VMware ESXi 向け Cisco HyperFlex System リリース 4.5 インストール ガイド

初版：2021 年 1 月 6 日

最終更新：2022 年 9 月 26 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

通信、サービス、偏向のない言語、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

Cisco バグ検索ツール

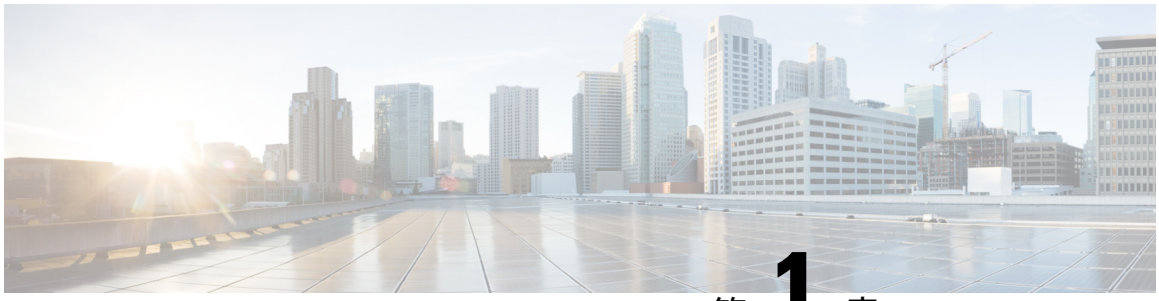
Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

偏向のない言語

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイ

通信、サービス、偏向のない言語、およびその他の情報

スにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



第 1 章

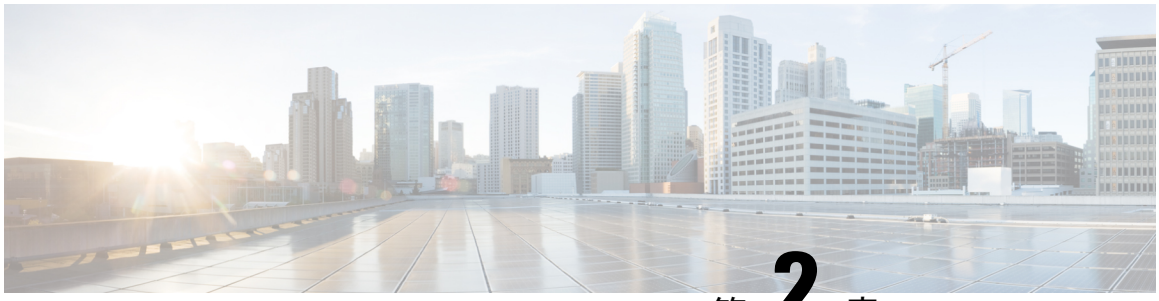
新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

特長	説明	追加日	参照先
VMware ESXi 向け Cisco HyperFlex System リリース 4.5 インストール ガイド	4.5 ガイドの最初のリリース。	2021 年 1 月 5 日	このマニュアル

新機能および変更された機能に関する情報



第 2 章

概要

この章では、Cisco HyperFlex System のコンポーネントの概要を示します。

Cisco HyperFlex HX シリーズ システム

Cisco HyperFlex HX シリーズ システムは、完全内包型の仮想サーバ プラットフォームを通じて、コンピューティング、ストレージ、ネットワークの 3 つのレイヤと強力な Cisco HX Data Platform ソフトウェア ツールを結合し、シングル ポイント接続による簡素化された管理を実現します。Cisco HyperFlex HX-Series System は、単一の UCS 管理ドメインに HX ノードを追加することによってスケールアウトするように設計されたモジュラ システムです。ハイパーコンバージド システムはユーザのワークロード ニーズに基づいて統一されたリソースのプールを提供します。

Cisco HyperFlex HX シリーズ システムのコンポーネント

- **Cisco HX シリーズ サーバー**：次のいずれかのサーバーを使用して Cisco HyperFlex システムを設定できます。
  - コンバージド ノード - **オールフラッシュ**：Cisco HyperFlex HXAF240c M5、HXAF220c M5、HXAF240c M4、および HXAF220c M4。
  - コンバージド ノード - **ハイブリッド**：Cisco HyperFlex HX240c M5、HX220c M5、HX240c M4、および HX220c M4。
  - コンピューティングのみ：Cisco B200 M3/M4、B260 M4、B420 M4、B460 M4、B480 M5、C240 M3/M4、C220 M3/M4、C480 M5、C460 M4、B200 M5、C220 M5 および C240 M5。

- **Cisco HX Data Platform**：HX Data Platform は次のコンポーネントで構成されています。
  - **Cisco HX Data Platform インストーラ**：ストレージ クラスタに接続されているサーバにこのインストーラをダウンロードします。HX Data Platform インストーラは、Cisco UCS Manager 内のサービス プロファイルとポリシーを設定し、コントローラ VM を展開し、ソフトウェアをインストールし、ストレージ クラスタを作成し、VMware vCenter プラグインを更新します。
  - **Storage Controller VM**：HX Data Platform インストーラ を使用して、管理対象のストレージ クラスタ内の各コンバージド ノードにストレージ コントローラ VM をインストールします。
  - **Cisco HX Data Platform プラグイン**：この統合 VMware vSphere インターフェイスは、ストレージ クラスタ内のストレージをモニタおよび管理します。

- **Cisco UCS ファブリック インターコネクト（FI）**

  ファブリック インターコネクトは、接続されている Cisco HX-Series Server にネットワーク接続機能と管理機能の両方を提供します。

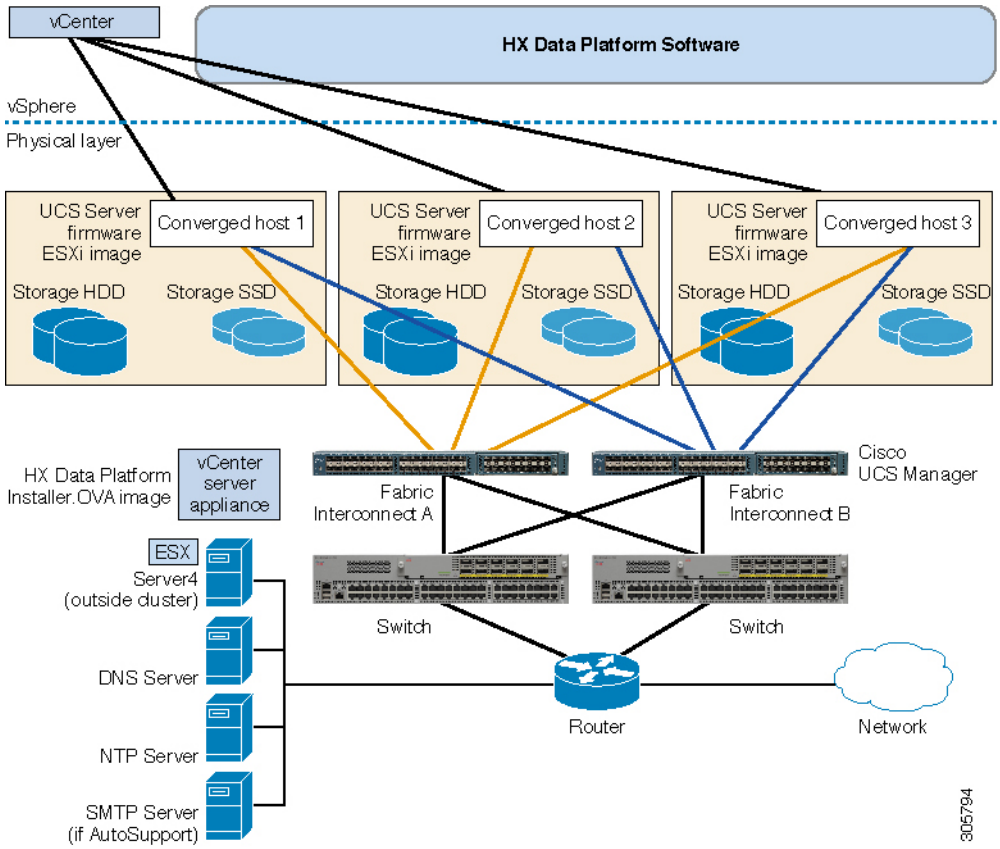
  Cisco HyperFlex System の一部として購入されて展開された FI は、このドキュメントでは**HX FI ドメイン**とも呼ばれます。サポートされているファブリック インターコネクトは次のとおりです。

  - Cisco UCS 6200 シリーズ Fabric Interconnect
  - Cisco UCS 6300 シリーズ Fabric Interconnect
  - Cisco UCS 6400 シリーズ ファブリック インターコネクト

- **Cisco Nexus スイッチ**

  Cisco Nexus スイッチによって、高密度で設定可能なポートが提供され、柔軟なアクセスの展開と移行を実現できます。

図 *1 : Cisco HyperFlex HX* シリーズ システムのコンポーネント



Cisco HyperFlex HX シリーズ システムの設定オプション

Cisco HyperFlex HX シリーズ システムは、環境内でストレージおよびコンピューティング機能を拡張するための柔軟でスケーラブルなオプションを提供します。Cisco HyperFlex システムにストレージ機能を追加するには、Cisco HyperFlex Server を追加するだけです。

（注） **HX クラスタ** は HX シリーズ サーバーのグループです。クラスタ内の各 HX シリーズ サーバは、HX ノードまたはホストと呼ばれます。

HX クラスタはさまざまな方法で構成できます。次の図に、一般的な構成例を示します。最新の互換性とスケーラビリティの詳細については、『Cisco HyperFlex推奨ソフトウェアリリースおよび要件ガイド』の Cisco HX Data Platform Compatibility and Scalability Details - 4.5(x) Releases の章をhttps://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/release-guidelines-and-support-timeline/b-recommended-hx-data-platform-sw-releases/m-recommended-releases.html参照してください。

図 *2 : Cisco HyperFlex* ハイブリッド *M5* 設定

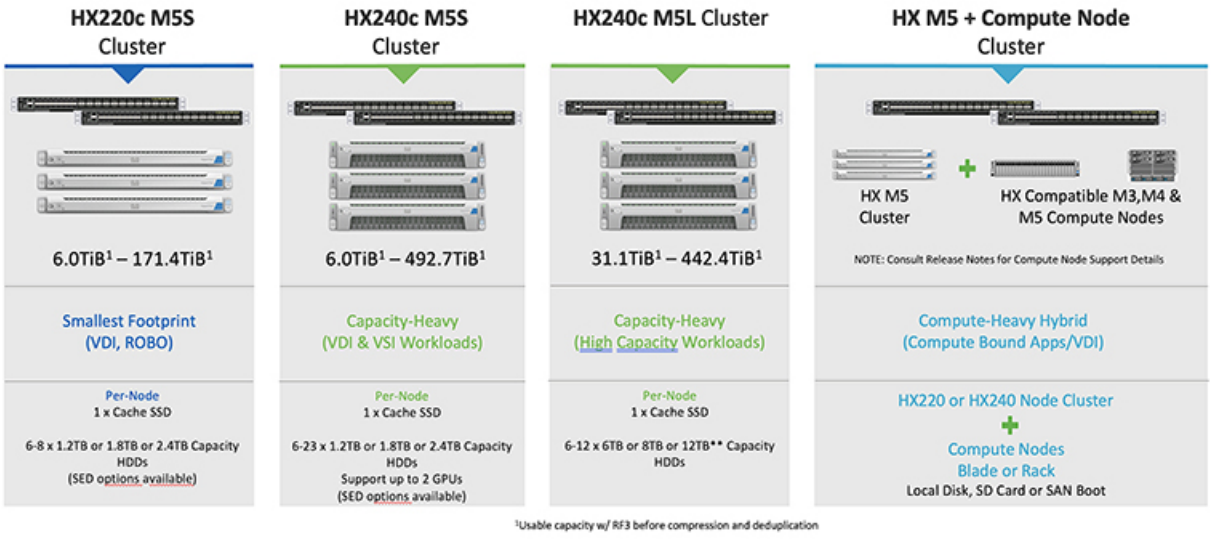


図 *3 : Cisco HyperFlex* ハイブリッド *M4* 設定

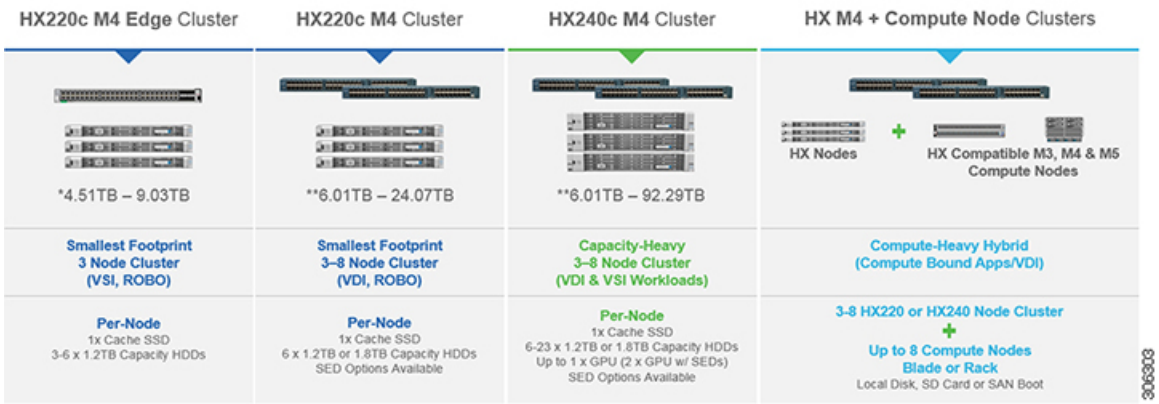


図 *4 : Cisco HyperFlex* オール フラッシュ *M5* 設定

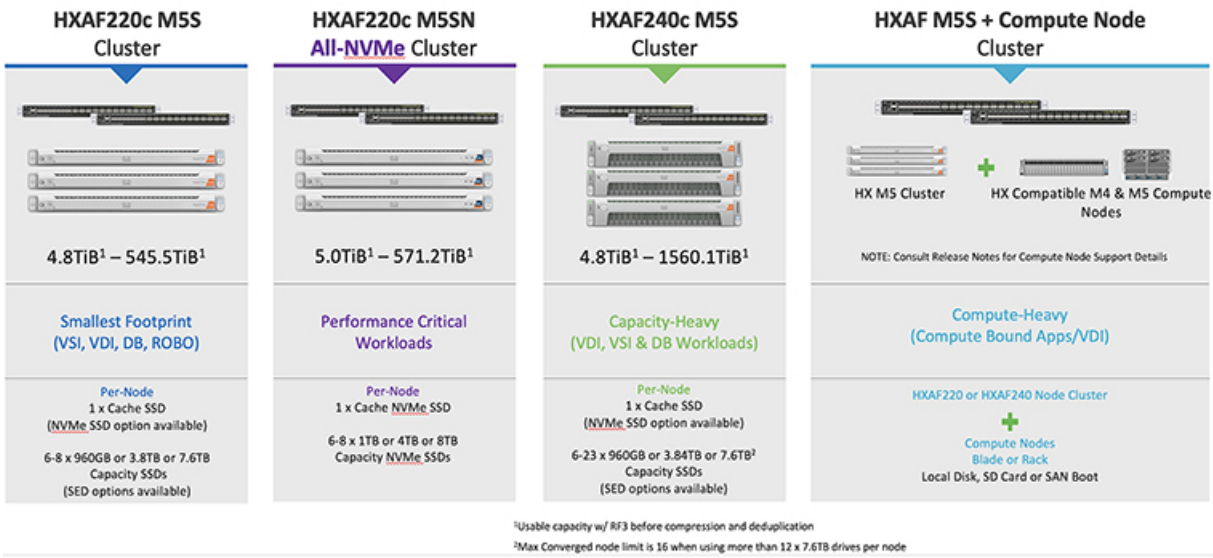
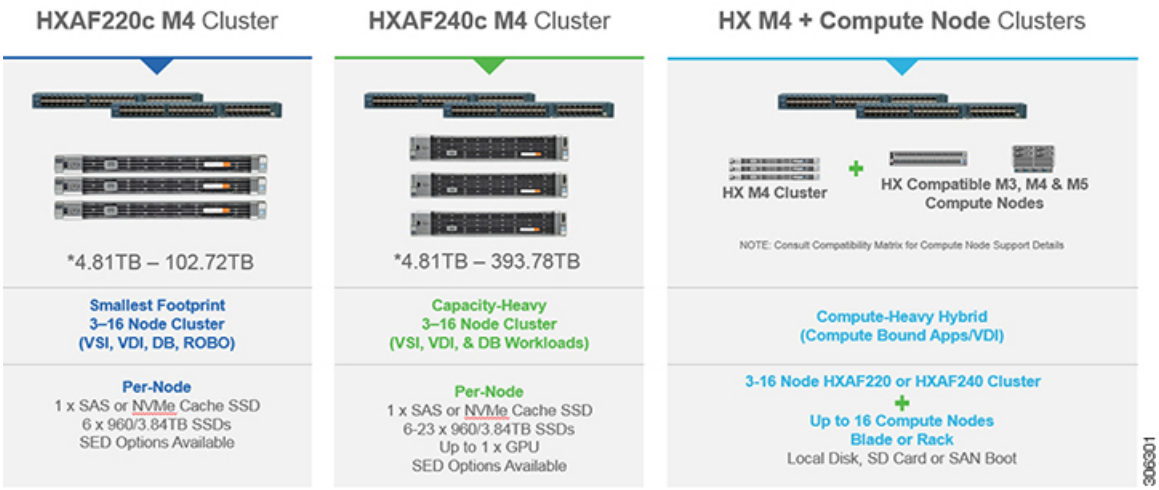


図 *5 : Cisco HyperFlex* オール フラッシュ *M4* 設定



Cisco HyperFlex HX シリーズ システムの管理コンポーネント

Cisco HyperFlex HX シリーズ システムは、次のシスコ ソフトウェア コンポーネントを使用して管理されます。

Cisco UCS Manager

Cisco UCS Manager は、ファブリック インターコネクトのペア上に存在する組み込みソフトウェアで、Cisco HX-Series Server のすべての設定機能と管理機能を備えています。UCS Manager

にアクセスする最も一般的な方法は、Web ブラウザを使用して GUI を開くことです。UCS Manager は、ロールベースのアクセス制御をサポートしています。

設定情報を 2 台の UCS Fabric Interconnects (FI) 間で複製することにより、高可用性ソリューションが実現します。一方の FI が使用不能になっても、もう一方が代わりを務めます。

UCS Manager の主なメリットは、ステートレス コンピューティングという概念です。HX クラスタの各ノードには設定がありません。たとえば、MAC アドレス、UUID、ファームウェア、BIOS 設定はすべて、サービス プロファイルの UCS Manager で設定され、すべての HX シリーズサーバーに均一に適用されます。これにより、設定の一貫性が保たれ、再利用が容易になります。新しいサービス プロファイルを数分以内に適用することができます。

Cisco HX Data Platform

Cisco HyperFlex Data Platform は、複数の Cisco サーバーをコンピューティング/ストレージ リソースからなる単一のプールに変換する、ハイパーコンバージド ソフトウェア アプライアンスです。これにより、ネットワーク ストレージの必要性がなくなり、VMware vSphere およびその既存の管理アプリケーションと緊密に統合して、シームレスなデータ管理エクスペリエンスが提供されます。加えて、ネイティブな圧縮と重複排除により、VM が占有する記憶域が削減されます。

HX Data Platform をインストールする場所は、vSphere などの仮想化プラットフォームです。仮想マシン、アプリケーション、およびデータ用のストレージを管理します。インストール時に Cisco HyperFlex HX クラスタ名を指定すると、HX Data Platform は各ノード上にハイパーコンバージドストレージクラスタを作成します。ストレージを増やす必要があり、HX クラスタにノードを追加する場合、Cisco HX データ プラットフォームは追加のリソース全体でストレージの平衡化を行います。

VMware vCenter 管理

Cisco HyperFlex System には、VMware vCenter ベースの管理機能があります。vCenter サーバーは、仮想化環境をモニターするために開発されたデータ センター管理サーバー アプリケーションです。HX Data Platform にも事前設定済みの vCenter サーバーからアクセスして、すべてのストレージのタスクを実行します。vCenter は、VMware vMotion、DRS、HA、および vSphere レプリケーションなそをサポートします。VMware スナップショットおよびクローニング機能に代わって、より拡張性の高いネイティブの HX Data スナップショットとクローンが使用されます。

HX Data Platform にアクセスするには個別のサーバーに vCenter インストールされている必要があります。vCenter は vSphere Client を通じてアクセスされ、それは管理者のラップトップまたは PC にインストールされています。

Cisco HyperFlex Connect ユーザ インターフェイスとオンライン ヘルプ

Cisco HyperFlex Connect（HX Connect）は、Cisco HyperFlex のユーザ インターフェイスを提供します。左側のナビゲーション ペインと右側の作業ペインの 2 つの主要なセクションに分かれています。

重要　HX Connect では、ほとんどのアクションの実行に管理者特権が必要です。

表 *1:* ヘッダー アイコン

アイコン	名前	説明
	メニュー	フルサイズのナビゲーション ペインと、アイコンのみのホバーオーバー ナビゲーション ペインを切り替えます。
	メッセージ	ユーザが開始するアクション（データ ストアの作成やディスクの削除など）の一覧が表示されます。 すべてのメッセージを削除して、メッセージ アイコンを非表示にするには、**[すべて消去（Clear All）]** を使用します。
	設定	**[サポート（Support）]**、**[通知（Notification）]**、および **[クラウド管理（Cloud Management）]** の設定にアクセスします。また **[サポート バンドル（Support Bundle）]** ページにアクセスすることもできます。
	アラーム	現在のエラーまたは警告のアラーム カウントが表示されます。エラーと警告の両方が存在する場合、カウントはエラー数を示します。 アラーム情報の詳細については、**[アラーム（Alarms）]** ページを参照してください。
	ヘルプ	状況に応じた HX 接続 のオンライン ヘルプ ファイルを開きます。
	ユーザ	タイムアウト設定やログアウトなどの設定にアクセスします。 **[ユーザ設定（User Settings）]** は管理者にのみ表示されます。

アイコン	名前	説明
	情報	その要素に関する詳細データにアクセスします。

オンライン ヘルプにアクセスするには：

- ユーザ インターフェイスの特定のページで、ヘッダーにある **[ヘルプ（Help）]** をクリックします。
- ダイアログボックスで、そのダイアログボックスの **[ヘルプ（Help）]** ボタンをクリックします。
- ウィザードで、**[ヘルプ（Help）]** をクリックします。

テーブル ヘッダーの共通フィールド

HX Connect 内のいくつかのテーブルには、テーブルに表示される内容を左右する次の 3 つのフィールドのどれかが表示されます。

UI 要素	基本的な情報
[更新（Refresh）] フィールドとアイコン	HX クラスタ の動的更新では、テーブルが自動的に更新されます。タイムスタンプは、テーブルが最後に更新された時刻を示します。 コンテンツを今すぐ更新するには、円形アイコンをクリックします。
[フィルタ（Filter）] フィールド	入力したフィルタ テキストと一致するリスト項目のみがテーブルに表示されます。以下の表の**現在**のページに一覧表示されている項目は自動的にフィルタ処理されます。入れ子になったテーブルはフィルタ処理されません。 **[フィルタ（Filter）]** フィールドに選択テキストを入力します。 **[フィルタ（Filter）]** フィールドを空にするには、**x** をクリックします。 テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてフィルタを適用します。

UI 要素	基本的な情報
[エクスポート（Export）] メニュー	テーブル データの**現在の**ページのコピーを保存します。テーブル コンテンツは、選択したファイルの種類でローカル マシンにダウンロードされます。リストの項目をフィルタ処理すると、フィルタ処理されたサブセット リストがエクスポートされます。 エクスポート ファイルの種類を選択するには、下向き矢印をクリックします。ファイルの種類のオプションは、`cvs`、`xls`、および `doc` です。 テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてエクスポートを適用します。

[ダッシュボード（Dashboard）] ページ

重要 読み取り専用ユーザの場合は、ヘルプに記載されているすべてのオプションが表示されないことがあります。HyperFlex (HX) Connect では、ほとんどのアクションの実行に管理者権限が必要です。

HX ストレージ クラスタのステータスの概要が表示されます。これは、Cisco HyperFlex Connect にログインすると最初に表示されるページです。

UI 要素	基本的な情報
[動作ステータス（Operational Status）] セクション	HX ストレージ クラスタの機能ステータスとアプリケーション パフォーマンスが表示されます。 **[情報（Information）]**（  ）をクリックして、HX ストレージ クラスタ名とステータス データにアクセスします。

UI 要素	基本的な情報
[クラスター ライセンスの状態（Cluster License Status）] セクション	HX ストレージ クラスタに初めてログインしたとき、または HX ストレージ クラスタ ライセンスが登録されるまでに、次のリンクが表示されます。 **クラスタ ライセンスが登録されていない**リンク：HX ストレージ クラスタが登録されていない場合に表示されます。クラスタ ライセンスを登録するには、このリンクをクリックし、**[スマート ソフトウェア ライセンス製品登録（Smart Software Licensing Product Registration）]** 画面で製品インスタンス登録トークンを指定します。製品インスタンス登録トークンを取得する方法の詳細については、『**Cisco HyperFlex システム インストール ガイド**』の「スマート ライセンスへのクラスタの登録」セクションを参照してください。
[復元力ヘルス（Resiliency Health）] セクション	HX ストレージ クラスタのデータ ヘルス ステータスと耐障害性が表示されます。 **[情報**（Information）]（  ）をクリックして復元力ステータスと、レプリケーションおよび障害データにアクセスします。
[容量（Capacity）] セクション	ストレージ合計の内訳と使用中または未使用のストレージ容量が表示されます。 また、ストレージの最適化、圧縮による節約、およびクラスタに格納されているデータに基づく重複排除比率も表示されます。
[ノード（Nodes）] セクション	HX ストレージ クラスタにおけるノード数とコンバージド ノード対コンピューティング ノードの区分が表示されます。ノード アイコンの上にカーソルを合わせると、ノードの名前、IP アドレス、ノード タイプが表示されます。また、容量、使用率、シリアル番号、およびディスク タイプ データにアクセスできるディスクがインタラクティブに表示されます。
[パフォーマンス（Performance）] セクション	設定可能な時間の HX ストレージ クラスタのパフォーマンス スナップショットが表示され、IOPS、スループット、および遅延データが示されます。 詳細については、**[パフォーマンス（Performance）] ページ**を参照してください。
[クラスタ時間（Cluster Time）] フィールド	クラスタのシステム日時。

テーブル ヘッダーの共通フィールド

HX Connect 内のいくつかのテーブルには、テーブルに表示される内容を左右する次の 3 つのフィールドのどれかが表示されます。

UI 要素	基本的な情報
[更新（Refresh）] フィールドとアイコン	HX クラスタ の動的更新では、テーブルが自動的に更新されます。タイムスタンプは、テーブルが最後に更新された時刻を示します。 コンテンツを今すぐ更新するには、円形アイコンをクリックします。
[フィルタ（Filter）] フィールド	入力したフィルタ テキストと一致するリスト項目のみがテーブルに表示されます。以下の表の**現在**のページに一覧表示されている項目は自動的にフィルタ処理されます。入れ子になったテーブルはフィルタ処理されません。 **[フィルタ（Filter）]** フィールドに選択テキストを入力します。 **[フィルタ（Filter）]** フィールドを空にするには、**x** をクリックします。 テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてフィルタを適用します。
[エクスポート（Export）] メニュー	テーブル データの**現在の**ページのコピーを保存します。テーブル コンテンツは、選択したファイルの種類でローカル マシンにダウンロードされます。リストの項目をフィルタ処理すると、フィルタ処理されたサブセット リストがエクスポートされます。 エクスポート ファイルの種類を選択するには、下向き矢印をクリックします。ファイルの種類のオプションは、`cvs`、`xls`、および `doc` です。 テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてエクスポートを適用します。

[動作ステータス（Operational Status）] ダイアログボックス

HX ストレージ クラスタの機能ステータスとアプリケーション パフォーマンスが表示されます。

UI 要素	基本的な情報
[クラスタ名（Cluster Name）] フィールド	この HX ストレージ クラスタの名前。
[クラスタ ステータス（Cluster Status）] フィールド	• **[オンライン（Online）]**：クラスタは利用可能です。 • **[オフライン（Offline）]**：クラスタは使用可能でありません。 • **読み取り専用**：クラスタは、書き込みトランザクションを受け入れることはできませんが、静的ラスタ情報の表示を継続することはできます。 • **容量不足**：クラスタ全体が容量不足であるか、または 1 つ以上のディスクが容量不足です。いずれの場合も、クラスタは、書き込みトランザクションを受け入れることはできませんが、静的ラスタ情報の表示を継続することはできます。
[休眠データ暗号化対応（Data-at-rest encryption capable）] フィールド	• **使用可能** • **サポート対象外** [はい（Yes）] と [いいえ（No）] のいずれかを使用できます。
[表示する理由（Reason to view）] ドロップダウン リスト	現在のステータスの要因を示すメッセージの数が表示されます。

[閉じる（Close）] をクリックします。

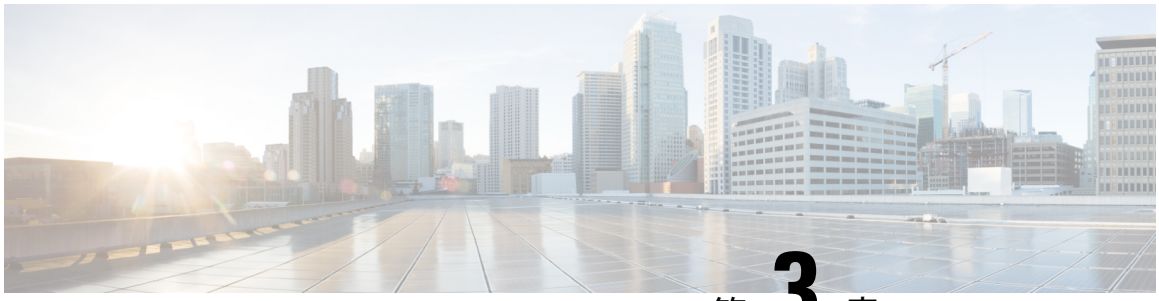
[復元力ヘルス（Resiliency Health）] ダイアログボックス

HX ストレージ クラスタのデータ ヘルス ステータスと耐障害性が表示されます。

名前	説明
[復元力ステータス（Resiliency Status）] フィールド	• [正常（Healthy）]：クラスタはデータおよび可用性に関して正常な状態です。 • [警告（Warning）]：データまたはクラスタの可用性に悪影響が生じています。 • [不明（Unknown）]：クラスタがオンラインになるまでの遷移状態。 色分けとアイコンを使用して、さまざまなステータスの状態が示されます。追加情報を表示するには、アイコンをクリックします。

名前	説明
[データ レプリケーション コンプライアンス（Data Replication Compliance）] フィールド	• コンプライアンス対応
[データ レプリケーション ファクタ（Data Replication Factor）] フィールド	HX ストレージ クラスタ全体の冗長なデータ レプリカの数が表示されます。
[許容ノード障害数（Number of node failures tolerable）] フィールド	HX ストレージ クラスタが処理できるノード中断の数が表示されます。
[許容永続デバイス障害数（Number of Persistent Device failures tolerable）] フィールド	HX ストレージ クラスタが処理できる永続デバイス中断の数が表示されます。
[許容キャッシングデバイス障害数（Number of Caching Device failures tolerable）] フィールド	HX ストレージ クラスタが処理できるキャッシュ デバイス中断の数が表示されます。
[表示する理由（Reason to view）] ドロップダウン リスト	現在のステータスの要因を示すメッセージの数が表示されます。

[閉じる（Close）] をクリックします。



第 3 章

インストールの前提条件

Cisco HXDP のサポートされているバージョンとシステム要件

Cisco HX Data Platform を正常にインストールするには、特定のソフトウェアおよびハードウェアのバージョン、ネットワーク設定が必要です。

表 *2 : Cisco HXDP* リリース *4.5(x)* のサポートされているバージョンとシステム要件

要件	詳細へのリンク
サーバのコンポーネント ファームウェアが、次の表に示されている最小バージョン以上であることを確認します。	詳細については、『Cisco HyperFlex Software Requirements and Recommendations』ドキュメントの「*FI/Server Firmware - 4.5(x)* リリース」トピックを参照してください。
推奨ブラウザのリスト。	詳細については、[Cisco HyperFlex ソフトウェアの要件と推奨事項のドキュメント（Cisco HyperFlex Software Requirements and Recommendations）]の「*[*ブラウザの推奨事項（*Browser Recommendations*）*]*」トピックを参照してください。

必要なハードウェア ケーブル

- 6200 シリーズ FI を使用する場合は、サーバごとに少なくとも 2 本の 10 Gb Small Form-Factor Pluggable（SFP）ケーブルを使用します。

  6300 シリーズ FI を使用する場合は、サーバごとに少なくとも 2 本の 40 GbE QSFP ケーブルを使用します。

- ファブリック インターコネクト コンソール ケーブル（CAB-CONSOLE-RJ45）の一方の端が RJ-45 コネクタで、もう一方の端が DB9 コネクタがあることを確認します。このケーブルは、ラップトップ上の RS-232 コンソール接続に接続するために使用します。

- 標準の電源コードで、電源モジュールとの接続側に IEC C13 コネクタが付いていることを確認します。オプションのジャンパ電源コードで、電源モジュールとの接続側に IEC C13 コネクタ、IEC C13 コンセントとの接続側に IEC C14 コネクタが付いていることを確認します。

  詳細については、Cisco UCS 6200 Series Fabric Interconnect Hardware Guideを確認してください。

- KVM ケーブルは、Cisco HX シリーズ サーバをシステムに接続します。DB9 シリアル コネクタ、モニタ用の VGA コネクタ、およびキーボードとマウス用のデュアル USB 2.0 ポートが付いています。このケーブルを使用すると、システムで稼動するオペレーティング システムや BIOS に直接接続できます。

（注） この同じ KVM ケーブルが UCS ラック マウント サーバとブレード サーバの両方に使用されます。

M4 または M5 サーバ用のケーブルとご注文情報の詳細については、それぞれ『Cisco HyperFlex HX-Series Models』と『Cisco UCS B200 Blade Server Installation and Service Note』を参照してください。

ホスト要件

Cisco HyperFlex クラスタには、少なくとも3つのコンバージド HyperFlex ノードが含まれます。追加のストレージが必要ない場合に計算能力を高めるために、compute-only ノードを追加するオプションが用意されています。HyperFlex クラスタ内の各サーバは、HyperFlex ノードとも呼ばれます。ストレージクラスタを展開する前に、各ノードに次の設定がインストールされ、構成されていることを確認してください。

詳細については、『Cisco HX240c/220c HyperFlex Node Installation Guides』を参照してください。

次のホスト要件が満たされていることを確認します。

- クラスタ内のすべてのサーバ（ノードまたはホスト）で同じ VLAN ID を使用する。
- ストレージクラスタ全体のすべての ESXi サーバで同じ管理者ログイン クレデンシャルを使用する。
- すべての ESXi ホストで SSH を有効なままにしてください。
- すべてのサーバ上で DNS と NTP を設定する。
- VMware vSphere をインストールして設定します。
- **VIC および NIC のサポート:**詳細については、『Cisco HyperFlex Systems: ネットワーキング トポロジ』のマニュアルを参照してください。

ディスクの要件

コンバージド ノードとコンピューティング専用ノードの間ではディスク要件が異なります。使用可能な CPU とメモリ容量を増やすには、必要に応じて、コンピューティング専用ノードで既存のクラスタを拡張できます。このコンピューティング専用ノードによって、ストレージパフォーマンスやストレージ容量が向上するわけではありません。

別の方法として、コンバージド ノードを追加すると、CPU リソースやメモリ リソースだけでなく、ストレージ パフォーマンスやストレージ容量も増えます。

ソリッドステートディスク（SSD）のみを備えたサーバはオールフラッシュ サーバです。SSD とハード ディスク ドライブ（HDD）の両方を備えたサーバはハイブリッド サーバです。

HyperFlex クラスタ内のすべてのディスクに以下が該当します。

- ストレージクラスタ内のすべてのディスクに同じストレージ容量が割り当てられます。ストレージ クラスタ内のすべてのノードに同じ数のディスクが割り当てられます。

- すべての **SSD** で TRIM をサポートし、TRIM が有効になっている必要があります。
- すべての **HDD** を SATA と SAS のどちらかのタイプにすることができます。ストレージ クラスタ内のすべての SAS ディスクをパススルー モードにする必要があります。
- SSD と HDD からディスク パーミッションを削除する必要があります。パーミッション付きのディスクは無視され、HX ストレージ クラスタに追加されません。
- オプションで、ディスク上の既存のデータを削除またはバックアップすることができます。指定されたディスク上のすべての既存のデータが上書きされます。

（注） 新しいファクトリ サーバは、適切なディスク パーティション設定で出荷されます。新しいファクトリ サーバからディスク パーティションを削除しなくでください。

- Cisco から直接購入したディスクのみがサポートされます。
- 自己暗号化ドライブ（SED）を備えたサーバでは、キャッシュ ドライブと永続ストレージ（容量）ドライブの両方を SED 対応にする必要があります。このようなサーバは、保管中のデータの暗号化（DARE）をサポートします。
- サポートされていないドライブまたはカタログのアップグレードに関するエラーが表示された場合は、互換性カタログを参照してください。

下の表に示すディスクに加えて、すべての M4 コンバージド ノードに、ESX がインストールされたミラー化設定の 2 X 64-GB SD FlexFlash カードが実装されています。すべての M5 コンバージド ノードに、ESX 搭載の M.2 SATA SSD が内蔵されています。

（注） 1 台のサーバまたはストレージ クラスタで、ストレージ ディスクのタイプやストレージ サイズを混在させないでください。ストレージ ディスク タイプの混在はサポートされません。

- キャッシュ ディスクまたは永続ディスクを交換する際は、元のディスクと同じタイプとサイズを常に使用します。
- 永続ドライブを混在させないでください。1 台のサーバでは、すべて HDD または SSD にして、同じサイズのドライブを使用します。
- ハイブリッド キャッシュ ドライブ タイプとオールフラッシュ キャッシュ ドライブ タイプを混在させないでください。ハイブリッド サーバではハイブリッド キャッシュ デバイスを使用し、オールフラッシュ サーバではオールフラッシュ キャッシュ デバイスを使用します。
- 暗号化されたドライブ タイプと暗号化されていないドライブ タイプを混在させないでください。SED ハイブリッド ドライブまたは SED オールフラッシュ ドライブを使用します。SED サーバでは、キャッシュ ドライブと永続ドライブの両方を SED タイプにする必要があります。
- すべてのノードで SSD を同じサイズと数量にする必要があります。異なる SSD タイプを混在させることはできません。

それぞれのサーバでサポートされているドライブのキャパシティと台数の詳細については、対応するサーバ モデルの仕様書を参照してください。

既存のクラスタを拡張する際の、互換性のある PID については、Cisco HyperFlex Drive Compatibility ドキュメントを参照してください。

コンピューティング専用ノード

次の表に、コンピューティング専用機能にサポートされるコンピューティング専用ノードの構成を示します。コンピューティング専用ノード上のストレージは、ストレージクラスタのキャッシュまたはキャパシティに含まれません。

（注） クラスタにコンピューティング ノードが追加されると、そのノードは、コンピューティング専用のサービス プロファイル テンプレートによって SD カードから起動できるように自動設定されます。別の形式のブート メディアを使用する場合は、ローカルのディスク設定ポリシーを更新してください。サーバに関連したポリシーについては、*Cisco UCS Manager* サーバ管理ガイドを参照してください。

サポートされているコンピューティング専用ノード サーバ	サポートされているブート方法 ESXi
• Cisco B200 M4/M5 • B260 M4 • B420 M4 • B460 M4 • C240 M4/M5 • C220 M4/M5 • C460 M4 • C480 M5 • B480 M5	任意の方法を選択します。 **重要** ESXi インストールでサーバに 1 つの形式のブート メディアだけが公開されていることを確認します。インストール後に、さらにローカルディスクまたはリモートディスクを追加できます。 HX コンピューティング専用ノードの USB ブートはサポートされていません。 • ESXi インストールされているミラー構成での SD カード。 • ローカル ドライブの HDD または SSD。 • SAN ブート • M.2 SATA SSD ドライブ。 （注） HW RAID M.2（UCS-M2-HWRAID および HX-M2-HWRAID）は、HX Data Platform リリース4.5(1a) 以降でサポートされるブート設定です。

ポート要件

ネットワークがファイアウォールの背後にある場合は、標準のポート要件に加え、VMware には VMware ESXi および VMware vCenter に対するポートが推奨されます。

- CIP-M は、クラスタ管理 IP に使用します。
- SCVM は、コントローラ VM の管理 IP です。
- ESXi は、ハイパーバイザの管理 IP です。

HyperFlex ソリューションのコンポーネント通信に必要なポートの包括的なリストは、HX Data Platform Security Hardening Guide の付録 A に記載されています。

ヒント 標準設定がなく、異なるポート設定が必要な場合は、環境のカスタマイズについて、表 C-5 ポートのリテラル値を参照してください。

HyperFlex 外部接続

外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
Intersight デバイス コネクタ	サポートされている HX システムは、各システムの管理コントローラに組み込まれているデバイス コネクタを介して Cisco Intersight に接続されます。	HTTPSポート番号：443 1.0.5-2084 以降（Cisco Intersight によって自動的にアップグレード）	

外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
			すべてのデバイス コネクタは、`svc.intersight.com` を適切に解決でき、かつポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。現在の HX インストーラでは、HTTP プロキシの使用がサポートされています。 ESXi 管理の IP アドレスは、インストーラから ESXi 管理に必要とされるすべてのポートを介して、Cisco UCS Manager から到達可能である必要があります。これにより、Cisco Intersight から ESXi 管理を展開できるようになります。 （注） ESXi ホストによって開始されたポート 443 でのアウトバウンド HTTPS 接続は、デフォルトの ESXi ファイアウォールによってブロックできます。この接続を許可するために、ESXi ファイアウォールを一時的に無効にすることができます。 ESXi ファイアウォールを無効

外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
			にするには、`esxcli network firewall set --enabled=false` コマンドを使用し、インストールが完了したら `esxcli network firewall set --enabled=false` コマンドを使用してファイアウォールを再度有効にします。 詳細については、Intersight ヘルプ センターのネットワーク接続要件を参照してください。
Auto Support	Auto Support（ASUP）は、HX Data Platform を通じて提供されるアラート通知サービスです。	SMTP ポート番号：25	Auto Support は、ノードのドライブ障害などのハードウェア問題が発生した際の診断に役立つハードウェア カウンタの履歴を提供するため、有効にすることを強く推奨します。

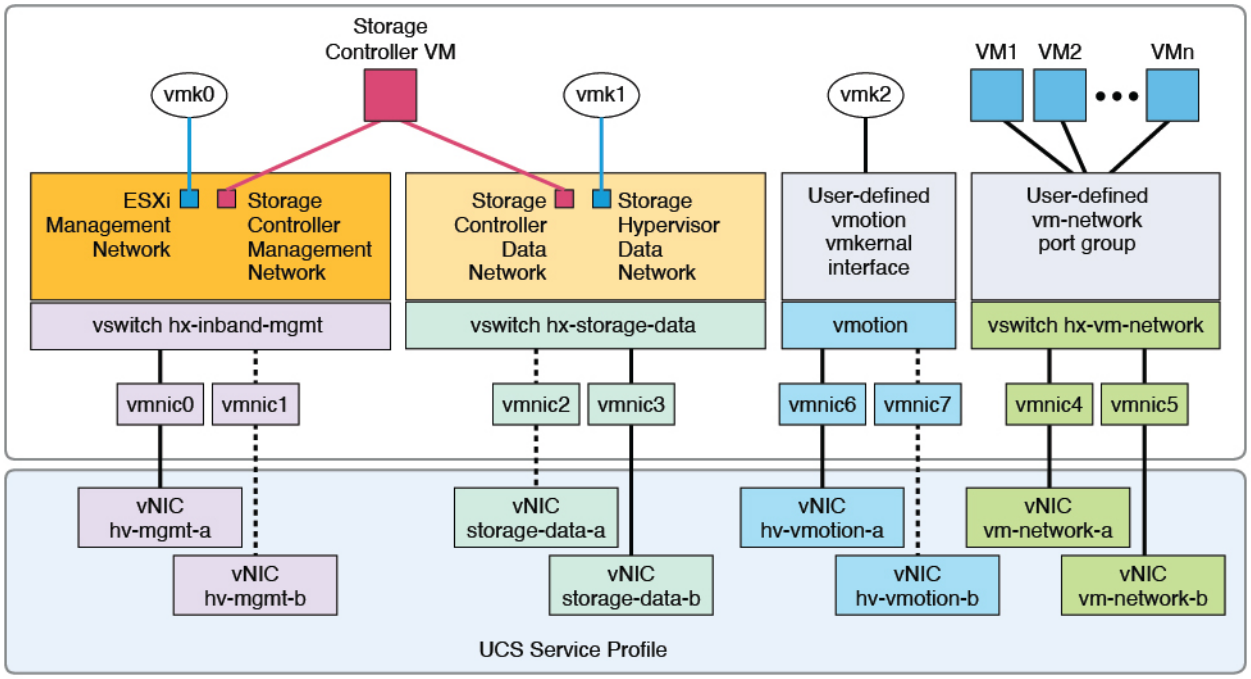
ファブリック インターコネクトのアップリンクのプロビジョニング

HyperFlex クラスタをセットアップする前に、最適なネットワーク トラフィック管理のためにアップストリーム帯域幅の容量を計画します。これにより、コンポーネントの障害や部分的なネットワーク停止が発生してもフローの安定状態が保証されます。

デフォルトでは、*hx-vm-network* vSwitch が**アクティブ/アクティブ**として設定されます。それ以外の vSwitch は、**アクティブ/スタンバイ**として設定されます。

（注） FI に対して Catalyst スイッチを実行しているクラスタの場合は、最適な Quality of Service (QOS) MTU を 9216 に設定します (LAN > LAN Cloud > QoS システム クラスにあります)。そうでない場合、フェールオーバーは失敗します。

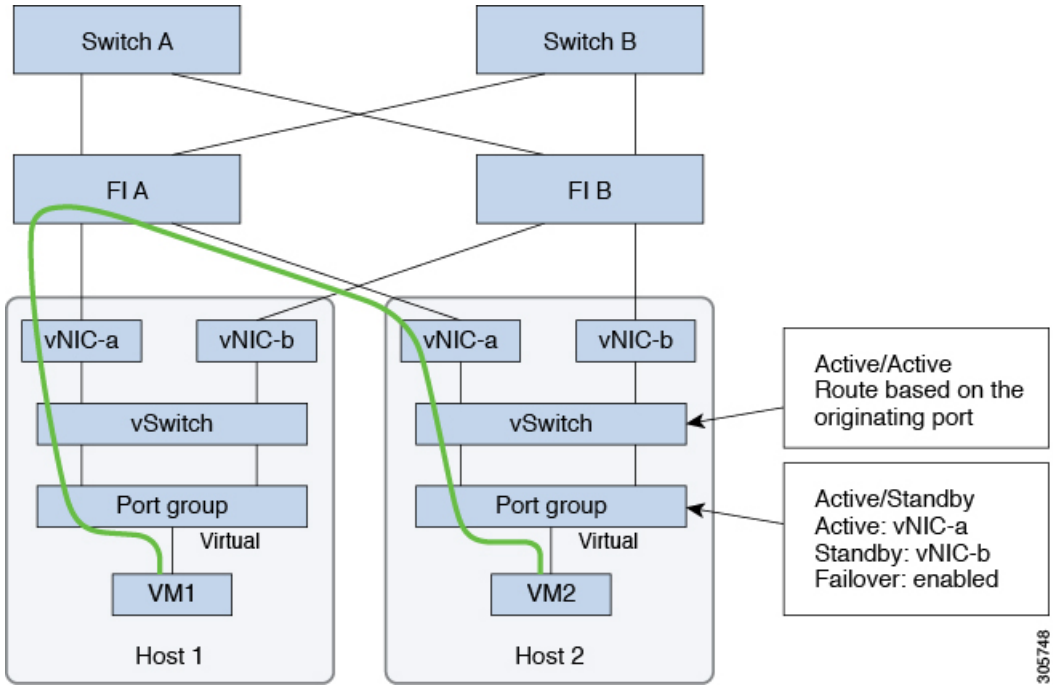
図 *6* : 単一ホストの *HyperFlex Data Platform* 接続



Note: 1. Dotted lines represent a **"standby"** link.
2. All **"a"** vNICs connect to FI-A.
3. All **"b"** vNICs conect to FI-B.
4. MTU of 9000 is needed for storage-data and vmotion networks.
5. All VLANs by default are tagged on the FI so frames are passed untagged to each vswitch.
6. The vm network port groups are automatically created in 1.8 installer with vlan suffix.

