Cisco HyperFlex Data Platform リリース 6.0 アドミニストレーション ガイド

最終更新：2024 年 10 月 30 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

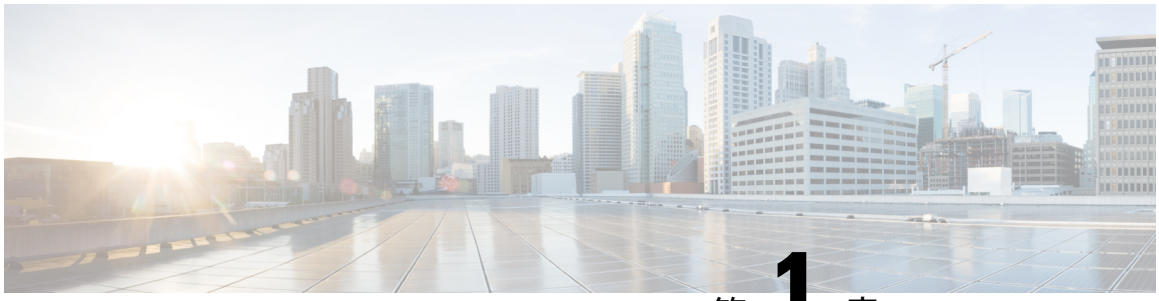
Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

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

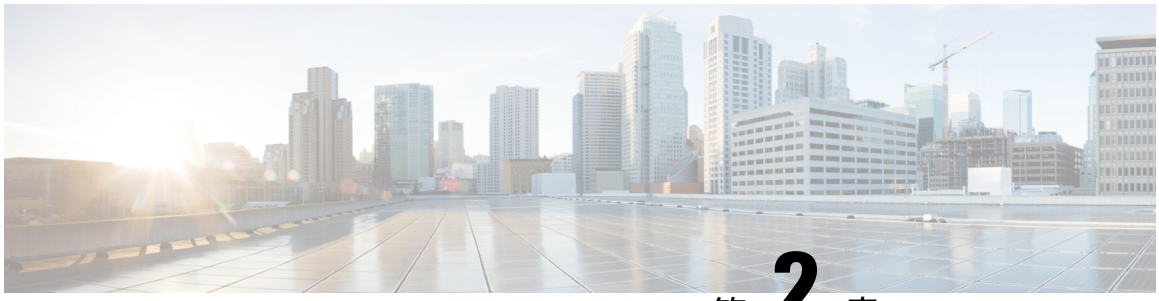
このリリースの新規情報および変更情報

このリリースの新規情報および変更情報

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	リリース/日付が追加されました	参照先
HyperFlex リリース 6.0(1a) の新しいガイド	-	6.0(1a)	本書です。

このリリースの新規情報および変更情報



第 2 章

HX ストレージ クラスタの概要

Cisco HX Data Platform の概要

Cisco HyperFlex Data Platform（HX Data Platform）は、複数の Cisco サーバ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 ストレージの必要がなくなり、仮想環境でのコンピューティングとストレージのシームレスな相互運用が可能になります。Cisco HX Data Platform で実現する極めて耐障害性に優れた分散ストレージ システムにより、データ整合性が確保されるだけでなく、仮想マシン（VM）ストレージ ワークロードのパフォーマンスが最適化されます。また、ネイティブ圧縮と重複排除によって、VM により占有される記憶域と VM ワークロードが削減されます。

Cisco HX Data Platform には多数の統合コンポーネントがあります。これらのコンポーネントには、Cisco Fabric Interconnects（FI）、Cisco UCS Manager、Cisco HX 固有のサーバーに加え、Cisco コンピューティング専用サーバとして VMware vSphere、ESXi サーバー、および vCenter が含まれます。さらに、Cisco HX Data Platform Installer、コントローラ VM、HX Connect、vSphere HX Data Platform Plug-in、および `hxcli` コマンドも使用できます。

Cisco HX Data Platform をインストールする場所は、VMware vSphere などの仮想化プラットフォームです。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、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。コンピューティング専用リソースを増やすには、コンピューティング専用ノードをストレージ クラスタに追加できます。

ストレージ クラスタの物理コンポーネントの概要

Cisco HyperFlex ストレージ クラスタは、以下のオブジェクトを含みます。これらのオブジェクトは、ストレージクラスタ用の HX Data Platform によってモニタリングされます。これらは HX ストレージ クラスタで追加または削除できます。

- **コンバージドノード**—コンバージドノードは、VM が実行されている物理的なハードウェアです。これらはディスク容量、メモリ、処理、電源、ネットワーク I/O などのコンピューティング リソースとストレージ リソースを提供します。

  コンバージド ノードをストレージ クラスタに追加すると、ストレージ コントローラ VM がインストールされます。HX Data Platform サービスは、ストレージ コントローラ VM を介して処理されます。コンバージドノードは、関連付けられたドライブを介してストレージ リソースをストレージ クラスタに追加します。

  HX Data Platform インストーラから クラスタ拡張 ワークフローを実行して、ストレージ クラスタにコンバージドノードを追加します。*hxcli* コマンドを使用してコンバージドノードを削除できます。

- **コンピューティング ノード**—コンピューティング ノードはコンピューティング リソースを追加するものですが、ストレージ クラスタへストレージ キャパシティを追加するものではありません。これらは、CPU とメモリを含むコンピューティング リソースを追加する手段として使用されます。キャッシング（SSD）ドライブやストレージ（HDD）ドライブは必要ありません。コンピューティング ノードは、HX ストレージ クラスタではオプションです。

  コンピューティング ノードをストレージクラスタに追加すると、エージェント コントローラ VM がインストールされます。HX Data Platform サービスは、エージェント コントローラ VM を介して処理されます。

  HX Data Platform インストーラから クラスタ拡張 ワークフローを実行して、ストレージ クラスタにコンピューティング ノードを追加します。*hxcli* コマンドを使用してコンピューティング ノードを削除できます。

- **ドライブ**—ストレージ クラスタ内のノードに必要なドライブには、ソリッド ステート ドライブ（SSD）とハード ディスク ドライブ（HDD）の 2 種類があります。HDD は通常、コンバージド ノードに関連付けられる物理ストレージ ユニットを提供します。SSD は通常、管理をサポートします。

  また、既存のコンバージドノードに HDD を追加しても、ストレージクラスタにストレージ キャパシティを追加できます。ストレージ クラスタ内の HX ノードにストレージを追加する場合は、ストレージクラスタ内のすべてのノードに同等の容量のストレージを追加する必要があります。

  ディスクの追加または削除すると、HX Data Platform はストレージ リソースの変更に応じて、ストレージ クラスタのバランスを再調整します。

コンバージド ノード上のディスクの追加や削除は、HX Data Platform によっては行われません。ディスクを追加または取り外す前に、ベスト プラクティスを確認してください。ノードでディスクを追加または取り外すための特定の手順については、サーバー ハードウェア ガイドを参照してください。

NVMe キャッシング SSD のスロット情報は、オール NVMe サーバ PID を除くと、どの AF サーバ PID も、HX-Connect から取得することができません。NVMe SSD のスロット情報は、UCSM 管理コンソールで確認してください。

- **データストア**—ストレージ容量とデータストア容量。これは、データストアを介してストレージ クラスタで使用できる消費可能な物理ストレージ合計であり、HX Data Platform によって管理されます。

  データストアは、ストレージの使用およびストレージ リソースを管理するために HX データ プラットフォームによって使用される論理的コンテナです。

  ホストは、仮想ディスク ファイルやその他の VM ファイルをデータストアに配置します。データストアは、物理ストレージ デバイスの仕様を非表示にし、VM ファイルを格納するための統一モデルを提供します。

HX Data Platform キャパシティの概要

（注） ディスクまたはノードを追加してクラスタの容量を追加すると、再調整が発生する可能性があります。このバックグラウンド アクティビティにより、クラスタ上の通常のユーザー IO との干渉が発生し、遅延が増加する可能性があります。パフォーマンスへの影響が許容される場合、ストレージ容量の期間をメモする必要があります。また、この操作は容量の追加を保証する緊急事態に実行される場合があります。

HX Data Platform では、キャパシティ（つまり容量）の概念がデータストアとストレージ クラスタの両方に適用されます。値は base-2（GiB/TiB）単位で測定されますが、簡素化と一貫性のために GB または TB という標識が付きます。

- **[クリーナ（Cleaner）]**：すべてのストレージ クラスタ データストアで実行されるプロセスです。これが完了した後、すべてのストレージ クラスタ データストアの合計容量は、ストレージ クラスタの合計容量からメタデータを差し引いた値とほぼ同じになるはずです。一般に、リストされるデータストア キャパシティ（容量）は HX ストレージ クラスタのキャパシティと一致しません。クリーナー コマンドに関する情報については、『Cisco HX Data Platform コマンド ライン インターフェイス リファレンス ガイド』を参照してください。
- **[クラスタ容量（Cluster capacity）]**：ストレージ クラスタに含まれる全ノード上のすべてのディスクの合計ストレージ容量。これには、各ディスク上のクリーンアップされていないデータとメタデータ オーバーヘッドが含まれます。

  クラスタの合計/使用済み/空き容量は、ストレージ全体の容量と使用済みストレージの量に基づきます。

- **条件**: HX ストレージ クラスタがスペース イベント状態になると、**[空き領域ステータス (Free Space Status)]** フィールドが表示されます。**[条件（Condition）]** フィールドにスペース イベント状態が示されます。オプションは、**[警告（Warning）]**、**[重大（Critical）]**、**[アラート（Alert）]** です。

- **利用可能なデータストア容量**：プロビジョニングなしでデータストアをプロビジョニングする際に使用できるストレージの量です。通常、この値はクリーンアップ後のストレージ クラスタ容量とほぼ同じですが、完全には一致しません。メタデータやクリーンアップされていないデータは含まれません。

  各データストアのプロビジョニング済み/使用済み/空き容量は、データストア (シン) プロビジョニング済み容量に基づいています。データストアはシンプロビジョニングされるので、（データストア作成時に管理者が指定する）プロビジョニング キャパシティが実際のストレージを超える場合もあります。

- **[未使用キャパシティ、ストレージ クラスタ（Free Capacity, storage cluster）]**：使用可能な容量と同じです。ストレージ クラスタの場合、これは、ストレージ クラスタで使用可能な容量とストレージ クラスタで使用されている容量との差です。

- **[未使用キャパシティ、データストア（Free capacity, datastore）]**：使用可能な容量と同じです。すべてのストレージ クラスタ データストアでは、これは、すべてのストレージ クラスタ データストアにプロビジョニングされた容量とすべてのストレージ クラスタ データストアで使用されている容量との差です。

  ストレージクラスタ全体で使用されている容量は、このデータストアの計算には含まれません。データストアは頻繁にオーバープロビジョニングされるので、[未使用キャパシティ（Free capacity）] では、すべてのストレージ クラスタ データストアの可用性に比べて、ストレージ クラスタのキャパシティ可用性がかなり低く表示される場合があります。

- **[複数ユーザ（Multiple users）]**：さまざまなデータストアに、さまざまなキャパシティ（容量）がプロビジョニングされる可能性があります。いずれの時点においても、ユーザは自分に割り振られたデータストア キャパシティを完全には使用しません。複数ユーザにデータストア キャパシティを割り振る場合、管理者は、各ユーザにプロビジョニングされるキャパシティが常に実施されるようにする必要があります。

- **[オーバー プロビジョニング（Over-provisioning）]**：すべてのデータストアに割り振られたストレージ容量が、ストレージ クラスタで使用できる量を超えると発生します。

  多くの場合、最初にオーバー プロビジョニングを行います。これにより、管理者はまずキャパシティを割り振り、後で実際のストレージに合わせていくことができます。

  この値は、使用可能な容量とプロビジョニングされた容量との差です。

  可能な最大物理量よりも多くの領域が割り振られていない場合は、ゼロ（0）が表示されます。

  オーバープロビジョニングされた容量を確認して、システムが領域不足の状態に達しないようにしてください。

- **プロビジョニング済み**：クラスタ データストアでの使用が許可され割り当てられたキャパシティの量です。

プロビジョニングされた容量は、ストレージ クラスタ データストアでの単独使用のために確保されているわけではありません。複数のデータストアのストレージが、同じストレージ キャパシティからプロビジョニングされる場合があります。

- **[Space Needed]**：HX ストレージ クラスタがスペース イベント状態になると、**[空き領域ステータス (Free Space Status)]** フィールドが表示されます。**[必要な領域（Space Needed）]** には、**[条件（Condition）]** にリストされている状態をクリアするために解放すべきストレージ量が示されます。
- **[使用済み（Used）]**：リストされたストレージ クラスタまたはデータストアで使用されているストレージ容量です。

  HX Data Platform 内部のメタデータは、0.5 ～ 1% の領域を使用します。このことにより、データストアにデータがない場合であっても、HX Data Platform プラグインまたは HX Connect に [ストレージ使用量 (Used Storage)] の値が表示される場合があります。

  ストレージの [使用済み（Used）] は、どの程度のデータストア領域が、設定ファイルやログ ファイル、スナップショット、クローンなどの仮想マシン ファイルによって占有されているかを表します。仮想マシンの実行中、使用されたストレージ領域にはスワップ ファイルも含まれます。
- **[使用可能容量（Usable Capacity）]**：データの保存に使用できるストレージ クラスタのストレージ容量です。

