模な導入環境に解決策を統合します。Cisco UCS Mini により、システム管理が簡素化され、低規模な導入のためのコストが削減されます。

ハードウェアコンポーネントとソフトウェアコンポーネントは、シスコのユニファイドファブリックをサポートしています。ユニファイドファブリックは、単一の統合ネットワークアダプタ上で複数のタイプのデータセンタートラフィックを処理します。

システムの初期セットアップ

Cisco UCS ドメイン内のファブリックインターコネクトに初めてアクセスすると、セットアップウィザードによって、システムの設定に必要な次の情報の入力が必要です。

- インストール方法（GUI または CLI）
- セットアップモード（フルシステムバックアップまたは初期セットアップからリストア）
- システム構成の種類（スタンドアロンまたはクラスタ構成）
- システム名
- 管理パスワード
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス

- デフォルトゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- DNS サーバの IPv4 アドレスまたは IPv6 アドレス
- デフォルトのドメイン名

次の表に、Fabric Interconnect A で Cisco UCS の初期設定を完了するために必要な情報を示します

詳細（ Detail ）	詳細 / 値
システム名	\<<var_UCS_clustername> を使用します
管理パスワード	<<var_password>>
管理 IP アドレス：ファブリックインターコネクト A	<<var_ucsa_mgmt_ip>> を追加します
管理ネットマスク： Fabric Interconnect A	<<var_ucsa_mgmt_mask>> を使用します
デフォルトゲートウェイ： Fabric Interconnect A	<<var_ucsa_mgmt_gateway>> を使用します
クラスタの IP アドレス	<<var_UCS_cluster_ip>>
DNS サーバの IP アドレス	<<var_nameserver_ip>>
ドメイン名	<<var_domain_name>> を参照してください

FlexPod 環境で使用するよう Cisco UCS を設定するには、次の手順を実行します。

1. 最初の Cisco UCS 6324 ファブリックインターコネクト A のコンソールポートに接続します

Enter the configuration method. (console/gui) ? console

Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

Enforce strong password? (y/n) [y]: Enter

Enter the password for "admin":<<var_password>>
Confirm the password for "admin":<<var_password>>

Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes

Enter the switch fabric (A/B) []: A

Enter the system name: <<var_ucs_clustername>>

Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

Cluster IPv4 address : <<var_ucs_cluster_ip>>

Configure the DNS Server IP address? (yes/no) [n]: y

DNS IP address : <<var_nameserver_ip>>

Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

Join centralized management environment (UCS Central)? (yes/no) [n]:
no

NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized. UCSM will be functional only after peer FI is configured in clustering mode.

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

Applying configuration. Please wait.

Configuration file - Ok

2. コンソールに表示される設定を確認します。正しい場合は、回答は設定を適用して保存します。
3. ログインプロンプトで設定が保存されたことを確認します。

次の表に、ファブリックインターコネクト B で Cisco UCS の初期設定を完了するために必要な情報を示します

詳細 (Detail)	詳細 / 値
システム名	\<<var_UCS_clustername> を使用します
管理パスワード	<<var_password>>
管理 IP アドレス - FI B	<<var_UCSB_mgmt_ip>> を追加します
管理ネットマスク - FI B	<<var_UCSB_mgmt_mask>> を使用します
デフォルトゲートウェイ - FI B	<<var_UCSB_mgmt_gateway>> を使用します
クラスタの IP アドレス	<<var_UCS_cluster_ip>>
DNS サーバの IP アドレス	<<var_nameserver_ip>>
ドメイン名 (Domain Name)	<<var_domain_name>> を参照してください

1. 2 番目の Cisco UCS 6324 ファブリックインターコネクト B のコンソールポートに接続します

```

Enter the configuration method. (console/gui) ? console

Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

Enter the admin password of the peer Fabric
interconnect:<<var_password>>
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
Cluster IPv4 address: <<var_ucs_cluster_address>>

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>

Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok

```

2. ログインプロンプトで、設定が保存されたことを確認します。

Cisco UCS Manager にログインします。

Cisco Unified Computing System （ UCS ） 環境にログインするには、次の手順を実行します。

1. Web ブラウザを開き、 Cisco UCS ファブリックインターコネクトクラスタのアドレスに移動します。

Cisco UCS Manager が起動するように 2 つ目のファブリックインターコネクトを設定した後、 5 分以上待つ必要があります。

2. Launch UCS Manager リンクをクリックして、 Cisco UCS Manager を起動します。
3. 必要なセキュリティ証明書を受け入れます。
4. プロンプトが表示されたら、ユーザ名に admin を入力し、管理者パスワードを入力します。
5. Login をクリックして、 Cisco UCS Manager にログインします。

Cisco UCS Manager ソフトウェアバージョン 4.0(1b)

このマニュアルでは、 Cisco UCS Manager ソフトウェアバージョン 4.0(1b) を使用することを前提としています。 Cisco UCS Manager ソフトウェアおよび Cisco UCS 6324 ファブリックインターコネクトソフトウェアのアップグレードについては、を参照してください "[Cisco UCS Manager インストールおよびアップグレードガイド](#)"

Cisco UCS Call Home を設定する

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

1. Cisco UCS Manager で、左側の Admin をクリックします。
2. [すべて] > [通信管理] > [コールホーム] の順に選択します。
3. 状態をオンに変更します。
4. 管理設定に従ってすべてのフィールドに入力し、 [変更の保存] をクリックして [OK] をクリックし、 Call Home の設定を完了します。

キーボード、ビデオ、マウスアクセス用の IP アドレスのブロックを追加します

Cisco UCS 環境で帯域内サーバのキーボード、ビデオ、マウス（ KVM ） アクセス用の IP アドレスブロックを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [Pools] > [root] > [IP Pools] を展開します。
3. [IP Pool ext-mgmt] を右クリックし、 [Create Block of IPv4 Addresses] を選択します。
4. ブロックの開始 IP アドレス、必要な IP アドレスの数、およびサブネットマスクとゲートウェイの情報を入力します。

Create Block of IPv4 Addresses

From :	192.168.156.101	Size :	12
Subnet Mask :	255.255.255.0	Default Gateway :	192.168.156.1
Primary DNS :	0.0.0.0	Secondary DNS :	0.0.0.0

OK Cancel

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

Cisco UCS を NTP に同期する

Cisco UCS 環境を Nexus スイッチの NTP サーバと同期させるには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Admin をクリックします。
2. [すべて] > [タイムゾーン管理] を展開します。
3. [タイムゾーン] を選択します。
4. [プロパティ] ペインで、[タイムゾーン] メニューから適切なタイムゾーンを選択します。
5. [Save Changes] をクリックし、[OK] をクリックします。
6. Add NTP Server をクリックします。
7. 「<switch-a-ntp-ip>」または「<nexus-a-mgmt-ip>」と入力し、[OK] をクリックします。[OK] をクリックします。

Add NTP Server

?

×

NTP Server :

OK

Cancel

- Add NTP Server をクリックします。
- 「<switch-b-ntp-ip>`」または「<nexus-B-mgmt-ip>`」と入力し、[OK] をクリックします。確認の [OK] をクリックします。

All /

General

Events

Actions

Add NTP Server

Properties

Time Zone :

NTP Servers

▼ Advanced Filter

↑ Export

🖨 Print

Name

NTP Server 10.1.156.4

NTP Server 10.1.156.5

シャーシ検出ポリシーを編集します

検出ポリシーを設定することで、Cisco UCS B シリーズシャーシの追加やファブリックエクステンダの追加が簡素化され、Cisco UCS C シリーズの接続性がさらに向上します。シャーシ検出ポリシーを変更するには、次の手順を実行します。

- Cisco UCS Manager で、左側の [Equipment] をクリックし、2 番目のリストで [Equipment] を選択します。
- 右側のペインで、[ポリシー] タブを選択します。
- Global Policies（グローバルポリシー）で、シャーシまたはファブリックエクステンダ（FEX）とファブリックインターコネクト間でケーブル接続されているアップリンクポートの最小数と一致するように、Chassis/FEX Discovery Policy（シャーシ/FEX 検出ポリシー）を設定します。
- Link Grouping Preference を Port Channel に設定します。設定する環境に大量のマルチキャストトラフィックが含まれている場合は、Multicast Hardware Hash（マルチキャストハードウェアハッシュ）設定を

47

Enabled（有効）に設定します。

5. [Save Changes] をクリックします。
6. [OK] をクリックします。

サーバ、アップリンク、およびストレージポートを有効にします

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

1. Cisco UCS Manager のナビゲーションペインで、Equipment タブを選択します。
2. Equipment > Fabric Interconnects > Fabric Interconnect A > Fixed Module の順に展開します。
3. [Ethernet ポート] を展開します。
4. Cisco Nexus 31108 スイッチに接続されているポート 1 と 2 を選択し、右クリックして、[Configure as Uplink Port] を選択します。
5. Yes をクリックしてアップリンクポートを確認し、OK をクリックします。
6. ネットアップストレージコントローラに接続されているポート 3 と 4 を選択し、右クリックして Configure as Appliance Port（アプライアンスポートとして設定）を選択します。
7. Yes をクリックして、アプライアンスのポートを確認します。
8. Configure as Appliance Port（アプライアンスポートとして設定）ウィンドウで、OK をクリックします。
9. [OK] をクリックして確定します。
10. 左側のペインで、Fabric Interconnect A の Fixed Module を選択します
11. [Ethernet Ports] タブで、[If Role] カラムにポートが正しく設定されていることを確認します。スケーラビリティポートにポート C シリーズサーバが設定されている場合は、そのサーバをクリックしてポート接続を確認します。

Equipment / Fabric Interconnects / Fabric Interconnect A (subordinate) / Fixed Module

General Ethernet Ports FC Ports Faults Events								
Advanced Filter Export Print All Unconfigured Network Server FCoE Uplink Unified Uplink Appliance Storage FCoE Storage Unified Storage Monitor								
Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:36:68	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:36:69	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:36:6A	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:36:6B	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:36:6C	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:36:6D	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:36:6E	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:36:6F	Unconfigured	Physical	Sfp Not Present	Disabled	

12. Equipment > Fabric Interconnects > Fabric Interconnect B > Fixed Module の順に展開します。
13. [Ethernet ポート] を展開します。

14. Cisco Nexus 31108 スイッチに接続されているイーサネットポート 1 および 2 を選択し、右クリックして、Configure as Uplink Port （アップリンクポートとして設定）を選択します。
15. Yes をクリックしてアップリンクポートを確認し、OK をクリックします。
16. ネットアップストレージコントローラに接続されているポート 3 と 4 を選択し、右クリックして Configure as Appliance Port （アプライアンスポートとして設定）を選択します。
17. Yes をクリックして、アプライアンスのポートを確認します。
18. Configure as Appliance Port （アプライアンスポートとして設定）ウィンドウで、OK をクリックします。
19. [OK] をクリックして確定します。
20. 左側のペインで、Fabric Interconnect B の Fixed Module を選択します
21. [Ethernet Ports] タブで、[If Role] カラムにポートが正しく設定されていることを確認します。スケーラビリティポートにポート C シリーズサーバが設定されている場合は、そのサーバをクリックしてポート接続を確認します。

Equipment / Fabric Interconnects / Fabric Interconnect B (primar... / Fixed Module / Ethernet Ports

Ethernet Ports									
Advanced Filter Export Print <input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Unconfigured <input checked="" type="checkbox"/> Network <input checked="" type="checkbox"/> Server <input checked="" type="checkbox"/> FCoE Uplink <input checked="" type="checkbox"/> Unified Uplink <input checked="" type="checkbox"/> Appliance Storage <input checked="" type="checkbox"/> FCoE Storage <input checked="" type="checkbox"/> Unified Storage <input checked="" type="checkbox"/> Monitor									
Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer	
1	0	1	00:DE:FB:30:3A:C8	Network	Physical	Up	Enabled		
1	0	2	00:DE:FB:30:3A:C9	Network	Physical	Up	Enabled		
1	0	3	00:DE:FB:30:3A:CA	Appliance Storage	Physical	Up	Enabled		
1	0	4	00:DE:FB:30:3A:CB	Appliance Storage	Physical	Up	Enabled		
1	5	1	00:DE:FB:30:3A:CC	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	2	00:DE:FB:30:3A:CD	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	3	00:DE:FB:30:3A:CE	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	4	00:DE:FB:30:3A:CF	Unconfigured	Physical	Sfp Not Present	Disabled		

Cisco Nexus 31108 スイッチへのアップリンクポートチャネルを作成します

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

1. Cisco UCS Manager で、ナビゲーションペインの [LAN] タブを選択します。



この手順では、2つのポートチャネルが作成されます。1つはファブリック A から両方の Cisco Nexus 31108 スイッチへ、もう1つはファブリック B から両方の Cisco Nexus 31108 スイッチへです。標準スイッチを使用している場合は、それに応じてこの手順を変更します。ファブリックインターコネクト上で1ギガビットイーサネット（1GbE）スイッチおよび GLC-T SFP を使用する場合は、ファブリックインターコネクト内のイーサネットポート 1/1 および 1/2 のインターフェイス速度を 1Gbps に設定する必要があります。

2. [LAN] > [LAN Cloud] で、[Fabric A] ツリーを展開します。
3. [ポートチャネル] を右クリックします。
4. ポートチャネルの作成を選択します。

5. ポートチャネルの一意の ID として 13 を入力します。
6. ポートチャネルの名前として「vPC-13-Nexus」と入力します。
7. 次へをクリックします。

The screenshot shows a 'Create Port Channel' window. On the left, a blue vertical bar contains two numbered steps: '1 Set Port Channel Name' and '2 Add Ports'. The main content area has two input fields: 'ID' with the value '13' and 'Name' with the value 'vPC-13-Nexus'. At the bottom right, there are four buttons: 'Previous' (disabled), 'Next >' (active), 'Finish' (disabled), and 'Cancel'.

8. ポートチャネルに追加する次のポートを選択します。
 - a. スロット ID 1 とポート 1
 - b. スロット ID 1 とポート 2
9. >> をクリックして、ポートチャネルにポートを追加します。
10. Finish をクリックして、ポートチャネルを作成します。[OK] をクリックします。
11. [ポートチャネル] で、新しく作成したポートチャネルを選択します。

ポートチャネルの全体的なステータスが up になっている必要があります。
12. ナビゲーションペインで、[LAN] > [LAN Cloud] の下の [Fabric B] ツリーを展開します。
13. [ポートチャネル] を右クリックします。
14. ポートチャネルの作成を選択します。
15. ポートチャネルの一意の ID として「14」を入力します。
16. ポートチャネルの名前として「vPC-14-Nexus」と入力します。次へをクリックします。
17. ポートチャネルに追加する次のポートを選択します。
 - a. スロット ID 1 とポート 1

b. スロット ID 1 とポート 2

18. >> をクリックして、ポートチャネルにポートを追加します。
19. Finish をクリックして、ポートチャネルを作成します。[OK] をクリックします。
20. [ポートチャネル] で、新しく作成したポートチャネルを選択します。
21. ポートチャネルの全体的なステータスが up になっている必要があります。

組織の作成（オプション）

組織は、リソースを整理し、IT 組織内のさまざまなグループへのアクセスを制限することで、コンピューティングリソースのマルチテナンシーを実現するために使用されます。



このドキュメントでは組織の使用は想定していませんが、この手順では組織の作成方法について説明します。

Cisco UCS 環境で組織を設定するには、次の手順を実行します。

1. Cisco UCS Manager で、ウィンドウ上部のツールバーの [新規作成（New）] メニューから、[組織の作成（Create Organization）] を選択します。
2. 組織の名前を入力します。
3. オプション：組織の概要を入力します。[OK] をクリックします。
4. 確認メッセージで [OK] をクリックします。

ストレージアプライアンスのポートおよびストレージ **VLAN** を設定します

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

1. Cisco UCS Manager で、[LAN] タブを選択します。
2. アプライアンスクラウドを拡張します。
3. アプライアンスクラウドの下の VLAN を右クリックします。
4. [Create VLANs] を選択します。
5. Infrastructure NFS VLAN の名前として「nfs-vlan」と入力します。
6. 共通 / グローバルを選択したままにします。
7. VLAN ID として「<<var_nfs_vlan_id>>」と入力します。
8. [共有タイプ] は [なし] のままにします。

Create VLANs

VLAN Name/Prefix : NFS-VLAN

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs : 3170

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

Check Overlap Ok Cancel

9. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。
10. アプライアンスクラウドの下の VLAN を右クリックします。
11. [Create VLANs] を選択します。
12. Infrastructure iSCSI Fabric A VLAN の名前として「iSCSI-A-VLAN」と入力します。
13. 共通 / グローバルを選択したままにします。
14. VLAN ID として「<<var_iscsi-a_vlan_id>>」と入力します。
15. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。
16. アプライアンスクラウドの下の VLAN を右クリックします。
17. [Create VLANs] を選択します。
18. インフラストラクチャ iSCSI ファブリック B VLAN の名前として「iSCSI-B-VLAN」と入力します。
19. 共通 / グローバルを選択したままにします。
20. VLAN ID として「<<var_iscsi-b_vlan_id>>」と入力します。
21. [OK] をクリックし、もう一度 [OK] をクリックして VLAN を作成します。

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

LAN / LAN Cloud / VLANs

VLANs

Advanced Filter Export Print

Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Name	Multicast Policy Name
VLAN default (1)	1	Lan	Ether	Yes	None		
VLAN 0002-Native (2)	2	Lan	Ether	No	None		
VLAN public (18)	18	Lan	Ether	No	None		
VLAN 0101-IB-MGMT (101)	101	Lan	Ether	No	None		
VLAN 0102-VM (102)	102	Lan	Ether	No	None		
VLAN 0103-vMotion (103)	103	Lan	Ether	No	None		
VLAN 0104-NFS (104)	104	Lan	Ether	No	None		
VLAN 0120-SCSI-A (120)	120	Lan	Ether	No	None		
VLAN 0121-SCSI-B (121)	121	Lan	Ether	No	None		

28. ナビゲーションペインで、[LAN] > [Policies] の下の [Appliances] を展開し、[Network Control Policies] を右クリックします。
29. Create Network Control Policy を選択します。
30. ポリシーに「Enable_cdp_LLDP」という名前を付け、CDP の横にある [有効] を選択します。
31. LLDP の送受信機能を有効にします。

Properties for: Enable_CDP

General Events

Actions

Delete

Show Policy Usage

Use Global

Properties

Name: Enable_CDP

Description:

Owner: Local

CDP: ☐ Disabled ☒ Enabled

MAC Register Mode: ☒ Only Native Vlan ☐ All Host Vlans

Action on Uplink Fail: ☒ Link Down ☐ Warning

MAC Security

Forge: ☒ Allow ☐ Deny

LLDP

Transmit: ☐ Disabled ☒ Enabled

Receive: ☐ Disabled ☒ Enabled

OK Cancel Help

32. [OK] をクリックし、もう一度 [OK] をクリックしてポリシーを作成します。
33. ナビゲーションペインの [LAN] > [Appliances Cloud] で、[Fabric A tree] を展開します。
34. [Interfaces] を展開します。
35. アプライアンス・インターフェイス 1/3 を選択します。
36. [User Label] フィールドに、「<storage_controller_01_name> : e0e」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。
37. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
38. [VLANs] で、iSCSI-A VLAN、NFS VLAN、およびネイティブ VLAN を選択します。ネイティブ VLAN をネイティブ VLAN として設定します。デフォルトの VLAN 選択をクリアします。
39. [変更を保存して OK] をクリックします。

LAN / Appliances / Fabric A / Interfaces / Appliance Interface 1/3

General | Ports | Vlanets

Actions

- Create Interface
- Discover Interface
- Add Ethernet Target Endpoint
- Remove Ethernet Target Endpoint

Properties

ID: 3

Slot ID: 1

Fabric ID: A

Aggregated Port ID: 0

User Label: AFFA200_Chis_01-e0e

Transceiver Type: SFP

Port: sfp/switch-A/Slot-1/switch-port/001-3

Admin Speed(gbps): ☐ 1 Gbps ☒ 10 Gbps ☐ 40 Gbps ☐ 25 Gbps ☐ 100 Gbps ☐ Auto

Priority:

Pin Group:

Network Control Policy:

Flow Control Policy:

VLANs

Port Mode:

☒ VLAN default (1)

☒ VLAN iSCSI-A-VLAN (124)
 ☐ VLAN iSCSI-B-VLAN (125)
 ☒ VLAN Native-VLAN (2)
 ☒ VLAN NFS-VLAN (104)

Native VLAN:

Disable VLAN

40. [Fabric A] の下にある [Appliance Interface] 1/4 を選択します
41. [User Label] フィールドに、「<storage_controller_02_name> : e0e」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。
42. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
43. [VLANs] で、iSCSI-A VLAN、NFS VLAN、およびネイティブ VLAN を選択します。
44. ネイティブ VLAN をネイティブ VLAN として設定します。
45. デフォルトの VLAN 選択をクリアします。
46. [変更を保存して OK] をクリックします。
47. ナビゲーションペインの [LAN] > [Appliances Cloud] で、[Fabric B] ツリーを展開します。
48. [Interfaces] を展開します。
49. アプライアンス・インターフェイス 1/3 を選択します。
50. [User Label] フィールドに、「<storage_controller_01_name> : e0f」など、ストレージコントローラポートを示す情報を入力します。[変更を保存して OK] をクリックします。

51. Enable_CDP Network Control Policy を選択し、 Save Changes and OK を選択します。
52. [VLANs] で、 [iSCSI-B-VLAN]、 [NFS VLAN]、 および [ネイティブ VLAN] を選択します。 ネイティブ VLAN をネイティブ VLAN として設定します。 デフォルト VLAN の選択を解除します。