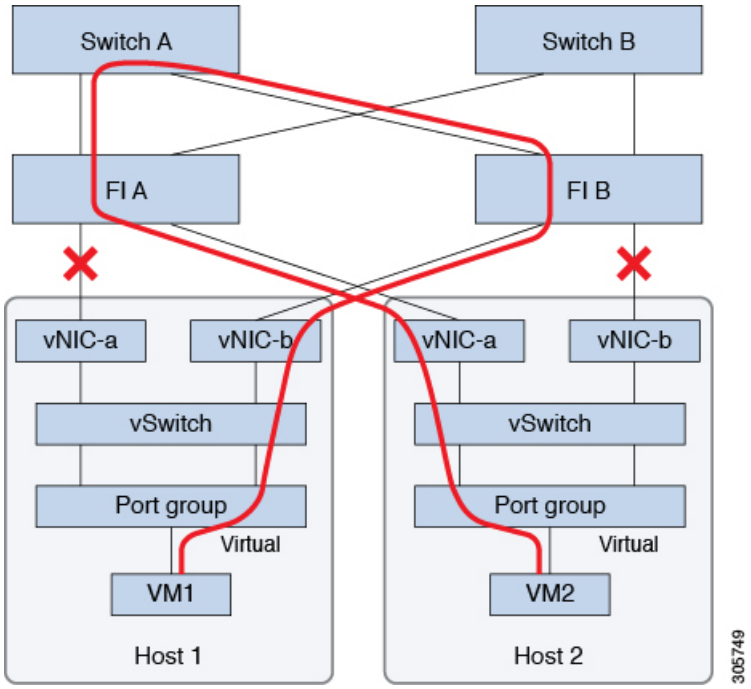
デフォルトの vSwitch NIC チーミング ポリシーとフェールオーバー ポリシーを [yes] に設定します。これにより、管理トラフィック、vMotion トラフィック、およびストレージ トラフィックのすべてが、ローカルでファブリック インターコネクトに転送されるようになり、フローを安定した状態に維持できます。vNIC-a で障害が発生すると、ESXi がロード バランシングを計算し、すべての仮想ポートを vNIC-b に再ピニングします。vNIC-a がオンライン状態に戻った時点で、再びピニングが適用され、vNIC-a と vNIC-b の間で仮想ポートが元のように均等に分配されます。これにより、Cisco UCS ファブリック インターコネクトのアップストリームでの遅延と帯域幅使用量が削減されます。

図 7: 安定した状態のトラフィック フロー



1 つ以上のサーバー リンクで障害が発生した場合（たとえばホスト 1 がファブリック A への接続を失い、ホスト 2 がファブリック B への接続を失った場合）は、トラフィックがアップ ストリーム スイッチを通過する必要があります。したがってアップリンク ネットワーク帯域幅の使用率が増加し、新しいアップリンクを追加する必要があります。

図 *8*: リンク障害発生時のトラフィック フロー



（注） 1 つのファブリック インターコネクトから 2 つの異なるアップストリーム スイッチへのアップリンクが存在する場合は、FI で**分離レイヤ 2**（DJL2）と呼ばれる状態が発生します。DJL2 は、FI がエンド ホスト モードとなっているときに DJL2 が適切に設定されていないと発生することが既知となっています。

DJL2 を適切に導入するには、『Cisco UCS 6300 Series Fabric Interconnect Hardware Guide—*Deploy Layer 2 Disjoint Networks Upstream in End Host Mode*』というホワイト ペーパーを参照してください。

ネットワーク設定

重要 すべての IP アドレスは IPv4 である必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

ベスト プラクティス

- ネットワークごとに異なるサブネットと VLAN を使用する必要があります。
- 10 Gbps ケーブルを使用して、各ホストを Cisco UCS ファブリック インターコネクトに直接接続します。

- デフォルトの VLAN である VLAN 1 を使用しないでください。特に Disjoint Layer 2 設定を使用している場合はネットワーキングの問題が発生する可能性があります。
- デフォルトで、インストーラは VLAN を非ネイティブとして設定します。非ネイティブ VLAN に対応するようにアップストリーム スイッチを確実に設定してください。
- UCSファブリック インターコネクトからすべての最上位ラック スイッチポートへのアップリンクは、スイッチのベンダーとモデルに応じて、**エッジ トランク** モードまたは**PortFast エッジ** モードでスパニング ツリーを設定する必要があります。この追加設定により、リンクがフラップまたは状態を変更したときに、不要なスパニング ツリー ステートを介して遷移せず、トラフィック転送が開始される前に遅延が発生することがなくなります。**PortFast Edge** モードで FI アップリンクを適切に設定しないと、HyperFlex ネイティブの高可用性ネットワーク設計を活用する障害シナリオおよびインフラストラクチャアップグレード中にネットワークおよびクラスタが停止する可能性があります。
- FI側のポートは、Port-Fast、スパニングツリーポートタイプのエッジトランク、またはポートをただちにフォワーディングモードにする類似のスパニングツリー設定を持つ必要があります。

ESXi ホストごとに、次のネットワークが必要です。

- **管理トラフィック ネットワーク**：vCenterから、ハイパーバイザ（ESXiサーバ）管理とストレージ クラスタ管理を処理します。
- **データ トラフィック ネットワーク**：ハイパーバイザとストレージのデータ トラフィックを処理します。
- **vMotion ネットワーク**
- **VM ネットワーク**

4 つの vSwitch があり、それぞれが異なるネットワークを伝送します。

- **vswitch-hx-inband-mgmt**：ESXi 管理とストレージ コントローラ管理に使用されます。
- **vswitch-hx-storage-data**：ESXi ストレージ データと HX Data Platform のレプリケーションに使用されます。

  この 2 つの vSwitch は、割り当てられた静的 IP アドレスでさらに 2 つのポート グループに分割され、ストレージ クラスタと ESXi ホスト間のトラフィックを処理します。
- **vswitch-hx-vmotion**：VM とストレージ vMotion に使用されます。

  この vSwitch には、vCenter クラスタ内のすべてのホストに接続する vSphere で定義された管理用ポート グループが 1 つあります。
- **vswitch-hx-vm-network**：VM データ トラフィックに使用されます。

  Cisco UCS Manager 内の対応する vNIC テンプレート上で VLAN を追加または削除することができます。詳細な手順については、『Managing VLANs in Cisco UCS Manager』と『Managing vNIC templates in Cisco UCS Manager』を参照してください。VSwitch 上でポー

ト グループを作成するには、『Adding Virtual Port Groups to VMware Standard vSwitch』を参照してください。

（注）

1. vSwitch は HX Data Platform インストーラによって自動的に作成されます。
2. HyperFlex ストレージクラスタの作成後に、vSphere の次のサービスを有効にする必要があります。
   - DRS （オプション、ライセンス登録されている場合）
   - VMotion
   - ハイ アベイラビリティ

VLAN と vSwitch の要件

少なくとも 3 つの VLAN ID を指定します。インストール中にファブリック インターコネクト上ですべての VLAN を設定する必要があります。

VLANタイプ	説明
（注） 次のネットワークごとに、異なるサブネットと VLAN を使用する必要があります。	
VLAN ESXi および HyperFlex 管理トラフィック	VLAN名：<user-defined> （たとえば、「hx-inband-mgmt」） VLAN ID：<user-defined>
VLAN HyperFlex ストレージ トラフィック	VLAN名：<user-defined> （たとえば、「hx-storage-data」） VLAN ID：<user-defined>
VLAN VM vMotion	VLAN名：<user-defined> （たとえば、「hx-vmotion」） VLAN ID：<user-defined>
VLAN VM ネットワーク	VLAN VM ネットワーク：<user-defined> （たとえば、「hx-vm-network」） VLAN ID：<user-defined>

外部スイッチ VLAN タギング（EST）を使用した VLAN タギングおよび vSwitch 設定は、UCS Manager プロファイルを使って適用されます。HX Data Platform インストーラは、このプロセスを簡素化します。

（注）
- デフォルトの VLAN である VLAN 1 を使用しないでください。特に Disjoint Layer 2 設定を使用している場合はネットワーキングの問題が発生する可能性があります。VLAN 1 以外の VLAN を使用します。

  デフォルトで、インストーラは VLAN を非ネイティブとして設定します。非ネイティブ VLAN に対応するようにアップストリーム スイッチを設定します。
- インバンド管理は、VLAN 2 または VLAN 3 ではサポートされていません。

Cisco UCS の要件

プロンプトが表示されたら、UCS ファブリック インターコネクトと UCS Manager に関するリストの内容を提供してください。

Cisco UCS ファブリック インターコネクトの要件

UI 要素	基本的な情報
アップリンク スイッチ モデル	スイッチ タイプと接続タイプを指定します（SFP + Twin Ax または光）。
ファブリックインターコネクト クラスタの IP アドレス	<*IP* アドレス>。
FI-A の IP アドレス	<*IP* アドレス>。
FI-B の IP アドレス	<*IP* アドレス>。
MAC Address Pool	00:00:00 MAC アドレス プールを確認します。
IPブロック	KVM IPプール。少なくとも 4 つの IP アドレス。
サブネット マスク	たとえば、*255.255.0.0* とします。
デフォルト ゲートウェイ	たとえば、*10.193.0.1* とします。

Cisco UCS Manager の要件

UI 要素	基本的な情報
UCS Managerのホスト名	ホスト名または *IP* アドレス。

UI 要素	基本的な情報
ユーザ名	<管理者ユーザ名>
パスワード	<管理者ユーザ名>

ハイパーバイザ要件

vCenter を介して、ストレージ管理ネットワークまたはストレージ データ ネットワーク上の ESXi サーバが使用できるアドレス範囲から、IP アドレスを入力します。すべてのネットワーク アドレスの静的 IP アドレスを指定します。

（注）
- データ ネットワークと管理ネットワークは異なるサブネット上になければなりません。
- ストレージ クラスタの作成後は、IP アドレスを変更できません。Cisco TAC に連絡して、サポートを受けてください。
- （必須の操作ではありませんが）DNS 名を指定する場合には、IP アドレスの転送と逆 DNS ルックアップを有効にしてください。
- インストーラの IP アドレスは、ハイパーバイザおよびストレージ コントローラ VM が使用する管理サブネットから到達可能である必要があります。インストーラ アプライアンスは、インストールするクラスタに含まれない VMware ワークステーションまたは ESXi ホストで動作する必要があります。

管理ネットワークの IP アドレス		データ ネットワークの IP アドレス	
ハイパーバイザ	ストレージコントローラ	ハイパーバイザ	ストレージコントローラ
<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>
<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>
<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>
<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>	<*IP*アドレス>
[VLAN タグ（VLAN Tags）]	*VLAN_ID*	*[VLAN タグ（VLAN Tags）]*	*VLAN_ID*
サブネット マスク		サブネット マスク	
デフォルト ゲートウェイ		デフォルト ゲートウェイ	

管理ネットワークの IP アドレス	データ ネットワークの IP アドレス
インストーラ アプライアンスの IP アドレス	
<*IP*アドレス>	<*IP*アドレス>

ストレージ クラスタ要件

ストレージ クラスタは、Cisco HX Data Platform のコンポーネントです。vSphere Web クライアントで単一のデータストアが容易にプロビジョニングされ、それによりストレージの複雑さを軽減します。コントローラ リソースを活用して高可用性を実現するために、ストレージ クラスタ内のすべてのサーバのディスクにデータが分散されます。

ストレージ クラスタは、関連する vSphere クラスタから独立しています。vSphere クラスタ内の ESXi ホストを使用してストレージ クラスタを作成できます。

ストレージ クラスタを定義するには、次のパラメータを指定します。

フィールド	説明
名前（Name）	ストレージ クラスタの名前を入力します。
管理 IP アドレス	これにより、各ESXiホスト上でストレージ管理ネットワークへのアクセスが可能になります。 • このIPアドレスは、ノードの管理IPアドレスと同じサブネット上に存在する必要があります。 • 同じサブネット上の他のクラスタとの間でクラスタ管理IPが最後のオクテットを共有できないようにしてください。 • これらのIPアドレスは、「ハイパーバイザ」のセクションで各ノードに割り当てる4つのIPアドレスとは別の追加的なアドレスです。
ストレージ クラスタ データの IP アドレス	これにより、各 ESXi ホスト上でストレージ データ ネットワークとストレージ コントローラ VM ネットワークへのアクセスが可能になります。 同じIPアドレスをクラスタ内のすべてのESXiノードに適用する必要があります。

フィールド	説明
データ レプリケーション ファクタ	データ レプリケーション係数により、ストレージ クラスタ全体のデータの冗長レプリカの数が定義されます。 これは HX Data Platform のインストール中に設定され、変更はできません。 [データ レプリケーション係数（Data Replication Factor）] を選択します。選択できる基準は、次のとおりです。 • **データ複製ファクタ 3**: Hyperflex Edge を除くすべての環境で複製ファクタ 3 を強く推奨しています。複製ファクタ 2 では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。 **注目** これは推奨オプションです。 • **データ レプリケーション係数 2**：データの冗長複製を2つ保持します。この場合、ストレージ リソースの消費量は少なくてすみますが、ノードやディスクの同時障害が発生した場合にデータ保護が低下します。 ストレージ クラスタ内のノードまたはディスクで障害が発生すると、クラスタの機能に影響が生じます。複数のノードで障害が発生する場合や、1つのノードと別のノード上のディスクで障害が発生する場合を、同時障害と呼びます。

vCenter 設定要件

vCenter用に管理者レベルのアカウントとパスワードを指定します。既存のvCenterサーバーが存在することを確認します。次の vSphere サービスが動作していることを確認します。

- ダイナミック リソース スケジューラ（DRS）を有効にします（オプション。ライセンス供与時に有効）。
- vMotion を有効にします。

- 高可用性（HA）を有効にします（フェールオーバー容量を定義するため、またデータストア ハートビートを拡張するために必要）。
- ユーザ VM はバージョン 9 以降である必要があります（HX Data Platform、ネイティブ スナップショット、および ReadyClones を使用するために必要）。

フィールド	説明
vCenter Server	現在の vCenter サーバ ー web アドレスを入力します。 例：*http://<IP* アドレス> など。
ユーザ名	<管理者ユーザ名> を入力します。
パスワード	<管理者パスワード> を入力します。
データセンター名 （注） 既存のデータセンター オブジェクトを使用できます。データセンターが vCenter に存在しない場合は、作成されます。	vCenter データセンター用の必要な名前を入力します。
クラスタ名	vCenter クラスタ用の必要な名前を入力します。クラスタには、3 つ以上の ESXi サーバが含まれる必要があります。

システム サービス要件

Cisco HX Data Platform をインストールする前に、次のネットワーク接続とサービスが稼働していることを確認します。

- DNS サーバ

注意 DNS サーバは HX ストレージ クラスタの外側に配置される必要があります。ネストされた DNS サーバは、DC 電源損失時など、クラスタ全体がシャットダウンした後にクラスタが起動しない可能性があります。

- NTP サーバ

注意 NTP サーバは HX ストレージ クラスタの外側に配置される必要があります。ネストされた NTP サーバは、DC 電源損失時など、クラスタ全体がシャットダウンした後にクラスタが起動しない可能性があります。

（注）

- ストレージ クラスタを設定する前に、NTP サーバが稼働状態で、信頼性の高い時間のソースを提供していることを手動で確認します。
- すべてのノード（コンバージドとコンピューティングの両方）とすべてのストレージ コントローラ VM に同じ NTP サーバを使用します。
- NTP サーバは、安定性があり、（クラスタの存続期間中に）中断せず、静的 IP アドレス経由で到達可能である必要があります。
- アクティブ ディレクトリを NTP サーバとして使用している場合、NTP サーバが Microsoft ベスト プラクティスに従って設定されていることを確認してください。詳細については、『Windows Time Service Tools and Settings』を参照してください。NTP サーバが適切に設定されていない場合、同期が行われず、クライアント側で時間同期を修正する必要が発生する可能性があります。詳細については、『Synchronizing ESXi/ESX time with a Microsoft Domain Controller』を参照してください。

- [タイム ゾーン（Time Zone）]

フィールド	基本的な情報
[DNSサーバ（DNS Server(s)）]	*<IP address>* HyperFlex Data Platform のインストール中にホスト名を使用する場合は、DNS サーバー アドレスが必須です。 （注） • DNS サーバを使用しない場合は、HX Data Platform インストーラの [クラスタの設定（Cluster Configuration）] ページの [システム サービス（System Services）] でホスト名を入力しないでください 。IP アドレスのみを使用します。 • 複数の *DNS* サーバ アドレスを指定するには、アドレスをカンマで区切ります。DNS サーバ アドレスが正しく入力されていることを注意深く確認してください。
NTPサーバ (信頼性の高い NTP サーバが必要です)	*<IP address>* NTP サーバは、以下の間のクロック同期に使用されます。 • ストレージ コントローラ VM • ESXi ホスト • vCenter Server 重要 NTP サーバの静的 IP アドレスは、ストレージ コントローラ VM、ESXi ホスト、および vCenter Server 間のクロック同期を保証するために必要です。 インストール中に、この情報がすべてのストレージ コントローラ VM および対応するホストに伝播されます。ストレージ クラスタの起動時に自動的に各サーバが同期されます。
[タイム ゾーン（Time Zone）]	<使用するタイム ゾーン> ストレージ コントローラ VM のタイム ゾーンを選択します。これは、スケジュール済みのスナップショットを取得するタイミングを決定するために使用されます。 （注） すべての VM を同じタイム ゾーンにする必要があります。

コントローラ VM の CPU リソース予約

ストレージ コントローラ VM は HyperFlex Data Platform 用の重要な機能を提供するので、HX Data Platform インストーラはコントローラ VM の CPU リソース予約を設定します。この予約により、コントローラ VM に最低限必要な CPU リソースが割り当てられることが保証されます。これは、ESXi ハイパーバイザー ホストの物理 CPU リソースがゲスト VM によって大量に消費される状況で役立ちます。次の表に、ストレージ コントローラ VM の CPU リソース予約の詳細を示します。

製品 ID	VM CPU の数	共有	予約	制限
HXAF220c-M5SN（すべて NVMe 220）	12	低	10,800 MHz	無制限
HX ブースト モードが有効な場合： HXAF220c-M5SN HXAF240c-M5SN	16	低	10,800 MHz	無制限
HX ブースト モードが有効な場合： HXAF220c-M4/M5/M6 HXAF240c-M4/M5SX/M6	12	低	10,800 MHz	無制限
他のすべてのモデル	8	低	10,800 MHz	無制限

コントローラ VM 用メモリ リソース予約

次の表に、ストレージ コントローラ VM 用のメモリ リソース予約の詳細を示します。

サーバ モデル	ゲスト メモリの量	すべてのゲスト メモリを予約
HX220c-M4/M5 HX-E-220M5SX	48 GB	はい
HXAF220C-M4	48 GB	はい
HXAF220C-M5 HXAF-E-220M5SX	48 GB 7.6 TB SSD（SED および非 SED）を搭載した構成の場合は 56 GB	○
HX240c-M4/M5SX	72 GB	はい

サーバ モデル	ゲスト メモリの量	すべてのゲスト メモリを予約
HXAF240c-M4/M5SX	72 GB 7.6 TB SSD（SED および非 SED）を搭載した構成の場合は 84 GB	○
HX240C-M5L	78 GB	Yes
HXAF220C-M5SN（すべての NVMe 220）	72 GB 8 TB NVMe 容量ドライブの構成の場合は 84 GB	対応
HXAF240C-M5SD HX240C-M5SD（奥行240）	48 GB （注） 7.6TB ドライブは HXAF240C-M5SD でサポートされますが、より高いメモリ構成は必要ありません。	はい

- C240 ラック サーバは、2 ラック ユニット（2RU）フォーム ファクタで非常に優れた拡張性と高いパフォーマンスを提供します。
- C220 サーバは、1 ラック ユニット（1RU）フォーム ファクタで拡張性を提供します。
- 16 TB LFF ドライブのサポートは有効になっていません。

（注） HX 5.0(2b) 以降、新しいコントローラ VM メモリ割り当ては、HX 5.0(2b) 以降を使用して新規インストールまたは SW 再展開として展開されたクラスタ、または 5.0(2b) の後に拡張されたノードに対して行われます。HX 5.0(2b) 以降にクラスタをアップグレードする場合、コントローラ VM に割り当てられるメモリが自動で変更されないように注意してください。CVM メモリを削減したい場合は、手動で行う必要があります。CVM メモリを手動で変更する方法の詳細については、Changing Controller Memory on a Cluster を参照してください。

Auto Support 要件

Auto Support（ASUP）は、HX Data Platform を通じて提供されるアラート通知サービスです。Auto Support を有効にすると、HX Data Platform から、指定されたメール アドレスまたは通知を受信したい電子メール エイリアスに通知が送信されます。

自動サポートを設定するには、次の情報が必要です。

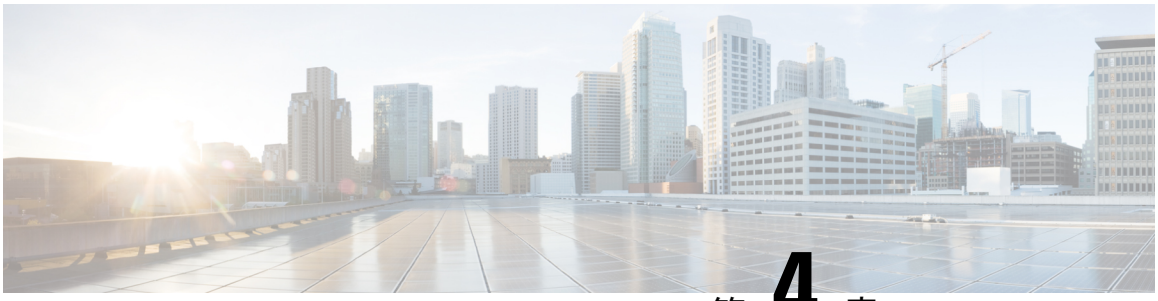
自動サポート	
[自動サポートの有効化（Enable Auto Support）] チェックボックス	HX ストレージ クラスタの作成時にこのボックスをオンにします。
メール サーバ	*<IP address>* Auto Support を有効にするには、ネットワーク上で SMTP メール サーバを設定する必要があります。すべてのストレージ コントローラ VM の IP アドレスから送信された電子メールを処理するために使用します。 （注）　未認証の SMTP のみが ASUP のサポート対象となります。
メール送信者	*<username@domain.com>* Auto Support 通知の送信に使用する電子メール アドレス。
ASUP受信者	Auto Support 通知を受信する電子メール アドレスまたは電子メール エイリアスのリスト。

（注）　Auto Support は、ノードのドライブ障害などのハードウェア問題が発生した際の診断に役立つハードウェア カウンタの履歴を提供することになるため、有効にすることを強く推奨します。

シングル サインオンの要件

SSO URL が vCenter から提供されます。コントローラ VM からその URL に直接到達できない場合は、[インストーラの詳細設定（Installer Advanced Settings）] を使用して場所を明示的に設定します。

シングルサインオン（**SSO**）	
SSO サーバの URL	SSO URL は、vCenter の **[vCenter サーバ（vCenter Server）] > [管理（Manage）] > [詳細設定（Advanced Settings）]** にあります（キー `config.vpxd.sso.sts.uri`）。



第 4 章

Cisco HyperFlex Systems サーバーのインストール

この章では、HyperFlexクラスタをセットアップするための物理コンポーネントのインストール方法を説明します。

ラック設置型 Cisco HyperFlex ノード

HyperFlex クラスタとノード制限の詳細については、『Release Notes for Cisco HX Data Platform』の最新版の「**Cisco HX Data Platform Storage Cluster Specifications**」を参照してください。

UCS C シリーズのインテグレーションの指針については、お使いのリリースの Cisco UCS C シリーズ サーバへの Cisco UCS Manager のインテグレーション設定ガイドを参照してください。

Cisco HyperFlex ノードのインストールの詳細については、下の表のそれぞれのリンクを参照してください。

インストールするノードの種類	参考資料
コンバージドノード数	
HyperFlex HX220c M4/M5 ノード	Cisco HyperFlex HX220c M5 ノード インストール ガイド
HyperFlex HX240c M4/M5 ノード	Cisco HyperFlex HX240c M5 ノード インストール ガイド
コンピューティング専用ノード	
Cisco UCS B200 M3/M4/M5 ノード	Cisco UCS B200 M3/M4/M5 Blade Server Installation and Service Note

インストールするノードの種類	参考資料
Cisco UCS B260 M4 ノード、B460 M4 ノード	Cisco UCS B260 M4 and B460 M4 Blade Server Installation and Service Note for Servers with E7 v4 CPUs Cisco UCS B260 M4 and B460 M4 Blade Server Installation and Service Note for Servers with E7 v3 and E7 v2 CPUs
Cisco UCS B420 M4 ノード	Cisco UCS B420 M4 Blade Server Installation and Service Note
Cisco UCS B480 M5 ノード	Cisco UCS B480 M5 Blade Server Installation and Service Note
Cisco UCS C240 M3/M4/M5 ラック ノード	Cisco UCS C240 サーバ インストレーションおよびサービス ガイド
Cisco UCS C220 M3/M4/M5 ラック ノード	Cisco UCS C220 サーバ インストレーションおよびサービス ガイド
Cisco UCS C480 M5 ノード	Cisco UCS C480 M5 Server Installation and Service Guide
Cisco UCS B420 M4 ノード	Cisco UCS 460 M4 Server Installation and Service Guide

ファブリック インターコネクトのセットアップ

高度な可用性をもたらすため、次のようにファブリック インターコネクトの冗長ペアを設定します。

1. L1 または L2 の高可用性ポート間で、イーサネット ケーブルを使用して直接 2 つのファブリック インターコネクトに接続します。
2. ファブリック インターコネクト A 上のポート L1を ファブリック インターコネクト B 上のポート L1 に接続し、ファブリック インターコネクト A 上のポート L2 をファブリック インターコネクト B 上のポート L2 に接続します。

これにより、2つのファブリック インターコネクトは、互いのステータスを継続的にモニターします。

ファブリック インターコネクトを接続する前に、以下の情報を確認し、取得してください。

項目	説明
ファブリック インターコネクトの物理的な接続を確認します。	• 1 つ目のファブリック インターコネクトのコンソール ポートが、コンピュータまたはコンソール サーバに物理的に接続されている。 • 管理イーサネット ポート（mgmt0）が外部のハブ、スイッチ、またはルータに接続されている。 • 両方のファブリック インターコネクトの L1 ポートが互いに直接接続されている。 • 両方のファブリック インターコネクトの L2 ポートが互いに直接接続されている。
コンピュータ端末でコンソール ポートのパラメータを確認します。	• 9600 ボー • 8 データ ビット • パリティなし • 1 ストップ ビット
初期セットアップに関する情報を入手します。	初期セットアップに関する次の情報を収集します。 • システム名 • 管理者アカウントのパスワード • 3 つの静的 IP アドレス • 3 つの静的 IP アドレスのサブネット マスク • デフォルト ゲートウェイの IP アドレス • DNS サーバの IP アドレス • システムのドメイン名

両方のファブリック インターコネクトが同じセットアップ プロセスを通過する必要があります。プライマリ ファブリック インターコネクトをセットアップして、クラスタ設定用に有効にします。同じプロセスを使用してセカンダリ ファブリック インターコネクトをセットアップするときには、最初のファブリック インターコネクトがピアとして検出されます。

Cisco UCS Manager GUI を使用したプライマリ ファブリック インターコネクトの設定

設定を始める前に、同じサブネットで次の 3 つの IP アドレスを指定します。

- プライマリ ファブリック インターコネクト FI A の管理ポート IP アドレス

- セカンダリ ファブリック インターコネクト FI B の管理ポートの IP アドレス
- HyperFlex クラスタの IP アドレス。

次のように Cisco UCS Manager GUI を使用してプライマリ ファブリック インターコネクトを設定します。

ステップ 1 コンソール ポートに接続します。詳細については、Cisco 6200 Series Fabric Interconnect Hardware Installation guideを参照してください。

ステップ 2 ファブリック インターコネクトの電源を入れます。ファブリック インターコネクトが起動する際、電源オン セルフテストのメッセージが表示されます。

ステップ 3 インストール方式プロンプトに *gui* と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

- ファブリック インターコネクトの管理ポートの IPv4 アドレス。
- ファブリック インターコネクトの管理ポートの IPv4 サブネット マスク。
- ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IPv4。

重要 すべての IP アドレスは IPv4 である必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

ステップ 5 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager 起動ページに移動します。

ステップ 6 **[Express Setup (Express セットアップ)]** を選択します。

ステップ 7 **[Initial Setup (初期セットアップ)]** を選択し、**[Submit (送信)]** をクリックします。

ステップ 8 **[Cluster and Fabric Setup (クラスタおよびファブリック セットアップ)]** 領域で、次のフィールドに値を入力します。

名前	説明
[Enable Cluster (クラスタの有効化)] オプション	[Enable Cluster (クラスタの有効化)] オプションを選択します。
[Fabric Setup] オプション	*[Fabric A (ファブリック A)]* を選択します。
[Cluster IP Address] フィールド	Cisco UCS Manager が使用する IPv4 アドレスを入力します。

ステップ 9 **[System Setup (システム セットアップ)]** 領域で、次のフィールドに値を入力します。

フィールド	説明
[システム名（System Name）] フィールド	Cisco UCS ドメインに割り当てられる名前。

フィールド	説明
[Admin Password] フィールド	ファブリック インターコネクト上の管理者アカウントに使用されるパスワード。 Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。このパスワードは空にできません。
[Confirm Admin Password] フィールド	ファブリック インターコネクト上の管理者アカウントに使用されるパスワード。
[Mgmt IP Address] フィールド	ファブリック インターコネクト上の管理ポートの固定 IP アドレス。
[Mgmt IP Netmask] フィールド	ファブリック インターコネクト上の管理ポートの IP サブネット マスク。
[Default Gateway] フィールド	ファブリック インターコネクト上の管理ポートに割り当てられるデフォルト ゲートウェイの IP アドレス。
[DNS Server IP] フィールド	ファブリック インターコネクト上の管理ポートに割り当てられる DNS サーバの IP アドレス。
[Domain name] フィールド	ファブリック インターコネクトが存在するドメインの名前。

ステップ 10 [送信（Submit）] をクリックします。
セットアップ操作の結果がページに表示されます。

Cisco UCS Manager GUI を使用したセカンダリ ファブリック インターコネクトの設定

セカンダリ ファブリック インターコネクトのコンソール ポートが、コンピュータまたはコンソール サーバに物理的に接続されていることを確認します。以前設定したプライマリ ファブリック インターコネクトでの管理者アカウントのパスワードを知っていることを確認します。

ステップ 1 コンソール ポートに接続します。詳細については、Cisco 6200 Series Fabric Interconnect Hardware Installation guideを参照してください。

ステップ 2 ファブリック インターコネクトの電源を入れます。ファブリック インターコネクトが起動する際、電源オン セルフテストのメッセージが表示されます。

ステップ 3 インストール方式プロンプトに *gui* と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

- ファブリック インターコネクトの管理ポートの IPv4 アドレス。
- ファブリック インターコネクトの管理ポートの IPv4 サブネット マスク。
- ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IPv4 アドレス。

（注） 設定時に両方のファブリック インターコネクトに同じ管理インターフェイスのアドレス タイプを割り当てる必要があります。

ステップ 5 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。

ステップ 6 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager 起動ページに移動します。

ステップ 7 **[Express Setup (Express セットアップ)]** を選択します。

ステップ 8 **[Initial Setup (初期セットアップ)]** を選択し、**[Submit (送信)]** をクリックします。

ファブリック インターコネクトは、第 1 ファブリック インターコネクトの設定情報を検出します。

ステップ 9 **[Cluster and Fabric Setup (クラスタおよびファブリック セットアップ)]** 領域で、次のフィールドに値を入力します。

名前	説明
[Enable Cluster (クラスタの有効化)] オプション	[Enable Cluster (クラスタの有効化)] オプションを選択します。
[Fabric Setup] オプション	*[Fabric B (ファブリック B)]* を選択します。

ステップ 10 **[System Setup (システム セットアップ)]** 領域の **[Admin Password of Master (マスターの管理者パスワード)]** フィールドに管理者アカウントのパスワードを入力します。**[Manager Initial Setup (Manager の初期セットアップ)]** 領域が表示されます。

ステップ 11 **[Manager Initial Setup (Manager の初期セットアップ)]** 領域で表示されるフィールドは、第 1 ファブリック インターコネクトを IPv4 のどちらの管理アドレスで設定したかによって異なります。次のように、設定に適したフィールドに入力します。

フィールド	説明
[Peer FI is IPv4 Cluster enabled. [local FI Mgmt0 IPv4 address (ローカル FI Mgmt0 IPv4 アドレス)] フィールドに入力してください。	ローカル ファブリック インターコネクトの Mgmt0 インターフェイスの IPv4 アドレスを入力します。

ステップ 12 [送信（Submit）] をクリックします。
セットアップ操作の結果がページに表示されます。

CLI を使用したプライマリ ファブリック インターコネクトの設定

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトが起動すると、電源投入時セルフテスト メッセージが表示されます。

ステップ 3 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

ステップ 4 **setup** と入力して、初期システム設定を続行します。

ステップ 5 **y** と入力して、初期設定を続行することを確認します。

ステップ 6 管理アカウントのパスワードを入力します。

ステップ 7 確認のために、管理アカウントのパスワードを再入力します。

ステップ 8 **yes** と入力して、クラスタ構成の初期設定を続行します。

ステップ 9 ファブリック インターコネクトのファブリックを入力します（**A** または **B**）。

ステップ 10 システム名を入力します。

ステップ 11 ファブリック インターコネクトの管理ポートの IPv4 アドレスを入力します。

IPv4 サブネット マスクを入力するように求められます。

ステップ 12 IPv4 サブネット マスクを入力し、**[Enter]** を押します。

ファブリックインターコネクトの管理ポート用に入力したアドレスタイプによって、デフォルト ゲートウェイの IPv4 アドレスを求められます。

ステップ 13 デフォルト ゲートウェイの IPv4 アドレスを入力します。

ステップ 14 DNS サーバの IP アドレスを指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。

ステップ 15 （任意） DNS サーバの IPv4 アドレスを入力します。

アドレス タイプはファブリック インターコネクトの管理ポートのアドレス タイプと同じである必要があります。

ステップ 16 デフォルトのドメイン名を指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。

ステップ 17 （任意） デフォルト ドメイン名を入力します。

ステップ 18 設定の概要を確認し、**yes** と入力して設定を保存および適用するか、**no** と入力して設定ウィザードを初めからやり直して設定を一部変更します。

設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

例

次に、コンソールおよび IPv4 管理アドレスを使用してクラスタ構成の最初のファブリック インターコネクトをセットアップする例を示します。

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup
or if you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Virtual IPv4 address: 192.168.10.12
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Management IP Address=192.168.10.10
  Management IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  Cluster Enabled=yes
  Virtual Ip Address=192.168.10.12
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

CLI を使用した従属ファブリック インターコネクトの設定

この手順は、管理ポートに対し IPv4 アドレスを使用して第 2 のファブリック インターコネクトをセットアップする方法について説明します。

（注） 新しいファブリック インターコネクトを既存の高可用性クラスタに追加する場合、たとえば、新規インストール時またはファブリック インターコネクトの交換時に、認証方式がリモートに設定されている限り、新しいデバイスはクラスタにログインできません。新しいファブリック インターコネクトをクラスタに正常に追加するには、認証方式を一時的にローカルに設定し、プライマリ ファブリック インターコネクトのローカル管理者資格情報を使用する必要があります。

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトが起動すると、電源投入時セルフテスト メッセージが表示されます。

ステップ 3 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

（注） ファブリック インターコネクトによって、クラスタ内のピア ファブリック インターコネクトが検出されます。検出されなかった場合は、L1 ポートと L2 ポート間の物理接続を調べ、ピア ファブリック インターコネクトがクラスタ設定でイネーブルになっていることを確認します。

ステップ 4 **y** と入力して、従属ファブリック インターコネクトをクラスタに追加します。

ステップ 5 ピア ファブリック インターコネクトの管理パスワードを入力します。

ステップ 6 従属ファブリック インターコネクト上の管理ポートの IP アドレスを入力します。

ステップ 7 設定の概要を確認し、 **yes** と入力して設定を保存および適用するか、 **no** と入力して設定ウィザードを初めからやり直して設定を一部変更します。

設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

例

次に、ピアのコンソールおよびIPv4アドレスを使用してクラスタ設定の第2のファブリック インターコネクトをセットアップする例を示します。

```
Enter the installation 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: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv4 Address: 192.168.10.11
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

コンソールのセットアップの確認

SSH 経由でファブリック インターコネクトにログインすることにより、両方のファブリック インターコネクトの設定が完全であることを確認できます。

Cisco UCS Manager CLI から次のコマンドを使用して、クラスタのステータスを確認します。

コマンド	目的	出力例

show cluster state	ハイ アベイラビリティ クラスタの両方のファブリック インターコネクトの動作状態およびリーダーシップ ロールを表示します。	次の例の表示では、両方のファブリック インターコネクトが Up 状態、HA が Ready 状態、ファブリック インターコネクト A がプライマリ ロール、ファブリック インターコネクト B が従属ロールです。
		`UCS-A# show cluster state`
		`Cluster Id:`
		`0x4432f72a371511de-0xb97c000de1b1ada4`
		
		`A: UP, PRIMARY`
		`B: UP,`
		`SUBORDINATE HA READY`

show cluster extended-state	クラスタの状態に関する拡張詳細が表示され、通常は問題のトラブルシューティングにこれが使用されます。	次の例は、クラスタの拡張状態の表示方法を示しています。
		`UCSC# show cluster extended-state 0x2e95deacbd0f11e2-0x8ff35147e84f3de2Start time: Thu May 16 06:54:22 2013Last election time: Thu May 16 16:29:28 2015System Management Viewing the Cluster State`
		`A: UP, PRIMARY`
		`B: UP, SUBORDINATE`
		
		`A: memb state UP, lead state PRIMARY, mgmt services state: UP`
		`B: memb state UP, lead state SUBORDINATE, mgmt services state: UP`
		`heartbeat state PRIMARY_OK`
		`HA READY`
		`Detailed state of the device selected for HA quorum data:`
		
		`Device 1007, serial: a66b4c20-8692-11df-bd63-1b72ef3ac801, state: active`
		`Device 1010, serial: 00e3e6d0-8693-11df-9e10-0f4428357744, state: active`
		`Device 1012, serial: 1d8922c8-8693-11df-9133-89fa154e3fa1, state: active`

HX シリーズ サーバと Cisco UCS ファブリック インターコネクトの接続

概要

Cisco HX220c および HX240c サーバは、ファブリック インターコネクトに直接接続します。直接接続を使用すれば、Cisco UCS Manager は、1 本のケーブルで HX シリーズ サーバの管理トラフィックとデータ トラフィックの両方を管理できます。

（注） サーバをファブリック インターコネクトに接続した後、そのサーバが検出された時点で、UCS Manager 設定フォームを使用して、Cisco UCS Manager で使用可能な C シリーズ ソフトウェア バンドルを更新します。

直接接続モードを使用する場合は、すべての Cisco UCS 管理対象アダプタをファブリック インターコネクト上のサーバ ポートに接続する必要があります。要件の章に列挙されている推奨ファームウェアが HX サーバにインストールされていることを確認してください。そうでない場合は、Cisco UCS Manager を使用してファームウェアを更新します。

（注） UCS の設定に関する次の制限事項に注意してください。

- Cisco HX に固有の UCS の設定に関する制限事項：HX M4 サーバーは 1227 VIC および 6332-16UP ファブリック インターコネクトと互換性がありません。
- Cisco UCS の設定に関する一般的な制限事項：Cisco UCS 6200、6332 および 6324 シリーズ Cisco UCS Manager コンフィギュレーション上限値ガイドを参照してください。

コンバージド ノードとファブリック インターコネクトの接続

このトピックでは、HX クラスタの作成や既存の HX クラスタへの追加を行うためにコンバージド ノードを物理的に追加する方法について説明します。

始める前に

重要

- Cisco UCS Manager と統合する前に、CIMC サーバを工場出荷時のデフォルトに設定します。
- 統合ノードでは、専用の CIMC ポートをネットワークに接続しないでください。これを行うと、サーバが Cisco UCS Manager で検出されなくなります。サーバが検出されない場合は、各サーバの CIMC を出荷時の設定にリセットします。
- 近い将来に FC ストレージを接続する必要がない場合は、ポート 1 ～ 16 のみを使用します。
- Cisco UCS FI 63xx および64xx では、ポート 1 ～ 6 を FC ポートとして設定することだけがサポートされています。今後 FC ストレージを接続する必要がある場合は、ポート 1 ～ 6 を FC に変換します。

（注） 変換により、HX の展開が中断される場合があります。

- CIMC サーバーを接続する前に、Cisco VIC 1227 が HXc240 の PCIe スロット 2 または HXc220 のライザ 1 スロット 1 に装着されており、Cisco UCS Manager と統合できることを確認します。カードが正しいスロットに装着されていないと、サーバの直接接続管理を有効にできません。
- サーバからファブリック インターコネクトへの物理的なケーブル接続を完了し、ポートをサーバ ポートとして設定します。

ステップ 1 ラックに HX サーバを設置します。詳細については、ラック設置型 Cisco HyperFlex ノード （41 ページ）を参照してください。

ステップ 2 ファブリック インターコネクト上のサーバ ポートを設定します。

a) サーバ上の 1 つのポートから 10-Gb SFP+ ケーブルをファブリック インターコネクト A に接続します。ファブリック インターコネクト A 上の任意のポートを使用できますが、サーバ トラフィックに対応可能なポートでなければなりません。

1 枚のカード用に、VIC からファブリック インターコネクトに 1 本のケーブルを接続します。両方のポートを同じファブリック インターコネクトに接続しないでください。

b) そのポートをサーバ ポートとして FI-A で設定します。詳細な手順については、『Cisco UCS Manager Network Management Guide』の「*Configuring Port Modes for a 6248 Fabric Interconnect*」を参照してください。

c) サーバ上のもう一方のポートから 10-Gb SFP+ ケーブルを FI B に接続します。FI B 上の任意のポートを使用できますが、サーバ トラフィックに対応可能なポートでなければなりません。

（注） アップリンクでSFP+タイプを混在させないでください。混在させると、「検出が失敗しました」というエラーが発生します。

d) そのポートをサーバ ポートとして FI-B で設定します。詳細な手順については、『Cisco UCS Manager Network Management Guide』の「*Configuring Port Modes for a 6248 Fabric Interconnect*」を参照してください。

ステップ 3 電源コードをノードの各電源装置に接続し、接地された AC 電源コンセントにも接続します。初期ブート時に、スタンバイ電源でノードが起動するまで約 2 分間待ちます。

（注）
1. 電力が供給されるようになると、ファブリック インターコネクトによってサーバが検出されます。UCS Manager でノードの検出を監視できます。
2. 前面パネルのノードの [電源ステータス LED（Power Status LED）] を調べて、ノードの電源ステータスを確認します。LED がオレンジ色の場合は、ノードがスタンバイ電源モードです。

ステップ 4 ステップ 1 ～ 4 を繰り返し、残りの HX シリーズ サーバを HyperFlex クラスタに接続します。

直接接続モードのクラスタ セットアップの物理的な接続の図

次の図は、C-Series Rack-Mount Serverと Cisco UCS Domain、Cisco UCS Manager リリース 3.1 以降との直接接続モードの物理接続の例を示しています。次の図は、UCS Manager と C-Series ラックマウント サーバを統合する場合の配線構成を示しています。金色で示されたパスでは、管理トラフィックとデータ トラフィックの両方が伝送されます。

図 *9*：直接接続ケーブル配線の設定

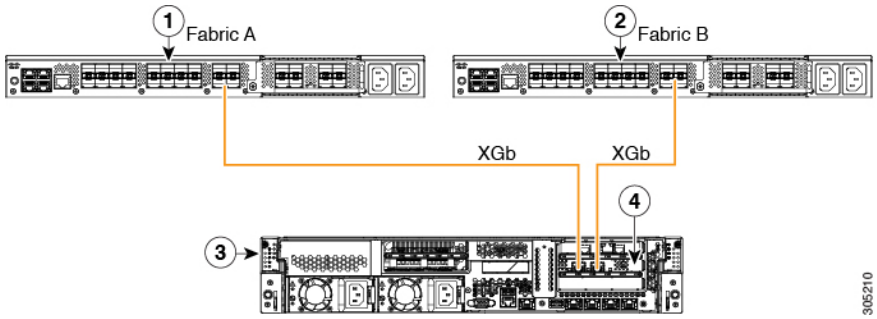
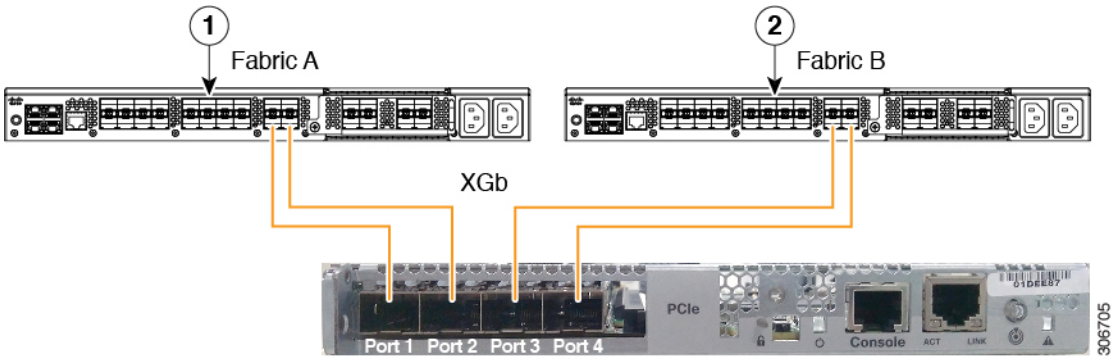


図 *10 : Cisco VIC 1455* との直接接続の配線構成



1	Cisco UCS 6454 ファブリック インターコネクトまたは Cisco UCS 6200、または 6300 シリーズ FI (ファブリック A)	3	C シリーズ ラックマウント サーバ
2	Cisco UCS 6454 ファブリック インターコネクトまたは Cisco UCS 6200 または 6300 シリーズ FI （ファブリック B）	4	サポート対象 PCIe スロット内の Cisco UCS VIC

XGb は 40 ギガビット イーサネット接続または 10 ギガビット イーサネット接続を表します。10 ギガビット イーサネットの場合、次のケーブルが使用されます。

- 4 X 10 ブレークアウト Small Form-Factor Pluggable（SFP）ケーブル
- 4 X 10 アクティブ光ケーブル（OAC）
- Qualified Security Assessor（QSA）モジュールを使用する 10G Small Form-Factor Pluggable（SFP）ケーブル

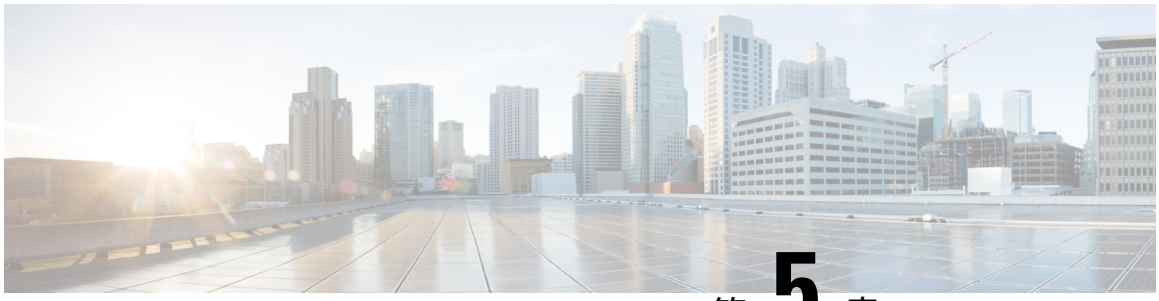
コンピューティング専用ノードとファブリックインターコネクトの接続

このトピックでは、既存の HyperFlex クラスタにコンピューティング専用ノードを物理的に追加する方法について説明します。

（注） HyperFlex ストレージ クラスタを作成して設定した後、HyperFlex クラスタにコンピュータ専用ノードを接続します。

1. HyperFlex ストレージ クラスタがすでに作成されていることを確認します。
2. コンピューティング ノードとなる HX サーバを接続します。コンピューティング専用ノードのインストールの詳細については、「ラック設置型 Cisco HyperFlex ノード （41 ページ）」を参照してください。

3. Cisco HX Data Platform を使用してクラスタ拡張ワークフローを実行します。コンピューティング専用ノードを追加するには、クラスタ拡張ワークフローを使用します。詳細な手順については、「既存のクラスタにコンピューティング専用ノードを追加する （176 ページ）」を参照してください。



第 5 章

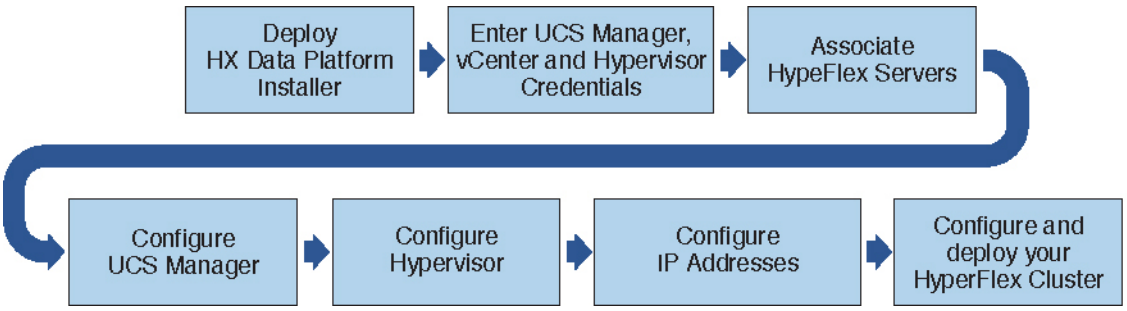
Cisco HyperFlex Systems の設定

この章では、Cisco HyperFlex System のコンポーネントの設定方法について説明します。

設置ワークフロー

（注） 以前に HyperFlex クラスタノードが他の HyperFlex クラスタの一部であった場合（または工場出荷前の場合）、クラスタの導入を開始する前にノードのクリーンアップ手順を実行します。詳細については、『HyperFlex Customer Cleanup Guides for FI and Edge』を参照してください。

次のインストール ワークフローは、HX データ プラットフォーム インストーラを使用して標準クラスタを作成する手順の概要です。



インストール時に従うワークフローは次のとおりです。

1. VSphere Web Client を使用して HX データ プラットフォーム インストーラ OVA を展開します。ハイパーバイザ ウィザードが新しい VM に IP アドレスを割り当てる際の DHCP に対してデフォルトの場合、静的 IP アドレスを持つ HX データ プラットフォーム インストーラ OVA を展開します。詳細については、vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開 （58 ページ） または 静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開 （61 ページ） を参照してください。
2. Syslog を設定して、syslog の一元的なリポジトリにすべてのログ情報を送信します。詳細については、Syslog の設定 （62 ページ）を参照してください。
3. UCS Manager、vCenter、およびハイパーバイザのクレデンシャルを入力します。
4. サーバー ポートを設定し、HyperFlex サーバーを関連付けます。詳細については、HyperFlex サーバの関連付け （63 ページ）を参照してください。
5. アウトオブバンド CIMC、iSCSi ストレージ、および FC ストレージの VLAN、MAC プール、' hx-ext-mgmt ' IPPool を設定します。詳細については、UCS Manager の設定 （65 ページ）を参照してください。
6. ハイパーバイザを設定します。詳細については、ハイパーバイザの構成 （69 ページ）を参照してください。
7. IP アドレスを設定します。詳細については、IP アドレスの設定 （71 ページ）を参照してください。
8. HyperFlex クラスタを設定し、展開します。詳細については、「HyperFlex クラスタの設定 （72 ページ）」を参照してください。

vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開

ESXi ホストに HX Data Platform をインストールするだけではなく、VMware Workstation、VMware Fusion または Virtual Box にも HX Data Platform インストーラを展開することができます。

（注）
- vCenter に接続して OVA ファイルを展開し、IP アドレス プロパティを指定します。ESXi ホストから直接展開しても、値を正しく設定することはできません。
- Cisco HX ストレージ クラスタ内のノードとなる ESXi サーバに HX Data Platform インストーラを展開しないでください。

ステップ 1 [ソフトウェアのダウンロード（Download Software）] で HX Data Platform インストーラ OVA ファイルを特定してダウンロードします。HX Data Platform ストレージ クラスタに使用されるストレージ管理ネットワーク上のノードに、HX Data Platform インストーラをダウンロードします。