キャパシティの節約について

[サマリー（Summary）] タブの [キャパシティ（Capacity）] ポートレットには、ストレージ クラスタの重複排除と圧縮によるキャパシティの節約状況が表示されます。たとえば、6TB のキャパシティを持つストレージ クラスタの全体的な節約率が 50% である場合、実際には 9TB のデータを保管できることになります。

HX Data Platform システムにより節約されるストレージ容量の合計は、2 つの要素を計算することで算出されます。

- **圧縮**—圧縮されているデータの量。
- **重複排除**—重複排除されているデータの量。重複排除とは、重複するデータを排除して、データが占有するストレージ スペースを削減する手法です。重複排除により、データの一意のインスタンスが 1 つだけが保管されるようになります。

重複排除による節約量と圧縮による節約量が単純に合計されるわけではありません。この2つは独立した処理ではないためです。これらは、次のような仕組みで関連してます。まず、原則として、ストレージで使用される固有のバイト数は重複排除を介して削減されます。重複排除が適用された後のストレージ使用量に圧縮を適用することで、ストレージクラスタで使用可能なストレージがさらに増えます。

VM クローンを使用する場合、重複排除と圧縮による削減は有用です。

節約量が 0% として表示されている場合、それは新しいストレージ クラスタであることを意味します。ストレージ クラスタに取り込まれたデータの合計量だけでは、意味のあるストレージ

削減量を判断することはできません。十分なデータがストレージクラスタに書き込まれるまで待つ必要があります。

次に例を示します。

1. 初期値

   100 GB の VM が 2 回複製されるとします。

   一意の使用スペースの合計（TUUS）= 100 GB

   総アドレス空間（TAS）= 100 □ 2 = 200 GB

   この例に基づく結果は次のとおりです。

   一意のバイト数の合計（TUB）= 25 GB

2. 重複排除による節約量

   ```
   = (1 - TUUS/TAS) * 100
   = (1 - 100GB / 200GB) *100
   = 50%
   ```

3. 圧縮節約量

   ```
   = (1 - TUB/TUUS) * 100
   = (1 - 25GB / 100GB) * 100
   = 75%
   ```

4. 算出された合計節約量

   ```
   = (1 - TUB/TAS) * 100
   = (1 - 25GB / 200GB) * 100
   = 87.5%
   ```

ストレージ容量イベント メッセージ

クラスタ ストレージ容量（キャパシティ）には、ストレージ クラスタに含まれる全ノード上のすべてのディスクのすべてのストレージ容量が含まれます。データの管理には、この使用可能な容量が使われます。

クラスタ キャパシティの計算

HyperFlex HX Data Platform クラスタの容量は次のように計算されます。

(((<GB 単位でのキャパシティ ディスク サイズ> * 10^9) / 1024^3) * <ノードあたりのキャパシティディスクの台数> * <HyperFlex のノード数> * 0.92) / レプリケーション ファクタ

TiB 単位の値を算出するには、この計算結果を 1024 で割ります。レプリケーション ファクタ値は、HX クラスタが RF=3 に設定されている場合は 3、HX クラスタが RF=2 に設定されている場合は 2 です。係数 0.92 は、各ディスクでさまざまな内部ファイルシステム処理のために HX Data Platform ソフトウェアによって確保される 8% の予約を示します。

計算例: <GB 単位でのキャパシティ ディスク サイズ> = 1200（1.2 Tb のディスクの場合）、<ノードあたりのキャパシティディスクの台数> = 15（HX240c-M6SX モデル サーバの場合）、<HyperFlex のノード数> = 8 、レプリケーション ファクタ = 3

結果: (((1200*10^9)/1024^3)*15*8*0.92)/3 = 41127.2049 41127.2049 / 1024 = 40.16 TiB

（注） クラスタ キャパシティ計算のためのこの公式は、ラージ フォーム ファクタ (LFF) のクラスタには適用されません。

エラー メッセージ

データ ストレージで使用可能な容量を大量に消費する必要がある場合はエラー メッセージが発行され、ストレージクラスタのパフォーマンスと正常性が影響を受けます。エラー メッセージは、vCenter のアラーム パネル、HX Connect、 の HX Data Platform Plug-in Alarms と Events ページに表示されます。

（注） vCenter と HX Connect で提供されるイベントとアラームの詳細は、必ずしも 1 対 1 の関係ではありません。HX Connect でメッセージを確認する場合は、vCenter のイベントとタスクも確認することをお勧めします。

（注） **警告または重大なエラーが表示された場合**：

容量を拡張するには、ドライブまたはノードを追加します。さらに、使用されていない仮想マシンとスナップショットを削除することも検討してください。パフォーマンスは、ストレージ容量が減少するまで影響を受けます。

- **SpaceWarningEvent**：エラーを発行します。これは第 1 レベルの警告です。

  できる限り早くスペースを再利用するためのクリーナーアクティビティの増加により、クラスタのパフォーマンスが影響を受けます。スループットと遅延に対する影響は、ワークロードと、実行される読み取りと書き込みの量によって異なります。

  使用されているストレージ容量を、警告しきい値（HX ストレージ クラスタの容量合計の 76%）を下回るまで削減します。

- **SpaceAlertEvent** – エラーが発行します。スペース容量の使用率はエラー レベルのままです。

  このアラートは、ストレージ容量が削減された後でも警告しきい値を上回っている場合に発行されます。

  クラスタのパフォーマンスが影響を受けます。

  使用されているストレージ容量を、警告しきい値（HX ストレージ クラスタの容量合計の 80%）を下回るまで削減し続けます。

- **SpaceCriticalEvent** – エラーを発行します。これは、重大な警告レベルです。

  クラスタは、読み取り専用状態です。

  使用されているストレージ容量がこの警告しきい値未満に削減されるまで、ストレージクラスタ操作を続けないでください。

- **SpaceRecoveredEvent**：これは通知ですクラスタ容量が正常範囲に戻りました。

  クラスタ記憶域の使用率が正常に戻りました。

HX Data Platform の高可用性の概要

HX Data Platform の高可用性（HA）機能により、3 つ以上のノードが完全に機能している正常なストレージクラスタの動作中に、すべてのデータのコピーが少なくとも 2 つ確実に維持されます。

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した場合や 1 つのノードと別のノード上のディスクで障害が発生した場合は、同時障害と呼ばれます。

ノード障害によるストレージクラスタの状態は、ストレージクラスタ内のノードの数と、データ レプリケーション ファクタおよびアクセス ポリシーの設定により判断されます。

（注） HX Data Platform の HA 機能を使用するには、その前に、vSphere Web クライアントで DRS と vMotion を有効にする必要があります。

ストレージ クラスタのステータス

HX Data Platform ストレージ クラスタのステータス情報は、HX Connect、HX Data Platform Plug-in、およびストレージ コントローラ VM の `hxcli` コマンドによって表示されます。ストレージ クラスタ ステータスは、復元力ステータス値と動作ステータス値により示されます。

ストレージ クラスタ ステータスは、以下の報告されたステータス要素により示されます。

- **動作ステータス**：—クラスタの機能ストレージ管理とストレージクラスタ管理をストレージ クラスタが実行できるかどうかを示します。ストレージ クラスタが操作をどれほど実行できるか説明します。
- **復元ステータス**—ストレージ クラスタ内でのノード障害を許容できるストレージ クラスタの能力を示します。ストレージ クラスタが混乱をどれほど実行できるか説明します。

ストレージクラスタが特定の動作と修復ステータスの状態に移行する場合、以下の設定は有効です。

- **データ複製係数**—冗長データ レプリカの数を設定します。

- **クラスタ アクセス ポリシー**—データ保護とデータ損失のレベルを設定します。

動作ステータスの値

クラスタの動作ステータスは、ストレージ クラスタの動作ステータスとアプリケーションの I/O 実行能力を示します。

動作ステータスのオプションは次のとおりです。

- **[オンライン（Online）]**：クラスタは I/O に利用可能です。
- **[オフライン（Offline）]**：クラスタは I/O に利用可能ではありません。
- **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。
- **[読み取り専用（Readonly）]**：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、静的クラスタ情報の表示を継続することはできます。
- **[不明（Unknown）]**：これは、クラスタがオンラインになるまでの遷移状態です。

クラスタのアップグレード中や作成中には、他の遷移状態が示されることもあります。

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。アイコンをクリックすると、追加情報が表示されます（現在の状態になっている理由を説明するメッセージなど）。

復元力ステータスの値

復元力ステータスは、データ復元力のヘルス ステータスとストレージ クラスタの障害許容力を示します。

復元力ステータスのオプションは次のとおりです。

- **[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）]**：クラスタは、オンラインへの遷移状態にあります。

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。アイコンをクリックすると、追加情報が表示されます（現在の状態になっている理由を説明するメッセージなど）。

HX Data Platform クラスタで許容される障害

HX 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、クラスタの動作能力に影響が生じます。複数のノードで障害が発生した場合や1つのノードと別のノード上のディスクで障害が発生した場合は、同時障害と呼ばれます。

ストレージ クラスタへの影響は、次のようにノード障害の数によって異なります。

- **クラスタのノード数**—ストレージ クラスタの応答は、3 ～ 4 ノードのクラスタと 5 ノード以上のクラスタで異なります。
- **データ レプリケーション ファクタ** — HX Data Platform のインストール中に設定されるもので、変更できません。オプションは、ストレージ クラスタ全体で 2 または 3 個のデータの冗長レプリカです。実稼働クラスタは常に RF3 を使用する必要があります。RF2 は、ラボとデモでの使用のために予約する必要があります。

重要 実稼働クラスタは、Data Replication Factor 3 に設定する必要があります。

- **アクセス ポリシー**—ストレージ クラスタの作成後にデフォルト設定から変更できます。オプションは、データ損失から保護する場合の strict か、より長いストレージ クラスタ可用性をサポートする場合の lenient です。

障害ノードの数によるクラスタの状態

次の表では、同時ノード障害の数に応じて、ストレージクラスタの機能がどのように変化するかを示します。

表 *1*: 障害が発生したノードの数を含む *5* つ以上のノードクラスタのクラスタ状態、*HX* リリース *4.5(x)* 以降

レプリケーション ファクタ	アクセスポリシー	障害ノードの数	
		読み取り/書き込み	Read-Only
3	Lenient	2	--
3	Strict	1	2
2	Lenient	1	--
2	Strict	--	1

表 *2 :* 障害が発生したノードの数が多い *3〜4* ノード クラスタのクラスタ状態 *HX* リリース *4.5(x)* 以降。

レプリケーションファクタ	アクセスポリシー	障害ノードの数	
		読み取り/書き込み	**Read-Only**
3	Lenient または Strict	1	--
2	Lenient	1	--
2	Strict	--	1

ディスク障害があるノード数に応じたクラスタの状態

次の表では、1 つ以上のディスクで障害が発生したノードの数に応じて、ストレージクラスタの機能がどのように変化するかを示します。ノード自体では障害が発生しておらず、ノード内のディスクで障害が発生していることに注意してください。**例**：2 は、2 台のノードでそれぞれ 1 台以上のディスクで障害が発生していることを示します。

SSD と HDD の 2 種類のディスクがサーバ上に存在する可能性があります。次の表で複数のディスク障害について説明する際は、ストレージキャパシティに使用されるディスクに言及しています。**例**：あるノードのキャッシュ SSD で障害が発生し、別のノードのキャパシティ SSD または HDD で障害が発生した場合は、アクセス ポリシーで Strict に設定されていても、ストレージ クラスタの可用性は高いままです。

次の表に、障害が発生したディスクの数と最悪のシナリオを示します。これは、3つ以上のノードからなるストレージ クラスタに当てはまります。**例**：自己修復中のレプリケーション ファクタが 3 の 3 ノード クラスタは、3 つの異なるノードで全部で 3 件の同時ディスク障害が発生した場合にのみシャットダウンします。

（注） HX ストレージクラスタは、シリアルディスク障害（同時ではないディスク障害）に耐えることができます。唯一の要件は、自己修復をサポートするのに十分なストレージ キャパシティ（容量）があることです。この表に示す最悪のシナリオは、HX が自動自己修復と再調整を実行している短期間にのみ当てはまります。

ディスク障害があるノード数に応じた、3 つ以上のノードからなるクラスタ

レプリケーションファクタ	アクセスポリシー	ディスク障害が発生したノードの数	
		読み取り/書き込み	読み取り専用
3	Lenient	2	--
3	Strict	1	2
2	Lenient	1	--
2	Strict	--	1

データ レプリケーション ファクタの設定

重要 データ レプリケーション係数は、ストレージ クラスタの構成後は変更できません。

データ レプリケーション係数は、ストレージ クラスタの構成時に設定されます。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。オプションは、2 または 3 個のデータの冗長レプリカです。

- ハイブリッド サーバ（SSD および HDD の両方を含むサーバ）の場合、デフォルト値は 3 です。
- オール フラッシュ サーバ（SSD のみを含むサーバ）を使用している場合は、HX Data Platform のインストール中に 2 と 3 のいずれかを明示的に選択する必要があります。

