Cisco HyperFlex システム リリース 5.0 アップグレード ガイド（VMware ESXi 向け）

初版：2021 年 11 月 10 日

最終更新：2022 年 8 月 18 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。

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、シスコ サービス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

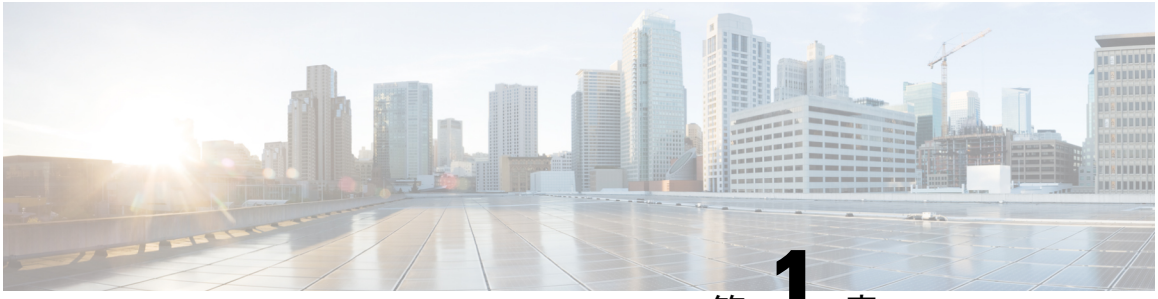
Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアの問題に関する詳細な情報を提供します。

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ーインターフェ

通信、サービス、偏向のない言語、およびその他の情報

イ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

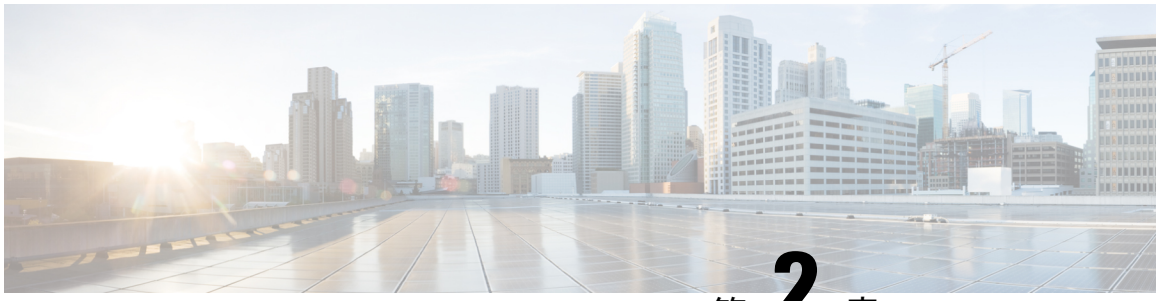
新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表に、最新リリースでの新機能とこのガイドにおける変更点の概要を示します。

特長	説明	HX のリリースまたは追加日	参照先
HyperFlex ソフトウェア暗号化	データを保護するソフトウェア暗号化の機能が追加されました。	HX 5.0(1b)	HyperFlex ソフトウェア暗号化を有効にする （37 ページ）
Cisco HyperFlex システム アップグレード ガイド（VMware ESXi 向け）	5.0(x) ガイドの最初のリリース	HX 5.0(1a)	n/a

新機能および変更された機能に関する情報



第 2 章

概要

このガイドについて

このドキュメントは、現在 HX リリース 3.5（2a）以降を実行しており、環境を最新の HX リリースにアップグレードする Cisco HyperFlex（HX）ユーザをガイドすることを目的としています。

クラスタが Intersight によって管理されている場合は、「Cisco HyperFlex Edge システムと Cisco Intersight のアップグレード」を参照してください。

オンプレミスの HyperFlex アップグレード：

- HyperFlex Connect を使用した HyperFlex Data Platform のアップグレード
- HyperFlex Edge のアップグレード
- HyperFlex ストレッチ クラスタのアップグレード
- アップグレード手順の分割

HX 展開の正しいアップグレード パスの判別

このドキュメントでは、HyperFlex Connect を使用した通常の HyperFlex 展開のアップグレードに重点を置いています。アップグレード タスクの多くは、エッジ構成とストレッチ クラスタ構成で同じですが、注意すべき違いがあります。特定の設定に基づいてこのドキュメント内を移動するには、次の情報を使用します。

1. ご使用の環境で現在実行されている Cisco HyperFlex Data Center リリースを選択し、アップグレードのワークフローに従って特定のアップグレードを行います。

現在ご使用の環境で実行されている Cisco HyperFlex データセンターのリリース	Cisco アップグレード ガイド	アップグレード ビデオのサポート
Cisco HX リリース 3.5(1a) 以前	サポートされていない Cisco HX リリース ガイドの Cisco HyperFlex システム アップグレード ガイド	シスコ コミュニティ データセンター トレーニング ビデオ
Cisco HX リリース 3.5(1b)〜4.0(x)	VMware 4.5 向け Cisco HyperFlex システム アップグレード ガイド（本ガイド）次の表に進み、展開のタイプを選択します。	近日提供予定

2. 目的のアップグレード リリースでサポートされている ESXi（vSphere）の最小バージョンを確認し、ステップ 3 に進みます。

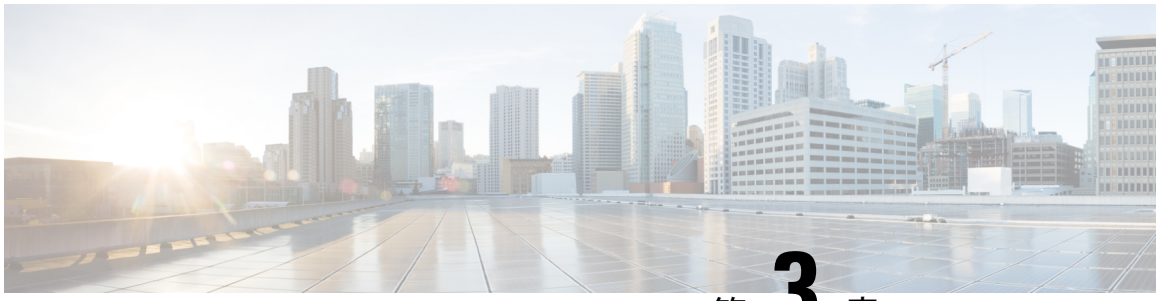
ターゲット リリース	ESXi（vSphere）の最小サポートバージョン
3.5(1a)〜4.0(2x)	6.0 U3
4.5(1a) 以降	6.5 U3

3. 展開のタイプを選択します。

展開タイプ	このガイドの章にリンク
従来型の HyperFlex 展開	HyperFlex ソフトウェアのアップグレードの前提条件（7 ページ）
HyperFlex Edge 展開	HyperFlex Edge アップグレード 概要 （39 ページ）
Intersight による HyperFlex Edge のアップグレード	Cisco Intersight を使用した Cisco HyperFlex Edge システムのアップグレード
HyperFlex ストレッチ クラスタ	ストレッチ クラスタ アップグレード 概要 （49 ページ）
分割アップグレード手順	CLI を使用した HyperFlex Data Platform ソフトウェアのみのオンライン アップグレード （59 ページ）

サポートされていない Cisco HyperFlex HX データ プラットフォーム ソフトウェア リリースからのアップグレード

サポートを終了した Cisco HyperFlex HX Data Platform ソフトウェア リリースから、Cisco ソフトウェア ダウンロード サイトの最新の提案されたリリースにアップグレードする必要がある Cisco HyperFlex ユーザーの場合、『サポートされていない Cisco HX リリースの Cisco HyperFlex システム アップグレード ガイド』で定義されている現在のリリースのアップグレード手順に従う必要があります。このガイドのステップは、古いソフトウェアを実行しているクラスタには適用されません。



第 3 章

前提条件とガイドライン

HyperFlex ソフトウェアのアップグレードの前提条件

アップグレード プロセスを開始する前に、次のタスクを実行する必要があります。

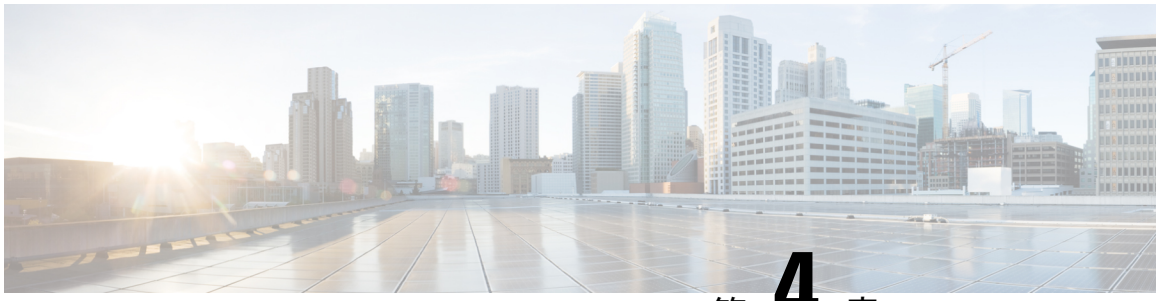
- HXDP バージョン 5.0 は、ESXi バージョン 6.5 U3 以降のみをサポートします。現在の ESXi バージョンが 6.5 U3 より前の場合は、HXDP と ESXi をターゲット レベル 6.5 U3 以降に組み合わせてアップグレードする必要があります。M6 ノードには、少なくとも ESXi 6.7 U3 以降のサポート対象バージョンが必要です。
- HX データ プラットフォーム（HXDP）ソフトウェア推奨リリース バージョン：Cisco HyperFlex HX シリーズ システムの Cisco HyperFlex アップグレード ガイドラインを見直します。
- vCenter のバージョン チェック：vCenter がバージョン 6.5 U3 以降で、アップグレードされる ESXi バージョンの最小要件を満たしていることを確認します。vCenter と ESXi の間の互換性を確保するには、VMware 製品の相互運用性マトリックスを参照してください。
- vMotion 互換性のために、すべての VM ネットワーク ポート グループがクラスタ内のすべてのノードに存在することを確認します。
- 計画されたファブリック フェールオーバー中の中断のない接続を確保するために、管理およびストレージ データの VLAN がトップオブラック ネットワーク スイッチで設定されていることを確認します。
- 環境内でジャンボ フレームを使用している場合は、ジャンボ フレームが、トップオブラック スイッチ上の vMotion およびデータ ネットワークで有効になっていることを確認します。
- アップグレード中に ESXi ホストがロックダウン モードになっていないことを確認します。ロックダウンモードは、アップグレードの完了後に再度有効にできます。

- ブレード パッケージとラック パッケージのバージョンは、ホスト ファームウェア パッケージ：M6 ノードの **HyperFlex-m5-con** および **HyperFlex-m6-con** に表示されません。
- HX CSI を使用している場合は、TAC にお問い合わせください。

アップグレードの推奨事項

サポートされたリリースのアップグレードについては、『HXデータプラットフォーム ソフトウェア推奨リリース バージョン：Cisco HyperFlex HX シリーズ システム』を参照してください。

サポートされなくなったリリースからアップグレードする場合は、『Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases』を参照してください。



第 4 章

アップグレード前の正常性検査ユーティリティ

Hypercheck: アップグレード前チェック ツール

シスコはアップグレードの前に Hypercheck 正常性チェック ツールを実行して、すべてのアップグレード要件が満たされていることを確認することを推奨します。Hypercheck: Hypercheck とアップグレード前チェック ツールは、アップグレード前にクラスタが正常であることを確認するために設計された、健全性およびアップグレード前の自動チェックです。この正常性チェックを実行するだけでなく、正常でないと判明したすべてのクラスタに対して修正措置を講じることが必要です。続行する前に、Hypercheck 正常性チェックによって報告されたすべての問題を修正します。

Hypercheck ツールを実行しない場合は、第 14 章の手動チェックリストを参照してください。これらのチェックは Hypercheck ほど包括的ではないため、手動検証は推奨されません。

Cisco HX リリース 4.5 以降向けの Hypercheck のアップグレード前ユーティリティ

HyperCheck 4.5 スクリプトが製品に含まれるようになり、Rest API の統合によりパフォーマンスが向上しました。クラスタが展開されると、Hypercheck はクラスタの一部になります。として含まれます。新機能とチェックには、クラスタ情報テーブル、DR（ローカルおよびリモートネットワーク）、およびそれらを有効にしたユーザの SED チェックが含まれます。

ステップ 1 チェックを開始するには、**hypercheck** コマンドを実行します。

ステップ 2 チェックが完了したら、結果を確認します。障害が発生した場合は、特定の回避策の手順を実行し、クラスタ ストレージの容量を確認し、設定を確認します。設定の詳細については、アップグレードの準備 （11 ページ） を参照してください。

アップグレード資格のテスト

Cisco HyperFlex リリース 4.0 (2a) 以降では、[アップグレード (Upgrade)] ページに、最後のクラスタ アップグレード資格テストの結果と、UCS サーバ、HX data platform、および ESXi の最後のテスト済みバージョンが表示されます。

UCS サーバ ファームウェア、HyperFlex Data Platform、ESXi をアップグレードする前に、[Upgrade (アップグレード)] ページのアップグレード資格テストを実行して、アップグレードに対するクラスタの準備状況とインフラストラクチャの互換性を検証します。

（注） アップグレード適格性テストでは、現在実行中の HyperFlex データプラットフォーム バージョンに含まれる検証を使用します。ターゲット HX バージョンに存在する新しい検証は含まれません。

アップグレード資格テストを実行するには、次の手順に従います。

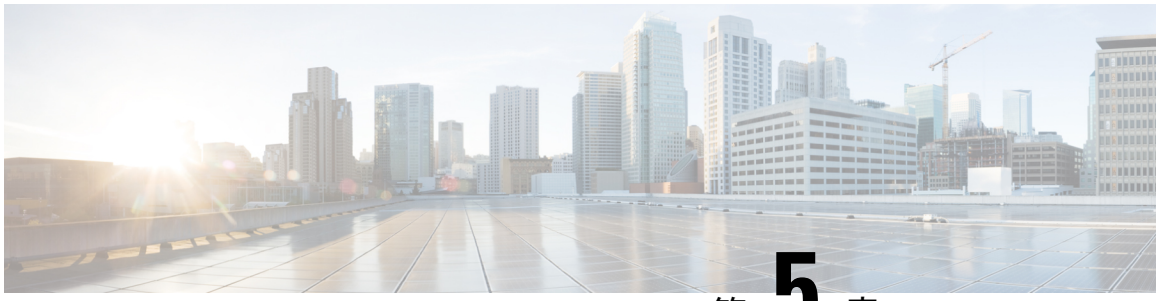
1. **[アップグレード (Upgrade)]** > **[アップグレード資格のテスト (Test upgrade 適格性)]** を選択します。
2. UCS サーバ ファームウェアのアップグレード資格をテストするには、**[UCS サーバファームウェア (UCS server firmware)]** チェックボックスをオンにします。

   Cisco UCS Manager の FQDN または IP アドレス、ユーザ名、パスワードを入力します。**[現行バージョン (Current Version)]** フィールドで、**[検出 (Discover)]** をクリックして、アップグレード前に検証する必要がある UCS ファームウェア パッケージのバージョンを選択します。
3. HyperFlex Data Platform のアップグレード資格をテストするには、**[HX Data platform]** チェックボックスをオンにします。

   vCenter のユーザ名とパスワードを入力します。アップグレードの前に検証する必要がある Cisco HyperFlex Data Platform アップグレード バンドルをアップロードします。
4. ESXi のアップグレードの適格性をテストするには、**[ESXi]** チェックボックスをオンにします。

   vCenter のユーザ名とパスワードを入力します。アップグレードの前に検証する必要がある Cisco HyperFlex カスタム イメージ オフライン バンドルをアップロードします。
5. **[検証（Validate）]** をクリックします。