```
Example:
Cisco-HX-Data-Platform-Installer-v4.5.1a-26363.ova
```

ステップ 2 VMware ハイパーバイザを使用して HX Data Platform インストーラを展開し、HX Data Platformインストーラ仮想マシンを作成します。

（注） 仮想ハードウェア リリース 10.0 以降をサポートする仮想化プラットフォームのリリースを使用してください。

vSphere はシステム要件です。vSphere シック クライアント、vSphere シン クライアント、または vSphere Web クライアントのいずれかを使用できます。HX Data Platform インストーラを展開するには、VMware Workstation、VMware Fusion、または VirtualBox を使用することもできます。

a) vSphere、VirtualBox、Workstation、Fusion などの仮想マシン ハイパーバイザを開きます。
b) HX Data Platform インストーラを展開するノードを選択します。

重要 vSphere Web Client を使用して HX インストーラ OVA を導入する際は、ユーザー クレデンシャルを必ず指定してください。

- vSphere シック クライアントを使用する—**[インベントリ リスト（Inventory list）]** > **[ホスト（Host）]** > **[ファイル（File）]** > **[OVA を展開（Deploy OVA）]** を展開します
- vSphere Web クライアントを使用する—**[vCenter インベントリ リスト（vCenter Inventory list）]** > **[ホスト（Hosts）]** > **[ホスト（Host）]** > **[OVA を展開（Deploy OVA）]** を展開します

ステップ 3 HX Data Platform インストーラの場所を選択します。デフォルト値を使用し、適切なネットワークを選択します。

ステップ 4 HX Data Platform インストーラ VM で使用する静的 IP アドレスを入力します。

（注）
- ネットワークで DHCP が設定されている場合でも、静的 IP アドレスが必要です。HX Data Platform インストーラを実行し、HX Data Platform をインストールし、HX Data Platform ストレージ クラスタを作成するには、静的 IP アドレスが必要です。
- 新しい VM への IP アドレス割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開 （61 ページ）の手順を実行して、静的 IP アドレスで HX Data Platform インストーラ VM をインストールします。インストーラ VM から DNS が到達可能である必要があります。

フィールド	説明
ホスト名	この VM のホスト名。 IP アドレスの逆引きを試みるには空白のままにします。
デフォルト ゲートウェイ	この VM のデフォルト ゲートウェイ アドレス。 DHCP を使用する場合は、空白のままにします。

フィールド	説明
DNS	この VM のドメイン ネーム サーバ（カンマ区切りリスト）。 DHCP を使用する場合は、空白のままにします。
IP アドレス	このインターフェイスの IP アドレス。 DHCP を使用する場合は、空白のままにします。
ネットマスク	このインターフェイスのネットマスクまたはプレフィックス。 DHCP を使用する場合は、空白のままにします。
Root パスワード	ルート ユーザー パスワード。 このフィールドは必須フィールドです。

ステップ 5 [次へ（Next）] をクリックします。リストされたオプションが正しいかどうか確認し、[導入後に電源をオンにする（Power on after deployment）] を選択します。

HX Data Platform インストーラを手動で電源オンにするには、仮想マシンのリストに移動し、インストーラ VM の電源をオンにします。

（注） HX Data Platform インストーラ仮想マシンの推奨設定は、3 つの vCPU と 4 GB のメモリです。これらの設定を小さくすると、CPU の使用率が 100% になり、ホストのスパイクが発生する可能性があります。

ステップ 6 [Finish] をクリックします。HX Data Platform インストーラ VM が vSphere インフラストラクチャに追加されるまで待ちます。

ステップ 7 HX Data Platform インストーラ仮想マシンを開きます。

初期コンソール画面に、HX Data Platform インストーラ仮想マシンの IP アドレスが表示されます。

```
Data Platform Installer.
****************************************
You can start the installation by visiting
the following URL:
http://192.168.10.210
****************************************
Cisco-HX-Data-Platform-Installer login:
```

ステップ 8 HX Data Platform インストーラにログインするための URL を使用します。

```
Example:
http://192.168.10.210
```

ステップ 9 自己署名証明書を受け入れます。

ステップ 10 ユーザー名 **root** と、OVA 導入の一部として設定したパスワードを使用してログインします。

静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開

新しい VM への IP アドレスの割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、以下の手順を使用して HX Data Platform インストーラを展開します。

ステップ 1 HX Data Platform ストレージ クラスタに使用されるストレージ管理ネットワーク上のノードに、VMware OVF Tool 4.1 以降をインストールします。詳細については、「OVF ツール ドキュメンテーション」を参照してください。

ステップ 2 VMware OVF がインストールされているノードの「ソフトウェアのダウンロード」から、HX Data Platform インストーラ OVA を見つけてダウンロードします。

ステップ 3 `ovftool` コマンドを使用して、ダウンロードした HX Data Platform インストーラ OVA を展開します。次に例を示します。

```
root@server:/tmp/test_ova# ovftool --noSSLVerify --diskMode=thin
--acceptAllEulas=true --powerOn --skipManifestCheck --X:injectOvfEnv
--datastore=qa-048-ssd1 --name=rfsi_static_test1 --network='VM Network'
--prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1
--prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8
--prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco
--prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5
--prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36
--prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0
--prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
vi://root:password@esx_server
```

このコマンドにより、HX Data Platform インストーラが展開され、HX Data Platform インストーラ VM の電源が入り、指定された静的 IP アドレスが設定されます。以下は処理応答の例です。

```
Opening OVA source:
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
Opening VI target: vi://root@esx_server:443/
Deploying to VI: vi://root@esx_server:443/
Transfer Completed
Powering on VM: rfsi_static_test
Task Completed
Completed successfully
```

インストーラ VM から DNS が到達可能である必要があります。静的 IP アドレスを正常に設定するために必要なコマンド オプションは以下のとおりです。

コマンド	説明
powerOn	HX Data Platform インストーラ VM の展開後に電源を投入します。
X:injectOvfEnv	HX Data Platform インストーラ VM に静的 IP のプロパティを挿入します。

コマンド	説明
prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1	適切なゲートウェイ IP アドレスを指定します。
prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8	適切な DNS IP アドレスを指定します。
prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco	適切なドメインを指定します。
prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5	適切な NTP IP アドレスを指定します。
prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36	適切なインストーラの静的IPアドレスを指定します。
prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0	適切なネットマスク アドレスを指定します。
prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword	root ユーザー パスワードを指定します。
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova	HX Data Platform インストーラ OVA の送信元アドレス。
vi://root:password@esx_server	HX データ プラットフォーム インストーラ VM がインストールされている宛先 ESX サーバ。適切な ESX サーバのルート ログイン クレデンシャルが含まれます。

Syslog の設定

集中型 syslog リポジトリにすべてのロギング情報を送信することをお勧めします。

注目 一般に、監査ログの長期保持が必要な場合は、syslog を使用した監査ログのエクスポートを設定することをお勧めします。特にSD カードから起動する HX220c ノードとコンピューティング専用ノード上で、永続ロギングに syslog 構成が必要です。Syslog サーバを設定しない場合、ログ ローテーション ポリシーにより監査ログが上書きされます。

（注） ESXi の永続的なスクラッチ ロケーションの宛先として NFS データストアを選択することはできません。永続的なスクラッチ ロケーションに HX データストアを選択すると、ESXi ホストのリロード後に削除されます。

すべての M5 および M6 サーバーについては、スクラッチとして使用するために M.2 ブート SSD が自動的に選択されます。これは、新しいインストールのボックスから設定されます。

HX240M4 (非 SED) の場合、固定ログ/スクラッチに Intel SSD が使用されます (220M5/240M5 では同じですが、異なるローカル SSD にも適用されます)。

HX220M4 および HX240M4 (SED) の場合、スクラッチ パーティションを保存する場所はありません。そのため、唯一のオプションは、ネットワーク上の永続的なロギングに syslog を使用することです。

ステップ 1 syslog サーバが稼動していること、および ESXi サーバからログを受信するために TCP/UDP ポートが開いていることを確認してください。

ステップ 2 ESXi シェルに SSH 接続して、次のコマンドを実行します。

```
a) esxcli system syslog config set --loghost='udp://remote-syslog-server-ip'
b) esxcli system syslog reload
c) esxcli network firewall ruleset set -r syslog -e true
d) esxcli network firewall refresh
```

ステップ 3 クラスタ内のすべての ESXi ホストに対してステップ 1 ～ 2 を繰り返します。

ステップ 4 リモート syslog サーバで、指定されたディレクトリにログが受信されているかどうかを確認します。

HyperFlex クラスタの設定と展開

HyperFlex サーバの関連付け

[サーバの選択（Server Selection）] ページで、右側にある [構成（Configuration）] ペインの [クレデンシャル（Credentials）] に、使用されているクレデンシャルの詳細なリストが表示されます。[サーバの選択（Server Selection）] ページの [関連付けなし（Unassociated）] タブには、関連付けられていない HX サーバのリストが表示され、[関連付け済み（Associated）] タブには検出されたサーバのリストが表示されます。

フィールド	説明
ロケータ LED（Locator LED）	サーバーの検索をオンにします。
サーバー名（Server Name）	サーバーに割り当てられた名前。
Status（ステータス）	• アクセス不可—

フィールド	説明
モデル（**Model**）	サーバー モデルが表示されます。
シリアル（**Serial**）	サーバーのシリアル番号を表示します。
関連付けのステータス（**Assoc State**）	• 関連 • 関連付けなし
サービス プロファイル（Service Profile）（関連付けられたサーバーに対してのみ）	サーバーに割り当てられているサービス プロファイル。 （注） HyperFlex サービス プロファイル テンプレートの編集はお勧めしません。
アクション（**Actions**）	• **[KVM コンソールの起動（Launch KVM Console）]**: HX Data Platform から直接 KVM コンソールを起動するには、このオプションを選択します。 • [サーバの関連付け解除（Disassociate Server）]: サーバからサービス プロファイルを削除するには、このオプションを選択します。

始める前に

UCS Manager、vCenter、およびハイパーバイザ クレデンシャルの入力を完了していることを確認します。

ステップ 1 [サーバ ポートの構成（Configure Server Ports）] をクリックして新しい HX ノードを検出します。[サーバ ポートの構成（Configure Server Ports）] ダイアログボックスに、サーバ ポートとして構成されるすべてのポートが一覧表示されます。[構成（Configure）] をクリックします。

（注） 一般的に、構成を始める前に、サーバ ポートは Cisco UCS Manager で構成されます。

ステップ 2 HyperFlex クラスタに含める **[関連付けなし（Unassociated）]** タブの下のサーバを選択します。

HX サーバがこのリストに表示されない場合は、[Cisco UCS Manager] をオンにして、検出されていることを確認します。

（注） 関連付けられていないサーバがない場合は、次のエラー メッセージが表示されます。

```
No unassociated servers found. Login to UCS Manager and ensure server ports are enabled.
```

ステップ 3 [続行（Continue）] をクリックして、UCS Manager の構成を続けます。「UCS Manager の設定 （65 ページ）」を参照してください。

UCS Manager の設定

[UCSM 構成（UCSM Configuration）] ページでは、CIMC、iSCSi ストレージ、FC ストレージに関する VLAN、MAC プール、「hx-ext-mgmt」IP プールを構成できます。

始める前に

HyperFlex クラスタにサーバを関連付けます。HyperFlex サーバの関連付け （63 ページ）を参照してください。

ステップ 1 [VLAN 設定（VLAN Configuration）] セクションで、次のフィールドに値を入力します。

（注） 次のそれぞれのネットワークに、別個のサブネットと VLAN を使用します。

フィールド	説明
ハイパーバイザとHyperFlex管理用のVLAN	
VLAN 名	hx-inband-mgmt
VLAN ID（Admin. VLAN ID）	デフォルト：3091
HyperFlexストレージトラフィック用のVLAN	
VLAN 名	hx-storage-data
VLAN ID（Admin. VLAN ID）	デフォルト: 3092
VM vMotion用のVLAN	
VLAN 名	hx-vmotion
VLAN ID（Admin. VLAN ID）	デフォルト: 3093
VMネットワーク用のVLAN	
VLAN 名	vm-network
VLAN ID	デフォルト: 3094 ゲスト VLAN のカンマ区切りリスト。

ステップ 2 [MAC プール（MAC Pool）] セクションの [MAC プールのプレフィックス（MAC Pool Prefix）] で、追加の 2 つの 16 進文字（0 ～ F）を指定して MAC プールのプレフィックスを構成します。

（注） すべての UCS ドメインにわたり、他の MAC アドレス プールで使用とされていないプレフィックスを選択します。

```
Example:
00:25:B5:A0:
```

ステップ 3 **[CIMC の 'hx-ext-mgmt' IP プール（'hx-ext-mgmt' IP Pool for CIMC）]** セクションで、次のフィールドに値を入力します。

フィールド	説明
[IP Blocks]	各 HyperFlex サーバーの CIMC に割り当てられた管理 IP アドレスの範囲。IP アドレスは範囲として指定し、複数の IP ブロックをカンマ区切りのリストとして指定できます。クラスタ内のサーバごとに少なくとも 1 つの一意の IP があることを確認します。アウトオブバンドの使用を選択する場合、この範囲はファブリック インターコネクトの mgmt0 インターフェイスで使用されているものと同じ IP サブネットに属している必要があります。 たとえば、*10.193.211.124-127, 10.193.211.158-163* などです。
[Subnet Mask]	上記の IP 範囲のサブネット マスクを指定します。 たとえば、 *255.255.0.0* とします。
[ゲートウェイ（Gateway）]	ゲートウェイの IP アドレスを入力します。 たとえば、*10.193.0.1* とします。

サーバー上の CIMC へのアクセスに使用される管理 IP アドレスは、次のいずれかです。

- **アウトオブバンド**：CIMC 管理トラフィックは、ファブリック インターコネクト上の制限帯域幅管理インターフェイス mgmt0 を介してファブリック インターコネクトを通過します。このオプションは最も一般的に使用され、ファブリック インターコネクト管理 VLAN と同じ VLAN を共有します。
- **インバンド**：CIMC 管理トラフィックは、ファブリック インターコネクトのアップリンク ポートを介してファブリック インターコネクトを通過します。この場合、管理トラフィックに使用できる帯域幅は、ファブリック インターコネクトのアップリンク帯域幅に相当します。インバンド オプションを使用している場合、Cisco HyperFlex インストーラは CIMC 管理通信専用の VLAN を作成します。このオプションは、Windows Server インストール ISO などの大きなファイルを OS インストール用の CIMC にマウントする必要がある場合に便利です。このオプションは、HyperFlex インストーラ VM でのみ使用でき、Intersight を介した展開には使用できません。

ステップ 4 CIMC 管理アクセスに使用する接続のタイプに基づいて、**アウトオブバンド** または **インバンド** を選択します。[インバンド（In-band）] を選択した場合は、管理 VLAN の VLAN ID を指定します。シームレスな接続のために、アップストリーム スイッチに CIMC 管理 VLAN を作成してください。

ステップ 5 外部ストレージを追加する場合は、次のフィールドに値を入力して [iSCSI ストレージ（iSCSI Storage）] を構成します。

フィールド	説明
[iSCSI ストレージの有効化（Enable iSCSI Storage）] チェックボックス	iSCSI ストレージを構成する場合、このチェックボックスをオンにします。
VLAN A 名（VLAN A Name）	プライマリ ファブリック インターコネクト（FI-A）で、iSCSI vNIC に関連付けらている VLAN の名前。
VLAN A ID	プライマリ ファブリック インターコネクト（FI-A）で、iSCSI vNIC に関連付けらている VLAN の ID。
VLAN B 名（VLAN B Name）	下位のファブリック インターコネクト（FI-B）で、iSCSI vNIC に関連付けらている VLAN の名前。
[VLAN B ID]	下位のファブリック インターコネクト（FI-A）で、iSCSI vNIC に関連付けらている VLAN の ID。

ステップ 6 外部ストレージを追加する場合は、次のフィールドに値を入力して [FC ストレージ（FC Storage）] を構成します。

フィールド	説明
[FC ストレージの有効化（Enable FC Storage）] チェックボックス	FC ストレージを有効にするには、このチェックボックスをオンにします。
WWxNプール	WW ノード名と WW ポート名の両方を含む WWN プール。それぞれのファブリック インターコネクトに対し、WWPN および WWNN 用の WWxN プールが作成されます。
VSAN A 名（VSAN A Name）	プライマリ ファブリック インターコネクト（FI-A）の VSAN の名前。 デフォルト—`hx-ext-storage-fc-a`。
VSAN A ID	プライマリ ファブリック インターコネクト（FI-A）のネットワークに割り当てられた一意の ID。 **注意** UCS または HyperFlex システムで現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。

フィールド	説明
VSAN B名	下位のファブリック インターコネクト（FI-B）の VSAN の名前。 デフォルト—`hx-ext-storage-fc-b`.
VSAN B ID	下位のファブリック インターコネクト（FI-B）のネットワークに割り当てられた一意の ID。 **注意** UCS または HyperFlex システムで現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。

ステップ 7 [詳細設定（Advanced）] セクションで、次の操作を行います。

フィールド	説明
UCS サーバー ファーム ウェアバージョン（UCS Server Firmware Version）	ドロップダウン リストから、HX サーバと関連付ける UCS サーバ ファームウェア バージョンを選択します。UCS ファームウェア バージョンは、UCSM バージョンと一致する必要があります。詳細については、最新の『Cisco HX Data Platform Release Notes』を参照してください。 たとえば、*3.2(1d)* とします。
HyperFlexクラスタ名	ユーザ定義の名前を指定します。HyperFlex クラスタ名は、特定のクラスタ内の HX サーバ グループに適用されます。HyperFlex クラスタ名によりサーバ プロファイルにラベルが追加され、クラスタを識別しやすくなります。
組織名	HyperFlex 環境を UCS ドメインの残りの部分から確実に分離できるような一意の組織名 を指定します。

ステップ 8 [続行（Continue）] をクリックして、ハイパーバイザの構成を続けます。「ハイパーバイザの構成 （69 ページ）」を参照してください。

ハイパーバイザの構成

（注） [ハイパーバイザの構成（Hypervisor Configuration）] ページの [構成（Configuration）] ペインで、VLAN、MAC プル、IP アドレス プールの情報を確認します。これらの VLAN ID は、環境によって変更されている可能性があります。デフォルトでは、HX Data Platform インストーラが VLAN を非ネイティブとして設定します。トランク構成を適切に適用することで、非ネイティブ VLAN に対応するアップストリーム スイッチを構成する必要があります。

注目 再インストールの場合、ESXi ネットワーキングが完了していれば、ハイパーバイザの構成をスキップできます。

始める前に

アウトオブバンド CIMC の VLAN、MAC プール、「hx-ext-mgmt」IP プールを構成します。外部ストレージを追加する場合は、iSCSI ストレージと FC ストレージを構成します。UCS サーバのファームウェア バージョンを選択し、HyperFlex クラスタの名前を割り当てます。UCS Manager の設定 （65 ページ）を参照してください。

ステップ 1 [共通ハイパーバイザ設定の構成（Configure Common Hypervisor Settings）] セクションで、次のフィールドに値を入力します。

フィールド	説明
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、*255.255.0.0* とします。
[ゲートウェイ（Gateway）]	ゲートウェイの IP アドレス。 たとえば、*10.193.0.1* とします。

フィールド	説明
[DNSサーバ（DNS Server(s)）]	DNS サーバの IP アドレス。 （注） • DNS サーバを使用しない場合、HX Data Platform インストーラの **[クラスタの設定（Cluster Configuration）]**ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。 • 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。

ステップ 2 [ハイパーバイザ設定（Hypervisor Settings）] セクションで、[IP アドレスとホスト名を順番に選択（Make IP Addresses and Hostnames Sequential）] を選択し、連続的な IP アドレスにします。次のフィールドに入力します。

（注） ドラッグ アンド ドロップ操作を使用してサーバの順番を並び替えることができます。

フィールド	説明
名前（Name）	サーバーに割り当てられた名前。
ロケータ LED（Locator LED）	サーバーの検索をオンにします。
シリアル（Serial）	サーバーのシリアル番号を表示します。
スタティックIPアドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。
ホスト名	ホスト名フィールドを空のままにしないでください。

ステップ 3 [続行（Continue）] をクリックして、IP アドレスの構成を続けます。「IP アドレスの設定 （71 ページ）」を参照してください。

IP アドレスの設定

始める前に

[ハイパーバイザ設定（Hypervisor Configuration）] ページでハイパーバイザの設定が完了していることを確認します。ハイパーバイザの構成 （69 ページ）を参照してください。

ステップ 1 [IP アドレス（IP Addresses）] ページで、[IP アドレスを連続させる（Make IP Addresses Sequential）] を選択し、連続的な IP アドレスにします。

ステップ 2 ハイパーバイザ、ストレージ コントローラ（管理）とハイパーバイザ、ストレージ コントローラ（データ）列の最初の行に IP アドレスを入力すると、 HX Data Platform Installer により、残りのノードのノード情報が増分されて自動入力されます。ストレージ クラスタ内のノードの最小数は 3 です。それより多くのノードがある場合は、**[追加（Add）]** ボタンを使用して、アドレス情報を指定します。

（注） コンピューティング専用ノードは、ストレージ クラスタを作成してからでないと追加できません。

各 HX ノードについて、ハイパーバイザ、ストレージ コントローラ、管理、データ IP アドレスを入力します。IP アドレスには、ネットワークがデータ ネットワークと管理ネットワークのどちらに属しているかを指定します。

フィールド	説明
管理ハイパーバイザ	ESXi ホストとストレージ コントローラ間のハイパーバイザ管理ネットワーク接続を処理するスタティック IP アドレスを入力します。
管理ストレージコントローラ	ストレージ コントローラ VM とストレージ クラスタ間のストレージ コントローラ VM 管理ネットワーク接続を処理する静的 IP アドレスを入力します。
Data Hypervisor	ESXi ホストとストレージ コントローラ間のハイパーバイザ データ ネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージ コントローラ	ストレージ コントローラ VM とストレージ クラスタの間のストレージ コントローラ VM データ ネットワーク接続を処理するスタティック IP アドレスを入力します。

ステップ 3 ここで指定する IP アドレスは、ストレージ クラスタ内の 1 つのノードに適用されます。ノードが使用できなくなった場合は、該当する IP アドレスがストレージ クラスタ内の別のノードに移動されます。すべてのノードには、これらの IP アドレスを受け入れるように構成されたポートが必要です。

次の IP アドレスを指定します。

フィールド	説明
管理クラスタ データの IP アドレス（Management Cluster Data IP Address）	HXデータ プラットフォーム ストレージ クラスタの管理ネットワーク IP アドレスを入力します。
データ クラスタ データ IP アドレス（Data Cluster Data IP Address）	HX Data Platform ストレージ クラスタのデータ ネットワークの IP アドレスを入力します。
管理サブネットマスク	VLAN と vSwitch のサブネット情報を入力します。 管理ネットワークの値を入力します。たとえば、*255.255.255.0* と入力します。
データサブネットマスク	データ ネットワークのネットワークの値を入力します。たとえば、*255.255.255.0* と入力します。
管理ゲートウェイ	管理ネットワークのネットワークの値を入力します。たとえば、*10.193.0.1* とします。
データゲートウェイ	データ ネットワークのネットワークの値を入力します。たとえば、*10.193.0.1* とします。

ステップ 4 [続行] をクリックして HyperFlex クラスタを設定します。「HyperFlex クラスタの設定 （72 ページ）」を参照してください。

HyperFlex クラスタの設定

[クラスタ構成（Cluster Configuration）] ページで、Cisco HX ストレージ クラスタに関する以下のフィールドに値を入力し、HyperFlex クラスタの導入を開始します。

始める前に

[IP アドレス（IP Addresses）] ページで IP アドレスの構成が完了していることを確認します。IP アドレスの設定 （71 ページ）を参照してください。

ステップ 1 [Cisco HX クラスタ（Cisco HX Cluster）] セクションで、次のフィールドに値を入力します。

フィールド	説明
クラスタ名（Cluster Name）	HXデータ プラットフォーム ストレージ クラスタの名前を指定します。

フィールド	説明
レプリケーション ファクタ（**Replication Factor**）	ストレージクラスタ全体でのデータの冗長レプリカの数を指定します。レプリケーションファクタを冗長レプリカ数 2 または 3 に設定します。 • ハイブリッド サーバ（SSD と HDD を含むサーバ）の場合、デフォルト値は 3 です。 • フラッシュ サーバー（SSD のみを含むサーバー）の場合は、2 または 3 を選択します。 • Hyperflex Edge を除くすべての環境で複製ファクタ 3 を強く推奨しています。複製ファクタ 2 では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。

ステップ 2 **[コントローラ VM（Controller VM）]**セクションで、HyperFlex クラスタの管理者ユーザの新しいパスワードを作成します。

コントローラ VM には、デフォルトの管理者ユーザ名とパスワードが適用されます。VM は、コンバージド ノードとコンピューティング専用ノードのすべてにインストールされます。

重要
- コントローラ VM またはコントローラ VM のデータストアの名前を変更することはできません。
- すべてのコントローラ VM に同じパスワードを使用します。異なるパスワードの使用はサポートされていません。
- 1 つの大文字、1 つの小文字、1 つの数字、1 つの特殊文字を含む、10 文字以上の複雑なパスワードを指定してください。
- コントローラ VM と、作成される HX クラスタには、ユーザ定義のパスワードを指定できます。パスワードに使用できる文字と形式に関する制限事項については、『*Cisco HX Data Platform Management Guide*』のセクション「Guidelines for HX Data Platform Special Characters」を参照してください。

ステップ 3 [vCenter の設定（vCenter Configuration）] セクションで、次のフィールドに値を入力します。

フィールド	説明
vCenter データセンター名（vCenter Datacenter Name）	Cisco HyperFlex クラスタの vCenter データセンターの名前を入力します。
vCenter クラスタ名（vCenter Cluster Name）	vCenter クラスタ名を入力します。

ステップ 4 [システム サービス（System Services）] セクションで、次のフィールドに値を入力します。

DNS サーバー（DNS Server(s)）	各 DNS サーバーの IP アドレスのカンマ区切りリスト。
NTP サーバー（NTP Server(s)）	各 NTP サーバの IP アドレスのカンマ区切りリスト。 （注） すべてのホストが同じ NTP サーバを使用して、ストレージ コントローラ VM と ESXi ホストで実行されているサービスの間でクロックを同期する必要があります。
DNS ドメイン名（DNS Domain Name）	DNS FQDN または IP アドレスが無効です
タイム ゾーン（Time Zone）	コントローラ VM のローカル タイム ゾーン。このタイム ゾーンに基づいて、スケジュールされたスナップショットを取るタイミングが決定されます。スケジュールされたネイティブ スナップショット アクションは、この設定に基づきます。

ステップ 5 [**コネクテッド サービス (Connected Services)**] セクションで、[**コネクテッド サービスを有効にする (Enable Connected Services)**] を選択して、自動サポート (Auto Support) および Intersight Management を有効にします。

フィールド	説明
コネクテッド サービスの有効化（Enable Connected Services）（推奨）	自動サポート (Auto Support) および Intersight Management を有効にします。HX Connect にログオンしてこれらのサービスを構成するか、またはそれらを選択的に**オン**または**オフ**にします。
サービス チケット通知の送信先（Send service ticket notifications to）	自動サポートによってトリガーされたときに SR 通知が送信される電子メール アドレス。

ステップ 6 [詳細設定（Advanced）] セクションで、次の操作を行います。

フィールド	説明
ジャンボ フレーム **ジャンボ フレームを有効化（Enable Jumbo Frames）**	ホスト vSwitches と vNIC、および各ストレージ コントローラ VM 上のストレージ データ ネットワークの MTU サイズを設定する場合は、このチェックボックスをオンにします。 デフォルト値は 9000 です。 （注） MTU サイズを 9000 以外の値に設定するには、Cisco TAC にご連絡ください。

フィールド	説明
ディスク パーティション ディスク パーティションのクリーン アップ（**Clean up Disk Partitions**）	ストレージクラスタに追加されたすべてのノードから既存のデータとパーティションをすべて削除して手動でサーバを準備する場合は、このチェックボックスをオンにします。既存のデータやパーティションを削除するには、このオプションを選択します。保持する必要があるデータはすべてバックアップする必要があります。 **注目** 工場で準備されたシステムの場合は、このオプションを選択しないでください。工場で準備されたシステムのディスクパーティションは正しく設定されています。
仮想デスクトップ**(VDI)**	VDI のみの環境でオンにします。 （注） ストレージ クラスタの作成後に VDI 設定を変更するには、リソースをシャットダウンまたは移動し、変更を加え (下の手順に記載)、クラスタを再起動します。 デフォルトでは、HyperFlex クラスタは VSI ワークロード用にパフォーマンス調整されるように設定されています。 このパフォーマンスのカスタマイズは、Hyperflex Data Platform クラスタで次の手順を実行することによって変更できます。HyperFlex クラスタを VDI から VSI ワークロード (またはその逆) に変更するには、次のようにします。 警告: メンテナンス ウィンドウが必要です。これにより、クラスタがオフラインの間はデータが使用できなくなります。 **1.** `~#stcli cluster shutdown` を実行してクラスタをシャット ダウンします。 **2.** すべてのコントローラ VM の storfs cfg を編集し、workloadType を Vsi または Vdi に変更します。 **3.** クラスタの作成後に、クラスタを起動し (`stcli cluster start`)、調整の変更を有効にします。

フィールド	説明
(オプション) vCenter Server のシングル サインオン（vCenter Single-Sign-On Server）	この情報は、SSO URL が到達可能でない場合のみ必要です。 （注） このフィールドは使用しないでください。これはレガシー展開に使用されます。 **[vCenter Server]** > **[Manage]** > **[Advanced Settings]** > **[key config.vpxd.sso.sts.uri]** にナビゲートして、vCenter で SSO URL を見つけることができます。

ステップ 7 **[開始（Start）]** をクリックして HyperFlex クラスタの展開を開始します。[進捗状況（Progress）] ページには、さまざまな設定タスクの進捗状況が表示されます。

注意 確認に関する警告を無視しないでください。

詳細については、「**警告**」セクションを参照してください。

次のタスク

- 検証エラーによっては、パラメータの再入力が必要になることがあります（たとえば、無効な ESXi パスワード、誤った NTPサーバ、不良 SSO サーバなどの誤った入力が原因のエラー）。**[値の再入力（Re-enter Values）]** をクリックして **[クラスタ構成（Cluster Configuration）]** ページに戻り、問題を解決します。
- これが完了すると、HyperFlex サーバがインストールされ、構成されます。正常にデプロイされたクラスタのステータスは、[オンライン（Online）] および [正常（Healthy）] として示されます。
- [HyperFlex Connect の起動 （Launch HyperFlex Connect）] をクリックし、データストアを作成してクラスタを管理します。

GPU が搭載された HyperFlex ノードのインストール

GPU が搭載された HyperFlex ノードをインストールする際は、特定の BIOS ポリシーを変更する必要があります。サポートされているすべての GPU カードで、4 GB 以上のメモリ マップド I/O（MMIO）を許可する BIOS 設定を有効にする必要があります。詳細については、「サポートされているすべての GPU に関する要件」を参照してください。

HyperFlex クラスタ作成後の GPU のインストール

クラスタの作成後に GPU をインストールする場合は、サーバに関連付けられたサービス プロファイルを変更して、BIOS ポリシー設定を有効にする必要があります。

「Cisco UCS Manager で制御されるサーバ」の記述に従って、BIOS 設定を有効にします。ステップ *3* で指定したように、4 GB を超えるメモリ マップド I/O を [有効（Enabled）] に設定します。

HyperFlex クラスタ作成前の GPU のインストール

クラスタの作成前に GPU カードをインストールする場合は、クラスタの作成中に、[高度なワークフロー（Advanced workflow）] を選択します。

1. HX データ プラットフォーム インストーラ ページで、[私は自分のやっていることがわかっているので、ワークフローをカスタマイズできるようにしてください（I know what I'm doing, let me customize my workflow）] を選択します。
2. [UCS マネージャ設定の実行（Run UCS Manager Configuration）] をクリックし、[続行（Continue）] をクリックします。

   これにより、HyperFlex ノードに必要なサービス プロファイルが作成されます。
3. 「Cisco UCS Manager で制御されるサーバ」の記述に従って、BIOS 設定を有効にします。ステップ *3* で指定したように、4 GB を超えるメモリ マップド I/O を [有効（Enabled）] に設定します。
4. HX データ プラットフォーム インストーラ ページの [高度なワークフロー（Advanced workflow）] に戻って、[ESX 設定の実行（Run ESX Configuration）]、[HX ソフトウェアの展開（Deploy HX Software）]、および [HX クラスタの作成（Create HX Cluster）] に進み、クラスタの作成を完了します。

HX Data Platform インストーラのナビゲーション支援ボタン

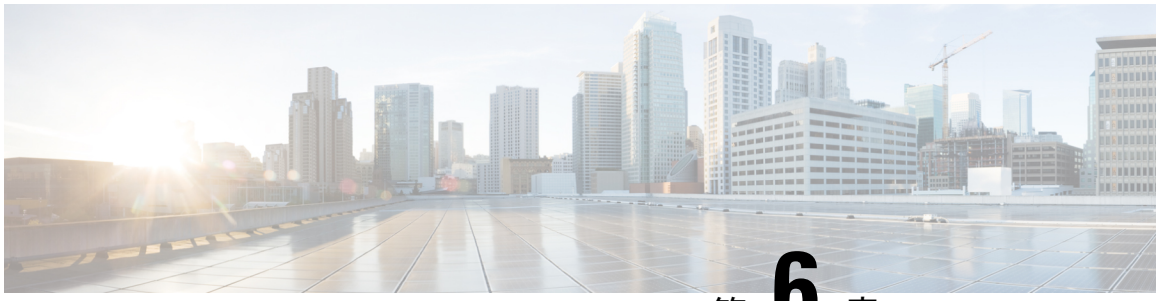
- **エクスポート設定（Export Configuration）**：JSON 設定ファイルをダウンロードするには、下矢印アイコンをクリックします。
- **ワークフロー情報（Workflow Info）**：現在のワークフローを表示するには、情報アイコンの上にカーソルを移動します。HyperFlex クラスタの作成に関するワークフロー情報は [ワークフローの作成 = Esx（Create Workflow = Esx）] です。
- **テクニカル サポート（Tech Support）**：HyperFlex Data Platform ソフトウェアのバージョンに関連する詳細を表示するには、疑問符アイコンをクリックします。Cisco TAC 用にテクニカル サポート バンドルを作成するには、[新しいバンドルの作成（Create New Bundle）] をクリックします。

- **変更の保存（Save Changes）**：HyperFlex クラスタの設定パラメータの変更内容を保存するには、円アイコンをクリックします。
- **設定（Settings）**：**もう一度やり直す**か、または**ログアウトする**には、歯車アイコンをクリックします。

警告およびエラー メッセージ

- UCSM の設定とハイパーバイザの設定は正常に完了したものの、導入またはクラスタ作成は失敗した：**[設定アイコン（Settings Icon）]>[初めからやり直す（Start Over）]** をクリックします。[操作内容を理解しているのでワークフローをカスタマイズします（I know what I'm doing, let me customize my workflow）] を選択すると、障害が発生した時点からクラスタの設定を開始できます。
- 値の再入力のために戻ると、IP アドレス画面が空白になっている：IP アドレスを手動で追加します。[サーバの追加（Add Server）] をクリックし、クラスタに含めるサーバをそれぞれ追加して、すべての IP アドレスをこのページで再入力します。
- インストーラ VM で DNS が正しく設定されていない（SSO エラー）ときに、サーバ到達可能性の問題が見られる：[SSO] フィールドを手動で編集して FQDN の代わりに IP アドレスを使用するか、DNS 設定をトラブルシューティングして修正します。
- 別のクラスタを作成するときに、Cisco HyperFlexバージョンに一致する Cisco UCS Manager バージョンが選択されていることを確認してください。一致するバージョンが選択されていない場合は、正しいバージョンを手動で入力します。

  現在の互換性マトリックスについては、『Release Notes for Cisco HX Data Platform』のソフトウェア バージョンの表を参照してください。



第 6 章

HyperFlex Data Platform でのライセンス設定

スマート ライセンスと HyperFlex

概要

シスコ スマート ソフトウェア ライセンシング（スマート ライセンス）はインテリジェントなソフトウェア ライセンス管理システムで、組織全体でライセンスを調達、導入、管理するなど、時間のかかる手動のライセンス タスクを自動化します。ライセンスの所有権と使用状況が可視化されるので、何を所有し、どのくらい使用しているかを把握できます。

スマート ライセンシングは、企業全体のライセンス プーリングを導入します。サーバ ベースのライセンスやスマート ライセンスは、デバイスにノードロックされないので、企業が所有する互換性のあるデバイスでこれらを使用できます。仮想アカウントを使用して、会社のライセンスと製品インスタンスを論理エンティティ（事業単位、製品タイプ、IT グループなど）に体系化すると、仮想アカウント間でデバイスとライセンスを簡単に移転できるようになります。

スマート ライセンシング機能は Cisco HyperFlex に統合されており、HX ストレージ クラスタを作成するとすぐに自動的に有効になります。HX ストレージ クラスタでライセンス消費の報告を開始するには、Cisco スマート アカウントを介して Cisco Smart Software Manager（SSM）に登録する必要があります。スマート アカウントは、会社全体のシスコ ソフトウェア ライセンスと製品インスタンスに関する完全な可視性とアクセス制御を提供するクラウドベースのリポジトリです。登録は、1 年間有効です。

登録すると、HyperFlex がスマート アカウントで識別され、ライセンス使用状況が Cisco Smart Software Manager または Smart Software Manager サテライトに報告されるようになります。登録後、HyperFlex はライセンス使用状況と現在のライセンス ステータスを Cisco Smart Software

Manager または Smart Software Manager サテライトに報告します。詳細については、以下のライセンス ステータス セクションを参照してください。

（注） これを機能させるには、すべての HyperFlex 管理 IP のポート 80 および 443 を `tools.cisco.com` に対して開く必要があります。

HX ストレージ クラスタを登録した後、Cisco Smart Software Manager または Smart Software Manager サテライトに対して HyperFlex を特定するために使われる証明書が通信メッセージに署名します。HyperFlex は次の要求を自動的に送信します。

- 6 か月ごとの登録更新要求。自動登録更新が発生しない場合は、`stcli license renew id` コマンドを使用して手動で更新してください。
- スマート ライセンシングでは、30 日ごとの承認更新要求が必要とされます。自動承認更新が発生しない場合は、`stcli license renew auth` コマンドを使用して手動で更新してください。スマートライセンシング承認を手動で更新する必要があるのは、更新しようとしたときに接続が使用不可である場合、または更新時刻が接続ウィンドウの範囲外である場合のみです。
- さらに、ライセンスの使用状況が変化するたびに、承認更新要求が Cisco Smart Software Manager または Smart Software Manager サテライトに送信されます。この承認は、90 日間有効です。90 日間承認を更新するよう HyperFlex が Cisco Smart Software Manager または Smart Software Manager サテライトに連絡しない場合は、HyperFlex によって消費されたライセンスが回収され、プールに戻されます。

ライセンスステータス

登録ステータス	説明	ステータスの検証	システム機能

評価モード	スマート ライセンシングは有効になっていますが、HX ストレージ クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されておらず、90 日間の評価期間内です。	ステータスを検証するか、または評価期間の残り時間を確認するには、次を実行します。
		`#stcli license show all`
		`Result: Mode = Eval & Remaining period(Number of Days:Hours:Minutes)`
			特性や機能には影響ありません。

登録ステータス	説明	ステータスの検証	システム機能
評価期限切れ	スマート ライセンシングは有効になっていますが、HX ストレージ クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていません。ライセンスは初期未確認状態です。コンプライアンス違反とは見なされません。	ステータスを検証するには、`#stcli license show all` を実行します。 `Result: Mode = Evaluation Expired`	特性や機能には影響ありません。 • Syslog メッセージを生成します。 • HX Connect UI で評価期限切れアラームを生成します。
適合	スマート ライセンシングが有効で、HX ストレージ クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されています。所有している数よりも少ないライセンスを消費しています。	—	—
HyperFlex リリース 5.0(2a) 以降は**[コンプライアンス違反（Out of Compliance）]**	-	-	特徴と機能への影響については、ライセンスの遵守とフィーチャの機能（84 ページ） セクションを参照してください。

登録ステータス	説明	ステータスの検証	システム機能
HyperFlex リリース 5.0（1b）以前の **[コンプライアンス違反（Out of Compliance）]**	所有している数よりも多いライセンスを消費しています。 **重要** デバイスがコンプライアンス違反の場合に、シスコがお客様のネットワークに干渉したり、シャットダウンしたりすることはありません。 • **初期登録状態でのコンプライアンス違反**—スマート ライセンスは有効で、HX ストレージ クラスタは Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、最初の登録後に十分なライセンスがありません。 • **初期状態後または一定期間のインコンプライアンス状態後でのコンプライアンス違反**—スマート ライセンスは有効で、HX ストレージ クラスタは Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、十分なライセンスがありません。	ステータスを検証するには、`#stcli license show all` を実行します。 `Result: Mode = Out of Compliance`	特性や機能には影響ありません。 • Syslog メッセージを生成します。 • クラスタ レベルの HX Connect UI でコンプライアンス違反アラームを生成します。 （注） コンプライアンス違反状態は知的財産 EULA を侵害するため、サポートを継続的に受けるにはライセンスの購入または更新が必要です。

登録ステータス	説明	ステータスの検証	システム機能
認証が期限切れ	スマート ライセンシングが有効で、HXストレージクラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、90 日間を超えて Cisco Smart Software Manager または Smart Software Manager サテライトと通信していません。	ステータスを検証するには、`#stcli license show status` を実行します。 `Result: Mode = Authorization Expired`	特性や機能には影響ありません。 • Syslog メッセージを生成します。 • HX Connect 上でイベントやアラームは発生しません。 • Cisco Smart Software Manager ポータルに、フラグと通知が表示されます。
エクスポート制御フラグが「不可」に設定された	スマート ライセンシングが有効で、HXストレージクラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、エクスポート制御を使用するように登録できません。	—	動作は、Cisco Smart Software Manager サーバによってほとんど制御されます。 **（注）** このステータスは、HX ストレージクラスタに制限付き機能が含まれている場合にのみ該当します。

登録ステータス	説明	ステータスの検証	システム機能

ID 証明書が期限切れ	スマート ライセンシングが有効で、HX ストレージ クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、6 か月を超えて ID 証明書が更新されていません。ライセンスは後続未確認状態で、コンプライアンス違反と見なされます。	ステータスを確認するには、次を実行します。
		`#stcli license show status`
		`Result: Mode: ID Certificate Expired`
		すべての条件をクリアしてコンプライアンス ステータスに戻すには、次のコマンドを実行します。
		`#stcli license renew <auth>/<id>`
			• Syslog メッセージを生成します。
			• HX Connect 上でイベントやアラームは発生しません。
			• Cisco Smart Software Manager ポータルに、フラグと通知が表示されます。

ライセンスの遵守とフィーチャの機能

Cisco HXDP リリース 5.0(2a) 以降、有効な Cisco HyperFlex ソフトウェア ライセンスが必要です。ライセンスが期限切れまたは不十分な HX Connect ユーザーは、特定のフィーチャにアクセスできないか、フィーチャの機能が制限されます。フィーチャがロックされる前に、目立つカウントダウン バナーが表示され、ライセンス コンプライアンスの必要性とライセンス更新ページへのリンクをユーザーに警告します。

Cisco HXDP リリース 5.0（2a）以降、評価の終了時またはライセンス遵守日の後の猶予期間が終了した時点でライセンスが期限切れまたは不十分なHXコネクトユーザーは、期限切れになる前にアクセスできたすべての機能にアクセスできなくなります。現在の構成では限られた情報しか得られず、構成の変更はサポートされていません。

機能がロックされる前に、目立つライセンス遵守カウントダウンバナーが表示され、ライセンス遵守の必要性とライセンス更新ページへのリンクをユーザーに警告します。

Cisco EULA を表示するには、https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html を参照してください。

図 *11 : 30* 日間の猶予期間を示すカウントダウン バナーの例

（注） 日数が減少して、フィーチャの機能がいつロックされるかが示されます。

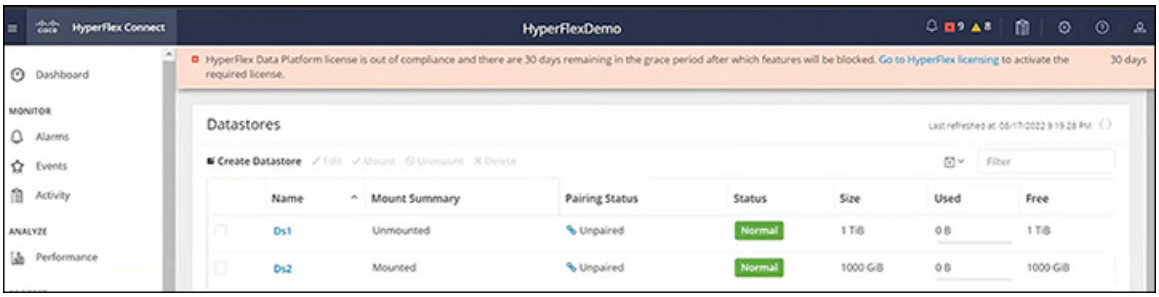
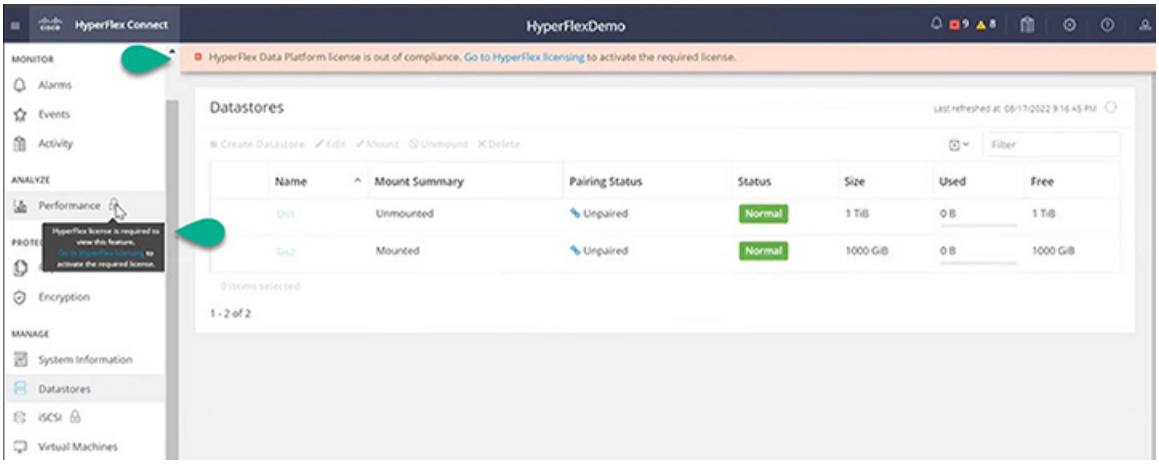


図 *12* : ライセンスの有効期限が切れたときに表示されるバナーとアイコン



1.	期限切れのライセンス バナー	HXDP ライセンスが遵守違反状態として示されます。「HyperFlex ライセンスに移動」リンクからライセンス更新ページが開きます。
2.	フィーチャのロックとホバーテキスト	特定のフィーチャがロックされていることを示します。ロックにカーソルをホバーさせると、ライセンス遵守ノートが表示され、ライセンス更新ページへのリンクが表示されます。

接続環境でのライセンスの管理

接続環境でライセンスを管理するには、次の手順を実行します。

スマート ライセンスにクラスタを登録する

スマート ライセンスは自動的に HX ストレージ クラスタに組み込まれ、デフォルトで有効になります。スマートライセンスをインストールする必要はありません。HX ストレージクラスタはスマート ライセンスに登録されず、90 日間の評価モードに入ります。90 日以内に、HX ストレージ クラスタを登録して機能をすべて使用できるようにする必要があります。

注目 HyperFlex クラスタを Smart Software Manager サテライトに登録する前に、プロキシが設定されていないことを確認します。プロキシが設定されている場合は、クラスタを Smart Software Manager サテライトに登録する前にプロキシを削除してください。

はじめる前に

- スマート ライセンスは、Cisco HX リリース2.5 で導入されました。クラスタで HX 4.0 リリース以降が実行されていることを確認することをお勧めします。
- スマート ライセンスの使用を開始する前に、Cisco スマート アカウントを持っている必要があります。ご注文時にスマートアカウントを作成（または選択）するか、ご注文時以外のときにスマートアカウントを作成して新規または既存のライセンスを追加していくことができます。

  スマート アカウントを作成するには、**[Cisco Software Central]** > **[スマート アカウントの申請（Request a Smart Account）]**（https://webapps.cisco.com/software/company/smartaccounts/home?route=module/accountcreation）を参照してください。

HX ストレージ クラスタは、次のいずれかの方法で Cisco スマート ソフトウェア マネージャ (SSM) に登録できます。

HX Connect を通してスマート ソフトウェア ライセンスによりクラスタを登録する

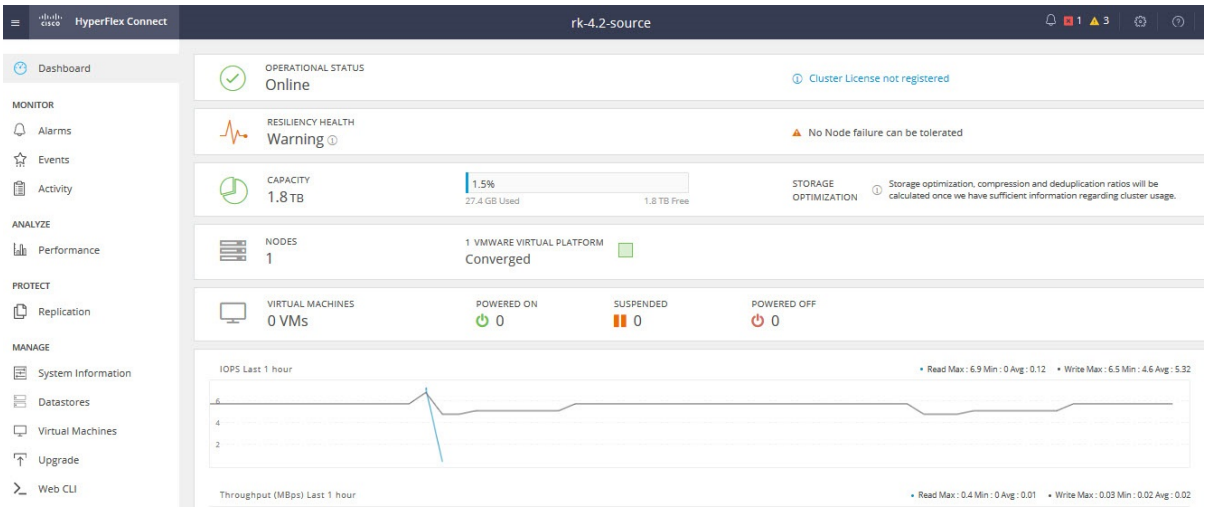
Cisco では、HX Connect を通してスマート ソフトウェア ライセンスを持つクラスとを登録することを推奨します。

始める前に

- 製品インスタンス登録トークンが必要です。トークンがない場合、Cisco スマート ソフトウェア マネージャでトークンを作成できます。製品インスタンス登録用のトークンを作成する方法の詳細については、登録トークンの作成 （88 ページ） を参照してください。

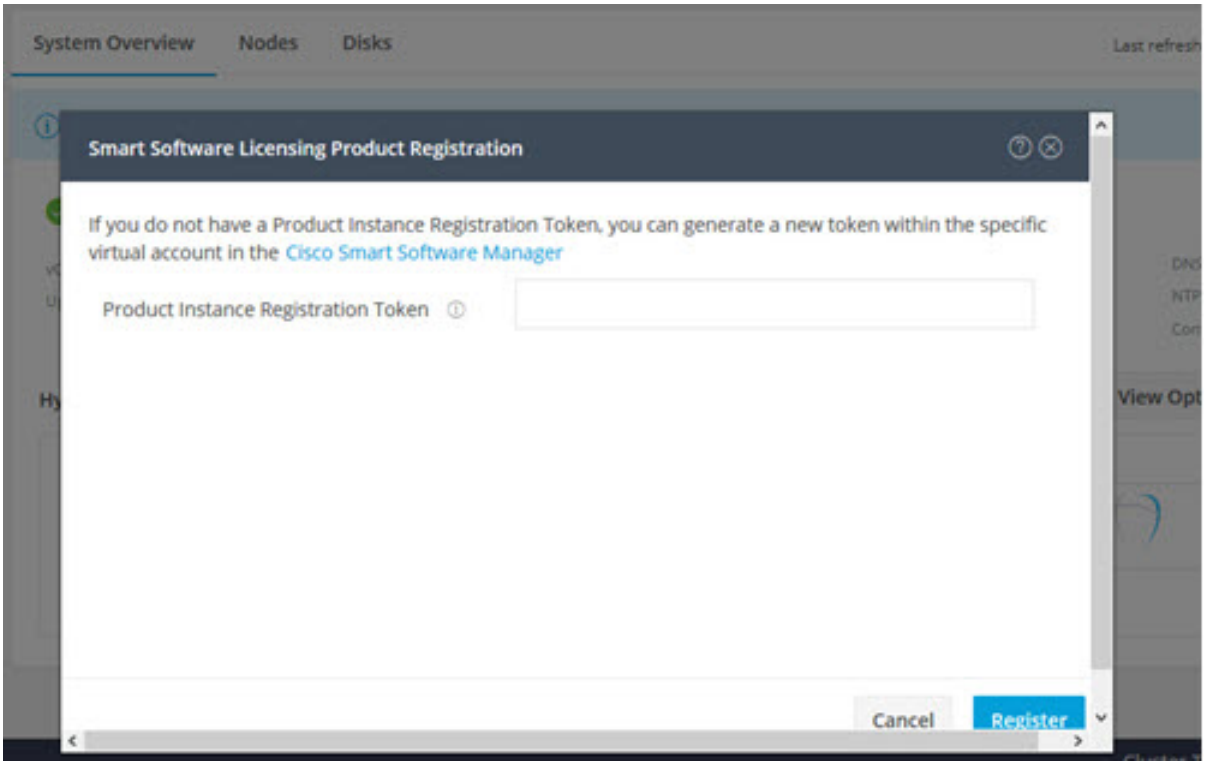
ステップ 1 HX Connect にログインします。

ステップ 2 **[Dashboard（ダッシュボード）]** ページで、**[Cluster License not registered（クラスタ ライセンスが登録されていません）]** をクリックします。



または、**[System Information（システム情報）]** ページの **[Register Now（今すぐ登録）]** リンクをクリックして登録を行うことができます。

ステップ 3 **[Smart Software Licensing Product Registration（スマート ソフトウェア ライセンス製品登録）]** ダイアログ ボックスで、**[Product Instance Registration Token（製品インスタンス登録トークン）]** フィールドに登録トークンを入力します。



製品インスタンス登録用のトークンを作成する方法の詳細については、登録トークンの作成（88 ページ）を参照してください。

ステップ 4 [Register] をクリックします。

登録に成功すると、**[System Information（システム情報）]**ページにライセンスの種類とライセンスの状態が表示されます。

- **ライセンス タイプ**：評価、Edge、標準、またはエンタープライズを HX ストレージ クラスタ ライセンス タイプとして表示します。
- **ライセンス ステータス**：HX ストレージ クラスタ ライセンス ステータスとして次のいずれかを表示します。
  - コンプライアンス
  - ライセンスの期限が <n> 日後に切れます。クラスタが登録されていません - 今すぐ登録します。（このステータスは評価タイプライセンスの場合にのみ表示されます。
  - ライセンスの期限が切れています。クラスタが登録されていません - 今すぐ登録します。（このステータスは評価タイプライセンスの場合にのみ表示されます。
  - コンプライアンス違反 - ライセンスが不十分です
  - 認証の有効期限切れ：HX が Cisco Smart Software Manager および Smart Software Manager サテライトと 90日 以上通信できない場合、このステータスが表示されます。

登録トークンの作成

登録トークンを使用して、製品にスマートライセンスを登録し、消費します。製品を登録し、製品インスタンスを特定のバーチャルアカウントに追加するには、トークンを生成する必要があります。

ステップ 1 使用しているリリースに応じて、ソフトウェア マネージャにログインします。

オプション	説明
Cisco Smart Software Manager	**Cisco Software Central**（https://software.cisco.com/）にナビゲートし、スマート アカウントにログインします。[ライセンス（License）] ペインで、[スマート ソフトウェア ライセンシング（Smart Software Licensing）] をクリックします。[インベントリ（Inventory）] をクリックします。
Smart Software Manager サテライト	`https://<IP address of the satellite>:8443` にアクセスし、管理者のクレデンシャルを使用してサテライトにログインします。

ステップ 2 HX ストレージクラスタを登録するバーチャルアカウントから、[全般（General）] をクリックして、[新しいトークン（New Token）] をクリックします。

ステップ 3 [登録トークンの作成（Create Registration Token）] ダイアログボックスで、次の操作を行い、[トークンの作成（Create Token）] をクリックします。

- トークンの簡潔な [説明（Description）] を追加します。

- トークンをアクティブにして他の製品で使用できるようにする日数を入力します。最大 = 365 日
- [このトークンに登録された製品の輸出規制された機能を許可する（Allow export-controlled functionality on the products registered with this token）] をオンにします。

ステップ 4 [新しい ID トークン（New ID Token）] 行で、[アクション（Actions）] ドロップダウン リストをクリックし、[コピー（Copy）] をクリックします。

コントローラ VM を介してスマート ソフトウェア ライセンスとともにクラスタを登録する

このセクションでは、スマート ソフトウェア ライセンスとともにクラスタを登録する別の方法を説明しています。

ステップ 1 コントローラ VM にログインします。

ステップ 2 HX ストレージ クラスタがスマート ライセンス モードになっていることを確認します。