手順

データ レプリケーション係数を選択します。選択できる基準は、次のとおりです。

- データ レプリケーション係数 3：（**推奨される使用法**：すべての実稼働環境）データの冗長レプリカを 3 つ保持します。この場合、ストレージ リソースの消費量は多くなりますが、ノード障害やディスク障害が発生した場合にデータを最大限に保護します。
- データ レプリケーション係数 2：（**推奨される使用法**：すべての実稼働環境）データの冗長レプリカを 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減少しますが、ノード障害やディスク障害が発生した場合にデータ保護が低下します。

クラスタアクセスポリシー

クラスタ アクセス ポリシーとデータ レプリケーション ファクタの組み合わせにより、データ保護レベルとデータ損失防止レベルが設定されます。クラスタ アクセス ポリシーには 2 つのオプションがあります。デフォルトでは `lenient`（寛容）に設定されます。インストール中にこれを設定することはできませんが、インストール後および初期ストレージクラスタ設定後に変更できます。

- **Strict**（厳格）：データ損失から保護するためのポリシーが適用されます。

  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。strict に設定すると、同時障害が発生した場合にデータを保護するのに役立ちます。

- **Lenient**（寛容）：より長いストレージ クラスタ可用性をサポートするためのポリシーが適用されます。これはデフォルトです。

ストレージ クラスタ ノード障害に対する応答

ストレージ クラスタの修復のタイムアウト時間は、ストレージ クラスタの自動修復前に HX Connect または HX Data Platform プラグインが待機する時間の長さになります。ディスク障害が発生した場合、修復のタイムアウト時間は1分になります。ノード障害が発生した場合、修復のタイムアウト時間は 2 時間になります。ディスクとノードに同時に障害が発生した場合や、ノード障害が発生し、修復が完了する前にディスク障害が発生した場合は、ノード障害のタイムアウトが優先されます。

クラスタの復元力ステータスが [警告（Warning）] の場合、HX Data Platform システムでは次のストレージ クラスタ障害と応答がサポートされます。

任意に、HXConnect および HXData Platform プラグインの関連するクラスタ ステータス/動作ステータスまたは復元力ステータス/復元力ヘルスをクリックして、現在の状態に何が影響しているかを説明する理由メッセージを表示します。

手順

表を確認して、示されている操作を実行します。

クラスタ サイズ	同時障害発生数	障害の発生したエンティティ	実行するメンテナンス アクション
3 ノード	1	1 つのノード。	ストレージ クラスタは自動的に修復されません。 ストレージクラスタヘルスを復元するために、障害が発生したノードを交換します。

クラスタ サイズ	同時障害発生数	障害の発生したエンティティ	実行するメンテナンス アクション
3 ノード	2	2 つのノード上の 2 つ以上のディスクがブロックリストに登録されているか、またはそれらのディスクで障害が発生している。	**1.** 1 台のキャッシュ SSD に障害が発生している場合、ストレージ クラスタは自動的に修復されません。 **2.** 1 台の HDD に障害が発生しているか取り外されている場合、ディスクはすぐにブロックリストに登録されます。ストレージ クラスタは、1 分以内に自動修復を開始します。 **3.** 複数の HDD に障害が発生している場合、システムは自動的にストレージ クラスタ ヘルスを復元しない可能性があります。 システムが復元されない場合、障害が発生したディスクを交換して、クラスタの再調整によってシステムを復元します。
4 ノード	1	1 つのノード。	ノードが 2 時間以内に復元されない場合、ストレージ クラスタは残りのノードのデータの再調整によって修復を開始します。 ノード障害をすぐに修復し、ストレージ クラスタを完全に復元させるには、次の手順に従います。 **1.** ノードの電源がオンになっていることを確認し、可能な場合は再起動します。ノードの交換が必要になる場合があります。 **2.** クラスタを再調整します。
4 ノード	2	2 つのノード上の 2 つ以上のディスク。	2 台の SSD に障害が発生している場合、ストレージ クラスタは自動的に修復されません。 ディスクが 1 分以内に復元されない場合、ストレージ クラスタは残りのノードのデータの再調整によって修復を開始します。

クラスタ サイズ	同時障害発生数	障害の発生したエンティティ	実行するメンテナンス アクション
5 個以上のノード	2	最大 2 つのノード。	ノードが 2 時間以内に復元されない場合、ストレージ クラスタは残りのノードのデータの再調整によって修復を開始します。 ノード障害をすぐに修復し、ストレージ クラスタを完全に復元させるには、次の手順に従います。 **1.** ノードの電源がオンになっていることを確認し、可能な場合は再起動します。ノードの交換が必要になる場合があります。 **2.** クラスタを再調整します。 ストレージクラスタがシャットダウンする場合は、「トラブルシューティング、2 つのノードで同時に障害が発生すると、ストレージ クラスタがシャットダウンする」のセクションを参照してください。
5 個以上のノード	2	2 つのノードのそれぞれで、2 つ以上のディスクに障害が発生する。	システムは、1 分後に自動的に再調整をトリガーし、ストレージ クラスタ ヘルスを復元します。

クラスタ サイズ	同時障害発生数	障害の発生したエンティティ	実行するメンテナンス アクション
5 個以上のノード	2	1 つのノードおよび別のノード上の 1 つ以上のディスク。	ディスクが **1 分**以内に復元されない場合、ストレージ クラスタは残りのノードのデータの再調整によって修復を開始します。 ノードが **2 時間**以内に復元されない場合、ストレージ クラスタは残りのノードのデータの再調整によって修復を開始します。 ストレージ クラスタ内のノードで障害が発生し、別のノード上のディスクにも障害が発生している場合、ストレージ クラスタは 1 分以内に障害発生ディスクの修復を開始します（障害発生ノードのデータは変更されません）。障害発生ノードが 2 時間経過後に稼動しない場合、ストレージ クラスタは障害発生ノードの修復も開始します。 ノード障害をすぐに修復し、ストレージ クラスタを完全に復元させるには、次の手順に従います。 **1.** ノードの電源がオンになっていることを確認し、可能な場合は再起動します。ノードの交換が必要になる場合があります。 **2.** クラスタを再調整します。

HX Data Platform Ready Clone の概要

HX Data Platform Ready Clones は、業界初のストレージ技術で、ホスト VM から複数のクローン VM をすぐに作成およびカスタムできます。スタンドアロン VM として使用可能な VM の複数のコピーを作成することができます。

Ready Clone（標準のクローンと同様に、既存の VM のコピーです）。既存の VM は、ホスト VM と呼ばれます。クローニング操作が完了すると、Ready Clone は別のゲスト VM となります。

Ready Clone に対して変更を行っても、ホスト VM には影響しません。Ready Clone の MAC アドレスおよび UUID は、ホスト VM の MAC アドレスおよび UUID とは異なります。

ゲスト オペレーティング システムとアプリケーションのインストールには、時間がかかることがあります。Ready Clone を実行すると、単一のインストールおよび設定プロセスで、多数の VM のコピーを作成できます。

クローンは、多数の同一の VM を 1 つのグループに配置する場合に役立ちます。

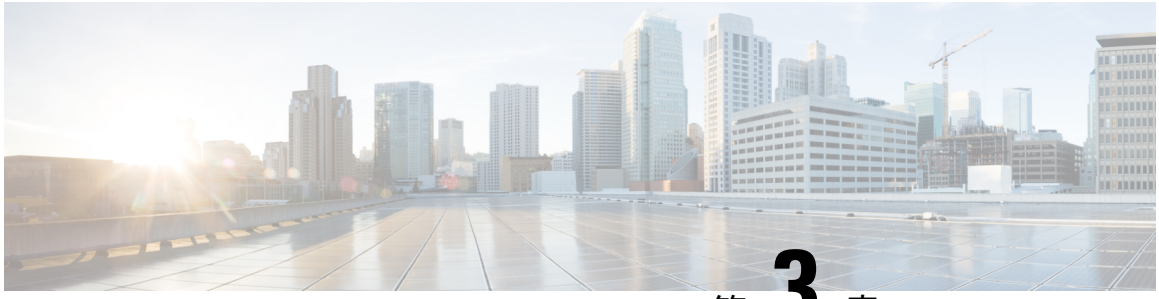
HX ネイティブ スナップショットの概要

HX ネイティブ スナップショットは、VM のバージョン（状態）を保存するバックアップ機能です。VM は、HX ネイティブ スナップショットを使用して、以前に保存したバージョンに戻すことができます。ネイティブ スナップショットはVMの複製で、ネイティブ スナップショットが作成された時点での、すべての VM ディスク上のデータの状態と VM の電源の状態（オン、オフ、またはサスペンド）が含まれます。保存した状態へ復元できるようにするには、ネイティブ スナップショットを取得して VM の現在の状態を保存します。

HX ネイティブ スナップショットの管理では、次の方法が使用されます。

- HTML 5 の vSphere クライアント プラグインでの HX ネイティブ スナップショットのサポートは、プラグイン バージョン 2.0.0 で導入されました。詳細については、今すぐスナップショットを作成 （420 ページ） を参照してください。
- HTML 5 の vSphere クライアント プラグインのスケジュール スナップショットのサポートは、プラグイン バージョン 2.1.0 で導入されました。詳細については、スナップショットのスケジュール （423 ページ）を参照してください。
- vSphere の「スナップショットの管理」機能は、特定の HX ネイティブ スナップショットに戻すことも、すべてのスナップショットを削除することもできます。
- Cisco HyperFlex Connect は、オンデマンドを作成し、HX ネイティブ スナップショットをスケジュールできます。
- HyperFlex コマンドライン ユーザー インターフェイスでは、HX ネイティブ スナップショットを作成できます。
- HX REST API は、HX ネイティブ スナップショットを作成および削除できます。
- Cisco HXDP リリース 5.5(x) 以降の重要な変更：
  - ESXi バージョン 6.5、6.7、および 7.0 U1 はサポートされていません。
  - Sentinel スナップショット作成ワークフローの代わりに、VMware VAAI スナップショット ワークフローが使用されます。

VMware スナップショットの詳細については、VMware Customer Connect サイトの「Overview of virtual machine snapshots in vSphere（KB 1015180）」を参照してください。



第 3 章

HX Data Platform インターフェイスへのログイン

HyperFlex クラスタ インターフェイスの概要

それぞれの HyperFlex インターフェイスから、HX ストレージ クラスタに関する情報にアクセスし、アクションを実行することができますHX。HXストレージクラスタのインターフェイスは次のとおりです。

- HX Connect—モニタリング、パフォーマンス チャート、およびアップグレード、暗号化、複製、データストア、ノード、ディスク、VM ready clones のタスク。
- HX Data Platform プラグイン—モニタリング、パフォーマンス チャート、データストア、ホスト（ノード）、ディスクのタスク。
- Admin Shellコマンドライン：HX Data Platform の `hxcli` コマンドを実行します。
- HyperFlex システム RESTful API—オンデマンドのステートレス プロトコルにより、HyperFlex システムの認証、レプリケーション、暗号化、モニタリング、および管理を可能にします。
- パフォーマンスを最も正確に読み取るには、HX Connect クラスタ レベルのパフォーマンス チャートを参照してください。他のグラフでは、HyperFlex のストレージを分散し、デー

タストアを介してVMが消費するという方法が原因で、全体像が把握しづらい場合があります。

他にも次のインターフェイスがあります。

- HX Data Platform インストーラ：HX Data Platform のインストール、HX ストレージ クラスタの展開と拡張、およびストレッチ クラスタの展開。
- Cisco UCS Manager — HX ストレージ クラスタのネットワーク、ストレージとストレージ アクセス、およびリソースの管理のタスク。
- VMware vSphere WebクライアントおよびvSphereクライアント：vCenterクラスタ内のすべてのVMware ESXiサーバを管理します。
- VMware ESXi — ホスト コマンド ラインを提供する個々の ESXi ホストの管理。

HX Data Platform ログイン情報に関するガイドライン

`hxcli` コマンドは、ログイン情報を要求します。

HX Data Platform インストーラの実行時に、事前定義された `admin` および `root` ユーザの管理シェルパスワードが指定されます。インストール後は、`hxcli` コマンドラインを使用してパスワードを変更できます。

ユーザーが 10 回連続で間違ったクレデンシャルでログインしようとした場合、アカウントは 2 分間ロックされます。SSH でログインの試行が失敗した場合、アカウントがロックされたことを示すエラー メッセージが表示されます。HX Connect または REST API でログインの試行が失敗した場合、10 回の試行中にアカウントがロックされたことを示すエラー メッセージが表示されます。

コンポーネント	権限レベル	ユーザー名	パスワード	注記
HX Data Platform インストーラVM	root	root	Cisco123	**重要**：システムに指定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。
HX 接続	管理者または読み取り専用	vCenter で定義されたユーザ。	vCenter で定義されたユーザ。	
		事前定義された `admin` または `root` ユーザ。	HX のインストール時に指定。	