LAN / Appliances / Fabric B / Interfaces / Appliance Interface 1/3

General Faults Events

Actions

- Enable interface
- Disable interface
- Act as Ethernet Target Endpoint
- Delete Ethernet Target Endpoint

Properties

ID : 3

Slot ID : 1

Fabric ID : B

Aggregated Port ID : 0

User Label : AFFA200_Clus_01:e0f

Transport Type : Ether

Port : sys/switch-B/slot-1/switch-ether/port-3

Admin Speed(gbps) : ☐ 1 Gbps ☒ 10 Gbps ☐ 40 Gbps ☐ 25 Gbps ☐ 100 Gbps ☐ Auto

Priority : Best Effort

Pin Group : <not set>

Network Control Policy : Enable_CDP

Flow Control Policy : default

VLANs

Port Mode : ☒ Trunk ☐ Access

☐ VLAN default (1)

☐ VLAN iSCSI-A-VLAN (124)

☒ VLAN iSCSI-B-VLAN (125)

☒ VLAN Native-VLAN (2)

☒ VLAN NFS_VLAN (104)

Native VLAN : VLAN Native-VLAN (2)

Create VLAN

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

Cisco UCS ファブリックでジャンボフレームを設定します

Cisco UCS ファブリックでジャンボフレームを設定して QoS を有効にするには、次の手順を実行します。

1. Cisco UCS Manager のナビゲーションペインで、 [LAN] タブをクリックします。
2. [LAN] > [LAN Cloud] > [QoS System Class] の順に選択します。
3. 右側のペインで、 [全般] タブをクリックします。
4. [ベストエフォート] 行で、 [MTU] 列の下ボックスに 9216 と入力します。

LAN / LAN Cloud / QoS System Class

General Events FSM

Actions: Use Global Properties: Owner: Local

Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	MTU	Multicast Optimized
Platinum	<input type="checkbox"/>	5	<input type="checkbox"/>	10	N/A	normal	<input type="checkbox"/>
Gold	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	9	N/A	normal	<input type="checkbox"/>
Silver	<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	8	N/A	normal	<input type="checkbox"/>
Bronze	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	7	N/A	normal	<input type="checkbox"/>
Best Effort	<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>	5	50	9216	<input type="checkbox"/>
Fibre Channel	<input checked="" type="checkbox"/>	3	<input type="checkbox"/>	5	50	10	N/A

5. [Save Changes] をクリックします。

6. [OK] をクリックします。

Cisco UCS シャーシを確認します

すべての Cisco UCS シャーシを確認するには、次の手順を実行します。

1. Cisco UCS Manager で、[Equipment] タブを選択し、右側の [Equipment] タブを展開します。
2. 機器 > シャーシを展開します。
3. シャーシ 1 のアクションでシャーシの確認を選択します。
4. [OK] をクリックし、[OK] をクリックしてシャーシの確認を完了します。
5. [閉じる] をクリックして、[プロパティ] ウィンドウを閉じます。

Cisco UCS 4.0(1b) ファームウェアイメージをロードします

Cisco UCS Manager ソフトウェアと Cisco UCS Fabric Interconnect ソフトウェアをバージョン 4.0(1b) にアップグレードするには、を参照してください ["Cisco UCS Manager インストールおよびアップグレードガイド"](#)。

ホストファームウェアパッケージを作成する

ファームウェア管理ポリシーを使用すると、管理者は特定のサーバ設定に対応するパッケージを選択できます。これらのポリシーには、多くの場合、アダプタ、BIOS、ボードコントローラ、FC アダプタ、ホストバスアダプタ（HBA）オプション ROM、ストレージコントローラプロパティのパッケージが含まれています。

Cisco UCS 環境で特定のサーバ設定のファームウェア管理ポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー] > [ルート] を選択します。
3. ホストファームウェアパッケージを展開します。
4. デフォルトを選択します。

5. アクションペインで、パッケージバージョンの変更を選択します。
6. 両方のブレードパッケージのバージョン 4.0(1b) を選択します。

Modify Package Versions

Blade Package : 4.0(1b)B

Rack Package : <not set>

Service Pack :

The images from Service Pack will take precedence over the images from Blade or Rack Package

Excluded Components:

- ☐ Adapter
- ☐ BIOS
- ☐ Board Controller
- ☐ CIMC
- ☐ FC Adapters
- ☐ Flex Flash Controller
- ☐ GPUs
- ☐ HBA Option ROM
- ☐ Host NIC
- ☐ Host NIC Option ROM
- ☒ Local Disk
- ☐ NVME Mswitch Firmware
- ☐ PSU
- ☐ SAS Expander

OK Apply Cancel Help

7. [OK] をクリックし、もう一度 [OK] をクリックして、ホストファームウェアパッケージを変更します。

MAC アドレスプールを作成します

Cisco UCS 環境に必要な MAC アドレスプールを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. プール／ルートを選択します。

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

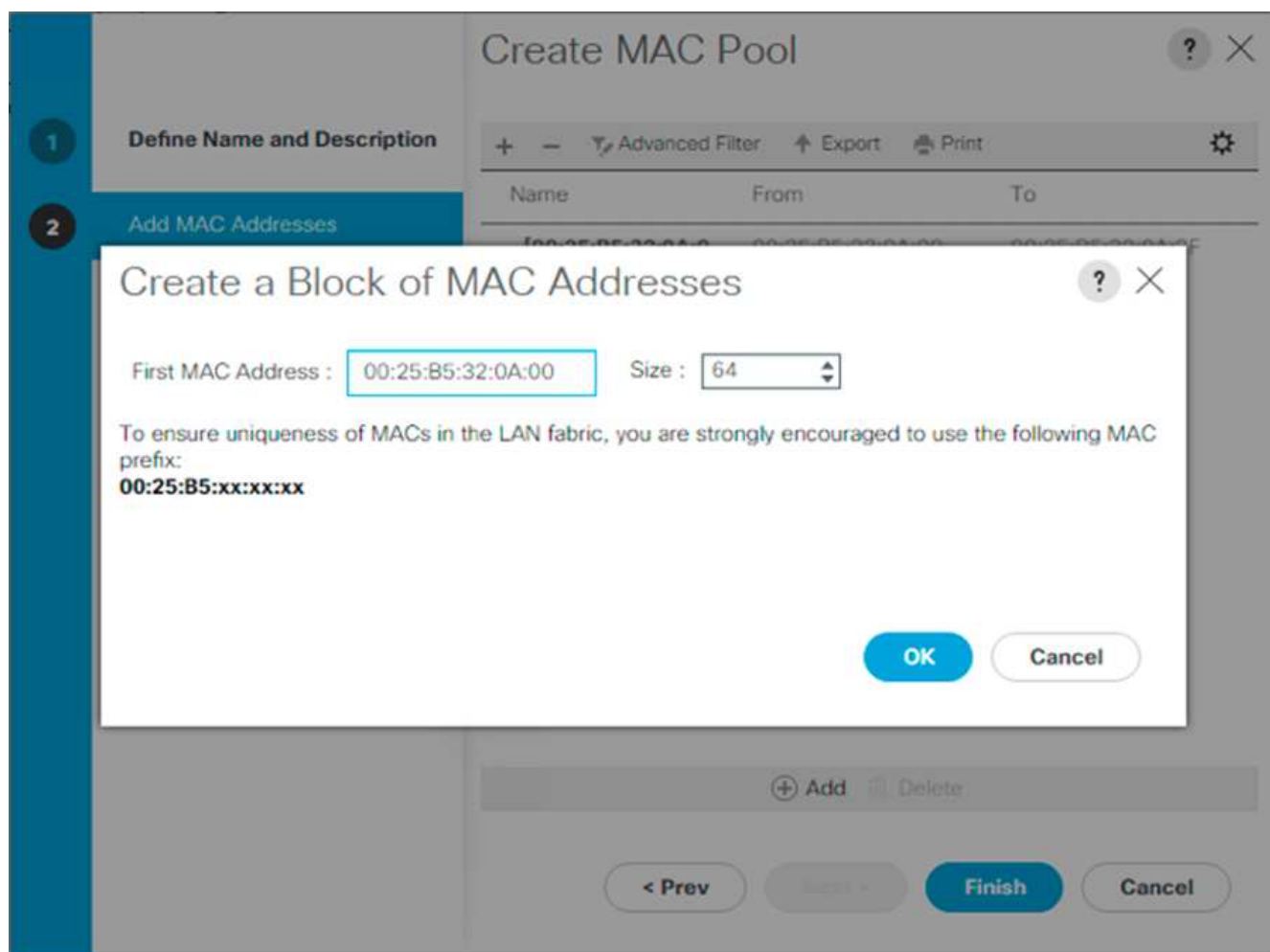
3. ルート組織の下にある [MAC Pools] を右クリックします。
4. MAC アドレスプールを作成するには、Create MAC Pool (MAC プールの作成) を選択します。
5. MAC プールの名前として「MAC-Pool-A」と入力します。
6. オプション：MAC プールの概要を入力します。

7. 割り当て順序（ Assignment Order ）のオプションとして順次（ Sequential ）を選択します。次へをクリックします。
8. 追加をクリックします。
9. 開始 MAC アドレスを指定します。



FlexPod 解決策では、開始 MAC アドレスの最後のオクテットに 0a を配置して、すべての MAC アドレスをファブリック A アドレスとして識別することを推奨します。この例では、最初の MAC アドレスとして 00 : 25 : B5 : 32 : 0a:00 を与える Cisco UCS ドメイン番号情報も組み込みました。

10. 使用可能なブレードまたはサーバリソースをサポートするのに十分な MAC アドレスプールのサイズを指定します。[OK] をクリックします。



11. 完了をクリックします。
12. 確認メッセージが表示されたら、[OK] をクリックします。
13. ルート組織の下にある [MAC Pools] を右クリックします。
14. MAC アドレスプールを作成するには、Create MAC Pool （ MAC プールの作成 ）を選択します。
15. MAC プールの名前として「 MAC-Pool-B 」と入力します。
16. オプション： MAC プールの概要を入力します。

17. 割り当て順序（ Assignment Order ）のオプションとして順次（ Sequential ）を選択します。次へをクリックします。
18. 追加をクリックします。
19. 開始 MAC アドレスを指定します。



FlexPod 解決策の場合、このプール内のすべての MAC アドレスをファブリック B アドレスとして識別するために、開始 MAC アドレスの最後のオクテットの隣に 0B を配置することを推奨します。この例では、最初の MAC アドレスとして 00 : 25 : B5 : 32 : 0B : 00 を与える Cisco UCS ドメイン番号情報も組み込みました。

20. 使用可能なブレードまたはサーバリソースをサポートするのに十分な MAC アドレスプールのサイズを指定します。[OK] をクリックします。
21. 完了をクリックします。
22. 確認メッセージが表示されたら、[OK] をクリックします。

iSCSI IQN プールを作成します

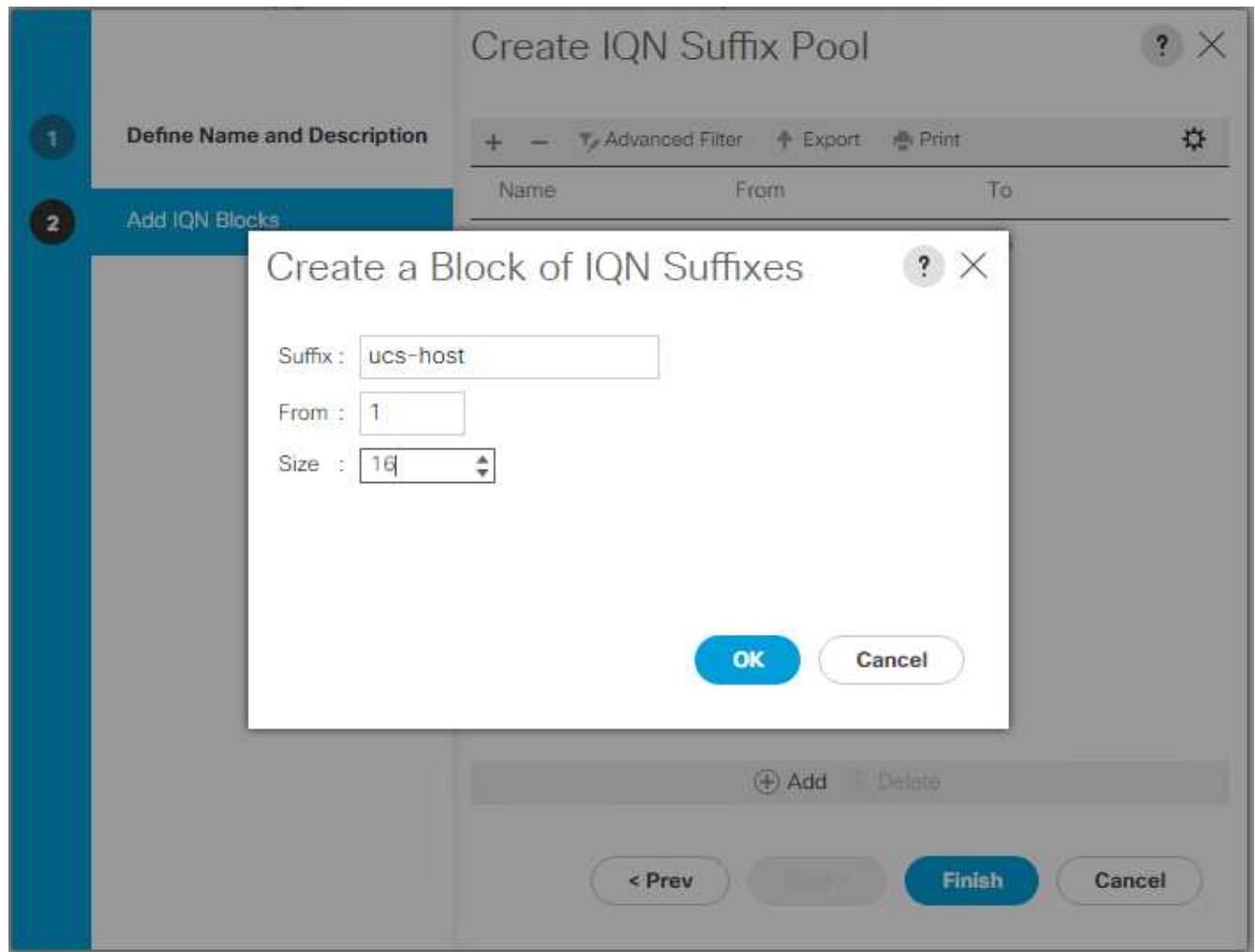
Cisco UCS 環境に必要な IQN プールを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [SAN] をクリックします。
2. プール／ルートを選択します。
3. IQN プールを右クリックします。
4. IQN サフィックスプールの作成を選択して IQN プールを作成します。
5. IQN プールの名前として「 IQN -Pool 」と入力します。
6. オプション： IQN プールの概要を入力します。
7. プレフィックスとして「 iqn.1992-08.com.cisco` 」と入力します。
8. [割り当て順序] で [順次] を選択します。次へをクリックします。
9. 追加をクリックします。
10. サフィックスに「 UCS-host 」と入力します。



複数の Cisco UCS ドメインを使用している場合は、さらに具体的な IQN サフィックスを使用する必要があります。

11. [From] フィールドに 1 を入力します。
12. 使用可能なサーバリソースを十分にサポートできる IQN ブロックのサイズを指定してください。[OK] をクリックします。



13. 完了をクリックします。

iSCSI イニシエータの IP アドレスプールを作成します

Cisco UCS 環境に必要な IP プール iSCSI ブートを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. プール／ルートを選択します。
3. [IP Pools] を右クリックします。
4. Create IP Pool を選択します。
5. IP プール名として「iSCSI-IP-Pool-A」と入力します。
6. オプション：IP プールの概要を入力します。
7. 割り当て順序の [順次] を選択します。次へをクリックします。
8. Add をクリックして IP アドレスのブロックを追加します。
9. [From] フィールドに、iSCSI IP アドレスとして割り当てる範囲の先頭を入力します。
10. サーバに対応できる十分なアドレスにサイズを設定してください。[OK] をクリックします。
11. 次へをクリックします。

12. 完了をクリックします。
13. [IP Pools] を右クリックします。
14. Create IP Pool を選択します。
15. IP プール名として「iSCSI-IP-Pool-B」と入力します。
16. オプション：IP プールの概要を入力します。
17. 割り当て順序の [順次] を選択します。次へをクリックします。
18. Add をクリックして IP アドレスのブロックを追加します。
19. [From] フィールドに、iSCSI IP アドレスとして割り当てる範囲の先頭を入力します。
20. サーバに対応できる十分なアドレスにサイズを設定してください。[OK] をクリックします。
21. 次へをクリックします。
22. 完了をクリックします。

UUID サフィックスプールを作成します

Cisco UCS 環境に必要な Universally Unique Identifier（UUID）サフィックスプールを設定するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. プール／ルートを選択します。
3. [UUID Suffix Pools] を右クリックします。
4. [Create UUID Suffix Pool] を選択します。
5. UUID サフィックスプールの名前として「UUID - プール」と入力します。
6. オプション：UUID サフィックスプールの概要を入力します。
7. 接頭部は派生オプションのままにします。
8. 割り当て順序（Assignment Order）に順次（Sequential）を選択し
9. 次へをクリックします。
10. Add をクリックして UUID のブロックを追加します。
11. デフォルト設定の [From] フィールドをそのまま使用します。
12. 使用可能なブレードまたはサーバリソースをサポートするのに十分な UUID ブロックのサイズを指定します。[OK] をクリックします。
13. 完了をクリックします。
14. [OK] をクリックします。

サーバプールを作成します

Cisco UCS 環境に必要なサーバプールを設定するには、次の手順を実行します。



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

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. プール／ルートを選択します。
3. [サーバプール] を右クリックします。
4. Create Server Pool を選択します。
5. サーバ・プールの名前として「 Infra-Pool 」と入力します。
6. オプション：サーバプールの概要を入力します。次へをクリックします。
7. VMware 管理クラスタに使用するサーバを 2 つ以上選択し '>>' をクリックして Infra-Pool' Server プールに追加します
8. 完了をクリックします。
9. [OK] をクリックします。

Cisco Discovery Protocol と Link Layer Discovery Protocol のネットワーク制御ポリシーを作成します

Cisco Discovery Protocol （ CDP ） および Link Layer Discovery Protocol （ LLDP ） のネットワーク制御ポリシーを作成するには、次の手順を実行します。

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

Create Network Control Policy

CDP : ☐ Disabled ☒ Enabled

MAC Register Mode : ☒ Only Native Vlan ☐ All Host Vlans

Action on Uplink Fail : ☒ Link Down ☐ Warning

MAC Security

Forge : ☒ Allow ☐ Deny

LLDP

Transmit : ☐ Disabled ☒ Enabled

Receive : ☐ Disabled ☒ Enabled

OK Cancel

電源制御ポリシーを作成します

Cisco UCS 環境の電源制御ポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers タブをクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [電源制御ポリシー] を右クリックします。
4. 電源制御ポリシーの作成を選択します。
5. 電源制御ポリシー名として No-Power-Cap と入力します。
6. 電力上限設定を [No Cap](キャップなし) に変更します
7. [OK] をクリックして、電源制御ポリシーを作成します。[OK] をクリックします。

Create Power Control Policy

?

×

Name

:

No-Power-Cap

Description

:

Fan Speed Policy

:

Any

Power Capping

If you choose **cap**, the server is allocated a certain amount of power based on its priority within its power group. Priority values range from 1 to 10, with 1 being the highest priority. If you choose **no-cap**, the server is exempt from all power capping.