```
# stcli license show status
```

フィードバックには、[スマート ライセンスは有効です（Smart Licensing is ENABLED）]、[ステータス：未登録（Status: UNREGISTERED）]、および 90 日の評価期間の残り時間（日、時、分、秒）が表示されます。スマート ライセンスの評価期間は、HX ストレージ クラスタでライセンス機能を使用し始めたときに開始され、これを更新することはできません。評価期間が過ぎると、スマート エージェントが通知を送信します。

ステップ 3 HX ストレージ クラスタを登録します。ここで *idtoken-string* は Cisco Smart Software Manager またはスマート ソフトウェア マネージャ サテライトからの**新しい ID トークン**です。

```
# stcli license register --idtoken idtoken-string
```

ステップ 4 HX ストレージ クラスタが登録されていることを確認します。

```
# stcli license show summary
```

別の方法として、**[Cisco Smart Software Manager]** > **[インベントリ（Inventory）]** > **[製品インスタンス（Product Instances）]** でも、HX ストレージ クラスタが登録されていることを確認できます。

例：

```
root@SpringpathController8OIW1HJOKW:~# stcli license show summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Corp X HyperFlex License
  Virtual Account: west-region
  Last Renewal Attempt: None
  Next Renewal Attempt: Aug 1 17:47:06 2017 PDT

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
```

```
  Next Communication Attempt: Mar 4 16:47:11 2017 PST

License Usage:
  License                    Entitlement Tag
         Count  Status

-----------------------------------------------------------------------------------------------------------------------

  Cisco Vendor String XYZ
regid.2016-11.com.cisco.HX-SP-DP-S001,1.0_1c06ca12-18f2-47bd-bcea-518ab1fd4520 3      InCompliance
```

スマート ライセンスからクラスタを登録解除する

ライセンスを解除して別の HX ストレージクラスタ用にプールに戻すか、または Cisco Smart Software Manager 登録を削除する（たとえばクラスタをデコミッションする）場合には、HX ストレージクラスタを登録解除します。HX ストレージクラスタを登録解除すると、評価期間が残っていれば HyperFlex は評価モードで実行されます。そうでない場合、HyperFlex は評価の有効期限切れの状態になります。期限切れの評価状態にあるクラスタを登録解除しても、クラスタの実稼働データには影響しません。

スマートエージェントは、ライセンスクラウドにアクセスして自身を登録解除します。プラットフォーム上のすべてのスマートライセンス資格と証明書が削除されます。信頼されているストアのすべての証明書と登録情報が削除されます。スマートエージェントは、登録解除のためにシスコと通信できない場合でも、非登録状態になることができます。スマートライセンスを再び使用する必要が生じた場合には、HX ストレージクラスタを再登録してください。コントローラ VM を介してスマート ソフトウェア ライセンスとともにクラスタを登録する（89 ページ）を参照してください。

始める前に

- 次のコマンドを使用して、HX ストレージクラスタがスマートライセンスに登録されていることを確認します。

  ```
  # stcli license show status
  ```

ステップ 1 コントローラ VM にログインします。

ステップ 2 スマート ライセンスから HX ストレージ クラスタを登録解除します。

```
# stcli license deregister
```

ステップ 3 HX ストレージ クラスタが登録解除されたことを確認します。

```
# stcli license show summary
```

スマート ライセンス承認の更新

始める前に

- 次のコマンドを使用して、HXストレージクラスタがスマートライセンスに登録されていることを確認します。

```
# stcli license show status
```

ステップ 1 コントローラ VM にログインします。

ステップ 2 次のコマンドを使用してスマート ライセンス承認を更新します。

```
# stcli license renew id
# stcli license renew auth
```

ステップ 3 HX ストレージ クラスタが更新され、承認されていることを確認します。

```
# stcli license show summary
```

非接続環境でのライセンスの管理

非接続環境でライセンスを管理するには、次の手順を実行します。

スマート ライセンスと Smart Software Manager サテライト

インターネット接続を使用してインストール ベースを管理することが許可されていない場合は、Smart Software Manager サテライトをオンプレミスでインストールし、Cisco Smart Software Managerのサブセットを使用してライセンスをローカルで管理できます。Smart Software Manager サテライトのダウンロード.

HyperFlex 用に Smart Software Manager サテライトを設定するには、 HX Data Platform CLI から次のコマンドを実行します。

```
stcli services sch set --portal-url http://<satellite-host>/Transportgateway/services/
DeviceRequestHandler --email <user-email-address>
```

Smart Software Manager サテライトが Cisco Smart Software Manager に登録されて稼働するようになったら、30 日ごとに Cisco Smart Software Manager と同期する必要があります。同期するには次の 2 つのオプションがあります。

- ネットワーク接続時に行うオンデマンドまたはスケジュール済み同期。
- 手動による同期。ライセンス ファイルをダウンロードした後、アップロードします。

（注） HX クラスタに Smart Satellite Server が構成されている場合、トークンは Smart Satellite Server の UI で生成される必要があるため、スマート ポータルのスマート ライセンス登録では生成されなくなります。

特定のライセンス予約および HyperFlex

シスコ固有ライセンスの予約 (SLR) は、ユーザが切断モードでデバイスを使用できるようにする新しいソフトウェアライセンス管理システムです。特に、外部ネットワーク接続 (air ギャップ) のない環境向けです。SLR には次のような追加の利点もあります。

- 時間のかかるライセンス タスクを自動化する
- ライセンスのステータスとソフトウェアの使用状況の傾向を追跡できます。
- コアの購入、管理、およびレポート機能をシンプル化

SLR により、顧客は仮想アカウントからライセンスを予約し、デバイス UDI に関連付けることができます。その後、これらのライセンスを使用してデバイスを切断モードで使用できます。また、お客様は、Cisco Smart Software Manager (CSSM) またはスマート ソフトウェア サテライト (オンサイト コレクタ) のいずれかと継続的に通信することなく、正常に動作させることができます。

HyperFlex SLR 対応 PID

次の HyperFlex PID のみが SLR モードで使用できます。

表 *3 :* 非接続およびエアギャップ展開用の *Cisco HyperFlex Data Platform (HXDP)* ソフトウェア *SKU*

HXDP SKU	説明
特定ライセンス登録	
HXDP-S-SLR	Cisco HyperFlex Data Platform 標準エディション特定ライセンス登録サブスクリプション
HXDP-P-SLR	Cisco HyperFlex Data Platform エンタープライズ エディション特定ライセンス登録サブスクリプション
HXDP-E-SLR	Cisco HyperFlex Data Platform エッジエディション特定ライセンス登録サブスクリプション

特定のライセンス予約 (SLR) ライセンスのインストール

この手順では、SLR ライセンスをインストールする方法、SLR ライセンスを返却する方法 (CSSM で再利用する場合)、または SLR ライセンス要求をキャンセルする方法について説明します。

SLR のインストール プロセスは、通常のスマート ライセンスのインストール プロセスと非常によく似ています。クラスタとスマート アカウントの間に通信がないため、手動プロセスを使用して、HTTP 接続で以前に存在していたのと同じ会話を行なう必要があります。

これらの会話は、要求コードが生成された場合に、Cisco ハードウェア クラスタから始まります。要求コードには、いくつかの基本的なクラスタ識別情報が含まれています。要求は、Cisco ポータルでスマート アカウントに転送され、要求コードに基づいて承認コードを要求します。Cisco がライセンス ID\ と権限付与情報の両方を含む承認コードを取得すると、承認コードがクラスタに戻され、インストールを開始できます。インストールが完了すると、ライセンスはクラスタで完全にアクティブ化されます。

Enable/Disable コマンドは、予約モードにするためのものです。これは、現在の登録機能のデフォルト モードです。コマンド内のすべての予約を設定するには、予約モードを明示的に有効にする必要があります。すでに CSSM に登録されているライセンスがある場合は、そのライセンスを再登録して、再利用できるようにする必要があります。CSSM から承認コードを取得したら、`reservation install` コマンドを使用して予約コードをインストールできます。ある時点で、クラスタを破棄するか、またはライセンスを再度 CSSM に戻して再利用できるようにする場合は、`reservation return` コマンドを使用して、再度登録できる返還コードを生成できます。

次の手順では、SLR ライセンスをインストール、返却、キャンセルする方法について説明します。

ステップ 1 HX ノードで `stcli license reservation enable` コマンドを入力して、予約モードを有効にします。

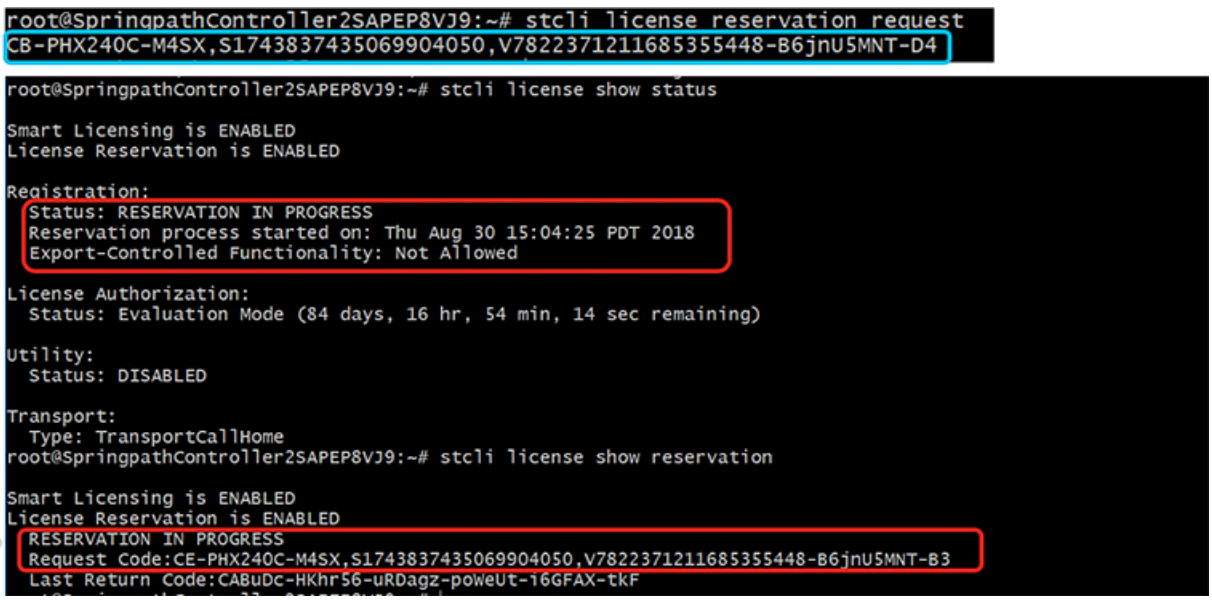
このコマンドを入力すると、設定モードが予約モードに切り替わります。ライセンス ステータスは変更されません。

次の画面の左側には、通常の登録で一般的なクラスタのステータスが表示されます。予約モードでは、そのステータスの違いを確認できます。一般的なデバイスの場合、予約ステータスを確認すると、登録済みとして表示されます。ライセンス認証ステータスが承認されます。個々にライセンスがある場合は、どのライセンスが準拠しているかがわかります。

右側には、システムが未登録の状態で、評価ライセンスを使用していることが表示されます。

ステップ 2 `stcli license reservation request` コマンドを入力して、予約要求を作成します。

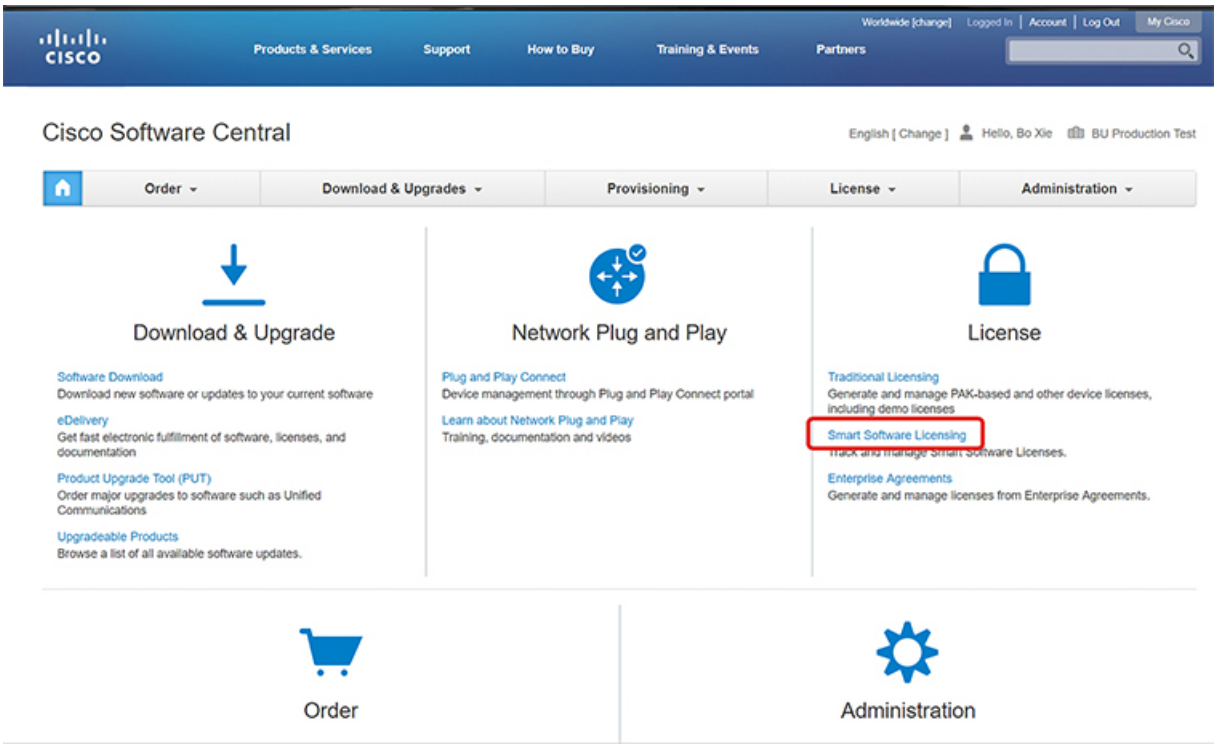
ライセンス要求コードは、次の画面の青色のボックスに表示されます。



予約要求を開始すると、登録ステータスが `RESERVATION IN PROGRESS` であることがわかります (赤いボックスに示されています)。要求コードがあれば、CSSM に移動して承認コードに変換できます。

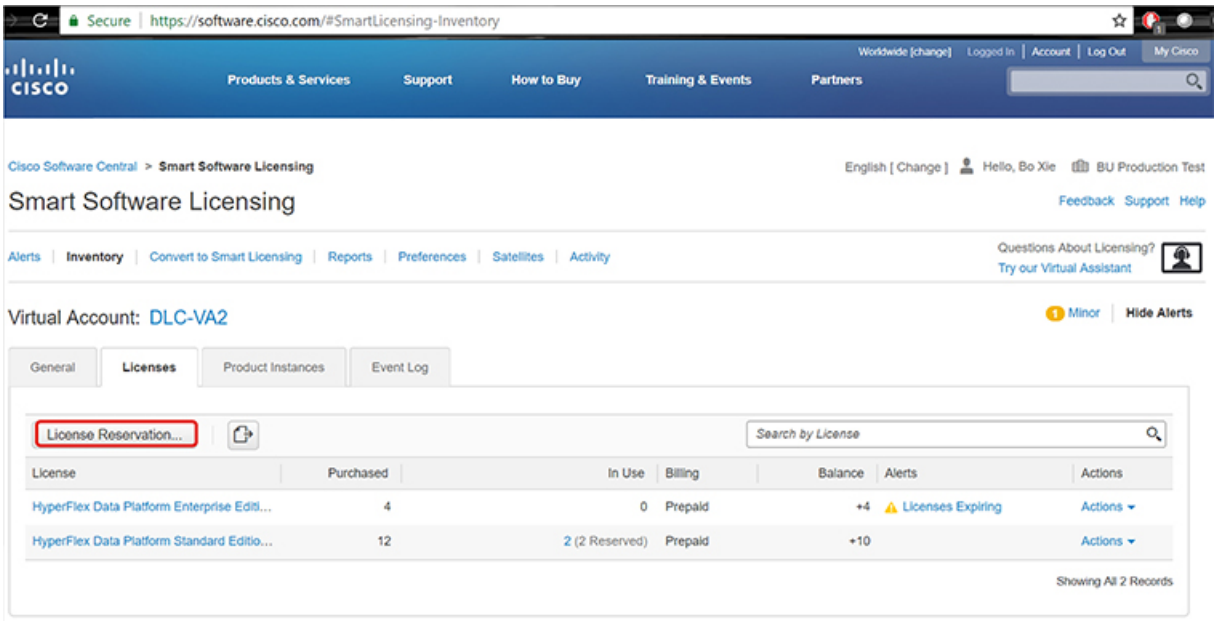
ステップ 3 CSSM（https://software.cisco.com）にログインします。

ステップ 4 **[ライセンス（License）]** セクションで、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** リンクをクリックします。



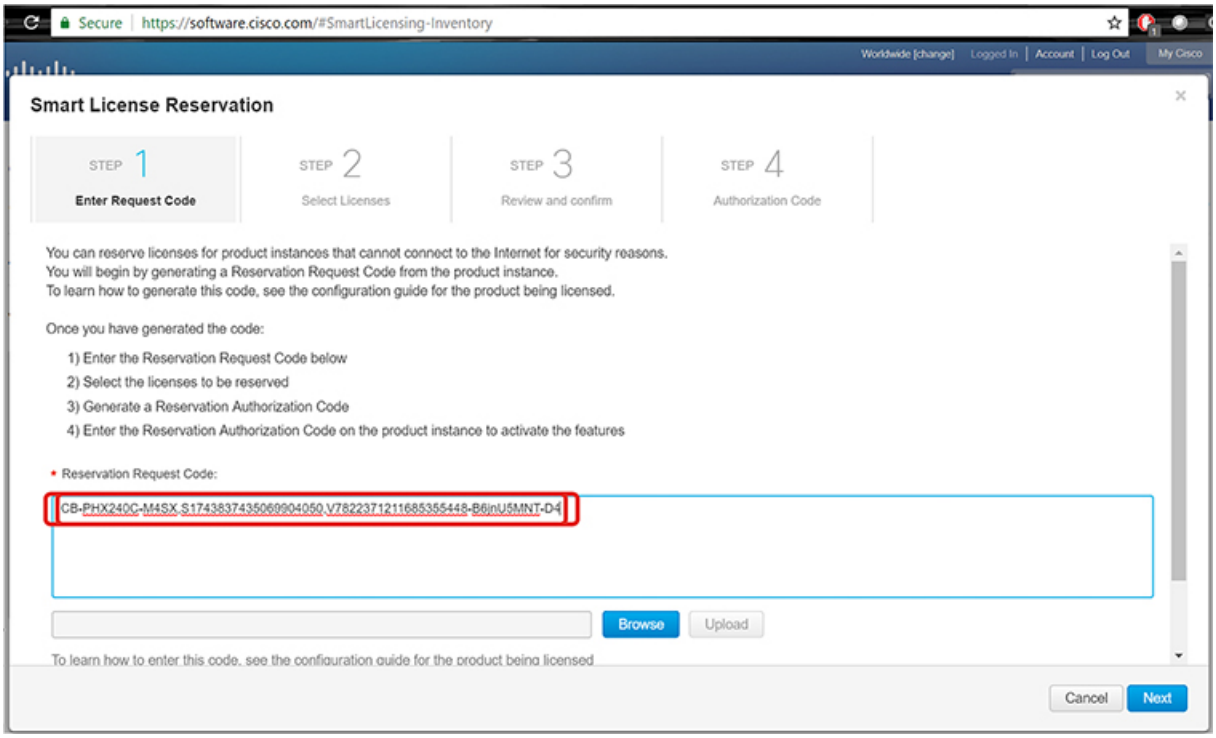
これにより、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** ページが表示されます。

ステップ 5 **[ライセンス（Licenses）]** タブの下で、**[ライセンス予約（License Reservation）]** をクリックします。

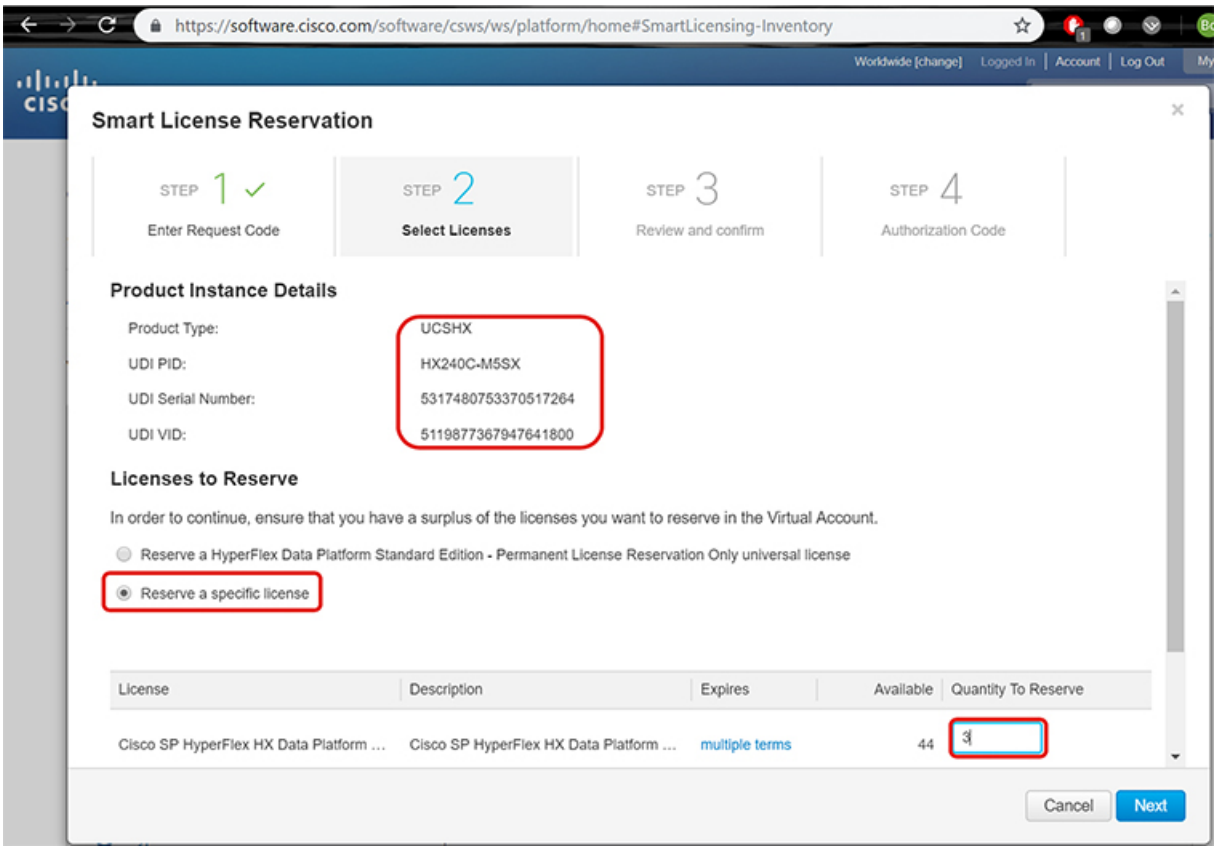


ステップ 6 4 ステップの SLR プロセスを完了して、要求コードを入力し、[ライセンス（Licenses）] を選択し、承認コードを確認して確認し、承認コードをダウンロードします。

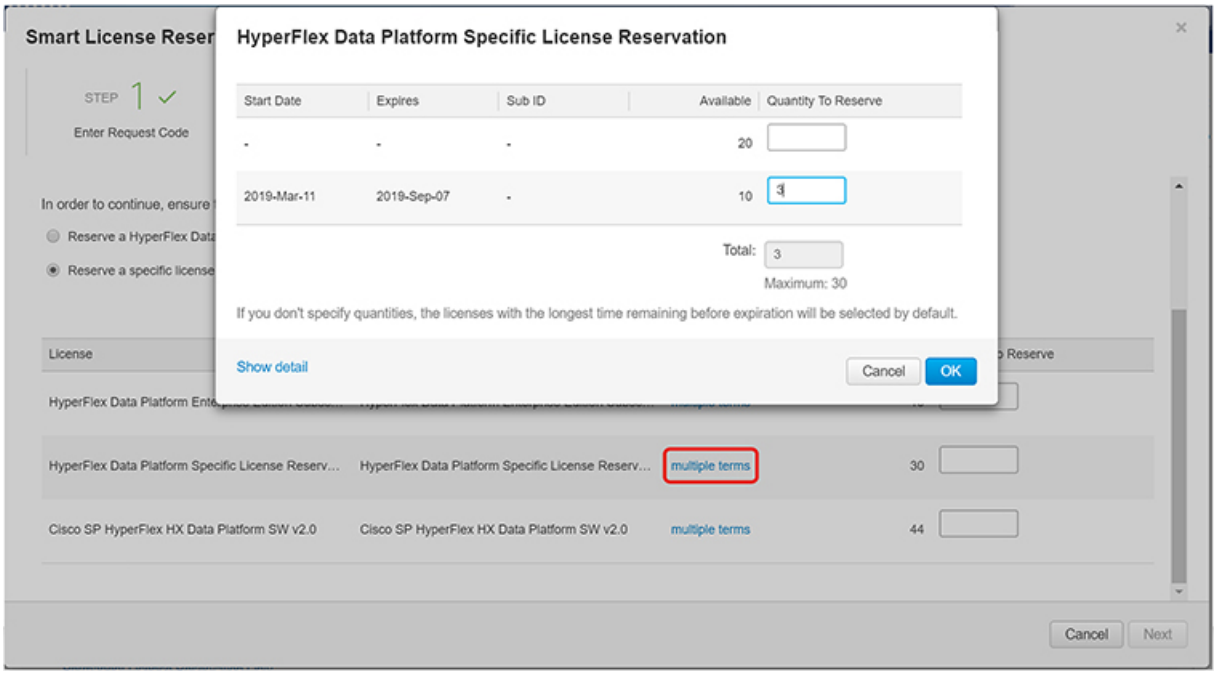
1. **[要求コードを入力（Enter the Request Code）]**: クラスタで生成された予約要求コードを入力します。



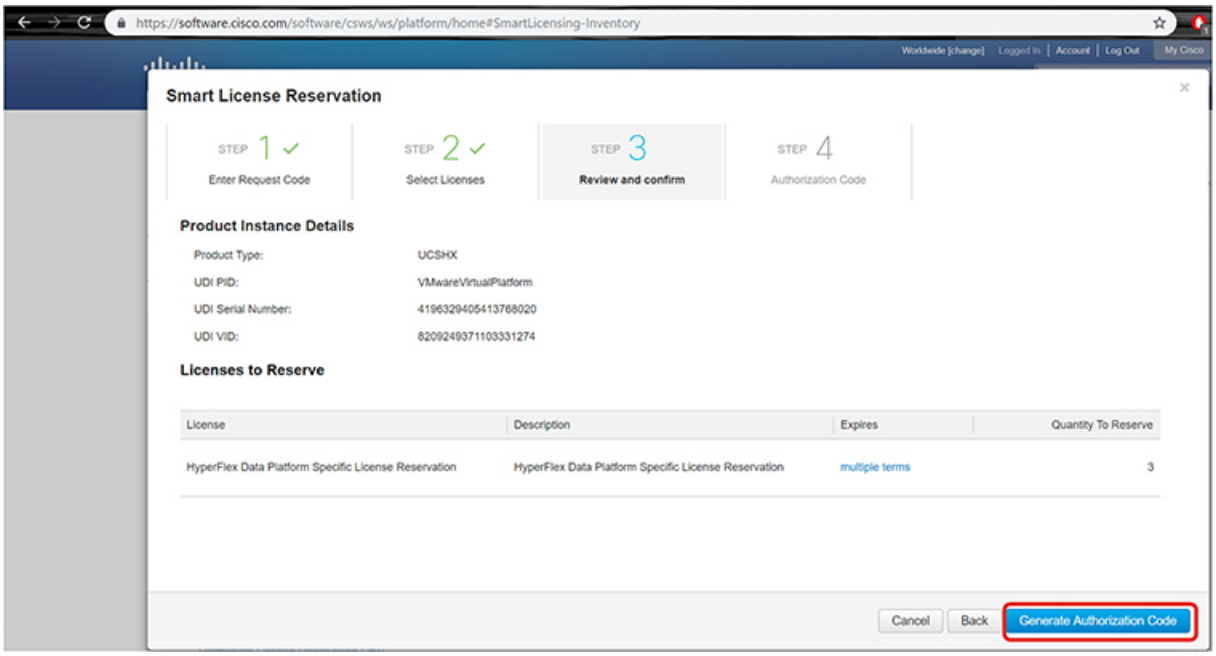
2. **[ライセンスを選択（Select Licenses）]**: この画面には、ライセンスの内容や、製品タイプ、UDI PID、UDI シリアル番号、UDI VID などの製品インスタンスの詳細が表示されます。提供された情報を確認し、チェックボックスをオンにして**特定のライセンスを予約**します。



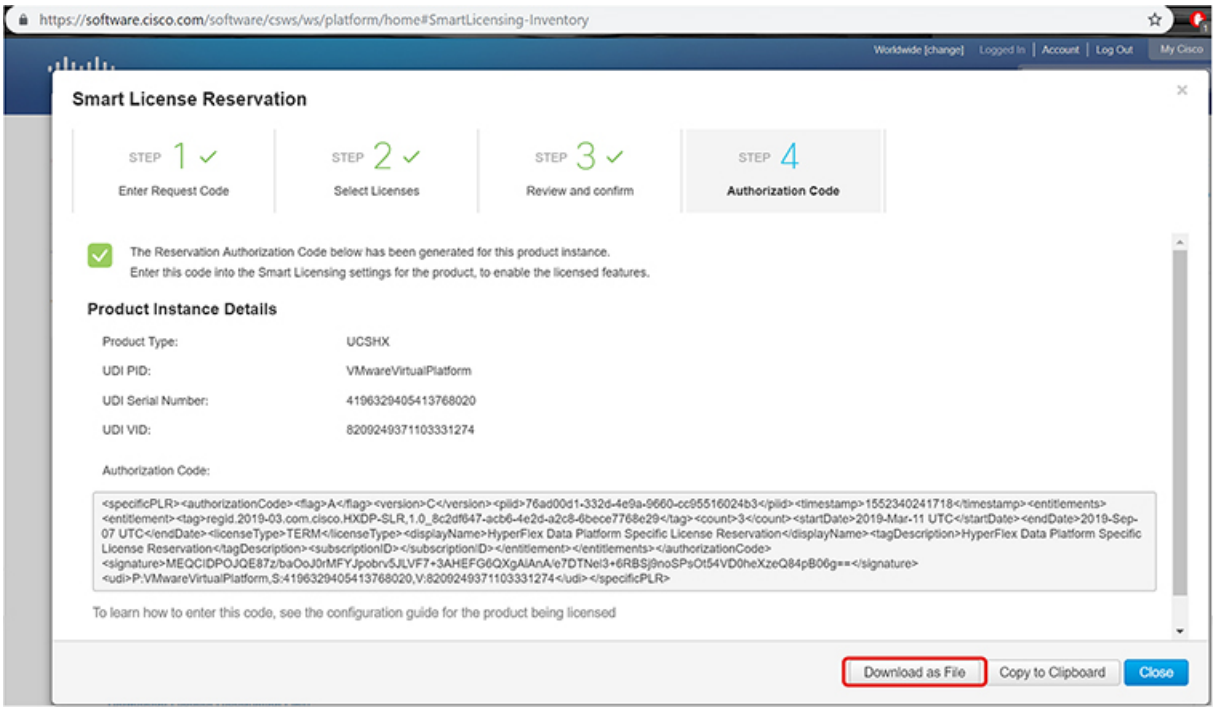
選択した特定のライセンスの予約について、**予約する数量**を入力します。



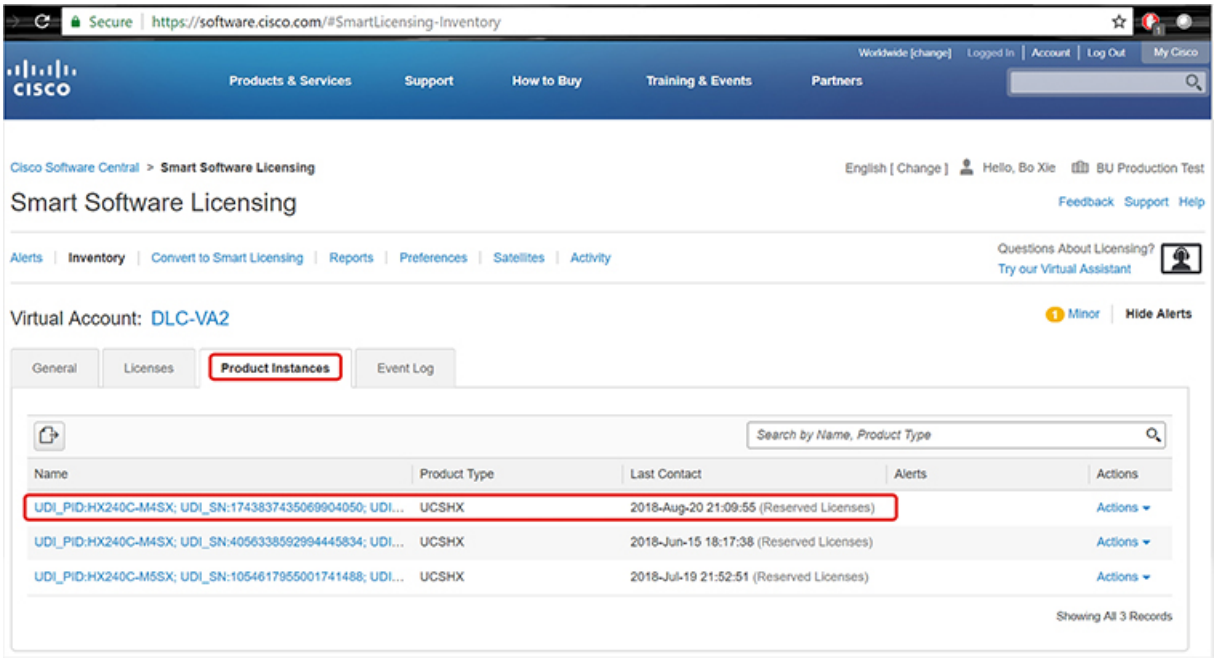
3. **[検証と確認（Review and Confirm）]**: 製品インスタンスの詳細と予約するライセンスを検証して確認し、画面の下部にある **[承認コードの生成（Generate Authorization Code）]** ボタンをクリックします。



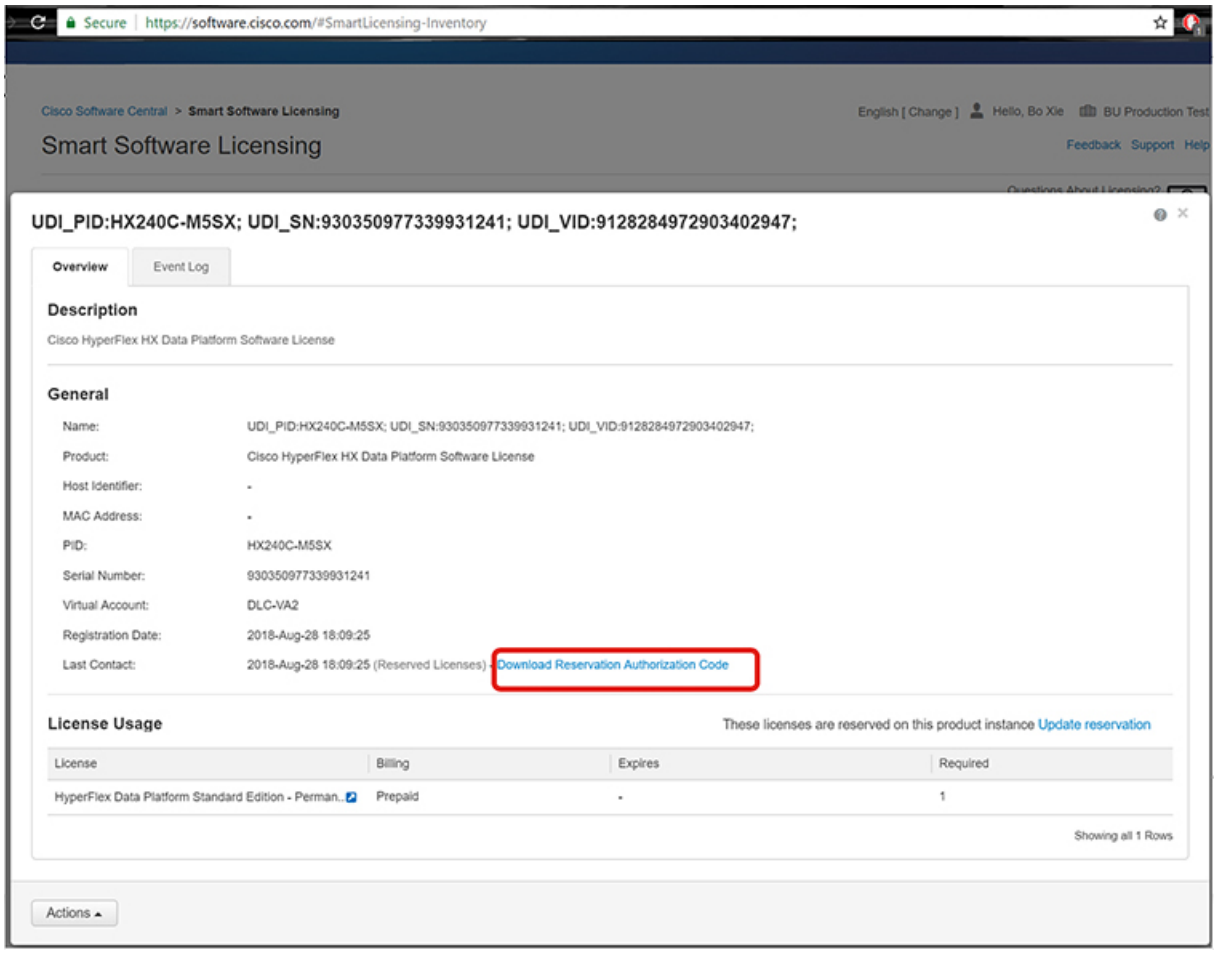
4. **[承認コード（Authorization code）]**: デバイス側で使用できる承認コードを表示し、画面下部の **[ファイルとしてダウンロード（Download as File）]** ボタンをクリックします。



ステップ 7 **[製品インスタンス（Product Instances）]** タブに移動して、予約のクラスとシリアル番号に対応する行にある予約済みのライセンスを表示します。この行のリンクをクリックします(赤いボックスに表示されます)。



ライセンスの説明を示すダイアログ ボックスが表示されます。



このページから、ライセンスの一般的な詳細を表示できます。特定のインスタンスで失われた場合に備えて、予約承認コード (上の赤色で強調表示) をダウンロードすることもできます。このページに戻って再度取得することもできます。

その後、**[ライセンス（Licenses）]** タブに戻り、現在のライセンスの使用状況を表示できます。

ステップ 8 HX ノードに `stcli license reservation install <enter authorization code>` コマンドを入力して、続いて承認コードを入力します。

```
root@SpringpathControllerR8KWZ2DM0U:~# stcli license reservation install --file ~/AuthorizationCode.txt
root@SpringpathControllerR8KWZ2DM0U:~# stcli license show reservation