コンポーネント	権限レベル	ユーザー名	パスワード	注記
管理シェル		HX のインストール時に定義されたユーザ。 事前定義された admin ユーザー。	HX のインストール時に指定。 強力なパスワードが必要です。	ストレージ クラスタ内のすべてのノードで一致している必要があります。 安全な admin シェルへの SSH のサポートは、ユーザー admin に制限されています。 インストール後、パスワードを変更するときは hxcli コマンドを使用します。
vCenter	admin	デフォルト：administrator@vsphere.local SSO 対応。 設定どおり（MYDOMAIN\name または name@mydomain.com）	SSO 対応。 設定どおり。	読み取り専用ユーザーは、HX Data Platform プラグインにアクセスできません。
ESXi サーバ	root	SSO 対応。 設定どおり。	SSO 対応。 設定どおり。	ストレージ クラスタ内のすべての ESX サーバで一致している必要があります。
ハイパーバイザ	root	root	HX のインストール時に指定。	HX のインストール後にパスワードを変更するには、vCenter または esxcli コマンドを使用します。
UCS Manager	admin	設定どおり。	設定どおり。	
ファブリック インターコネクト	admin	設定どおり。	設定どおり。	

HX Data Platform の名前、パスワード、文字

ほとんどの印刷可能 ASCII 文字と拡張 ASCII 文字を名前とパスワードに使用できます。ただし一部の文字は、HX Data Platform のユーザ名、パスワード、仮想マシン名、ストレージ コント

ローラ VM 名、およびデータストア名に使用できません。フォルダとリソース プールには、使用できない文字はありません。

パスワードは、少なくとも 1 つの小文字、1 つの大文字、1 つの数字、および次のうち 1 つの特殊文字を含む、10 文字以上で指定する必要があります。

アンパサンド（&）、アポストロフィ（'）、アスタリスク（*）、アットマーク（@）、バック スラッシュ（\）、コロン（:）、カンマ（,）、ドル記号（$）、感嘆符（!）、スラッシュ（/）、小なり記号（<）、大なり記号（>）、パーセント（%）、パイプ（|）、シャープ（#）、疑問符（?）、セミコロン（;）

特殊文字を入力するときは、使用するシェルを考慮してください。シェルによって、注意が必要な文字が異なります。名前またはパスワードに特殊文字がある場合は、引用符で囲んでください（例：'speci@lword!'）。フィールドから HyperFlex Installer パスワードの単一引用符内で、パスワードを入力する必要はありません。

HX ストレージ クラスタの名前

HX クラスタ名の最大文字数は 50 文字です。

HX ストレージ クラスタのホスト名

HX クラスタ ホスト名は 80 文字以内です。

仮想マシンとデータストアの名前

仮想マシン名、コントローラ VM 名、またはデータストア名の作成時にはほとんどの文字を使用できます。エスケープされた文字を、仮想マシン名、コントローラ VM 名、またはデータストア名に使用できます。

最大文字数：仮想マシン名には 80 文字まで使用できます。

除外される文字：スナップショットの対象となるユーザ仮想マシン名やデータストア名には、次の文字を使用しないでください。

- アクセント（`）

特殊文字：次の特殊文字を、ユーザの仮想マシンまたはデータストア名で使用できます。

- アンパサンド（&）、アポストロフィ（'）、アスタリスク（*）、アットマーク（@）、バック スラッシュ（\）、サーカムフレクス（^）、コロン（:）、カンマ（,）、ドル記号（$）、ドット（.）、二重引用符（"）、等号（=）、感嘆符（!）、スラッシュ（/）、ハイフン（-）、左波カッコ（{）、左丸カッコ（(）、左角カッコ（[）、小なり記号（<）、大なり記号（>）、パーセント（%）、パイプ（|）、プラス記号（+）、シャープ（#）、疑問符（?）、右波カッコ（}）、右丸カッコ（)）、右角カッコ（]）、セミコロン（;）、ティルダ（~）、アンダースコア（_）

ユーザ名の要件

ユーザ名として HX Data Platform のコンポーネントに固有のものを指定でき、UCS Manager のユーザ名要件を満たす必要があります。

UCS Manager ユーザ名の要件。

- 文字数：6 ～ 32 文字
- Cisco UCS Manager 内で一意である必要があります。
- 英文字から始まる必要があります。
- 英文字（大文字または小文字）が必要です。
- 数字を含めることができます。すべて数字にすることはできません。
- 特殊文字：アンダースコア（_）、ダッシュ（-）、およびドット（.）に限定

コントローラ VM パスワードの要件

コントローラ VM の root ユーザ/admin ユーザのパスワードには、次の規則が適用されます。

（注） パスワードに関する一般的な規則：コマンド文字列にパスワードを含めないでください。コマンドがパスワードの入力を求めることができる状態にします。

- 最小長：10
- 最小 1 大文字
- 最小で 1 つの大文字
- 最小で 1 つの数字
- 最小で 1 つの特殊文字
- 最大 3 回の再試行で新しいパスワードを設定

コントローラ VM のパスワードを変更するには、必ず `hxcli` コマンドを使用します。Unix パスワード コマンドなどの他のパスワード変更コマンドを使用しないでください。

1. 管理コントローラ VM にログインします。
2. `hxcli` コマンドを実行します。

   hxcli security password set [-h] [--user USER]

   変更は、HX クラスタですべてのコントローラ Vm に伝達されます。

UCS Manager および ESX のパスワード形式と文字の要件

UCS Manager と VMware ESXi のパスワードの形式と文字の要件の概要は次のとおりです。詳細については、Cisco UCS Manager および VMware ESX のドキュメントを参照してください。

- **文字クラス**：小文字、大文字、数字、特殊文字。

  パスワードは大文字と小文字が区別されます。

- **文字長**：最小 6、最大 80

  4 つすべての文字クラスの文字が含まれる場合は、6 文字以上が必要です。

  3 つ以上の文字クラスの文字が含まれる場合は、7 文字以上が必要です。

  1 つまたは 2 つの文字クラスの文字しか含まれない場合は、8 文字以上が必要です。

- **開始文字と終了文字**：パスワードの先頭の大文字またはパスワードの末尾の数字は文字数の合計に含まれません。

  パスワードが大文字で始まる場合は、2 つの大文字が必要です。パスワードが数字で終わる場合は、2 つの数字が必要です。

  要件を満たす例：

  h#56Nu：6 文字。4 クラス。大文字で始まっていません。数字で終わっていません。

  h5xj7Nu：7 文字。3 クラス。大文字で始まっていません。数字で終わっていません。

  XhUwPcNu：8 文字。2 クラス。大文字で始まっていません。数字で終わっていません。

  Xh#5*Nu：6 文字としてカウントされます。4 つの文字クラス。大文字で始まっています。数字で終わっていません。

  h#5*Nu9：6 文字としてカウントされます。4 つの文字クラス。大文字で始まっていません。数字で終わっています。

- **連続文字数**：最大 2。たとえば、hhh###555 は許容されません。

  ただし、VSphere SSO ポリシーでこの値を設定することは可能です。

- **除外文字**：

  UCS Manager のパスワードには、エスケープ（\）文字を使用できません。

  ESX パスワードには、これらの文字を使用できません。

  - ユーザ名と同じものやユーザ名を逆にしたものは使用できません。
  - 辞書に載っている単語は使用できません。
  - パスワードには、エスケープ文字（\）、ドル記号（$）、疑問符（?）、等号（=）を使用できません。

- **辞書に載っている単語**：

  辞書に載っている単語は使用しないでください。

AAA 認証 REST API

Cisco HyperFlex は、ストレージクラスタのリソースにアクセスするための REST API を提供します。AAA 認証 REST API は、ユーザを認証し、入力されるログイン情報とアクセス トーク

ンを交換するためのメカニズムを提供します。このアクセス トークンは他の REST API コール を呼び出すために使用できます。

認証 REST API (/auth) には、レート制限が適用されます。15 分のウィンドウでは、/auth は最大 5 回呼び出せます (正常に呼び出せた場合)。各ユーザは、取り消されていないトークンを最大 8 つ作成することができます。次に /auth を呼び出すと、新しいトークンの余地を設けるため、最も古い発行済みトークンが自動的に取り消されます。システムには、最大で 16 の取り消されていないトークンが存在できます。ブルートフォース攻撃を防ぐために、認証試行が 10 回連続で失敗した場合、ユーザアカウントは 120 秒間ロックされます。発行されたアクセス トークンは 18 日間 (1555200 秒) 有効です。

（注） HxConnect はログインのために /auth コールを使用します。この場合も同じ制限が適用されます。

HX Connect へのログイン

Cisco HyperFlex Connect は、HX ストレージのクラスタ モニタリング、およびレプリケーション、暗号化、データストア、および仮想マシンのタスクに対し、HTML5 ベースのアクセスを提供します。

セッションについて

HX Connectへの各ログインはセッションです。セッションは、HX Connect にログインした時からログアウトする時までの間のアクティビティの期間です。セッション中にブラウザの Cookie を手動でオフにしないでください。それにより、セッションもドロップされるためです。ドロップした場合でも、セッションを閉じるためにブラウザを閉じないでください。そのセッションは、引き続きオープンなセッションとしてカウントされます。デフォルトのセッションの最大値は次のとおりです。

- ユーザごとに 8 の同時セッション
- HX ストレージ クラスタ全体での 16 の同時セッション。

始める前に

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。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。
- vCenter 上の時間とコントローラ VM 上の時間が同期またはほぼ同期していることを確認します。vCenter の時間とクラスタの時間のずれが大きすぎると、AAA 認証は失敗します。

手順

ステップ 1 HX ストレージ クラスタ管理 IP アドレスを探します。

個々の Storage Controller VM ではなく、管理 IP アドレスの完全修飾ドメイン名（FQDN）を使用します。

ステップ 2 ブラウザで、HX ストレージ クラスタ管理 IP アドレスを入力します。

ステップ 3 HXストレージクラスタのログインクレデンシャルを入力します。

- **RBAC ユーザ**：次のロールに基づくアクセス制御（RBAC）ログインを Cisco HyperFlex Connect サポートします。
  - **管理者**：管理者ロールを持つユーザには、読み取りおよび変更操作の権限があります。これらのユーザは、HXストレージクラスタを変更できます。
  - **読み取り専用**：読み取り専用ロールを持つユーザには、読み取り（表示）権限があります。HXストレージクラスタに変更を加えることはできません。

  これらのユーザーは vCenter を介して作成されます。vCenter ユーザー名の形式は `<name>@domain.local` で、ユーザー プリンシパル名（UPN）形式で指定されています。例：`administrator@vsphere.local`。ユーザー名に「ad:」などのプレフィックスを追加しないでください。

- **HX 事前定義ユーザ**： HX データ プラットフォーム事前定義ユーザ `admin` または `root` を使用してログインするには、`local/` プレフィックスを入力します。例：`local/root` または `local/admin`。

  `local/` ログインで実行したアクションは、ローカル クラスタにのみ影響します。

  vCenter は HX Connect でセッションを認識します。このため vCenter で発生するシステム メッセージは `local/root` ではなくセッションのユーザを示す可能性があります。たとえば、アラームで、`Acknowledged By might list com.springpath.sysmgmt.domain-c7` と表示されます。

目のアイコンをクリックすると、パスワードフィールドのテキストが表示または非表示となります。このアイコンは、他のフィールド要素によって見えにくくなる場合があります。それでも、目のアイコンの領域をクリックすると、切り替え機能は動作します。

次のタスク

- HX Connect に表示されたコンテンツを更新するには、更新（円形）アイコンをクリックします。これによってページが更新されない場合は、キャッシュをクリアして、ブラウザをリロードします。
- HX Connect をログアウトして、適切にセッションを閉じるには、**[ユーザ（User）]** メニュー（右上）> **[ログアウト（Logout）]** を選択します。

コントローラ VM (hxcli) コマンド ラインへのログイン

すべての `hxcli` コマンドは、HX クラスタ情報を読み取るコマンドと HX クラスタを変更するコマンドに分かれています。

- 変更のコマンド：管理者レベルのアクセス許可が必要です。例：

  ```
  hxcli cluster create
  ```

  ```
  hxcli datastore create
  ```

- 読み取りのコマンド：管理者レベルのアクセス許可または読み取り専用レベルのアクセス許可で許可されます。例：

  ```
  hxcli <cmd> -help
  ```

  ```
  hxcli cluster info
  ```

  ```
  hxcli datastore info
  ```

HX Data Platform の `hxcli` コマンドを実行するには、HX Data Platform ストレージ コントローラ VM コマンド ラインにログインします。

重要 コマンド文字列にパスワードを含めないでください。コマンドは、プレーンテキストとしてログに頻繁に渡されます。コマンドからパスワードの入力を求められるまで待ちます。これは、ログイン コマンドだけでなく `hxcli` コマンドにも当てはまります。

ストレージ コントローラ VM の HX Data Platform コマンドライン インターフェイスには、次の方法でログインできます。

- コマンド ターミナルから
- HX Connect Web CLI ページから

  HX Connect では直接コマンドのみサポートされます。

  - 直接コマンド：1 回のパスで完了し、コマンド ラインを介した応答を必要としないコマンド。直接コマンドの例：`hxcli cluster info`
  - 間接コマンド：コマンドラインを介したライブ応答を必要とするマルチレイヤのコマンド。対話型コマンドの例：`hxcli cluster reregister`