☒ No Cap

☐ cap

Cisco UCS Manager **only enforces power capping** when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

OK

Cancel

サーバプール認定ポリシーの作成（オプション）

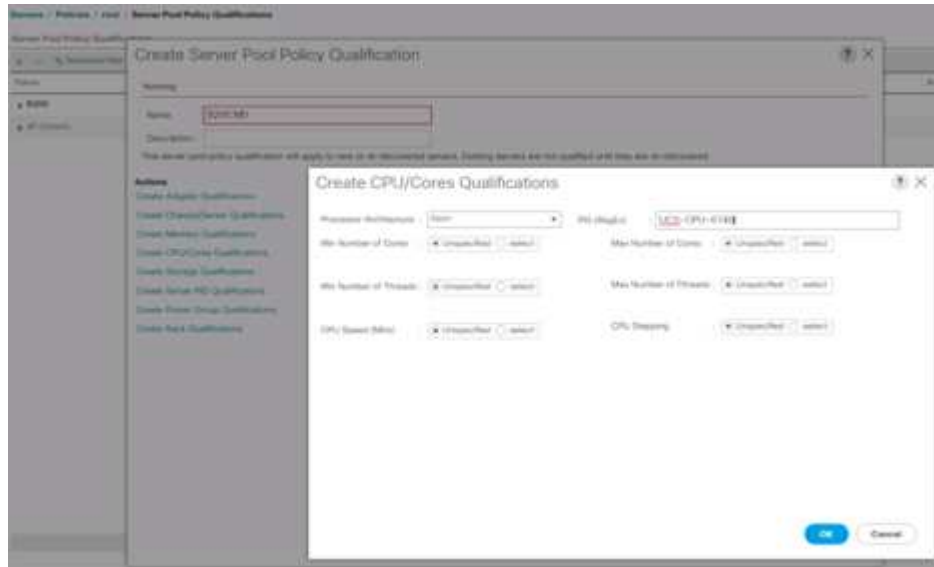
Cisco UCS 環境のオプションのサーバプール認定ポリシーを作成するには、次の手順を実行します。



この例では、Intel E2660 v4 Xeon Broadwell プロセッサを搭載した Cisco UCS B シリーズサーバ用のポリシーを作成します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー]>[ルート]を選択します。
3. [サーバプールポリシーの条件]を選択します。
4. Create Server Pool Policy Qualification（サーバプールポリシーの作成条件）または Add（追加）を
5. ポリシーにインテルという名前を付けます。
6. Create CPU/ Cores Qualifications]を選択します。
7. プロセッサ / アーキテクチャに Xeon を選択します。

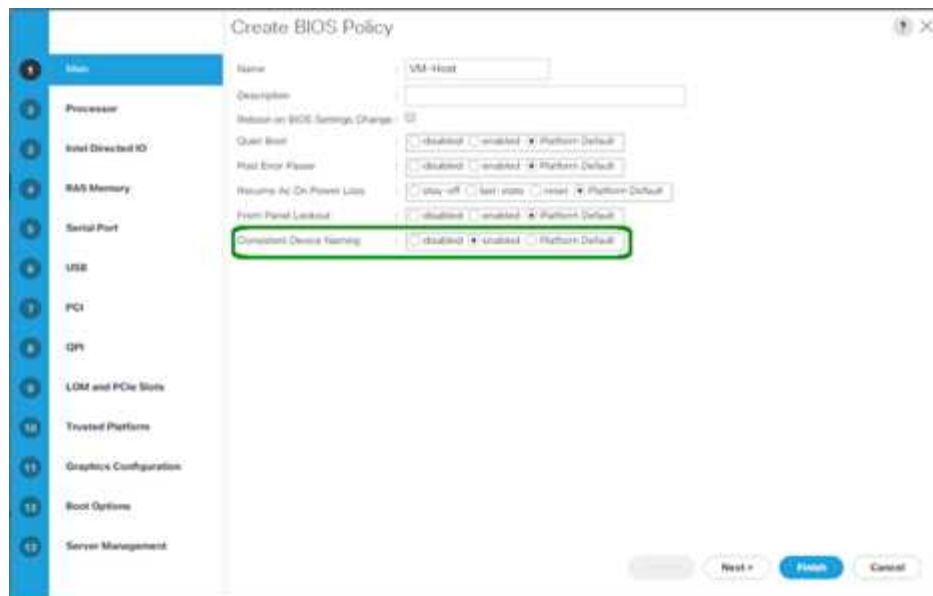
8. プロセス ID（PID）として「<UCS-CPU-PID>`」と入力します。
9. [OK] をクリックして、CPU/ コアの資格情報を作成します。
10. [OK] をクリックしてポリシーを作成し、[OK] をクリックして確認します。



サーバ BIOS ポリシーを作成します

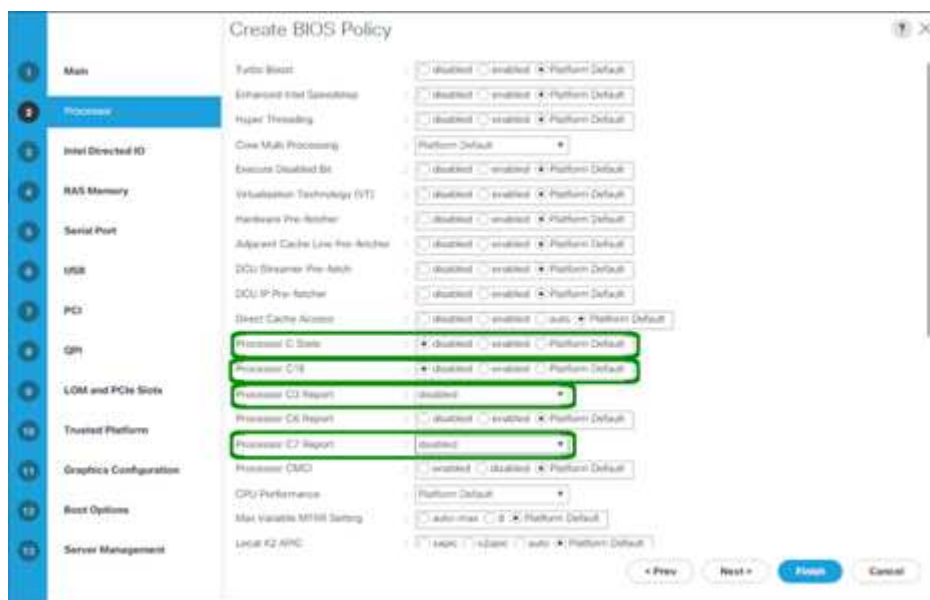
Cisco UCS 環境のサーバ BIOS ポリシーを作成するには、次の手順を実行します。

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



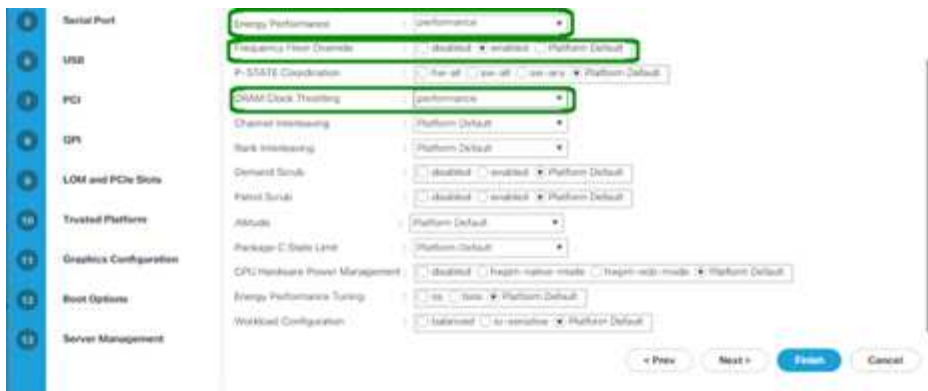
8. [プロセッサ] タブを選択し、次のパラメータを設定します。

- プロセッサ C の状態：無効
- プロセッサ C1E：無効
- プロセッサ C3 レポート：無効
- プロセッサ C7 レポート：無効



9. 残りのプロセッサオプションまで下にスクロールして、次のパラメータを設定します。

- エネルギー性能：パフォーマンス
- 周波数下限のオーバーライド：有効
- DRAM Clock Throttling：パフォーマンス



10. [RAS メモリ] をクリックして、次のパラメータを設定します。

- LV DDR モード：パフォーマンスモード



11. Finish をクリックして、BIOS ポリシーを作成します。

12. [OK] をクリックします。

デフォルトのメンテナンスポリシーを更新する

デフォルトのメンテナンスポリシーを更新するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [ポリシー]>[ルート]を選択します。
3. [メンテナンスポリシー]>[デフォルト]を選択します。
4. Reboot Policy を User Ack に変更します
5. [次のブート時]を選択して、メンテナンス時間をサーバー管理者に委任します。

Servers / Policies / root / Maintenance Poli... / default

General Events

Actions

Cancel

Show Policy Usage

Use Global

Properties

Name : default

Description :

Owner : Local

Soft Shutdown Timer : 150 Secs


Reboot Policy : ☐ Immediate ☒ User Ack ☐ Timer Automatic

☒ On Next Boot (Apply pending changes at next reboot.)

6. [Save Changes] をクリックします。
7. [OK] をクリックして変更を確定します。

vNIC テンプレートを作成します

Cisco UCS 環境用に複数の仮想ネットワークインターフェイスカード（vNIC）テンプレートを作成するには、この項で説明する手順を実行します。

 合計 4 つの vNIC テンプレートが作成されます。

インフラストラクチャ vNIC を作成します

インフラストラクチャ vNIC を作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [vNIC Templates] を右クリックします。
4. [Create vNIC Template] を選択します。
5. vNIC テンプレート名として「ite-XX-vnic_a」と入力します。
6. [テンプレートタイプ] として [更新テンプレート] を選択します。
7. [Fabric ID] に [Fabric A] を選択します
8. [Enable Failover] オプションが選択されていないことを確認します。
9. [冗長性タイプ] の [プライマリテンプレート] を選択します。
10. ピア冗長性テンプレートを「<not set>」のままにします。
11. [ターゲット] で、[アダプタ] オプションのみが選択されていることを確認します。
12. ネイティブ VLAN として 'Native - VLAN' を設定します
13. CDN ソースの vNIC 名を選択します。
14. MTU の場合は 9000 と入力します。
15. [Permitted VLANs] で、[Native - VLAN]、[Site-XX-IB-MGMT]、[Site-XX-NFS]、[Site-XX-VM-Traffic] を選択します。 および Site-XX-MvMotion複数選択するには、Ctrl キーを使用します。
16. 選択をクリックします。これらの VLAN が Selected VLANs の下に表示されます。

17. [MAC Pool] リストで、[M AC_Pool_A] を選択します。
18. [ネットワーク制御ポリシー] リストで、[プールA] を選択します
19. [ネットワーク制御ポリシー] リストで、[有効 - CDP-LLDP] を選択します。
20. [OK] をクリックして、vNIC テンプレートを作成します。
21. [OK] をクリックします。

LAN > Policies > root > vNIC Templates > vNIC Template vNIC_Template_A

General vNICs vNIC Groups Fabric Export

Actions

- Modify vNICs
- Modify vNIC Groups
- Create
- Show Policy Usage
- Use Default

Properties

Name: **vNIC_Template_A**

Description:

Owner: Local

Fabric ID: ☐ Fabric A ☐ Fabric B ☒ Enable Failover

Redundancy

Redundancy Type: ☐ No Redundancy ☒ Primary Template ☐ Secondary Template

Peer Redundancy Template: vNIC_Template_B [Create vNIC Template](#)

Target

☒ vNICs ☐ vNIC

Template Type: ☐ Initial Template ☒ Updating Template

CDV Source: ☒ vNIC Name ☐ User Defined

VPI: 9000

Policies

MAC Pool: MAC_Pool_AfterV

QoS Policy: vnic_def

Network Control Policy: Enable_CDP

Pin Group: vnic_def

State Threshold Policy: default

Connection Policies

☒ Dynamic vNIC ☐ vNIC ☐ VAG

Dynamic vNIC Connection Policy: vnic_def

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

1. Cisco UCS Manager で、左側の [LAN] をクリックします。
2. [ポリシー]>[ルート] を選択します。
3. [vNIC Templates] を右クリックします。
4. [Create vNIC Template] を選択します。
5. vNIC テンプレート名として「ite-XX-vnic_B」と入力します。
6. [テンプレートタイプ] として [更新テンプレート] を選択します。
7. [Fabric ID] に [Fabric B] を選択します
8. [Enable Failover] オプションを選択します。



フェールオーバーを選択することは、ハードウェアレベルでリンクのフェールオーバー時間を改善し、仮想スイッチで検出されない NIC 障害の可能性を防ぐための重要なステップです。

9. [冗長性タイプ] の [プライマリテンプレート] を選択します。
10. ピア冗長性テンプレートは 'vNIC_Template_A' のままにします
11. [ターゲット] で、[アダプタ] オプションのみが選択されていることを確認します。
12. ネイティブ VLAN として 'Native - VLAN' を設定します
13. CDN ソースの vNIC 名を選択します。
14. MTU には '9000' と入力します
15. [Permitted VLANs] で、[Native - VLAN]、[Site-XX-IB-MGMT]、[Site-XX-NFS]、[Site-XX-VM-Traffic] を選択します。 および Site-XX-MvMotion複数選択するには、Ctrl キーを使用します。
16. 選択をクリックします。これらの VLAN が Selected VLANs の下に表示されます。
17. [MAC Pool] リストで、[MAC_Pool_b] を選択します。
18. [Network Control Policy] リストで、[Pool-B] を選択します
19. [ネットワーク制御ポリシー] リストで、[有効 - CDP-LLDP] を選択します。
20. [OK] をクリックして、vNIC テンプレートを作成します。
21. [OK] をクリックします。

LAN / Policies / root / vNIC Template / vNIC Template vNIC_Template_B

Current VLANs VLAN Groups Pools Policies

Actions

- Modify VLANs
- Modify VLAN Groups
- Delete
- Show Policy Usage
- Use Default

Properties

Name: vNIC_Template_B

Description:

Owner: Local

Fabric ID: ☐ Fabric A ☒ Fabric B ☒ Enable Fabric

Redundancy

Redundancy Type: ☐ No Redundancy ☐ Primary Template ☒ Secondary Template

Peer Redundancy Template: vNIC_Template_A

Create vNIC Template

Target

☒ Adapter ☐ VM

Template Type: ☐ New Template ☒ Updating Template

CDN Source: ☒ vNIC Name ☐ User Defined

MTU: 9000

Policies

MAC Pool: MAC_Pool_B(56/54)

QoS Policy: ☐ null ☒ 0

Network Control Policy: ☒ Standard_CDP

Pin Group: ☐ null ☒ 0

Stats Threshold Policy: ☐ null ☒ 0

Connection Policies

☒ Dynamic vNIC ☐ usfnc ☐ VMQ

Dynamic vNIC Connection Policy: ☐ null ☒ 0

iSCSI vNIC を作成します

iSCSI vNIC を作成するには、次の手順を実行します。

1. 左側の [LAN] を選択します。
2. [ポリシー]>[ルート] を選択します。
3. [vNIC Templates] を右クリックします。
4. [Create vNIC Template] を選択します。
5. vNIC テンプレート名として「'Site-01-iSCSI_A'」を入力します。
6. [Fabric A] を選択します[Enable Failover] オプションは選択しないでください。
7. 冗長性タイプを冗長性なしに設定したままにします。
8. [ターゲット] で、[アダプタ] オプションのみが選択されていることを確認します。
9. [テンプレートタイプ] で [テンプレートの更新] を選択します。
10. [VLANs] で、[Site-01-iSCSI_A_VLAN] だけを選択します。
11. [Site-01-iSCSI_A_VLAN] をネイティブ VLAN として選択します。
12. CDN ソースに対して vNIC 名を設定したままにします。
13. MTU の下に 9000 と入力します。
14. MAC Pool リストから MAC-Pool-A を選択します
15. Network Control Policy リストから、Enable-CDP-LLDP を選択します。
16. [OK] をクリックして、vNIC テンプレートの作成を完了します。
17. [OK] をクリックします。

General VLANs VLAN Groups Faults Events

Actions

- Modify VLANs
- Modify VLAN Groups
- Delete
- Show Policy Usage
- Use Global

Properties

Name : Site_01_ISCSI-A

Description :

Owner : Local

Fabric ID : ☒ Fabric A ☐ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Target

☒ Adapter ☐ VM

Template Type : ☐ Initial Template ☒ Updating Template

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

Policies

MAC Pool : MAC_Pool_A(56/64)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

18. 左側の [LAN] を選択します。
19. [ポリシー]>[ルート]を選択します。
20. [vNIC Templates] を右クリックします。
21. [Create vNIC Template] を選択します。
22. vNIC テンプレート名として「Site-01-iSCSI_B」を入力します。
23. ファブリック B を選択します[Enable Failover] オプションは選択しないでください。
24. 冗長性タイプを冗長性なしに設定したままにします。
25. [ターゲット]で、[アダプタ] オプションのみが選択されていることを確認します。
26. [テンプレートタイプ]で[テンプレートの更新]を選択します。
27. [VLANs]で、[s it-01-iscsi_B_VLAN]のみを選択します。
28. ネイティブ VLAN として [s it-01-iSCSI_B_VLAN] を選択します。
29. CDN ソースに対して vNIC 名を設定したままにします。
30. MTU の下に 9000 と入力します。
31. [MAC Pool] リストから、[MAC-Pool-B] を選択します。
32. [ネットワーク制御ポリシー] リストから、[有効 - CDP-LLDP-M] を選択します。
33. [OK] をクリックして、vNIC テンプレートの作成を完了します。

34. [OK] をクリックします。

The screenshot shows the Cisco UCS Manager interface for configuring a vNIC Template. The breadcrumb navigation at the top is LAN / Policies / root / vNIC Templates / vNIC Template Site_01_ISCSI-B. The left sidebar has tabs for General, VLANs, VLAN Groups, Faults, and Events, with 'General' selected. Under the 'Actions' section, there are links for 'Modify VIFs', 'Modify VLAN Groups', 'Delete', 'Show Policy Usage', and 'View Config'. The main configuration area is divided into 'Properties' and 'Policies' sections. In the 'Properties' section, 'Name' is 'Site_01_ISCSI-B', 'Description' is empty, 'Owner' is 'Local', 'Fabric ID' is 'Fabric B' (selected over 'Fabric A'), and 'Enable Failover' is unchecked. The 'Redundancy' section shows 'Redundancy Type' as 'No Redundancy' (selected over 'Primary Template' and 'Secondary Template'). The 'Target' section has 'Add Target' and 'VIF' buttons. The 'Template Type' section shows 'Initial Template' and 'Updating Template' (selected). The 'CDN Source' section shows 'vNIC Name' (selected over 'User Defined'). The 'MTU' is set to '9000'. The 'Policies' section includes 'MAC Pool' (MAC_Pool_B156/64), 'QoS Policy' (<not set>), 'Network Control Policy' (Enable_CDP), 'Pin Group' (<not set>), and 'Stats Threshold Policy' (default). The 'Connection Policies' section shows 'Dynamic vNIC' (selected over 'usNIC' and 'VMD') and 'Dynamic vNIC Connection Policy' (<not set>).

iSCSI ブート用の LAN 接続ポリシーを作成します

この手順環境は、2つの iSCSI LIF がクラスタノード 1（「iscsi_dlif01a」および「iscsi_dlif01b」）にあり、2つの iSCSI LIF がクラスタノード 2（「iscsi_dlif02a」および「iscsi_dlif02b」）にある Cisco UCS 環境です。また、A LIF がファブリック A（Cisco UCS 6324 A）に接続され、B LIF がファブリック B（Cisco UCS 6324 B）に接続されていると想定しています。

必要なインフラストラクチャ LAN 接続ポリシーを設定するには、次の手順を実行します。

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

8. [Use vNIC Template] オプションを選択します。
9. [vNIC Template] リストで、[vNIC_Template_A] を選択します。
10. [Adapter Policy] ドロップダウンリストから [VMware] を選択します。
11. [OK] をクリックして、この vNIC をポリシーに追加します。

Modify vNIC

Name : Site-01-vNIC-A

Use vNIC Template: ☒

Create vNIC Template

vNIC Template: vNIC_Template_A ▼

Adapter Performance Profile

Adapter Policy : VMWare ▼

Create Ethernet Adapter Policy

Create QoS Policy

Create Network Control Policy

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

OK Cancel

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

23. [OK] をクリックして、この vNIC をポリシーに追加します。
24. vNIC を追加するには、上部の Add オプションをクリックします。
25. [Create vNIC] ダイアログボックスで、vNIC の名前として「Site-01-iSCSI-B」と入力します。
26. [Use vNIC Template] オプションを選択します。
27. [vNIC Template] リストで、[Site-01-iSCSI-B] を選択します。
28. [Adapter Policy] ドロップダウンリストから [VMware] を選択します。
29. [OK] をクリックして、この vNIC をポリシーに追加します。
30. Add iSCSI vNICs オプションを展開します。
31. [Add iSCSI vNICs] スペースの下側の [Add] オプションをクリックして、iSCSI vNIC を追加します。
32. [Create iSCSI vNIC] ダイアログボックスで、vNIC の名前として「Site-01-iSCSI-A」を入力します。
33. [Overlay vNIC] を [Site-01-iSCSI-A] として選択します。
34. [iSCSI Adapter Policy] オプションは [Not Set] のままにします。
35. VLAN を「Site-01-iSCSI-Site-A」（ネイティブ）として選択します。
36. MAC アドレスの割り当てとして、None（なし）（デフォルトで使用）を選択します。
37. [OK] をクリックして、iSCSI vNIC をポリシーに追加します。

Modify iSCSI vNIC ? ×

Name : **Site-01-ISCSI-A**

Overlay vNIC :

iSCSI Adapter Policy : [Create iSCSI Adapter Policy](#)

VLAN :

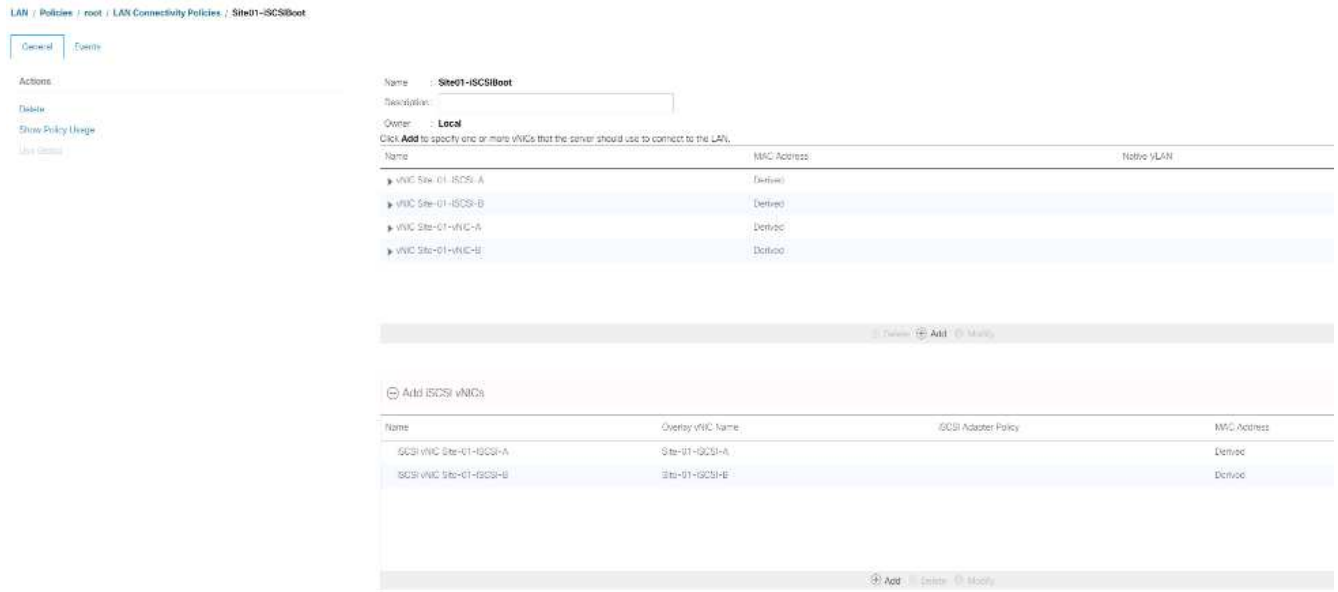
iSCSI MAC Address

MAC Address Assignment:

[Create MAC Pool](#)

OK **Cancel**

38. [Add iSCSI vNICs] スペースの下側の [Add] オプションをクリックして、iSCSI vNIC を追加します。
39. [Create iSCSI vNIC] ダイアログボックスで、vNIC の名前として「`Site-01-iSCSI-B」を入力します。
40. Overlay vNIC を Site-01-iSCSI-B として選択します
41. [iSCSI Adapter Policy] オプションは [Not Set] のままにします。
42. VLAN を「ite-01-iSCSI-Site-B」 (ネイティブ) として選択します。
43. MAC アドレスの割り当てとして、[なし] (デフォルトで使用) を選択します。
44. [OK] をクリックして、iSCSI vNIC をポリシーに追加します。
45. [Save Changes] をクリックします。



VMware ESXi 6.7U1 インストールブート用の vMedia ポリシーを作成します

NetApp Data ONTAP のセットアップ手順では、NetApp Data ONTAP と VMware ソフトウェアのホストに使用する HTTP Web サーバが必要です。ここで作成される vMedia ポリシーは、VMware ESXi 6 をマッピングします。ESXi のインストールをブートするために Cisco UCS サーバに接続された 7U1 ISO。このポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の [Servers] を選択します。
2. [ポリシー]>[ルート] を選択します。
3. [vMedia Policies] を選択します。
4. [追加] をクリックして、新しい vMedia ポリシーを作成します。
5. ポリシーに「esxi- 6.7U1-HTTP」という名前を付けます。
6. 概要フィールドに ESXi 6.7U1 用のマウント ISO と入力します。
7. [マウント失敗時の再試行] で [はい] を選択します
8. 追加をクリックします。
9. マウントに esxi- 6.7U1-HTTP という名前を付けます。
10. CDD デバイスタイプを選択します。
11. HTTP プロトコルを選択します。
12. Web サーバの IP アドレスを入力します。



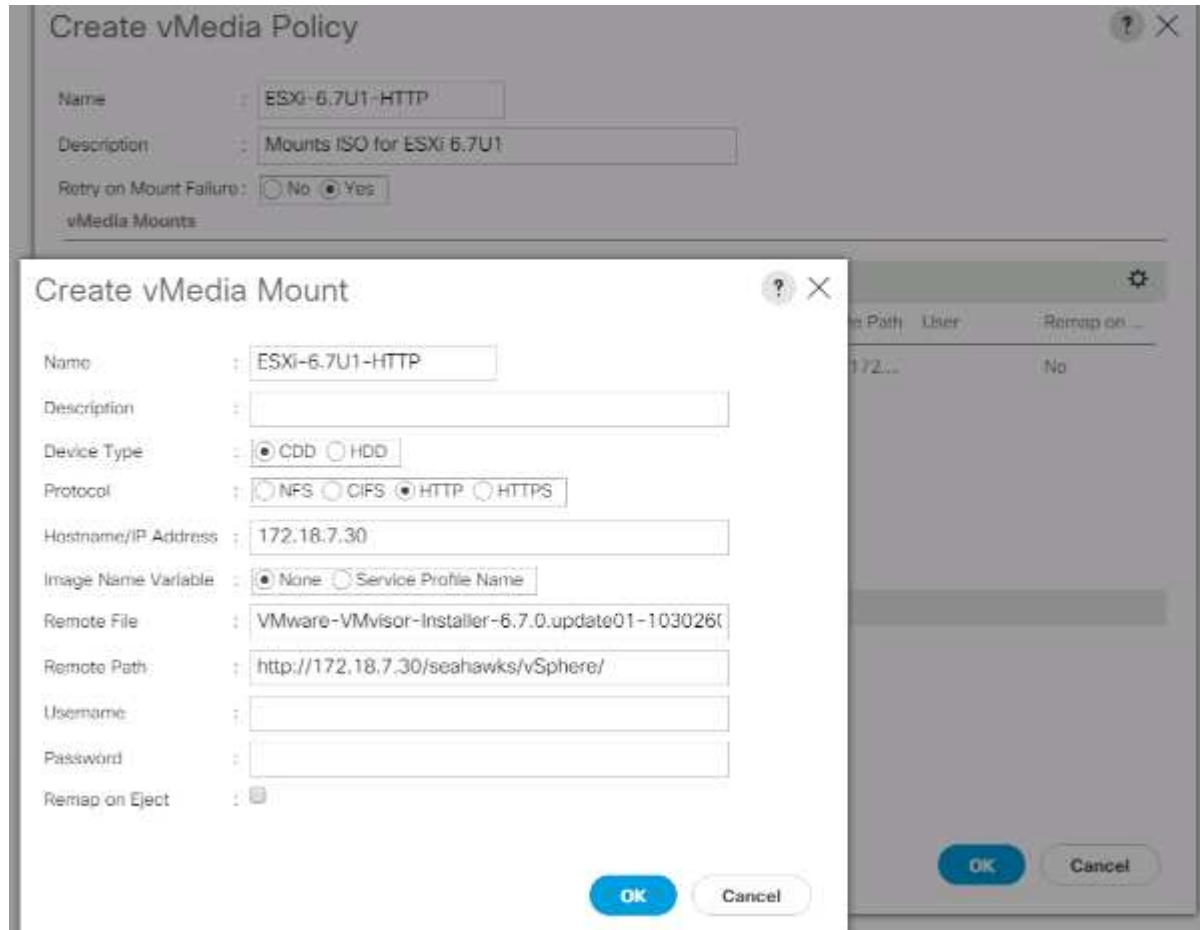
DNS サーバの IP は KVM IP に入力されていなかったため、ホスト名ではなく Web サーバの IP を入力する必要があります。

13. リモートファイル名として「VMware-VMvator-Installer-6.7.0.update01-10302608.x86_64 .iso」と入力します。

この VMware ESXi 6.7U1 ISO は、からダウンロードできます ["VMware のダウンロード"](#)。

14. [リモートパス] フィールドに ISO ファイルへの Web サーバパスを入力します。
15. [OK] をクリックして、vMedia マウントを作成します。
16. [OK] をクリックし、もう一度 [OK] をクリックして、vMedia ポリシーの作成を完了します。

Cisco UCS 環境に追加された新しいサーバでは、vMedia サービスプロファイルテンプレートを使用して ESXi ホストをインストールできます。SAN でマウントされたディスクが空の場合、初回ブート時に ESXi インストーラでホストがブートします。ESXi のインストール後、起動ディスクがアクセス可能である限り、vMedia は参照されません。



iSCSI ブートポリシーを作成します

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

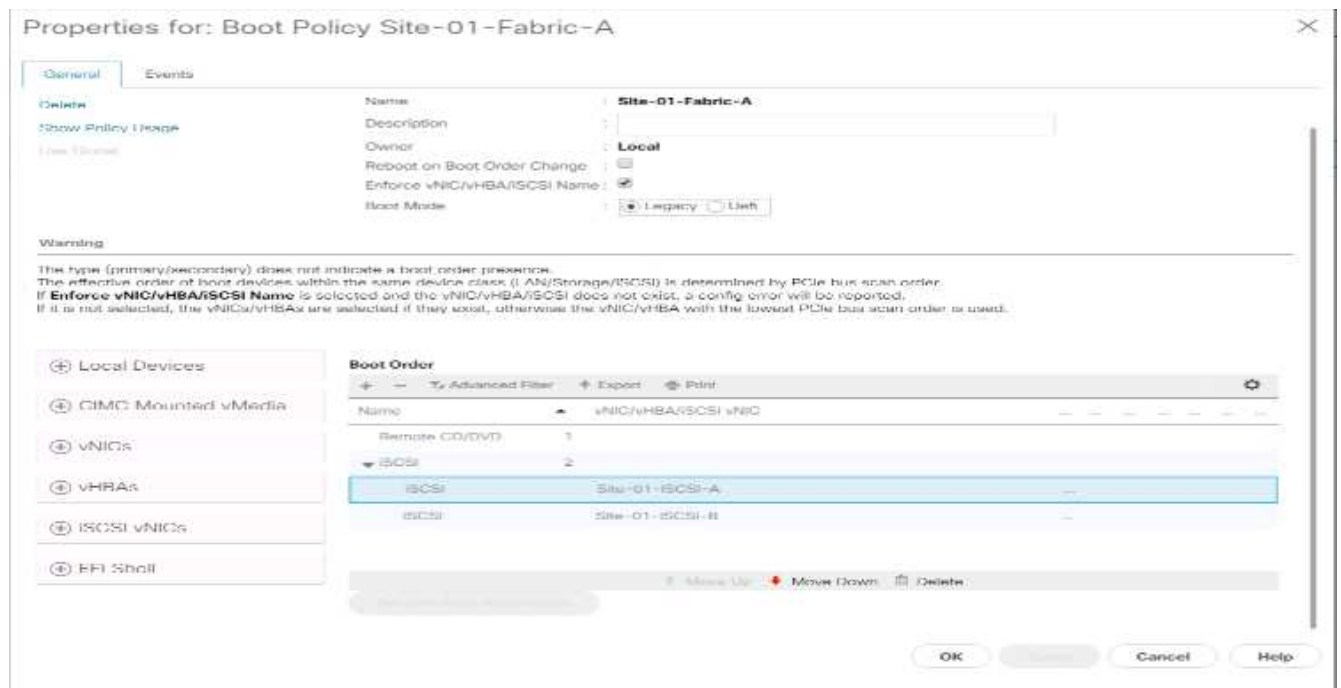


この手順には、1つのブートポリシーが設定されています。このポリシーでは、プライマリ・ターゲットを iSCSI lif01a に設定します

Cisco UCS 環境のブートポリシーを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。

2. [ポリシー]>[ルート]を選択します。
3. [Boot Policies] を右クリックします。
4. Create Boot Policy を選択します。
5. ブートポリシーの名前として「'Site-01-Fabric-a」を入力します。
6. オプション：ブートポリシーの概要を入力します。
7. Boot Order Change オプションを選択解除したまま再起動します。
8. 起動モードはレガシーです。
9. [ローカルデバイス] ドロップダウンメニューを展開し、[リモート CD/DVD の追加] を選択します。
10. [iSCSI vNICs] ドロップダウンメニューを展開し、[Add iSCSI Boot] を選択します。
11. [Add iSCSI Boot] ダイアログボックスに「'Site-01-iSCSI-A」を入力します。[OK] をクリックします。
12. Add iSCSI Boot を選択します。
13. [Add iSCSI Boot] ダイアログボックスに「'Site-01-iSCSI-B」を入力します。[OK] をクリックします。
14. [OK] をクリックして、ポリシーを作成します。



サービスプロファイルテンプレートを作成します

この手順では、ファブリック A ブート用にインフラ ESXi ホスト用のサービスプロファイルテンプレートが 1 つ作成されます。

サービスプロファイルテンプレートを作成するには、次の手順を実行します。

1. Cisco UCS Manager で、左側の Servers をクリックします。
2. [サービスプロファイルテンプレート]>[ルート]を選択します。
3. ルートを右クリックします。

4. [サービスプロファイルテンプレートの作成] を選択して、[サービスプロファイルテンプレートの作成] ウィザードを開きます。
5. サービス・プロファイル・テンプレートの名前として 'VM-Host-Infra-iSCSI-A' を入力しますこのサービスプロファイルテンプレートは、ファブリック A のストレージノード 1 からブートするように設定されています
6. [テンプレートの更新] オプションを選択します。
7. [UUID] で、[UUID_Pool] を UUID プールとして選択します。次へをクリックします。

The screenshot shows the 'Create Service Profile Template' wizard. The left sidebar has steps 1 through 11. Step 1 is selected. The main area has the following fields:

- Name:** VM-Host-Infra-iSCSI-A
- Where:** org-root
- Type:** Updating Template
- UUID Assignment:** UUID_Pool(16/16)
- Description:** (Empty text area)

Buttons at the bottom: Back, Next >, Finish, Cancel.

ストレージプロビジョニングを設定する

ストレージプロビジョニングを設定するには、次の手順を実行します。

1. 物理ディスクを持たないサーバーがある場合は、ローカルディスク設定ポリシーをクリックし、SAN ブートローカルストレージポリシーを選択します。それ以外の場合は、デフォルトのローカルストレージポリシーを選択します。
2. 次へをクリックします。

ネットワークオプションを設定します

ネットワークオプションを設定するには、次の手順を実行します。

1. ダイナミック vNIC 接続ポリシーのデフォルト設定を保持します。
2. Use Connectivity Policy オプションを選択して、LAN 接続を設定します。
3. [LAN Connectivity Policy] ドロップダウンメニューから [iSCSI-Boot] を選択します。
4. [イニシエータ名の割り当て] で [IQN_Pool] を選択します次へをクリックします。

SAN 接続を設定

SAN 接続を設定するには、次の手順を実行します。

1. vHBA の場合は、SAN 接続を構成する方法を選択します。オプション
2. 次へをクリックします。

ゾーニングを設定します

ゾーニングを設定するには「次へ」をクリックします

vNIC/vHBA の配置を設定します

vNIC/vHBA の配置を設定するには、次の手順を実行します。

1. 配置を選択 (Select Placement) ドロップダウンリストから「配置ポリシー」をシステムが配置を実行できるようにします
2. 次へをクリックします。

vMedia ポリシーを設定します

vMedia ポリシーを設定するには、次の手順を実行します。

1. vMedia ポリシーは選択しないでください。
2. 次へをクリックします。

サーバのブート順序を設定します

サーバのブート順序を設定するには、次の手順を実行します。

1. ブート・ポリシーに [Boot - Fabric-a] を選択します

Create Service Profile Template

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: Site-01-Fabric-A [Create Boot Policy](#)

Name: Site-01-Fabric-A
Description:
Reboot on Boot Order Change: No
Enforce vNIC/vHBA/iSCSI Name: Yes
Boot Mode: Legacy

WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Boot Order

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	LUN Na...	WWN	Slot Nu...	Boot Na...	Boot Path	Descripti...
HBA	1								
iSCSI	2								
iSCSI Site-01-SCSI-A		Site-01-SCSI-A	Primary						
iSCSI Site-01-SCSI-B		Site-01-SCSI-B	Secondary						

< Prev Next > Finish Cancel

2. Boot 注文で、「ライト -01-iSCSI-A」を選択します。

3. iSCSI 起動パラメータの設定をクリックします。

4. iSCSI ブートパラメータの設定ダイアログボックスで、環境に適した認証プロファイルを個別に作成していない限り、認証プロファイルオプションを Not Set のままにします。

5. [イニシエータ名の割り当て] ダイアログボックスは、前の手順で定義した単一のサービスプロファイルのイニシエータ名を使用するように設定されていないままにします。

6. 「iSCSI_IP_Pool_A」をイニシエータ IP アドレス・ポリシーとして設定します。

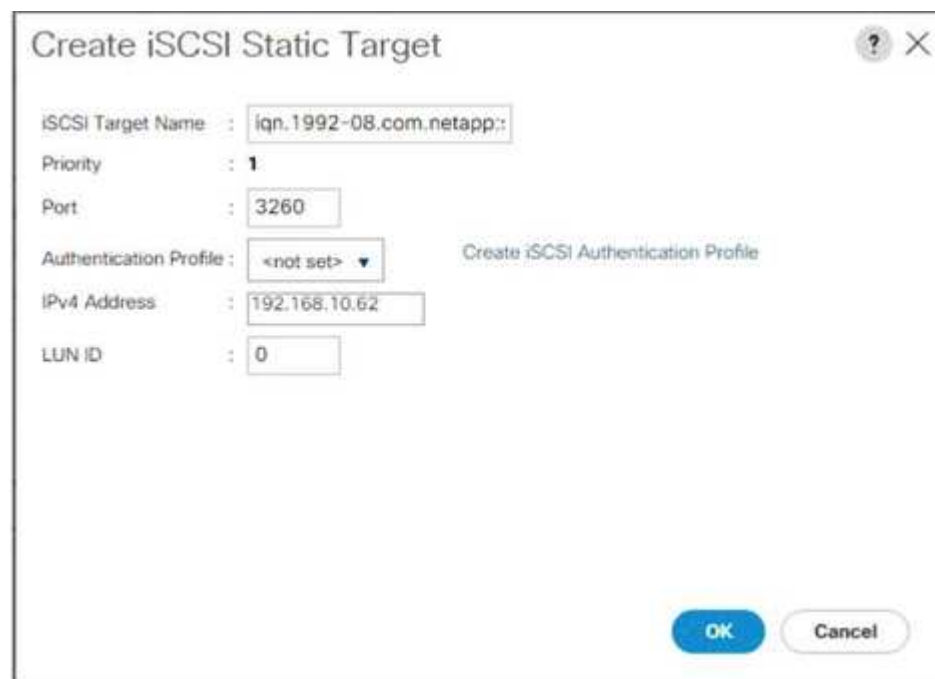
7. iSCSI Static Target Interface オプションを選択します。

8. 追加をクリックします。

9. iSCSI ターゲット名を入力します。Infra-SVM の iSCSI ターゲット名を取得するには 'ストレージ・クラスタ管理インタフェースにログインして 'iSCSI show コマンドを実行します

```
bb04-aff300::> iscsi show
Target          Target          Status
Vserver Name      Alias           Admin
-----
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                               Infra-SVM       up
```

10. IPv4 Address フィールドに「iSCSI_LIF_02a」の IP アドレスを入力します。

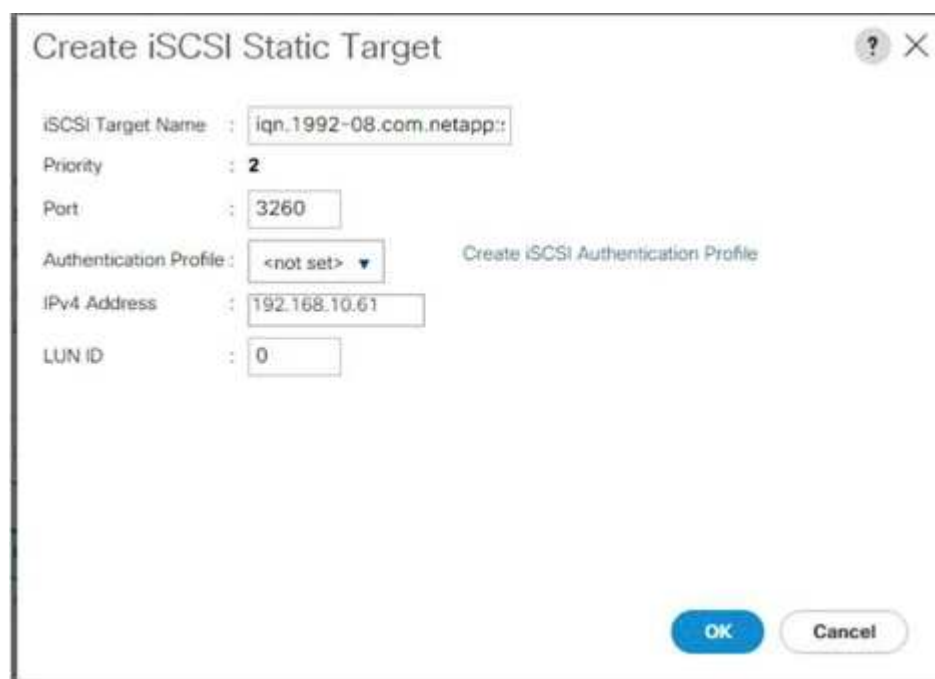


The dialog box titled "Create iSCSI Static Target" contains the following fields and values:

Field	Value
iSCSI Target Name	iqn.1992-08.com.netapp::
Priority	1
Port	3260
Authentication Profile	<not set>
IPv4 Address	192.168.10.62
LUN ID	0

Buttons: OK, Cancel

11. OK をクリックして、iSCSI 静的ターゲットを追加します。
12. 追加をクリックします。
13. iSCSI ターゲット名を入力します。
14. IPv4 Address フィールドに 'iSCSI_LIF_01a' の IP アドレスを入力します



The dialog box titled "Create iSCSI Static Target" contains the following fields and values:

Field	Value
iSCSI Target Name	iqn.1992-08.com.netapp::
Priority	2
Port	3260
Authentication Profile	<not set>
IPv4 Address	192.168.10.61
LUN ID	0

Buttons: OK, Cancel

15. OK をクリックして、iSCSI 静的ターゲットを追加します。

Set iSCSI Boot Parameters

Name : **iSCSI-A-vNIC**

Authentication Profile : <not set> [Create iSCSI Authentication Profile](#)

Initiator Name

Initiator Name Assignment: <not set>

[Create IQN Suffix Pool](#)

WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

Initiator Address

Initiator IP Address Policy: iSCSI_IP_Pool_A(12/16)

IPv4 Address : 0.0.0.0
 Subnet Mask : 255.255.255.0
 Default Gateway : 0.0.0.0
 Primary DNS : 0.0.0.0
 Secondary DNS : 0.0.0.0

[Create IP Pool](#)
[Reset Initiator Address](#)
 The IP address will be automatically assigned from the selected pool.