   アップグレード資格テストの進行状況が表示されます。



第 5 章

アップグレードの準備

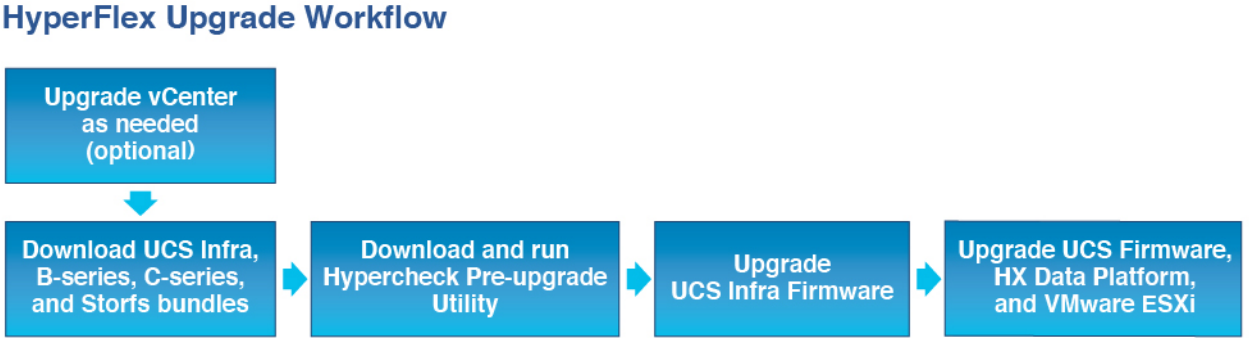
HyperFlex アップグレードの準備

（注） 次のアップグレード プロセスは、ユーザーが Cisco HX リリース 3.5(x) 以降からアップグレードする場合にのみ適用されます。

（注） HyperFlex 標準クラスタではなく、次のいずれかをアップグレードする場合：

- HyperFlex Edge クラスタについては、HyperFlex Edge アップグレード （39 ページ）を参照してください。
- ストレッチクラスタについては、ストレッチクラスタアップグレード（49ページ）を参照してください。
- 分割アップグレード手順については、HyperFlex オフラインアップグレードのワークフローと CLI アップグレード オプション （59 ページ） を参照してください。

次の図は、フルスタックの HyperFlex 標準クラスタの一般的なアップグレード ワークフローを示しています。



アップグレードでは、次のタスクをこの順序で実行する必要があります。

1. このガイドの「前提条件」の項に記載されているすべてのタスクを完了します。
2. Hypercheck システムで Hypercheck 健全性およびアップグレード前ツールを実行して、その安定性と復元力を確認します。Hypercheck：Hyperflex 健全性およびアップグレード前チェック ツール
3. VMware vCenter のバージョンが 6.5 U3 以降であることと vCenter と ESXi が互換性があることを確認します。VMware 製品の相互運用性マトリックス を参照してください。また、vCenter バージョンがターゲット HXDP バージョンと互換性があることを確認します。

クラスタのストレージ容量の確認

シスコは、Cisco HX データ プラットフォームの既存のインストールのアップグレードを開始する前に、クラスタ ストレージ容量をチェックすることをお勧めします。クラスタ内のストレージ使用率（容量とオーバーヘッド）が 76% 以上の場合、アップグレードの検証は失敗します。

クラスタ ストレージ容量をチェックすることの背景の詳細については、『*Cisco HyperFlex* データ プラットフォーム管理ガイド』の HX ストレージ クラスタの概要」の章を参照してください。

アップグレードを開始する前に、各 HyperFlex ノードで次の検証を実行します。

- HyperFlex クラスタが正常でオンラインであることを検証します。
- すべての HyperFlex クラスタ ノードが vCenter に接続されており、オンラインであることを確認します。
- DRS が有効であり、DRS に対して完全自動化に設定されていることを確認します。DRS が無効に設定されている場合、アップグレードプロセスでプロンプトが表示されたら、手動で VM を vMotion する必要があります。
- すべてのノードで vMotion が設定されていることを確認します。vMotion が設定されていない場合は、アップグレードを開始する前に、 HX クラスタの vMotion 設定を確認するを参照してください。

- ESX Agent Manager（EAM）の状態が正常であることを確認します。
- Cisco UCS Manager で UCSM ファブリック インターコネクト クラスタの状態を確認します。

Cisco UCS Manager の UCS ファブリック インターコネクト クラスタの正常性を確認する

ステップ 1 ファブリック インターコネクトの高可用性ステータスに、両方のファブリック インターコネクトが稼働中であると示されているかどうかを確認します。詳細については、『Cisco UCS Manager System Monitoring Guide』を参照してください。

ステップ 2 すべてのサーバが検出されていることを確認します。

ステップ 3 HyperFlex サーバにエラーがないことを確認します。

ステップ 4 vNIC のエラーが解消されて、VMware ESXi vSwitch アップリンクが稼働中であることを確認します。

ステップ 5 データ パスが稼働中であることを確認します。詳細については、『Cisco UCS Manager ファームウェア管理ガイド』を参照してください。

HyperFlex クラスタのヘルスの表示

CLI の使用

ストレージ クラスタ内の任意のコントローラ VM にログインします。`stcli cluster storage-summary --detail` コマンドを実行します。

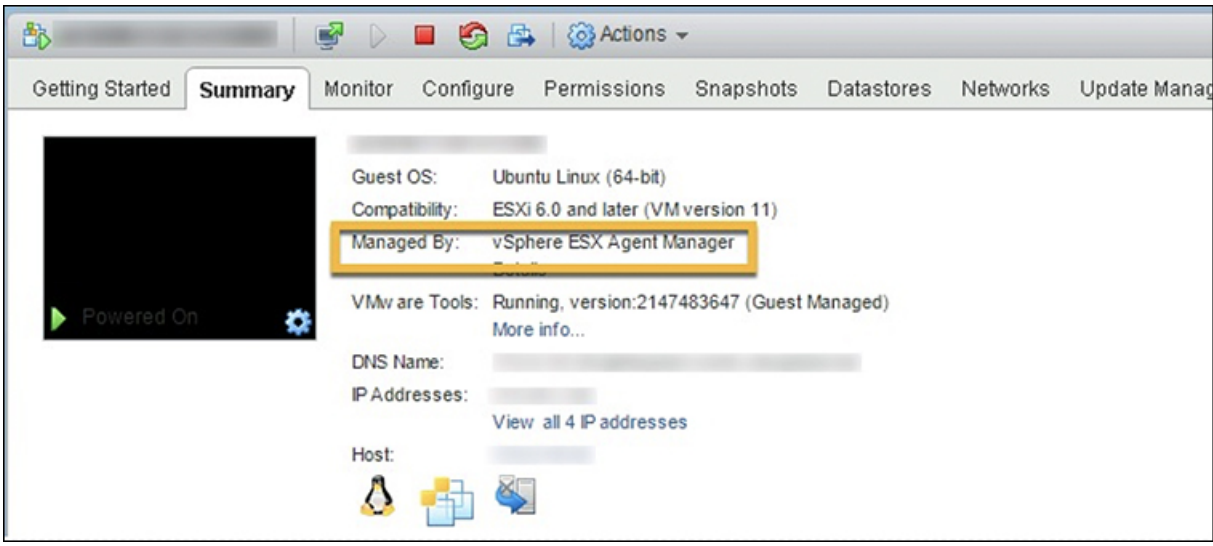
```
address: 192.168.100.82
name: HX-Cluster01
state: online
uptime: 0 days 12 hours 16 minutes 44 seconds
activeNodes: 5 of 5
compressionSavings: 78.1228617455
deduplicationSavings: 0.0
freeCapacity: 38.1T
healingInfo:
    inProgress: False
resiliencyDetails:
        current ensemble size:5
        # of ssd failures before cluster shuts down:3
        minimum cache copies remaining:3
        minimum data copies available for some user data:3
        minimum metadata copies available for cluster metadata:3
        # of unavailable nodes:0
        # of nodes failure tolerable for cluster to be available:2
        health state reason:storage cluster is healthy.
        # of node failures before cluster shuts down:3
```

```
        # of node failures before cluster goes into readonly:3
        # of hdd failures tolerable for cluster to be available:2
        # of node failures before cluster goes to enospace warn trying to move the
existing data:na
        # of hdd failures before cluster shuts down:3
        # of hdd failures before cluster goes into readonly:3
        # of ssd failures before cluster goes into readonly:na
        # of ssd failures tolerable for cluster to be available:2
resiliencyInfo:
    messages:
     Storage cluster is healthy.
     state: healthy
     hddFailuresTolerable: 2
     nodeFailuresTolerable: 1
     ssdFailuresTolerable: 2
spaceStatus: normal
totalCapacity: 38.5T
totalSavings: 78.1228617455
usedCapacity: 373.3G
clusterAccessPolicy: lenient
dataReplicationCompliance: compliant
dataReplicationFactor: 3
```

次の例の応答は、HyperFlex ストレージ クラスタがオンラインかつ正常な状態であることを示します。

ESX Agent Manager の表示

アップグレードする HyperFlex クラスタが 4.0(1a) より前のバージョンの HXDP で展開されていた場合、HyperFlex コントローラ VM は ESX Agent Manager（EAM）によって管理されます。代わりに、**[vCenter]にログインして、>[HyperFlex コントローラ VM >[サマリ（Summary）]** をクリックする（Click on the HyperFlex Controller VM）]（vCenter Click on the HyperFlex Controller VM Summary）]ことで、EAM によって管理されているかどうかを確認できます。**[Managed By**：**vSphere ESX Agent Manager]** が表示されている場合、HyperFlex コントローラ VM は EAM によって管理されているため、次のプロセスに従って EAM の健全性を確認する必要があります。それ以外の場合、このセクションは省略できます。

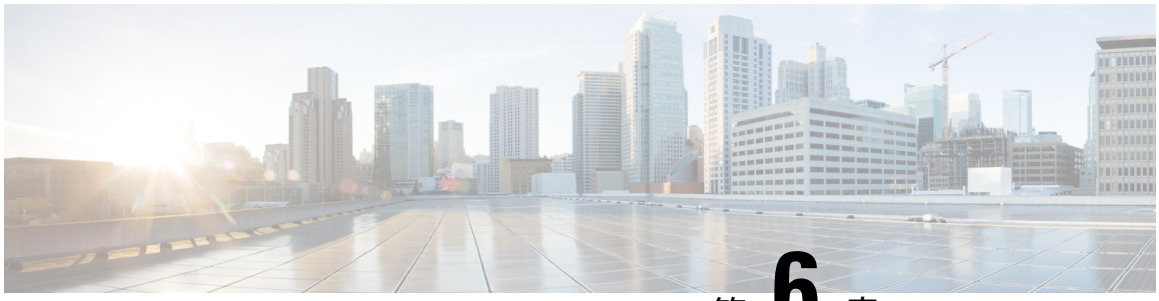


EAM ヘルスの確認：

---

vSphere Web クライアントのナビゲータで、**[管理（Administration）]** > **[vCenter Server 拡張機能（vCenter Server Extensions）]** > **[vSphere ESX Agent Manager]** > **[サマリ（Summary）]** を選択します。

ESX Agent Manager（EAM）の状態が正常であることを確認します。



第 6 章

ソフトウェア バンドルをダウンロードします

ソフトウェアのダウンロード

HyperFlex のアップグレードを正常に完了できるよう、Cisco HyperFlex ダウンロード Web サイトから次の Cisco HyperFlex System コンポーネント バンドルをダウンロードできるようになっています。

ステップ 1 https://www.cisco.com/support に移動し、[製品の選択（Select a Product）] 検索バーに **HX Data Platform** と入力します。HyperFlex HX Data Platform のダウンロード リンクをクリックします。

ステップ 2 現在の**推奨リリース** バージョンをクリックします。

ステップ 3 既存の HyperFlex クラスタを以前のリリース（`.tgz` ファイル）からアップグレードするには、最新の Cisco HyperFlex Data Platform アップグレード バンドルのカート アイコンをクリックします。

（注） ダウンロードを続行する前に、ソフトウェア アドバイザリを読み、環境に問題があるかどうかを確認してください。

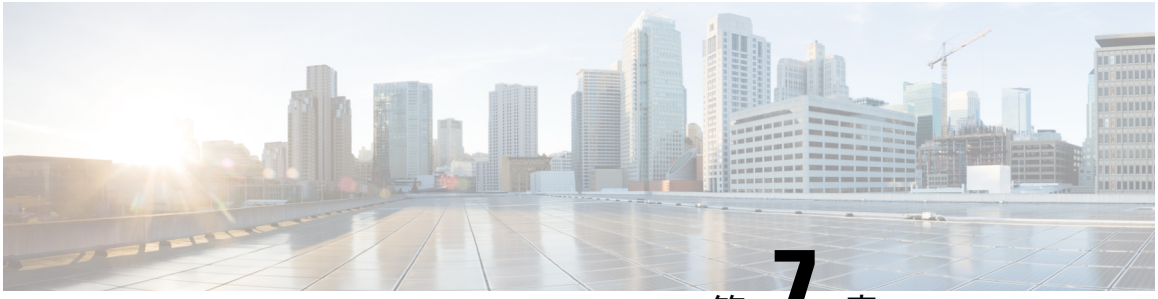
ステップ 4 FI モデルに基づいて、対応する UCS インフラストラクチャ ソフトウェア バンドルのカート アイコンをクリックします。

ステップ 5 UCS B シリーズおよび C シリーズ ブレードおよびラックマウント サーバ用ソフトウェアのカート アイコンをクリックします。

ステップ 6 vSphere をアップグレードするには、以前の ESXi バージョンからアップグレードするための ESXi オフライン バンドルの最新の HX カスタム イメージのカート アイコンをクリックします。

ステップ 7 画面の下部にあるカート アイコンをクリックしてバンドルを確認し、**[すべてダウンロード（Download All）]** をクリックします。

ステップ 8 使用許諾契約に同意して、**[OK]** をクリックして各ファイルを保存します。



第 7 章

UCS インフラストラクチャ ファームウェアのアップグレード

UCS インフラストラクチャ ファームウェア ワークフローのアップグレード

アップグレード タイプ	手順
HyperFlex クラスタ	以下のワークフローを参照してください。
HyperFlex Edge アップグレード クラスタ	HyperFlex Edge アップグレード （39 ページ）
HyperFlex ストレッチ クラスタ	ストレッチ クラスタ アップグレード （49 ページ）
アップグレード手順の分割	HyperFlex オフライン アップグレードのワークフローと CLI アップグレード オプション （59 ページ）

UCS Infra Firmware をアップグレードするには、次のタスクを実行します。

- アップグレードを開始する前に、HyperFlex ソフトウェアのアップグレードの前提条件 （7 ページ） を見直します。
- UCSM ファブリック インターコネクト クラスタの IP アドレスにログインします。
- 適切なインフラ、B シリーズ、および C シリーズ バンドルをファブリック インターコネクト にアップロードします。

注意事項と制約事項

UCSインフラ ファームウェアのアップグレードを実行する前に、次の点を考慮してください。

- 先に進む前に、hx-storage-data および vMotion のアップストリーム スイッチが**ジャンボ フレーム**用に設定されていることを確認してください。このように設定しておかないと、アップグレード ウィンドウ中で、HyperFlex クラスタでネットワークとストレージの停止が発生します。
- UCS インフラストラクチャ ファームウェアのアップグレード中には UCS Manager への接続が失われます。これは正常な動作です。

UCS インフラストラクチャ ファームウェアのアップグレード

始める前に

インフラ、B シリーズ、および C シリーズ ファブリック インターコネクトのアップグレードバンドルをダウンロードします。詳細については、ソフトウェアのダウンロード（17ページ）を参照してください。

ステップ 1 管理者権限を使用して、ファブリック インターコネクト クラスタ IP アドレスへの UCS Manager にログオンします。

ステップ 2 **[機器（Equipment）]** > **[ファームウェア管理（Firmware Management）]** > **[インストール済みのファームウェア（Installed Firmware）]**に移動します。