手順

ステップ 1 コントローラ VM の DNS 名を探します。

1. **[VM]** > **[概要（Summary）]** > **[DNS 名（DNS Name）]** を選択します。

2. vSphere Web クライアント **[ホーム（Home）]** > **[VVM とテンプレート（VMs and Templates）]** > **[vCenter サーバ（vCenter server）]** > **データセンター** > **[ESX エージェント（ESX Agents）]** > **[VM]** から。
3. コントローラ VM のストレージ クラスタ リストにクリック スルーします。

ステップ 2 ブラウザから、DNS 名と `/cli` パスを入力します。

a) パスを入力します。

例

```
# cs002-stctlvm-a.eng.storvisor.com/cli
```

想定されるユーザ名：`admin`、パスワード： HX クラスタ作成時に定義。

b) プロンプトが表示されたら、パスワードを入力します。

ステップ 3 コマンド ライン ターミナルから `ssh` を使用します。

（注） `ssh` ログイン文字列にパスワードを含めないでください。ログインは、プレーンテキストとしてログに渡されます。

a) `ssh` コマンド文字列を入力します。

b) 証明書の警告が表示される場合があります。`yes` と入力して警告を無視して続行します。

```
------------------------------------------------------------
                  !!! ALERT !!!
This service is restricted to authorized users only.
All activities on this system are logged. Unauthorized
access will be reported.
------------------------------------------------------------
HyperFlex StorageController 2.5(1a)# exit
logout
Connection to 10.198.3.22 closed.]$ssh admin@10.198.3.24
The authenticity of host '10.198.3.24 (10.198.3.24)' can't be established.
ECDSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)?
```

c) プロンプトが表示されたら、パスワードを入力します。

```
# ssh admin@10.198.3.22
 HyperFlex StorageController 2.5(1a)
admin@10.198.3.22's password:
```

ステップ 4 [HX Connect] から：[HX Connect] にログインし、**[Web CLI]** を選択します。

（注） HX Connect Web CLI からは非対話型のコマンドのみを実行できます。

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。

手順

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。

```
# hxcli security password set
```

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

（注） 新しいコンピューティング ノードを追加し、**hxcli security password set** コマンドを使用してクラスタ パスワードを再設定しようとすると、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。

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。

Cisco HX Data Platform インストーラへのログイン

次に、HX Data Platform ソフトウェアをインストールします。

（注） Cisco HX Data Platform インストーラを起動する前に、ストレージ クラスタに含める予定の vCenter クラスタにあるすべての ESXi サーバがメンテナンス モードであることを確認します。

手順

ステップ 1 ブラウザで、HX データ プラットフォーム インストーラがインストールされた VM の URL を入力します。

このアドレスは、前のセクション「**HX Data Platform インストーラの展開**」で入手しています。たとえば、*http://10.64.4.254* です。

ステップ 2 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**（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。

EULA を読みます。[利用規約に同意します（I accept the terms and conditions）] をクリックします。

右下隅に記載された製品バージョンが正しいことを確認します。**[ログイン（Login）]**をクリックします。

ステップ 3 [HX Data Platform Installer Workflow] ページには、さらに移動するための 2 つのオプションがあります。

- **[クラスタの作成]** ドロップダウン リスト：標準のクラスタ、または拡張クラスタを展開できます。
- **クラスタ展開**：データを提供して、既存の標準的なストレージ クラスタにコンバージド ノードやコンピューティング ノードを追加できます。

SCVM のルート パスワードの復元

ルート パスワードを復元するために実行する唯一のオプションは、Linux シングル ユーザー モードを使用することです。

手順

Cisco TAC に連絡してこのプロセスを完了してください。

SCVM の管理パスワードの復元

HX 4.5(2c) および HX 5.0(2x) 以降では、RSA キーを使用して ESXi ホストから SSH を使用し、**recover-password** コマンドを実行することにより、ストレージ コントローラ VM（SCVM）Admin パスワードを回復できます。 このプロセスを完了するには、TAC に連絡する必要があります。

始める前に

同意トークン ワークフローをサポートするには、TAC にお問い合わせください。

手順

ステップ 1 SSH を使用して ESXi ホストにログインします。

ステップ 2 ESXi 7.0 および 8.0 の場合、**host_ecdsa_key** コマンドを使用して、ESXi から、パスワードを回復する必要があるストレージ コントローラ VM に SSH で接続します。

例：

```
[root@ucsblr625:~] ssh admin@`/opt/hxtools/bin/getstctlvmip.sh "Storage
 Controller Data Network"` -i /etc/ssh/ssh_host_ecdsa_key
The authenticity of host '10.21.24.89 (10.21.24.89)' can't be established.
```

```
ECDSA key fingerprint is SHA256:OkA9czzcL7I5fYbfLNtSI+D+Ng5dYp15qk/9C1cQzzk.
This key is not known by any other names

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.21.24.89' (ECDSA) to the list of known hosts.
 HyperFlex StorageController 5.5(1a)

This is a Restricted shell.
Type '?' or 'help' to get the list of allowed commands.
```

ステップ 3 `recover-password` コマンドを実行します。同意トークンを要求するプロンプトが表示されます。

（注） 同意トークンの提供については、TAC にお問い合わせください。

a) オプション 1 を入力してチャレンジを生成します。
b) 同意トークンをコピーします。
c) オプション 2 を入力して応答を受け入れます。
d) 同意トークンを入力します。
e) 管理者のための新しいパスワードを入力します。
f) 管理者のための新しいパスワードを再入力します。

例

```
admin:~$ recover-password
Consent token is needed to reset password. Do you want to continue?(y/[n]):
y
-----------------------------------
1.  Generate Challenge
2.  Accept Response
3.  Exit
-----------------------------------
Enter Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
**************************************BEGIN TOKEN*****************************************
2g9HLgAAAQEBAAQAAAABAgAEAAAAAQMACL7HPAX+PhhABAAQo9ijSGjCx+Kj+Nk1YrwKlQUABAAAAGQGAAlIeXBl
cmZsZXgHAAxIeXBlcmZsZXhfQ1QIAAlIWVBFUkZMRVgJACBhNzAxY2VhMGZlOGVjMDQ2NDllMGZhODVhODIyYTY2NA==
**************************************END TOKEN*******************************************
-----------------------------------
1.  Generate Challenge
2.  Accept Response
3.  Exit
-----------------------------------
Enter Option:
2
Starting background timer of 30 mins
Please input the response when you are ready:
Gu4aPQAAAQEBAAQAAAABAgAEAAAAAQMBYnlQdnRGY1NiNkhtOUlyanlDQVJic0ZXYnp3MVpzdm1pcVh3ZzJLSlZZSVl
yeXBydU9oejVQWkVXdlcvWWdFci8NCnBrVFVpS1d0dVRlczZ6TkdITXl0T3dNaFhaT2lrM3pKL1M5cDJqR0xxcGFOY1
Ruc05SVFNybCtQeGwvK1Z1b1gNCjBHYVVxcExXdUhtUUc0UG9ZU2FBL0lwelRFYzlaRmFNeUFmYUdkOThMSmliZnl2UF
c2d0tNY1FCM3lPWmRjU1ENCklGeWZJTVpKL1RWd1lOaERZT001dXQveHZxUU1HN1hTbjdXb2R4Wng2NVNqVktWK2lId
FMyZzdxZUIzc3R2TEgNCld1VWNYS3lWdFdOaXRiaHBvWUIwT1J0N2l3dHlrSkcyWldWbnk4KzZIUUNJbW9xdnFoSU91S
kk4aElsWWNNaUENCnlEbEpkQ0wwcHVObSswNVVyTWM0M1E9PQ==
Response Signature Verified successfully !
Response processed successfully.
Consent token workflow is successful, allowing password reset.
Enter the new password for admin:
Re-enter the new password for admin:
Changing password for admin...
Password changed successfully for user admin.
```

recover-password コマンドを使用してパスワードを変更すると、パスワードはすべてのノードで同期されなくなります。すべてのノードでパスワードを再度変更および同期するには、**hxcli security password set** を使用する必要があります。

ステップ 4 すべてのノードでパスワードを同期するには、任意のノードから **hxcli security password set** コマンドを実行し、新しいパスワードを入力します。

例

```
admin:~$ hxcli security password set
Enter new password for user admin:
Re-enter new password for user admin:
admin:~$
```

HX Data Platform REST API へのアクセス

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 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。

HTTP 動詞を使用した Cisco HyperFlex System RESTful API は、HTTP 呼び出しを実行するように構成できる他のサードパーティ製の管理および監視ツールと統合されています。また、オンデマンド ステートレス プロトコルを介した HyperFlex システムの認証、レプリケーション、暗号化、監視、および管理を可能にします。この API を使用すれば、外部アプリケーションを HyperFlex の管理プレーンと直接インターフェイスさせることができます。

これらのリソースには URI（Uniform Resource Identifier）を介してアクセスし、これらのリソースに対する操作は POST（作成）、GET（読み取り）、PUT（更新）、DELETE（削除）などの HTTP 動詞を使用して実行します。

REST API は、Python、JAVA、SCALA、Javascript などのさまざまな言語でクライアント ライブラリを生成することも可能な Swagger を使用して記述されます。このように生成したライブラリを使用して、HyperFlex リソースを使用するためのプログラムとスクリプトを作成できます。

HyperFlex は、組み込み REST API アクセス ツールである REST エクスプローラも備えています。このツールは、リアルタイムで HyperFlex リソースにアクセスし、応答を監視するために使用します。REST エクスプローラは、コマンドラインから実行可能な CURL コマンドも生成します。

手順

ステップ 1 ブラウザを開いて、https://developer.cisco.com/docs/ucs-dev-center-hyperflex/ DevNet アドレスにアクセスします。

ステップ 2 [Login] をクリックし、必要に応じてクレデンシャルを入力します。

Secure Admin Shell

Starting with Cisco HX Release 4.5(1a), limiting access provides the following:

- Controller VMs from outside the clusters through remote **root** access over SSH is disabled.
- Admin users have limited shell access with only restricted commands available. To know the allowed commands in the admin shell, execute **priv** and **help** or **?** commands.
- Access is only available through local **root** Consent Token process.
- Logging into the root shell of a controller, for troubleshooting purposes, requires Cisco TAC to be involved.

Administrators of HX clusters deployed in air-gapped networks can enable a persistent root shell on the HX Controller VM command line interface (CLI) after a one-time authentication with Consent Token (CT) with assistance from Cisco TAC. This enables an authenticated user on the CLI to switch user to root thereafter without further intervention by TAC. For more information, see Facilitating Controller VM Root Access for Air-Gapped Clusters in the Cisco HyperFlex Systems Installation Guide for VMware ESXi, Release 5.0.

注意事項と制約事項

- クラスタ外からコントローラVMへのSSH経由のリモートルートアクセスは無効になります。クラスタの一部のノードのみが、データネットワークを介して他のノードへのルートとしてSSH接続できます。
- 同意トークンの生成中または生成前にESXノードをメンテナンスモード（MM）にすると、そのSCVMでトークンを使用できなくなり、ノードがMMになりSCVMがオンラインに戻った後に同期ユーティリティを起動する必要があります。
- HX リリース 4.0(x) 以前のクラスタにルート対応ユーザが存在する場合は、HX リリース 4.5(1a) へのアップグレードを開始する前に削除します。ルート対応ユーザーが削除されない場合、アップグレードは続行されません。

同意トークンに関する情報

同意トークンは、管理者と Cisco Technical Assistance Centre（Cisco TAC）の相互の同意により、システム シェルにアクセスする組織のシステム ネットワーク管理者を認証するために使用されるセキュリティ機能です。

一部のデバッグシナリオでは、Cisco TAC エンジニアが特定のデバッグ情報を収集したり、実稼働システムでライブデバッグを実行する必要がある場合があります。このような場合、Cisco TACエンジニアは、デバイスのシステムシェルにアクセスするようユーザー（ネットワーク管理者）に依頼します。同意トークンは、システムシェルへの特権アクセス、制限アクセス、およびセキュアアクセスを提供する、ロック、ロック解除、および再ロックのメカニズムです。

セキュアシェル限定アクセスの場合、ネットワーク管理者とCisco TACが明示的な同意を提供する必要があります。Admin としてログインすると、admin として診断コマンドを実行するか、または TAC 支援を要求して **root** シェルを要求することができます。**root** シェル アクセスは、HyperFlex データ プラットフォーム内の問題のトラブルシューティングと修正のみを目的としています。

TAC が必要なトラブルシューティングを完了したら、同意トークンを無効にして root アクセスを無効にすることを推奨します。

diag ユーザーの概要

HX 5.0(2a) 以降、HyperFlex のコマンド ライン インターフェイスである HX シェルに、新しく「diag」ユーザーが導入されました。このアカウントは、トラブルシューティング用に設計され、昇格された権限を持つ、ローカルユーザーアカウントです。HXシェルへのログインは引き続き「admin」ユーザー アカウントに制限されています。ログイン後、diag ユーザーのへの切り替えコマンド（su）を入力し、パスワードを入力し、CAPTCHA テストに合格することにより、「diag」ユーザーに切り替える必要があります。「diag」ユーザーを使用する場合は、次の点に注意してください。