☒ iSCSI Static Target Interface ☐ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pro.	iSCSI IPv4 Address	LUN id
iqn.1992-08.c...	1	3260		192.168.10.62	0
iqn.1992-08.c...	2	3260		192.168.10.61	0

OK Cancel



ストレージノード 02 の IP を最初に、ストレージノード 01 の IP を 2 番目にして、ターゲット IP を入力しました。これは、ブート LUN がノード 01 にあることを前提としています。この手順で順序が使用されている場合、ホストはノード 01 へのパスを使用してブートします。

16. 起動順序で、[iSCSI-B-vNIC] を選択します。
17. iSCSI 起動パラメータの設定をクリックします。
18. iSCSI ブートパラメータの設定ダイアログボックスで、環境に適した認証プロファイルを個別に作成していない限り、認証プロファイルオプションは Not Set のままにします。
19. [イニシエータ名の割り当て] ダイアログボックスは、前の手順で定義した単一のサービスプロファイルのイニシエータ名を使用するように設定されていないままにします。
20. イニシエータの IP アドレス・ポリシーとして 'iSCSI_IP_Pool_B' を設定します
21. iSCSI Static Target Interface オプションを選択します。
22. 追加をクリックします。
23. iSCSI ターゲット名を入力します。Infra-SVM の iSCSI ターゲット名を取得するには 'ストレージ・クラスタ管理インタフェースにログインして 'iSCSI show コマンドを実行します

```
bb04-aff300::> iscsi show
```

Vserver	Target Name	Target Alias	Status Admin
Infra-SVM	iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3	Infra-SVM	up

24. IPv4 Address フィールドに 'iSCSI_LIF_02b' の IP アドレスを入力します



The dialog box titled "Create iSCSI Static Target" contains the following fields and values:

- iSCSI Target Name : iqn.1992-08.com.netapp::
- Priority : 1
- Port : 3260
- Authentication Profile : <not set> (with a dropdown arrow)
- IPv4 Address : 192.168.20.62
- LUN ID : 0

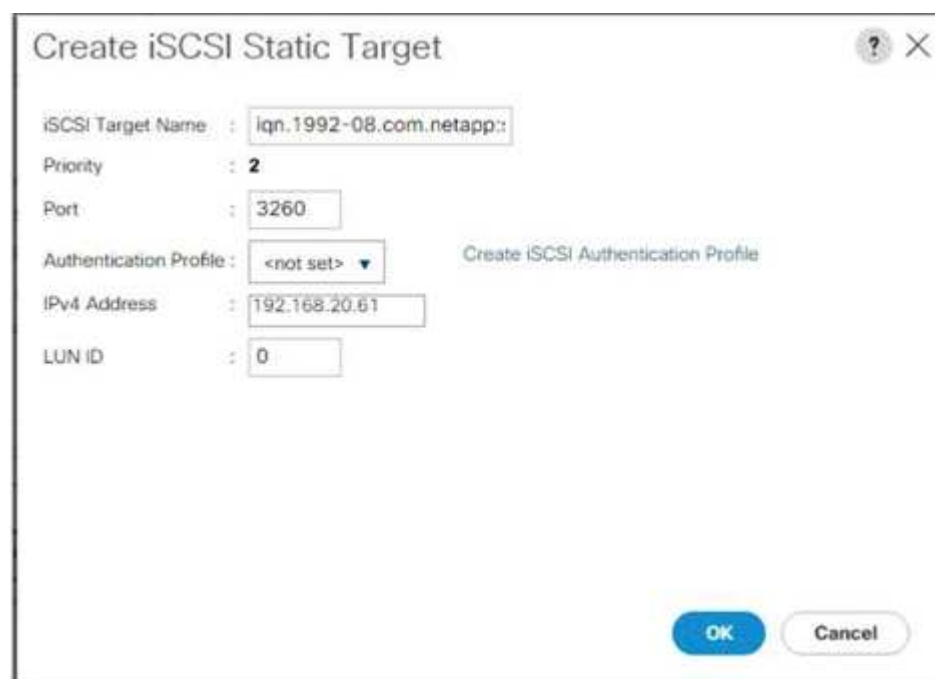
Buttons at the bottom: OK (blue), Cancel (grey). A link "Create iSCSI Authentication Profile" is visible next to the Authentication Profile field.

25. OK をクリックして、iSCSI 静的ターゲットを追加します。

26. 追加をクリックします。

27. iSCSI ターゲット名を入力します。

28. IPv4 Address フィールドに 'iSCSI_LIF_01b' の IP アドレスを入力します



The dialog box titled "Create iSCSI Static Target" contains the following fields and values:

- iSCSI Target Name : iqn.1992-08.com.netapp::
- Priority : 2
- Port : 3260
- Authentication Profile : <not set> (with a dropdown arrow)
- IPv4 Address : 192.168.20.61
- LUN ID : 0

Buttons at the bottom: OK (blue), Cancel (grey). A link "Create iSCSI Authentication Profile" is visible next to the Authentication Profile field.

29. OK をクリックして、iSCSI 静的ターゲットを追加します。

Set iSCSI Boot Parameters

Create IQN Suffix Pool

WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

Initiator Address:

Initiator IP Address Policy: iSCSI_IP_Pool_B(12/16) ▼

IPv4 Address : **0.0.0.0**

Subnet Mask : **255.255.255.0**

Default Gateway : **0.0.0.0**

Primary DNS : **0.0.0.0**

Secondary DNS : **0.0.0.0**

Create IP Pool

Reset Initiator Address

The IP address will be automatically assigned from the selected pool.

☒ iSCSI Static Target Interface ☐ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pro.	iSCSI IPv4 Address	LUN Id
iqn.1992-08.c...	1	3260		192.168.20.62	0
iqn.1992-08.c...	2	3260		192.168.20.61	0

[Add](#) [Delete](#) [Info](#)

Minimum one instance of iSCSI Static Target interface and maximum two are allowed.

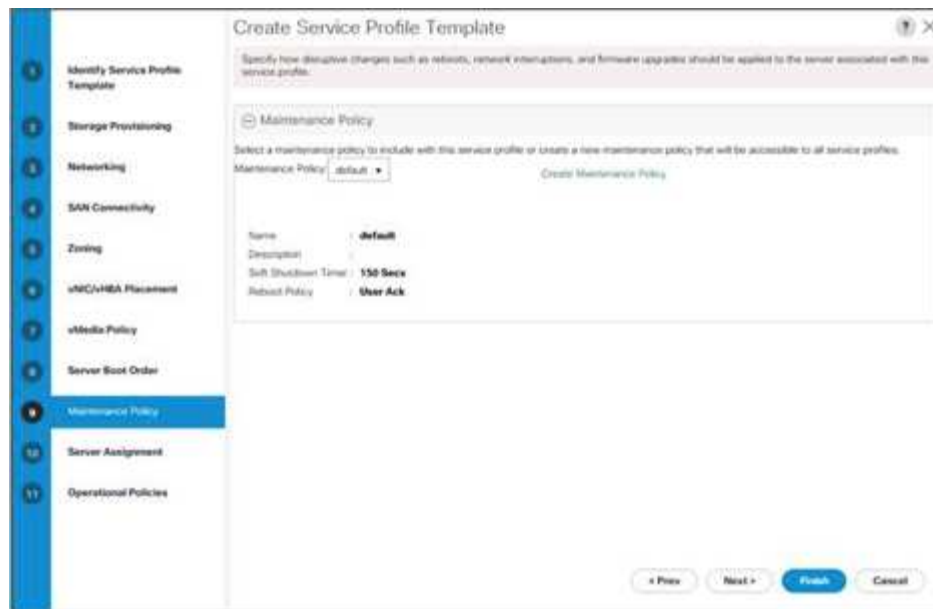
OK Cancel

30. 次へをクリックします。

メンテナンスポリシーを設定する

メンテナンスポリシーを設定するには、次の手順を実行します。

1. メンテナンスポリシーをデフォルトに変更します。



2. 次へをクリックします。

サーバの割り当てを設定します

サーバ割り当てを設定するには、次の手順を実行します。

1. [プールの割り当て] リストで [インフラプール] を選択します。
2. プロファイルがサーバーに関連付けられている場合に適用する電源状態として、[Down] を選択します。
3. ページ下部のファームウェア管理を展開し、デフォルトポリシーを選択します。

4. 次へをクリックします。

運用ポリシーを設定

運用ポリシーを設定するには、次の手順を実行します。

1. BIOS Policy ドロップダウンリストから VM-Host を選択します。
2. Power Control Policy Configuration （電源制御ポリシーの設定）を展開し、Power Control Policy （電源制御ポリシー）ドロップダウンリストから No-Power-Cap （電源なし - 電力上限）を選択します。

3. [完了] をクリックして、サービスプロファイルテンプレートを作成します。
4. 確認メッセージで [OK] をクリックします。

vMedia 対応のサービスプロファイルテンプレートを作成します

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

1. UCS Manager に接続し、左側の [サーバ] をクリックします。
2. サービスプロファイルテンプレート > ルート > サービステンプレート VM-Host-Infra-iSCSI-A を選択します
3. [VM-Host-Infra-iSCSI-A] を右クリックし、[クローンの作成] を選択します。
4. クローンに 'VM-Host-Infra-iSCSI-A-VM' という名前を付けます
5. 新しく作成した VM-Host-Infra-iSCSI-A-VM を選択し、右側の [vMedia Policy] タブを選択します。
6. Modify vMedia Policy をクリックします。
7. ESXi-6 を選択します。7U1 - HTTP vMedia Policy (HTTP vMedia ポリシー) を選択し、OK をクリックします。
8. [OK] をクリックして確定します。

サービスプロファイルを作成する

サービスプロファイルテンプレートからサービスプロファイルを作成するには、次の手順を実行します。

1. Cisco UCS Manager に接続し、左側の [サーバ] をクリックします。
2. [サーバー] > [サービスプロファイルテンプレート] > [ルート] > [サービステンプレート] を展開します。
3. [アクション] で、[テンプレートからサービスプロファイルを作成] をクリックし、次の手順を実行します。
 - a. 命名プレフィックスとして「Site-01-Infra-0」を入力します。
 - b. 作成するインスタンスの数として「2」を入力します。
 - c. ルートを組織として選択します。
 - d. [OK] をクリックして、サービスプロファイルを作成します。



4. 確認メッセージで [OK] をクリックします。
5. サービスプロファイル「Site-01-Infra-01」および「Site-01-Infra-02」が作成されていることを確認します。



サービスプロファイルは、割り当てられたサーバプール内のサーバに自動的に関連付けられます。

ストレージ構成パート 2：ブート LUN とイニシエータグループ

ONTAP ブートストレージのセットアップ

igroup を作成します

イニシエータグループ（igroup）を作成するには、次の手順を実行します。

1. クラスタ管理ノードの SSH 接続から次のコマンドを実行します。

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-01 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-01-iqn>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-02 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-02-iqn>
igroup create -vserver Infra-SVM -igroup MGMT-Hosts -protocol iscsi
-ostype vmware -initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```



IQN 情報には、表 1 と表 2 の値を使用します。

2. 作成した 3 つの igroup を表示するには、「igroup show」コマンドを実行します。

ブート LUN を igroup にマッピングします

ブート LUN を igroup にマッピングするには、次の手順を実行します。

1. ストレージクラス管理 SSH 接続から、次のコマンドを実行します。

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- A  
-igroup VM-Host-Infra-01 -lun-id 0  
lun map -vserver Infra-SVM -volume  
esxi_boot -lun VM-Host-Infra- B -igroup VM-Host-Infra-02 -lun-id 0
```

VMware vSphere 6.7U1 導入手順

ここでは、FlexPod Express 構成に VMware ESXi 6.7U1 をインストールする手順について説明します。手順が完了すると、ブートした 2 台の ESXi ホストがプロビジョニングされます。

VMware 環境に ESXi をインストールする方法はいくつかあります。これらの手順では、Cisco UCS Manager に組み込まれている KVM コンソールと仮想メディア機能を使用して、リモートインストールメディアを個々のサーバにマッピングし、それらのブート LUN に接続する方法に焦点を当てています。

ESXi 6.7U1 用の Cisco カスタムイメージをダウンロードします

VMware ESXi カスタムイメージがダウンロードされていない場合は、次の手順を実行してダウンロードを完了します。

1. 次のリンクをクリックします。 [VMware vSphere Hypervisor \(ESXi\) 6.7U1](#)。 ^
2. ユーザ ID とパスワードが必要です "[VMware.com](#)" このソフトウェアをダウンロードします。
3. 「.iso」 ファイルをダウンロードします。

Cisco UCS Manager の略

Cisco UCS IP KVM を使用すると、管理者はリモートメディアを介して OS のインストールを開始できます。IP KVM を実行するには、Cisco UCS 環境にログインする必要があります。

Cisco UCS 環境にログインするには、次の手順を実行します。

1. Web ブラウザを開き、Cisco UCS クラスタアドレスの IP アドレスを入力します。このステップは、Cisco UCS Manager アプリケーションを起動します。
2. HTML の下の [UCS Manager の起動] リンクをクリックして、HTML 5 UCS Manager GUI を起動します。
3. セキュリティ証明書を承認するかどうかを尋ねられたら、必要に応じて受け入れます。
4. プロンプトが表示されたら、ユーザ名として「admin」と入力し、管理パスワードを入力します。
5. Cisco UCS Manager にログインするには、Login をクリックします。
6. メインメニューの左側にある [サーバー] をクリックします。
7. Servers > Service Profiles > root > 'VM-Host-Infra-01' を選択します
8. [VM-Host-Infra-01] を右クリックし [KVM Console] を選択します
9. プロンプトに従って Java ベースの KVM コンソールを起動します。
10. Servers > Service Profiles > root > 'VM-Host-Infra-02' を選択します

11. [VM-Host-Infra-02] を右クリックします。KVM コンソールを選択します。

12. プロンプトに従って Java ベースの KVM コンソールを起動します。

VMware ESXi のインストールをセットアップする

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

OS をインストールするサーバを準備するには、各 ESXi ホストで次の手順を実行します。

1. KVM ウィンドウで、仮想メディアをクリックします。
2. Activate Virtual Devices をクリックします。
3. 暗号化されていない KVM セッションを許可するかどうかを尋ねられたら、必要に応じて受け入れます。
4. [仮想メディア] をクリックし、[CD/DVD のマップ] を選択します。
5. ESXi インストーラの ISO イメージファイルを参照し、開くをクリックします。
6. Map Device をクリックします。
7. KVM タブをクリックして 'サーバの起動を監視します'

◦ ESXi のインストール *

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

VMware ESXi をホストの iSCSI ブート可能 LUN にインストールするには、各ホストで次の手順を実行します。

1. [Boot Server] を選択し、[OK] をクリックして、サーバを起動します。次に、もう一度 [OK] をクリックします。
2. リブート時に、ESXi インストールメディアがマシンで検出されます。表示されたブートメニューから ESXi インストーラを選択します。
3. インストーラのロードが完了したら、Enter キーを押してインストールを続行します。
4. エンドユーザライセンス契約（EULA）を読んで同意します。F11 キーを押して確定し、続行します。
5. ESXi のインストールディスクとして設定していた LUN を選択し、Enter キーを押してインストールを続行します。
6. 適切なキーボードレイアウトを選択し、Enter キーを押します。
7. ルートパスワードを入力して確定し、Enter キーを押します。
8. 選択したディスクが再パーティショニングされることを示す警告が表示されます。F11 キーを押してインストールを続行します。
9. インストールが完了したら、[Virtual Media] タブを選択し、ESXi インストールメディアの横にある P マークをクリアします。はいをクリックします。



ESXi のインストールイメージのマッピングを解除して、サーバがインストーラではなく ESXi でリブートされるようにする必要があります。

10. インストールが完了したら、Enter キーを押してサーバをリブートします。

11. Cisco UCS Manager では、現在のサービスプロファイルを vMedia 以外のサービスプロファイルテンプレ

ートにバインドして、ESXi インストール ISO over HTTP をマウントできないようにします。

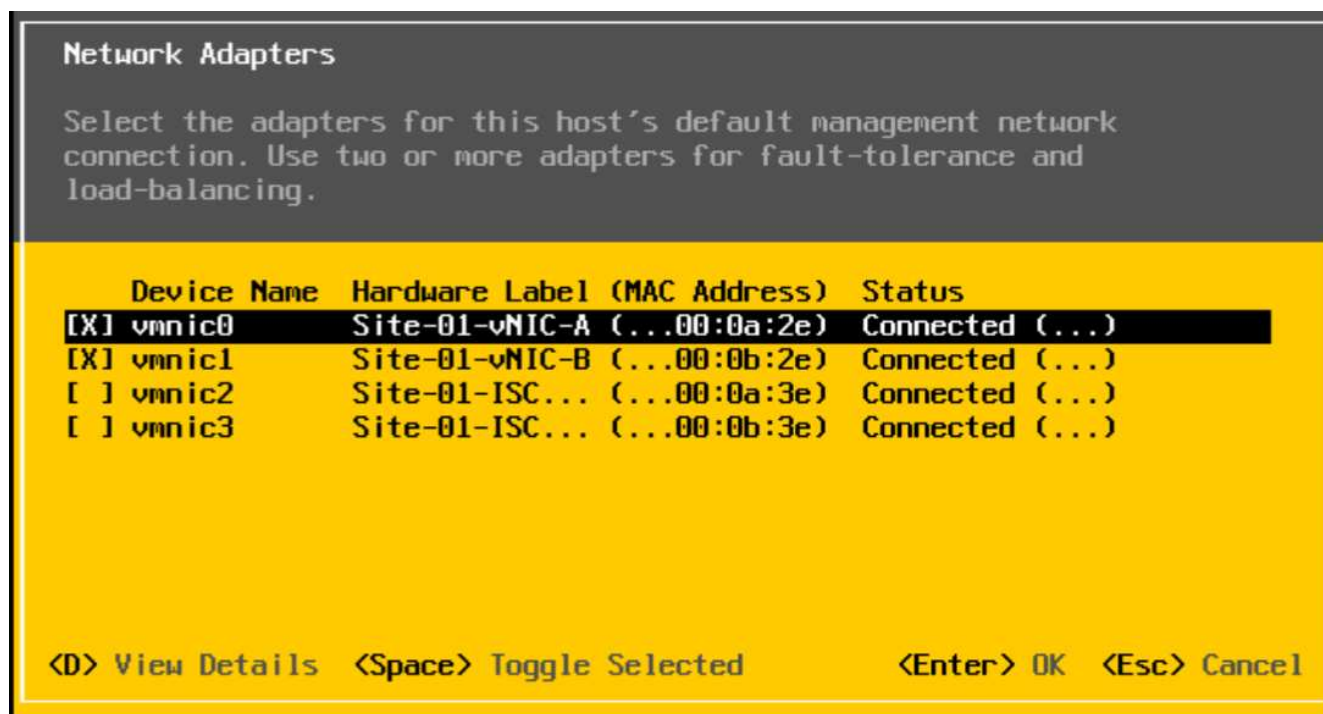
ESXi ホストの管理ネットワークをセットアップします

ホストの管理には、各 VMware ホストに管理ネットワークを追加する必要があります。VMware ホストの管理ネットワークを追加するには、各 ESXi ホストで次の手順を実行します。

ESXi ホスト VM-Host-Infra-01 と VM-Host-Infra-02

各 ESXi ホストから管理ネットワークにアクセスできるように設定するには、次の手順を実行します。

1. サーバーの再起動が完了したら、F2 キーを押してシステムをカスタマイズします。
2. root としてログインし ' 対応するパスワードを入力し 'Enter キーを押してログインします
3. [トラブルシューティングオプション] を選択し、Enter キーを押します。
4. [Enable ESXi Shell] を選択し、Enter キーを押します。
5. SSH を有効にするを選択し、Enter キーを押します。
6. Esc キーを押して、トラブルシューティングオプションメニューを終了します。
7. Configure Management Network （管理ネットワークの設定）オプションを選択し、Enter キーを押します。
8. [ネットワークアダプタ] を選択し、Enter キーを押します。
9. [ハードウェアラベル] フィールドの番号が [デバイス名] フィールドの番号と一致していることを確認します。
10. Enter キーを押します。



11. VLAN （オプション）オプションを選択し、Enter キーを押します。
12. 「<ib-mgmt-vlan-id>」を入力し、Enter キーを押します。

13. IPv4 Configuration (IPv4 設定) を選択し、Enter を押します。
14. スペースバーを使用して、静的 IPv4 アドレスとネットワーク設定を設定オプションを選択します。
15. 最初の ESXi ホストを管理するための IP アドレスを入力します。
16. 最初の ESXi ホストのサブネットマスクを入力します。
17. 最初の ESXi ホストのデフォルトゲートウェイを入力します。
18. Enter キーを押して、IP 設定の変更を確定します。
19. DNS Configuration オプションを選択し、Enter キーを押します。



IP アドレスは手動で割り当てられるため、DNS 情報も手動で入力する必要があります。

20. プライマリ DNS サーバの IP アドレスを入力します。
21. オプション：セカンダリ DNS サーバの IP アドレスを入力します。
22. 最初の ESXi ホストの FQDN を入力します。
23. Enter キーを押して、DNS 設定の変更を確定します。
24. Esc キーを押して、Configure Management Network (管理ネットワークの設定) メニューを終了します。
25. 管理ネットワークのテストを選択して管理ネットワークが正しく設定されていることを確認し、Enter キーを押します。
26. Enter キーを押してテストを実行し、テストが完了したら Enter キーを再度押し、失敗した場合は環境を確認します。
27. Configure Management Network (管理ネットワークの設定) をもう一度選択し、Enter キーを押します。
28. IPv6 設定オプションを選択し、Enter キーを押します。
29. スペースバーを使用して、[Disable IPv6 (restart required)] を選択し、Enter キーを押します。
30. Esc キーを押して、Configure Management Network サブメニューを終了します。
31. Y キーを押して変更を確認し、ESXi ホストをリブートします。

VMware ESXi ホストの VMkernel ポート vmk0 MAC アドレスのリセット (オプション)

ESXi ホスト VM-Host-Infra-01 と VM-Host-Infra-02

デフォルトでは、管理 VMkernel ポート vmk0 の MAC アドレスは、配置されているイーサネットポートの MAC アドレスと同じです。ESXi ホストのブート LUN が異なる MAC アドレスを持つ別のサーバに再マッピングされた場合、vmk0 では ESXi システム設定がリセットされないかぎり、割り当てられた MAC アドレスが保持されるため、MAC アドレスの競合が発生します。vmk0 の MAC アドレスを、VMware が割り当てたランダムな MAC アドレスにリセットするには、次の手順を実行します。

1. ESXi コンソールメニューのメイン画面で、Ctrl+Alt+F1 キーを押して VMware コンソールのコマンドラインインターフェイスにアクセスします。UCSM KVM では、静的マクロのリストに Ctrl-Alt-F1 が表示されます。
2. root としてログインします。
3. 「esxcfg-vmknics -l」と入力して、インタフェース vmk0 の詳細な一覧を表示します。vmk0 は、管理ネ

ットワークのポートグループの一部にする必要があります。vmk0 の IP アドレスおよびネットマスクに注意してください。

4. vmk0 を削除するには、次のコマンドを入力します。