ステップ 3 **[UCS Manager]** を展開し、UCS Manager の実行バージョンを確認します。

ステップ 4 **[タスクのダウンロード（Download Tasks）]**> **[ファームウェアのダウンロード（Download Firmware）]** に移動します。

ステップ 5 保存したファブリック インターコネクト バンドルを参照し、以前に保存したインフラ A、B シリーズ、および C シリーズ バンドルを選択して、**[開く（Open）]** および **[OK]** をクリックします。

ステップ 6 ファイルが転送されたら、**[ファームウェア自動インストール（Firmware Auto Install）]** をクリックし、**[アクション（Actions）]** で**[インフラストラクチャ ファームウェアのインストール（Install Infrastructure Firmware）]** をクリックします。

（注） 続行する前に、すべての警告を慎重に確認し、必要に応じて問題を解決してください。

ステップ 7 問題が解決したら、**[すべて無視（Ignore All）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 8 ドロップダウンから適切な**インフラパック**を選択し、**[今すぐアップグレード（Upgrade Now）]** をオンにして、**[終了（Finish）]** をクリックします。

（注） **[はい（Yes）]** をクリックして、選択されていないサービス パックの警告を無視できます。

UCS インフラストラクチャ ファームウェアのアップグレード

ステップ 9 **[FSM]** タブをクリックして、アップグレードの進行状況を確認します。アップグレードには時間がかかります。

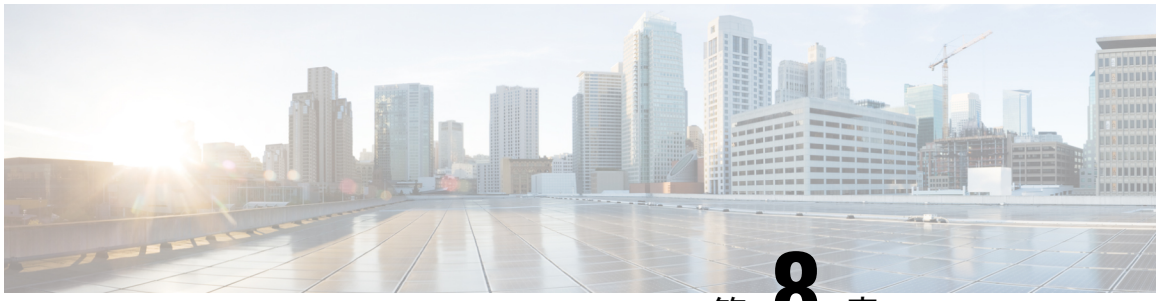
ステップ 10 一番上の **[保留中のアクティビティ（Pending Activities）]** をクリックし、**[ファブリック インターコネクト（Fablic Interconnects）]** をクリックして、プライマリ ファブリック インターコネクトのリブートを確認応答する前に、セカンダリ ファブリック インターコネクトからデータ パスが正常に復元されていることを確認します。

ステップ 11 **[今すぐ再起動（Reboot Now）]** をクリックし、**[はい（Yes）]** および **[OK]** をクリックします。

（注） アップグレード プロセス中に、ファブリック インターコネクト UI からログアウトします。再度ログインして、アップグレードの進行状況を表示します。

ステップ 12 アップグレード プロセスが完了したら、**[インストール済みのファームウェア（Installed Firmware）]** タブで更新されたバージョンを確認します。

UCS インフラストラクチャ ファームウェアのアップグレード



第 8 章

UCS サーバ ファームウェア、および HX Data Platform と VMware vSphere のアップグレード：複合アップグレード

Cisco UCS ファームウェア、HX Data Platform、および VMware vSphere ワークフローのアップグレード

Cisco HyperFlex の「フルスタック」アップグレード プロセスでは、次の 3 つのコンポーネントがアップグレードされます。

- Cisco HyperFlex データ プラットフォーム
- VMware vSphere ESXi
- Cisco UCS サーバ ファームウェア

シスコでは、HyperFlex Connect からのこれら 3 つのコンポーネントすべてを組み合わせてアップグレードすることを推奨しています。同じアップグレード ワークフローで、1 つ、2 つ、または 3 つすべてのコンポーネントをアップグレードすることを選択できます。1 つのアップグレードプロセスで複数のコンポーネントを組み合わせる場合は、次の手順に従います。それ以外の場合は、個々のコンポーネントのアップグレード手順について第 9 章を参照してください。

このセクションでは、HyperFlex Data Platform ソフトウェア、VMware ESXi、および UCS サーバファームウェアを組み合わせてアップグレードする手順について説明します。このプロセス

では、VMware vMotion を使用することで、HyperFlex ノードはワークロードを中断することなく、最適化されたローリング リブートを実行します。

（注） HX Connect から開始されるサーバ ファームウェア アップグレード操作の一部として、UCS ポリシーの一部が、新しい HXDP バージョンと互換性を持つように更新される場合があります。これらの変更は、アップグレードされるクラスタの一部であるノードにのみ適用されます。ポリシーの変化を避けるために、HX Connect を使用してサーバファームウェアのアップグレードを開始することを強くお勧めします。

アップグレード タイプ	手順
HyperFlex クラスタ	以下のワークフローを参照してください。
HyperFlex Edge クラスタ	HyperFlex Edge アップグレード （39 ページ）
HyperFlex ストレッチ クラスタ	ストレッチ クラスタ アップグレード （49 ページ）
アップグレード手順の分割	HyperFlex オフライン アップグレードのワークフローと CLI アップグレード オプション （59 ページ）

UCS ファームウェアおよび HX Data Platform をアップグレードするには、次のタスクを実行します。

- アップグレードを開始する前に HyperFlex ソフトウェアのアップグレードの前提条件 （7 ページ） を確認してください。
- 管理者権限で、HX Connect にログインしてください。
- [アップグレード（Upgrade）] ページから適切なオプションを選択します。
- 必要なファイルをアップロードし、必要なユーザー入力を完了します。

ガイドラインと制約事項

アップグレードを実行する前に、次の点を考慮してください。

- DRS が有効で、完全自動モードに設定されている場合、VM はローリング アップグレード プロセス中に他のホストに自動的に vMotion されます。

（注） DRS が 無効 に設定されている場合は、VM に対して手動で vMotion を実行して、アップグレード プロセスを続行します。詳細については、VMware のマニュアルで、vMotion を使用した移行の説明を参照してください。

- ESXi および HXDP のダウングレードはサポートされていません。
- リリース 3.5(1a) よりも前である HyperFlex リリースを実行している場合に示すように、手動ブート ストラップ プロセスを実行して Cisco HX データ プラットフォームをアップグレードする必要があります。これらの手順は、『サポートされていない Cisco HX リリース ガイドの Cisco HyperFlex システム アップグレード ガイド』で取り上げています。
- HXDP、UCS ファームウェア、および VMware ESX のソフトウェア互換性については、リリースノートを参照してください。また、ESXi をアップグレードする前に、vCenter が互換性のあるバージョンにアップグレードされていることを確認します。詳細については、Cisco HX Data Platform、リリース 5.0 のリリース ノート、Cisco HyperFlex HX シリーズ システム向けの Cisco HyperFlex HX Data Platform 推奨ソフトウェア リリース、および VMware Product Interoperability Matrices を参照してください。
- UCS Manager で使用可能なツールを使用して UCS サーバ ファームウェアを手動でアップグレードしないでください。HyperFlex サーバ用の UCS Manager のポリシーに対する変更は、オーケストレーションされたサーバ ファームウェア アップグレード プロセスによって提供されます。帯域外のファームウェア更新を手動で実行すると、これらの重要な設定の更新が失われます。
- HX 4.5 のアップグレード中に SSL 証明書が再生成されるため、新しい証明書が再インポートされるまで VEEAM 統合が中断されます。

HX Connect を使用した HyperFlex Data Platform ソフトウェア、VMware ESXi、および Cisco UCS サーバ ファームウェアのアップグレード

始める前に

- [ソフトウェアのダウンロード（Downloading Software）から、既存のクラスタを以前のリリースからアップグレードするための最新の Cisco HX Data Platform アップグレード バンドルをダウンロードします。
- https://www.cisco.com/ から適切な ESXi オフライン アップグレード バンドルをダウンロードします。
- ストレージ コントローラ VM でスナップショット スケジュールを無効にします。HyperFlex クラスタ IP に SSH 接続し、`stcli snapshot-schedule -disable` snapshot schedule コマンドを実行します。

ステップ 1 HX Connect にログインします。

a) 管理者ユーザのユーザ名とパスワードを入力します。

b) **[Login]** をクリックします。

ステップ 2 ナビゲーション ペインで、**[Upgrade]** を選択します。

ステップ 3 **[アップグレードのタイプの選択（Select Upgrade Type）]** ページで **[HX Data Platform]**、 **[ESXi]** および **UCS サーバ ファームウェア（UCS Server Firmware）]** を選択し、次のフィールドの値を入力します。

フィールド	基本的な情報
UCS Manager の接続	
UCS Manager FQDN/IP	Cisco UCS Manager 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。
ユーザー名	Cisco UCS Manager <admin> username を入力します。
[管理パスワード（Admin Password）]	Cisco UCS Manager <admin> パスワードを入力します。
HX サーバ ファームウェア	
検出	**[[検出（Discover）]**をクリックして、現在の UCS ファームウェア パッケージ バージョンを表示します。
M3/M4 の望ましいバージョン/ M5/M6 の望ましいバージョン（クラスタ内のノードに依存）	適切な C シリーズ ファームウェア バージョンを選択します。 オプションで、クラスタにコンピューティングのみの B シリーズ UCS ブレードがある場合は、適切な B シリーズ ファームウェア バージョンを選択します。 UCS Manager にアップロードされた C & B バンドルのみがリストに表示されます。目的のバージョンが表示されていない場合は、UCS インフラストラクチャ ファームウェア ワークフローのアップグレード （19 ページ） に戻ります。 互換性のあるファームウェア バージョンのみがドロップダウン リストに表示されます。目的のバージョンが表示されない場合は、HX リリースノートで HXDP とサーバファームウェア間の互換性を確認します。

（注） UI のドロップダウンに目的の UCS サーバファームウェア バージョンが表示されない場合は、HX Connect UCS サーバ ファームウェア 選択ドロップダウンにファームウェア バージョン 4.1 以降がリストされていない （71 ページ） を参照してください。

ステップ 4 HyperFlex データ プラットフォーム アップグレード パッケージ（storfs-package）をアップロードします。

フィールド	基本的な情報
HX ファイルをここにドラッグするか、または [参照] をクリックします	[ソフトウェアのダウンロード - HyperFlex HX Data Platform] から取得した、以前の release.tgz パッケージ ファイルを使用している既存のクラスタをアップグレードするために、Cisco HyperFlex Data Platform アップグレード バンドルの最新版をアップロードします。 サンプル ファイル名の形式: `storfs-packages-4.5.1a-31601.tgz.`
現在のバージョン	現在の HyperFlex Data Platform バージョンが表示されます。
現在のクラスタの詳細	**HyperFlex バージョン**および **クラスタ アップグレード状態** のような HyperFlex クラスタの詳細がリストされます。
Bundle version	アップロードされたバンドルの HyperFlex Data Platform バージョンが表示されます。
（オプション）**[Checksum]**	MD5 チェックサム番号は、Cisco.com Software Download セクションのファイル名の上にカーソルを合わせてホバーさせることで確認できます。 このオプション ステップは、アップロードされたアップグレード パッケージ バンドルの整合性を検証するのに役立ちます。

ステップ 5 ESXi オフライン アップグレード バンドルをアップロードします。

ステップ 6 vCenter ログイン情報を指定します。

フィールド	基本的な情報
ユーザー名	vCenter <*admin*> ユーザー名を入力します。
[管理パスワード（Admin Password）]	vCenter <*admin*> パスワードを入力します。

ステップ 7 **[アップグレード]** をクリックして、複合アップグレード プロセスの最初のステップを開始します。

ステップ 8 **[アップグレードの進行状況（Upgrade Progress）]** ページの **[検証画面（Validation Screen）]** に、実行中の検査の進行状況が表示されます。検証エラーがある場合は修正します。

（注） この時点で、すべてのアップグレード前のチェックと検証が、最初のアップグレード段階とともに実行されます。数分以内に HX Connect が戻り、ユーザーにアップグレードの第 2 段階を確認して開始するように求めます。両方の手順が UI で実行されるまで、アップグレードは完了しません。システムは、アップグレードの最初のステップのみが完了した状態のままにしないでください。

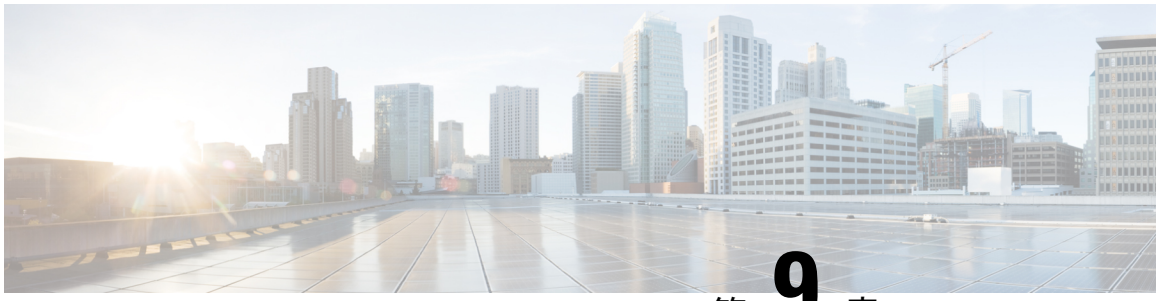
（注） UCS Manager でサーバを手動で確認応答しないでください。サーバが pending-ack 状態になる間、管理者が手動で介入することはできません。HyperFlex プラットフォームは、各サーバを正しい時間に自動的に確認応答します。

ステップ 9 HyperFlex Connect の UI は、アップグレードの最初のステップの後に更新され、UCS および vCenter のクレデンシャルを入力してアップグレードプロセスの第 2 段階を開始するように求めるバナーがポップアップ表示されます。アップグレード ページをモニタし、アップグレードが完了したことを確認します。

アップグレードが進行中の時に、「Websocket の接続が失敗しました」というメッセージが表示される場合があります。自動更新が無効になりました。エラー メッセージを消去するには、ページの表示を更新するか、ログアウトしてからログインし直します。このエラー メッセージは問題なく無視することができます。

次のタスク

アップグレードが完了したら、アップグレード後のタスクのアップグレードが完了したことの確認 （35 ページ） に進みます。アップグレードが失敗した場合は、アップグレードを再試行するか、Cisco TAC に連絡してサポートを受けてください。アップグレードの失敗後に修復なしでクラスタを実行することは推奨されません。アップグレードをできるだけ早く完全に完了するように、注意を払う必要があります。



第 9 章

UCS ファームウェア、HX Data Platform および VMware vSphere のアップグレード：個別コンポーネントのアップグレード

概要

シスコでは、HyperFlex Connect からのフルスタック アップグレードを組み合わせて、これら 3 つのコンポーネントをすべてアップグレードすることを推奨しています。一度に 1 つ、2 つ、または 3 つすべてのコンポーネントをアップグレードできます。単一のアップグレードプロセスで 2 つ以上のコンポーネントを組み合わせる場合は、前の章で説明した手順に従います。それ以外の場合は、個々のコンポーネントのアップグレード手順を 1 つずつ実行します。

Cisco HyperFlex Data Platform のアップグレード

始める前に

- 既存のクラスタを以前のリリースからアップグレードするための最新の *Cisco HX Data Platform* アップグレード バンドルを、ソフトウェアのダウンロード （17 ページ） からダウンロードします。
- ストレージ コントローラ VM でスナップショット スケジュールを無効にします。HyperFlex クラスタ IP に SSH 接続し、**stcli snapshot-schedule -disable** snapshot schedule コマンドを実行します。