Smart Licensing is ENABLED
License Reservation is ENABLED
Specified License Reservations:
  Status: SPECIFIC INSTALLED - SUCCEEDED on Mon Mar 11 10:49:05 PDT 2019
  Export-Controlled Functionality: Allowed
  Request Code: CB-PHX240C-M5SX,$531748075337051726 4,V:511987736794764180 0-B6jnU5MNT-86
  Last Authorization Code: <specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>50f8e2da-bbfb-4af4-bbb1-9beb6d6ab8ed</pi
d><timestamp>1552325956764</timestamp><entitlements><entitlement><tag>regid.2016-11.com.cisco.HX-SP-DP-S001,1.0_1c06ca12-18f2-47bd-bcea-518a
b1fd4520</tag><count>3</count><startDate>2018-Oct-29 UTC</startDate><endDate>2019-Apr-27 UTC</endDate><licenseType>TERM</licenseType><displa
yName>Cisco SP HyperFlex HX Data Platform SW v2.0</displayName><tagDescription>Cisco SP HyperFlex HX Data Platform SW v2.0</tagDescription><
subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>MEQCIBaYGBvLz5LxmwzSHW6dU17Y2f1QAo171zqdJLtq9wd9
AiAVvh2aShbY3oZtPBVu21IuJ1AsZutJKA6JQhJLCbbi/g==</signature><udi>P:HX240C-M5SX,S:531748075337051726 4,V:511987736794764180 0</udi></specificPL
R>
  Last Confirmation Code: f40513fe
    License Type: TERM
    Description: Cisco SP HyperFlex HX Data Platform SW v2.0
    Start Date:2018-Oct-29 UTC
    End Date:2019-Apr-27 UTC
    Count: 3
```

予約が成功すると、REGISTERED – SPECIFIC LICENSE RESERVATION として表示されるステータスを表示できます。認証では、UTHORIZED – RESERVED であることを示しています。

```
root@slcvm3:~# stcli license show all

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Thu Feb 21 09:23:52 PST 2019
  Last Renewal Attempt: None

License Authorization:
  Status: AUTHORIZED - RESERVED on Thu Feb 21 09:23:52 PST 2019

Export Authorization Key:
  Last request status:
  Features Authorized:
   None
  Last return status:
  Return Keys in process:
   None

Utility:
  Status: DISABLED

Transport:
  Type: TransportCallHome

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 87 days, 4 hr, 20 min, 45 sec

License Usage
=============
License Authorization Status:
  Status: AUTHORIZED - RESERVED on Mon Mar 04 14:37:18 PST 2019
  Last Communication Attempt: SUCCEEDED on Mar 4 14:37:18 2019 PST
  Next Communication Attempt: NONE

HyperFlex Data Platform Enterprise Edition Subscription (regid.2017-12.com.cisco.HXDP-P001,1.0_454a6b54-8b33-45bd-9d11-b1567c4a741e)
  Description:
  Count: 3
  Version: 1.0
  Status: ReservedInCompliance
  Export status: NOT_RESTRICTED
  Feature Name: null
  Feature Description: null
  Reservation:
    Reservation Status: SPECIFIC INSTALLED
    Total Reserved Count: 4

Product Information
===================
UDI: PID:HX240C-M5SX,SN:2432415792187588918,VID: 6984912678611873514

Agent Version
=============
Smart Agent for Licensing: 2.1.3
```

また、HX ノードで stcli license show reservation コマンドを入力して、SLR 予約を表示することもできます。この応答は、SLR がインストールされていることを示しています。

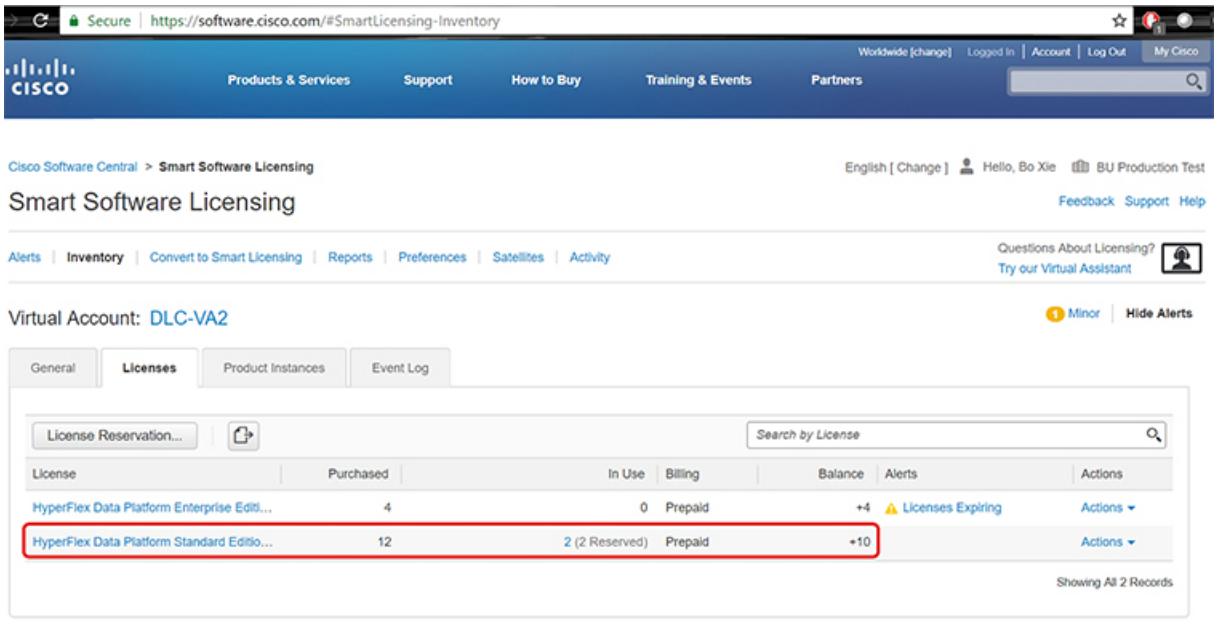
特定のライセンス予約 (SLR) ライセンスのキャンセル

この手順では、SLR ライセンス要求をキャンセルする方法について説明します。

ステップ 1 (承認コードを取得するために CSSM に進む前に) 開始した予約要求をキャンセルするには、stcli license reservation cancel コマンドを使用します。

ステップ 2 **stcli license show reservation** コマンドを使用して予約要求がキャンセルされたことを確認します。

このコマンドを入力すると、ステータスが未登録に戻ったことを確認できます。



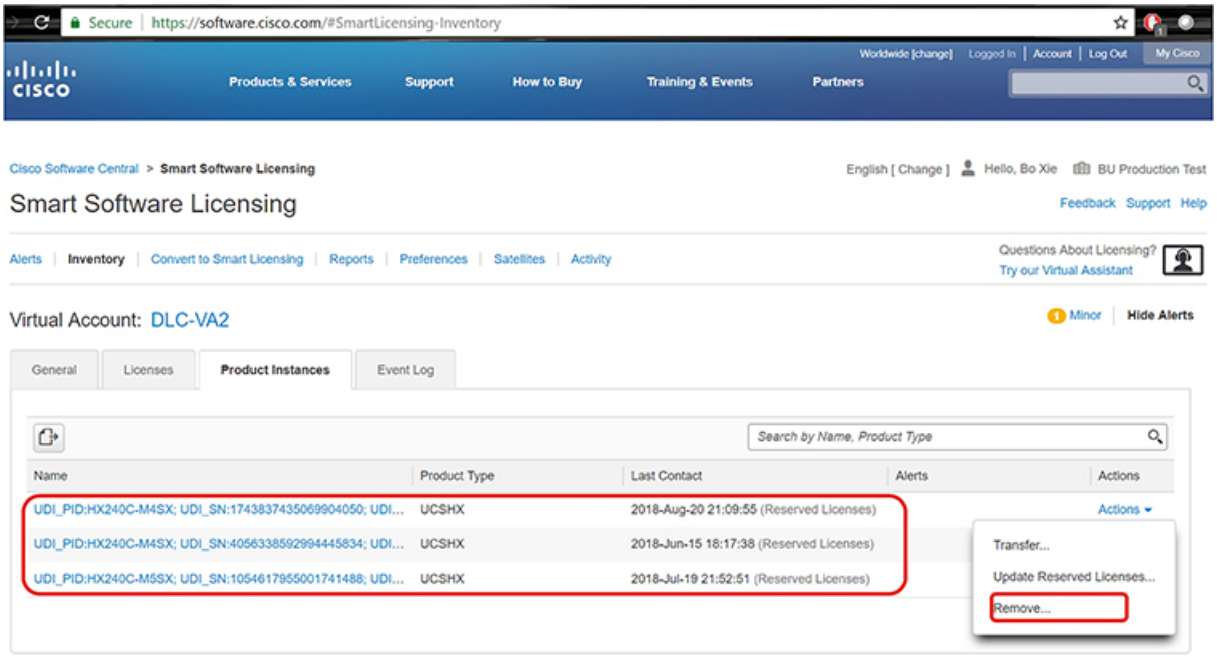
特定のライセンス予約 (SLR) ライセンスを返す

クラスタのライセンスが完全にアクティブになったので、後でクラスタを破棄し、別のクラスタに再利用できるようにCSSMにライセンスを戻すことができます。次の手順では、SLRライセンスを返す方法について説明します。

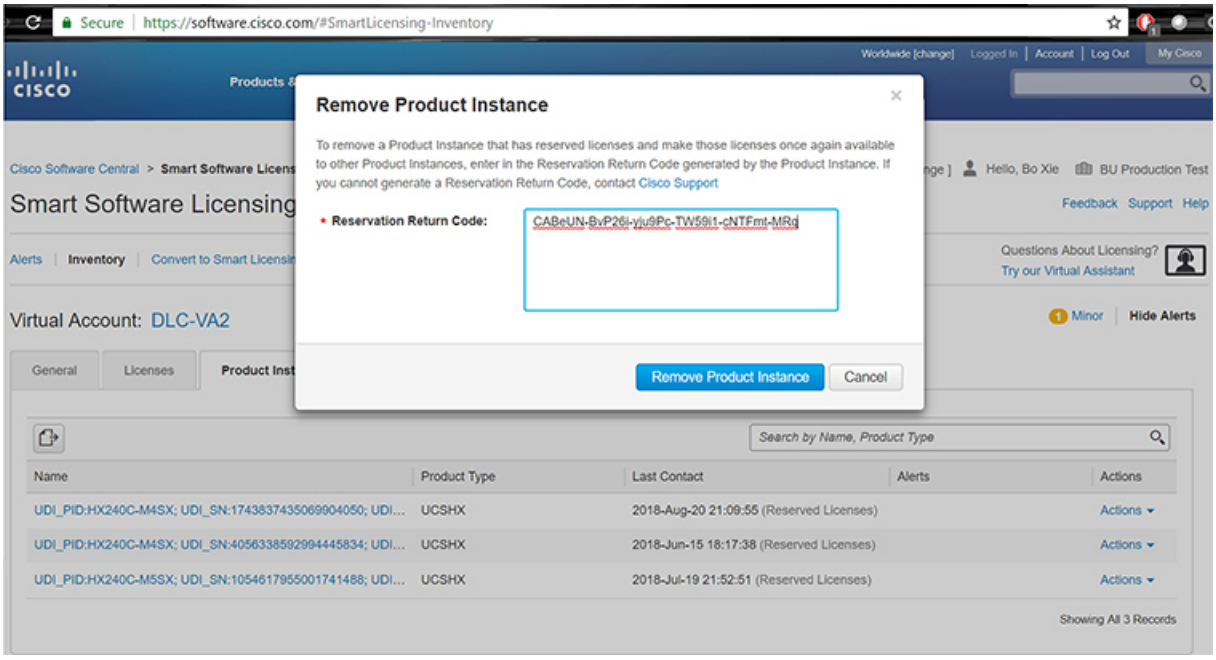
ステップ 1 `stcli license reservation return` コマンドを入力します。その後、CSSMで使用できる返還コードが生成されます。ステータスを確認すると、ライセンスは登録前と同様に、未登録の評価ライセンスに戻ります。

```
root@SpringpathController2SAPEP8VJ9:~# stcli license reservation return
CABeUN-BvP26i-yju9Pc-TW59i1-cNTFmt-MRq
root@SpringpathController2SAPEP8VJ9:~# stcli license show reservation

Smart Licensing is ENABLED
License Reservation is ENABLED
  Last Return Code:CABeUN-BvP26i-yju9Pc-TW59i1-cNTFmt-MRq
root@SpringpathController2SAPEP8VJ9:~# stcli license show status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 23 hr, 32 min, 3 sec
  Last Communication Attempt: SUCCEEDED on Aug 20 14:12:06 2018 PDT
  Next Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: TransportCallHome
```

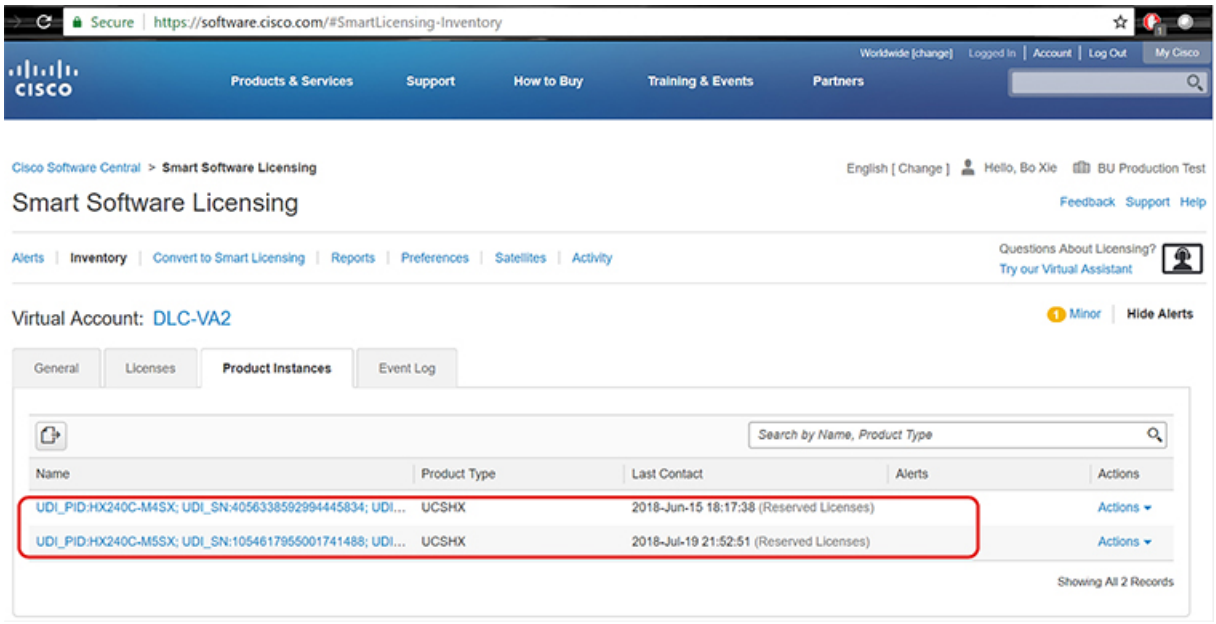
ステップ 2 [CSSM] に戻り、ライセンスをプールに戻します。**[製品インスタンス（Product Instances）]** タブに戻り、**[アクション（Actions）]** メニューを使用して、**[削除（Remove）]** をクリックします。



[製品インスタンスの削除（Remove Product Instance）] ダイアログ ボックスが表示され、返還コードを入力できます。返還コードを入力し、**[製品インスタンスの削除（Remove Product Instance）]** をクリックします。



[製品インスタンス（Product Instances）] タブで、以前登録した SLR ライセンスが削除されたことを確認できます。3 個使用されるのに対して、使用中なのは 2 個だけです。この時点で、ライセンスが正常に返却されています。

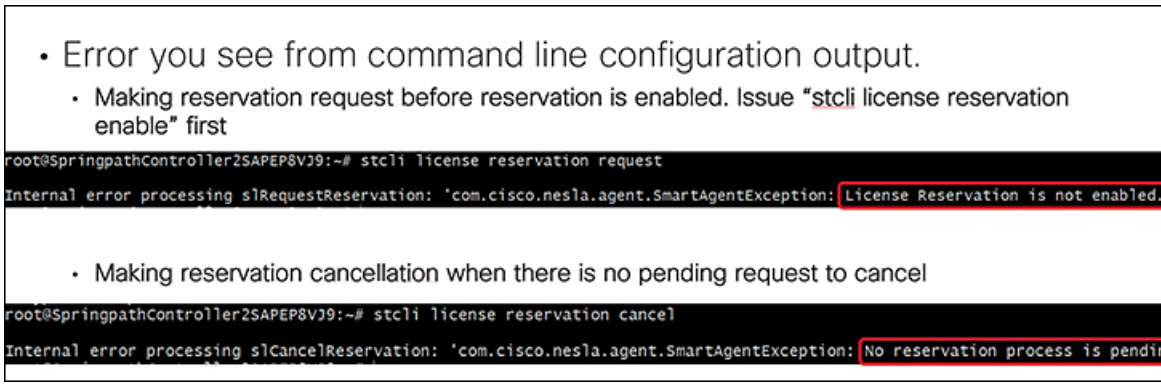


特定のライセンスの予約のトラブルシューティング (SLR)

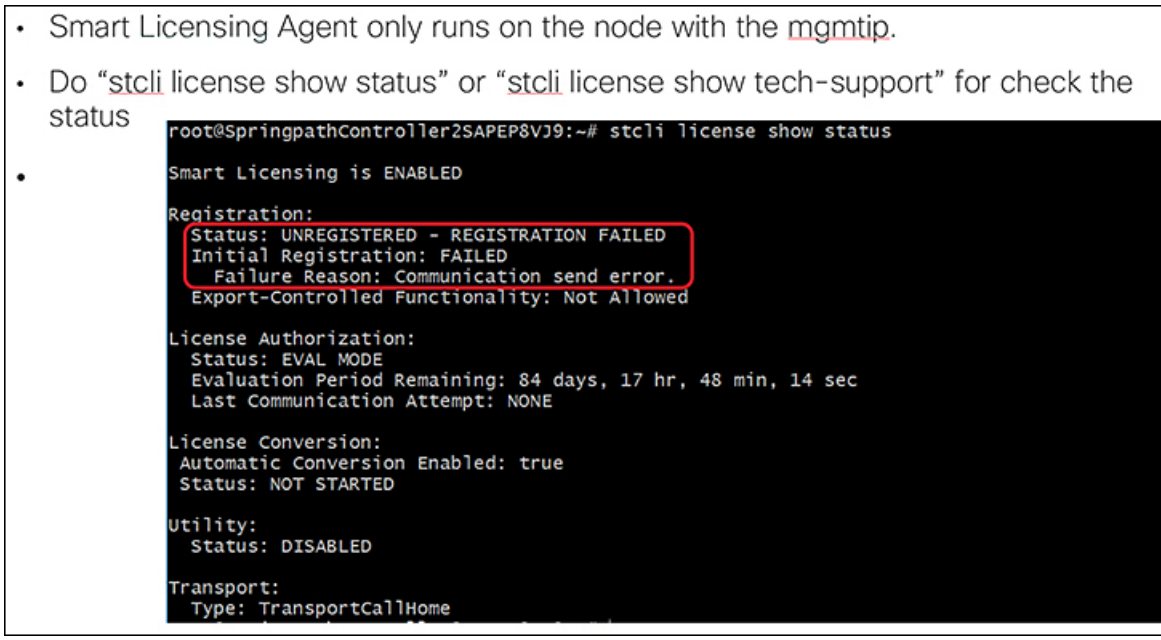
このセクションでは、特定のライセンス予約 (SLR) を設定して使用する際に表示される可能性のある一般的なエラー メッセージについて説明します。また、該当する場合のトラブルシューティング方法に関する推奨事項も提供します。

表示される可能性のある 2 個の一般的なエラー メッセージは次のとおりです。

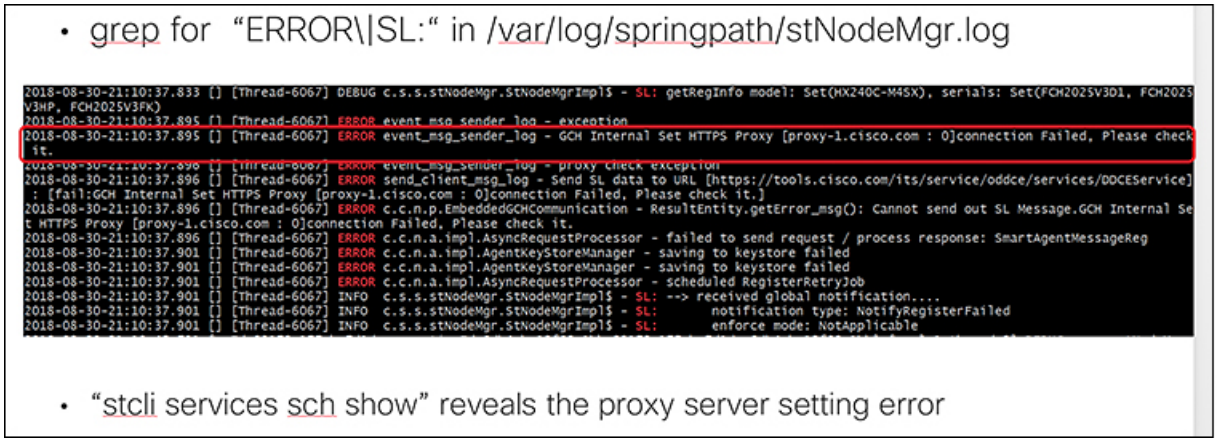
- 設定中に予約モードを有効にする前に予約要求コマンドを発行すると、「ライセンス予約が有効になっていません」というエラー メッセージが表示されます。または、要求しなかった操作をキャンセルするよう要求した場合は、「保留中の予約プロセスはありません」というメッセージが表示されます。次の図は、これらのエラーを示しています。



- ライセンス ステータスが変更されたランタイム時に、最初の登録が通信の送信エラーで失敗します。通常、このメッセージは、 `show status`コマンドを入力したときに表示されます。ライブラリはエラーを上位に伝播しませんが、ログを使用して実際の理由を確認できます。

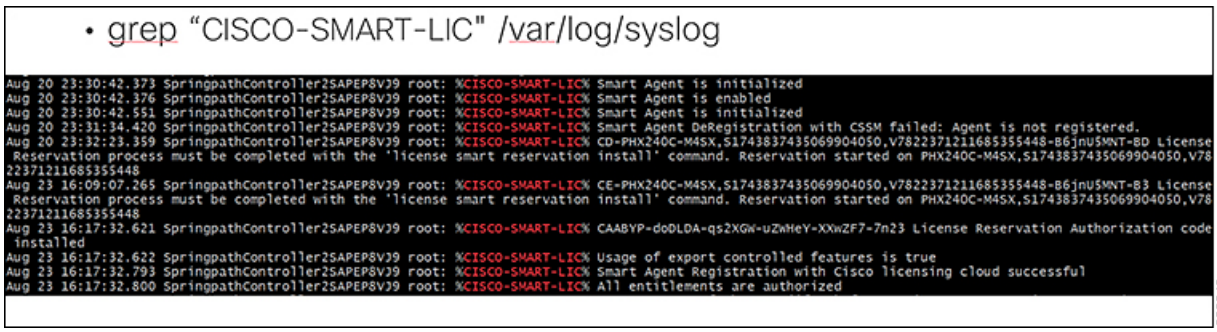


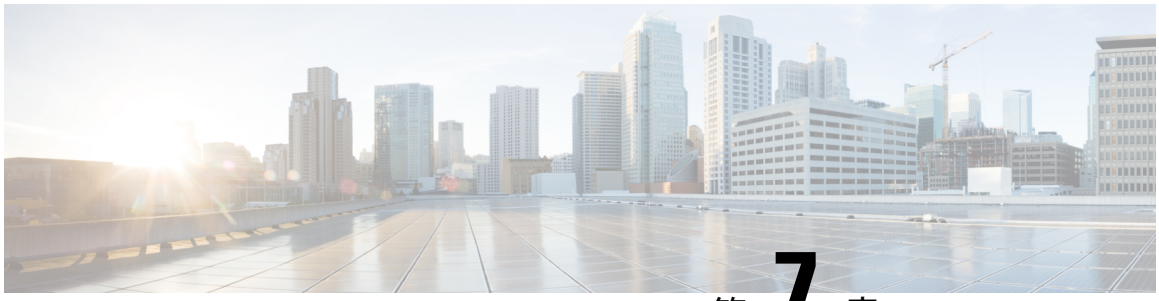
ステップ 1 `grep` コマンドを発行し、SL カラムを表示して、ログに記録されているエラーおよびその他のすべての SL 関連メッセージを特定します。たとえば、次の図は、プロキシが使用されていること、およびプロキシ接続が失敗したことを示しています。これにより、ライセンス サーバのプロキシ設定が正しくないことが分かります。



ステップ 2 これを解決するには、`stcli services sch show` コマンドを使用して、プロキシのセットアップを確認し、エラーを修正してから、もう一度やり直してください。

ステップ 3 また、「CISCO-SMART-LIC」で `grep` コマンドを発行して、移行中に生成されたスマート ライセンスの syslog メッセージを確認することもできます。





第 7 章

HyperFlex ハードウェア アクセラレーション カードの設定

この章では、Cisco HyperFlex ハードウェア アクセラレーション カードを設定する方法について説明します。

HyperFlex ハードウェア アクセラレーション カードの概要

この章では、HyperFlex ノード上の HyperFlex ハードウェア アクセラレーション カード (PID: HX-PCIE-OFFLOAD-1) のインストール、ポストインストール、およびトラブルシューティングの詳細と、初期クラスタの設定について説明します。これらのカードにより、ほとんどのストレージ ワークロードのパフォーマンスと圧縮効率が向上します。

（注） HyperFlex ハードウェア アクセラレーション カードをインストールおよび設定するには、HXDP-P エンタープライズ ライセンスが必要です。

PCIe スロットおよびライザー カード (およびその他の関連情報) の説明については、『Cisco HX240c M5 HyperFlex ノード (ハイブリッドおよびオールフラッシュ モデル) インストレーション ガイド』を参照してください。

Install HyperFlex Hardware Acceleration Cards

始める前に

HyperFlex ハードウェア アクセラレーション カードの取り付けプロセスを開始する前に、次の点に注意してください。

- インストールは、新規展開でのみサポートされています。
- インストールは、次の HX 240 M5/M6 サーバーでのみサポートされています。
  - HXAF240C-M5SX Cisco HyperFlex HX240c M5 All Flash
  - HXAF240C-M6S Cisco HyperFlex HX240c M6 All Flash
  - HX240C-M5SX Cisco HyperFlex HX240c M5
  - HX240C-M6SX Cisco HyperFlex HX240c M6
  - HX240C-M5L HyperFlex HX240c M5 LFF
  - HX240C-M6S HyperFlex HX240c M6 LFF
- インストールは Hyper-v ではサポートされておらず、ストレッチ クラスタにもサポートされていません。
- HX クラスタ内のすべてのノードには、HyperFlex ハードウェア アクセラレーション カードが含まれている必要があります。

（注） 検証中にいずれかのノードにアクセラレーション カードが含まれていない場合は、インストーラが機能不全になり、エラー メッセージが表示されます。

- クラスタ タイプは、すべてフラッシュ/ハイブリッド ESXi である必要があります。
- インストールは、HX 240 M5/M6 サーバーでのみサポートされています。
- ハードウェア アクセラレーション カードは、Cisco HX データ複製では動作しません。
- HX リリース 4.0(2b) 以降、ストレッチ クラスタ構成のハードウェア オフロード オプションがサポートされています。

ステップ 1 新しい PCIe カードを取り付けます。これは、Cisco がサポートするインストールです。

ステップ 2 HX インストーラを使用してクラスタを設定します。詳細については、以下を参照してください。

- VSphere Web Client を使用した HX データ プラットフォーム インストーラ OVA を展開します。

- HX クラスタの設定と展開

vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開

ESXi ホストに HX Data Platform をインストールするだけではなく、VMware Workstation、VMware Fusion または Virtual Box にも HX Data Platform インストーラを展開することができます。

（注）
- vCenter に接続して OVA ファイルを展開し、IP アドレス プロパティを指定します。ESXi ホストから直接展開しても、値を正しく設定することはできません。
- Cisco HX ストレージ クラスタ内のノードとなる ESXi サーバに HX Data Platform インストーラを展開しないでください。

ステップ 1 [ソフトウェアのダウンロード（Download Software）] で HX Data Platform インストーラ OVA ファイルを特定してダウンロードします。HX Data Platform ストレージ クラスタに使用されるストレージ管理ネットワーク上のノードに、HX Data Platform インストーラをダウンロードします。

```
Example:
Cisco-HX-Data-Platform-Installer-v4.5.1a-26363.ova
```

ステップ 2 VMware ハイパーバイザを使用して HX Data Platform インストーラを展開し、HX Data Platform インストーラ仮想マシンを作成します。

（注） 仮想ハードウェア リリース 10.0 以降をサポートする仮想化プラットフォームのリリースを使用してください。

vSphere はシステム要件です。vSphere シック クライアント、vSphere シン クライアント、または vSphere Web クライアントのいずれかを使用できます。HX Data Platform インストーラを展開するには、VMware Workstation、VMware Fusion、または VirtualBox を使用することもできます。

a) vSphere、VirtualBox、Workstation、Fusion などの仮想マシン ハイパーバイザを開きます。
b) HX Data Platform インストーラを展開するノードを選択します。

重要 vSphere Web Client を使用して HX インストーラ OVA を導入する際は、ユーザー クレデンシャルを必ず指定してください。

- vSphere シック クライアントを使用する—**[インベントリ リスト（Inventory list）] > [ホスト（Host）] > [ファイル（File）] > [OVA を展開（Deploy OVA）]** を展開します
- vSphere Web クライアントを使用する—**[vCenter インベントリ リスト（vCenter Inventory list）] > [ホスト（Hosts）] > [ホスト（Host）] > [OVA を展開（Deploy OVA）]** を展開します

ステップ 3 HX Data Platform インストーラの場所を選択します。デフォルト値を使用し、適切なネットワークを選択します。

ステップ 4 HX Data Platform インストーラ VM で使用する静的 IP アドレスを入力します。

（注）
- ネットワークで DHCP が設定されている場合でも、静的 IP アドレスが必要です。HX Data Platform インストーラを実行し、HX Data Platform をインストールし、HX Data Platform ストレージ クラスタを作成するには、静的 IP アドレスが必要です。
- 新しい VM への IP アドレス割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開 （61 ページ）の手順を実行して、静的 IP アドレスで HX Data Platform インストーラ VM をインストールします。インストーラ VM から DNS が到達可能である必要があります。

フィールド	説明
ホスト名	この VM のホスト名。 IP アドレスの逆引きを試みるには空白のままにします。
デフォルト ゲートウェイ	この VM のデフォルト ゲートウェイ アドレス。 DHCP を使用する場合は、空白のままにします。
DNS	この VM のドメイン ネーム サーバ（カンマ区切りリスト）。 DHCP を使用する場合は、空白のままにします。
IP アドレス	このインターフェイスの IP アドレス。 DHCP を使用する場合は、空白のままにします。
ネットマスク	このインターフェイスのネットマスクまたはプレフィックス。 DHCP を使用する場合は、空白のままにします。
Root パスワード	ルート ユーザー パスワード。 このフィールドは必須フィールドです。

ステップ 5 [次へ（Next）] をクリックします。リストされたオプションが正しいかどうか確認し、[導入後に電源をオンにする（Power on after deployment）] を選択します。

HX Data Platform インストーラを手動で電源オンにするには、仮想マシンのリストに移動し、インストーラ VM の電源をオンにします。

（注） HX Data Platform インストーラ仮想マシンの推奨設定は、3 つの vCPU と 4 GB のメモリです。これらの設定を小さくすると、CPU の使用率が 100% になり、ホストのスパイクが発生する可能性があります。

ステップ 6 [Finish] をクリックします。HX Data Platform インストーラ VM が vSphere インフラストラクチャに追加されるまで待ちます。

ステップ 7 HX Data Platform インストーラ仮想マシンを開きます。

初期コンソール画面に、HX Data Platform インストーラ仮想マシンの IP アドレスが表示されます。

```
Data Platform Installer.
****************************************
You can start the installation by visiting
the following URL:
http://192.168.10.210
****************************************
Cisco-HX-Data-Platform-Installer login:
```

ステップ 8 HX Data Platform インストーラにログインするための URL を使用します。

```
Example:
http://192.168.10.210
```

ステップ 9 自己署名証明書を受け入れます。

ステップ 10 ユーザー名 **root** と、OVA 導入の一部として設定したパスワードを使用してログインします。

静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開

新しい VM への IP アドレスの割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、以下の手順を使用して HX Data Platform インストーラを展開します。

ステップ 1 HX Data Platform ストレージ クラスタに使用されるストレージ管理ネットワーク上のノードに、VMware OVF Tool 4.1 以降をインストールします。詳細については、「OVF ツール ドキュメンテーション」を参照してください。

ステップ 2 VMware OVF がインストールされているノードの「ソフトウェアのダウンロード」から、HX Data Platform インストーラ OVA を見つけてダウンロードします。

ステップ 3 `ovftool` コマンドを使用して、ダウンロードした HX Data Platform インストーラ OVA を展開します。次に例を示します。

```
root@server:/tmp/test_ova# ovftool --noSSLVerify --diskMode=thin
--acceptAllEulas=true --powerOn --skipManifestCheck --X:injectOvfEnv
--datastore=qa-048-ssd1 --name=rfsi_static_test1 --network='VM Network'
--prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1
--prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8
--prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco
--prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5
--prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36
--prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0
--prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
vi://root:password@esx_server
```

このコマンドにより、HX Data Platform インストーラが展開され、HX Data Platform インストーラ VM の電源が入り、指定された静的 IP アドレスが設定されます。以下は処理応答の例です。

```
Opening OVA source:
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
Opening VI target: vi://root@esx_server:443/
Deploying to VI: vi://root@esx_server:443/
Transfer Completed
Powering on VM: rfsi_static_test
Task Completed
Completed successfully
```

インストーラ VM から DNS が到達可能である必要があります。静的 IP アドレスを正常に設定するために必要なコマンド オプションは以下のとおりです。

コマンド	説明
powerOn	HX Data Platform インストーラ VM の展開後に電源を投入します。
X:injectOvfEnv	HX Data Platform インストーラ VM に静的 IP のプロパティを挿入します。
prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1	適切なゲートウェイ IP アドレスを指定します。
prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8	適切な DNS IP アドレスを指定します。
prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco	適切なドメインを指定します。
prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5	適切な NTP IP アドレスを指定します。
prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36	適切なインストーラの静的IPアドレスを指定します。
prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0	適切なネットマスク アドレスを指定します。
prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword	root ユーザー パスワードを指定します。
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova	HX Data Platform インストーラ OVA の送信元アドレス。
vi://root:password@esx_server	HX データ プラットフォーム インストーラ VM がインストールされている宛先ESXサーバ。適切なESX サーバのルート ログイン クレデンシャルが含まれます。

HyperFlex クラスタの設定と展開

クレデンシャルの入力

[クレデンシャル（Credentials）]ページでは、必要な設定データをJSONファイルからインポートすることも、必須フィールドに手動でデータを入力することもできます。

（注） HyperFlex クラスタの初回インストールの場合は、シスコの担当者に連絡して工場出荷時のプレインストール JSON ファイルを入手してください。

クラスタを作成するには、*JSON* 設定ファイルから設定データをインポートするために次の操作を行います。

1. [ファイルの選択（Select a file）] をクリックし、該当する *JSON* ファイルを選択して設定データを読み込みます。**[構成を使用（Use Configuration）]** を選択します。
2. インポートした Cisco UCS Manager の値が異なる場合は、[Overwrite Imported Values] ダイアログボックスが表示されます。[Use Discovered Values] を選択します。

ステップ 1 Webブラウザで、HX Data Platform Installer VM の IP アドレスまたはノード名を入力します。**[承認（Acceot）]** または**[続行（Continue）]**をクリックしてSSL証明書エラーをバイパスします。[HX Data Platform Installer] ログインページで、ログイン画面の右下隅にある [HX Data Platform Installer **Build ID**] を確認します。

ステップ 2 ログイン ページで、次のクレデンシャルを入力します。

[ユーザ名（Username）]：`root`

[パスワード（Password）]（デフォルト）：`Cisco123`

注目 システムに同梱されているデフォルトのパスワード`Cisco123`は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

ステップ 3 [利用規約に同意します（I accept the terms and conditions）] チェック ボックスをオンにして、[ログイン（Login）] をクリックします。

ステップ 4 [ワークフローの選択（Select a Workflow）] ページで、[クラスタの作成（Create Cluster）] ドロップダウンリストから [標準クラスタ（Standard Cluster）] を選択します。

ステップ 5 [クレデンシャル（Credentials）] ページで、次の設定データを入力します。

フィールド	説明
UCS Manager のホスト名（UCS Manager Host Name）	UCS Manager の FQDN または IP アドレスを入力します。 たとえば、*10.193.211.120* とします。
UCS Manager のユーザー名（UCS Manager User Name）	[administrative username] を入力します。
パスワード（Password）	管理者パスワードを入力します。

vCenterクレデンシャル

フィールド	説明
vCenter サーバー（vCenter Server）	vCenter Server の FQDN または IP アドレスを入力します。 たとえば、*10.193.211.120* とします。 （注） • クラスタを動作可能にするには、その前に vCenter Server を準備する必要があります。 • vCenter のアドレスとクレデンシャルには、vCenter に対するルート レベルの管理者権限が必要です。 • ネストされた vCenter を構築する場合、vCenter Server の入力はオプションです。詳細については Nested vCenter TechNote を参照してください。
ユーザ名	管理者ユーザ名を入力します。 たとえば、*administrator@vsphere.local* とします。
[管理パスワード（Admin Password）]	管理者パスワードを入力します。

ステップ 6 [ハイパーバイザの設定（Hypervisor Configuration）] ページで、次の設定データを入力します。

ハイパーバイザのクレデンシャル

フィールド	説明
管理者ユーザー名（Admin User Name）	管理者ユーザ名を入力します。 工場出荷時のノードでのユーザ名は **root** です。

フィールド	説明
新しいパスワード（New Password）	重要　ハイパーバイザの工場出荷時パスワードを変更する必要があります。 次のガイドラインを使用してハイパーバイザの新しいパスワードを作成します。 • 長さは 6 ～ 80 字である必要があります。 • 1 個の大文字、1 個の小文字、1 個の数字、1 個の特殊文字が必要です。 • パスワードが大文字で始まる場合、2 個の大文字が必要です。 • パスワードが数字で終わる場合、2 桁の数字が必要です。
新しいパスワードの確認（Confirm New Password）	ハイパーバイザ用の新しいパスワードを再入力します。

ステップ 7 [続行（Continue）] をクリックして、HyperFlex サーバの関連付けを開始します。「HyperFlex サーバの関連付け （63 ページ）」を参照してください。

HyperFlex サーバの関連付け

[サーバの選択（Server Selection）] ページで、右側にある [構成（Configuration）] ペインの [クレデンシャル（Credentials）] に、使用されているクレデンシャルの詳細なリストが表示されます。[サーバの選択（Server Selection）] ページの [関連付けなし（Unassociated）] タブには、関連付けられていない HX サーバのリストが表示され、[関連付け済み（Associated）] タブには検出されたサーバのリストが表示されます。

フィールド	説明
ロケータ LED（Locator LED）	サーバーの検索をオンにします。
サーバー名（Server Name）	サーバーに割り当てられた名前。
Status（ステータス）	• アクセス不可—
モデル（Model）	サーバー モデルが表示されます。
シリアル（Serial）	サーバーのシリアル番号を表示します。

フィールド	説明
関連付けのステータス（Assoc State）	• 関連 • 関連付けなし
サービス プロファイル（Service Profile）（関連付けられたサーバーに対してのみ）	サーバーに割り当てられているサービス プロファイル。 （注） HyperFlex サービス プロファイル テンプレートの編集はお勧めしません。
アクション（Actions）	• **[KVM コンソールの起動（Launch KVM Console）]**: HX Data Platform から直接 KVM コンソールを起動するには、このオプションを選択します。 • [サーバの関連付け解除（Disassociate Server）]: サーバからサービス プロファイルを削除するには、このオプションを選択します。

始める前に

UCS Manager、vCenter、およびハイパーバイザ クレデンシャルの入力を完了していることを確認します。

ステップ 1 [サーバ ポートの構成（Configure Server Ports）] をクリックして新しい HX ノードを検出します。[サーバ ポートの構成（Configure Server Ports）] ダイアログボックスに、サーバ ポートとして構成されるすべてのポートが一覧表示されます。[構成（Configure）] をクリックします。

（注） 一般的に、構成を始める前に、サーバ ポートは Cisco UCS Manager で構成されます。

ステップ 2 HyperFlex クラスタに含める **[関連付けなし（Unassociated）]** タブの下のサーバを選択します。

HX サーバがこのリストに表示されない場合は、[Cisco UCS Manager] をオンにして、検出されていることを確認します。

（注） 関連付けられていないサーバがない場合は、次のエラー メッセージが表示されます。

```
No unassociated servers found. Login to UCS Manager and ensure server ports are enabled.
```

ステップ 3 [続行（Continue）] をクリックして、UCS Manager の構成を続けます。「UCS Manager の設定 （65 ページ）」を参照してください。

UCS Manager の設定

[UCSM 構成（UCSM Configuration）] ページでは、CIMC、iSCSi ストレージ、FC ストレージに関する VLAN、MAC プール、「hx-ext-mgmt」IP プールを構成できます。

始める前に

HyperFlex クラスタにサーバを関連付けます。HyperFlex サーバの関連付け （63 ページ）を参照してください。

ステップ 1 [VLAN 設定（VLAN Configuration）] セクションで、次のフィールドに値を入力します。

（注） 次のそれぞれのネットワークに、別個のサブネットと VLAN を使用します。

フィールド	説明
ハイパーバイザとHyperFlex管理用のVLAN	
VLAN 名	hx-inband-mgmt
VLAN ID（Admin. VLAN ID）	デフォルト：3091
HyperFlexストレージトラフィック用のVLAN	
VLAN 名	hx-storage-data
VLAN ID（Admin. VLAN ID）	デフォルト: 3092
VM vMotion用のVLAN	
VLAN 名	hx-vmotion
VLAN ID（Admin. VLAN ID）	デフォルト: 3093
VMネットワーク用のVLAN	
VLAN 名	vm-network
VLAN ID	デフォルト: 3094 ゲスト VLAN のカンマ区切りリスト。

ステップ 2 [MAC プール（MAC Pool）] セクションの [MAC プールのプレフィックス（MAC Pool Prefix）] で、追加の 2 つの 16 進文字（0 ～ F）を指定して MAC プールのプレフィックスを構成します。

（注） すべての UCS ドメインにわたり、他の MAC アドレス プールで使用とされていないプレフィックスを選択します。