```
esxcfg-vmknic -d "Management Network"
```

5. ランダム MAC アドレスを使用して vmk0 を再び追加するには、次のコマンドを入力します。

```
esxcfg-vmknic -a -i <vmk0-ip> -n <vmk0-netmask> "Management Network".
```

6. vmk0 がランダム MAC アドレスで再び追加されていることを確認します

```
esxcfg-vmknic -l
```

7. コマンド・ライン・インターフェイスからログアウトするには、「exit」と入力します。

8. ESXi コンソールメニューインターフェイスに戻るには、Ctrl+Alt+F2 を押します。

VMware ホストクライアントを使用して **VMware ESXi** ホストにログインします

ESXi ホスト VM-Host-Infra-01

VMware Host Client を使用して VM-Host-Infra-01 ESXi ホストにログインするには、次の手順を実行します。

1. 管理ワークステーションで Web ブラウザを開き 'VM-Host-Infra-01' 管理 IP アドレスに移動します
2. [VMware ホストクライアントを開く] をクリックします。
3. ユーザ名に「root」と入力します。
4. root パスワードを入力します。
5. ログインをクリックして接続します。
6. この手順を繰り返して 'VM-Host-Infra-02' に別のブラウザタブまたはウィンドウでログインします

Cisco Virtual Interface Card (VIC; 仮想インターフェイスカード) 用の **VMware** ドライバのインストール

次の VMware VIC ドライバのオフラインバンドルをダウンロードして、管理ワークステーションに展開します。

- nenic ドライババージョン 1.0.25.0

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

ESXi ホスト VM-Host-Infra-01 および VM-Host-Infra-02 に VMware VIC ドライバをインストールするには、次の手順を実行します。

1. 各ホストクライアントで、Storage (ストレージ) を選択します。
2. datastore1 を右クリックし、Browse を選択します。

3. データストアブラウザで、[アップロード]をクリックします。
4. ダウンロードした VIC ドライバの保存先に移動し、VMW-ESX-6.7.0-nenic-1.0.25.0 -offline_bundle-11271332.zip を選択します。
5. データストアブラウザで、[アップロード]をクリックします。
6. [開く]をクリックして、このファイルを datastore1 にアップロードします。
7. 両方の ESXi ホストにファイルがアップロードされていることを確認してください。
8. 各ホストがメンテナンスモードになっていない場合は、メンテナンスモードにします。
9. 各 ESXi ホストへは、シェル接続または putty 端末から ssh を使用して接続します。
10. root パスワードを使用して root としてログインします。
11. 各ホストで次のコマンドを実行します。

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-  
nenic-1.0.25.0-offline_bundle-11271332.zip  
reboot
```

12. 再起動が完了したら各ホストでホストクライアントにログインし、メンテナンスモードを終了します。

VMkernel ポートおよび仮想スイッチを設定します

ESXi ホスト VM-Host-Infra-01 と VM-Host-Infra-02

ESXi ホスト上の VMkernel ポートおよび仮想スイッチを設定するには、次の手順を実行します。

1. ホストクライアントで、左側の [ネットワーク] を選択します。
2. 中央のペインで、[Virtual switches] タブを選択します。
3. vSwitch0 を選択します。
4. [設定の編集] を選択します
5. MTU を 9000 に変更します。
6. NIC チーミングを展開します。
7. フェイルオーバー順序 (Failover order) セクションで、vmnic1 を選択し、アクティブとしてマーク (Mark active) をクリックします。
8. vmnic1 のステータスがアクティブになっていることを確認します。
9. [保存] をクリックします。
10. 左側の [ネットワーク] を選択します。
11. 中央のペインで、[Virtual switches] タブを選択します。
12. iScsiBootvSwitch を選択します。
13. [設定の編集] を選択します
14. MTU を 9000 に変更します
15. [保存] をクリックします。

16. [VMkernel NICs] タブを選択します。
17. 「vmk1 iScsiBootPG」を選択します。
18. [設定の編集] を選択します
19. MTU を 9000 に変更します。
20. IPv4 設定を展開し、IP アドレスを UCS iSCSI-IP-Pool-A の外部のアドレスに変更します



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

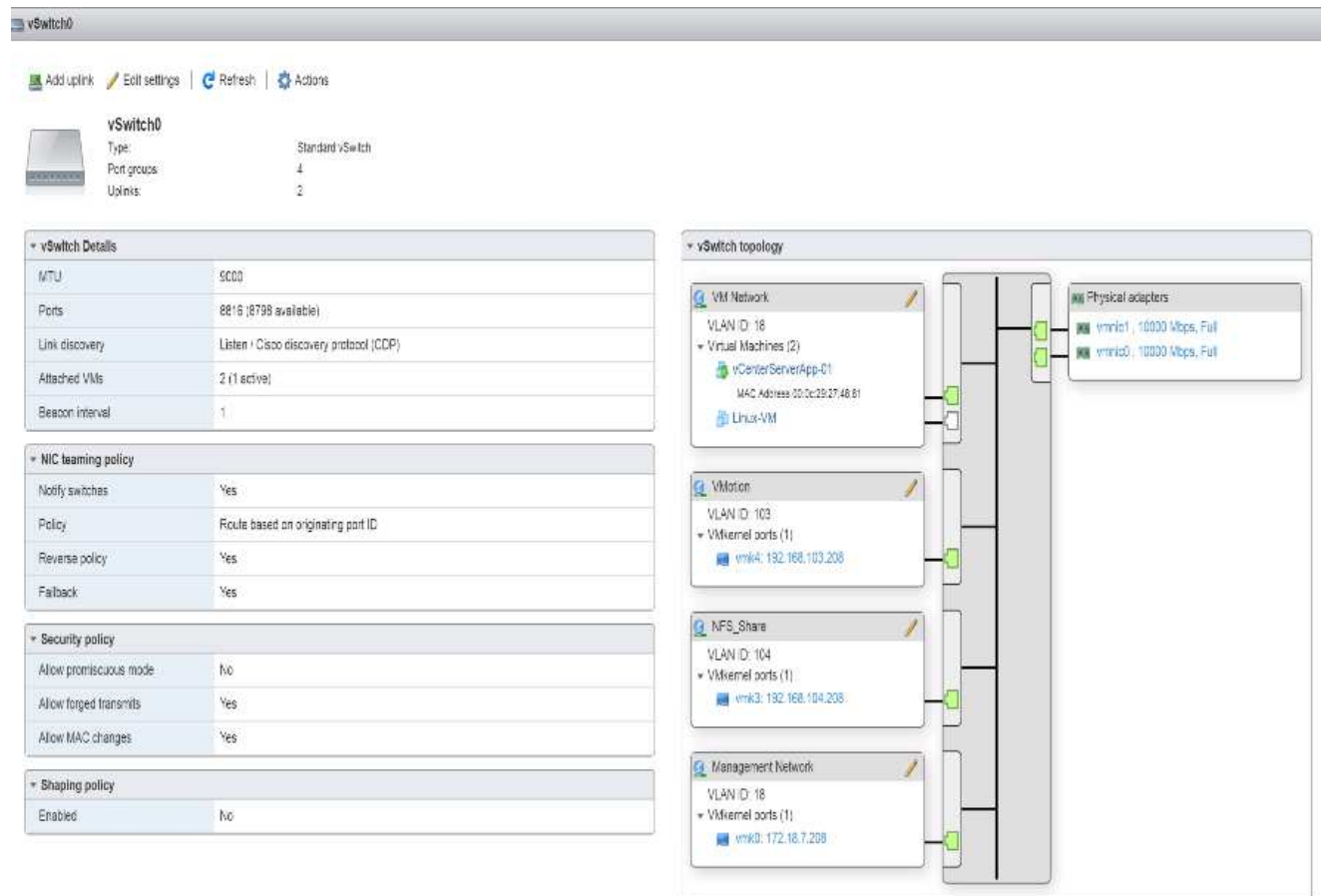
21. [保存] をクリックします。
22. [Virtual switches] タブを選択します。
23. Add standard virtual switch を選択します。
24. vSwitch 名には「iScsiBootvSwitch -B」という名前を付けます。
25. MTU を 9000 に設定します。
26. [Uplink 1] ドロップダウンメニューから [vmnic3] を選択します。
27. 追加をクリックします。
28. 中央のペインで、[VMkernel NICs] タブを選択します。
29. Add VMkernel NIC を選択します
30. 新しいポートグループ名として、iScsiBootPG-B を指定します
31. 仮想スイッチに [iScsiBootvSwitch -B] を選択します。
32. MTU を 9000 に設定します。VLAN ID は入力しないでください。
33. IPv4 設定では Static を選択し、Configuration 内で Address と Subnet Mask を指定するオプションを展開します。



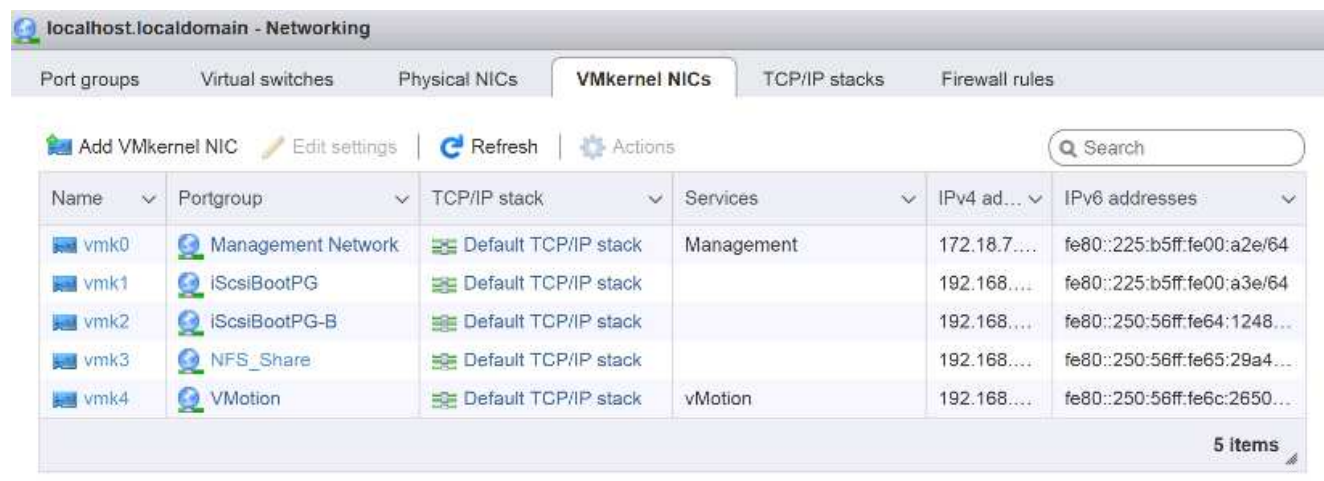
IP アドレスの競合を避けるため、Cisco UCS iSCSI IP プールアドレスを再割り当てする必要がある場合は、iSCSI VMkernel ポートに対して同じサブネット内の異なる IP アドレスを使用することを推奨します。

34. Create をクリックします。
35. 左側で、[ネットワーク] を選択し、[ポートグループ] タブを選択します。
36. 中央のペインで、[VM Network] を右クリックし、[削除] を選択します。
37. Remove をクリックして、ポートグループの削除を完了します。
38. 中央のペインで、Add port group (ポートグループの追加) を選択します。
39. ポートグループに「Management Network」という名前を付け、VLAN ID フィールドに「<ib-mgmt-vlan-id>」と入力して、仮想スイッチ vSwitch0 が選択されていることを確認します。
40. [Add] をクリックして、IB-MGMT ネットワークの編集を終了します。
41. 上部で、[VMkernel NICs] タブを選択します。
42. Add VMkernel NIC をクリックします。

43. 新規ポートグループの場合は、vMotion と入力します。
44. 仮想スイッチの場合は、vSwitch0 を選択します。
45. VLAN ID に「<vMotion-vlan-id>」と入力します。
46. MTU を 9000 に変更します。
47. 静的 IPv4 設定を選択し、IPv4 設定を展開します。
48. ESXi ホストの vMotion IP アドレスとネットマスクを入力します。
49. vMotion スタック TCP/IP スタックを選択します。
50. Services（サービス）で vMotion（vMotion）を選択
51. Create をクリックします。 .
52. Add VMkernel NIC をクリックします。
53. 新しいポートグループの場合は、nfs_Share と入力します。
54. 仮想スイッチの場合は、vSwitch0 を選択します。
55. VLAN ID に「<infra-nfs-vlan-id>」と入力します
56. MTU を 9000 に変更します。
57. 静的 IPv4 設定を選択し、IPv4 設定を展開します。
58. ESXi ホストインフラの NFS IP アドレスとネットマスクを入力します。
59. サービスは選択しないでください。
60. Create をクリックします。 .
61. 仮想スイッチタブを選択して、vSwitch0 を選択します。vSwitch0 VMkernel NIC のプロパティは、次の例のように設定します。



62. [VMkernel NICs] タブを選択して、設定済みの仮想アダプタを確認します。次の例のようなアダプタが表示されます。



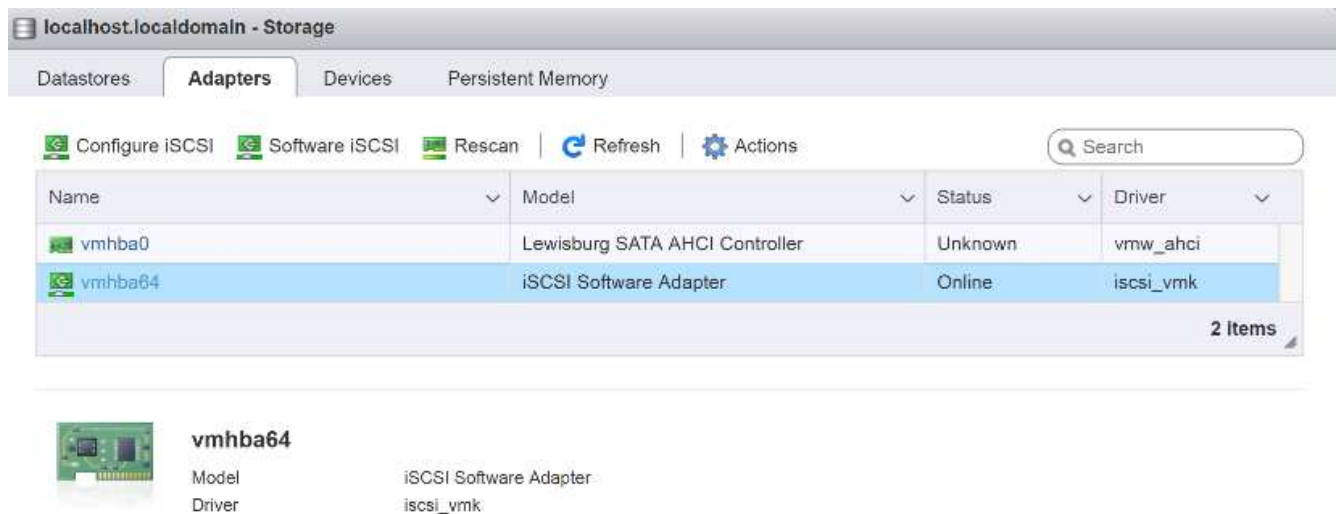
iSCSI マルチパスをセットアップします

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

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

1. 各ホストクライアントで、左側の [ストレージ] を選択します。

2. 中央のペインで、[アダプタ] をクリックします。
3. iSCSI ソフトウェアアダプタを選択し、Configure iSCSI （iSCSI の設定）をクリックします。



4. [動的ターゲット] で、[動的ターゲットの追加] をクリックします。
5. IP アドレスに「iscsi_dlif01a」と入力します。
6. これらの IP アドレスの入力を繰り返します：'iSCSI_lif01b'iSCSI_lif02a'iSCSI_lif02b'
7. [Save Configuration] をクリックします。

Configure iSCSI - vmhba64

iSCSI enabled: ☐ Disabled ☒ Enabled

Name & alias: iqn.1992-08.com.cisco:ucs-host:3

CHAP authentication: Do not use CHAP

Mutual CHAP authentication: Do not use CHAP

Advanced settings: Click to expand

Network port bindings:

Add port binding Remove port binding

VMkernel NIC Port group IPv4 address

No port bindings

Static targets:

Add static target Remove static target Edit settings Search

Target	Address	Port
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.124.3	3260
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.124.1	3260
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.125.3	3260
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.125.1	3260

Dynamic targets:

Add dynamic target Remove dynamic target Edit settings Search

Address	Port
192.168.124.1	3260
192.168.125.1	3260
192.168.125.3	3260

Save configuration Cancel

「iscsi_lif」の IP アドレスをすべて取得するには、NetApp ストレージ・クラスタ管理インターフェイスにログインし、「network interface show」コマンドを実行します。



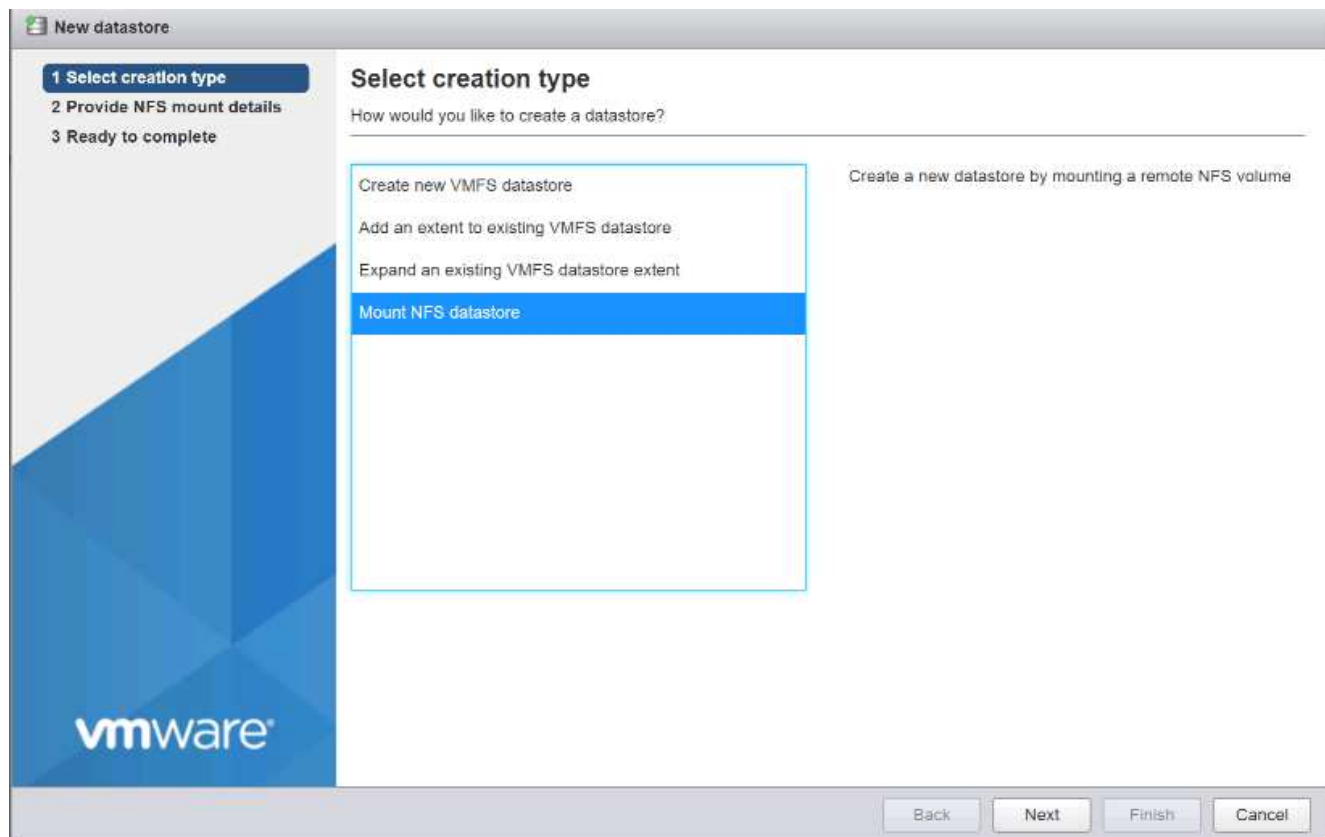
ホストが自動的にストレージアダプタとターゲットを再スキャンし、静的ターゲットに追加します。