ステップ 1 HX Data Platform インストーラにログインします。

a) 管理者ユーザのユーザ名とパスワードを入力します。

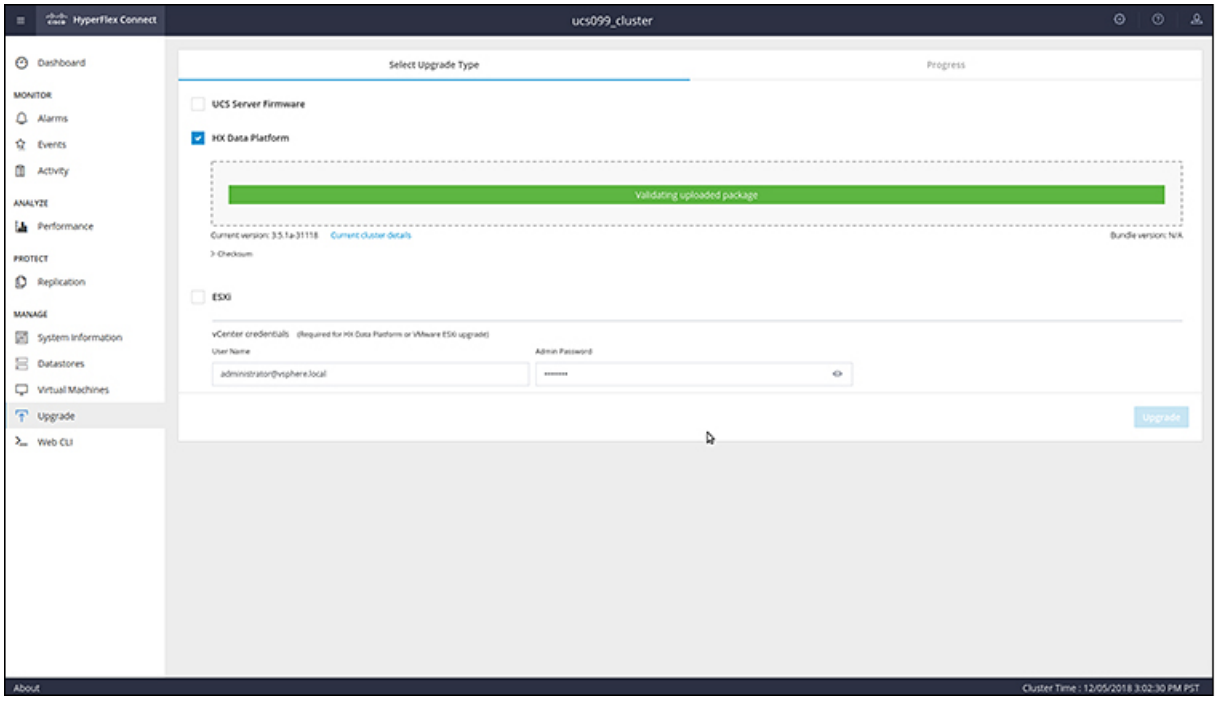
b) **[Login]** をクリックします。

ステップ 2 ナビゲーション ペインで、**[Upgrade]** を選択します。

ステップ 3 **[Select Upgrade Type]** ページで **[HX Data Platform]** を選択し、次のフィールドの値を入力します。

UI 要素	基本的な情報
HX ファイルをここにドラッグするか、または [参照] をクリックします	以前の *release.tgz* を使用する既存のクラスタをアップグレードするための *Cisco HyperFlex Data Platform* アップグレード バンドルの最新パッケージ ファイルを、「ソフトウェアのダウンロード - HyperFlex HX Data Platform」からアップロードします。 サンプル ファイル名の形式: *storfs-packages-4.5.1a-31601.tgz*.
（オプション）**[チェックサム（Checksum）]** フィールド	*MD5* チェックサム番号は、[Cisco ソフトウェア ダウンロード（Cisco Software Download）] セクションのファイル名にカーソルを合わせてホバーさせると表示されます。 このオプション ステップは、アップロードされたアップグレード パッケージ バンドルの整合性を検証するのに役立ちます。

図 *1 : [Select Upgrade Type]* ページ



ステップ 4 **vCenter クレデンシャル** を入力します。

UI 要素	基本的な情報
[ユーザ名（User Name）] フィールド	vCenter <管理者> ユーザ名を入力します。
[Admin Password] フィールド	vCenter <*admin*> パスワードを入力します。

ステップ 5 **[Upgrade]** をクリックして、クラスタ アップグレード プロセスを開始します。

ステップ 6 **[アップグレードの進行状況（Upgrade Progress）]** ページの [Validation Screen] に、実行中の検査の進行状況が表示されます。検証エラーがある場合は修正します。

（注） この時点で、アップグレード前のすべてのチェックと検証が、最初のアップグレード段階とともに実行されます。数分以内に HX Connect が返され、アップグレードの確認と開始を求めるプロンプトが表示されます。両方の手順が UI で実行されるまで、アップグレードは完了しません。システムは、アップグレードの最初のステップのみが完了した状態のままにしないでください。

ステップ 7 HyperFlex Connect の UI は、アップグレードの最初のステップの後に更新され、UCS および vCenter のクレデンシャルを入力してアップグレードプロセスの第 2 段階を開始するように求めるバナーがポップアップ表示されます。アップグレード ページをモニタし、アップグレードが完了したことを確認します。

アップグレードが進行中の時に、**「Websocket の接続が失敗しました」というメッセージが表示される場合があります。自動更新が無効になりました。**エラー メッセージを消去するには、ページの表示を更新するか、ログアウトしてからログインし直します。このエラー メッセージは問題なく無視することができます。

次のタスク

アップグレードが完了したら、アップグレード後のタスクのアップグレードが完了したことの確認 （35 ページ） に進みます。アップグレードが失敗した場合は、アップグレードを再試行するか、Cisco TAC に連絡してサポートを受けてください。

（注） アップグレードの失敗後に修復なしでクラスタを実行することは推奨されません。アップグレードをできるだけ早く完全に完了するように、注意を払う必要があります。

Cisco UCS Server Firmware のアップグレード

始める前に

- UCS B シリーズおよび C シリーズ サーバのファームウェア パッケージがファブリック インターコネクトにダウンロードされていることを確認します。

- ストレージコントローラ VM でスナップショット スケジュールを無効にします。HyperFlex クラスタ IP に SSH 接続し、`stcli snapshot-schedule -disable` snapshot schedule コマンドを実行します。

ステップ 1 HX Connect にログインします。

a) 管理者ユーザのユーザ名とパスワードを入力します。

b) **[Login]** をクリックします。

ステップ 2 ナビゲーション ペインで、**[Upgrade]** を選択します。

ステップ 3 **[アップグレードのタイプの選択（Select Upgrade Type）]** ページで **[UCS サーバ ファームウェア（UCS Server Firmware）]** を選択し、次のフィールドの値を入力します。

フィールド	基本的な情報
UCS Manager の接続	
UCS Manager FQDN/IP	Cisco UCS Manager 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。
ユーザー名	Cisco UCS Manager <admin> username を入力します。
[管理パスワード（Admin Password）]	Cisco UCS Manager <admin> パスワードを入力します。
HX サーバ ファームウェア	
検出	**[[検出（Discover）]** をクリックして、現在の UCS ファームウェア パッケージ バージョンを表示します。
M3/M4 の望ましいバージョン/ M5/M6 の望ましいバージョン（クラスタ内のノードに依存）	適切な C シリーズ ファームウェア バージョンを選択します。 オプションで、クラスタにコンピューティングのみの B シリーズ UCS ブレードがある場合は、適切な B シリーズ ファームウェア バージョンを選択します。 UCS Manager にアップロードされた C & B バンドルのみがリストに表示されます。目的のバージョンが表示されていない場合は、UCS インフラストラクチャ ファームウェア ワークフローのアップグレード （19 ページ） に戻ります。 互換性のあるファームウェア バージョンのみがドロップダウン リストに表示されます。目的のバージョンが表示されない場合は、HX リリースノートで HXDP とサーバファームウェア間の互換性を確認します。

ステップ 4 **[Upgrade]** をクリックして UCS ファームウェアのアップグレード プロセスを開始します。

ステップ 5 **[アップグレードの進行状況（Upgrade Progress）]** ページの **[検証画面（Validation Screen）]** に、実行中の検査の進行状況が表示されます。検証エラーがある場合は修正します。アップグレード ページをモニタし、アップグレードが完了したことを確認します。

アップグレードが進行中の時に、「Websocket の接続が失敗しました」というメッセージが表示される場合があります。自動更新が無効になりました。エラー メッセージを消去するには、ページの表示を更新するか、ログアウトしてからログインし直します。このエラー メッセージは問題なく無視することができます。

（注） UCS Manager でサーバを手動で確認応答しないでください。サーバが pending-ack 状態になる間は、管理者が手動で介入することはできません。HyperFlex プラットフォームは、各サーバを正しい時間に自動的に確認応答します。

VMware vSphere/ESXi のアップグレード

次の手順に従って、HyperFlex Connect から VMware ESXi のみをアップグレードします。この手順は、ESXi パッチのアップグレードにも適用できます。

アップグレードでは、次のタスクをこの順序で実行する必要があります。

- HXDP、UC、および VMware のソフトウェアの互換性については、リリースノートを参照し、アップグレードする前に vCenter がアップグレードされていることを確認してください。詳細については、、 Cisco HX Data Platform、リリース 5.0 のリリース ノート、Cisco HyperFlex 推奨ソフトウェア リリースおよび要件ガイド、および VMware 製品相互運用性マトリクスを参照してください。
- 管理者権限を使用して HX Connect にログインし、[アップグレード（Upgrade）] ページに移動します。

始める前に

適切な ESXi オフライン アップグレード バンドルをダウンロードします。詳細については、ソフトウェアのダウンロード （17 ページ）を参照してください。シスコでは、非 HX カスタマイズ ESXi バンドルの使用は推奨していませんが、サポートされています。HX カスタマイズ バンドルを使用すると、すべての最新ドライバが更新され、HyperFlex ハードウェアとの互換性が確保されます。

ステップ 1 管理者権限で HX Connect にログインします。

ステップ 2 [システム情報（System Information）] タブに移動し、実行中のハイパーバイザのバージョンを確認します。

ステップ 3 [アップグレード（Upgrade）] タブをクリックし、**[ESXi]** を選択します。

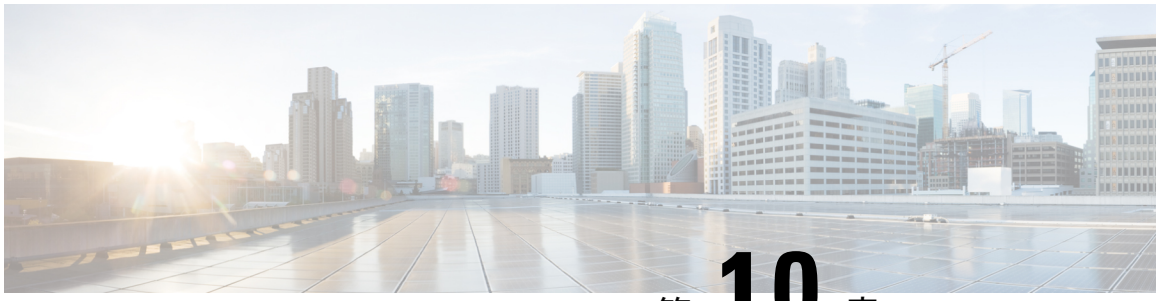
ステップ 4 バンドル バージョン ウィンドウ内をクリックし、以前に保存した ESXi オフライン バンドルに移動して、**[開く（Open）]** をクリックします。

ステップ 5 バンドルがアップロードされたら、vCenter クレデンシャルを入力し、**[アップグレード（Upgrade）]** をクリックします。

（注） アップグレード プロセスは中断せず、一度に 1 台のサーバをアップグレードします。

ステップ 6 ブラウザ画面を更新して、[ダッシュボード（Dashboard）] タブにアップグレードの変更を表示します。

（注） [システム情報（System Information）] タブをクリックして、すべてのノードがオンラインであることを確認します。



第 10 章

アップグレード後の作業

アップグレードが完了したことの確認

ステップ 1 Cisco UCS Manager にログインして、保留中のサーバ アクティビティが HX ノードに存在しないことを確認します。

[サーバ（Servers）] タブ > 、[サーバ（Servers）] > [保留中のアクティビティ（Pending Activities）] タブで、すべてのサーバ アクティビティを確認してください。

ステップ 2 HX ノードが、期待されるファームウェア バージョンに一致することを確認します。

Cisco UCS Manager で、**[機器（Equipment）] > [ファームウェア管理（Firmware Management）] > [インストールされたファームウェア（Installed Firmware）]** タブを選択し、正しいファームウェア バージョンであることを確認します。

ステップ 3 SSH を介していずれかのコントローラ VM にログインします。

```
# ssh admin@controller_vm_ip
```

ステップ 4 HyperFlex Data Platform バージョンを確認します。

```
# stcli cluster version


Cluster version: 4.5(1a)
Node hx220-m5-node1 version: 4.5(1a)
Node hx220-m5-node3 version: 4.5(1a)
Node hx220-m5-node3 version: 4.5(1a)
Node hx220-m5-node4 version: 4.5(1a)
```

ステップ 5 HX ストレージ クラスタがオンラインであり、正常な状態であることを確認します。

```
# stcli cluster info|grep -i health
```

```
Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

ステップ 6 アップグレードが完了し、成功したことを確認します。