```
Example:
00:25:B5:A0:
```

ステップ 3 **[CIMC の 'hx-ext-mgmt' IP プール（'hx-ext-mgmt' IP Pool for CIMC）]** セクションで、次のフィールドに値を入力します。

フィールド	説明
[IP Blocks]	各 HyperFlex サーバーの CIMC に割り当てられた管理 IP アドレスの範囲。IP アドレスは範囲として指定し、複数の IP ブロックをカンマ区切りのリストとして指定できます。クラスタ内のサーバごとに少なくとも 1 つの一意の IP があることを確認します。アウトオブバンドの使用を選択する場合、この範囲はファブリック インターコネクトの mgmt0 インターフェイスで使用されているものと同じ IP サブネットに属している必要があります。 たとえば、*10.193.211.124-127, 10.193.211.158-163* などです。
[Subnet Mask]	上記の IP 範囲のサブネット マスクを指定します。 たとえば、 *255.255.0.0* とします。
[ゲートウェイ（Gateway）]	ゲートウェイの IP アドレスを入力します。 たとえば、*10.193.0.1* とします。

サーバー上の CIMC へのアクセスに使用される管理 IP アドレスは、次のいずれかです。

- **アウトオブバンド**：CIMC 管理トラフィックは、ファブリック インターコネクト上の制限帯域幅管理インターフェイス mgmt0 を介してファブリックインターコネクトを通過します。このオプションは最も一般的に使用され、ファブリック インターコネクト管理 VLAN と同じ VLAN を共有します。
- **インバンド**：CIMC 管理トラフィックは、ファブリック インターコネクトのアップリンク ポートを介してファブリック インターコネクトを通過します。この場合、管理トラフィックに使用できる帯域幅は、ファブリックインターコネクトのアップリンク帯域幅に相当します。インバンドオプションを使用している場合、Cisco HyperFlex インストーラは CIMC 管理通信専用の VLAN を作成します。このオプションは、Windows Server インストール ISO などの大きなファイルを OS インストール用の CIMC にマウントする必要がある場合に便利です。このオプションは、HyperFlex インストーラ VM でのみ使用でき、Intersight を介した展開には使用できません。

ステップ 4 CIMC 管理アクセスに使用する接続のタイプに基づいて、**アウトオブバンド** または **インバンド** を選択します。[インバンド（In-band）] を選択した場合は、管理 VLAN の VLAN ID を指定します。シームレスな接続のために、アップストリーム スイッチに CIMC 管理 VLAN を作成してください。

ステップ 5 外部ストレージを追加する場合は、次のフィールドに値を入力して [iSCSI ストレージ（iSCSI Storage）] を構成します。

フィールド	説明
[iSCSI ストレージの有効化（Enable iSCSI Storage）] チェックボックス	iSCSI ストレージを構成する場合、このチェックボックスをオンにします。
VLAN A 名（VLAN A Name）	プライマリ ファブリック インターコネクト（FI-A）で、iSCSI vNIC に関連付けらている VLAN の名前。
VLAN A ID	プライマリ ファブリック インターコネクト（FI-A）で、iSCSI vNIC に関連付けらている VLAN の ID。
VLAN B 名（VLAN B Name）	下位のファブリック インターコネクト（FI-B）で、iSCSI vNIC に関連付けらている VLAN の名前。
[VLAN B ID]	下位のファブリック インターコネクト（FI-A）で、iSCSI vNIC に関連付けらている VLAN の ID。

ステップ 6 外部ストレージを追加する場合は、次のフィールドに値を入力して [FC ストレージ（FC Storage）] を構成します。

フィールド	説明
[FC ストレージの有効化（Enable FC Storage）] チェックボックス	FC ストレージを有効にするには、このチェックボックスをオンにします。
WWxNプール	WW ノード名と WW ポート名の両方を含む WWN プール。それぞれのファブリック インターコネクトに対し、WWPN および WWNN 用の WWxN プールが作成されます。
VSAN A 名（VSAN A Name）	プライマリ ファブリック インターコネクト（FI-A）の VSAN の名前。 デフォルト—`hx-ext-storage-fc-a`。
VSAN A ID	プライマリ ファブリック インターコネクト（FI-A）のネットワークに割り当てられた一意の ID。 **注意** UCS または HyperFlex システムで現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。
VSAN B名	下位のファブリック インターコネクト（FI-B）の VSAN の名前。 デフォルト—`hx-ext-storage-fc-b`.

フィールド	説明
VSAN B ID	下位のファブリック インターコネクト（FI-B）のネットワークに割り当てられた一意の ID。 **注意** UCS または HyperFlex システムで現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。

ステップ 7 [詳細設定（Advanced）] セクションで、次の操作を行います。

フィールド	説明
UCS サーバー ファーム ウェアバージョン（UCS Server Firmware Version）	ドロップダウン リストから、HX サーバと関連付ける UCS サーバ ファームウェア バージョンを選択します。UCS ファームウェア バージョンは、UCSM バージョンと一致する必要があります。詳細については、最新の『Cisco HX Data Platform Release Notes』を参照してください。 たとえば、*3.2(1d)* とします。
HyperFlexクラスタ名	ユーザ定義の名前を指定します。HyperFlex クラスタ名は、特定のクラスタ内の HX サーバ グループに適用されます。HyperFlex クラスタ名によりサーバ プロファイルにラベルが追加され、クラスタを識別しやすくなります。
組織名	HyperFlex 環境を UCS ドメインの残りの部分から確実に分離できるような一意の組織名 を指定します。

ステップ 8 [続行（Continue）] をクリックして、ハイパーバイザの構成を続けます。「ハイパーバイザの構成 （69 ページ）」を参照してください。

ハイパーバイザの構成

（注） [ハイパーバイザの構成（Hypervisor Configuration）] ページの [構成（Configuration）] ペインで、VLAN、MAC プル、IP アドレス プールの情報を確認します。これらの VLAN ID は、環境によって変更されている可能性があります。デフォルトでは、HX Data Platform インストーラが VLAN を非ネイティブとして設定します。トランク構成を適切に適用することで、非ネイティブ VLAN に対応するアップストリーム スイッチを構成する必要があります。

注目 再インストールの場合、ESXi ネットワーキングが完了していれば、ハイパーバイザの構成をスキップできます。

始める前に

アウトオブバンド CIMC の VLAN、MAC プール、「hx-ext-mgmt」IP プールを構成します。外部ストレージを追加する場合は、iSCSI ストレージと FC ストレージを構成します。UCS サーバのファームウェア バージョンを選択し、HyperFlex クラスタの名前を割り当てます。UCS Manager の設定 （65 ページ）を参照してください。

ステップ 1 [共通ハイパーバイザ設定の構成（Configure Common Hypervisor Settings）] セクションで、次のフィールドに値を入力します。

フィールド	説明
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、*255.255.0.0* とします。
[ゲートウェイ（Gateway）]	ゲートウェイの IP アドレス。 たとえば、*10.193.0.1* とします。

フィールド	説明
[DNSサーバ（DNS Server(s)）]	DNS サーバの IP アドレス。 （注） • DNS サーバを使用しない場合、HX Data Platform インストーラの **[クラスタの設定（Cluster Configuration）]**ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。 • 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。

ステップ 2 [ハイパーバイザ設定（Hypervisor Settings）] セクションで、[IP アドレスとホスト名を順番に選択（Make IP Addresses and Hostnames Sequential）] を選択し、連続的な IP アドレスにします。次のフィールドに入力します。

（注） ドラッグ アンド ドロップ操作を使用してサーバの順番を並び替えることができます。

フィールド	説明
名前（Name）	サーバーに割り当てられた名前。
ロケータ LED（Locator LED）	サーバーの検索をオンにします。
シリアル（Serial）	サーバーのシリアル番号を表示します。
スタティックIPアドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。
ホスト名	ホスト名フィールドを空のままにしないでください。

ステップ 3 [続行（Continue）] をクリックして、IP アドレスの構成を続けます。「IP アドレスの設定 （71 ページ）」を参照してください。

IP アドレスの設定

始める前に

[ハイパーバイザ設定（Hypervisor Configuration）] ページでハイパーバイザの設定が完了していることを確認します。ハイパーバイザの構成 （69 ページ）を参照してください。

ステップ 1 [IP アドレス（IP Addresses）] ページで、[IP アドレスを連続させる（Make IP Addresses Sequential）] を選択し、連続的な IP アドレスにします。

ステップ 2 ハイパーバイザ、ストレージ コントローラ（管理）とハイパーバイザ、ストレージ コントローラ（データ）列の最初の行に IP アドレスを入力すると、 HX Data Platform Installer により、残りのノードのノード情報が増分されて自動入力されます。ストレージ クラスタ内のノードの最小数は 3 です。それより多くのノードがある場合は、**[追加（Add）]** ボタンを使用して、アドレス情報を指定します。

（注） コンピューティング専用ノードは、ストレージ クラスタを作成してからでないと追加できません。

各 HX ノードについて、ハイパーバイザ、ストレージ コントローラ、管理、データ IP アドレスを入力します。IP アドレスには、ネットワークがデータ ネットワークと管理ネットワークのどちらに属しているかを指定します。

フィールド	説明
管理ハイパーバイザ	ESXi ホストとストレージ コントローラ間のハイパーバイザ管理ネットワーク接続を処理するスタティック IP アドレスを入力します。
管理ストレージコントローラ	ストレージ コントローラ VM とストレージ クラスタ間のストレージ コントローラ VM 管理ネットワーク接続を処理する静的 IP アドレスを入力します。
Data Hypervisor	ESXi ホストとストレージ コントローラ間のハイパーバイザ データ ネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージ コントローラ	ストレージ コントローラ VM とストレージ クラスタの間のストレージ コントローラ VM データ ネットワーク接続を処理するスタティック IP アドレスを入力します。

ステップ 3 ここで指定する IP アドレスは、ストレージ クラスタ内の 1 つのノードに適用されます。ノードが使用できなくなった場合は、該当する IP アドレスがストレージ クラスタ内の別のノードに移動されます。すべてのノードには、これらの IP アドレスを受け入れるように構成されたポートが必要です。

次の IP アドレスを指定します。

フィールド	説明
管理クラスタ データの IP アドレス（**Management Cluster Data IP Address**）	HXデータ プラットフォーム ストレージ クラスタの管理ネットワーク IP アドレスを入力します。
データ クラスタ データ IP アドレス（**Data Cluster Data IP Address**）	HX Data Platform ストレージ クラスタのデータ ネットワークの IP アドレスを入力します。
管理サブネットマスク	VLAN と vSwitch のサブネット情報を入力します。 管理ネットワークの値を入力します。たとえば、*255.255.255.0* と入力します。
データサブネットマスク	データ ネットワークのネットワークの値を入力します。たとえば、*255.255.255.0* と入力します。
管理ゲートウェイ	管理ネットワークのネットワークの値を入力します。たとえば、*10.193.0.1* とします。
データゲートウェイ	データ ネットワークのネットワークの値を入力します。たとえば、*10.193.0.1* とします。

ステップ 4 [続行] をクリックして HyperFlex クラスタを設定します。「HyperFlex クラスタの設定 （72 ページ）」を参照してください。

HyperFlex クラスタの設定

[クラスタ構成（Cluster Configuration）] ページで、Cisco HX ストレージ クラスタに関する以下のフィールドに値を入力し、HyperFlex クラスタの導入を開始します。

始める前に

[IP アドレス（IP Addresses）] ページで IP アドレスの構成が完了していることを確認します。IP アドレスの設定 （71 ページ）を参照してください。

ステップ 1 [Cisco HX クラスタ（Cisco HX Cluster）] セクションで、次のフィールドに値を入力します。

フィールド	説明
クラスタ名（**Cluster Name**）	HXデータ プラットフォーム ストレージ クラスタの名前を指定します。

フィールド	説明
レプリケーション ファクタ（**Replication Factor**）	ストレージクラスタ全体でのデータの冗長レプリカの数を指定します。レプリケーションファクタを冗長レプリカ数 2 または 3 に設定します。 • ハイブリッド サーバ（SSD と HDD を含むサーバ）の場合、デフォルト値は 3 です。 • フラッシュ サーバー（SSD のみを含むサーバー）の場合は、2 または 3 を選択します。 • Hyperflex Edge を除くすべての環境で複製ファクタ 3 を強く推奨しています。複製ファクタ 2 では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。

ステップ 2 **[コントローラ VM（Controller VM）]** セクションで、HyperFlex クラスタの管理者ユーザの新しいパスワードを作成します。

コントローラ VM には、デフォルトの管理者ユーザ名とパスワードが適用されます。VM は、コンバージド ノードとコンピューティング専用ノードのすべてにインストールされます。

重要
- コントローラ VM またはコントローラ VM のデータストアの名前を変更することはできません。
- すべてのコントローラ VM に同じパスワードを使用します。異なるパスワードの使用はサポートされていません。
- 1 つの大文字、1 つの小文字、1 つの数字、1 つの特殊文字を含む、10 文字以上の複雑なパスワードを指定してください。
- コントローラ VM と、作成される HX クラスタには、ユーザ定義のパスワードを指定できます。パスワードに使用できる文字と形式に関する制限事項については、『*Cisco HX Data Platform Management Guide*』のセクション「Guidelines for HX Data Platform Special Characters」を参照してください。

ステップ 3 [vCenter の設定（vCenter Configuration）] セクションで、次のフィールドに値を入力します。

フィールド	説明
vCenter データセンター名（vCenter Datacenter Name）	Cisco HyperFlex クラスタの vCenter データセンターの名前を入力します。
vCenter クラスタ名（vCenter Cluster Name）	vCenter クラスタ名を入力します。

ステップ 4 [システム サービス（System Services）] セクションで、次のフィールドに値を入力します。

DNS サーバー（DNS Server(s)）	各 DNS サーバーの IP アドレスのカンマ区切りリスト。
NTP サーバー（NTP Server(s)）	各 NTP サーバの IP アドレスのカンマ区切りリスト。 （注） すべてのホストが同じ NTP サーバを使用して、ストレージ コントローラ VM と ESXi ホストで実行されているサービスの間でクロックを同期する必要があります。
DNS ドメイン名（DNS Domain Name）	DNS FQDN または IP アドレスが無効です
タイム ゾーン（Time Zone）	コントローラ VM のローカル タイム ゾーン。このタイム ゾーンに基づいて、スケジュールされたスナップショットを取るタイミングが決定されます。スケジュールされたネイティブ スナップショット アクションは、この設定に基づきます。

ステップ 5 [**コネクテッド サービス (Connected Services)**] セクションで、[**コネクテッド サービスを有効にする (Enable Connected Services)**] を選択して、自動サポート (Auto Support) および Intersight Management を有効にします。

フィールド	説明
コネクテッド サービスの有効化（Enable Connected Services）（推奨）	自動サポート (Auto Support) および Intersight Management を有効にします。HX Connect にログオンしてこれらのサービスを構成するか、またはそれらを選択的に**オン**または**オフ**にします。
サービス チケット通知の送信先（Send service ticket notifications to）	自動サポートによってトリガーされたときに SR 通知が送信される電子メール アドレス。

ステップ 6 [詳細設定（Advanced）] セクションで、次の操作を行います。

フィールド	説明
ジャンボ フレーム **ジャンボ フレームを有効化（Enable Jumbo Frames）**	ホスト vSwitches と vNIC、および各ストレージ コントローラ VM 上のストレージ データ ネットワークの MTU サイズを設定する場合は、このチェックボックスをオンにします。 デフォルト値は 9000 です。 （注） MTU サイズを 9000 以外の値に設定するには、Cisco TAC にご連絡ください。

フィールド	説明
ディスク パーティション ディスク パーティションのクリーン アップ（**Clean up Disk Partitions**）	ストレージクラスタに追加されたすべてのノードから既存のデータとパーティションをすべて削除して手動でサーバを準備する場合は、このチェックボックスをオンにします。既存のデータやパーティションを削除するには、このオプションを選択します。保持する必要があるデータはすべてバックアップする必要があります。 **注目** 工場で準備されたシステムの場合は、このオプションを選択しないでください。工場で準備されたシステムのディスクパーティションは正しく設定されています。
仮想デスクトップ**(VDI)**	VDI のみの環境でオンにします。 （注） ストレージ クラスタの作成後に VDI 設定を変更するには、リソースをシャットダウンまたは移動し、変更を加え (下の手順に記載)、クラスタを再起動します。 デフォルトでは、HyperFlex クラスタは VSI ワークロード用にパフォーマンス調整されるように設定されています。 このパフォーマンスのカスタマイズは、Hyperflex Data Platform クラスタで次の手順を実行することによって変更できます。HyperFlex クラスタを VDI から VSI ワークロード (またはその逆) に変更するには、次のようにします。 警告: メンテナンス ウィンドウが必要です。これにより、クラスタがオフラインの間はデータが使用できなくなります。 **1.** `~#stcli cluster shutdown` を実行してクラスタをシャット ダウンします。 **2.** すべてのコントローラ VM の storfs cfg を編集し、workloadType を Vsi または Vdi に変更します。 **3.** クラスタの作成後に、クラスタを起動し (`stcli cluster start`)、調整の変更を有効にします。

フィールド	説明
(オプション) vCenter Server のシングル サインオン（vCenter Single-Sign-On Server）	この情報は、SSO URL が到達可能でない場合のみ必要です。 （注） このフィールドは使用しないでください。これはレガシー展開に使用されます。 **[vCenter Server]** > **[Manage]** > **[Advanced Settings]** > **[key config.vpxd.sso.sts.uri]** にナビゲートして、vCenter で SSO URL を見つけることができます。

ステップ 7 **[開始（Start）]** をクリックして HyperFlex クラスタの展開を開始します。[進捗状況（Progress）] ページには、さまざまな設定タスクの進捗状況が表示されます。

注意 確認に関する警告を無視しないでください。

詳細については、「**警告**」セクションを参照してください。

次のタスク

- 検証エラーによっては、パラメータの再入力が必要になることがあります（たとえば、無効な ESXi パスワード、誤った NTPサーバ、不良 SSO サーバなどの誤った入力が原因のエラー）。**[値の再入力（Re-enter Values）]** をクリックして **[クラスタ構成（Cluster Configuration）]** ページに戻り、問題を解決します。
- これが完了すると、HyperFlex サーバがインストールされ、構成されます。正常にデプロイされたクラスタのステータスは、[オンライン（Online）] および [正常（Healthy）] として示されます。
- [HyperFlex Connect の起動 （Launch HyperFlex Connect）] をクリックし、データストアを作成してクラスタを管理します。

HyperFlex ハードウェア アクセラレーション カードの取り付けの確認

HyperFlex ハードウェア アクセラレーション カードが正常にインストールされたことを確認するには、次の手順を実行します。

ステップ 1 コントローラ VM にログインします。

ステップ 2 次の調整ファイルを探します。 `/opt/springpath/config/offload.tunes`

（注） 調整ファイルは、システム管理者とルート ユーザーのみが表示できます。これらのユーザーがこのファイルにアクセスできる場合、インストールは成功しています。システム管理者またはルート ユーザー権限を持っていない場合は、UI にエラー メッセージまたはイベント存在しないことで、インストールが成功したことを確認できます。

HyperFlex ハードウェア アクセラレーション カードのトラブルシューティング

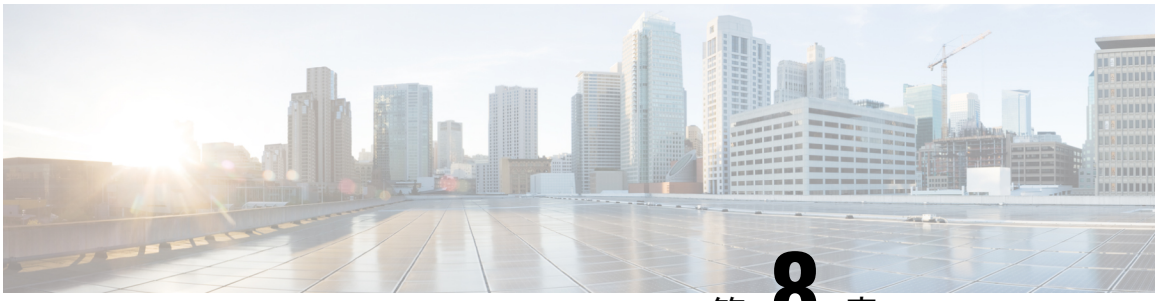
次のように、インストール後の HyperFlex ハードウェア アクセラレーション カードに関連する問題をトラブルシューティングします。

症状	回避策
クラスタは動作していますが、vCenter と HX Connect UI で汎用アラートに注意するようにしてください。	サポートについては、Cisco の営業担当者にご連絡ください。
NR ペアリングが試行されると、クラスタはペアリング エラーを報告します。	いずれかのクラスタが 4.5(1a) より前のリリースであり、HX ハードウェア アクセラレーション カードで有効になっている場合、NR ペアリングは許可されません。 HX ハードウェア アクセラレーション カードとの NR ペアリングは、ペアの両方のクラスタに HX ハードウェア アクセラレーション カードがある場合にのみサポートされます。

HyperFlex ハードウェア アクセラレーション カードのに関する追加情報

HyperFlex ハードウェア アクセラレーション カードに関するその他の注意事項は、次のとおりです。

- 圧縮ゲインの値は、HX connect UI ダッシュボードに表示されます。
- 次のコマンドを使用して、8K の読み取りワークロードのパフォーマンスを向上させます。
  - **root @ ucs984scvm: ~ # echo 3 >/sys/module/fdma/parameters/decompress_min_t**
  - **root@ucs984scvm:~# echo 3 > /sys/module/fdma/parameters/decompress_max_t**



第 8 章

クラスタ設定後のタスク

クラスタ設定後のガイドライン

重要

- すべての ESXi ホストで SSH を有効なままにしてください。これは、これ以降の Cisco HyperFlex post クラスタ設定後の作業で必要となります。
- これらの事前設定された値は、シスコの承認を得ずに変更しないでください。

ホスト上のネットワーク デバイスの PCI パススルー有効化

パススルーデバイスは、より効率的にリソースを使用して環境内のパフォーマンスを向上させるための手段を提供します。PCI パススルーを有効化することで、VM はホスト デバイスを、VM に直接接続されているように使用できます。

⚠

注意 HXDP クラスタの重要なデバイスを PCI パススルー用にセットアップしないでください。

次の手順では、ESXi ホスト上の PCI パススルー用にネットワーク デバイス（NVIDIA GPU など）を設定する方法を説明します。

ステップ 1 vSphere Client のナビゲーション パネルで ESXi ホストを参照します。

ステップ 2 GPU がインストールされているノードで、HX メンテナンス モードを開始します。メンテナンス モードを開始するには、ノードを右クリックし、**[Cisco HX Maintenance Mode (Cisco HX メンテナンス モード)>]** > **[Enter HX Maintenance Mode (HX メンテナンス モードの開始)]** の順に選択します。

ステップ 3 新しいブラウザ ウィンドウで、ESXi ノードに直接ログインします。

ステップ 4 [Manage] をクリックします。

ステップ 5 [Hardware] タブで、 [PCI Devices] をクリックします。利用可能なパススルー デバイスのリストが表示されます。

ステップ 6 パススルーに対して有効にする PCI デバイスを選択します。**[Toggle passthrough (パススルーのトグル)]** をクリックします。

ステップ 7 ホストを再起動して、PCI デバイスを利用可能にします。

ステップ 8 リブートが完了したら、ノードがメンテナンス モードになっていないことを確認します。

ステップ 9 vCenter Server にログインします。

ステップ 10 VM を検索して右クリックし、**[Edit Settings (設定の編集)]** を選択します。

ステップ 11 [New device] ドロップダウン メニューで [PCI Device] を選択して、[Add] をクリックします。

ステップ 12 使用するパススルー デバイス（例：NVIDIA GPU）をクリックして、[OK] をクリックします。

ステップ 13 ESXi ホストにログインし、仮想マシンの構成ファイル（.vmx）をテキスト エディタで開きます。

```
cd /vmfs/volumes/[datastore_name]/[vm_name]
vi [vmname].vmx
```

ステップ 14 次の行を追加して保存し、テキスト エディタを終了します。

```
# pciPassthru.64bitMMIOSizeGB = "64"
# Firmware = "efi"
# pciPassthru.use64bitMMIO = "TRUE"
```

インストール後のスクリプトの実行

インストーラ後のスクリプトを実行することで、インストール後のタスクを完了できます。

重要
- HyperFlex System を展開した後、ただちに *hx_post_install* を実行して、ネットワークの動作を確認してください。

1. SSH クライアントを使用して、admin ログインを使用してクラスタ仮想 IP に接続します。
2. 「`hx_post_install`」と入力して、`Enter` キーを押します。
3. 次の表に指定しているように、インストール後スクリプト パラメータを設定します。

（注） インストール後スクリプトに問題が発生した場合は、インストール後スクリプトのパラメータを手動で設定します。

パラメータ	説明
Enable HA/DRS on cluster?（クラスタで HA/DRS を有効にするか）	ベスト プラクティスに従って vSphere 高可用性（HA）機能を有効にします。
Disable SSH warning?（SSH 警告を無効にするか）	vCenter 内での SSH 警告とシェル警告を抑制します。
Add vMotion interfaces（vMotion インターフェイスの追加）	ベスト プラクティスに従って vMotion インターフェイスを設定します。*IP* アドレスと *VLAN ID* の入力が必要です。
Add VM network VLANs（VM ネットワーク VLAN の追加 ）	すべてのクラスタ ホスト上の ESXi 内、および Cisco UCS Manager にゲスト VLAN を追加します。

4. ネットワーク エラーが報告された場合には修正します。

サンプルのインストール後のスクリプト: オプション 1 新規/既存のクラスタ

```
admin@SpringpathController:~$ hx_post_install

Select hx_post_install workflow-

1. New/Existing Cluster
2. Expanded Cluster (for non-edge clusters)
3. Generate Certificate
```

```
Note: Workflow No.3 is mandatory to have unique SSL certificate in the cluster. By
Generating this certificate, it will replace your current certificate. If you're performing
 cluster expansion, then this option is not required.

Selection: 1
Logging in to controller HX-01-cmip.example.com
HX CVM admin password:
Getting ESX hosts from HX cluster...
vCenter URL: 192.168.202.35
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Found datacenter HX-Clusters
Found cluster HX-01

post_install to be run for the following hosts:
HX-01-esxi-01.example.com
HX-01-esxi-02.example.com
HX-01-esxi-03.example.com

Enter ESX root password:

Enter vSphere license key? (y/n) n

Enable HA/DRS on cluster? (y/n) y
Successfully completed configuring cluster HA.

Disable SSH warning? (y/n) y

Add vmotion interfaces? (y/n) y
Netmask for vMotion: 255.255.254.0
VLAN ID: (0-4096) 208
vMotion MTU is set to use jumbo frames (9000 bytes). Do you want to change to 1500 bytes?
 (y/n) y
vMotion IP for HX-01-esxi-01.example.com: 192.168.208.17
Adding vmotion-208 to HX-01-esxi-01.example.com
Adding vmkernel to HX-01-esxi-01.example.com
vMotion IP for HX-01-esxi-02.example.com: 192.168.208.18
Adding vmotion-208 to HX-01-esxi-02.example.com
Adding vmkernel to HX-01-esxi-02.example.com
vMotion IP for HX-01-esxi-03.example.com: 192.168.208.19
Adding vmotion-208 to HX-01-esxi-03.example.com
Adding vmkernel to HX-01-esxi-03.example.com

Add VM network VLANs? (y/n) y
 Attempting to find UCSM IP
 Found UCSM 10.75.61.254, logging with username admin.  Org is HX-Cluster
 UCSM Password:
 Port Group Name to add (VLAN ID will be appended to the name): USERS
 VLAN ID: (0-4096) 1219
 Adding VLAN 1219 to FI
 Adding VLAN 1219 to vm-network-a VNIC template
 Adding USERS-1219 to HX-01-esxi-01.example.com
 Adding USERS-1219 to HX-01-esxi-02.example.com
 Adding USERS-1219 to HX-01-esxi-03.example.com
Add additional VM network VLANs? (y/n) n

Run health check? (y/n) y

Validating cluster health and configuration...

Cluster Summary:
Version - 4.5.1a-39020
Model - HXAF220C-M5SX
Health - HEALTHY
```

```
ASUP enabled - False
admin@SpringpathController:~$
```

サンプルのインストール後のスクリプト: オプション 3 Generate Certificate

```
admin@SpringpathController:~$ hx_post_install

Select post_install workflow-

 1. New/Existing Cluster
 2. Expanded Cluster
 3. Generate Certificate

 Note:  Workflow No.3 is mandatory to have unique SSL certificate in the cluster.
 By Generating this certificate, it will replace your current certificate.
 If you're performing cluster expansion, then this option is not required.

 Selection: 3
 Certificate generation workflow selected

Logging in to controller 10.20.1.64
HX CVM admin password:
Getting ESX hosts from HX cluster...

Select Certificate Generation Workflow-

 1. With vCenter
 2. Without vCenter

 Selection: 1
vCenter URL: 10.33.16.40
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Starting certificate generation and re-registration.
Trying to retrieve vCenterDatacenter information ....
Trying to retrieve vCenterCluster information ....
Certificate generated successfully.
Cluster re-registration in progress ....
Cluster re-registered successfully.
admin@SpringpathController:~$
```

ネットワーク エラーの例

```
Host: esx-hx-5.cpoc-rtp.cisco.com
No errors found

Host: esx-hx-6.cpoc-rtp.clsco.com
No errors found

Host: esx-hx-1.cpoc-rtp.cisco.com
No errors found

Host: esx-hx-2.cpoc-rtp.cisco.com
No errors found

controller VM clocks:
stctlVM-FCH1946V34Y - 2016-09-16 22:34:04
stCtlVM-FCH1946V23M - 2016-09-16 22:34:04
stctIVM-FCH1951V2TT - 2016-09-16 22:34:04
stctlVM-FCH2004VINS - 2016-09-16 22:34:04

Cluster:
```

```
Version - 1.8.1a-19499
Model - HX220C-M4S
Health - HEALTHY
Access policy - LENIENT
ASUP enabled - False
SMTP server - smtp.cisco.com
```

ESXi ホストのルート パスワードの変更

次のシナリオで、デフォルトの ESXi パスワードを変更できます。

- 標準およびストレッチ クラスタの作成時（コンバージド ノードのみをサポート）
- 標準クラスタの拡張時 （コンバージド ノードまたはコンピューティング ノードの両方の拡張をサポート）
- エッジ クラスタの作成時

（注） 上記の場合、インストールが完了するとすぐに ESXi のルート パスワードが保護されます。後続のパスワード変更が必要である場合、下に概要を示している手順をインストール後に使用して、ルート パスワードを手動で変更することができます。

ESXi は工場出荷時のデフォルト パスワードで提供されているため、セキュリティ上の理由からパスワードを変更する必要があります。インストール後のデフォルトの ESXi ルート パスワードを変更するには、次の手順を実行します。

（注） ESXi ルート パスワードを忘れた場合は、パスワードの復旧について Cisco TAC にお問い合わせください。

ステップ 1 SSH を使用して ESXi ホスト サービス制御にログインします。

ステップ 2 ルート権限を取得します。

```
su -
```

ステップ 3 現在のルート パスワードを入力します。

ステップ 4 ルート パスワードを変更します。

```
passwd root
```

ステップ 5 新しいパスワードを入力し、**Enter** キーを押します。確認のためにパスワードを再入力します。

（注） 2 回目に入力したパスワードが一致しない場合は、最初からやり直す必要があります。

ストレージ コントローラのパスワードの変更

インストール後に HyperFlex ストレージ コントローラのパスワードをリセットするには、次の手順を実行します。

ステップ 1 ストレージ コントローラ VM にログインします。

ステップ 2 Cisco HyperFlex ストレージ コントローラ パスワードを変更します。

```
# stcli security password set
```

このコマンドによって、ストレージ クラスタ内のすべてのコントローラ VM に変更が適用されます。

（注） 新しいコンピューティング ノードを追加し、**stcli security password set** コマンドを使用してクラスタ パスワードをリセットしようとすると、コンバージド ノードは更新されますが、コンピューティング ノードはデフォルト パスワードのままになることがあります。コンピューティング ノードのパスワードを変更するには、次の手順を使用します。

ステップ 3 新しいパスワードを入力します。

ステップ 4 **Enter** を押します。

VMware vCenter の Cisco HyperFlex HTML プラグイン

Cisco HyperFlex vCenter プラグインは、vSphere Web クライアントと統合され、HX Data Platform のインストール後の管理およびモニタリング機能をすべてサポートします。インストールと使用法に関する完全な情報については、『Cisco HyperFlex Data Platform Administration Guide』の「Cisco HyperFlex HTML Plugin for VMware vCenter」の章を参照してください。

ストレージ クラスタでのデータストアの追加

新しい HyperFlex クラスタでは、仮想マシン ストレージ用のデフォルト データストアが設定されていないため、VMware vSphere Web クライアントを使用してデータストアを作成する必要があります。

（注） 高可用性を実現するために、最低 2 つのデータストアを作成することを推奨します。

ステップ 1 Web クライアント ナビゲータの **[Global Inventory Lists]** で、**[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > **[cluster]** > **[Manage]** > **[Datastores]** の順に展開します。

ステップ 2 [データストアの作成（Create Datastore）] アイコンをクリックします。

ステップ 3 データストアの**名前**を入力します。vSphere Web クライアントはデータストア名に 42 文字の制限を適用します。各データストアに固有の名前を割り当てます。

ステップ 4 データストアの**サイズ**を指定します。ドロップダウンリストから、[GB] または [TB] を選択します。[OK] をクリックします。

ステップ 5 新しいデータストアを表示するには、[Refresh] ボタンをクリックします。

ステップ 6 新しいデータストアの [マウント ステータス（Mount Status）] を表示するには、[ホスト（Hosts）] タブをクリックします。

HA ハートビートの設定

vSphere HA の設定では、使用可能なデータストアのリストから任意のデータストアを選択できるように、[ハートビーティングのデータストア（Datastore for Heartbeating）] オプションを必ず設定してください。

ステップ 1 vSphere にログインします。

ステップ 2 DRS が有効になっていることを確認します。

vSphere の**[ホーム (Home)]** > **[ホストとクラスタ (Hosts and Clusters)]** > 、**[クラスタ (cluster)]** > **[設定 (Configure)]**、**[サービス (Services)]**を選択します。[vSphere DRS] をクリックします。

ステップ 3 [Edit] ボタンをクリックします。[vSphere HA] をクリックします。[編集（Edit）] をクリックします。

ステップ 4 選択されていなければ、**[vSphere HA をオンにする (Turn on vSphere HA)]** を選択します。

ステップ 5 ドロップダウン メニューから **[アドミッション コントロール (Admission Contro)l]** > **[フェールオーバ容量の定義 (Define Fallover capacity by)]** > **[クラスタ リソース割合 (Cluster resource percentage)]** を展開します。デフォルト値を使用することも、[Override calculated failover capacity] を有効にしてパーセンテージを入力することもできます。

ステップ 6 [Heartbeat Datastores] を展開し、[Use datastore only from the specified list] を選択します。含めるデータストアを選択します。

ステップ 7 [OK] をクリックします。

HyperFlex の自動サポートと Smart Call Home

HX ストレージクラスタを構成して、文書化されたイベントに関する自動化された電子メール通知を送信することができます。通知内の収集されたデータを使用して、HX ストレージクラスタの問題のトラブルシューティングに役立てることができます。

（注） Auto Support (ASUP) および Smart Call Home (SCH) は、プロキシ サーバの使用をサポートしています。プロキシ サーバの使用を有効にし、HX Connect を使用して、両方のプロキシ設定を構成できます。

Auto Support（ASUP）

Auto Support は、HX Data Platform を通じて提供されるアラート通知サービスです。Auto Support を有効にすると、HX Data Platform から、指定されたメール アドレスまたは通知を受信したい電子メール エイリアスに通知が送信されます。通常、Auto Support は、HX ストレージ クラスタの作成時に、SMTP メール サーバを設定し、電子メールの受信者を追加して設定します。

（注） 未認証の SMTP のみが ASUP のサポート対象となります。

構成中に **[Enable Auto Support (Auto Support を有効にする)]** チェック ボックスが選択されていない場合、次の方法を使用して Auto Support をクラスタの作成後に有効にすることができます。

クラスタ作成後の ASUP 構成方法	関連トピック
HX Connect ユーザ インターフェイス	HX Connect を使用した自動サポートの設定 （140 ページ）
コマンドライン インターフェイス（CLI）	CLI を使用した通知設定の構成 （141 ページ）
REST API	Cisco HyperFlex は Cisco DevNet での REST API をサポートします。

Auto Support は、監視ツールに HX ストレージ クラスタを接続するためにも使用できます。

Smart Call Home（SCH）

Smart Call Home は、HX ストレージ クラスタを監視し、ビジネスの運営に影響をおよぼす前に問題にフラグ付けして解決を開始する、自動化されたサポート機能です。これにより高いネットワーク可用性と運用効率の向上をもたらします。

Call Home は、さまざまな障害や重要なシステム イベントを検出してユーザに通知する、Cisco デバイスのオペレーティング システムに埋め込まれている製品機能です。Smart Call Home は、基本的な Call Home 機能を強化するための自動化と便利な機能を追加します。Smart Call Home を有効にすると、Call Home のメッセージとアラートは Smart Call Home に送信されます。

Smart Call Home は Cisco の多くのサービス契約に含まれており、次が含まれます。

- 自動化された、24 時間の機器監視、プロアクティブな診断、リアルタイムの電子メール アラート、サービス チケットの通知、および修復の推奨。

- Call Home 診断とインベントリ アラームをキャプチャおよび処理することにより指定された連絡先に送信される、プロアクティブなメッセージング。これらの電子メール メッセージには、自動的に作成された場合に Smart Call Home ポータルと TAC ケースへのリンクが含まれています。
- Cisco Technical Assistance Center（TAC）による優先サポート。Smart Call Home では、アラートが十分に重大な場合、TAC ケースが自動的に生成され、デバッグおよび他の CLI 出力が添付されて、`https` 経由で適切なサポート チームにルーティングされます。
- カスタマイズ可能なステータス レポートおよびパフォーマンス分析。
- 次に対する Web ベースのアクセス 1 箇所における修復のためのすべての Call Home メッセージ、診断、および推奨、TAC ケースのステータス、すべての Call Home デバイスの最新のインベントリおよび構成情報。

HX ストレージ クラスタ、ユーザ、サポートの間で自動的に通信が行われるように設定する方法については、データ収集用の Smart Call Home の設定 （142 ページ）を参照してください。

HX Connect を使用した自動サポートの設定

一般に、Auto Support（ASUP）は HX ストレージ クラスタの作成中に設定されます。設定されなかった場合は、クラスタ作成後に HX Connect ユーザ インターフェイスを使用して有効にすることができます。

ステップ 1 HX Connect にログインします。

ステップ 2 バナーで、**[設定の編集（Edit settings）]**（歯車アイコン）>**[自動サポートの設定（Auto Support Settings）]** をクリックして、次のフィールドに値を入力します。

UI 要素	基本的な情報
[自動サポートの有効化（推奨）（Enable Auto Support (Recommended)）] チェックボックス	以下を有効にすることにより、この HX ストレージ クラスタの Call Home を設定します。 • Cisco TAC への分析用データの配信。 • プロアクティブ サポートの一環としてのサポートからの通知。
[サービス チケット通知の送信先（Send service ticket Notifications to）] フィールド	通知を受信する電子メール アドレスを入力します。
[Terms and Conditions (使用条件)] チェック ボックス	エンドユーザー使用契約。自動サポート機能を使用するには、このチェック ボックスをオンにする必要があります。

UI 要素	基本的な情報
[プロキシ サーバを使用（Use Proxy Server）] チェックボックス	• **Web プロキシ サーバ** URL • **[ポート（Port）]** • **ユーザー名（Username）** • **パスワード**

ステップ 3 [OK] をクリックします。

ステップ 4 バナーで、**[設定の編集（Edit settings）]**（歯車アイコン）>**[通知の設定（Notifications Settings）]** をクリックして、次のフィールドに値を入力します。

UI 要素	基本的な情報
[電子メール通知によるアラームの送信（Send email notifications for alarms）] チェックボックス	オンにした場合は、次のフィールドに値を入力します。 • **メールサーバアドレス** • **送信元アドレス（From Address）**：サポート サービス チケットでHXストレージクラスタを特定するために使われる電子メールアドレスを、自動サポート通知の送信者として入力します。現在、この電子メールアドレスにはサポート情報が送信されません。 • **受信者リスト(カンマ区切り)**

ステップ 5 [OK] をクリックします。

CLI を使用した通知設定の構成

HX ストレージ クラスタからアラーム通知を受信する設定を構成および検証するには、次の手順に従います。

（注） 未認証の SMTP のみが ASUP のサポート対象となります。

ステップ 1 `ssh` を使用して HX ストレージ クラスタ内のストレージ コントローラ VM にログインします。

ステップ 2 SMTP メール サーバを設定し、設定を確認します。

指定された受信者に電子メール通知を送信するために SMTP メール サーバで使用される電子メール アドレスです。

構文：`stcli services smtp set [-h] --smtp SMTPSERVER --fromaddress FROMADDRESS`

例：

```
# stcli services smtp set --smtp mailhost.eng.mycompany.com --fromaddress smtpnotice@mycompany.com

# stcli services smtp show
```

ステップ 3 ASUP 通知を有効にします。

```
# stcli services asup enable
```

ステップ 4 受信者の電子メール アドレスを追加して、設定を確認します。

電子メール通知を受信する一連の電子メールアドレスまたは電子メールエイリアスのリストです。複数の電子メールはスペースで区切ります。

構文：`stcli services asup recipients add --recipients RECIPIENTS`

例：

```
# stcli services asup recipients add --recipients user1@mycompany.com user2@mycompany.com
# stcli services asup show
```

ステップ 5 HX ストレージ クラスタの eth1:0 IP アドレスを所有しているコントローラ VM から、電子メールでテスト ASUP 通知を送信します。

```
# sendasup -t
```

eth1:0 IP アドレスを所有しているノードを判別するには、`ssh` を使用して HX ストレージ クラスタの各ストレージ コントローラ VM にログインし、`ifconfig` コマンドを実行します。他のノードから `sendasup` コマンドを実行しても、出力は何も返されず、受信者はテストを受信しません。

ステップ 6 すべてのストレージ コントローラ VM の IP アドレスから電子メールを送信できるように電子メール サーバを設定します。

データ収集用の Smart Call Home の設定

データ コレクションはデフォルトで有効にされますが、インストール時にオプトアウト（無効化）することができます。クラスタ作成後のデータ コレクションを有効にすることもできます。アップグレード中、Smart Call Home の有効化はレガシー構成によって決まります。たとえば、`stcli services asup show` を有効にすると、アップグレード時に Smart Call Home が有効になります。

HX ストレージ クラスタに関するデータ コレクションは、`https` を介して Cisco TAC に転送されます。インストールされているファイアウォールがある場合、Smart Call Home のプロキシ サーバの構成は、クラスタ作成の後に完了します。

（注） HX クラスタからの発信接続がプロキシ サーバを通過する必要がある展開では、Smart Call Home はプロキシ サーバの使用をサポートしていません。

（注） HyperFlex Data Platform リリース 2.5(1.a) では、Smart Call Home Service Request（SR）の生成でプロキシ サーバは使用されません。

Smart Call Home を使用するには、次のものが必要です。

- 対応する Cisco Unified Computing Support Service 契約または Cisco Unified Computing Mission Critical Support Service 契約と関連付けられた Cisco.com ID。
- 登録されるデバイス用の Cisco Unified Computing Support Service または Cisco Unified Computing Mission Critical Support Service

ステップ 1 HX ストレージ クラスタ内のストレージ コントローラ VM にログインします。

ステップ 2 HX ストレージ クラスタをサポートに登録します。

HX ストレージ クラスタを登録すると、収集されたデータに ID を追加し、Smart Call Home を自動的に有効にします。HX ストレージ クラスタを登録するには、電子メール アドレスを指定する必要があります。登録後、問題が発生して TAC サービス要求が生成されるたびに、このメール アドレスはサポート通知を受け取ります。

構文：

```
stcli services sch set [-h] --email EMAILADDRESS
```

例：

```
# stcli services sch set --email name@company.com
```

ステップ 3 HX ストレージ クラスタからサポートへのデータ フローが機能していることを確認します。

データ フローが機能していれば、問題が発生した場合にサポートがそれをトラブルシューティングするうえで役立つ関連情報が確実に得られます。

（注） TAC に連絡して接続を確認してください。

```
# asupcli [--all] ping
```

`--all` オプションは、HX クラスタ内のすべてのノード上でコマンドを実行します。

ステップ 4 （省略可能）ポート 443 を介した Smart Call Home のアクセスを有効にするためにプロキシ サーバを設定します。

クラスタの作成後、HX ストレージ クラスタがファイアウォールの背後にある場合は、Smart Call Home プロキシ サーバを構成する必要があります。サポートは、`url: https://diag.hyperflex.io:443` エンドポイントでデータを収集します。

1. 既存の登録メールとプロキシ設定をすべてクリアします。

   ```
   # stcli services sch clear
   ```

2. プロキシと登録メールを設定します。

   構文：

stcli services sch set [-h] --email EMAILADDRESS [--proxy-url PROXYURL] [--proxy-port PROXYPORT] [--proxy-user PROXYUSER] [--portal-url PORTALURL] [--enable-proxy ENABLEPROXY]

構文の説明

Option	必須またはオプション	説明
--email EMAILADDRESS	必須。	シスコ サポートから電子メールを受信するユーザのために、電子メールアドレスを追加します。配信リストまたはエイリアスを使用することをお勧めします。
--enable-proxy ENABLEPROXY	オプション。	プロキシの使用を明示的に有効または無効にします。
--portal-url PORTALURL	オプション。	代替の Smart Call Home ポータル URL を指定します（該当する場合）。
--proxy-url PROXYURL	オプション。	HTTP または HTTPS プロキシの URL を指定します（該当する場合）。
--proxy-port PROXYPORT	オプション。	HTTP または HTTPS プロキシの ポート を指定します（該当する場合）。
--proxy-user PROXYUSER	オプション。	HTTP または HTTPSプロキシの URL を指定します（該当する場合）。 HTTP または HTTPS プロキシのパスワードを指定します（メッセージが表示される場合）。

例：

```
# stcli services sch set
  --email name@company.com
  --proxy-url www.company.com
  --proxy-port 443
  --proxy-user admin
  --proxy-password adminpassword
```

3. プロキシ サーバが動作していること、および HX ストレージ クラスタからサポート ロケーションにデータが流れることを確認するために ping を送信します。

（注） TAC に連絡して接続を確認してください。

```
# asupcli [--all] ping
```

`--all` オプションは、HX クラスタ内のすべてのノード上でコマンドを実行します。

ステップ 5 Smart Call Home が有効になっていることを確認します。

Smart Call Home 構成が設定されると、自動的に有効になります。

```
# stcli services sch show
```

ステップ 6 自動サポート（ASUP）通知を有効にします。

一般に、Auto Support（ASUP）は HX ストレージ クラスタの作成中に設定されます。設定されなかった場合、HX Connect または CLI を使用してクラスタ作成後の設定を有効にすることができます。

Smart Call Home が無効になっている場合は、手動で有効にします。

```
# stcli services sch enable
```

自己署名の証明書を CA 署名の証明書で置き換える

（注） リリース 5.0(1x) 以前の場合、次の証明書置換スクリプトを実行するには、コントローラ VM へのルート レベルのアクセスが必要です。TAC に連絡して、証明書置換プロセスを完了してください。リリース 5.0(2a) 以降では、**diag** ユーザー シェルにアクセスして CAPTCHA テストを完了する必要があります。プロセスの説明については、『Cisco HyperFlex Data Platform 管理ガイド、リリース 5.0』の 「Diag ユーザーの概要」 を参照してください。

CA 証明書のインポートは、シェルスクリプトによって自動化されています。任意の CVM、できれば CIP ノードから CSR（証明書署名要求）を生成します。各 CVM は同じ証明書でインストールする必要があるため、クラスタに必要な CSR は 1 つだけです。CSR を生成するときに、管理 CIP に割り当てられたホスト名をサブジェクトの識別名の共通名として入力する必要があります。

次に例を示します。

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:HyperFlex
Common Name (e.g. server FQDN or YOUR name) []:<hostname-cluster-management-IP>
Email Address []:support@cisco.com
```

CA 証明書を取得した後で、自動スクリプトを使用して証明書をインポートします。スクリプトは、その CVM の証明書のみを更新します。

（注） クラスタ拡張の場合は、証明書をインポートするために、同じ証明書とキーファイルを使用して、拡張されたノード CVM でスクリプトを再度実行する必要があります。

diag シェルにアクセスしたら、次の手順を実行します。

ステップ 1 CVM でのスクリプトの場所は、/usr/share/springpath/storfs-misc/hx-scripts/ です。

```
diag/usr/share/springpath/storfs-misc/hx-scripts/certificate_import_input.certificate_import_input.sh

    run stcli cluster reregister
```

ステップ 2 コントローラ VM（CIP を指す）で、このコマンドを実行して CSR 要求を生成します。

```
openssl req -nodes -newkey rsa:2048 -keyout /etc/ssl/private/<Host Name of the CVM>.key -out
/etc/ssl/certs/<Host Name of the CVM>.csr
   cat /etc/ssl/certs/<host name mapped to the management CIP>.csr - Copy the request to any notepad.

    Send the request to CA to generate the certificate
```

ステップ 3 CA（.crt ファイル）から証明書を受信したら、証明書とキーを各 CVM にコピーします。

ステップ 4 各CVMで、./certificate_import_input.sh スクリプトを使用して証明書をインポートします。

```
root@SpringpathControllerVUFSTDS58L:/usr/share/springpath/storfs-misc/hx-scripts#
./certificate_import_input.sh
```

ステップ 5 キーのパスとして、/etc/ssl/private/<CVM のホスト名>.key を入力します。

ステップ 6 <CA へのパス.crt ファイル> という証明書形式で証明書のパスを入力します。

（注） すべての入力を入力した後、インポート プロセスが完了するまでにいくらか時間がかかります。

ステップ 7 CIP をポイントしている CVM から **stcli reregister** コマンドを実行して、クラスタを vCenter に再登録します。証明書をインポートしたら、クラスタを再登録する必要があります。

レプリケーション ペアリング

レプリケーション クラスタ ペアの作成は、VM をレプリケーション用にセットアップするための前提条件です。レプリケーション ペアを作成する前に、レプリケーション ネットワークと少なくとも 1 つのデータストアを設定する必要があります。

クラスタ 2 とクラスタ 1 をペアリングすることによって、レプリケーション用に明示的に設定されたクラスタ 1 上のすべての VM はクラスタ 2 にレプリケートでき、レプリケーション用に明示的に設定されたクラスタ 2 上のすべての VM はクラスタ 1 にレプリケートできることを指定しています。

クラスタ 1 のデータストア A とクラスタ 2 のデータストア B をペアリングすることによって、レプリケーション用に明示的に設定されたクラスタ 1 上のすべての VM では、データストア A にファイルがある場合、それらのファイルはクラスタ 2 のデータストア B にレプリケートされることを指定しています。同様に、レプリケーション対象として明示的に設定されたクラスタ 2 上のすべての VM では、データストア B にファイルがある場合、それらのファイルがクラスタ 1 のデータストア A にレプリケートされます。

ペアリングは厳密に 1 対 1 で行われます。クラスタは、他のクラスタのうち 1 つとだけペアリング可能です。ペアリングされるクラスタ上のデータストアは、もう一方のクラスタ上の 1 つのデータストアとだけペアリングできます。

レプリケーション ペアの作成、編集、および削除の詳細な手順については、『Cisco HyperFlex Systems Administration Guide』を参照してください。

プライベート VLAN の追加

プライベート VLAN について

プライベート VLAN では VLAN のレイヤ 2 ブロードキャスト ドメインがサブドメインに分割されるので、スイッチで相互にポートを分離できます。サブドメインは、1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN で構成されます。プライベート VLAN ドメインには、プライマリ VLAN が 1 つのみ含まれています。プライベート VLAN ドメインの各ポートは、プライマリ VLAN のメンバーで、プライマリ VLAN は、プライベート VLAN ドメイン全体です。

プライベート VLAN ポートの概要

表 *4 :* プライベート *VLAN* ポートのタイプ

VLAN ポート	説明
Promiscuous Primary VLAN	プライマリ VLAN に属しています。無差別ポートに関連付けられているセカンダリ VLAN に属しているインターフェイス、およびプライマリ VLAN に関連付けられているインターフェイスのすべてと通信できます。それらのインターフェイスには、コミュニティ ポートと独立ホスト ポートも含まれます。セカンダリ VLAN からのすべてのパケットは、この VLAN を経由します。
独立したセカンダリ VLAN	度クリスしたセカンダリ VLAN に属するホスト ポートです。このポートは同じプライベート VLAN ドメイン内のその他のポートから完全に分離されていますが、関連付けられている無差別ポートとは通信できます。
コミュニティ セカンダリ VLAN	コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよびアソシエートされている無差別ポートと通信します。

HX の導入に従い、VM ネットワークはデフォルトで通常の VLAN を使用します。VM ネットワークにプライベート VLAN を使用する場合は、次のセクションを参照してください。

- 既存の VM を使用しない VM ネットワーク上でのプライベート VLAN の設定 （148 ページ）。

• 既存の VM を使用した VM ネットワーク上でのプライベート VLAN の設定 （148 ページ）.