- admin ユーザーよりは権限が緩いものの、root ユーザーより制限されている
- bash をデフォルトのシェルとして使用して、lshell の制限を緩和できます
- 管理シェルから **su diag** を実行することによってのみアクセスできます。ssh により diag への直接ログインを試みると、ブロックされます。
- diag のパスワードを入力すると、CAPTCHA テストが表示されます。diag シェルに入るには、正しい CAPTCHA を入力する必要があります。
- 書き込み権限は、diagユーザー向けに事前定義されたファイルセットに制限されています

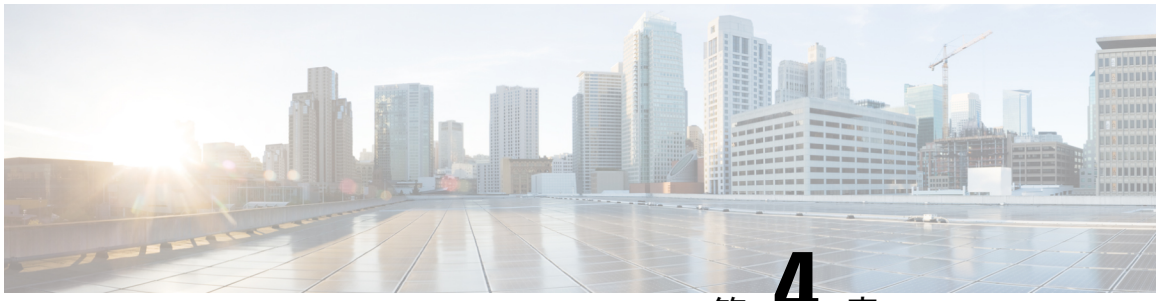
システム ソフトウェアを変更する可能性のあるコマンドは、「diag」ユーザーではブロックされます。ブロックされるコマンドのデフォルトのリストは次のとおりです。

- **sudo**
- **apt-get**

- **li**
- **dpkg**
- **apt**
- **easy_install**
- **setfacl**
- **adduser**
- **deluser**
- **userdel**
- **groupadd**
- **groupdel**
- **addgroup**
- **delgroup**

次に、**diag user** コマンドの出力例を示します。

```
This is a Restricted shell.
Type '?' or 'help' to get the list of allowed commands.
hxshell:~$ su diag
Password:
 _____          ____            _  _ _                          _
| ___|    _    |___ \          | \ | (_)_ __  ___     _    / |
|___ \   _| |_    __) | _____  |  \| | | '_ \ / _ \ _| |_  | |
 ___) | |_  _| / __/ |_____| | |\  | | | | | __/ |_  _| | |
|____/    |_|  |_____|       |_| \_|_|_| |_|\___|  |_|  |_|


Enter the output of above expression: -1
Valid captcha
diag#
```



第 4 章

HX ストレージ クラスタのモニタリング

HyperFlex クラスタのモニタリング

この章では、次の HX Storage Cluster インターフェイスを通じて利用できるモニタリングの内容について説明します。

- Cisco HX Connect
- Cisco HX データ プラットフォーム プラグイン
- ストレージ コントローラ VM のコマンド ライン

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、すべての機能と構成の変更には、有効な Cisco HyperFlex ソフトウェア ライセンスが必要です。評価の終了時またはライセンス準拠日の後の猶予期間に期限切れ、または不十分なライセンスを持つ HX Connect ユーザーには、ライセンス準拠の必要性を警告する目立つカウントダウン バナーが表示され、ライセンスの期限切れが解消されるまでるまでライセンス更新ページへのリンクが提供されます。

ライセンスがその有効期限日と猶予期間のカウントダウンの両方の期限日を過ぎた場合、現在の構成は限られた情報で動作します。ライセンスを更新すると、ユーザーはすべての機能を再開し、構成を変更できます。バナーの詳細と例については、『Cisco HyperFlex Systems Ordering and Licensing Guide』の「License Compliance and Feature Functionality」セクションを参照してください。

シスコ エンドユーザー ライセンス契約（Cisco EULA）を確認するには、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。

HX Connect を使用した HyperFlex クラスタのモニタリング

Cisco HX Connect ユーザー インターフェイスは、Cisco HX ストレージ クラスタのステータス、コンポーネント、および暗号化やレプリケーションなどの機能のビューを提供します。

主要なモニタリング ページには、ローカルの Cisco HX ストレージ クラスタに関する情報が含まれています。

- **[ダッシュボード（Dashboard）]**：Cisco HXストレージ クラスタ ステータスの概要です。
- アラーム、イベント、アクティビティ：詳細については、『Cisco HyperFlex システム トラブルシューティング リファレンス ガイド』を参照してください。https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-troubleshooting-guides-list.html
- **[パフォーマンス（Performance）]**：IOPS、スループット、遅延、およびレプリケーション ネットワーク帯域幅のグラフ。
- **[システム情報 (System Information)]**：ノードとディスクのデータを含めた HX ストレージ クラスタ システムに関連する情報を表示し、HXDP メンテナンス モードにアクセスします。

  『Cisco HyperFlex システム トラブルシューティング リファレンス ガイド』には、バンドルの生成方法、ストレージ クラスタ メンテナンス操作の概要 （85 ページ）メンテナンス モードの開始と終了方法、および ビーコンの設定 （88 ページ） ノードまたはディスク ビーコンを設定する方法について記されています。
- [データストア（Datastores）]：データストアのステータスと関連タスク。
- [仮想マシン（Virtual Machines）]：仮想マシンのステータスと仮想マシン保護に関連するタスク

さらに、次の Cisco HX Connect ページから管理機能にアクセスできます。

- [暗号化（Encryption）]：ディスクおよびノードに保存されるデータの暗号化タスク。
- [レプリケーション（Replication）]：ディザスタ リカバリでの VM 保護タスク。

[アップグレード（Upgrade）] ページでは、HX Data Platform および Cisco UCS Manager ファームウェア アップグレード タスクにアクセスできます。

[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。
[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、『**VMware ESXi の 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。 HXDP リリース 5.0(2a) 以降、ライセンスが期限切れまたは不十分な HX Connect ユーザーは、特定の機能にアクセスできないか機能が制限されます。詳細については、 ライセンスの遵守とフィーチャの機能 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。

UI 要素	基本的な情報
VM セクション	クラスタ内の VM の総数と、VM の内訳をステータス（電源オン/オフ、一時停止、スナップショットのある VM およびスナップショットスケジュールのある VM）別に表示します。
[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。

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。

[Activity (アクティビティ)] ページ

HX ストレージ クラスタ上の最近のアクティビティのリストを表示します。これにより、VM の動作、クラスタのアップグレード/拡張、メンテナンス モードの開始/終了、およびリカバリ ジョブの進捗状況をモニタできます。

UI 要素	基本的な情報
[アクティビティ（Activity）] リスト	最近のタスクのリストと、次の詳細が表示されます。 • ID • 説明 • VM 電源のオン/オフ/一時停止ステータス • タスクのステータス： • **進行中** • **成功** • **失敗** VM 電源の操作に失敗した場合は、**[既存の状態（Existing State）]** フィールドと **[必要な状態（Required State）]** フィールドも表示されます。 • 日時スタンプ • 進捗バー 展開されたリストには、タスクの手順名とステータスが表示されます。 コンテンツを今すぐ更新し、最近のアクティビティを取得するには、円形のアイコンをクリックします。ページは 2 分ごとに自動的に更新されます。

UI 要素	基本的な情報
[リカバリ (Recovery)] リスト	次の詳細を含む、リカバリ関連のすべてのジョブ (移行、リカバリ、テスト リカバリ、再保護など) の進行状況を表示します。 • ID • 説明 • タスクのステータス： **• 進行中** **• 成功** **• 失敗** • 日時スタンプ • 進捗バー 展開されたリストには、タスクの手順名とステータスが表示されます。 コンテンツを今すぐ更新し、最近のアクティビティを取得するには、円形のアイコンをクリックします。ページは 2 分ごとに自動的に更新されます。
[すべて展開/すべて折り畳む（Expand All/Collapse All）] ボタン	ジョブ リストのビューを切り替えて、最上位のタスク情報またはタスク詳細を表示します。 個別のタスクを展開したり折りたたんだりすることもできます。

次の表に、[アクティビティ（Activity）]ページでHXタスクを作成するスナップショット操作を示します。

表 *3:* アクティビティ ページで *HX* タスクを作成するスナップショット操作

操作	アクティビティページでの HX タスクの作成
HX プラグインからの Ready Clone	HX タスクが作成されていません。
HX Connect からの Ready Clone	HX タスクが [アクティビティ（Activity）] ページに追加されました。
HX プラグインからのスケジュールされたスナップショットタスクの作成	HX タスクが作成されていません。
HX Connect からのスケジュールされたスナップショットタスクの作成	HX タスクが [アクティビティ（Activity）] ページに追加されました。

スケジュールスナップショットからのスナップショットの作成	HX タスクが [アクティビティ（Activity）] ページに追加されました。
HX プラグインからのスナップショット	HX タスクが作成されていません。
HX Connect からのスナップショット	HX タスクが [アクティビティ（Activity）] ページに追加されました。

[システム情報（System Information）] 概要ページ

ノードとディスクを含め、HX ストレージ クラスタのシステム関連の情報が表示されます。また、ここから HXDP メンテナンス モードにアクセスできます。

HX ストレージ クラスタ構成データ (HX Storage Cluster Configuration Data)

この HX ストレージ クラスタの基本構成情報が表示されます。

UI 要素	基本的な情報
[HX ストレージ クラスタ (HX storage cluster)] フィールド	ストレージ クラスタの名前。
[Cluster License Status（クラスター ライセンスの状態）] 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、**[今すぐ登録 (Register Now)]** リンクが表示されます。 **[今すぐ登録 (Register Now)]** リンク：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、**[Smart Software Licensing Product Registration (スマート ソフトウェア ライセンス製品登録)]** 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、『**VMware ESXi の 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。 （注） クラスタ ライセンスを登録するには、**[アクション (Actions)]** ドロップダウン フィールドから **[クラスタの登録 (Register Cluster)]** を選択することもできます。

UI 要素	基本的な情報
[ライセンスの使用状況 (License Usage)] セクション	• **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。 HXDP リリース 5.0(2a) 以降、ライセンスが期限切れまたは不十分な HX Connect ユーザーは、特定の機能にアクセスできないか機能が制限されます。詳細については、ライセンスの遵守とフィーチャの機能を参照してください。 • 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。 （注） ライセンス証明書を更新するか、ライセンス認証を更新するには、**[アクション (Actions)]** ドロップダウン フィールドからそれぞれのオプションを選択します。
[HX ストレージ クラスタ ステータス (HX storage cluster status)] フィールド	HX ストレージ クラスタの機能ステータスが示されます。 • **[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（Read Only）]**：クラスタは領域外です。 • **[不明（Unknown）]**：クラスタがオンラインになるまでの遷移状態。

UI 要素	基本的な情報
[vCenter] リンク	この HX ストレージ クラスタに関連付けられている VMware vSphere のセキュア URL。リンクをクリックして vSphere Web クライアントにリモート アクセスします。
[ハイパーバイザ（Hypervisor）] フィールド	この HX ストレージ クラスタにインストールされているハイパーバイザのバージョン。
[HXDP バージョン（HXDP Version）] フィールド	この HX ストレージ クラスタにインストールされているインストーラ パッケージのバージョン。
[データ レプリケーション ファクタ（Data Replication Factor）] フィールド	この HX ストレージ クラスタに保存されている冗長データ レプリカの数。
[稼働時間（Uptime）] フィールド	この HX ストレージ クラスタがオンラインであった期間。
[合計容量（Total Capacity）] フィールド	このクラスタ全体のストレージ サイズ。
[使用可能な容量（Available Capacity）] フィールド	このクラスタの空きストレージの容量。
[DNSサーバ（DNS Server(s)）]	この HX ストレージ クラスタの DNS サーバの IP アドレス。
NTPサーバ	この HX ストレージ クラスタの NTP サーバの IP アドレス。

コントローラ VM アクセス

アクションを使用して、管理者としてSSHを使用してコントローラVMにアクセスし、**SSHを介したコントローラアクセスの有効化**、**SSHを介したコントローラアクセスの無効化**、またはライセンスの登録などのアクションを実行します。

（注） SSH を有効または無効にするアクションは、ローカル ユーザーではなく、**ドメイン** ユーザーのみが実行できます。ドメイン ユーザーは、VC（ESXi）のユーザーです。

UI 要素	基本的な情報
SSH を介したコントローラのアクセスを無効化	セキュアシェル（SSH）は、デフォルトでは無効にされています。
今すぐ登録	ライセンスを登録します。
vCenterの再登録	vCenter 経由でライセンスを再登録

UI 要素	基本的な情報
セキュアブートステータスの確認	セキュアブートステータスの確認

ディスク ビューのオプション

ディスク ビューの表示をカスタマイズします。[ノード データ（Node Data）] セクションに表示されるフィールドを選択および選択解除するには、チェックボックス リストを使用します。