```
stcli cluster upgrade-status
```

```
Nodes up to date:
[HX-Cluster, HX-Node-1(1.1.1.1), HX-Node-2(1.1.1.2), HX-Node-3(1.1.1.3)]
Cluster upgrade succeeded.
```

ステップ 7 使用するブラウザ インターフェイスごとに、キャッシュを空にしてブラウザ ページをリロードし、HX Connect のコンテンツを更新します。

クリーナが実行中であるかどうかの確認

アップグレードが失敗した場合

アップグレードが失敗した場合は、クリーナを実行します。たとえアップグレードを続行しない場合でも、この作業は必須です。

クリーナを手動で実行するには、次のコマンドを使用してストレージ クラスタ クリーナを再起動します。

stcli cleaner start [-h] [--id ID | --ip NAME]

構文の説明

Option	必須またはオプション	説明
--id ID	オプション。	ストレージ クラスタ ノードの ID。ID は、`stcli cluster info` コマンドでリストされます。
--ip NAME	オプション。	ストレージクラスタ ノードの IP アドレス。IP は、`stcli cluster info` コマンドでリストされます。

アップグレードが完了した場合

アップグレードが完了した場合は、クリーナが実行中であるかどうかを確認します。指定のノードのストレージ クラスタ クリーナに関する情報を取得するには、次のコマンドを使用します。

stcli cleaner info [-h] [--id ID | --ip NAME]

構文の説明

Option	必須またはオプション	説明
--id ID	オプション。	ストレージ クラスタ ノードの ID。ID は、`stcli cluster info` コマンドでリストされます。
--ip NAME	オプション。	ストレージクラスタ ノードの IP アドレス。IP は、`stcli cluster info` コマンドでリストされます。

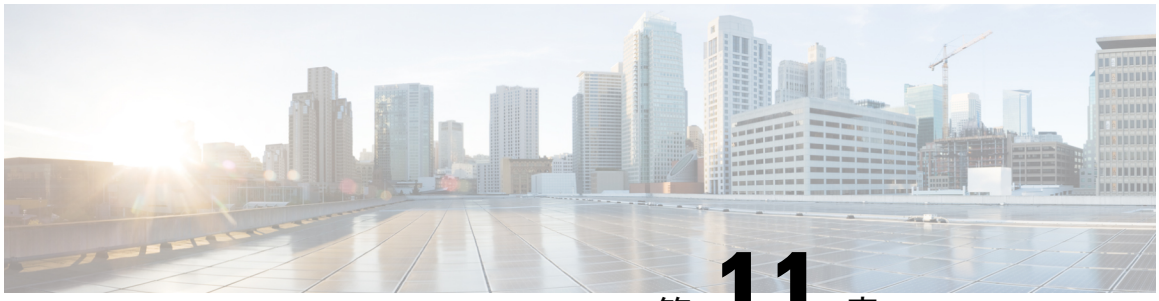
スナップショットスケジューラを有効にする（オプション）

アップグレードを開始する前にスナップショットスケジューラを無効にしていた場合は、ここでスケジュールを有効にします。HyperFlex クラスタ IP に SSH で接続し、コマンド *stcli snapshot-schedule –enable* snapshot schedule を実行します。

HyperFlex ソフトウェア暗号化を有効にする

HyperFlex ソフトウェア暗号化は、保存データのファイル レベルのエンドツーエンド AES 256 ビット暗号化を提供します。HyperFlex ソフトウェア暗号化の機能を活用して、ドライブ、サーバー、またはクラスタ全体などのデバイスの窃盗からデータの機密性を保護できます。暗号化キーは、Intersight SaaS と Intersight 仮想アプライアンスの両方で利用可能な Intersight Key Manager によって安全にリモートに保存されます。

クラスタで HyperFlex ソフトウェア暗号化を有効にするには、HX Data Platform および Intersight のライセンス要件を満たしていることを確認してください。『Cisco HyperFlex Systems 注文およびライセンシング ガイド』を参照してください。https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/b_Cisco_HyperFlex_Systems_Ordering_and_Licensing_Guide.htmlライセンス要件が満たされていることを確認した後、HyperFlex ソフトウェア暗号化を有効にするには、My Cisco Entitlement から暗号化パッケージをダウンロードし、パッケージをインストールしてから、Intersight からの暗号化を有効にする必要があります。詳細については、HyperFlex ソフトウェア暗号化を参照してください。



第 11 章

HyperFlex Edge アップグレード

概要

このセクションでは、HX Connect からの Cisco HyperFlex Edge システムのアップグレードに関連する情報を提供します。クラスタが Cisco Intersight を使用して展開されている場合は、Intersight を使用してクラスタのアップグレードを実行してください。Intersight を使用した Edge クラスタのアップグレードに関する詳細なアップグレードの前提条件と手順については。

重要

- HyperFlex Edge システムのアップグレードには、サーバ ファームウェア、HyperFlex Data Platform ソフトウェア、および VMware ESXi のアップグレードが含まれます。
- HyperFlex Connect を使用して、HyperFlex Data Platform と VMware ESXI の複合アップグレードを実行することも、分割アップグレードを実行することもできます。
- UCS サーバ ファームウェアのアップグレードは、HX Connect からはサポートされていません。代わりに、Host Upgrade Utility（HUU）ツールまたは統合管理コントローラ（IMC）スーパバイザを使用して個別にファームウェアのアップグレードを実行します。

Cisco HyperFlex Edge ファームウェア推奨バージョン

- 『Cisco HyperFlex Release Notes Release Notes for Cisco HX Data Platform、Release 4.5』、および『推奨 Cisco HyperFlex HX-Series Systems 向け Cisco HyperFlex HX Data Platform ソフトウェア リリース』の「Cisco HyperFlex アップグレード ガイドライン」を確認します。
- アップグレードがサポートされているリリースについては、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。
- サポートされなくなったリリースからアップグレードする場合は、『Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases』を参照してください。
- HX Connect を使用してアップグレードされた HyperFlex Edge クラスタの場合、HyperFlex Data Platform のアップグレードには、HyperFlex Data Platform ソフトウェアに加えて、組み込みストレージファームウェアのアップグレードが含まれます。この組み込みファームウェア アップグレードには、分散ストレージ プラットフォームを実行する SAS パススルー ストレージコントローラおよび関連するドライブ（ハウスキーピング、キャッシュ、およびキャパシティ）への更新が含まれます。これらのコンポーネントの手動アップグレードは実行しないでください。HX Connect を使用してサーバーファームウェアのアップグレードを完了することをお勧めします。これらのストレージ コンポーネントを手動でアップグレードまたはダウングレードする必要がある場合は、次のことを確認してください。
  - ホスト アップデート ユーティリティ（HUU）を使用してシャーシ ファームウェアをアップグレードする場合は、SAS コントローラをアップグレードするオプションのチェックを外し、ドライブをアップグレードしないでください（必要に応じて、ブート ドライブを除きます）。
  - デフォルトでストレージコントローラが含まれるため、HUU の [すべてアップグレード（Upgrade All）] ボタンの使用は避けてください。
  - これらのデバイスのファームウェア管理は、HyperFlex Data Platform によって自動的に処理されるため、他のユーティリティを使用して手動で変更しないでください。HUU を使用してこれらのコンポーネントをアップグレードするのは、トラブルシューティングに必要と判断される場合、または Cisco TAC の指示に従う場合に限定されます。
  - バージョン 4.1(3b) より前の Cisco IMC バージョンを実行しているクラスタの場合、サーバーファームウェアのアップグレードを実行するには、セキュアブートを一時的に無効にする必要があります。Cisco IMC バージョン 4.1(3b) のバージョン以降でクラスタ内のすべてのノードで実行されている場合は、ファームウェア アップグレードのためにセキュアブートを有効にすることができます。

Cisco Host Upgrade Utility ツールを使用したサーバ ファームウェアのアップグレード

次の表で、Cisco HX サーバのサーバ ファームウェア アップグレードのワークフローの概要を説明します。

ステップ	説明	参考資料
1.	ノードを HX メンテナンス モードにします。 （注） アップグレード中にクラスタをオンラインのままにするには、ノードを一度に 1 つずつアップグレードします。	Cisco HyperFrex のメンテナンス モードの開始
2.	Host Upgrade Utility ツールを使用してサーバ ファームウェアをアップグレードします。	『Cisco Host Upgrade Utility User Guide』の「Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU」を参照してください。
3.	ノードを再起動して再びESXiにします。HX メンテナンス モードを終了します。	
4.	クラスタが完全に正常な状態になるまで待機します。	HyperFlex クラスタのヘルスの表示 （13 ページ）
5.	ローリング方式で、残りの HX ノードに対して手順 1 ～ 4 を繰り返します。 （注） クラスタ内の次のホストをメンテナンス モードにする前に、正常な状態かどうかを確認します。	

『*Cisco Host Upgrade Utility User Guide*』の最新のリリースと過去のリリースは https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.htmlにあります。

Cisco Integrated Management Controller Supervisor を使用したサーバ ファームウェアのアップグレード

次の表で、Cisco HX サーバのサーバ ファームウェア アップグレードのワークフローの概要を説明します。

ステップ	説明	参考資料
1.	ノードを HX メンテナンス モードにします。 （注） アップグレード中にクラスタをオンラインのままにするには、ノードを一度に 1 つずつアップグレードします。	
2.	ラック グループを作成します。IMC Supervisor インベントリにサーバを追加します。	『*Cisco IMC Supervisor* ラック マウントサーバ管理ガイド』の「サーバ検出、ラック グループ、およびラック アカウントの管理」を参照してください。
3.	自動検出プロファイルを設定します。	『*Cisco IMC Supervisor* ラック マウント サーバ管理ガイド』の「自動検出プロファイルの設定」を参照してください。
4.	ラック グループでインベントリを実行します。	『*Cisco IMC Supervisor* ラック マウントサーバ管理ガイド』の「ラック アカウントまたはラック グループのインベントリの収集」を参照してください。

ステップ	説明	参考資料
5.	ファームウェア プロファイルを作成します。	『*Cisco IMC Supervisor* ラックマウントサーバ管理ガイド』で、次のタスクを参照してください。 • ローカル サーバへのイメージの追加 • ローカル ファイル システムからのイメージのアップロード • ネットワーク サーバからのイメージの追加
6.	メンテナンス モードになっているノードで IMC Supervisor を使用してファームウェアをアップグレードします。	『*Cisco IMC Supervisor* ラックマウントサーバ管理ガイド』の「ファームウェアのアップグレード」を参照してください。
7.	ノードを再起動して再びESXiにします。HX メンテナンス モードを終了します。	
8.	クラスタが完全に正常な状態になるまで待機します。	
9.	ローリング方式で、残りのHXノードに対して手順 6 を繰り返します。 （注） クラスタ内の次のホストをメンテナンス モードにする前に、正常な状態かどうかを確認します。	

https://www.cisco.com/c/en/us/support/servers-unified-computing/integrated-management-controller-imc-supervisor/products-installation-and-configuration-guides-list.html で、『*Cisco IMC Supervisor* ラック マウント サーバ管理ガイド』の最新リリースと過去のリリースを確認できます:。

Cisco IMC Supervisor を使用した Cisco UCS C シリーズ サーバのファームウェアの更新

Cisco IMC バージョン 2.0(x) にアップグレードする場合、デフォルトの Cisco IMC パスワードを変更する必要があります。

（注） Cisco IMC Supervisor をアップグレードする前に、ファームウェア プロファイルがすでに設定されている場合は、Cisco.com クレデンシャルとプロキシの詳細が設定されていることを確認してください。

ステップ 1 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Firmware Upgrades (ファームウェア アップグレード)]** をクリックします。

ステップ 3 [アップグレードの実行（Run Upgrade）] をクリックします。警告メッセージが表示され、選択したサーバのアップグレードを実行すると、ホストがリブートしてファームウェア更新ツールが起動することが通知されます。ファームウェアのアップデートが完了すると、サーバはホスト OS を再起動します。

ステップ 4 **[OK]** をクリックして確定します。

ステップ 5 **[Upgrade Firmware (ファームウェア アップグレード)]** 画面で、次のフィールドに入力します。

フィールド	説明
[プロファイルの選択（Select Profile）] ドロップダウンリスト	ドロップダウン リストからプロファイルを選択します。
[Platform] フィールド	[Select] をクリックして、リストからサーバを選択します。選択したプロファイルで設定されているプラットフォームに一致するサーバだけがリストに表示されます
[Image Version (イメージ バージョン)] フィールド	
[Image Path (イメージ パス)] フィールド	
[後でスケジュール（Schedule later）] チェックボックス	このチェックボックスをオンにして、アップグレードを実行する既存のスケジュールを選択します。[+]アイコンをクリックして新しいスケジュールを作成することもできます。

ステップ 6 [Submit] をクリックします。

HX Connect を使用した HyperFlex Edge のアップグレード

Cisco HyperFlex Edge クラスタのアップグレード プロセスでは、次の 3 つのコンポーネントがアップグレードされます。

- Cisco HyperFlex データ プラットフォーム
- VMware vSphere ESXi
- Cisco UCS スタンドアロン サーバ ファームウェア

HyperFlex Data Platform と VMware ESXi のアップグレードを組み合わせて、HyperFlex Edge クラスタの単一のアップグレードにすることができます。シスコでは、HyperFlex Connect からのこれら 2 つのコンポーネントを組み合わせてアップグレードすることを推奨しています。一度に 1 つまたは 2 つのコンポーネントをアップグレードすることを選択できます。

個々のコンポーネントを 1 つずつアップグレードする場合は、VMware vSphere/ESXi のアップグレード （33 ページ） を参照してください。標準クラスタと HyperFlex Edge クラスタのコンポーネント アップグレード プロセスは同じです。

このセクションでは、HyperFlex データ プラットフォームと VMware vSphere ESXi の複合アップグレードを実行する手順について説明します。このプロセスでは、HyperFlex ノードは、VMware vMotion を使用してワークロードを中断することなく、最適化されたローリング リブートを実行します。

（注） Intersight 経由で展開された HyperFlex Edge クラスタは、Hyperflex Connect から機能をアップグレードしません。アップグレードは、Intersight でのみサポートされています。

ステップ 1 HX Connect にログインします。

a) 管理者ユーザのユーザ名とパスワードを入力します。

b) **[Login]** をクリックします。

ステップ 2 ナビゲーション ペインで、**[Upgrade]** を選択します。

ステップ 3 **[アップグレード タイプの選択（Select Upgrade Type）]** ページで **[HX Data Platform]** および **[ESXi]** を選択し、次のフィールドの値を入力します。

ステップ 4 HyperFlex データ プラットフォーム アップグレード パッケージ（storfs-package）をアップロードします。

表 *1 : Cisco HX* データプラットフォーム

UI 要素	基本的な情報
HX ファイルをここにドラッグするか、または [参照] をクリックします	「Download Software ： HyperFlex HX Data Platform」から、前の release.tgz パッケージを使用した既存のクラスタをアップグレードするための Cisco HyperFlex Data Platform アップグレード バンドルをアップロードします。 サンプル ファイル名の形式: storfs-packages-4.5.1a-31601.tgz
現在のバージョン	現在の HyperFlex Data Platform バージョンが表示されます。
現在のクラスタの詳細	**[HyperFlex リリース（HyperFlex release）]**および **[クラスタ アップグレード状態（cluster upgrade state）]** のような HyperFlex クラスタの詳細がリストされます。
Bundle version	アップロードされたバンドルの HyperFlex Data Platform バージョンが表示されます。
（任意）**[チェックサム（Checksum）]** フィールド	MD5 チェックサム番号は、Cisco.com のソフトウェア ダウンロードセクションのファイル名にカーソルを合わせてホバーさせると表示されます。 このオプション ステップは、アップロードされたアップグレード パッケージ バンドルの整合性を検証するのに役立ちます。

ステップ 5 VMware ESXi カスタム イメージのオフライン アップグレード バンドルをアップロードします。

ステップ 6 vCenter ログイン情報を指定します。

基本情報（Essential Information）	基本的な情報
[ユーザ名（User Name）] フィールド	vCenter <admin> ユーザ名を入力します。
[Admin Password] フィールド	vCenter <admin> パスワードを入力します。

ステップ 7 **[アップグレード（Upgrade）]** をクリックして、複合アップグレード プロセスを開始します。

ステップ 8 **[アップグレードの進行状況（Upgrade Progress）]** ページの [Validation Screen] に、実行中の検査の進行状況が表示されます。検証エラーがある場合は修正します。

（注） この時点で、すべてのアップグレード前のチェックと検証が、最初のアップグレード段階とともに実行されます。数分以内に HX Connect が返され、アップグレードの確認と開始を求めるプロンプトが表示されます。両方の手順が UI で実行されるまで、アップグレードは完了しません。システムは、アップグレードの最初のステップのみが完了した状態のままにしないでください。

ステップ 9 HyperFlex Connect の UI は、アップグレードの最初のステップの後に更新され、UCS および vCenter のクレデンシャルを入力してアップグレードプロセスの第 2 段階を開始するように求めるバナーがポップアップ表示されます。アップグレード ページをモニタし、アップグレードが完了したことを確認します。

アップグレードが進行中の時に、**「Websocket の接続が失敗しました」というメッセージが表示される場合があります。自動更新が無効になりました。**エラー メッセージを消去するには、ページの表示を更新するか、ログアウトしてからログインし直します。このエラー メッセージは問題なく無視することができます。

（注） アップグレードが完了したら、アップグレード後のタスクのアップグレードが完了したことの確認 （35 ページ） に進みます。アップグレードが失敗した場合は、アップグレードを再試行するか、Cisco TAC に連絡してサポートを受けてください。

HyperFlex Edge のアップグレード後の作業

アップグレードが完了して HyperFlex Edge クラスタがアップグレードされた後、HX Connect からログアウトして再びログインし、アップグレードによる変更を確認します。

ステップ 1 HX ノードが、期待されるファームウェア バージョンに一致することを確認します。

IMC Supervisor GUI または Cisco IMC UI でファームウェア バージョンをチェックして、正しいファームウェア バージョンであることを確認します。

ファームウェアバージョンを表示するには、IMC Supervisor GUI で、**[システム（Systems）] > [ファームウェア管理（Firmware Management）]** タブに移動します。詳細については、『Upgrading Firmware using IMC Supervisor』を参照してください。

ステップ 2 SSH を介していずれかのコントローラ VM にログインします。