既存の VM を使用しない VM ネットワーク上でのプライベート VLAN の設定

ステップ 1 Cisco UCS Managerでプライベート VLAN を設定するには、『 Cisco UCS Manager Network Management Guide』を参照してください。

ステップ 2 上流に位置するスイッチでプライベート VLAN を設定するには、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

ステップ 3 ESX ホストでプライベート VLAN を設定するには、ESX ホスト上でのプライベート VLAN の設定 （148 ページ）を参照してください。

ESX ホスト上でのプライベート VLAN の設定

ESX ホストでプライベート VLAN を設定するには、次の手順を実行します。

ステップ 1 VMware vSphere クライアントから vSphere 標準スイッチ上の VMNIC を削除します。

ステップ 2 前の手順で削除した VMNIC を使用して新しい vSphere 分散型スイッチを作成します。

ステップ 3 無差別（プロミスキャス）、独立、およびコミュニティ VLAN を作成します。

既存の VM を使用した VM ネットワーク上でのプライベート VLAN の設定

ステップ 1 Cisco UCS Managerでプライベート VLAN を設定するには、『 Cisco UCS Manager Network Management Guide』を参照してください。

ステップ 2 上流に位置するスイッチでプライベート VLAN を設定するには、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

ステップ 3 ESX ホストでプライベート VLAN を設定するには、を参照してください。 ESX ホスト上でのプライベート VLAN の設定 （148 ページ）

ステップ 4 vSphere 標準スイッチから、新しく作成された vSphere 分散型スイッチに VM を移行します。

a) vCenter 仮想マシンを右クリックして、[Migrate Virtual Machine Networking] をクリックします。

b) ドロップダウン リストから、[送信元ネットワーク（source network）] および [送信先ネットワーク（destination network）] を選択します。

c) [次へ（Next）] をクリックします。

d) 移行する [仮想マシン（Virtual Machines）] を選択します。

e) [Finish] をクリックします。

ステップ 5 VM 上のネットワーク アダプタのネットワーク接続をプライベート VLAN に変更します。

a) vCenter 仮想マシンを右クリックして、[設定の編集（Edit Settings）] をクリックします。
b) [ハードウェア（Hardware）] タブから、変更するネットワーク アダプタを選択します。
c) [ネットワーク ラベル（Network Label）] ドロップダウン リストから、使用する [ネットワーク接続（Network Connection）] を選択します。
d) [OK] をクリックします。

VSphere 標準スイッチ上での VMNIC の削除

ステップ 1 VMware vSphere クライアントにログオンします。
ステップ 2 [ホーム（Home）] > [ホストとクラスタ（Hosts and Clusters）] を選択します。
ステップ 3 削除する VMNIC がある ESX ホストを選択します。
ステップ 4 [設定（Configuration）] タブを開きます。
ステップ 5 [Networking] をクリックします。
ステップ 6 VMNIC を削除する**スイッチ**を選択します。
ステップ 7 [Manage the physical adapters connected to the selected switch] ボタンをクリックします。
ステップ 8 削除する **vminc** を選択し、[削除（Remove）] をクリックします。
ステップ 9 [はい（Yes）] をクリックして、選択内容を確認します。
ステップ 10 [閉じる（Close）] をクリックします。

vSphere 分散型スイッチの作成

ステップ 1 VMware vSphere クライアントにログオンします。
ステップ 2 [Home] > [Networking] を選択します。
ステップ 3 クラスタを右クリックして、[Distributed Switch] > [New Distributed Switch] を選択します。
ステップ 4 [Name and Location] ダイアログボックスに、分散スイッチの名前を入力します。
ステップ 5 [Select Version] ダイアログボックスで、バージョンと構成の要件に対応する分散スイッチ バージョンを選択します。
ステップ 6 [Next] をクリックします。
ステップ 7 [Edit Settings] ダイアログボックスで、次のように指定します。

- [Number of uplink ports]
- [Network I/O Control] を**有効化**します。
- [Create a default port group] をオンにします。

• [Port Group Name] ボックスに、デフォルト ポート グループの**名前**を入力します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Ready to Complete] ダイアログボックスで、設定した内容を確認します。

ステップ 10 **[終了]** をクリックします。

vSphere 分散型スイッチ上でのプライベート VLAN の作成

ステップ 1 VMware vSphere クライアントから、[インベントリ（Inventory）]>[ネットワーキング（Networking）] を選択します。

ステップ 2 dvSwitch を右クリックします。

ステップ 3 [Edit Settings] をクリックします。

ステップ 4 [プライベート VLAN（Private VLAN）] タブを選択します。

ステップ 5 [プライマリ プライベート VLAN ID（Primary private VLAN ID）] タブで、**プライベート VLAN ID** を入力します。

ステップ 6 [セカンダリ プライベート VLAN ID（Secondary private VLAN ID）] タブで、**プライベート VLAN ID** を入力します。

ステップ 7 [タイプ（Type）] ドロップダウン リストから、VLAN のタイプを選択します。有効な値は次のとおりです。

- **隔離**
- **コミュニティ**
- **無差別**(デフォルト)

ステップ 8 [OK] をクリックします。

分散型ポート グループ内のプライベート VLAN の設定

始める前に

vSphere 分散スイッチでプライベート VLAN を作成します。

ステップ 1 [dvSwitch] の下の [dvPortGroup] を右クリックして、[設定の編集（Edit Settings）] をクリックします。

ステップ 2 [ポリシー（Policies）] > [VLAN] をクリックします。

ステップ 3 [VLAN タイプ（VLAN type）] ドロップダウン リストから [プライベート VLAN（Private VLAN）] を選択します。

ステップ 4 [プライベート VLAN エントリ（Private VLAN Entry）] ドロップダウン リストから、プライベート VLAN のタイプを選択します。次のいずれかを指定できます。

- 隔離
- コミュニティ

（注） コミュニティ プライベート VLAN が推奨されています。

混合モード ポートはサポートされていません。

ステップ 5 [OK] をクリックします。

分散型仮想スイッチと Cisco Nexus 1000v

分散型スイッチを導入する際の検討事項

（注）

- 分散型仮想スイッチ（DVS）または Cisco Nexus 1000v（NK1v）の使用はオプションであり、必須の手順ではありません。
- VMotion ネットワークの DVS は、環境に vSphere の Enterprise Plus ライセンスが設定されている場合にのみ使用できます。
- 特定の時点で 2 つのスイッチのどちらかだけを使用できます。
- Hyperflex と Nexus 1000v の間で Quality of Service（QoS）ポリシーが競合する可能性があります。HyperFlex ポリシーに従って N1Kv の QoS クラスが設定されていることを確認する必要があります。『Network and Storage Management Guide』の「*Creating a QoS Policy*」を参照してください。
- N1Kv スイッチを導入する場合は、HyperFlex ホスト間のトラフィックが安定した状態で FI 上をローカルに流れるように、説明に従って設定を適用します。正確に設定しない場合、ほとんどのトラフィックがアップストリーム スイッチを通過して遅延が発生する可能性があります。このシナリオを回避するには、ストレージコントローラ、管理ネットワーク、および vMotion ポート グループがアクティブ/スタンバイで設定され、フェールオーバーが有効になっていることを確認してください。

1. UCS Manager を使用して、[ネットワーク制御ポリシー（Network Control Policies）] の [リンク ステータス（link status）] を設定します。詳細については、『Cisco UCS Manager GUI Configuration Guide』の「Configuring Network Control Policy」のセクションを参照してください。
2. vCenter で vSwitch プロパティを設定します。

   a. [ネットワーク障害検出（Network Failure Detection）] を [リンク ステータスのみ（Link Status only）] に設定します。

   b. [フェールバック（Failback）] を [はい（Yes）] に設定します。詳細については、『Cisco UCS Manager VM-FEX for VMware Configuration guide』の「Configuring the VM-FEX for VMware」のセクションを参照してください。

分散型スイッチにより、各ノードで同じ設定が確実に使用されます。こうしてトラフィックに優先順位を付けることができ、アクティブな vMotion トラフィックがないときに、使用可能な帯域幅を他のネットワーク ストリームで活用できるようになります。

HyperFlex（HX）Data Platform では、非 HyperFlex 依存ネットワークに分散型仮想スイッチ（DVS）ネットワークを使用できます。

このような非 HX 依存ネットワークには以下のものが含まれます。

- VMware vMotion ネットワーク
- VMware アプリケーション ネットワーク

HX Data Platform には、次のネットワークが標準的な vSwitch を使用するという依存関係があります。

- vswitch-hx-inband-mgmt：ストレージ コントローラ管理ネットワーク
- vswitch-hx-inband-mgm：管理ネットワーク
- vswitch-hx-storage-data：ストレージ ハイパーバイザ データ ネットワーク
- vswitch-hx-storage-data：ストレージ コントローラ データ ネットワーク

HX Data Platform のインストール時に、すべてのネットワークで標準 vSwitch ネットワークが設定されます。ストレージクラスタを設定した後、非HX依存ネットワークをDVSネットワークに移行することができます。次に例を示します。

- vswitch-hx-vm-network：VM ネットワーク
- vmotion：vmotion pg

vMotion ネットワークを分散型仮想スイッチに移行する方法の詳細については、『Network and Storage Management Guide』の「*Migrating vMotion Networks to Distributed Virtual Switches (DVS) or Cisco Nexus 1000v (N1Kv)*」を参照してください。

HX Data Platform 上での vCenter のホスト

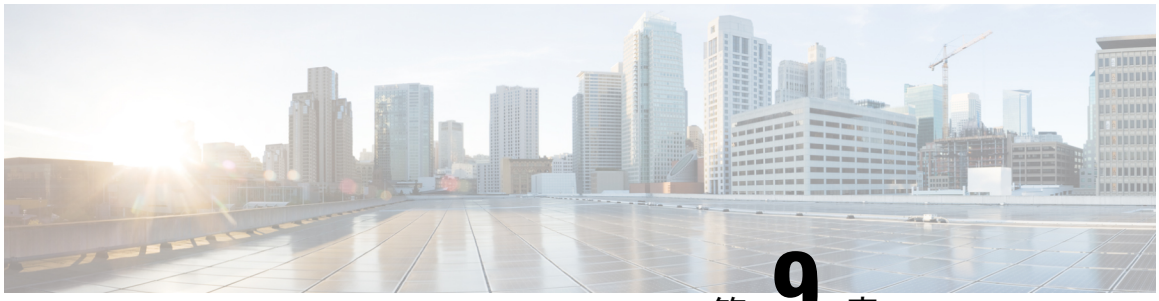
HyperFlex クラスタ上で vCenter の展開をサポートする場合、いくつかの制約があります。詳細については、『How to Deploy vCenter on the HX Data Platform』テクニカル ノートを参照してください。

AMD GPU の展開

AMD FirePro S7150 シリーズ GPU は HX240c M5/M6 ノードでサポートされます。これらのグラフィック アクセラレータでは、非常に安全な高いパフォーマンス、そしてコスト効率の良い VDI 展開を有効にします。HyperFlex に AMD GPU を展開するには、次の手順に従います。

ステップ	アクション	手順の説明
1	サーバに接続されているサービス プロファイルの BIOS ポリシーを変更します。	サポートされるすべてのGPUに関する要件：メモリマップド I/O 4 GB 以上
2	サーバにGPUカードをインストールします。	GPU カードのインストール
3	サーバの電源をオンにして、GPUがサーバの Cisco UCS Manager インベントリに表示されることを確認します。	—

ステップ	アクション	手順の説明
4	AMD GPU カードの vSphere インストール バンドル（VIB）をインストールして、再起動します。	Cisco ソフトウェア ダウンロードから、VMware ESXi 上の AMD 用の C シリーズ スタンドアロンファームウェア/ソフトウェア バージョンバンドル 3.1(3) の最新ドライバ ISO を含むインベントリ リストをダウンロードします。
5	VM 設定を使用してクラスタ上で Win10 VM を作成します。	対象の仮想マシンの指定
6	各 ESXi ホストで、`MxGPU.sh` スクリプトを実行して GPU を設定し、GPU から仮想機能を作成します。	MxGPU セットアップ スクリプトの使用
7	前のステップで作成した仮想機能（VF）を Win10 Vm に割り当てます。	—



第 9 章

複数の HX クラスタの設定

複数のクラスタの設定

複数の HyperFlex クラスタを同じ UCS ドメイン (ファブリック インターコネクトのペア) の下に共存させることができます。次のガイドラインに従い、ドメインに接続されているすべての機器に対して、スムーズに運用できるようにする必要があります。

（注） 2 つの異なる HX リリースの HX クラスタを同じ UCSM ドメインで使用する構成は、必要なサーバー ファームウェア バンドルが UCSM インフラストラクチャ リリースでサポートされている限りサポートされます。HXDP リリースは、リリース ノートごとに UCSM サーバー ファームウェア バンドルにマッピングされます。UCSM インフラストラクチャのリリースには依存しません。

推奨事項

- 標準 HXDP ライセンスを使用する場合、コンピューティング専用ノードの数は、コンバージド ノードの数以下にする必要があります。エンタープライズ HXDP ライセンスでは、コンバージド ノードに対して、最大 2:1 比のコンピューティングを使用できます。
- 新しい HyperFlex クラスタを作成するには、第 2 章に示されている要件をすべて満たしていることを確認してください。また、第 4 章に示されているプロセスに従ってください。
- HX クラスタのすべてのノードは、同じポリシーとサービス プロファイルを参照する必要があります。

（注） HyperFlex サービス プロファイル テンプレートの編集は推奨されません。

- 各 HX クラスタの一意の名前を割り当てます。

- 各 HX クラスタは、インストールの一部として固有のサブ組織に作成されます。この階層は、固有のポリシーがクラスタごとに作成されるようにするため、変更しないでください。
- 各クラスタは、固有のストレージ データ VLAN を使用して、すべてのストレージ トラフィックを分離しておく必要があります。複数のクラスタにわたってこの VLAN を再利用することは推奨されません。
- Cisco では、ストレッチ クラスタを含む、ファブリック インターコネクトに接続されたクラスタごとに固有のストレージ データ VLAN が必要です。このようなデプロイメントでのストレージ データへの共有 VLAN の使用は、クラスターの停止につながる可能性があるため、サポートされていません。

  他のデプロイメント タイプでは、すべてのストレージ トラフィックを分離しておくために、クラスタごとに一意のストレージデータ VLAN を使用することを強くお勧めします。複数のクラスタに同じストレージデータ VLAN を使用している場合は、適切なネットワーク分離を確認してください。適切なネットワーク分離なしで複数のクラスターで同じストレージ データ VLAN を使用することはサポートされていません。
- VLAN (管理およびゲスト トラフィック VLAN など) を再利用する場合は、UCSM にすでに存在していても、VLAN ごとに新しい固有の VLAN 名を作成します。これにより、そのドメイン内の他のクラスタやサーバが中断されることはなくなります。
- 互換性のある Cisco UCS Manager と Cisco HyperFlex リリースを選択していることを確認します。

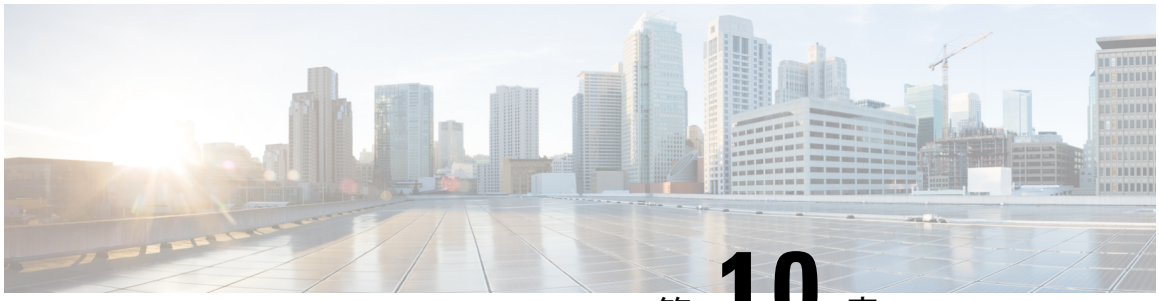
  最新の互換性マトリックスについては、『Release Notes for Cisco HX Data Platform』のソフトウェア バージョンの表を参照してください。
- 同じ Cisco HX データ プラットフォーム インストーラを使用して別の vCenter に 2 番目のクラスタを設定する前に、ブラウザのキャッシュをクリアしてください。これにより、古いクラスタの IP アドレスがキャッシュされ展開が失敗するなどの問題が回避されます。

（注） トラフィックに応じて、さらにアップリンク ポートを追加する必要がある場合があります。

（注） ファブリック インターコネクトの同じペアに接続されている複数のクラスタ間で、同じ VLAN を使用することができます (管理、vMotion、VM ゲスト VLAN など)。これは、IP が重複しない限り可能です。ただし、ストレージ トラフィックが安全に分離されるように、クラスタごとに HX ストレージ VLAN を異なる状態に保つことを推奨します。ベスト プラクティスに対してストレージ VLAN を再利用する場合は、IP の重複を避けるために細心の注意をしてください。重複 IP があると、別のクラスタの既存のストレージ トラフィックが中断される可能性があります。

ステップ 1 HX Data Platform インストーラにログインします。

ステップ 2 標準クラスタの [Create Cluster] ワークフローに従って、追加のクラスタを作成します。詳細については、Cisco HyperFlex Systems の設定 （57 ページ）を参照してください。



第 10 章

Cisco HyperFlex システム クラスタの展開

クラスタ拡張ガイドライン

クラスタを拡張する前に、これらのガイドラインを確認してください。

（注） LAZが設定されている場合（サイズ8以上のクラスタではデフォルトで有効）、拡張を進める前に ロジカル アベイラビリティ ゾーン （182 ページ） を確認してください。

- レプリケーションが設定済みの場合は、アップグレード、拡張、またはクラスタ メンテナンスを実行する前に、レプリケーションを一時停止モードにしてください。アップグレードや拡張、クラスタのメンテナンスが完了した後、レプリケーションを再開します。タスクを実行するローカルクラスタとの間でレプリケーションが設定されているすべてのクラスタで、一時停止と再開を実行します。
- RESTful API を使用してクラスタ拡張を実行する場合は、タスクの実行時間が予想以上に長くなる場合があります。

- ESXi インストールは、M4 コンバージド ノードの SD カードおよび M5 コンバージド ノードの M.2 SATA SSD でサポートされています。コンピューティング専用ノードの場合、ESXi インストールは SD カード、SAN ブート、フロント アクセス対応 SSD/HDD、または M.2 SSD (UCS-MSTOR-M2 コントローラを使用) でサポートされています。コンピューティング専用ノードでは、USB フラッシュへの ESXi のインストールはサポートされていません。

（注） HW RAID M.2（UCS-M2-HWRAID および HX-M2-HWRAID）は、HX Data Platform リリース4.5(1a) 以降でサポートされるブート設定です。

- 検出されたクラスタをクリックして、3.5x またはそれ以前のリリースの標準 ESX クラスタの拡張を続行します。そうしないとエラーになります。
- 拡張ワークフローの中でコントローラ VM の管理ログイン情報のみを使用します。管理以外の他のクレデンシャルを使用すると、拡張に失敗する可能性があります。
- サポートされていないドライブまたはカタログのアップグレードに関するエラーが表示された場合は、互換性カタログ を参照してください。
- HX リリース 4.0(2e) 以降では、Intersight を介して 3 ノードで ESXi ベースの 10/25 GbE HyperFlex Edge クラスタを拡張できます。

  HyperFlex エッジ クラスタの拡張は、Intersight を使用して展開されたクラスタの場合にのみサポートされます。Intersight を使用したエッジ クラスタの拡張は、HyperFlex OVA インストーラを介して展開されたクラスタではサポートされていません。

（注） この機能によるクラスタの拡張は、HyperFlex 2 ノード エッジ クラスタではサポートされていません。Hyperflex リリース 4.0(2e) より前のエッジ クラスタの拡張はサポートされていません。

すべての要件については、Intersight のドキュメントを参照してください：クラスタ拡張要件

ESXi インストール ガイドライン

1. コンピューティング ノードのブート ポリシーを変更します。

   M5 サーバの HyperFlex ストレッチ クラスタ コンピューティング専用ノードのテンプレートおよびブート ポリシーを変更するには:

   1. テンプレートの複製
   2. コンピューティング M5 ノードにフラッシュ カードがない場合、ローカル ブート ポリシーから Flex flash のチェックを外します。

3. 適切な WWPN で SAN ブートをブート順序に追加します。

2. DPI 拡張ワークフローを開始します。
3. プロンプトされる場合、ISO イメージを使用して ESXi をインストールします。
4. DPI 拡張ワークフローに戻り、ESXi インストール ワークフローを完了します。

（注） Hypervisor 設定が失敗し、SOL ロギングの障害メッセージが表示される場合、ルートおよびデフォルト パスワードを使用して SSH で インストーラ CLI にアクセスし、ESXi ハイパーバイザを設定します。そして、高度なインストーラを実行し、**[HX Storage Software (HX ストレージ ソフトウェア)]** および **[Expand Cluster (クラスタの拡張)]** チェック ボックスをチェックして、ESXi インストール プロセスを続行します。

M4/M5 クラスタを拡張する場合の前提条件

M4/M5 クラスタ内でクラスタ拡張を開始する前に、次のタスクを実行する必要があります。

- **Hypercheck ヘルス チェック ユーティリティ**: アップグレードする前に、Hypercheck クラスタでこの予防的ヘルス チェック ユーティリティを実行することを推奨します。これらのチェックにより、注意が必要なエリアがすぐに見やすくなり、シームレスなアップグレード エクスペリエンスを保証します。Hypercheck のインストールと実行方法の完全な手順の詳細については、『Hyperflex 健全性および事前アップグレード チェック ツール』を参照してください。
- HX クラスタと UCS Manager を、展開に適した推奨リリースにアップグレードします。詳細については、Cisco HyperFlex 推奨ソフトウェア リリースおよび要件ガイドを参照してください。
- 拡張ワークフローを実行するには、一致するリリース HX データ プラットフォーム インストーラ（クラスタと同じリリース）をダウンロードして展開します。
- M4 サーバ：既存の M4 サーバファームウェアを 3.2(1) 以降のファームウェアにアップグレードします。
- vCenter を 6.5 以降にアップグレードします。vCenter 6.5 がないと、Broadwell EVC モードを有効にできません。vCenterのアップグレードのみが必要です。ESXiについては、VMware ソフトウェア相互運用性マトリクスに従って古いバージョンのままにすることができます。EVCモードをオフにしたまま先に進むことはできず、将来的に運用上の問題が生じる可能性があります。

混合クラスタ展開のガイドライン - Cisco HX リリース 4.5(x)

- Hypercheck ヘルス チェック ユーティリティ: アップグレードする前に、Hypercheck クラスタでこの予防的ヘルス チェック ユーティリティを実行することを推奨します。これらのチェックにより、注意が必要なエリアがすぐに見やすくなり、シームレスな**アップグレード** エクスペリエンスを保証します。Hypercheck のインストールと実行方法の完全な手順の詳細については、『HyperFlex 健全性および事前アップグレード チェック ツール』を参照してください。
- M5 コンバージド ノードを使用して既存の M4 クラスタを拡張する操作はサポートされます。
- M4 コンバージド ノードを使用して既存の M5 クラスタを拡張する操作はサポートされません。
- M4 または M5 コンバージド ノードを使用して既存の M4/M5 混在クラスタを拡張する操作はサポートされます。
- サポートされているコンピューティング専用ノードを追加することは、HX Data Platform 2.6 またはそれ以降のインストーラを使用した M4、M5、混合 M4/M5 クラスタすべてで許可されています。組み合わせの例を以下に示しますが、他にもさまざまな組み合わせが可能です。

```
Example combinations:
Expand mixed M4/M5 cluster with compute-only B200, C220, C240 M4/M5
Expand M4 cluster with compute-only B200 M5, C220 M5, C240M5
```

- 混在クラスタを作成する場合は、拡張ワークフローのみがサポートされます。混在 M4/M5 サーバを使用した初期クラスタの作成はサポートされません。
- すべての M5 サーバが、既存の M4 サーバのフォーム ファクタ（220/240）、タイプ（ハイブリッド/AF）、セキュリティ機能（非 SED のみ）、およびディスク設定（数量、容量、非 SED）と一致する必要があります。ドライブの互換性の詳細については、『Cisco HyperFlex Drive Compatibility』ドキュメントを参照してください。
  - HX220-M4 と組み合わせるとき、HX220-M5 は最大 6 の容量ディスク（2 ディスク スロットは空のまま）を使用します。
- HX Edge、SED、LFF、Hyper-v、およびストレッチ クラスタは、混合 M4/M5 クラスタをサポートしていません。

混在クラスタ拡張中の手順

- 検証手順では、拡張が開始される前に EVC チェックが実行されます。表示される指示に従い、既存のクラスタの EVC モードをこの時点で手動で有効にしてください。

注意 警告が出されたときに EVC を有効にしない場合、後の時点で、ストレージクラスタおよび関連するすべての VM を完全にシャットダウンする必要が生じます。この警告をスキップしないでください。

- vCenter で EVC モード設定を実行した後、検証をやり直してください。
- クラスタ拡張で 2 回目の検証が行われ、拡張が続行されます。

コンバージド（HX220c/HX240c）ノードを追加するための前提条件

コンバージド ノードは、クラスタ作成後に HyperFlex クラスタに追加可能です。コンバージド ノード上のストレージは、自動的にクラスタのストレージ容量に追加されます。

既存のストレージ クラスタへのコンバージド ノードの追加を開始する前に、次の前提条件が満たされていることを確認します。

- ストレージ クラスタの状態が正常であることを確認します。
- 新しいノードが、「**インストールの前提条件**」に記載されたシステム要件（ネットワーク要件とディスク要件を含む）を満たしていることを確認します。
- 新しいノードがストレージクラスタ内の他のノードと同じ設定を使用していることを確認します。これには、VLAN ID とスイッチ タイプ（vSwitch かどうか）、外部スイッチ VLAN タギング（EST）を使用した VLAN タギング、仮想スイッチ タギング（VST）を使用した VLAN タギング、または仮想分散型スイッチが含まれます。

（注） ストレージクラスタが容量不足の状態にある場合は、新しいノードを追加すると、システムが自動的にストレージクラスタを再調整します。これは、24 時間ごとに実施される再調整とは別の追加的な動作です。

- 追加するノードが、同じモデル（HX220 または HX240）タイプ（ハイブリッドまたはオールフラッシュ）および同じディスク設定（SED または SED 以外）になっていることを確認します。加えて、容量ディスクの数が既存のクラスタ ノードの数と一致することを確認します。
- HyperFlex クラスタですでに使用されているものとは異なる CPU ファミリを持つノードを追加するには、EVC を有効にします。詳細については、『*Cisco HyperFlex Systems* インストール ガイド（*VMware ESXi* 向け）』の「混在 *CPU* を伴うクラスタの設定」の項を参照してください。

- ノードのソフトウェア リリースが、 Cisco HX Data Platform バージョン、ESXi バージョン、vCenter バージョンと一致していることを確認します。ソフトウェア リリースを特定するには、vCenter の [ストレージ クラスタの概要（Storage Cluster Summary）] タブに移動し、最上部のセクションで [HX Data Platform のリリース（HX Data Platform release）] を確認します。必要に応じてアップグレードします。

（注） クラスタをアップグする場合は、クラスタで実行されているHXDPの現在のリリースに一致する新しいインストーラ VM をダウンロードしてインストールする必要があります。

- 新しいノードで少なくとも 1 つの有効な DNS と NTP サーバが設定されていることを確認します。
- SSO または自動サポートを使用する場合は、ノードが SSO サービスと SMTP サービス用に設定されていることを確認します。
- HX Data Platform インストーラおよび既存のクラスタ管理 IP アドレス間で ping するために ICMP が許可されていること。

コンバージド ノードの準備

コンバージド ノードを既存のストレージ クラスタのハードウェアとネットワークに接続します。

既存のクラスタにコンバージド ノードを追加する

（注） RESTful API を使用してクラスタ展開を実行する場合、そのタスクに想定よりも時間がかかることがあります。

ステップ 1 Cisco HX Data Platform インストーラ を起動します。

a) Web ブラウザで、HX データ プラットフォーム インストーラ VM の IP アドレスまたはノード名を入力します。**[承認（Acceot）]** または **[続行（Continue）]** をクリックして SSL 証明書エラーをバイパスします。Cisco HX Data Platform インストーラ のログイン ページが表示されます。ログイン画面の右下隅でHX データ プラットフォーム インストーラ **ビルド ID** を確認します。

b) ログイン ページで、次のクレデンシャルを入力します。

[ユーザ名（Username）]：`root`

[パスワード（Password）]（デフォルト）：`Cisco123`

（注） システムに同梱されているデフォルトのパスワード `Cisco123` は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

c) EULA の内容を読み、**[利用規約に同意します（I accept the terms and conditions）]** チェックボックスをオンにして、**[ログイン（Login）]** をクリックします。

ステップ 2 **[ワークフロー（Workflow）]** ページで **[クラスタ展開（Cluster Expansion）]** を選択します。

ステップ 3 **[クレデンシャル（Credentials）]** ページで、次のフィールドに値を入力します。

クラスタを作成するには、必要な構成データが格納された *JSON* コンフィギュレーション ファイル をインポートできます。JSON ファイルをインポートする場合は、次の 2 つのステップを行います。インポートしない場合は、必須フィールドに手動でデータを入力できます。

（注） 初回インストールの場合は、シスコの担当者に連絡して工場出荷時のプレインストール JSON ファイルを入手してください。

1. **[ファイルの選択（Select a file）]** をクリックし、該当する *JSON* ファイルを選択して構成をロードします。**[構成を使用（Use Configuration）]** を選択します。
2. インポートされた値が Cisco UCS Manager の値と異なる場合には、**[インポートされた値を上書きする（Overwrite Imported Values）]** ダイアログボックスが表示されます。**[検出された値を使用（Use Discovered Values）]** を選択します。

フィールド	説明
UCS Managerクレデンシャル	
UCS Managerのホスト名	UCS Manager の FQDN または IP アドレス たとえば、*10.193.211.120* とします。
ユーザ名	<管理者> ユーザ名
パスワード	<管理者> パスワード。
vCenter クレデンシャル	

フィールド	説明
vCenter Server	vCenter Server の FQDN または IP アドレス たとえば、*10.193.211.120* とします。 （注） • クラスタを動作可能にするには、その前に vCenter Server を準備する必要があります。 • vCenter のアドレスとクレデンシャルには、vCenter に対するルート レベルの管理者権限が必要です。 • ネストされた vCenter を構築する場合、vCenter Server の入力はオプションです。詳細については Nested vCenter TechNote を参照してください。
ユーザ名	<管理者> ユーザ名 たとえば、*administrator@vsphere.local* とします。
[管理パスワード（Admin Password）]	<*root*> パスワード。
ハイパーバイザのクレデンシャル	
管理者ユーザ名	<管理者> ユーザ名。 これはファクトリ ノードの**ルート**です。
[管理パスワード（Admin Password）]	<*root*> パスワード。 デフォルトのパスワードは、ファクトリ ノードの `Cisco123` です。 （注） システムに同梱されているデフォルトのパスワード `Cisco123` は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

ステップ 4 **[続行（Continue）]**をクリックします。**[クラスタ展開の設定（Cluster Expand Configuration）]**ページが表示されます。拡張する *HX* クラスタを選択します。

拡張する HX クラスタが見つからない場合、もしくはクラスタのロードに時間がかかる場合、**[管理 IP アドレス（Management IP Address）]** フィールドにクラスタ管理アドレスの IP を入力します。

ステップ 5 **[サーバの選択（Server Selection）]**ページの **[関連付けなし（Unassociated）]** タブには関連付けられていない HX サーバのリストが表示され、**[関連付け済み（Associated）]** タブには検出されたサーバのリストが表示されます。**[関連付けなし（Unassociated）]** タブで、HyperFlex クラスタに含めるサーバを選択します。

HX サーバがこのリストに表示されていない場合は、Cisco UCS Manager を調べて、HX サーバが検出されていることを確認します。

サーバごとに、**[アクション（Actions）]** ドロップダウン リストのを使用して、以下を設定できます。

- **[KVM コンソールの起動（Launch KVM Console）]**: HX データ プラットフォーム インストーラ から直接 KVM コンソールを起動するには、このオプションを選択します。
- **[サーバの関連付け解除（Disassociate Server）]**: サーバからサービス プロファイルを削除するには、このオプションを選択します。

（注） 関連付けられていないサーバがない場合は、次のエラー メッセージが表示されます。

```
No unassociated servers found. Please login to UCS Manager and ensure server ports are
 enabled.
```

[サーバ ポートの設定（Configure Server Ports）] ボタンを使用すると、新しい HX ノードをすべて検出できます。通常は、構成の開始前から Cisco UCS Manager でサーバ ポートが構成されています。

ステップ 6 **[続行（Continue）]**をクリックします。**[UCSM の設定（UCSM Configuration）]** ページが表示されます。

（注） 最初に JSON ファイルをインポートした場合、既存の HX クラスタから得られた必要な設定データが **[Credentials]** ページに取り込まれているはずです。この情報は、既存のクラスタ構成に一致している必要があります。

ステップ 7 **[続行（Continue）]**をクリックします。**[ハイパーバイザの設定（Hypervisor Configuration）]** ページが表示されます。次のフィールドに入力します。

注目 再インストールの場合や、ESXiネットワーキングがすでに完了している場合は、この手順で説明したフィールドの入力を省略できます。

フィールド	説明
共通ハイパーバイザ設定の構成	
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、*255.255.0.0* とします。
[ゲートウェイ（Gateway）]	ゲートウェイの IP アドレス。 たとえば、*10.193.0.1* とします。
[DNSサーバ（DNS Server(s)）]	DNS サーバの IP アドレス。 DNS サーバを使用しない場合、HX Data Platform インストーラの **[クラスタの設定（Cluster Configuration）]**ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。 （注） 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。

フィールド	説明
ハイパーバイザ設定 **[IP アドレスとホスト名を連続的に入力する（Make IP Addresses and Hostnames Sequential）]** を選択して、IP アドレスが順番に並ぶようにしてください。 （注）　ドラッグ アンド ドロップ操作を使用してサーバの順番を並び替えることができます。	
名前	サーバ名。
シリアル	サーバのシリアル番号。
スタティックIPアドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。
ホスト名	ホスト名フィールドを空のままにしないでください。

ステップ 8　**[続行（Continue）]**をクリックします。**[IP アドレス（IP Addresses）]**ページが表示されます。**[コンピューティング サーバの追加]** または **[コンバージド サーバの追加]** をクリックして、さらにコンピューティングまたはコンバージド サーバを追加できます。

[IP アドレスを連続させる（Make IP Addresses Sequential）] を選択して、IP アドレスを順番に並べるようにしてください。IP アドレスには、ネットワークがデータ ネットワークと管理ネットワークのどちらに属するかを指定します。

各 HX ノードでは、ハイパーバイザ管理 IP アドレスとデータ IP アドレスに関する次のフィールドに値を入力します。

フィールド	説明
管理ハイパーバイザ	ESXi ホストとストレージ コントローラ間のハイパーバイザ管理ネットワーク接続を処理するスタティック IP アドレスを入力します。
管理ストレージコントローラ	ストレージ コントローラ VM とストレージ クラスタの間の HX Data Platform ストレージ コントローラ VM 管理ネットワーク接続を処理する静的 IP アドレスを入力します。
Data Hypervisor	ESXi ホストとストレージ コントローラ間のハイパーバイザ データ ネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージ コントローラ	ストレージ コントローラ VM とストレージ クラスタの間の HX Data Platform ストレージ コントローラ VM データ ネットワーク接続を処理する静的 IP アドレスを入力します。

フィールド	説明
[ハイパーバイザ（管理）（Hypervisor (Management)）]、[ストレージ コントローラ VM（管理）（Storage Controller VM（Management））]、[ハイパーバイザ（データ）（Hypervisor（Data））]、および [ストレージ コントローラ VM（データ）（Storage Controller VM（Data））] 列の最初の行に IP アドレスを入力すると、HX データ プラットフォーム インストーラによって、他のノードのノード情報に増分自動入力が適用されます。ストレージ クラスタ内のノードの最小数は 3 です。それより多くのノードがある場合は、**[追加（Add）]** ボタンを使用して、アドレス情報を指定します。 （注） コンピューティング専用ノードは、ストレージ クラスタを作成してからでないと追加できません。	
コントローラVMパスワード	デフォルトの管理者ユーザー名とパスワードがコントローラ VM に適用されます。VM は、コンバージド ノードとコンピューティング専用ノードのすべてにインストールされます。 **重要** • コントローラ VM またはコントローラ VM のデータストアの名前を変更することはできません。 • すべてのコントローラ VM に同じパスワードを使用します。異なるパスワードの使用はサポートされていません。 • 1 つの大文字、1 つの数字、1 つの特殊文字を含み、合計で少なくとも 10 文字になる複雑なパスワードを指定してください。 • コントローラ VM と、作成される HX クラスタには、ユーザ定義のパスワードを指定できます。パスワードに使用できる文字と形式に関する制限事項については、『*Cisco HX Data Platform Management Guide*』のセクション「Guidelines for HX Data Platform Special Characters」を参照してください。
詳細設定	
ジャンボ フレーム [ジャンボ フレームを有効化（Enable Jumbo Frames）] チェックボックス	ホスト vSwitches と vNIC、および各ストレージ コントローラ VM 上のストレージデータ ネットワークの MTU サイズを設定する場合は、このチェックボックスをオンにします。 デフォルト値は 9000 です。 （注） MTU サイズを 9000 以外の値に設定するには、Cisco TAC にご連絡ください。

フィールド	説明
ディスク パーティション [ディスク パーティションのクリーンアップ（Clean up Disk Partitions）] チェックボックス	ストレージ クラスタに追加されたすべてのノードから既存のデータおよびパーティションをすべて削除するには、オンにします。保持する必要があるデータはすべてバックアップする必要があります。 **重要** 工場で準備されたシステムの場合は、このオプションを選択しないでください。工場で準備されたシステムのディスク パーティションは正しく設定されています。手動で準備されたサーバで、既存のデータとパーティションを削除するにはこのオプションを選択します。

ステップ 9 [スタート（Start）] をクリックします。**[進捗状況（Progress）]** ページに、さまざまな設定タスクの進捗状況が表示されます。

（注） vCenter クラスタで EVC が有効になっている場合、展開プロセスが失敗し、「`The host needs to be manually added to vCenter`」というメッセージが出されます。展開操作を正常に実行するには、次のようにします。

- vSphere クライアント に追加する ESXi ホストにログインします。
- コントローラ VM の電源をオフにします。
- vSphere Web クライアント でホストをvCenterクラスタに追加します。
- HX データ プラットフォーム インストーラ で、[Retry Deploy] をクリックします。

ステップ 10 クラスタ展開が完了したら、**[HyperFlex Connect を起動（Launch HyperFlex Connect）]** をクリックしてストレージ クラスタの管理を開始します。

（注） 既存のストレージ クラスタにノードを追加した場合、スケジュールされた時間に自動再調整が行われるまでの間、クラスタのHA復元力は引き続き元のストレージクラスタと同じです。

再調整は通常、24 時間の期間でスケジュールされ、ノードの障害発生の 2 時間後、またはストレージ クラスタの領域がなくなったときに行われます。

スケジュールされた時間よりも前にストレージクラスタを再調整するために、ストレージクラスタの再調整コマンドを手動で開始するために、次の手順を実行します。

1. ストレージ クラスタ コントローラ VM コマンド ラインから、`# stcli rebalance start --force` コマンドを実行します。
2. リバランスステータスをモニタするには、`stcli rebalance status` コマンドを実行します。

ステップ 11 HyperFlex `hx_post_install` スクリプトを使用して、または手動でクラスタ内の他のノードと一致するように、必要な VM ネットワーク ポート グループと vMotion vmkernel インターフェイスを作成します。

a) HyperFlex クラスタ管理 IT への SSH。
b) admin ユーザとしてログインします。
c) `hx_post_install` コマンドを実行します。

d) vMotion と VM ネットワークの作成から始まる画面上の指示に従います。設定ステップはオプションです。

ステップ 12 新しいノードがストレージ クラスタに追加された後、高可用性（HA）サービスがリセットされ、HA が追加されたノードを認識できるようになります。

a) vCenter にログインします。
b) vSphere Web Client で、**[Home]** > **[vCenter]** > **[Inventory Lists]** > **[Hosts and Clusters]** > **[vCenter]** > **[Server]** > **[Datacenter]** > **[Cluster]** > **[Host]** でホストに移動します。
c) 新規ノードを選択します。
d) 右クリックして [Reconfigure for vSphere HA] を選択します。

コンピューティング専用ノードを追加するための前提条件

クラスタ作成後にコンピューティング専用ノードを HyperFlex クラスタに追加できます。これを追加すると、追加的なコンピューティング リソースが提供されます。Cisco UCS サーバは、クラスタにストレージ容量をもたらさないため、キャッシュ ドライブまたは永久ドライブを装備する必要はありません。

コンピューティング専用ノードを追加する前に、次の前提条件が満たされていることを確認します。

- ストレージ クラスタの状態が正常であることを確認します。
- 新しいノードが、ネットワークやディスクの要件など インストールの前提条件 に記載されているコンピューティング専用システム要件を満たしていることを確認します。
- サービス プロファイルを関連付けた後に、ESXi ハイパーバイザをインストールします。
- 新しいノードがストレージクラスタ内の他のノードと同じ設定を使用していることを確認します。これには、VLAN ID とスイッチタイプ（vSwitch かどうか）、外部スイッチ VLAN タギング（EST）を使用した VLAN タギング、仮想スイッチタギング（VST）を使用した VLAN タギング、または仮想分散型スイッチが含まれます。

（注） ストレージクラスタが容量不足の状態にある場合は、新しいノードを追加すると、システムが自動的にストレージクラスタを再調整します。これは、24 時間ごとに実施される再調整とは別の追加的な動作です。

- 追加する新しいノードに、HX クラスタ内ですでに使用されているものとは異なる CPU ファミリが使用されている場合は、EVC を有効にします。詳細については、『*Cisco*

HyperFlex Systems インストール ガイド（*VMware ESXi* 向け）』の「混在 *CPU* を伴うクラスタの設定」の項を参照してください。

- ノードのソフトウェア リリースが、 Cisco HX Data Platform リリース、ESXi リリース、vCenter リリースと一致していることを確認します。ソフトウェア リリースを特定するには、vCenter の **[ストレージ クラスタの概要（Storage Cluster Summary）]** タブに移動し、最上部のセクションで *[HX Data Platform* バージョン（*HX Data Platform version*）*]* を確認します。必要に応じてアップグレードします。
- 新しいノードで少なくとも 1 つの有効な DNS と NTP サーバが設定されていることを確認します。
- SSO または自動サポートを使用する場合は、ノードが SSO サービスと SMTP サービス用に設定されていることを確認します。
- ESXi インストールは、M4 コンバージド ノードの SD カードおよび M5 コンバージド ノードの M.2 SATA SSD でサポートされています。コンピューティング専用ノードの場合、ESXi インストールは SD カード、SAN ブート、フロント アクセス対応 SSD/HDD、または M.2 SSD (UCS-MSTOR-M2 コントローラを使用) でサポートされています。コンピューティング専用ノードでは、USB フラッシュへの ESXi のインストールはサポートされていません。

（注） HW RAID M.2（UCS-M2-HWRAID および HX-M2-HWRAID）は、HX Data Platform リリース4.5(1a) 以降でサポートされるブート設定です。

- ブート ハードウェアに基づいてディスクおよびブート ポリシーを自動的に検出および設定することで、コンピューティング専用ノードが展開されました。

  HX Data Platform リリース 4.5(1a) 以降、コンピューティング専用ノードは、インベントリされたブート ハードウェアに基づいて、ディスクおよびブート ポリシーの自動検出および設定を使用して展開されます。ユーザーは UCSM ポリシーを直接選択できません。代わりに、ブート デバイスは、サーバで検出された最初の受け入れ可能なブート メディアに基づいて自動的に決定されます。次の表に、 M4/M5 世代サーバーの優先順位を示します。上から下に読むと、インベントリされたハードウェアに基づいて一致する最初のエントリがクラスタ拡張時に自動的に選択されます。たとえば、単一の M.2 ブート SSD を備えた B200 コンピューティング ノードで拡張する場合、次の表の 2 番目のルールは一致し、SPT の関連付けに使用されます。

  リストされていないメカニズム（SAN ブートなど）を使用してサーバが起動された場合、**anyld** の包括的ポリシーが選択され、管理者は必要に応じて UCSM ポリシーとプロファイルを変更してサーバを起動できます。

表 *5 : M6* の優先順位

M6 の優先順位			
優先度	**SPT** 名	ブート デバイス	ディスク数
1	compute-nodes-m6-m2r1	M6 - M.2 - 2 ディスク	2
2	compute-nodes-m6-m2sd	M6 - M.2 - 1 ディスク	1
3	compute-nodes-m6-ldr1	MegaRAID コントローラ	2
4	compute-nodes-m6-anyld	M6：汎用	すべて

表 *6 : M5* の優先順位

M5 の優先順位			
優先度（**Priority**）	**SPT** 名	ブート デバイス	ディスク数
1	compute-nodes-m5-m2r1	M.2 Raid	2
2	compute-nodes-m5-m2pch	PCH/Non-RAID M.2	1
3	compute-nodes-m5-sd	[FlexFlash]	2
4	compute-nodes-m5-ldr1	MegaRAID	2
5	compute-nodes-m5-sd	[FlexFlash]	1
6	compute-nodes-m5-anyld	その他の設定	いずれか（Any）

表 *7 : M4* の優先順位

M4 の優先順位			
優先度（**Priority**）	**SPT** 名	ブート デバイス	ディスク数
1	compute-nodes-sd	[FlexFlash]	1 または 2
2	compute-nodes-anyld	その他の設定	いずれか（Any）

コンピューティング専用ノードの準備

ステップ 1 サポート対象の HX サーバであること、およびサーバの要件を満たしていることを確認します。詳細については、『*Cisco HyperFlex Systems* インストール ガイド（*VMware ESXi* 向け）』の「ホスト要件」の項を参照してください。

ステップ 2 Cisco UCS Manager にログインします。

a) ブラウザを開き、ストレージ クラスタ ネットワークのファブリック インターコネクト用の Cisco UCS Manager アドレスを入力します。

b) **[UCS Manager の起動（Launch UCS Manager）]** ボタンをクリックします。

c) プロンプトが表示された場合は、Java をダウンロードし、インストールして、受け入れます。

d) 管理者クレデンシャルを使用してログインします。

[ユーザ名（Username）]：**admin**

[パスワード（Password）]：**<管理者パスワード>**

ステップ 3 サーバを見つけて、ストレージクラスタと同じFIドメインにサーバが追加済みであること、承認されたコンピューティング専用モデルであることを確認します。互換性のあるコンピューティング専用ノードの詳細なリストについては、最新の『Cisco HX Data Platform のリリース ノート』を確認してください。

HX Data Platform インストーラの確認

ステップ 1 ストレージクラスタに追加されるコンピューティング ノードおよびストレージクラスタ内のすべてのノードと通信できる 1 つのノード上に、HX Data Platform インストーラがインストールされていることを確認します。

ステップ 2 HX Data Platform インストーラがインストールされていない場合は、「HX Data Platform インストーラの展開」を参照してください。

UCS Manager を使用したコンピューティングのみ ノードへの HX プロファイルの適用

Cisco UCS Manager では、ネットワーク ポリシーが HX プロファイルにグループ化されます。HXインストーラは、コンピューティング専用ノードの自動サービスプロファイルアソシエーション（関連付け）を処理します。手動アソシエーションは不要です。

インストールが開始したら、UCS Manager でコンピューティング専用ノードのサービス プロファイル アソシエーションを監視してください。ESXi のインストールに進む前に、サーバが完全に関連付けられるまで待ちます。

コンピューティング ノードへの VMware ESXi のインストール

重要 各コンピューティング専用ノード上に VMware ESXi をインストールします。

サポートされている ESXi のリリース Cisco HX Data Platform をインストールします。サポートされている ESXi バージョンのリストについては、『Cisco HyperFlex Data Platform Release Notes』を参照してください。

コンピューティング専用ノードに ESXi がすでにインストール済みの場合、Cisco HX カスタム イメージで再イメージ化する必要があります。

始める前に

必要なハードウェアとネットワークの設定が満たされていることを確認します。詳細については、『*Cisco HyperFlex Systems* インストール ガイド（*VMware ESXi* 向け）』の「インストールの前提条件」の項を参照してください。前の手順でサービス プロファイルの関連付けが完了していることを確認します。

ステップ 1 *ESXi* の *HX* カスタム イメージを Cisco HyperFlex の Cisco.com ダウンロード サイトからダウンロードします。「ソフトウェアのダウンロード」を参照してください。

Cisco UCS Manager を介してアクセス可能なネットワーク ロケーションを選択します。

ステップ 2 Cisco UCS Manager にログインします。

ステップ 3 Cisco UCS Manager からサーバーの KVM コンソールにログインします。

a) ナビゲーション ウィンドウで、**[サーバー (Servers)]** > **[サービス プロファイル (Service Profiles)]** > **[サブ組織 (Sub-Ogranizations)]** > ***[hx-cluster]*** をクリックします。

b) ***[hx-cluster]*** を右クリックして、**[KVM コンソール（KVM Console）]** を選択します。

ステップ 4 コンピューティング サーバの KVM パスに *HX-Vmware.iso* イメージをコピーします。

例：

HX-Vmware-ESXi-60U3-5050593-Cisco-Custom-6.0.3.1.iso

ステップ 5 KVM コンソール セッションから、**[仮想メディア（Virtual Media）]** > **[マップ CD/DVD（Map CD/DVD）]** を選択し、*ESXi* の *HX* カスタム イメージをマウントします。[マップ CD/DVD（Map CD/DVD）] オプションが表示されない場合は、まず仮想デバイスをアクティブにします。

a) **[仮想メディア（Virtual Media）]** > **[仮想デバイスのアクティブ化（Activate Virtual Devices）]** を選択します。

これはポップアップ ウィンドウで開きます。

b) **[セッションの受け入れ（Accept the session）]** > **[適用（Apply）]** をクリックします。

ステップ 6 **[マップ CD/DVD（Map CD/DVD）]** オプションから、*HX-Vmware.iso* ファイルの場所にマップします。

a) *HX-Vmware.iso* ファイルを選択します。

b) **[マップ デバイス（Map Device）]** を選択します。

プロセスが完了したら、マップされた場所にファイルがあることを示すチェック マークが付きます。マッピングされたファイルのフルネームには ESXi ビルド ID が含まれます。

ステップ 7 コンピューティング サーバをリセットします。

a) KVM コンソールで **[リセット（Reset）]** ボタンをクリックします。**[OK]** をクリックして確定します。

b) **[電源の再投入（Power Cycle）]** を選択します。[OK] をクリックします。

ステップ 8 *HX-Vmware.iso* ファイルを指すようにブート パスを変更します。

a) **F6** キーを押します。

b) **[起動選択の入力（Enter boot selection）]** メニューから、矢印キーを使用して ***Cisco vKVM-Mapped vDVD1.22*** オプションを強調表示します。

c) **Enter** キーを押して選択します。

これにより ESXi インストーラ ブートローダーが起動します。目的のブート タイプに基づいて 3 つのコンピューティング専用ノードオプション（SD カード、ローカルディスク、またはリモートディスク）のいずれかを選択します。**yes**（すべて小文字）を入力して選択を確定します。インストールの残りの部分は自動化されています。ESXi は数回、再起動します。警告が表示されて短い待機期間の後に自動的に消える場合は、正常な動作です。インストールが終了すると ***ESXi DCUI*** が完全に表示されるので、それまで待ちます。

ステップ 9 各 Cisco HyperFlex サーバに対してステップ 3 ～ 8 を繰り返します。

ステップ 10 ESXi が完全にインストールされたら、**[続行（Continue）]** をクリックします。次に **[Hypervisor 設定の再試行（Retry Hypervisor Configuration）]** をクリックして、クラスタ拡張の残りの部分を完了します。

既存のクラスタにコンピューティング専用ノードを追加する

既存の HyperFlex システム クラスタに HyperFlex コンピューティング専用ノードを追加するには、次の手順を実行します。

（注） RESTful API を使用してクラスタ拡張を実行する場合は、タスクの実行時間が予想以上に長くなる場合があります。

（注） 既存のクラスタにコンピューティング専用ノードを追加した後、vmotion の vmk2 インターフェイスを手動で設定する必要があります。

ステップ 1 Cisco HX Data Platform インストーラ を起動します。

a) Web ブラウザで、HX データ プラットフォーム インストーラ VM の IP アドレスまたはノード名を入力します。**[承認（Acceot）]** または **[続行（Continue）]** をクリックして SSL 証明書エラーをバイパスします。Cisco HX Data Platform インストーラ のログイン ページが表示されます。ログイン画面の右下隅でHX データ プラットフォーム インストーラ **ビルド ID** を確認します。

b) ログイン ページで、次のクレデンシャルを入力します。

[ユーザ名（Username）]：`root`

[パスワード（Password）]（デフォルト）：`Cisco123`

（注） システムに同梱されているデフォルトのパスワード `Cisco123` は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

c) EULA の内容を読み、**[利用規約に同意します（I accept the terms and conditions）]** チェックボックスをオンにして、**[ログイン（Login）]** をクリックします。