必要なデータストアをマウント

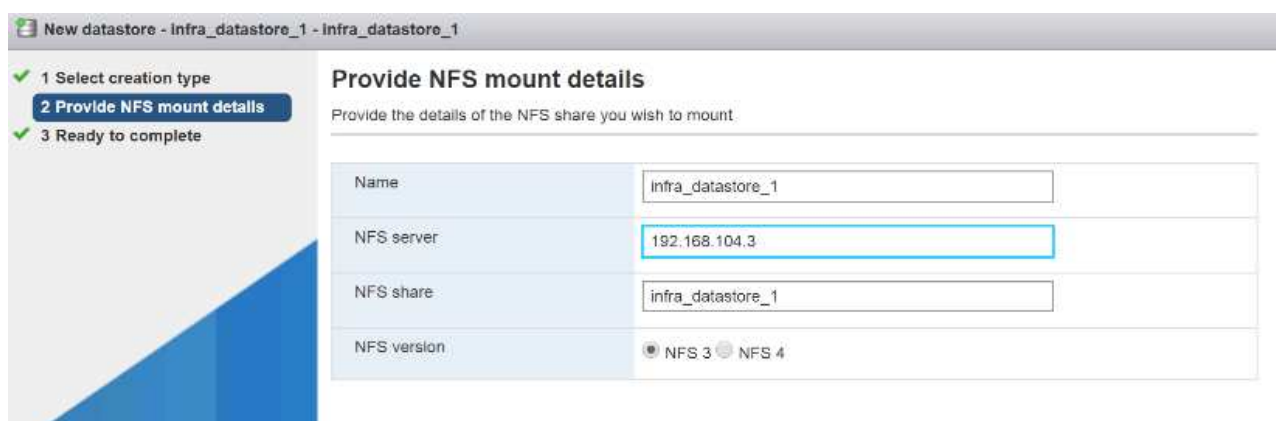
ESXi は VM-Host-Infra-01 と VM-Host-Infra-02 をホストします

必要なデータストアをマウントするには、各 ESXi ホストで次の手順を実行します。

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

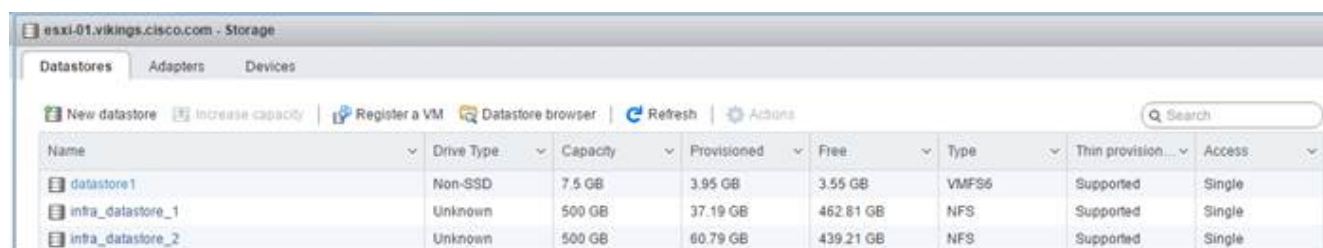


5. [Provide NFS Mount Details] ページで、次の手順を実行します。
 - a. データストア名として「infra_datastore_1」と入力します。
 - b. NFS サーバの「NFS_lif01_a」 LIF の IP アドレスを入力します。
 - c. NFS 共有の場合は '/infra_datastore_1' と入力します
 - d. NFS のバージョンは NFS 3 のままにします。
 - e. 次へをクリックします。



6. 完了をクリックします。これで、データストアがデータストアのリストに表示されます。
7. 中央のペインで、New Datastore（新規データストア）を選択して新しいデータストアを追加します。
8. New Datastore（新規データストア）ダイアログボックスで、Mount NFS Datastore（NFS データストアのマウント）を選択し、Next（次へ）をクリック

9. [Provide NFS Mount Details] ページで、次の手順を実行します。
 - a. データストア名として「infra_datastore_2」と入力します。
 - b. NFS サーバの「nfs_lif02_a」 LIF の IP アドレスを入力します。
 - c. NFS 共有の場合は '/infra_datastore_2' と入力します
 - d. NFS のバージョンは NFS 3 のままにします。
 - e. 次へをクリックします。
10. 完了をクリックします。これで、データストアがデータストアのリストに表示されます。



Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provision...	Access
datastore1	Non-SSD	7.5 GB	3.95 GB	3.55 GB	VMFS6	Supported	Single
infra_datastore_1	Unknown	500 GB	37.19 GB	462.81 GB	NFS	Supported	Single
infra_datastore_2	Unknown	500 GB	60.79 GB	439.21 GB	NFS	Supported	Single

11. 両方の ESXi ホストに両方のデータストアをマウントします。

ESXi ホストで NTP を設定

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

ESXi ホストで NTP を設定するには、各ホストで次の手順を実行します。

1. ホストクライアントから、左側の [管理] を選択します。
2. 中央のウィンドウ枠で、[時刻と日付] タブを選択します。
3. 設定の編集をクリックします。
4. [ネットワークタイムプロトコルを使用する (NTP クライアントを有効にする)] が選択されていることを確認します。
5. ドロップダウンメニューを使用して、Start (開始) および Stop with Host (ホストで停止) を選択します。
6. 2 つの Nexus スイッチの NTP アドレスを、カンマで区切って NTP サーバボックスに入力します。

Edit time configuration

Specify how the date and time of this host should be set.

☐ Manually configure the date and time on this host

10/13/2016 4:09 PM

☒ Use Network Time Protocol (enable NTP client)

NTP service startup policy: Start and stop with host

NTP servers: 10.1.156.4,10.1.156.5

Separate servers with commas, e.g. 10.31.21.2, fe00::2800

Save Cancel

7. Save をクリックして、設定の変更を保存します。
8. Actions > NTP service > Start の順に選択します。
9. NTP サービスが実行中で、クロックが正しい時刻に設定されたことを確認します



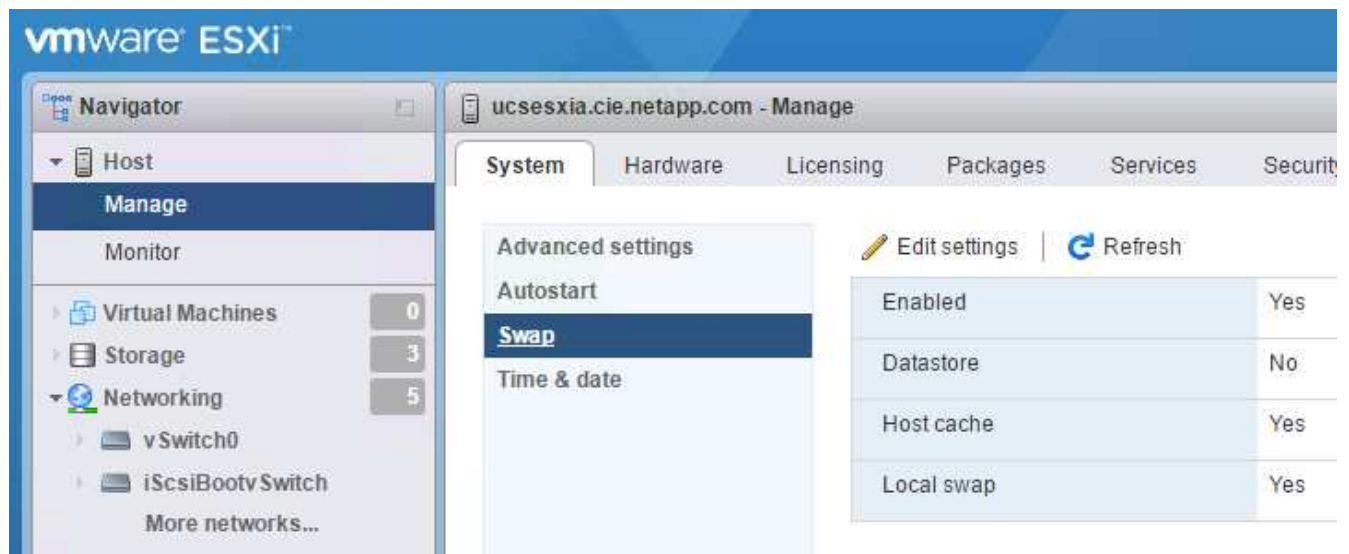
NTP サーバの時間はホストの時間とは多少異なる場合があります。

ESXi ホストのスワップを設定

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

ESXi ホストでホストのスワップを設定するには、各ホストで次の手順を実行します。

1. 左側のナビゲーションペインで、[管理] をクリックします。右側のペインで System （システム）を選択し、Swap （交換）をクリックします。



2. 設定の編集をクリックします。データストアのオプションから 'infra_swap' を選択します



3. [保存] をクリックします .

NetApp NFS Plug-in 1.1.2 for VMware VAAI をインストールします

NetApp NFS Plug-in 1 をインストールします。1.2 VMware VAAI の場合は、次の手順を実行します。

1. NetApp NFS Plug-in for VMware VAAI をダウンロードします。
 - a. にアクセスします ["ネットアップのソフトウェアダウンロードページ"](#)。
 - b. 下にスクロールして、 NetApp NFS Plug-in for VMware VAAI をクリックします。
 - c. ESXi プラットフォームを選択します。
 - d. 最新のプラグインのオフラインバンドル（.zip）またはオンラインバンドル（.vib）をダウンロードします。
2. NetApp NFS Plug-in for VMware VAAI ONTAP は IMT 9.5 への対応が保留中であり、相互運用性の詳細は NetApp IMT に近日中に公開されます。
3. ESX CLI を使用して、 ESXi ホストにプラグインをインストールします。

4. ESXi ホストをリブートします。

VMware vCenter Server 6.7 をインストールする

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



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

VMware vCenter Server Appliance をインストールする

vCSA をインストールするには、次の手順を実行します。

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

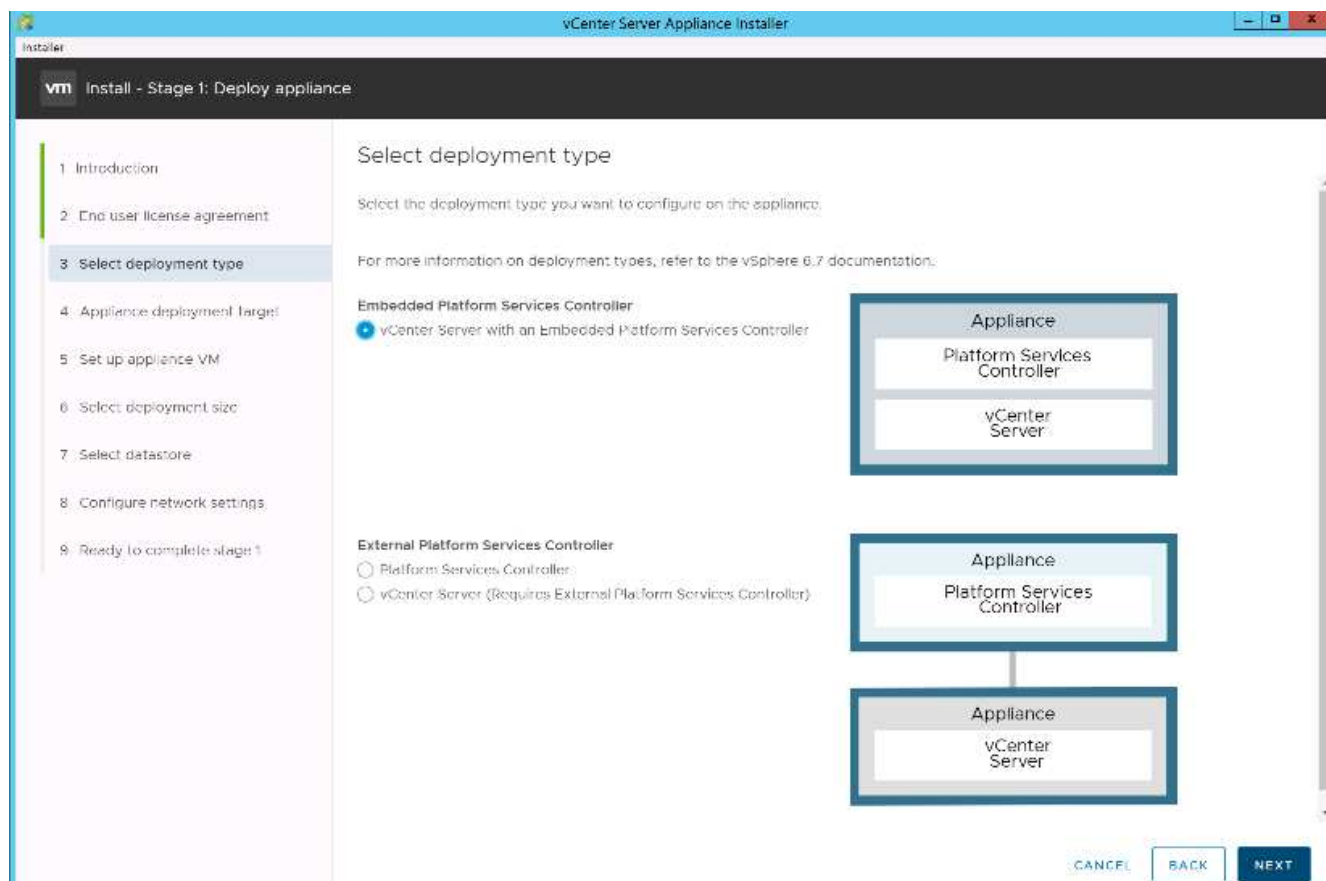


2. vCSA を VMware サイトからダウンロードします。



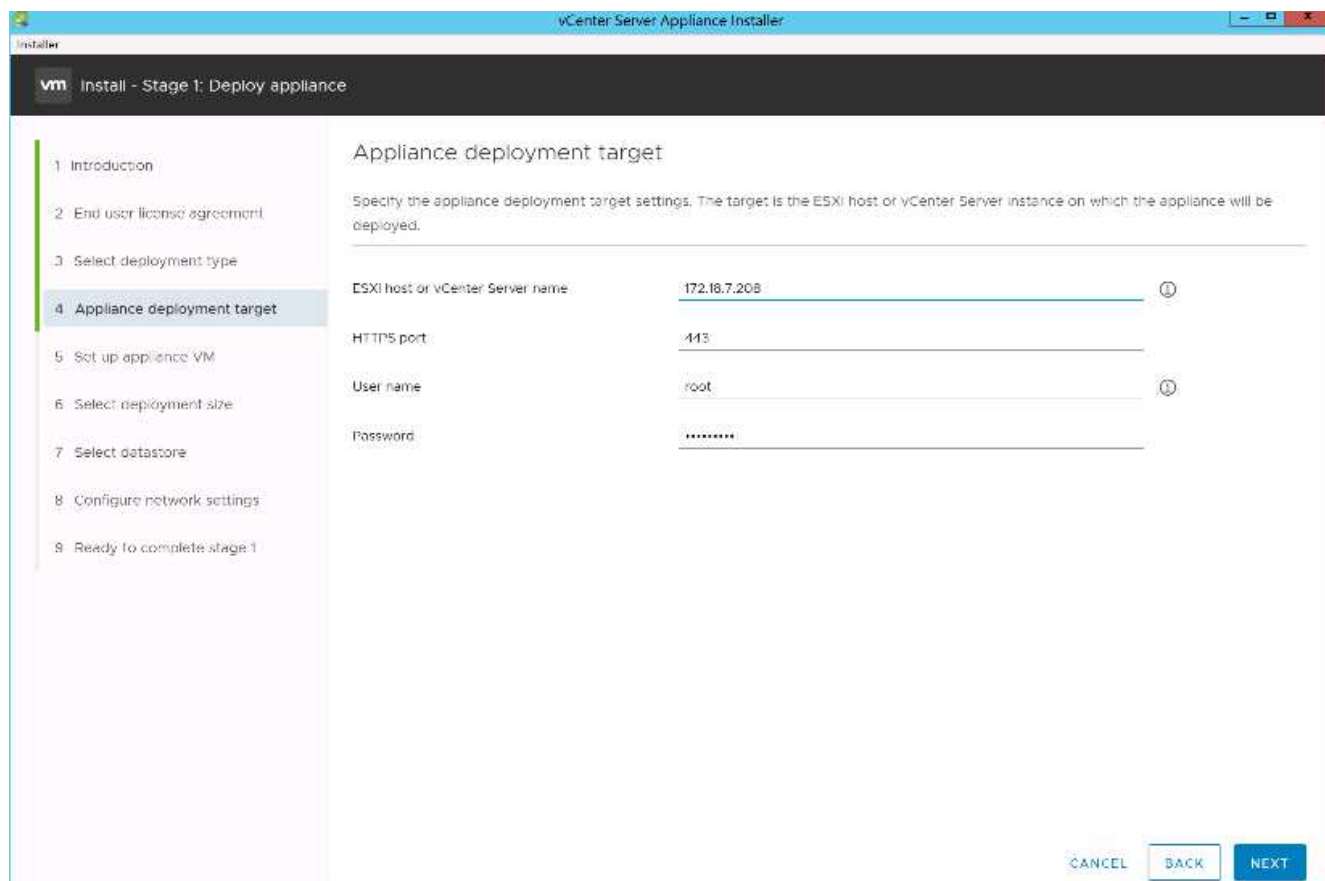
インストール可能な Microsoft Windows vCenter Server がサポートされますが、VMware では新しい導入に vCSA を推奨します。

3. ISO イメージをマウントします。
4. 「VCSA -ui-sinstaller」 > 「win32」ディレクトリに移動します。「installer.exe」をダブルクリックします。
5. [インストール] をクリックします
6. [はじめに] ページで [次へ] をクリックします。
7. EULA に同意します。
8. 展開タイプとして、Embedded Platform Services Controller を選択します。