```
# ssh root@controller_vm_ip
```

ステップ 3 HyperFlex Data Platform バージョンを確認します。

```
# stcli cluster version


Cluster version: 2.5(1c)
Node HX02 version: 2.5(1c)
Node HX01 version: 2.5(1c)
Node HX03 version: 2.5(1c)
```

ステップ 4 HX ストレージ クラスタがオンラインであり、正常な状態であることを確認します。

```
# stcli cluster info|grep -i health
```

```
Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

ステップ 5 データストアが稼働中であり、ESXi ホストに適切にマウントされていることを確認します。

HX コントローラ VM から、次のコマンドを実行します。

```
# stcli datastore list
```

ESXi ホストから次のコマンドを実行します。

```
# esxcfg-nas -l
```

ステップ 6 使用するブラウザ インターフェイスごとに、キャッシュを空にしてブラウザ ページをリロードし、HX Connect のコンテンツを更新します。

第 12 章

ストレッチ クラスタ アップグレード

概要

このセクションでは、Cisco HyperFlex ストレッチ クラスタのアップグレードに関連する情報を示します。ストレッチ クラスタのアップグレードを実行する手順は、通常の HyperFlex クラスタのアップグレード手順と似ています。

Cisco HyperFlex ストレッチ クラスタのアップグレード プロセスでは、次の 3 つのコンポーネントがアップグレードされます。

- Cisco HyperFlex データ プラットフォーム
- VMware vSphere ESXi
- Cisco UCS サーバ ファームウェア

HyperFlex データ プラットフォームと VMware ESXi のアップグレードを組み合わせて、HyperFlex ストレッチ クラスタの単一のアップグレードにすることができます。シスコでは、HyperFlex Connect からのこれら 2 つのコンポーネントを組み合わせてアップグレードすることを推奨しています。一度に 1 つまたは 2 つのコンポーネントをアップグレードすることを選択できます。

個別のコンポーネントを 1 つずつアップグレードする場合は、「HX Connect を使用した Cisco HyperFlex Data Platform または Cisco UCS サーバ ファームウェアまたは VMware ESXi のアップグレード：個別コンポーネント」を参照してください。標準クラスタと HyperFlex Edge クラスタのコンポーネント アップグレード プロセスは同じです。

このセクションでは、HyperFlex データ プラットフォームと VMware vSphere ESXi の複合アップグレードを実行する手順について説明します。このプロセスでは、HyperFlex ノードは、VMware vMotion を使用してワークロードを中断することなく、最適化されたローリング リブートを実行します。

ストレッチ クラスタのアップグレードのガイドライン

- UCS ファームウェアのアップグレードは、HX Connect を通じてサポートされていません。UCS ファームウェアのアップグレードは、Cisco UCS Managerを使用して手動で行う必要があります。Cisco UCS Manager によるファームウェアの管理を参照してください。
- HyperFlex Witness ノードのアップグレードは、ストレッチ クラスタをアップグレードするときには必要ありませんが、強く推奨されます。使用可能な最新の Witness バージョンについては、HyperFlex Data Platform リリースノートを参照してください。
- 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。詳細については、Hypercheck: アップグレード前チェック ツール （9 ページ）を参照してください。

HX Connect を使用した HyperFlex ストレッチ クラスタのアップグレード

始める前に

- アップグレード前の検証チェックを完了します。
- 既存のクラスタを以前のリリースからアップグレードするための最新の *Cisco HX Data Platform Upgrade Bundle* を [Software Download] から、ダウンロードします。
- Cisco UCS インフラストラクチャをアップグレードします。
- ストレージコントローラ VM でスナップショット スケジュールを無効にします。HyperFlex クラスタ IP に SSH 接続し、**stcli snapshot-schedule –disable** snapshot schedule コマンドを実行します。
- DRS が有効な場合、VM は自動的に vMotion を持つ他のホストに移行されます。

（注） DRS が 無効 に設定されている場合は、VM に対して手動で vMotion を実行して、アップグレード プロセスを続行します。詳細については、VMware のマニュアルで、vMotion を使用した移行の説明を参照してください。

ステップ 1 HX Connect にログインします。

a) 管理者ユーザのユーザ名とパスワードを入力します。

b) **[Login]** をクリックします。

ステップ 2 ナビゲーション ペインで、**[Upgrade]** を選択します。

ステップ 3 **[アップグレード タイプの選択（Select Upgrade Type）]** ページで **[HX Data Platform]** および **[ESXi]** を選択し、次のフィールドの値を入力します。

ステップ 4 **[Select Upgrade Type]** ページで **[HX Data Platform]** を選択し、次のフィールドの値を入力します。

UI 要素	[基本情報（Essential Information）]
HX ファイルをここにドラッグするか、または [参照] をクリックします	「Download Software ： HyperFlex HX Data Platform」から、前の release.tgz パッケージを使用した既存のクラスタをアップグレードするための Cisco HyperFlex Data Platform アップグレード バンドルをアップロードします。 サンプル ファイル名の形式: storfs-packages-4.5.1a-31601.tgz
現在のバージョン	現在の HyperFlex Data Platform バージョンが表示されます。
現在のクラスタの詳細	**HyperFlex バージョン**および **クラスタ アップグレード状態** のような HyperFlex クラスタの詳細がリストされます。
Bundle version	アップロードされたバンドルの HyperFlex Data Platform バージョンが表示されます。
（任意）**[チェックサム（Checksum）]** フィールド	MD5 チェックサム番号は、Cisco.com のソフトウェア ダウンロードセクションのファイル名にカーソルを合わせてホバーさせると表示されます。 このオプション ステップは、アップロードされたアップグレード パッケージ バンドルの整合性を検証するのに役立ちます。

ステップ 5 VMware ESXi カスタム イメージのオフライン アップグレード バンドルをアップロードします。

ステップ 6 vCenter ログイン情報を指定します。

基本情報（Essential Information）	基本的な情報
[ユーザ名（User Name）] フィールド	vCenter <admin> ユーザ名を入力します。
[Admin Password] フィールド	vCenter <admin> パスワードを入力します。

ステップ 7 **[アップグレード（Upgrade）]** をクリックして、複合アップグレード プロセスを開始します。

ステップ 8 **[アップグレードの進行状況（Upgrade Progress）]** ページの [Validation Screen] に、実行中の検査の進行状況が表示されます。検証エラーがある場合は修正します。

（注） この時点で、すべてのアップグレード前のチェックと検証が、最初のアップグレード段階とともに実行されます。数分以内にHX Connectが返され、アップグレードの確認と開始を求めるプロンプトが表示されます。両方の手順がUIで実行されるまで、アップグレードは完了しません。システムは、アップグレードの最初のステップのみが完了した状態のままにしないでください。

（注） UCS Manager でサーバを手動で確認応答しないでください。サーバが pending-ack 状態になる間は、管理者が手動で介入することはできません。HyperFlex プラットフォームは、各サーバを正しい時刻に自動的に認識します。

ステップ 9 HyperFlex Connect の UI は、アップグレードの最初のステップの後に更新され、UCS および vCenter のクレデンシャルを入力してアップグレードプロセスの第 2 段階を開始するように求めるバナーがポップアップ表示されます。アップグレード ページをモニタし、アップグレードが完了したことを確認します。

アップグレードが進行中の時に、**「Websocket の接続が失敗しました」というメッセージが表示される場合があります。自動更新が無効になりました。**エラー メッセージを消去するには、ページの表示を更新するか、ログアウトしてからログインし直します。このエラー メッセージは問題なく無視することができます。

（注） アップグレードが完了したら、アップグレード後のタスクを実行します。アップグレードが失敗した場合は、アップグレードを再試行するか、Cisco TAC に連絡してサポートを受けてください。

監視 VM のアップグレード

始める前に

- アップグレードする HXDP バージョンをサポートする Witness VM バージョンを選択します。サポートされているバージョンについては、*HX Data Platform Software Versions for HyperFlex Witness Node for Stretched Cluster* の HX Data Platform Software Versions for HyperFlex Witness Node for Stretched Cluster セクションを参照してください。
- HyperFlex ストレッチ クラスタのアップグレード
- アップグレードされた HyperFlex ストレッチ クラスタは正常な状態である必要があります。アップグレード後にストレッチ クラスタのヘルス状態を確認するには、次のコマンドを実行します。

```
root@StCtlVM:~# stcli cluster info | grep healthy
```

ステップ 1 SSH を使用して監視 VM にログインし、次のコマンドを実行してサービス exhibitor を停止します。

```
root@WitnessVM:~# service exhibitor stop
```

ステップ 2 `/Usr/share/exhibitor/` パスで使用可能な `exhibitor` ファイルを、 `exhibitor.properties` ファイルを取得できるリモート マシンにコピーします。

```
scp root@<Witness-VM-IP>:/usr/share/exhibitor/exhibitor.properties
user@<Remote-Machine>:/directory/exhibitor.properties
```

ステップ 3 監視 VM からログアウトします。電源をオフにして、監視 VM の名前を WitnessVM に変更します。

（注） Ping を使用して、古い監視 VM の IP アドレスが到達不能であることを確認します。

ステップ 4 新しい監視 VM を展開し、古い監視 VM と同じ IP アドレスを設定します。

（注） IP アドレスに到達できない場合、監視 OVA の導入には `/var/run/network` ディレクトリ内の古いエントリが含まれている可能性があります。これらのエントリを手動で削除し、VM を再起動して、割り当てられた IP アドレスがネットワーク上で到達可能になるようにする必要があります。

VM をリブートするには、vCenter/vSphere で VM コンソールを開き、次のコマンドを実行します。

```
rm -rf /var/run/network/*
reboot
```

ステップ 5 SSH を使用して新しい監視 VM にログインし、次のコマンドを実行してサービス exhibitor を停止します。

```
root@WitnessVM:~# service exhibitor stop
```

ステップ 6 `Exhibitor` ファイルをリモート マシン (ステップ 2 でコピー) から新しい監視 VM の `/usr/share/exhibitor/` パスにコピーします。

```
scp /directory/exhibitor.properties root@<Witness-VM-IP>:
/usr/share/exhibitor/exhibitor.properties
```

ステップ 7 次のシンボリック リンクが新しい監視 VM に保持されているかどうかを確認します。

```
root@Cisco-HX-Witness-Appliance:~# cd /etc/exhibitor/
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ls -al
total 8
drwxr-xr-x 2 root root 4096 Sep 11 13:00 .
drwxr-xr-x 88 root root 4096 Sep 11 12:55 ..
lrwxrwxrwx 1 root root 41 Sep 11 13:00 exhibitor.properties
lrwxrwxrwx 1 root root 37 Jul 24 16:49 log4j.properties
```

シンボリック リンクが使用できない場合は、次のコマンドを実行します。

```
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ln -s /usr/share/exhibitor/exhibitor.properties
exhibitor.properties
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ln -s /usr/share/exhibitor/log4j.properties
log4j.properties
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ls -al
total 8
drwxr-xr-x 2 root root 4096 Sep 11 13:00 .
drwxr-xr-x 88 root root 4096 Sep 11 12:55 ..
lrwxrwxrwx 1 root root 41 Sep 11 13:00 exhibitor.properties ->
/usr/share/exhibitor/exhibitor.properties
lrwxrwxrwx 1 root root 37 Jul 24 16:49 log4j.properties -> /usr/share/exhibitor/log4j.properties
```

ステップ 8 `/usr/share/exhibitor/setexhibitorconfig.sh` コマンドを実行して、Witness Node バージョン 1.1.1 にアップグレードします。

（注）
- この手順は、Witness VM Node バージョン 1.1.1 以降に移行するユーザーに必要です。他のバージョンにアップグレードする場合は、このステップをスキップしてください。
- setexhibitorconfig.sh は、showor.properties ファイルの編集プロセスを自動化し、対応するコントローラ VM ごとに、すべてのデータ IP アドレスを管理 IP アドレスに置き換えます。
- このコマンドには出力がありません。
- Cisco HXDP 4.5(2a) は、Witness VM バージョン 1.1.2 以降をサポートしています。

ステップ 9 次のコマンドを実行して、service exhibitor を起動します。

```
root@Cisco-HX-Witness-Appliance:~# service exhibitor start
exhibitor start/running, process <ID>
```

Cisco HyperFlex Stretch Cluster 4.5(x) に対して ESXi を手動でアップグレードする

ステップ 1 いずれかのホストを選択し、vSphere Web クライアントを使用して HX メンテナンス モードにします。ホストがメンテナンス モードになったら、次の手順を実行します。

ステップ 2 SCP を使用してファイルをコピーするには、同様に、接続先 ESXi ホストの SSH サービスを開始します。

（注）
- HX240 では、ローカルの SpringpathDS データストアまたはマウントされた HX データストアを使用できます。
- HX220 では、マウントされた HX データストアを使用するか、一時的な RAM ディスクを作成することができます。

```
scp local_filename user@server:/path/where/file/should/go
```

ステップ 3 ESXiにログインし、次のコマンドを実行して使用可能なイメージプロファイルの一覧を照会し、プロファイル名を確認します。

```
esxcli software sources profile list -d <データストア上の ESXi zip バンドルの場所>
```

注目 esxcli ソフトウェア コマンドを使用する際はフル パスを指定する必要があります。

例：

```
[root@localhost:~] esxcli software sources profile list -d /vmfs/volumes/5d3a21da-7f370812-ca58-0025
b5a5a102/HX-ESXi-6.0U3-13003896-Cisco-Custom-6.0.3.9-upgrade-bundle.zip
Name                                        Vendor  Acceptance Level  Creation Time
Modification Time
------------------------------------------  ------  ----------------  -------------------
-------------------
```

```
HX-ESXi-6.0U3-13003896-Cisco-Custom-6.0.3.9  Cisco   PartnerSupported  2019-04-02T00:14:56
2019-04-02T13:38:34
```

ステップ 4 次のコマンドを実行して、アップグレードを実行します。

```
esxcli software profile update -d <path_to_profile_ZIP_file> -p < profile name>
```

例：

```
[root@HX-ESXi-01:/vmfs/volumes/1a234567-89bc1234] esxcli software profile update -d
/vmfs/volumes/1a234567-89bc1234/HX-Vmware-ESXi-60U2-4192238-Cisco-Custom-Bundle-6.0.2.3.zip
-p HX-ESXi-6.0U3-13003896-Cisco-Custom-6.0.3.9
```

ステップ 5 ESXi ホストが起動したら、ホストが適切なバージョンで起動済みであることを確認します。

```
vmware -vl
```

ステップ 6 vSphere Web クライアントを使用して、メンテナンス モードを終了します。

ステップ 7 次の ESXi のアップグレードに進む前に、クラスタが正常な状態になっていることを確認します。

```
stcli cluster storage-summary --detail
```