ステップ 2 **[ワークフロー（Workflow）]** ページで **[クラスタ展開（Cluster Expansion）]** を選択します。

ステップ 3 **[クレデンシャル（Credentials）]** ページで、次のフィールドに値を入力します。

クラスタを作成するには、必要な構成データが格納された *JSON* コンフィギュレーション ファイル をインポートできます。JSON ファイルをインポートする場合は、次の 2 つのステップを行います。インポートしない場合は、必須フィールドに手動でデータを入力できます。

（注） 初回インストールの場合は、シスコの担当者に連絡して工場出荷時のプレインストール JSON ファイルを入手してください。

1. **[ファイルの選択（Select a file）]** をクリックし、該当する *JSON* ファイルを選択して構成をロードします。**[構成を使用（Use Configuration）]** を選択します。
2. インポートされた値が Cisco UCS Manager の値と異なる場合には、**[インポートされた値を上書きする（Overwrite Imported Values）]** ダイアログボックスが表示されます。**[検出された値を使用（Use Discovered Values）]** を選択します。

フィールド	説明
UCS Managerクレデンシャル	
UCS Managerのホスト名	UCS Manager の FQDN または IP アドレス たとえば、*10.193.211.120* とします。
ユーザ名	<管理者> ユーザ名
パスワード	<管理者> パスワード。
vCenter クレデンシャル	
vCenter Server	vCenter Server の FQDN または IP アドレス たとえば、*10.193.211.120* とします。 （注） • クラスタを動作可能にするには、その前に vCenter Server を準備する必要があります。 • vCenter のアドレスとクレデンシャルには、vCenter に対するルート レベルの管理者権限が必要です。 • ネストされた vCenter を構築する場合、vCenter Server の入力はオプションです。詳細については Nested vCenter TechNote を参照してください。
ユーザ名	<管理者> ユーザ名 たとえば、*administrator@vsphere.local* とします。
[管理パスワード（Admin Password）]	<*root*> パスワード。
ハイパーバイザのクレデンシャル	
管理者ユーザ名	<管理者> ユーザ名。 これはファクトリ ノードの**ルート**です。
[管理パスワード（Admin Password）]	<*root*> パスワード。 デフォルトのパスワードは、ファクトリ ノードの `Cisco123` です。 （注） システムに同梱されているデフォルトのパスワード `Cisco123` は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

ステップ 4 **[続行（Continue）]**をクリックします。**[クラスタ展開の設定（Cluster Expand Configuration）]**ページが表示されます。拡張する *HX* クラスタを選択します。

拡張する HX クラスタが見つからない場合、もしくはクラスタのロードに時間がかかる場合、**[管理 IP アドレス（Management IP Address）]** フィールドにクラスタ管理アドレスの IP を入力します。

ステップ 5 **[続行（Continue）]**をクリックします。**[サーバの選択（Server Selection）]**ページが表示されます。**[サーバの選択（Server Selection）]** ページの **[関連付け（Associated）]** タブに、接続済みのすべての HX サーバが一覧表示されます。それらを選択しないでください。**[関連付けなし（Unassociated）]** タブで、クラスタに追加するサーバを選択します。

ステップ 6 **[続行（Continue）]**をクリックします。**[ハイパーバイザの設定（Hypervisor Configuration）]**ページが表示されます。次のフィールドに入力します。

注目 再インストールの場合や、ESXi ネットワーキングがすでに完了している場合は、この手順で説明したフィールドの入力を省略できます。

フィールド	説明
共通ハイパーバイザ設定の構成	
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、*255.255.0.0* とします。
[ゲートウェイ（Gateway）]	ゲートウェイの IP アドレス。 たとえば、*10.193.0.1* とします。
[DNSサーバ（DNS Server(s)）]	DNS サーバの IP アドレス。 DNS サーバを使用しない場合、HX Data Platform インストーラの **[クラスタの設定（Cluster Configuration）]**ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。 （注） 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。
ハイパーバイザ設定 **[IP アドレスとホスト名を連続的に入力する（Make IP Addresses and Hostnames Sequential）]** を選択して、IP アドレスが順番に並ぶようにしてください。 （注） ドラッグ アンド ドロップ操作を使用してサーバの順番を並び替えることができます。	
名前	サーバ名。
シリアル	サーバのシリアル番号。
スタティックIPアドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。

フィールド	説明
ホスト名	ホスト名フィールドを空のままにしないでください。

ステップ 7 **[続行（Continue）]**をクリックします。**[IP アドレス（IP Addresses）]**ページが表示されます。**[コンピューティング専用ノードの追加（Add Compute-only Node）]** をクリックし、新しいノードを追加します。

複数のコンピューティング専用ノードを追加する場合は、**[IP アドレスをシーケンシャルにする（Make IP Addresses Sequential）]** を選択します。

フィールド	情報
管理ハイパーバイザ	ESXi ホストとストレージ コントローラの間のハイパーバイザ管理ネットワーク接続を処理する静的 IP アドレスを入力します。
管理ストレージコントローラ	なし。
Data Hypervisor	ESXi ホストとストレージ コントローラ間のハイパーバイザ データ ネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージ コントローラ	なし。
コントローラ VM	コントローラ VM が既存の HX クラスタにインストールされたときにそれらの VM に適用されたデフォルトの管理者ユーザ名とパスワードを入力します。 （注） コントローラ VM の名前は変更できません。既存のクラスタ パスワードを使用してください。

ステップ 8 [スタート（Start）] をクリックします。**[進捗状況（Progress）]** ページに、さまざまな設定タスクの進捗状況が表示されます。

（注） デフォルトで、FlexFlash (SD カード) からブートする場合にはユーザの介入は必要はありません。ただし、ローカル ディスクからブートするようコンピューティング専用ノードを設定する場合は、Cisco UCS Managerの次の手順を完了します。

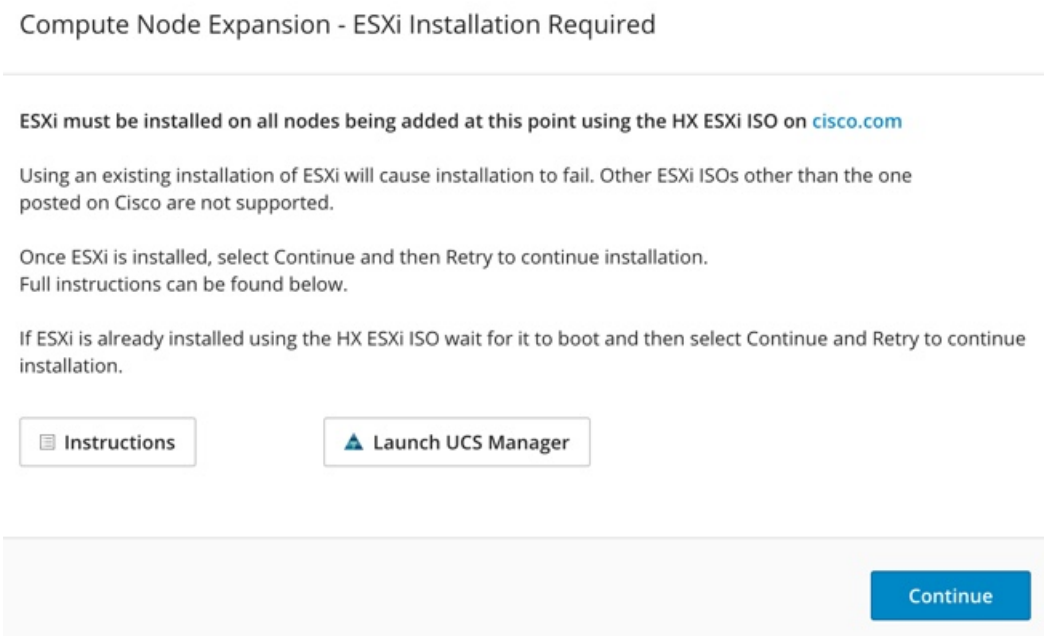
1. HX データ プラットフォーム インストーラ によって作成されたサービス プロファイルをクリックします。

   たとえば *blade-1(HX_Cluster_Name)* です。

2. **[全般（General）]** タブで、**[テンプレートからアンバインドする（Unbind from the Template）]** をクリックします。

3. 作業中のペインで、**[ストレージ（Storage）]** タブをクリックします。**[ローカル ディスクの設定ポリシー（Local Disk Configuration Policy）]** サブ タブをクリックします。

4. [アクション（Actions）] 領域で、**[ローカル ディスク設定のポリシーの変更（Change Local Disk Configuration Policy）] > [ローカル ディスク設定ポリシーの作成（Create Local DiskConfiguration Policy）]** を選択します。。
5. **[ローカル ディスク設定ポリシーの作成（Create Local Disk Configuration Policy）]** で、ポリシーの名前を入力し、残りの部分をデフォルトのままにします。[OK] をクリックします。
6. **[ローカル ディスク設定のポリシーの変更（Change Local Disk Configuration Policy）]** の [アクション（Actions）] 領域で、ドロップダウン リストから、新しく作成されたローカル ディスク設定ポリシーを選択します。[OK] をクリックします。
7. それから HX データ プラットフォーム インストーラ UI に戻り、**[Continue (続行)]** をクリックして、**[Retry UCSM Configuration (UCSM 構成の再試行)]** をクリックします。



（注） vCenterクラスタでEVCが有効になっている場合、展開プロセスが失敗し、「ホストは手動で `vCenter` に追加する必要があります（`The host needs to be manually added to vCenter`）」というメッセージが出されます。展開操作を正常に実行するには、次のようにします。

a) vSphere クライアント に追加する ESXi ホストにログインします。
b) コントローラ VM の電源をオフにします。
c) vCenter で vSphere Web クライアント クラスタにホストを追加します。
d) HX インストーラで、**[展開を再試行（Retry Deploy）]** をクリックします。

ステップ 9 インストールが完了したら、**[HyperFlex Connect の起動（Launch HyperFlex Connect）]** をクリックしてストレージ クラスタの管理を開始します。

ステップ 10 新しいノードがストレージ クラスタに追加された後、HA サービスがリセットされ、追加されたノードを HA が認識できるようになります。

a) VMware vSphere クライアントにログインします。
b) [Home] > [Hosts and Clusters] > [Datacenter] > [Cluster] > [Host] の順に選択します。
c) 新規ノードを選択します。
d) 右クリックして [Reconfigure for vSphere HA] を選択します。

ステップ 11 既存のクラスタにコンピューティング専用ノードを追加した後、vmotion の vmk2 インターフェイスを手動で設定する必要があります。

クラスタ拡張の障害の解決

エラー ダイアログボックスが表示され、ストレージ クラスタの拡張が完了しない場合は、次に示す解決オプションに進みます。

ステップ 1 **[構成の編集（Edit Configuration）]**：[クラスタの設定（Cluster Configuration）] ページに戻ります。検証ページに記載されている問題を修正してください。

ステップ 2 **[初めからやり直す (Start Over)]**：進捗テーブル エントリを消去することで、適用した設定を無効にし、[Cluster Configuration] ページに戻って新しい展開を再度開始できます。テクニカル アシスタンス センター（TAC）を参照してください。

ステップ 3 **[続行（Continue）]**：障害でエラーが発生した状態のまま、ストレージ クラスタにノードを追加します。テクニカル アシスタンス センター（TAC）を参照してください。

（注） 障害についてよく理解し、予測できない動作の可能性を受け入れる用意がある場合にのみ、[続行（Continue）] ボタンを選択してください。

HyperFlex の再展開を目的としたノードのクリーンアップの詳細については、『HyperFlex Customer Cleanup Guides for FI and Edge』を参照してください。

ロジカル アベイラビリティ ゾーン

論理アベイラビリティゾーン（LAZ）機能は、高い復元力を可能にするノードの固定数プールにクラスタ ストレージ ノードをグループ化します。レプリケーション係数やクラスタ サイズなどのクラスタ パラメータに基づいて自動的に設定するか、手動で選択できるゾーンの数。8 つ以上のストレージノードを持つ HyperFlex クラスタでは、LAZ はデフォルトで有効になっています。この機能は、インストール時またはインストール後のいずれかで明示的に無効にしない限り、クラスタのライフサイクルを通じて有効のままになります。

ロジカル アベイラビリティ ゾーンの利点

分散システムで大規模なクラスタの障害を減らすことは、インストール時に LAZ を有効にする主な利点です。分散ストレージシステムでは、クラスタ内のリソースの数が増えると、障害

リスクも増大します。複数の障害が同時に発生すると、永続的なデータが使用できなくなる可能性があります。

LAZは、複数のコンポーネントおよびノードの同時障害が致命的な障害を引き起こすリスクを軽減するのに役立ちます。これは、いくつかの基本的な制約に基づいてリソースをグループ化することで実現します。LAZ を使用しない同じクラスタと比較して、可用性を 20%ー70% 向上させることができます。改善の程度は、クラスタ レプリケーション係数（RF）および設定されているゾーンの数によって異なります。原則として、クラスタの数が少なく、レプリケーション係数が高いほど、最適な結果が得られます。さらに、LAZは同じゾーンにグループ化された複数のリソースでメンテナンスタスクを実行することで時間を節約します。これは、LAZがないクラスタでは不可能なオプションです。

HyperFlex クラスタのインストール時に LAZ を有効にすることをお勧めします。インストール時に LAZ を有効にすると、最適なクラスタ パフォーマンスとデータ可用性が提供されます。サポートのガイダンスに従って、LAZ はコマンド ライン インターフェイス（CLI）を使用して後で有効または無効にできます。無効にする前に、LAZ のガイドラインを確認してください。

ゾーン数の指定とバランスの最適化

ゾーンの数はデフォルトで自動的に設定され、推奨されます。インストーラでゾーン数を決定する場合、ゾーン数はクラスタのノード数い基づいて決定されます。

容量の利用とデータの分散を最もバランス良く保つため、クラスタ内のノード数を ゾーン、3、4、または 5 の倍数にすることをお勧めします。たとえば、8 ノードは 2 台のサーバーによる 4 つのゾーンに均等に分割され、9 ノードは 3 台のサーバーによる 3 つのゾーンに均等に分割されます。11 ノードでは、ゾーン間でノード数のバランスが悪くなり、ノードにおける容量の利用のバランスが悪くなります。必要なユーザは、3、4、または5ゾーンを手動で指定できます。

LAZ のガイドラインと考察事項

- HyperFlex クラスタは、各ゾーンに参加するノードを決定します。この設定は変更できません。
- リソースの数を変更する場合は、設定された各ゾーンから同じ数のリソースを追加または削除します。
- **クラスタ拡張**：バランスの取れたゾーンを維持するために、ゾーンに見合っただけノード数も増やして拡張を実行します。バランスの取れたゾーンとは、インストールまたは拡張時に追加されたゾーンごとのノード数（またはゾーンのノードの永続的な障害が発生して変化したゾーンごとのノード数）が等しい場合、そのように考えます。たとえば、12 ノードと 4 ゾーンのクラスタはバランスの取れたゾーンです（各ゾーンに 3 ノードずつ）。この場合、拡張時には 4 つのノードを追加することをお勧めします。
- **アンバランスなゾーン**：インストールまたは拡張時に追加されたゾーンごとのノード数（またはゾーンのノードの永続的な障害が発生して変化したゾーンごとのノード数）が等しくない場合、ゾーンはアンバランスなものとなる可能性があります。アンバランスなゾーンはパフォーマンスの最適化を損なう可能性があるため、**お勧めしません**。たとえ

ば、11 ノードと 4 ゾーンのクラスターでは、最後のゾーンを除き、ゾーンごとに 3 つのノードが存在するようになります。この場合、バランスを取るために 1 つのノードを追加する必要があります。新しいノードは、最後のゾーンに自動的に追加されます。

- **LAZ の無効化と再有効化**：LAZ を動的に無効または有効にできます。ゾーンの数が異なる同じクラスタで LAZ を無効にしてから再度有効にすることは推奨されません。これを行うと、すでにデータが含まれているクラスタで LAZ がオンになっている場合に、既存のデータ分散ルールに準拠するために、クラスタ全体でデータの移動と再編成が過剰に行われる可能性があります。これにより、クラスタの使用率がすでに 25% を超えている場合など、クラスタがゾーンに準拠しなくなることがあります。

LAZ のステータスと接続

- HX Connectダッシュボードから LAZ情報を表示するには、HX Connectにログインし、**[システム情報（System information）]** および **[HyperFlex Connect]** > **[ダッシュボード（Dashboard）]**メニューを使用します。
- `stcli cluster get-zone` コマンドを実行して、CLI から LAZ の詳細を表示することもできます。次に、`stcli cluster get-zone` コマンドの出力例を示します。

```
stcli cluster get-zone

zones:
    ----------------------------------------
    pNodes:
        ----------------------------------------
        state: ready
        name: 10.10.18.61
        ----------------------------------------
        state: ready
        name: 10.10.18.59
        ----------------------------------------
    zoneId: 0000000057eebaab:0000000000000003
    numNodes: 2
    ----------------------------------------
    pNodes:
        ----------------------------------------
        state: ready
        name: 10.10.18.64
        ----------------------------------------
        state: ready
        name: 10.10.18.65
        ----------------------------------------
    zoneId: 0000000057eebaab:0000000000000001
    numNodes: 2
    ----------------------------------------
    pNodes:
        ----------------------------------------
        state: ready
        name: 10.10.18.60
        ----------------------------------------
        state: ready
        name: 10.10.18.63
        ----------------------------------------
    zoneId: 0000000057eebaab:0000000000000004
    numNodes: 2
    ----------------------------------------
    pNodes:
```

```
        ----------------------------------------
        state: ready
        name: 10.10.18.58
        ----------------------------------------
        state: ready
        name: 10.10.18.62
        ----------------------------------------
    zoneId: 0000000057eebaab:0000000000000002
    numNodes: 2
    ----------------------------------------
isClusterZoneCompliant: True
zoneType: logical
isZoneEnabled: True
numZones: 4
AboutCluster Time : 08/22/2019 2:31:39 PM PDT
```

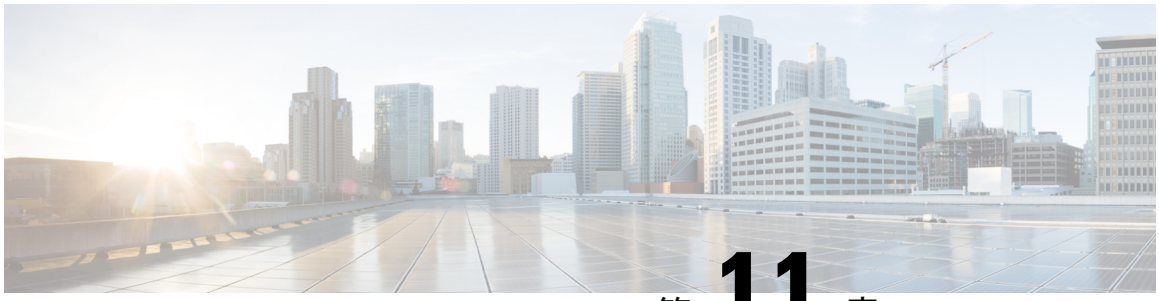
LAZ 関連コマンド

次の STCLI コマンドは、LAZ 操作に使用されます。詳細については、『Cisco HyperFlex Data Platform CLI ガイド』を参照してください。

この手順で LAZ の無効化操作と LAZ の有効化操作を連続的に実行する場合、実行の間隔を少なくとも 10 秒ほど空けるようにしてください。

コマンド	説明
stcli cluster get-zone	ゾーンの詳細を取得します。Gets the zone details. このオプションは、ゾーンが有効になっているか確認するために使用されます。
stcli cluster set-zone --zone 0	ゾーンを有効または無効にします。

コマンド	説明
stcli cluster set-zone --zone 1 **stcli rebalance start**	（**推奨**）ゾーンを有効化して作成します（デフォルトのゾーン数） **重要** ゾーンを有効化および作成したら、**rebalance start** コマンドを実行する必要があります。 ゾーン分割を有効化せずに作成されたクラスタは、ゾーン分割を有効化し、再調整を正常に完了した後にのみゾーンに対応できるようになります。 **警告** リバランスは重要なバックグラウンドサービスです。サービスを無効にすると、クラスタの復元力が失われるなど、予期しない動作が発生する可能性があります。このコマンドのサポートは、シスコ テクニカル サポートに限定されます。一般的な使用はサポートされていません。 再調整アクティビティをトリガーすると、クラスタ内の複数のノード間で大規模なデータ移動が行われる場合があります。これにより、クラスタ内のIOパフォーマンスが低下する可能性があります。
stcli cluster set-zone --zone 1 --numzones **<integer-value>** **stcli rebalance start**	ゾーンを有効化し、特定の数のゾーンを作成します。 **重要** ゾーンの数は、3、4、または 5 のみです。 **重要** ゾーンを有効化および作成したら、**rebalance start** コマンドを実行する必要があります。 **警告** リバランスは重要なバックグラウンドサービスです。サービスを無効にすると、クラスタの復元力が失われるなど、予期しない動作が発生する可能性があります。このコマンドのサポートは、シスコ テクニカル サポートに限定されます。一般的な使用はサポートされていません。



第 11 章

混在 CPU を伴うクラスタの設定

この章では、同じ FI 上に複数の Intel CPU バージョンが搭載された HX ノードを追加する方法について説明します。

概要

HyperFlex は、同じファブリック インターコネクト上で Intel v3 CPU と Intel v4 CPU をサポートします。Intel v3 CPU と Intel v4 CPU の間で仮想マシンを移行するには、VMware の拡張 vMotion 互換性（EVC）を有効にします。EVC を有効にすると、HyperFlex クラスタ内のすべてのホストの設定で、下位モデル CPU の機能を伴う基準が適用されます。どのホストで稼働しているかに関係なく、同一の CPU 機能が仮想マシンに公開されるので、HyperFlex クラスタ内のホスト間で仮想マシンを移行できます。これにより、ホストの基盤となるハードウェアが異なる場合でも、vMotion の CPU 互換性が保証されます。

混合 CPU を使用するための前提条件

- EVC 対応クラスタでは、単一のベンダー製の CPU だけを使用できます。EVC 対応クラスタに別のベンダー製のホストを追加することはできません。
- 複数のリビジョン番号（v2、v3、または v4）を持つ Xeon E3 または Xeon E5 ファミリの Intel プロセッサを搭載したクラスタ用に EVC を有効にする場合は、EVC 基準が必要です。
- 高度な仮想 CPU 機能が使用可能な場合は、BIOS でこれを有効にします。そうしないと、EVC 互換性チェックで特定の CPU に存在するはずの機能を検出が機能不全になり、EVC の有効化で問題が発生する可能性があります。

- 次のシナリオでは、EVC クラスタ内に仮想マシンが存在しても、vMotion を使用した仮想マシンの移行が失敗する可能性があります。
  - ホストが vCenter Server システムに接続されていない場合。
  - ホストが vMotion 用に設定されていない場合。
  - 仮想マシンが送信元ホストと宛先ホストの共有ストレージ上に存在しない場合。

EVC モードと CPU の互換性

ご使用の CPU と互換性のある拡張 VMotion 互換性 (EVC) モードを特定するには、『VMware Compatibility Guide』を検索してください。サーバ モデルまたは CPU ファミリを検索し、CPU シリーズ列のエントリをクリックすると、互換性のある EVC モードが表示されます。

ホストの現在の EVC モードの検索

各 EVC モードは、同じ名前のプロセッサで使用できる機能に緊密に対応しています。

vSphere Web クライアントの使用

1. vSphere Web Client Navigator から **[ホストとクラスタ（Hosts and Cluster）]** > **[HX クラスタ（HX Cluster）]** > **[サマリー（Summary）]** を選択します。[サマリー（Summary）] タブには、EVC が有効になっているかどうかと、ホストの現在の EVC モードが表示されます。
2. ホストでサポートされるすべての EVC モードのリストを表示するには、EVC モードの横にある青色のアイコンをクリックします。

VMware 共有ユーティリティ ツールの使用

VMware は、互換性 EVC モードを表示する無料 CPU 識別ユーティリティに加えて、他の CPU 機能も備えています。このユーティリティをダウンロードし、共有ユーティリティを使って ISO イメージからホストを起動できます。

既存のクラスタでの vMotion との拡張された互換性（EVC）の有効化

クラスタ内のホスト間で vMotion による移行が確実に行われるようにするには、EVC を有効にします。EVC モードは、同じ HyperFlex クラスタ内で異なる CPU ファミリを混在させる場合に必要です。EVC モードが有効になると、設定された EVC モードの最小要件を満たすホストだけがクラスタに追加されます。クラスタの拡張中でも、中断することなく EVC モードを有効にすることができます。

（注）
- EVC はデフォルトで無効になっています。クラスタ設定の [VMware EVC] で EVC を有効にすることができます。
- これは HX Data Platform の制約ではなく、VMware の制限です。詳細については、VMware KB の記事『EVC and CPU Compatibility FAQ (1005764)』を参照してください。

（注）
- EVC モードを有効にする場合は、EVC モードが Advanced Encryption Standard New Instructions（AES-NI）をサポートしていることを確認します。
- これは HX Data Platform の制約ではなく、VMware の制限です。詳細については、VMware KB の記事『EVC and CPU Compatibility FAQ (1005764)』を参照してください。

新世代のサーバを追加する統一クラスタ、そしてサーバの世代が混合した既存のクラスタという考慮すべき 2 つのパスがあります。

均一クラスタへの新世代サーバの追加

クラスタが現在均一で、新世代サーバをクラスタに追加する場合は、VC で現在の世代の EVC モードを選択することで、EVC オンラインを中断せずに有効にすることができます。次に、拡張を使用して通常どおりに続行します(コンバージドまたはコンピューティングのみ)。拡張が試行される前に、EVC モードが設定されていることが必須です。

クラスタ拡張を実行する前に、均一クラスタで EVC モードを有効にするには、次の手順を実行します。

ステップ 1 HX クラスタで vMotion との拡張された互換性 (EVC) を有効にする

a) vSphere Web Client Navigator から **[ホストとクラスタ（Hosts and Cluster）]** > **[データセンター（Datacenter）]** > ***[HX クラスタ（HX Cluster）]*** を選択します。

b) EVC を有効にする対象となるクラスタを選択します。[ワーク（Work）] ペインで、[管理（Manage）] または [設定（Configure）] タブをクリックします。[VMware EVC] を選択します。

c) [編集（Edit）] ボタンをクリックし、該当する [EVC モード（EVC mode）] を選択します。[OK] をクリックします。

ステップ 2 HyperFlex インストーラを使用したコンピューティングのみまたはコンバージド ノードの展開を続行します。

既存のクラスタへの混合または旧世代サーバの追加

クラスタにはすでにサーバの世代が混在しているか、既存のクラスタに旧世代のサーバを追加する必要があります (コンピューティング専用ノード)。

（注） 新しいノードを持つクラスタ拡張ワークフロー中にEVCモードが有効になっていない場合は、これらの手順に従ってください。

旧世代サーバを既存のクラスタに追加するには、次の手順を実行します。

ステップ 1 開始する前に、HyperFlex クラスタが正常であり、すべてのノードがオンラインであることを確認してください。

- **vSphere Web クライアントの使用**

  vSphere Web クライアント ナビゲータから、[Home] > [Global Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [HX Cluster] > [Summary] の順に選択します。

  レスポンスの例：

  ```
  Operational Status: Online
  Resiliency Status: Healthy
  ```

- **コントローラ VM を使用**

  コントローラ VMで、`#stcli cluster info` コマンドを実行します。

  レスポンスの例：

  ```
  healthstate: healthy
  state: online
  ```

ステップ 2 すべての非ストレージ コントローラ仮想マシンの電源をオフにします。

ステップ 3 1 つのストレージ コントローラ VM にログインし、`stcli cluster shutdown` コマンドを実行します。実行が完了するまで待ちます。

ステップ 4 すべてのストレージ コントローラ VM をシャットダウンします。

a) vSphere Web Client ナビゲータから、**[VM とテンプレート（VMs and Templates）]** > **[vCenter サーバー （vCenter server）]** > **[データセンター（Datacenter）]** > **[検出された仮想マシン（Discovered virtual machine）]** > **[仮想マシン（Virtual Machines）]** > **[controller_vm]**を選択します。

b) **controller_vm** を右クリックするか、 [Actions] メニューから **[Power]** > **[Shut Down Guest OS]** を選択します。

ステップ 5 各 HX ホストをメンテナンス モードにします。

a) vSphere Web Client Navigator から **[ホストとクラスタ（Hosts and Cluster）]** > **[データセンター（Datacenter）]** > ***[HX クラスタ（HX Cluster）]*** > ***[ノード（node）]*** を選択します。

b) ノードを右クリックし、**[Maintenance Mode]** > **[Enter Maintenance Mode]** の順に選択します。

（注） この操作に [Cisco HX メンテナンス モード（Cisco HX Maintenance Mode）] メニューを使用しないでください。

ステップ 6 HX クラスタで vMotion との拡張された互換性 (EVC) を有効にする

a) vSphere Web Client Navigator から **[ホストとクラスタ（Hosts and Cluster）]** > **[データセンター（Datacenter）]** > ***[HX クラスタ（HX Cluster）]*** を選択します。

b) EVC を有効にする対象となるクラスタを選択します。[ワーク（Work）]ペインで、[管理（Manage）] または [設定（Configure）] タブをクリックします。[VMware EVC] を選択します。

c) [編集（Edit）] ボタンをクリックし、該当する [EVC モード（EVC mode）] を選択します。[OK] をクリックします。

ステップ 7 メンテナンス モードを終了します。

a) vSphere Web Client Navigator から **[ホストとクラスタ（Hosts and Cluster）]** > **[データセンター（Datacenter）]** > ***[HX クラスタ（HX Cluster）]*** > ***[ノード（node）]*** を選択します。

b) ノードを右クリックし、**[Maintenance Mode]** > **[Exit Maintenance Mode]** の順に選択します。

（注） この操作に [Cisco HX メンテナンス モード（Cisco HX Maintenance Mode）] メニューを使用しないでください。

ステップ 8 ホストのメンテナンス モードが終了した後、コントローラ VM が自動的に電源オンになるはずです。コントローラ VM の電源が自動的にオンにならない場合は、次の操作を行います。

a) vSphere Web Client ナビゲータから、**[VM とテンプレート（VMs and Templates）]** > **[vCenter サーバ（vCenter server）]** > **[データセンター（Datacenter）]** > **[ESXi エージェント（ESXi Agents）]** > **[仮想マシン（Virtual Machines）]** > **[controller_vm]**を選択します。

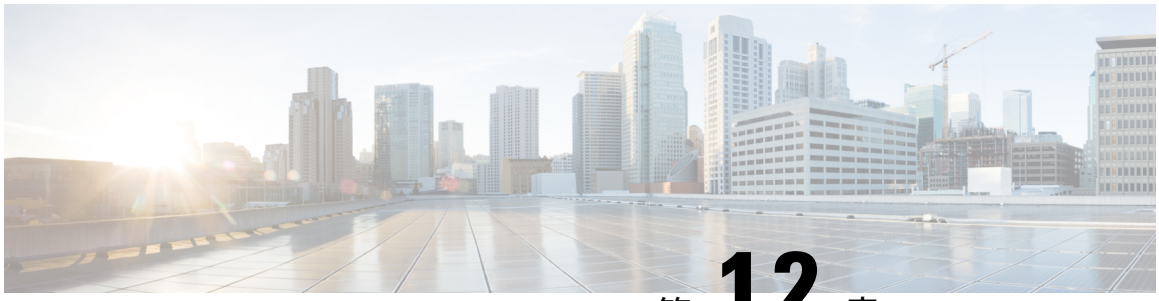
b) [controller_vm] を右クリックするか、[アクション（Actions）] メニューからクリックします。**[電源（Power）]** > **[電源オンまたは電源（Power On or Power）]** > **[電源オン（Power ON）]** を選択します。

ステップ 9 すべてのコントローラ VM が完全に起動していることを確認してください。次に、コントローラ VM の 1 つにログインし、`stcli cluster start` コマンドを実行します。

ステップ 10 すべてのデータストアが vCenter HX プラグインからマウントされていることを確認し、クラスタが正常であることを確認します。

ステップ 11 ユーザ VM を開始します。

ステップ 12 HyperFlex インストーラを使用したコンピューティングのみの展開を続行します。



第 12 章

Cisco HyperFlex Systems のカスタマイズされたインストール方法

概要

この章では、インストール手順に移る前に手動で HyperFlex サーバを準備するプロセスについて説明します。このカスタマイズされたインストール方法を、次のシナリオで使用することができます。

- HyperFlex クラスタにコンピューティング専用ノードを追加する。
- Cisco HyperFlex システムの再展開。

実行するタスクは、事前設定された HyperFlex Systems を展開する場合と基本的に同じです。事前設定されていないシステムに固有の新しいタスクは、VMware ESXi のインストールです。

事前設定されていない Cisco HyperFlex システムのインストールおよび設定のワークフロー

始める前に

Cisco HyperFlex System のインストールと設定の要件を確認します。詳細については、「インストールの前提条件」を参照してください。

ステップ 1 vCenter でクラスタを削除することにより、既存の環境をクリーンアップします。Cisco UCS で、vCenter MOB エントリ、UCS Manager サービス プロファイル、および VLAN を削除します。

ステップ 2 「ソフトウェアのダウンロード」から **Cisco HyperFlex Data Platform インストーラ OVA** ファイルをダウンロードします。

例：

```
Cisco-HX-Data-Platform-Installer-v2.5.1b-26284.ova
```

ステップ 3 HX Data Platform のインストーラを起動してサインインします。

a) [カスタマイズされたワークフロー（Customized Workflow）] を選択します。

b) [UCS Manager 設定の実行（Run UCS Manager configuration）] を選択して、UCS サービス プロファイルを設定します。『Cisco HyperFlex Systems Installation Guide for VMware ESXi』の「Configuring Cisco UCS Manager and HX Data Platform」のセクションに記載されている手順に従います。

ステップ 4 vMedia を使用して、新規の ESXi インストールを実行します。

（注） 自動 IP アドレス割り当てに Dynamic Host Configuration Protocol（DHCP）を使用することは推奨されません。デフォルトでは、HX Data Platform Installer によって、ESXi サーバーに静的 IP アドレスが割り当てられます。DHCP を使用する場合は、適切な VLAN を使用して ESXi でネットワークを手動で設定します。

ステップ 5 HX Data Platform のインストーラを再び起動します。

a) [カスタマイズされたワークフロー（Customized Workflow）] を選択します。

b) [ESX 設定の実行（Run ESX Configuration）]、[HX ソフトウェアの展開（Deploy HX Software）]、および [HX クラスタの作成（Create HX Cluster）] を選択します。

ウィザードで必ず [既存のパーティションの削除（Delete Existing Partitions）] を選択してください。

VMware ESXi のインストール

サーバーには、VMware ESXi のサポートされているバージョンが必要です。最適な HX スナップショットのパフォーマンスと機能を実現するには、ESXi 7.0 U2 以降をインストールすることを推奨します。 サポートされる ESXi バージョンのリストについては、最新の『Release notes for Cisco HX Data Platform』を参照してください。

重要 各 HX サーバで ESXi をインストールします。

Cisco HyperFlex Data Platform のソフトウェア ダウンロード ページから VMware ESXi イメージをダウンロードします。Cisco UCS Manager を介してアクセス可能なネットワーク ロケーションを選択します。

HX カスタム ISO は、Cisco カスタム ESXi リリースに基づいています。

たとえば、

```
HX-Vmware-ESXi-60U2-4192238-Cisco-Custom-6.0.2.3.iso
```

。

次のタスク

- Cisco UCS Manager を通じた vMedia およびブート ポリシーの構成
- リモート KVM コンソールを開きます。
- サーバを再起動してインストールを開始します。
- Cisco UCS Manager を介して vMedia およびブート ポリシーの変更を元に戻します。

Cisco UCS Manager での vMedia およびブート ポリシーの設定

Cisco UCS vMedia ポリシーとブート ポリシーを設定するには、次の手順を実行します。

始める前に

HX Data Platform インストーラにログインします。Cisco UCS Manager の設定に応じて、標準クラスタ用の [クラスタの作成（Create Cluster）] ワークフローを実行します。

（注） サーバからサービスプロファイルの関連付けを解除する際に特定しやすくするために、*Temporary* という名前のクラスタを作成してください。

ステップ 1 Cisco UCS Manager のナビゲーション ペインで [サーバ（Servers）] タブをクリックします。

ステップ 2 **[サーバ（Servers）] > [ポリシー（Policies）] > [ルート（root）] > [下位組織（Sub-Organizations）] > [hx-cluster] > [vMedia ポリシー（vMedia Policies）]** を展開します。

ステップ 3 [vMedia ポリシー HyperFlex（vMedia Policy HyperFlex）] をクリックします。

ステップ 4 設定ペインで、[vMedia マウントの作成（Create vMedia Mount）] をクリックしします。

ステップ 5 マウントの名前を入力します（例：**ESX**）。

ステップ 6 [CDD オプション（CDD option）] を選択します。

ステップ 7 プロトコルとして [HTTP] を選択します。

ステップ 8 [IP アドレス（IP Address）] に HyperFlex インストーラ VM の IP アドレスを入力します（例：**192.168.10.210**）。

ステップ 9 [変数イメージ名（Image Variable Name）] として [なし（None）] を選択します。

ステップ 10 [Remote File（リモート ファイル）] に **HX-Vmware-ESXi-6.0.0-3380124-Custom-Cisco-6.0.1.2.iso** と入力します。

ステップ 11 [リモート パス（Remote Path）] に **/images/** と入力します。

ステップ 12 [変更の保存（Save Changes）] をクリックし、[OK] をクリックします。

ステップ 13 設定ペインで、**[サーバ（Servers）]** > **[サービス プロファイル テンプレート（Service Profile Templates）]** > **[ルート（root）]** > **[サブ組織（Sub-Organizations）]** > **[hx-cluster]** > **[サービス テンプレート hx-nodes（Service Template hx-nodes）]** を選択します。

ステップ 14 **[vMedia Policy]** タブをクリックします。

ステップ 15 [vMedia ポリシーの変更（Modify vMedia Policy）] をクリックします。

ステップ 16 ドロップダウン選択項目から [HyperFlex vMedia ポリシー（HyperFlex vMedia Policy）] を選択して、[OK] を 2 回クリックします。

ステップ 17 **[サーバ（Servers）]** > **[ポリシー（Policies）]** > **[ルート（root）]** > **[サブ組織（Sub-Organizations）]** > **[hx-cluster]** > **[Boot Policy HyperFlex]** を選択します。

ステップ 18 ナビゲーション ペインで、[CIMC マウント vMedia（CIMC Mounted vMedia）] というセクションを展開します。

ステップ 19 [CIMC マウント CD/DVD の追加（Add CIMC Mounted CD/DVD）] という名前のエントリをクリックします。

ステップ 20 [ブート順序（Boot Order）] リストで [CIMC マウント CD/DVD（CIMC Mounted CD/DVD）] エントリを選択し、[上へ（Move Up）] ボタンを何度かクリックして [CIMC マウント CD/DVD（CIMC Mounted CD/DVD）] エントリをリストの先頭に移動させます。

ステップ 21 [変更の保存（Save Changes）] をクリックし、[OK] をクリックします。

次のタスク

サブ組織 *Temporary* を削除します。

リモート KVM コンソールを開く

1 つ以上のサーバの進行状況をモニタするには、リモート KVM コンソール セッションを開いてインストール状況を監視することを推奨します。

KVM コンソールを開くには、以下の手順を実行します。

ステップ 1 Cisco UCS Manager のナビゲーション ペインで [サーバ（Servers）] をクリックします。

ステップ 2 **[サーバ (Servers)]** > **[サービス プロファイル (Service Profiles)]** > **[ルート (Root)]** > **[サブ組織 (Sub-Organizaitons)]** > **[HX クラスタ (hx-cluster)]** > **[ラック ユニット番号 (rack-unit-number)]** の順に展開します。

ステップ 3 [ワーク（Work）] ペインで、[全般（General）] タブをクリックします。

ステップ 4 [アクション（Actions）] 領域で、[KVM コンソール（KVM Console）] をクリックします。

ステップ 5 セキュリティ アラートが表示される場合は [続行（Continue）] をクリックします。しばらくしてリモート **KVM コンソール** ウィンドウが開き、サーバのローカル コンソール出力が表示されます。

ステップ 6 インストール中に **KVM コンソール**をモニタする対象のサーバごとに、ステップ 2 ～ 4 をさらに繰り返します。

サーバの再起動

vMedia ポリシー、ブート ポリシー、およびサービス プロファイル テンプレートを変更した後、インストールを開始するにはサーバを再起動します。

サーバを再起動するには、次の手順を実行します。

始める前に

サーバの再起動の進行状況をモニタリングするには、リモート KVM コンソール セッションを開きます。

ステップ 1 Cisco UCS Manager のナビゲーション ペインで [サーバ（Servers）] をクリックします。

ステップ 2 **[機器（Equipment）]** > **[ラック マウント（Rack Mounts）]** > **[サーバ（Servers）]**を展開します。

ステップ 3 [ワーク（Work）] ペインで、最初に再起動するサーバをクリックし、最後に再起動するサーバを **Shift キーを押しながらクリック**して、すべてのサーバを選択します。

ステップ 4 マウスを**右クリック**して、[リセット（Reset）] をクリックします。

ステップ 5 [OK] をクリックします。

ステップ 6 [電源の再投入（Power Cycle）] を選択し、[OK] をクリックします。

これにより、KVM コンソール ウィンドウでモニタしているサーバが即時に再起動し、リモート vMedia マウントから起動して Cisco カスタマイズ ESXi ISO をインストールします。エラー メッセージがある場合は、無視しても差し支えありません。

VMedia とブート ポリシーの変更を元に戻す

サーバがブート ループに陥ってインストール用 ISO ファイルから起動し続けることを防ぐには、ブート ポリシーの変更を元に戻します。

始める前に

すべてのサーバがリモート vMedia ファイルからすでに起動し、インストール プロセスが開始済みであることを確認します。

ステップ 1 Cisco UCS Manager のナビゲーション ペインで [サーバ（Servers）] をクリックします。

ステップ 2 **[サーバ（Servers）]** > **[ポリシー（Policies）]** > **[ルート（Root）]** > **[サブ組織（Sub-Organizaitons）]** > ***[hx-cluster_name]*** > **[ブート ポリシー（Boot Policies）]** > **[ブート ポリシー HyperFlex（Boot Policy HyperFlex）]** を展開します。

ステップ 3 [ワーク（Work）] ペインで、[全般（General）] タブをクリックします。

ステップ 4 [アクション（Actions）] 領域で、**CIMC マウント CD/DVD**をクリックします。

ステップ 5 [ブート順序（Boot Order）] リストから [CIMC マウント CD/DVD（CIMC Mounted CD/DVD）] エントリを選択し、[削除（Delete）] をクリックします。

ステップ 6 [変更の保存（Save Changes）] をクリックし、[OK] をクリックします。

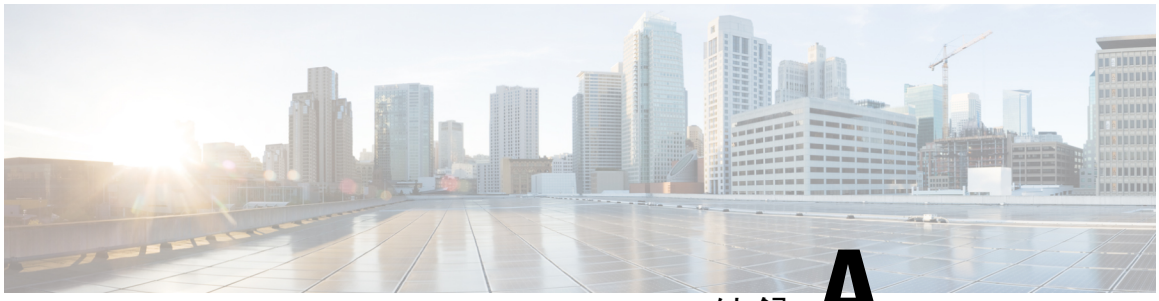
次のタスク

新しいノード

過去にクラスタ内で使用したことがない新しいノードを追加する場合は、HX クラスタを拡張します。詳細については、「クラスタ拡張ガイドライン」を参照してください。

既存のノードの再インストール

このノードが過去にクラスタに含まれ、何かを修正するためにイメージを再作成した場合には、Cisco TAC に連絡して指示を受けてください。



付録 A

ロックダウン モード

概要

このセクションでは、ロックダウン モードの概要を説明します。ロックダウン モードは、ホストへのアクセス許可を制限することにより、ESXi ホストのセキュリティを強化するために使用されます。このモードを有効にすると、ESXi ホストには vCenter Server または Direct Console ユーザー インターフェイス（DCUI）からのみアクセスできます。ロックダウン モードの有効化は、どのユーザーがホスト サービスへのアクセスを認可されるかに影響します。

（注） ロックダウン モードを有効にする場合、hxuser アカウントを各 ESXi ホスト例外ユーザー リストに追加する必要があります。

（注） ロックダウン モードが有効になり、root または administrator@vsphere.local、 またはその他のユーザーが例外ユーザー リストに含まれていない場合、これらのユーザーは ESX への SSH 接続が許可されません。同様に、何らかの理由によりホストが vCenter から削除された場合、vCenter にホストを再び追加することは許可されません。

表 *8:* ロックダウン モードの動作

サービス	通常モード	通常のロックダウン モード	厳密なロックダウン モード
vSphere Web サービス API	すべてのユーザー（権限に基づく）	vCenter（vpxuser） 例外にユーザーが含まれます（権限に基づく）。	vCenter（vpxuser） 例外にユーザーが含まれます（権限に基づく）。 vCloud Director（vslauser、該当する場合）

サービス	通常モード	通常のロックダウン モード	厳密なロックダウン モード
CIM プロバイダ	ホスト上の管理者権限を持つユーザー。	vCenter（vpxuser） 例外にユーザーが含まれます（権限に基づく）。 vCloud Director（vslauser、該当する場合）	vCenter（vpxuser） 例外にユーザーが含まれます（権限に基づく）。 vCloud Director（vslauser、該当する場合）
Direct Console UI（DCUI）	ホスト上の管理者権限を持つユーザーおよびDCUI 内のユーザー。アクセスの詳細オプション。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。	DCUI サービスが停止します。
ESXi シェル （イネーブルな場合）	ホスト上の管理者権限を持つユーザー。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。
SSH（イネーブルな場合）	ホスト上の管理者権限を持つユーザー。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。	DCUI アクセス詳細オプションで定義されたユーザー。 例外にホスト上の管理者権限を持つユーザーが含まれます。

- ロックダウン モードの有効化または無効化 （200 ページ）
- ロックダウン モードのトラブルシューティング （201 ページ）

ロックダウン モードの有効化または無効化

このセクションでは、DCUI から、または vSphere Web Client からロックダウン モードを有効または無効にする方法について説明します。

（注） ロックダウン モードが有効になり、root または administrator@vsphere.local、 またはその他のユーザーが例外ユーザー リストに含まれていない場合、これらのユーザーは ESX への SSH 接続が許可されません。同様に、何らかの理由によりホストが vCenter から削除された場合、vCenter にホストを再び追加することは許可されません。

DCUI からのロックダウン モードの有効化または無効化：

ステップ 1 ESXi ホストに直接にログインします。
ステップ 2 ホストで Direct Console ユーザー インターフェイス（DCUI）を開きます。
ステップ 3 初期設定用の **F2 キー**を押します。
ステップ 4 [ロックダウン モードの設定（Configure Lockdown Mode）] の設定を切り替えるには **Enter** を押します。
ステップ 5 VSphere Web Client のインベントリでホストを特定します。

vSphere Web Client からのロックダウンモードの有効化または無効化：

ステップ 1 VSphere Web Client のインベントリでホストを特定します。
ステップ 2 [**Manage**] タブをクリックし、[Settings] をクリックします。
ステップ 3 [System] で、**[Security profile]** を選択します。
ステップ 4 [Lockdown Mode] パネルで、**[Edit]** をクリックします。
ステップ 5 **[例外ユーザー（Exception Users）]** をクリックし、[+ ユーザーの追加（+Add user）] を選択して、hxuser (すべて小文字) を追加します。
ステップ 6 **[ロックダウン モード（Lockdown Mode）]** をクリックして、いずれかのロックダウン モード オプションを選択します。

ロックダウン モードのトラブルシューティング

ロックダウンモードでエラーダイアログボックスが表示されたりソフトウェアのアップグレードが失敗したりする場合は、次のいずれかのシナリオに応じて以下の解決オプションを実行してください。

- 少なくとも 1 つのホストがロックダウン モードである。
- アップグレードの進行中にホストがロックダウン モードである。

少なくとも 1 つのホストがロックダウン モードである場合：

1. アップグレード前の検証でホスト ロックダウン モードをチェックします。
2. 状態を検出し、エラーをスローしてクラスタのアップグレードを中止します。
3. ロックダウン モードを無効にして、アップグレードを再試行します。

アップグレードの進行中にホストがロックダウン モードである場合：

ステップ 1 ホストをアップグレードする前に、ホスト ロックダウン モードをチェックします。
ステップ 2 状態を検出してエラーを送出し、アップグレードに失敗します。
ステップ 3 ロックダウン モードを無効にして、アップグレードを再試行します。

展開フェーズでの vCenter へのホスト追加エラー

HX インストール中のロックダウンの検証は、「root」ユーザーを使用した ESXi ホストの SSH アクセシビリティ チェックです。例外リストにルート ユーザーを追加すると、ロックダウン モードの展開検証チェックがバイパスされます。この場合、展開フェーズで vCenter にホストが追加されると、そのホストは失敗し、HX のインストールも失敗します。

展開フェーズで vCenter にホストを追加すると失敗し、エラー メッセージ「**vCenter のホストを追加できません**」が表示されます。

ロックダウン モードのステータスを確認し、無効にして、「root」ユーザーを例外から削除します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。