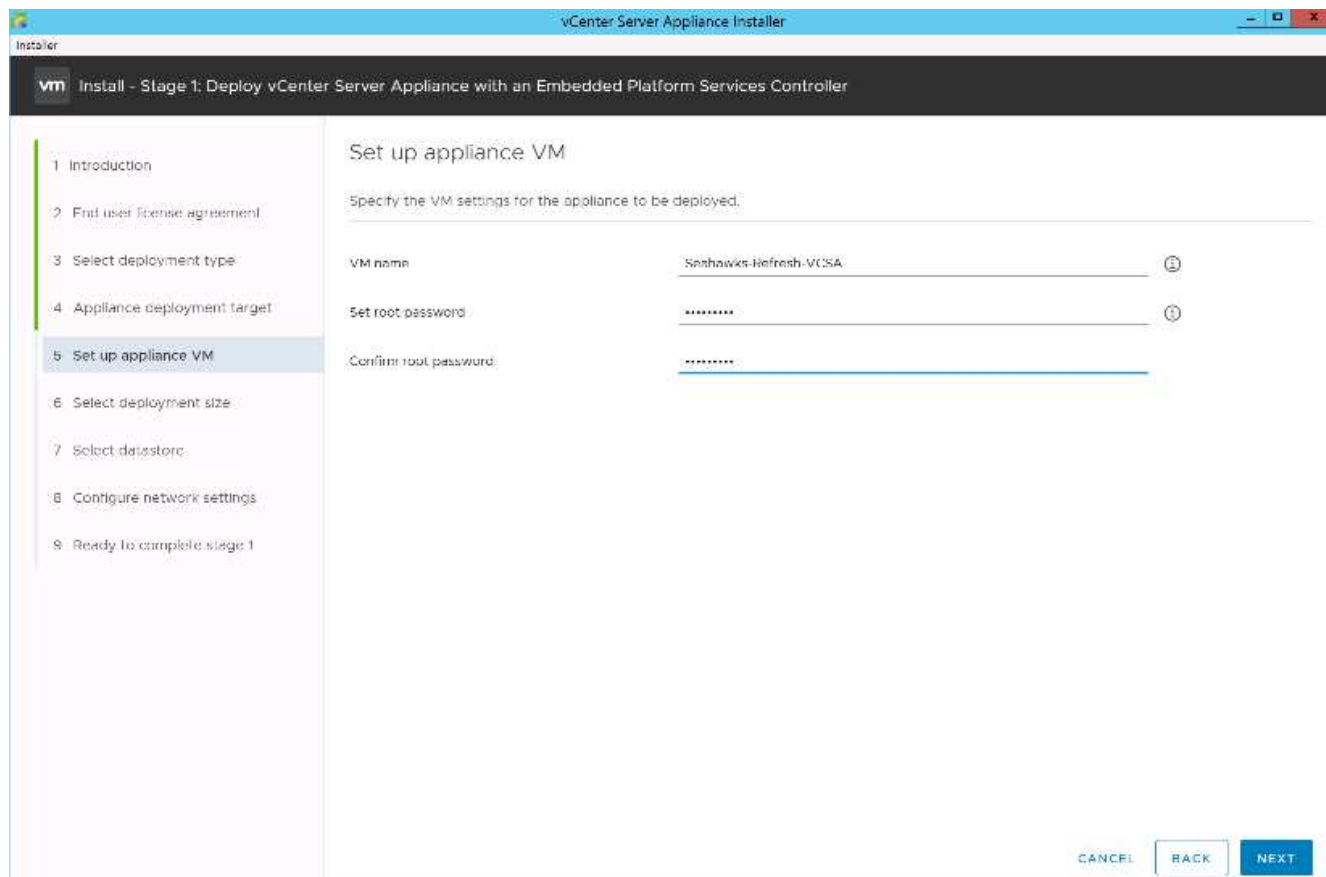


必要に応じて、FlexPod Express 解決策の一部として、外部プラットフォームサービスコントローラの導入もサポートされます。

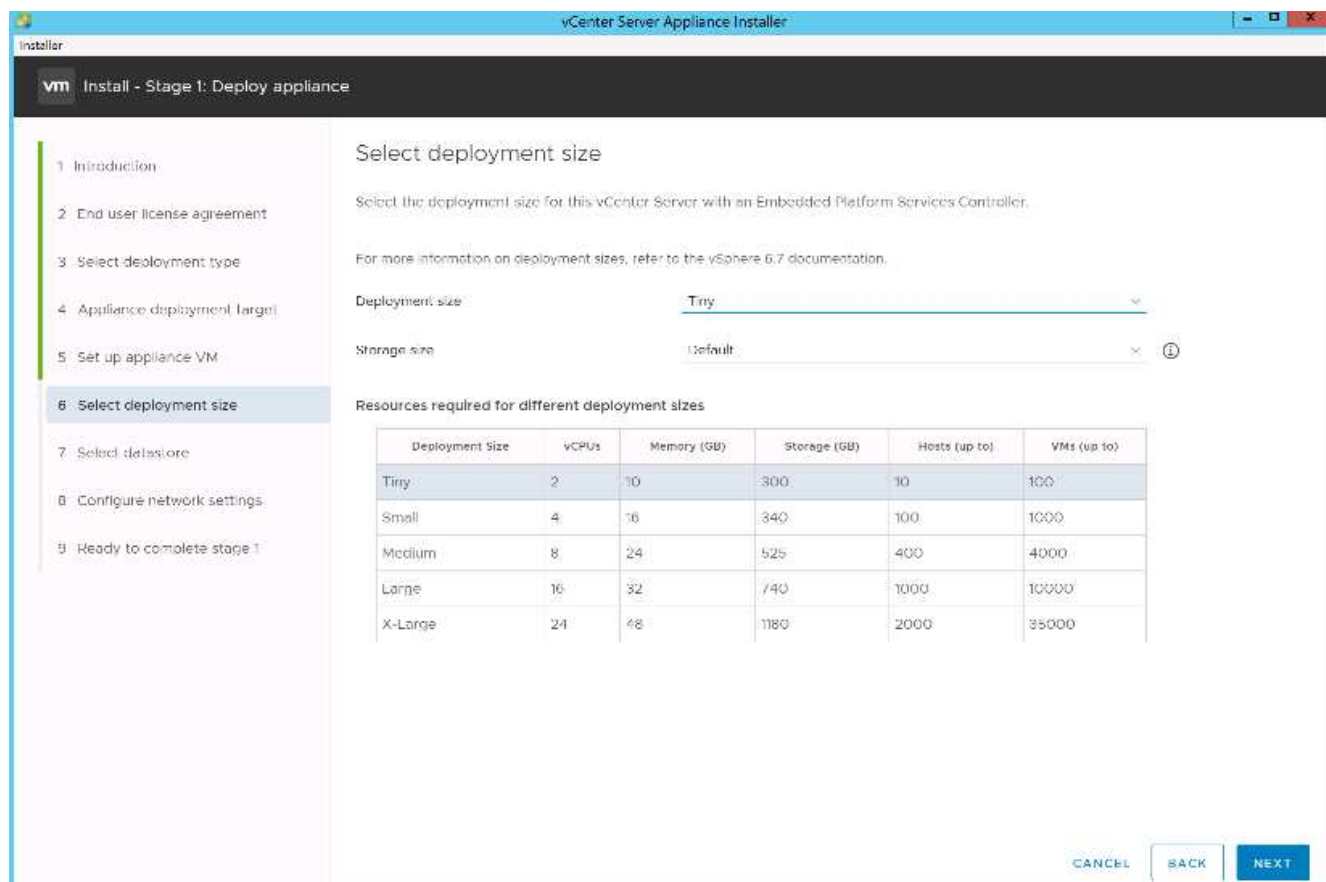
9. アプライアンス導入ターゲットページで、導入した ESXi ホストの IP アドレス、ルートユーザ名、および root パスワードを入力します。次へをクリックします。



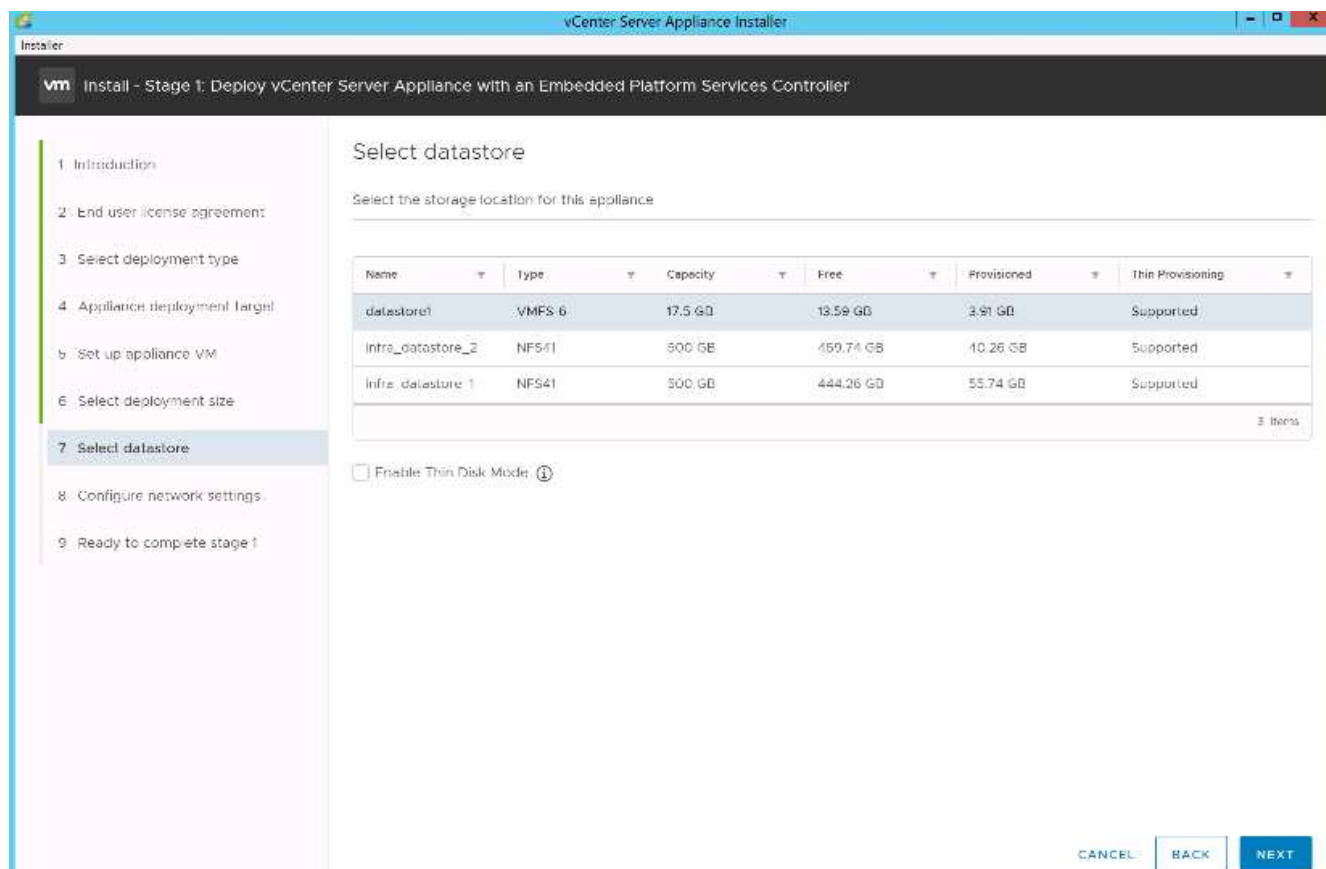
10. vCSA に VM 名および vCSA に使用するルートパスワードとして VCSA を入力して、アプライアンス VM を設定します。次へをクリックします。



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

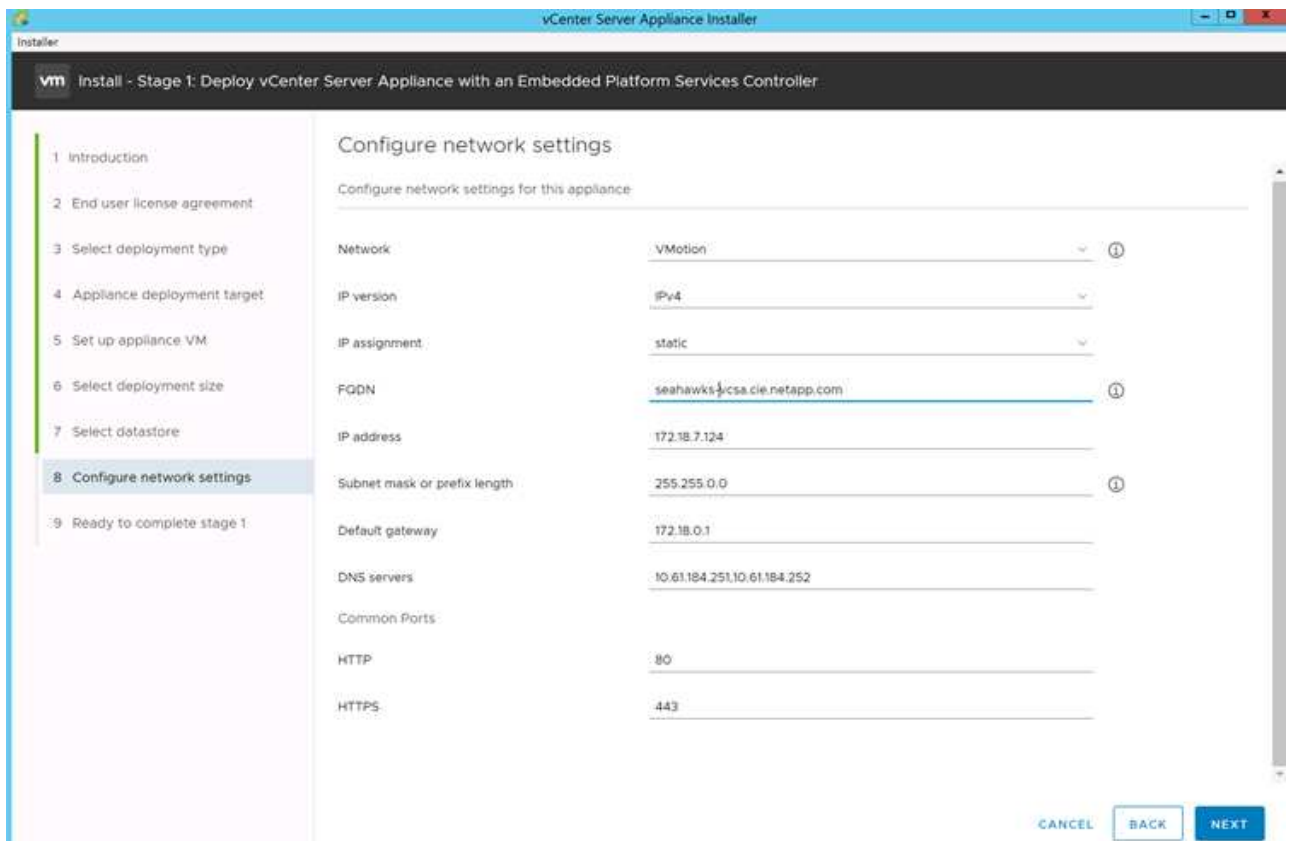


12. 「infra_datastore_1」 データストアを選択します。次へをクリックします。



13. [Configure Network Settings] ページで次の情報を入力し、[Next] をクリックします。

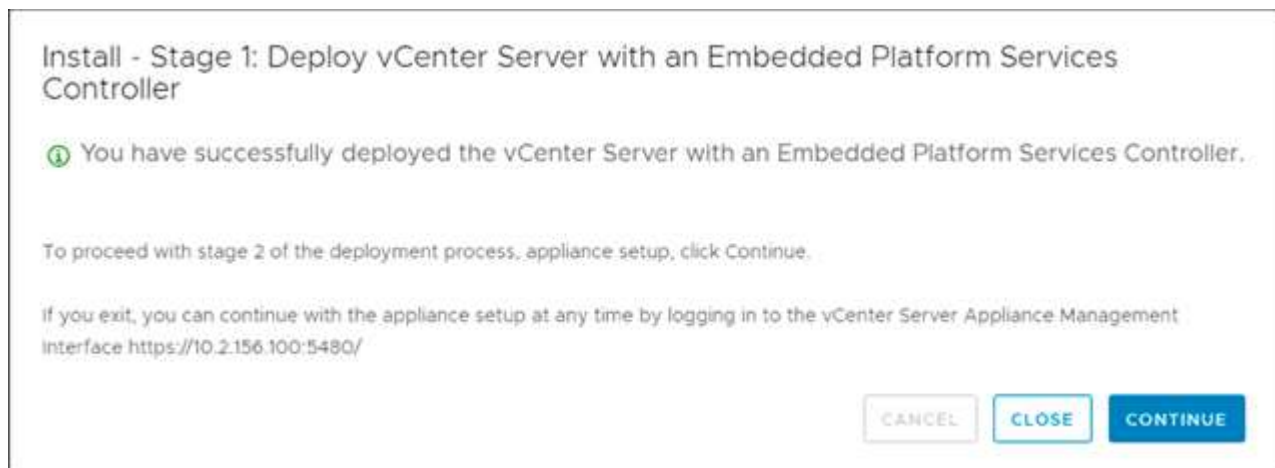
- ネットワークとして MGMT-Network を選択します。
- vCSA に使用する FQDN または IP を入力します。
- 使用する IP アドレスを入力します。
- 使用するサブネットマスクを入力します。
- デフォルトゲートウェイを入力します。
- DNS サーバを入力します。



14. 「ステージ 1 を完了する準備ができました」 ページで、入力した設定が正しいことを確認します。完了をクリックします。

vCSA がインストールされます。このプロセスには数分かかります。

15. ステージ 1 が完了すると、完了したことを示すメッセージが表示されます。「続行」をクリックしてステージ 2 の設定を開始します。



16. 「ステージ 2 の紹介」 ページで、「次へ」をクリックします。
17. NTP サーバのアドレスとして「\<var_ntp_id>>」と入力します。複数の NTP IP アドレスを入力できます。

vCenter Server の高可用性機能を使用する場合は、SSH アクセスが有効になっていることを確認してください。

18. SSO ドメイン名、パスワード、およびサイト名を設定します。次へをクリックします。

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

19. 必要に応じて、VMware カスタマーエクスペリエンスプログラムに参加します。次へをクリックします。

20. 設定の概要を確認します。[完了] をクリックするか、[戻る] ボタンを使用して設定を編集します。

21. インストールの開始後に、インストールを一時停止または終了できないことを示すメッセージが表示されます。[OK] をクリックして続行します。

アプライアンスの設定が続行されます。これには数分かかります。

セットアップが正常に完了したことを示すメッセージが表示されます。



インストーラが vCenter Server にアクセスするために提供するリンクはクリック可能です。

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

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

1. <https://<FQDN> /vsphere-client/> または IP of vCenter >> /vsphere-client/ に移動します。
2. vSphere Client の起動をクリックします。
3. vCSA のセットアッププロセスで入力したユーザ名 administrator@vsphere.local と SSO パスワードを使用してログインします。
4. vCenter 名を右クリックし、New Datacenter を選択します。
5. データセンターの名前を入力し、[OK] をクリックします。
 - vSphere クラスタを作成 *

vSphere クラスタを作成するには、次の手順を実行します。

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

Name	Express
Location	Flexpod_SeaHawks
DRS	<input checked="" type="checkbox"/>
vSphere HA	<input checked="" type="checkbox"/>
vSAN	<input type="checkbox"/>

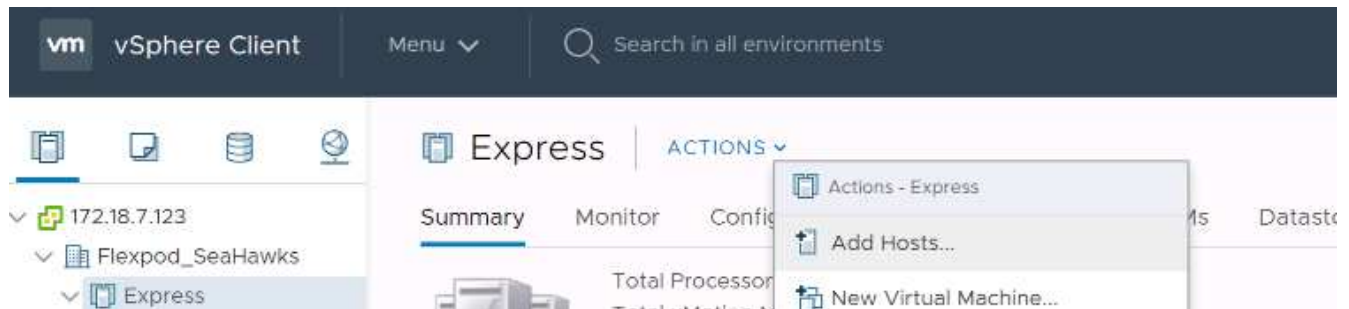
These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

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. クラスタの Actions （アクション）メニューで Add Host （ホストの追加）を選択します。



2. ESXi ホストをクラスタに追加するには、次の手順を実行します。
 - a. ホストの IP または FQDN を入力します。次へをクリックします。
 - b. root ユーザ名とパスワードを入力します。次へをクリックします。
 - c. Yes をクリックして、ホストの証明書を VMware 証明書サーバによって署名された証明書に置き換えます。
 - d. [Host Summary] ページで [Next] をクリックします。
 - e. 緑の + アイコンをクリックして、vSphere ホストにライセンスを追加します。



この手順は、必要に応じてあとで実行できます。

- f. [次へ] をクリックして、ロックダウンモードを無効のままに

- g. [VM の場所] ページで [次へ] をクリックします。
 - h. [Ready to Complete] ページを確認します。[戻る] ボタンを使用して変更を行うか、[完了] を選択します。
3. Cisco UCS ホスト B に対して手順 1 と 2 を繰り返します

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

ESXi ホストにコアダンプを設定します

iSCSI ブートホスト用の ESXi ダンプコレクタのセットアップ

VMware iSCSI ソフトウェアイニシエータを使用して iSCSI でブートされた ESXi ホストは、vCenter の一部である ESXi ダンプコレクタにコアダンプを実行するように設定する必要があります。ダンプコレクタは、vCenter Appliance ではデフォルトで有効になっていません。この手順は、vCenter の導入セクションの最後で実行する必要があります。ESXi Dump Collector をセットアップするには、次の手順を実行します。

1. vSphere Web Client に `mailto : administrator@vsphere.local` | `[administrator@vsphere.local]` としてログインし、[ホーム] を選択します。
2. 中央のペインで、システム構成をクリックします。
3. 左側のペインで、[サービス] を選択します。
4. [Services] で、[VMware vSphere ESXi Dump Collector] をクリックします。
5. 中央のペインで、緑の開始アイコンをクリックしてサービスを開始します。
6. [アクション] メニューの [スタートアップの種類の編集] をクリックします。
7. 自動を選択します。
8. [OK] をクリックします。
9. SSH を使用して、各 ESXi ホストに root として接続します。
10. 次のコマンドを実行します。

```
esxcli system coredump network set -v vmk0 -j <vcenter-ip>
esxcli system coredump network set -e true
esxcli system coredump network check
```

最後のコマンドを実行すると '構成された netdump サーバが動作していることを確認しました' というメッセージが表示されます



FlexPod Express にホストを追加する場合は、このプロセスを完了する必要があります。

まとめ

FlexPod Express は、業界をリードするコンポーネントを使用した検証済みの設計を提供することで、シンプルで効果的な解決策を実現します。FlexPod Express は、コンポーネントを追加することで拡張できるため、特定のビジネスニーズに合わせてカスタマ

イズできます。FlexPod Express は、中小規模の企業や、専用のソリューションを必要とする ROBO などの企業を念頭に置いて設計されました。

追加情報

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

- NVA-1130-design : FlexPod Express with VMware vSphere 6.7U1 and NetApp AFF A220 with Direct-Attached IP = Based Storage NVA Design

["https://www.netapp.com/us/media/nva-1130-design.pdf"](https://www.netapp.com/us/media/nva-1130-design.pdf)

- AFF システムと FAS システムのドキュメントセンター

["http://docs.netapp.com/platstor/index.jsp"](http://docs.netapp.com/platstor/index.jsp)

- ONTAP 9 ドキュメンテーション・センター

["http://docs.netapp.com/ontap-9/index.jsp"](http://docs.netapp.com/ontap-9/index.jsp)

- ネットアップの製品マニュアル

["https://docs.netapp.com"](https://docs.netapp.com)

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。