ステップ 8 クラスタ内のすべてのホストに対して順番にこのプロセスを繰り返します。

（注） ESXiをアップグレードするごとに、クラスタが正常な状態であることを確認してから、次のESXiのアップグレードに進んでください。

UCS FW アップグレード用のストレッチ クラスタの設定

アップグレード時に、次に示すカスタマイズされたUCSポリシーが検証され、HyperFlex用に調整されます。

- HFP（ホスト ファームウェア パッケージ）：ホスト ファームウェア パッケージは、HyperFlex ノードの複数のコンポーネントに一貫したファームウェア ファイルを提供します。これには、CIMC、BIOS、HBA および SAS エクスパンダ ファームウェア、VIC およびその他のコンポーネントが含まれます。通常の UCS ホスト ファームウェア パッケージとは異なり、これらのファームウェア ファイルは、ディスク ファームウェアも制御します。HyperFlex データ プラットフォームにおいては、このことが特に重要だからです。自己暗号化ドライブ（SED）ファームウェアは、UCSマネージャポリシーではなく、HyperFlex データ プラットフォームによって直接制御されることに注意してください。
- VNICテンプレート：仮想NIC（VNIC）テンプレートは、UCSファブリック間のVNICの一貫した設定を提供します。HyperFlex VNIC テンプレートは、1 つの UCS ファブリック上の HyperFlex VNIC への変更がもう一方に適用されるように、冗長ペアとして設定されます。
- イーサネット アダプタ ポリシー：イーサネット アダプタ ポリシーは、HyperFlex VNICのパフォーマンス関連のプロパティを提供します。

- BIOS ポリシー：BIOS ポリシーは、HyperFlex ノード上の主要なハードウェア リソース（CPU やメモリなど）の設定とパフォーマンスを制御します。HyperFlex は、一貫して高いパフォーマンスを提供するため、特定の設定を使用します。
- VNIC/VHBA 配置ポリシー：VNIC/VHBA 配置ポリシーは、特定の VNIC/VHBA の HyperFlex ノードに提供される PCI アドレスを決定します。HyperFlex はこれを一貫した方法で設定するので、さらに詳細な構成も適切に行えます。

ステップ 1 サイト上の任意の CVM に SSH で接続し、ディレクトリを / tmp に変更します。

ステップ 2 `/usr/local/bin/hx.py --upgrade-cluster-config` コマンドを実行します。これにより、`customer_site_config.json` というファイルが生成され、/tmp ディレクトリに保存されます。

ステップ 3 `customer_site_config.json` ファイルを編集して、ファームウェアのバージョンと組織名を適切に変更します。次に例を示します。

例：

```
{
    "id": "Advanced",
    "collapse": true,
    "label": "Advanced",
    "groups": [
      {
        "id": "firmware",
        "label": "UCS Firmware",
        "items": [
          {
            "id": "version",
            "label": "UCS Firmware Version",
            "type": "text",
            "description": "UCS Firmware Version to be used on the HX servers",
            "placeholder": "ex: 3.2(2d)",
            "defaultValue": "3.2(2d)",
            "value": "4.1(1d)"  #<<<<<----------------- Change this
          },
          {
            "id": "version-m5",
            "label": "UCS Firmware Version",
            "type": "text",
            "description": "UCS Firmware Version to be used on the M5 HX servers",
            "placeholder": "ex: 3.2(2d)",
            "defaultValue": "3.2(2d)",
            "value": "4.1(1i)" #<<<<<----------------- Change this
          }
        ]
      },
      {
        "id": "org",
       "items": [
                    {
                          "id": "name",
                          "label": "Hyperflex Org name",
                          "type": "text",
                          "value": "Faridabad", #<<<<<----------------- Change this
                         "description": "The name of the org in ucsm which is to be used for creation
 of all the policies and profiles for this Hyperflex cluster"
                    }
        ]
```

```
    }
  ]
```

ステップ 4 コマンドを再度実行し、UCSM IP とクレデンシャルを入力します。

次に例を示します。

```
/usr/local/bin/hx.py --upgrade-cluster-config
```

例：

```
[root@SpringpathControllerVP0RX5DWTC:/# /usr/local/bin/hx.py --upgrade-cluster-config
                [UCS Manager] [in_progress][  0.00%][ETA:  0:18:00] Login to UCS API
                 UCS host name or virtual IP address: 10.42.17.11
                 Connecting to admin@10.42.17.11...
                Password:
```

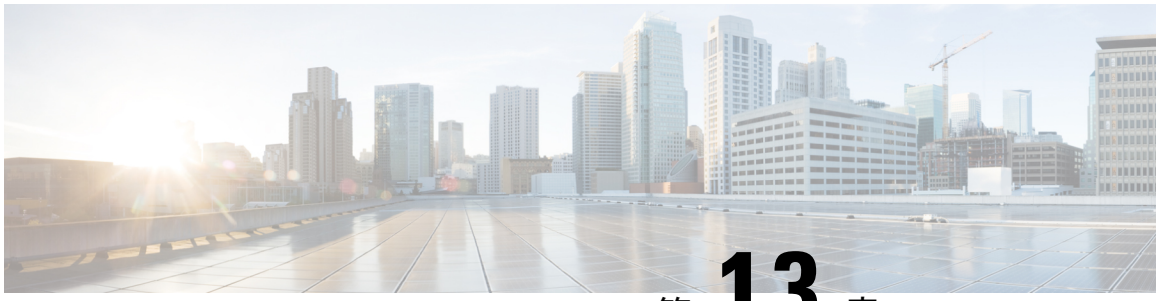
ステップ 5 コマンドがエラーを出さずに実行されることを確認します。エラーがあれば、Cisco TAC に連絡してください。

（注） このコマンド（hx.py）は、第 1 のサイト FI ドメインに対して実行されます。後で第 2 のサイト FI ドメインに対して同じ手順を実行する必要があります。

ステップ 6 vCenter および UCSM で次の手順を実行します。

a) UCSM の保留中のアクティビティに [Pending reboot] が表示されていることを確認します。
b) ホストをメンテナンス モードにします。
c) サーバを再起動し、サーバがオンラインになり、クラスタがオンライン/正常になるまで待ちます。
d) 残りのノードで同じ手順を実行します。

ステップ 7 他のサイトに対してステップ 4、5、および 6 を繰り返します。



第 13 章

HyperFlex オフライン アップグレードのワークフローと CLI アップグレード オプション

CLI を使用した HyperFlex Data Platform ソフトウェアのみのオンライン アップグレード

注目 HyperFlex Connect UI を使用して HyperFlex クラスタをアップグレードすることを推奨します。次の手順に、CLI を使用して HyperFlex クラスタをアップグレードするために使用するコマンドを示します。

1. UCSM（A バンドル）または UCS サーバーファームウェア（C バンドル）のアップグレードが必要な場合、Cisco UCS インフラストラクチャ A、ブレード バンドル B、およびラック バンドル C をダウンロードします。ソフトウェア ダウンロード を参照してください。
2. 必要に応じて Cisco UCS インフラストラクチャ バンドルをアップグレードします。UCS インフラストラクチャ ファームウェアのアップグレード （20ページ）を参照してください。
3. 管理者アクセス権でクラスタの CIP-M にログインし、tmp ディレクトリ、つまり /home/admin/tmp を作成します。
4. ターゲットの storfs-package-<>.tgz を tmp ディレクトリにコピーします。

5. ターゲットのハイパーバイザ アップグレード バンドルを tmp ディレクトリにコピーします。
6. コマンドの使用状況を確認するには、stcli cluster upgrade –-h コマンドを使用します。
7. –-dryrun を使用して、実際のアップグレードを開始する前に、コマンドへのすべての入力とアップグレードの互換性を確認します。
8. 実際のアップグレードを実行し、次の例に記載されている詳細に従ってください。

（注）
- UCS インフラストラクチャおよび UCS Server ファームウェアのアップグレードを実行する必要がある場合は、手順 1 と手順 2 が必要です。
- ハイパーバイザのアップグレードを実行する必要がある場合は、手順5が必要です。

Cisco HX Data Platform、ESXi、Cisco UCS ファームウェアの複合アップグレード

M6 クラスタ：

```
# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor –location
 /home/admin/tmp/<storfs package name> --hypervisor-bundle
 /home/admin/tmp/<ESXi package name> --ucsm-host <IP/FQDN of UCSM>
 --ucsm-user <UCSM User> --ucsm6-fw-version <UCSM Firmware Version>
 --vcenter-user administrator@vsphere.local
```

M6 の例：

```
~# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor –location
 /home/admin/tmp/storfs-packages-5.0.1a-40733.tgz --hypervisor-bundle
 /home/admin/tmp/HX-ESXi-6.7U3-17700523-Cisco-Custom-6.7.3.16-upgrade-bundle.zip
 --ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucsm6fw-version '4.2(1i)'
 --vcenter-user administrator@vsphere.local
```

M5 クラスタ：

```
# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor
--location /home/admin/tmp/<storfs package name> --hypervisor-bundle
 /home/admin/tmp/<ESXi package name> --ucsm-host <IP/FQDN of UCSM>
 --ucsm-user <UCSM User> --ucsm5-fw-version <UCSM Firmware Version>
 --vcenter-user administrator@vsphere.local
```

M5 の例：

```
~# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor –location
 /home/admin/tmp/storfs-packages-5.0.1a-40733.tgz --hypervisor-bundle
 /home/admin/tmp/HX-ESXi-6.7U3-17700523-Cisco-Custom-6.7.3.16-upgrade-bundle.zip
 --ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin –-ucsm5fw-version '4.2(1i)'
 --vcenter-user administrator@vsphere.local
```

M4 クラスタ：

```
# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor –location
 /home/admin/tmp/<storfs package name> --hypervisor-bundle
 /home/admin/tmp/<ESXi package name> --ucsm-host <IP/FQDN of UCSM>
 --ucsm-user <UCSM User> --ucs-fw-version <UCSM Firmware Version>
 --vcenter-user administrator@vsphere.local
```

M4 の例：

```
~# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor –location
 /home/admin/tmp/storfs-packages-5.0.1a-40733.tgz --hypervisor-bundle
 /home/admin/tmp/HX-ESXi-6.7U3-17700523-Cisco-Custom-6.7.3.16-upgrade-bundle.zip
 --ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin –-ucs-fw-version '4.2(1i)'
 --vcenter-user administrator@vsphere.local
```

Cisco HX Data Platform と ESXi の複合アップグレード

M6 / M5 / M4 クラスタ：

```
# stcli cluster upgrade --components hxdp,hypervisor –location
 /home/admin/tmp/<storfs package name> --hypervisor-bundle
 /home/admin/tmp/<esxiupgrade_bundle.zip> --vcenter-user administrator@vsphere.local
```

例：

```
~# stcli cluster upgrade --components hxdp,hypervisor –location
 /home/admin/tmp/storfs-packages-5.0.1a-40733.tgz --hypervisor-bundle
 /home/admin/tmp/HX-ESXi-6.7U3-17700523-Cisco-Custom-6.7.3.16-upgrade-bundle.zip
 --vcenter-user administrator@vsphere.local
```

Cisco HX Data Platform と Cisco UCS ファームウェアのコンパインド アップグレード

M6 クラスタ：

```
# stcli cluster upgrade --components ucs-fw,hxdp –location
 /home/admin/tmp/<storfs package name> --ucsm-host <IP/FQDN of UCSM>
 --ucsm-user <UCSM User> --ucsm6-fw-version <UCSM Firmware Version>
 --vcenter-user administrator@vsphere.local
```

M6 の例：

```
~# stcli cluster upgrade --components ucs-fw,hxdp –location
 /home/admin/tmp/storfs-packages-5.0.1a-40733.tgz
 --ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin
 --ucsm6fw-version '4.2(1i)' --vcenter-user administrator@vsphere.local
```

M5 クラスタ：

```
# stcli cluster upgrade --components ucs-fw,hxdp --location
/home/admin/tmp/<storfs package name> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsm5-fw-version <UCSM Firmware Version>
 --vcenter-user administrator@vsphere.local
```

M5 の例：

```
~# stcli cluster upgrade --components ucs-fw,hxdp –location
 /home/admin/tmp/storfs-packages-5.0.1a-40733.tgz --ucsm-host
 eng-fi16.eng.storvisor.com --ucsm-user admin –-ucsm5fw-version
 '4.2(1i)' --vcenter-user administrator@vsphere.local
```

M4 クラスタ：

```
# stcli cluster upgrade --components ucs-fw,hxdp --location
/home/admin/tmp/<storfs package name> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucs-fw-version <UCSM Firmware Version>
--vcenter-user administrator@vsphere.local
```

M4 の例：

```
~# stcli cluster upgrade --components ucs-fw,hxdp --location
/home/admin/tmp/storfs-packages-5.0.1a-40733.tgz --ucsm-host eng-fi16.eng.storvisor.com
```

```
--ucsm-user admin --ucs-fw-version '4.2(1i)' --vcenter-user administrator@vsphere.local
```

Cisco HX Data Platform のアップグレード

M6 / M5 / M4 クラスタ：

```
# stcli cluster upgrade --components hxdp --location /home/admin/tmp/<storfs
 package name> --vcenter-user administrator@vsphere.local
```

例：

```
~# stcli cluster upgrade --components hxdp --location
/home/admin/tmp/storfs-packages-5.0.1a-40733.tgz --vcenter-user administrator@vsphere.local
```

GUI のみを使用した Cisco HX Data Platform のアップグレード

HX Data Platform のみのアップグレードを開始します。Cisco UCS ファームウェア、HX Data Platform、および VMware vSphere ワークフローのアップグレード を参照してください。

GUI で Cisco UCS ファームウェアのみをアップグレードする

UCS ファームウェアのみのアップグレードを開始します。UCS インフラストラクチャ ファームウェアのアップグレード を参照してください。

オフライン アップグレードに関するガイドライン

重要

- オフラインのアップグレードは、HX Connect UI から、または CLI を使用して、結合アップグレードまたは分割アップグレードのいずれかで実行できます。続行する前に、次のガイドラインを考慮してください。

- Cisco は、HX Connect UI からオンラインのアップグレードを実行して、操作に影響を与えずに中断のないアップグレード エクスペリエンスを実現することを推奨しています。
- オフラインのアップグレードでは、クラスタをシャットダウンする必要があります。
- 新しいバージョンの Cisco HX Data Platform ソフトウェアを使ってノードがアップグレードされ、一度に 1 つずつリブートされます。
- ネストされた vCenter を使用したオフライン クラスタのアップグレードはサポートされていません。

オフライン アップグレード プロセスのワークフロー

ステップ	説明	参考資料
1.	UCSM（A バンドル）または UCS サーバ ファームウェア（Cバンドル）のアップグレードが必要な場合、Cisco UCS インフラストラクチャ A、ブレード バンドル B、およびラック バンドル C をダウンロードします。	[ソフトウェアのダウンロード（Software Download）]
2.	必要に応じて Cisco UCS インフラストラクチャ バンドルをアップグレードします。	UCS インフラストラクチャ ファームウェアのアップグレード （20 ページ）
3.	vSphere Web クライアントを起動し、HX サーバ上に存在するすべてのユーザーの VM (HyperFlex Controller VM は電源オンのまま) と HX データストア上で稼働中のすべてのユーザーの VM の電源をオフにします。これには、コンピューティング専用ノード上で稼働中の VM も含まれます。VM がシャットダウンされた後、クラスタの正常性を確認し、グレースフル シャットダウンを実行します。 **重要** HyperFlex コントローラ VM（stCtlVM）は、電源オンのままにしておく必要があります。	詳細については、Cisco HX ストレージ クラスタのシャットダウンと電源オフを参照してください。
4.	（オプション）管理者ユーザーとしてクラスタ管理 IP に SSH で接続し、スナップショットのスケジュールを無効にします。	コマンド `stcli snapshot-schedule --disable` を実行します。

ステップ	説明	参考資料
5.	管理者ユーザーとして HX Connect にログインし、複合化したアップグレードまたは個別のコンポーネントのアップグレードを実行します。	複合化したアップグレードについては、HX Connect を使用した HyperFlex Data Platform ソフトウェア、VMware ESXi、および Cisco UCS サーバ ファームウェアのアップグレード（25 ページ）を参照してください。 個別のコンポーネントのアップグレードについては、概要を参照してください。
6.	アップグレードが完了したことを確認し、アップグレード後のタスクを実行します。	アップグレード後の作業 （35 ページ）
7.	クラスタを開始します。	HX ストレージ クラスタのメンテナンスの準備
8.	（オプション）以前の手順 4 で無効にした場合は、スナップショットのスケジュールを有効にします。	コマンド `stcli snapshot-schedule --disable` を実行します。