ディスク ビューの凡例

ディスクの凡例アイコンと説明を表示するには、**[ディスク表示の凡例]** をクリックします。

ノード データ（Node Data）

このHXストレージクラスタ内の各ノードに関するデータが表示されます。この情報を表形式で表示するには、**[ノード（Nodes）]** ページに移動します。

UI 要素	基本的な情報
ノード（Nodes）	このクラスタ上のノードの名前です。
モデル（Model）	このノードの物理ハードウェアのモデル番号です。
ディスク	このノードの永続的なディスクに対するキャッシュ ディスクの数です。
ノード ステータス	• オンライン • オフライン • メンテナンス中 • Healthy • 警告
HXDP バージョン	このクラスタにインストールされている HyperFlex データ プラットフォームのバージョン。
タイプ	• ハイパーコンバージド • コンピューティング
ハイパーバイザ ステータス	• オンライン • オフライン • メンテナンス中 • 進行中

UI 要素	基本的な情報
ハイパーバイザ アドレス	この HX ストレージ クラスタの管理ネットワークで使用する IP アドレスです。
ディスクの概要	各ノードで使用中のディスクの数、使用タイプ、および空のスロットの数のグラフィック表示。 （注） 赤色のアイコンが付いたディスク アウトラインは、認識されず、カタログのアップグレードが必要なディスクを示します。

ディスクがあるノードでは、ディスクの上にカーソルを置くと、次のような情報がインタラクティブに表示されます。

ディスク

UI 要素	基本的な情報
スロット番号	ドライブの場所 (たとえば、スロット番号 2)。
ディスクのタイプ	• システム（System） • Cache • 永続
ディスクの状態	• 請求済み • 応対可 • 無視 • ブロック • OK して削除 • 不明
ロケータ LED	ディスクを特定しやすくするためにホスト上の物理的なライトをアクティブにします。オプションは、[オン（On）] と [オフ（Off）] です。
容量	ディスク サイズの合計です。
[使用済み/総容量 (Used / Total Capacity)] (永続ディスクのみ)	合計ディスク サイズに対する使用されているディスクの容量です。
シリアル番号（Serial Number）	このディスクの物理シリアル番号です。

UI 要素	基本的な情報
[ストレージ使用率 (Storage Usage)] (永続ディスクのみ)	使用されているディスク ストレージの割合です。
バージョン	ディスク ドライブのバージョン。
ディスク ドライブ インターフェイス	ディスク ドライブのインターフェイス タイプ (たとえば、SAS または SATA)。

[ノード（Nodes）] ページ

表にこのHXのストレージクラスタ内のすべてのノードに関するデータが表示されます。それぞれの列（カラム）を基準にデータをソートできます。

UI 要素	基本的な情報
[HXDP メンテナンス モードの開始（Enter HXDP Maintenance Mode）] ボタン	このボタンにアクセスするノードを選択します。 **[HXDP メンテナンス モードの確認（Confirm HXDP Maintenance Mode）]** ダイアログボックスが開きます。
[HXDP メンテナンス モードの終了（Exit HXDP Maintenance Mode）] ボタン	このボタンにアクセスするノードを選択します。 すべてのメンテナンス タスクを完了した後、手動で HXDP メンテナンス モードを終了する必要があります。
[ノード（Node）] カラム	この HX ストレージ クラスタ内のノードの名前。
[ハイパーバイザ アドレス（Hypervisor Address）] カラム	[ノード (Node)] 列で参照されるノードの管理ネットワークの IP アドレス。
[Hypervisor Status] カラム	• **[オンライン (Online)]** ：ノードは使用できます。 • **[オフライン (Offline)]** ：ノードは使用できません。 • **メンテナンス中**：実行中 (および電源がオフ) になっているノードは、ホストから切断されています。 • **[進行中 (In Progress)]** ： バックアップ ジョブが進行中です。
[Controller Address] カラム	[ノード (Node)] 列で参照されるノードの HX ストレージ コントローラ VM の IP アドレス。

UI 要素	基本的な情報
[Controller Status] カラム	• **[オンライン (Online)]**：VM とディスクの間の接続を使用できます。 • **[オフライン (Offline)]**：VM とディスク間の接続は使用できません。 • **[メンテナンス中 (In Maintenance)]**：VM とディスクの間の接続はホストから電源がオフになります。
[モデル（Model）] カラム	このノードの物理ハードウェアのモデル番号。
[バージョン（Version）] カラム	このノードにインストールされている HyperFlex Data Platform インストーラ パッケージのバージョン。
[ディスク（Disks）] カラム	ノード内のディスクの数。 数値をクリックすると、選択されたノード名でフィルタリングされた **[ディスク（Disks）]** ページが開きます。

[ディスク（Disks）] ページ

7 列のテーブルに、この HX ストレージ クラスタ内のすべてのディスクに関するデータが表示されます。それぞれの列（カラム）を基準にデータをソートできます。

UI 要素	基本的な情報
[ノード（Node）] カラム	ディスクが存在するノードの名前。
[スロット（Slot）] カラム	SED ドライブの場所。これは、メンテナンス作業のためにドライブを識別します。
[容量（Capacity）] カラム	ディスクの合計サイズ。

UI 要素	基本的な情報	
[ステータス（Status）] カラム		次の状態は無視しても構いません。 • 無効（Invalid） • 標準 • [削除済み（Removed）]：[安全に消去する（Secure Erase）] オプションを使用した後に SED ディスクが削除されるときの状態です。 • タイムアウト • 不明

UI 要素	基本的な情報	
	• **[クレーム済み（Claimed）]**：ディスクが認識され、使用中の状態です。 • **[利用可能（Available）]**：新しく追加された、保管中データ対応のディスクの初期状態です。また、ディスクが他のいずれかの状態に移るときの遷移状態でもあります。 • **[無視（Ignored）]**：ディスクがクラスタによって使用されていない状態です。たとえば、HX コントローラ VM システム ディスク、他のデータ（有効なファイル システム パーティション）を含むディスク、または I/O の障害が発生しているディスクです。 • **[ブロック済み（Blocked）]**：ソフトウェアのエラーまたは I/O エラーが原因でディスクがクラスタによって使用されていないときの状態です。これは、まだ利用可能なディスクをクラスタが修復しようとしたときに **[修復（Repairing）]** 状態に移行する前の遷移状態である可能性があります。 • **[削除 OK（Ok To Remove）]**：これは、**[安全に消去する（Secure Erase）]** オプションを使って SED ディスクがすでに安全に消去されており、安全に削除できる状態です。 • **[修復（Repairing）]**：ブロック済みディスクが現在修復されている状態です。 • **[削除対象（To Be Removed）]**：ディスクが RMA にスケジュールされているとき	

UI 要素	基本的な情報
	の状態です。
[暗号化（Encrypted）] カラム	• **[有効（Enabled）]**：この保管中データ対応ディスクの暗号化が設定されています。 • **[無効（Disabled）]**：この保管中データ対応ディスクの暗号化は設定されていません。この状態は、新しいディスクが存在するものの、キーがまだ適用されていない場合に発生します。 • **ロック済み** • **不明**
[タイプ（Type）] カラム	• **不明** • **[循環（Rotational）]**：ハイブリッド ドライブ • **[ソリッド ステート（Solid State）]**：SSD ドライブ
使用状況（Usage）] カラム	• **不明** • **Cache** • **永久的（Persistent）**
[ロケータをオンにする（Turn On Locator LED）] および **[ロケータ LED をオフにする（Turn Off Locator LED）]** オプション ボタン	ディスクを 1 つ選択してオプション ボタンにアクセスします。 ディスクを探すために役立つホスト上の物理光またはビーコンをアクティブ化または非アクティブ化します。
（任意）**[安全に消去する（Secure erase）]** ボタン	このボタンは、HX ストレージ クラスタがローカル キー暗号を使って暗号化されている場合にのみ表示されます。 ディスクを 1 つ選択してこのボタンにアクセスします。 クラスタで使用中の暗号キーを入力し、**[安全に消去する（Secure Erase）]** をクリックしてから、**[はい、このディスクを消去します（Yes, erase this disk）]** をクリックしてローカル暗号キーを安全に消去します。

HX Connect を使用した監査ロギング

監査ロギングは、すべての監査ログをリモート syslog サーバに保存することを意味します。現在、各コントローラ VM は監査ログを保存していますが、これらのログは無期限に保存される

わけではありません。ログは、コントローラ VM に設定されている保持ポリシーに基づいて上書きされます。監査ログを保存するようにリモート syslog サーバを設定することにより、ログが長期間保持できます。

次に、リモート syslog サーバにエクスポートできる監査ログを示します。

- REST 関連のログ
  - /var/log/springpath/audit-rest.log
  - /var/log/springpath/hxmanager.log
  - /var/log/springpath/hx_device_connector.log
  - /var/log/shell.log
  - /var/log/springpath/stSSOMgr.log
  - /var/log/springpath/hxcli.log
- /var/log/nginx/ssl-access.log

監査ロギングを有効にすると、これらのログはリモート syslog サーバにエクスポートされます。コントローラ VM からのログがリモート sylog サーバにプッシュされていない場合、またはリモート syslog サーバに到達できない場合は、HX 接続ユーザー インターフェイスでアラームが生成されます。ただし、HX 接続はリモート syslog サーバで使用可能なディスク領域をモニタしません。リモート syslog サーバのディスクが満杯の場合、HX 接続ユーザー インターフェイスでアラームが表示されません。

注目

- 監査ロギングを有効にできるのは、管理者ユーザーのみです。
- コンピューティング専用ノードと監視ノードからのログは、リモート syslog サーバにプッシュされません。

監査ロギングを有効にした後、監査ロギングを一時的に無効にするか、または監査ロギングサーバ設定の詳細を削除するかを選択できます。

監査ロギングの有効化

始める前に

- リモート syslog サーバを設定します。HX Connect で監査ロギングを有効にするには、サーバ IP、ポート番号、証明書ファイルなどのサーバの詳細を設定する必要があります。
- コントローラ VM とリモート syslog サーバとの間に暗号化された接続を設定するには、コントローラ VM で syslog クライアントの自己署名証明書または CA 署名付き証明書と秘密キーを生成する必要があります。

- さまざまなタイプのログをそれぞれのファイルに分類するようにリモート syslog サーバを設定します。

手順

ステップ 1 **[Settings (設定)]** > **[Audit Log Export Settings (監査ログ エクスポート設定)]** を選択します。

ステップ 2 **[Enable audit log export to an external syslog server (監査ログ エクスポートを外部 sysylog サーバに有効にする)]** チェック ボックスをチェックします。

ステップ 3 次の詳細を入力します。

UI 要素	基本的な情報
Syslog サーバ	Syslog サーバの IP アドレスを入力します。
Port	syslog サーバのポート番号を入力します。
[接続タイプ (Connection Type)] ドロップダウン リスト	接続タイプとして **[TLS]** または **[TCP]** を選択します。デフォルト値と推奨値は TLS です。TLS 接続タイプは、TLS を介した暗号化されている転送用です。TCP 接続タイプは、TCP を介した暗号化されていない転送用です。
クライアント証明書	**[Choose (選択)]** をクリックして、コントローラ VM に保存する必要がある証明書ファイルを検索します。この証明書により、コントローラ VM とリモート syslog サーバの間に TLS 接続を作成します。TLS 接続によって、ログ ファイルが確実に暗号化されます。 ユーザーが生成した自己署名証明書または CA 署名付き証明書のいずれかをアップロードする必要があります。
秘密キー（Private Key）	**[Choose (選択)]** をクリックして、コントローラ VM に保存する必要がある生成されたプライベート キーファイルを検索します。このキーにより、コントローラ VM とリモート syslog サーバの間に TLS 接続を作成します。 Syslog サーバの証明書と秘密キーを選択すると、ログ ファイルが確実に暗号化されます。Syslog サーバの証明書は、CA 証明書または自己署名証明書のいずれかにすることができます。
自己署名証明書を使用しますか?	Syslog サーバが自己署名証明書を使用する場合は、このチェックボックスをオンにします。 **[Choose (選択)]** をクリックして、syslog サーバの自己署名証明書を検索します。

ステップ 4 **[OK]** をクリックします。

リモート syslog サーバの設定

監査ロギングを有効にする前に、リモートsyslogサーバに設定ファイルを作成して、異なるログファイルを別々のファイルに分類する必要があります。/Etc/syslog-ng/conf.dディレクトリの hx-audit.conf というタイトルのファイルを作成できます。