CLI を使用したオフライン アップグレード

重要 分割アップグレードを実行する必要がある場合は、最初に HX Data Platform をアップグレードする必要があります。HX Data Platform をリリース 3.5(1x) にアップグレードした後は、UCSM のみ、または ESXi のみ、および/またはその両方の分割アップグレードを実行できます。

（注） すべての例の ucs ファームウェアのバージョンを、リリース ノートの推奨バージョンに更新してください。https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-release-notes-list.html

Cisco HX Data Platform、ESXi、Cisco UCS ファームウェアの複合アップグレード

M6 サーバー

```
# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor --location /tmp/
<storfs package name> --hypervisor-bundle /tmp/<ESXi package name> --ucsm-host <IP/FQDN
 of UCSM>
--ucsm-user <UCSM User> --ucsm6-fw-version <UCSM Firmware Version>
```

M6 サーバーの例：

```
~# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor --location
/tmp/storfs-packages-5.0.1a-19712.tgz --hypervisor-bundle
/tmp/ESXi-6.7-U3-offline-bundle.zip
--ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucs6fw-version '4.0(2g)'
```

M5 サーバ

```
# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor --location /tmp/
<storfs package name> --hypervisor-bundle /tmp/<ESXi package name> --ucsm-host <IP/FQDN
 of UCSM>
--ucsm-user <UCSM User> --ucsm5-fw-version <UCSM Firmware Version>
```

M5 サーバの例:

```
~# stcli cluster upgrade --components ucs-fw,hxdp,hypervisor --location
/tmp/storfs-packages-4.5.1a-19712.tgz --hypervisor-bundle
/tmp/ESXi-6.7-U3-offline-bundle.zip
--ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucs5fw-version '4.0(2g)'
```

M4 サーバ

```
# stcli cluster upgrade --components ucs-fw, hxdp, hypervisor --location/tmp/
<storfs package name, ESXi package name> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsfw-version <UCSM Firmware Version>
```

M4 サーバの例：

```
~# stcli cluster upgrade --components ucs-fw, hxdp, hypervisor --location
/tmp/storfs-packages-4.5.1a-19712.tgz
--ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucsfw-version '4.0(2g)'
```

Cisco HX Data Platform と ESXi の複合アップグレード

M5 サーバ

```
# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/
hxupgrade_bundle.tgz --hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

M5 サーバの例:

```
~# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/
hxupgrade_bundle.tgz --hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

M4 サーバ

```
# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/
hxupgrade_bundle.tgz --hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

M4 サーバの例：

```
~# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/
hxupgrade_bundle.tgz --hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

Cisco HX Data Platform と Cisco UCS ファームウェアのコンパインド アップグレード

M5 サーバ

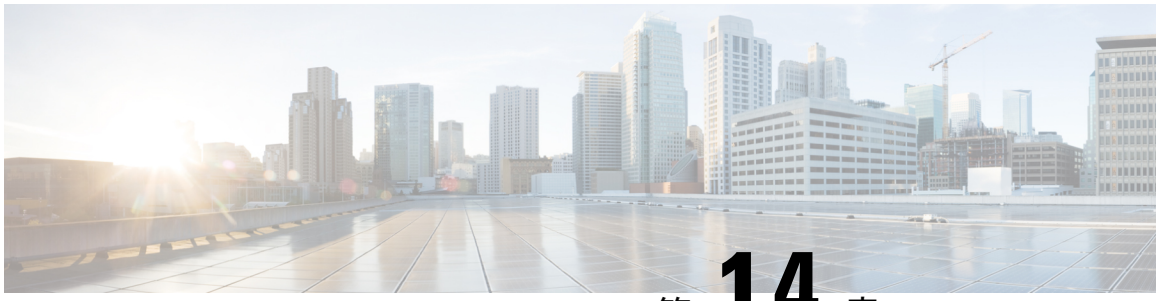
```
# stcli cluster upgrade --components hxdp,ucs-fw --location/tmp/
<storfs package name> --vcenter-user <vcuser> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsm5-fw-version <UCSM Firmware Version>
```

M4 サーバ

```
# stcli cluster upgrade --components hxdp,ucs-fw --location/tmp/
<storfs package name> --vcenter-user <vcuser> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsfw-version <UCSM Firmware Version>
```

M4 サーバの例：

```
~# stcli cluster upgrade --components hxdp,ucs-fw --location
/tmp/storfs-packages-1.8.1c-19712.tgz --vcenter-user administrator@vsphere.local
--ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucsfw-version '3.1(2b)'
```



第 14 章

手動のアップグレード前の検証

概要

この項では、Hypercheck: アップグレード前チェック ツール （9 ページ） で説明されている Hypercheck ツールを実行できない場合のアップグレード前の手動検証について説明します。これらのチェックを手動で実行するよりも、Hypercheck を実行することを強く推奨します。

クラスタのストレージ容量の確認

シスコは、Cisco HX データ プラットフォームの既存のインストールのアップグレードを開始する前に、クラスタ ストレージ容量をチェックすることをお勧めします。クラスタ内のストレージ使用率が 70% を超える場合、アップグレードの検証は失敗します。

クラスタ ストレージ容量をチェックすることの背景の詳細については、『*Cisco HyperFlex* データ プラットフォーム管理ガイド』の HX ストレージ クラスタの概要」の章を参照してください。

Net.TeamPolicyUpDelay のデフォルト値の確認と設定

ファブリック インターコネクトのリブート中にストレージ ア クセスが失われないようにするには、UCSM インフラストラクチャのアップグレードの前にこのチェックを実行します。

3.0(1)、3.5(1)、3.5(2)、4.0(1)、4.0(2) へのアップグレードでは、ESXi host Net.TeamPolicyUpDelay のデフォルト値が 30000 に設定されている必要があります。次の手順を実行して確認し、必要に応じて、ESXi host Net.TeamPolicyUpDelay のデフォルト値を 30000 に変更します。

（注） この変更によってESXiホストをリブートする必要はなく、リブート後も維持されます。

ステップ 1 vSphere Web クライアント ナビゲータから、各 [ESXi Host (ESXi ホスト)] > **[Configure (設定)]** > **[System (システム)]** > **[Advanced System Settings (詳細なシステム設定)]** をクリックします。

ステップ 2 **[Advanced System** Settings (詳細なシステム設定)] で、**[Net.TeamPolicyUpDelay]** までスクロールダウンします。

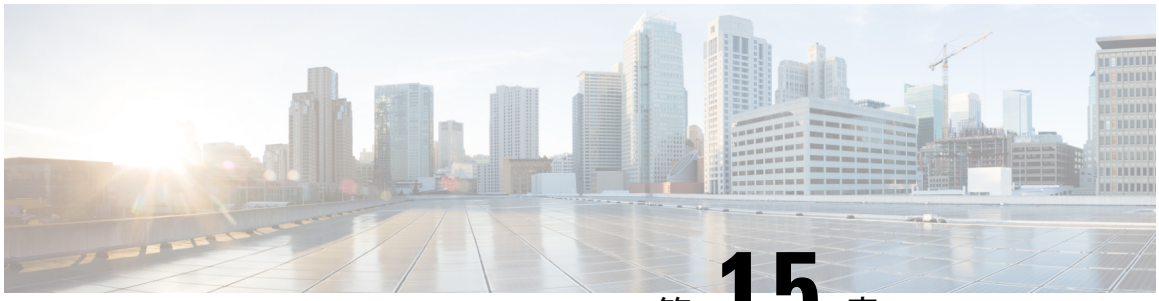
ステップ 3 必要に応じて、値を *30000* に変更します。デフォルト値は 100 です。

a) ビルド 16075168 以下の ESXi 6.7 バージョンの場合、クラスタ内の各 ESXi ホストに SSH で接続します。

b) **netdbg vswitch runtime set TeamPolicyUpDelay 30000** を実行します。

c) **netdbg vswitch runtime get,** を実行して設定を確認し、**Net.TeamPolicyUpDelay** が *30000* と同等であることを確認します。

d) この設定は、ESXi ホストの再起動後に保持されないため、ESXi local.sh ファイルにコマンド **netdbg vswitch runtime set TeamPolicyUpDelay 30000** を 追加してください（VMware KB https://kb.vmware.com/s/article/2043564 を参照）。



第 15 章

HyperFlexアップグレードのトラブルシューティング

VMs はアップグレードしている時は移行しません

説明

ESXi クラスタのアップグレードは、「ノードのメンテナンス モードが失敗しました」というエラーで失敗します。これは、DRS と HA が有効になっているオンラインで正常な ESXi クラスタで発生します。

アクション（Action）

次の回避策を次の順序で試してください。

1. HA アドミッション コントロール ポリシーが有効で、スロット ポリシーに設定されている場合は、クラスタ 技術情報の割合に変更して 1 つのホストの障害を許容してから、アップグレードを再試行します。
2. HA アドミッション コントロール ポリシーを無効にするか、HA を無効にしてから、アップグレードを再試行します。

3. いくつかの VM をパワーオフするか、ノードを追加して、少なくとも 1 つのノードの障害を許容できる十分なフェイルオーバー キャパシティがクラスタにあることを確認してから、アップグレードを再試行します。

ロックダウン モードの ESXi ホストまたは HyperFlex コントローラ

説明

ESXi ホストがロックダウン モードの場合は、アップグレード前の検証が失敗し、エラーメッセージ *[auth cancel]* が表示されます。

アクション: ESXi ホストでロックダウン モードを無効にし、アップグレードが成功したら有効にします。

ロックダウン モードの有効化または無効化

HyperFlex コントローラ VM の使用

1. HX Connect にログインします。
2. 左側の [Navigation] ペインで、**[System Overview]** を選択します。
3. **システムの概要**]タブで、**アクション**ドロップダウンリストからの有効化またはコントローラ VM へのアクセスを無効にする管理者として、SSH を使用します。

ESXi ホストの使用

1. vSphere Web クライアントにログインします。
2. VSphere Web Client のインベントリでホストを特定します。
3. [**Manage**] タブをクリックし、[Settings] をクリックします。
4. [System] で、**[Security profile]** を選択します。
5. [Lockdown Mode] パネルで、**[Edit]** をクリックします。
6. **[ロックダウンモード（Lockdown Mode）]**をクリックし、モードを [無効] に設定します。

アップグレード中に HX Connect への接続が失われる

説明：HX 3.5 (2g) から HX 4.0 (2a) へのアップグレード前の手順の後、HX 接続への接続が失われました。アップグレード中に、アップグレードのソースバージョンに期限切れの証明書がある場合、ブラウザはアップグレード前の手順を実行した後にユーザーをログアウトします。サーバの証明書が事前アップグレード後に変更されたため、これは承認された安全な動作を承認します。

アクション：ブラウザを更新し、再度ログインします。

HyperFlex VIB のアップグレードに失敗しました

説明：

HX 4.5（1a）以上への HXDP アップグレードのエラー：「*HyperFlex VIB* のアップグレードに失敗しました。理由：いくつかの（システム エラー）。」

次のエラー ログが ESXi `esxupdate.log` ファイルに表示されます。

```
2020-12-01T11:59:22Z esxupdate: 333049: root: ERROR:
vmware.esximage.Errors.LiveInstallationError: ([], '([], "Error in running rm
/tardisks/scvmclie.v00:\\nReturn code: 1\\nOutput: rm: can\'t remove
\'/tardisks/scvmclie.v00\': Device or resource busy\\n\\nIt is not safe to continue. 完了していないアップデートを破棄するには、ホストをただちに再起動してください。 」
```

アクション：次の手順に従って、`getstctlvmlogs` に対応するプロセスを強制終了し、アップグレードを再試行します。

1. root ログインで ESXi に SSH 接続します。
2. コマンド `ps -c | grep -e cisco -e springpath` を実行し、プロセス ID（PID）をメモします。次に例を示します。

   ```
   ps -c | grep -e cisco -e springpath
   ```

   ```
   112056 112056 sh /bin/sh /opt/springpath/support/getstctlvmlogs
   ```

3. コマンド `kill-9<PID from previous command>` を使用してプロセスを強制終了します。次に例を示します。

   ```
   kill -9 112056
   ```

4. HX Connect または Intersight に戻り、アップグレードを再試行します。問題がまだ続く場合は、Cisco TAC にお問い合わせください。

HX Connect UCS サーバ ファームウェア 選択ドロップダウンにファームウェア バージョン 4.1 以降がリストされていない

説明

HX Connect UI から複合アップグレードを実行しようとすると、UCS サーバ ファームウェアを選択するドロップダウンにバージョン 4.1 以降が表示されません。

アクション

UCS Manager にログインし、ファブリック インターコネクトに UCS B および C ファームウェア バンドルをアップロードしたことを確認します。そうでない場合は、それらをアップロードし、アップグレードを再試行します。UCS B および C ファームウェア バンドルがファブリック インターコネクトにすでにアップロードされている場合は、以下の回避策を適用してアップグレードを続行します。

1. [アップグレード タイプの選択（Select Upgrade Type）] ページで、**[HX データ プラットフォーム（HX Data Platform）]** のみを選択します。
2. アップグレードに適した HXDP アップグレード パッケージを参照して選択します。[1]
3. vCenter ログイン情報を入力します。
4. **[アップグレード（Upgrade）]**をクリックします。これにより、管理コンポーネントがブートストラップされます。UI 画面を更新します。
5. UI が更新されたら、複合アップグレード手順を試してください。これで、UCS サーバ ファームウェア バージョン 4.1 以降がドロップダウン メニューに表示されます。

クラスタ ノードをメンテナンス モードにする手順でアップグレードが失敗しました

説明

クラスタ ノードをメンテナンス モードにする手順の失敗は、vSwitch とポート グループでの MTU の不一致が原因で発生します。ノード拡張方式を使用して後で追加されたノードがクラスタにある場合、新しく追加されたノードの MTU は 9000 に設定され、他のノードは MTU 1500 に設定されます。

（注） 以下の修復は、クラスタにクラスタ拡張の一部として追加された 1 つ以上のノードがあり、元のクラスタノードが 1500 の MTU に設定されている間に MTU が 9000 に設定されている場合にのみ適用されます。これがシナリオではない場合は、TAC にお問い合わせください。

アクション

- vCenter にログインします。
- すべてのノードで設定されている MTU 値を確認します。

[1] [バージョンは HXDP 4.5 以降である必要があります。（The version must be HXDP 4.5 or later.）]

- 最初に構築されたクラスタの一部であったノードの MTU が 1500 に設定されており、他の一部のノード（クラスタ拡張の一部として後で追加されたノード）の MTU が 9000 に設定されている場合は、そのようなすべてのノードの MTU を 1500 に変更します。
- アップグレードを再試行します。

vGPU が設定された VM を含むクラスタのメンテナンス モードが自動にならない

説明

vGPU が設定された VM を含むクラスタの場合、DRS が完全に有効になっていても、メンテナンス モードは自動的には開始しません。ローリング アップグレード時には、これらの VM を手動で処理して、各 ESXi ホストがメンテナンス モードに入り、適切なタイミングでアップグレードを続行できるようにする必要があります。

アクション

次のいずれかの方法を使用して続行します。

1. vGPU が設定された VM について、クラスタ内の別の ESXi ホストに、手動で vMotion の操作を行います。
2. vGPU が設定された VM の電源を一時的にオフにします。ESXi ホストが再起動し、クラスタに再参加したら、再度電源をオンにすることができます。

（注） これは DRS ホストの退避に関する制限で、ドキュメント化されています。DRS が vGPU 対応の VM を自動的に移行しない（66813）を参照してください。

vGPU が設定された VM を含むクラスタのメンテナンス モードが自動にならない

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。