次に、syslog サーバとの暗号化された接続を確立するための設定ファイルの例を示します。

```
## Audit Logging Configuration ###
    source demo_tls_src {
            tcp(ip(0.0.0.0) port(6515)
                tls(
                     key-file("/etc/syslog-ng/CA/serverkey.pem")
                     cert-file("/etc/syslog-ng/CA/servercert.pem")
                     peer-verify(optional-untrusted)
                )
            ); };


    filter f_audit_rest { match("hx-audit-rest" value("MSGHDR")); };
    filter f_device_conn { match("hx-device-connector" value("MSGHDR")); };
    filter f_stssomgr { match("hx-stSSOMgr" value("MSGHDR")); };
    filter f_ssl_access { match("hx-ssl-access" value("MSGHDR")); };
    filter f_hxmanager { match("hx-manager" value("MSGHDR")); };
    filter f_hx_shell { match("hx-shell" value("MSGHDR")); };
    filter f_hxcli { match("hx-cli" value("MSGHDR")); };

    destination d_audit_rest { file("/var/log/syslog-ng/audit_rest.log"); };
    destination d_device_conn { file("/var/log/syslog-ng/hx_device_connector.log"); };
    destination d_stssomgr { file("/var/log/syslog-ng/stSSOMgr.log"); };
    destination d_ssl_access { file("/var/log/syslog-ng/ssl_access.log"); };
    destination d_hxmanager { file("/var/log/syslog-ng/hxmanager.log"); };
    destination d_hx_shell { file("/var/log/syslog-ng/shell.log"); };
    destination d_hxcli { file("/var/log/syslog-ng/hxcli.log"); };

    log { source(demo_tls_src); filter(f_audit_rest); destination(d_audit_rest);
flags(final); };
    log { source(demo_tls_src); filter(f_device_conn); destination(d_device_conn);
flags(final); };
   log { source(demo_tls_src); filter(f_stssomgr); destination(d_stssomgr); flags(final);
 };
    log { source(demo_tls_src); filter(f_ssl_access); destination(d_ssl_access);
flags(final); };
    log { source(demo_tls_src); filter(f_hxmanager); destination(d_hxmanager);
flags(final); };
   log { source(demo_tls_src); filter(f_hx_shell); destination(d_hx_shell); flags(final);
 };
    log { source(demo_tls_src); filter(f_hxcli); destination(d_hxcli); flags(final); };

########################
```

次に、リモート syslog サーバとの TCP 接続を確立するための設定ファイルの例を示します。

```
######################
## Audit Logging Configuration ###
    source demo_tls_src {
            tcp(ip(0.0.0.0) port(6515)
            ); };

    filter f_audit_rest { match("hx-audit-rest" value("MSGHDR")); };
    filter f_device_conn { match("hx-device-connector" value("MSGHDR")); };
    filter f_stssomgr { match("hx-stSSOMgr" value("MSGHDR")); };
    filter f_ssl_access { match("hx-ssl-access" value("MSGHDR")); };
```

```
    filter f_hxmanager { match("hx-manager" value("MSGHDR")); };
    filter f_hx_shell { match("hx-shell" value("MSGHDR")); };
    filter f_hxcli { match("hx-cli" value("MSGHDR")); };

    destination d_audit_rest { file("/var/log/syslog-ng/audit_rest.log"); };
    destination d_device_conn { file("/var/log/syslog-ng/hx_device_connector.log"); };
    destination d_stssomgr { file("/var/log/syslog-ng/stSSOMgr.log"); };
    destination d_ssl_access { file("/var/log/syslog-ng/ssl_access.log"); };
    destination d_hxmanager { file("/var/log/syslog-ng/hxmanager.log"); };
    destination d_hx_shell { file("/var/log/syslog-ng/shell.log"); };
    destination d_hxcli { file("/var/log/syslog-ng/hxcli.log"); };

    log { source(demo_tls_src); filter(f_audit_rest); destination(d_audit_rest);
flags(final); };
    log { source(demo_tls_src); filter(f_device_conn); destination(d_device_conn);
flags(final); };
   log { source(demo_tls_src); filter(f_stssomgr); destination(d_stssomgr); flags(final);
 };
    log { source(demo_tls_src); filter(f_ssl_access); destination(d_ssl_access);
flags(final); };
    log { source(demo_tls_src); filter(f_hxmanager); destination(d_hxmanager);
flags(final); };
   log { source(demo_tls_src); filter(f_hx_shell); destination(d_hx_shell); flags(final);
 };
    log { source(demo_tls_src); filter(f_hxcli); destination(d_hxcli); flags(final); };

########################
```

監査ロギングの無効化

監査ロギングを一時的に無効にするようを選択できます。これにより、以前に設定したサーバ IP やポートなどのリモート syslog サーバの詳細がシステムに保持されます。後で監査ロギングを再度有効にする場合は、サーバの詳細を再度入力する必要はありません。監査ロギングを有効にするために必要なのは、証明書と秘密キー ファイルをアップロードすることだけです。

手順

ステップ 1 **[Settings (設定)]** > **[Audit Log Export Settings (監査ログ エクスポート設定)]** を選択します。

ステップ 2 **[外部 syslog サーバへの監査ログのエクスポートの有効化]** チェック ボックスのチェックを外します。

ステップ 3 [OK] をクリックします。

監査ロギングは、デフォルトでは無効になっています。

監査ロギング サーバの設定の削除

管理者として、システムからリモート syslog サーバの設定の詳細を削除できます。これを行うと、システムはリモート syslog サーバにサーバ ログをプッシュしません。監査ロギングを有効にするには、サーバの詳細を再度入力する必要があります。

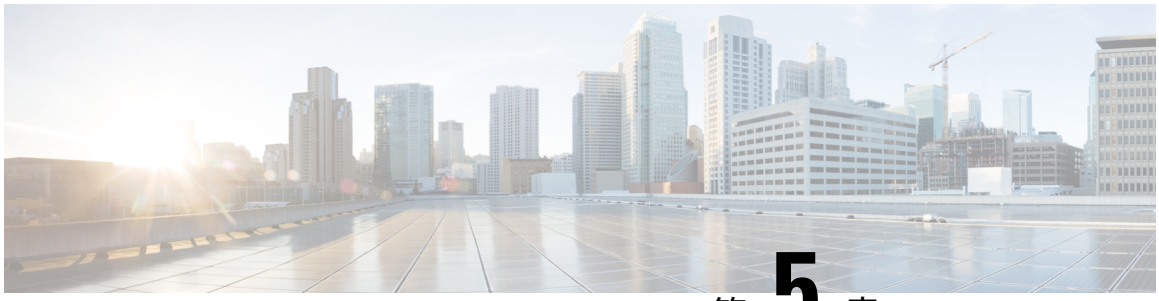
手順

ステップ 1 **[Settings (設定)]** > **[Audit Log Export Settings (監査ログ エクスポート設定)]** を選択します。

ステップ 2 **[削除（Delete）]** をクリックします。

ステップ 3 **[Confirm Delete (削除の確認)]** ダイアログ ボックスで、**[Delete (削除)]** をクリックします。

リモート syslog サーバの詳細がシステムから削除されます。



第 5 章

HX ストレージ クラスタの管理

クラスタ アクセス ポリシー レベルの変更

手順

ステップ 1 クラスタ アクセス ポリシーを「strict」（厳格）に変更する前に、ストレージ クラスタが正常な状態になっている必要があります。

ステップ 2 ストレージ クラスタ内のストレージ コントローラ VM のコマンド ラインから、次のコマンドを入力します。

```
# stcli cluster get-cluster-access-policy
```

```
# stcli cluster set-cluster-access-policy --name {strict,lenient}
```

クラスタのリバランス

ストレージクラスタは定期的なスケジュールで再調整されます。これは、使用可能なストレージの変更すべてに対して保存されているデータの分散を再調整し、ストレージクラスタの健全性を回復するために使用されます。新しいノードが既存のクラスタに追加される場合、追加されたノードは、既存のクラスタに参加するとすぐに新しい書き込みを実行します。必要に応じて (通常は 24 時間以内に) クラスタが自動的に再調整され、ストレージ全体の使用率が低い場合、新しいノードは最初に既存のコンバージドノードよりも少ないストレージ使用率を示すことがあります。現在のストレージ使用率が高く、新しいノードがクラスタに追加されると、データは一定期間にわたって新しいノード ドライブに再調整されます。

制約事項 次のワークフローは、Cisco TAC のみが実行する必要があります。クラスタを手動で再調整する必要がある場合は、TAC にお問い合わせください。

（注） 手動の再調整を行うことにより、クラスタ上の通常のユーザー IO との干渉が発生し、遅延が増加する可能性があります。したがって、HyperFlex システムは、パフォーマンスのペナルティを最小限に抑えるために必要な場合にのみ、再調整を開始します。

手順

ストレージ コントローラ VM から再調整ステータスを確認します。

a) コマンド ラインで、次のコマンドを入力します。

```
# stcli rebalance status
rebalanceStatus:
rebalanceState:
cluster_rebalance_ongoing
percentComplete: 10
rebalanceEnabled: True
```

b) コマンド ラインを再入力して、プロセスの完了を確認します。

```
# stcli rebalance status
rebalanceStatus:
rebalanceState: cluster_rebalance_not_running
rebalanceEnabled: True
```

この例では再調整が有効で、再調整を実行する準備ができていますが、現在ストレージクラスタを再調整していないことを示します。

クラスタの再調整ステータスと自己修復ステータスの確認

ストレージクラスタのリバランスは定期的に行われ、クラスタ内の利用可能なストレージ量が変化したときにも行われます。さらに、利用可能なストレージ量が変化した場合にも、リバランスがトリガーされます。これは自動自己修復機能です。

重要 再調整は、通常、1 つのディスクの使用率が 50 % を超えた場合またはクラスタの集約ディスク使用率が 50 % 以上の場合にのみ発生します。

HX Data Platform プラグインまたはストレージ コントローラ VM コマンドラインから再調整ステータスを確認できます。

手順

ステップ 1 HX Data Platform プラグインからの再調整ステータスの確認

a) vSphere Web クライアント ナビゲータから、**[vCenter Inventory Lists]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***cluster*** > **[サマリ (Summary)]** の順に選択します。

[状態（Status）] ポートレットには**自己修復ステータス**がリストされます。

b) [復元ステータス] を展開して、[自己修復ステータス] セクションを表示します。[Self healing status] フィールドには、再調整アクティビティまたは N/A（再調整が現在アクティブではない場合）が示されます。

ステップ 2 ストレージ コントローラ VM コマンド ラインから再調整ステータスを確認する。

a) `ssh` を使用してコントローラ VM にログインします。

b) コントローラ VM のコマンド ラインから、次のコマンドを実行します。

```
# stcli rebalance status
```

次の出力は、ストレージ クラスタで再調整が現在実行されていないことを示しています。

```
rebalanceStatus:
percentComplete: 0
rebalanceState: cluster_rebalance_not_running
rebalanceEnabled: True
```

HX Data Platform プラグインの [最近のタスク（Recent Tasks）] タブに、ステータス メッセージが表示されます。

スペース不足エラーの処理

システムで [スペース不足（Out of Space）] エラーが表示された場合、ノードを追加して空き容量を増やすか、使用されていない既存の VM を削除して領域を解放できます。

[スペース不足（Out of Space）] の状態の場合、VM は応答しません。

（注） ストレージ コントローラ VM は削除しないでください。ストレージ コントローラ VM の名前には、`stCtlVM` というプレフィックスが付いています。

手順

ステップ 1 ノードを追加するには、HX Data Platform インストーラのクラスタ拡張機能を使用します。

ステップ 2 未使用の VM を削除するには、次の手順を実行します。

a) どのゲスト VM が削除可能であるかを判断します。VM や命名規則によって使用されるディスク領域などの要因を考慮できます。

b) **[vCenter]** > **[仮想マシン（Virtual Machines）]** に移動して、インベントリ内の仮想マシンを表示します。

c) 削除する VM をダブルクリックします。

d) **[概要（Summary）]** > **[質問に回答（Answer Questions）]** をクリックしてダイアログボックスを表示します。

e) **[キャンセル（Cancel）]** オプション ボタンをクリックして、**[OK]** をクリックします。

f) VM の電源をオフにします。

g) VM を削除します。

ステップ 3 [スペース不足（Out of Space）] の状態がクリアされた後で、次の操作を行います。

a) **[vCenter]** > **[仮想マシン（Virtual Machines）]** に移動して、インベントリ内の VM を表示します。

b) 使用する VM をダブルクリックします。

c) **[概要（Summary）]** > **[質問に回答（Answer Questions）]** をクリックしてダイアログボックスを表示します。

d) **[再試行（Retry）]** オプション ボタンをクリックして、**[OK]** をクリックします。

現在の vCenter サーバから新しい VCenter サーバへのストレージ クラスタの移動

始める前に

- このタスクはメンテナンス時間帯に実行します。
- クラスタが正常であることおよびアップグレードの状態が問題なく正常であることを確認します。コントローラ VM コマンドラインから `stcli` コマンドを使用して、状態を表示できます。

```
# stcli cluster info
```

応答を確認します。

```
Resiliency Health: HEALTHY
```

- vCenter が動作している必要があることを確認します。
- vCenter クラスタ間でストレージ クラスタを移動する場合、スナップショット スケジュールはストレージ クラスタと共に移動されません。

手順

ステップ 1 現在の vCenter から、クラスタを削除します。

これは HX ストレージ クラスタの作成時に指定された vCenter クラスタです。

注意 分散仮想スイッチ（DVS）ユーザー：クラスタで DVS を使用している場合は、クラスタを削除することは推奨されません。

ステップ 2 新しい vCenter では、同じクラスタ名を使用して新しいクラスタを作成します。

ステップ 3 新しく作成されたクラスタで新しい vCenter に ESX ホストを追加します。

次のタスク

vCenter クラスタからのストレージ クラスタの登録解除 （65 ページ） に進みます。

vCenter クラスタからのストレージ クラスタの登録解除

この手順はオプションであり、必須ではありません。古い vCenter では、HX Data Platform プラグインの登録をそのままにしておくことをお勧めします。

始める前に

vCenter サーバから別の vCenter サーバへストレージ クラスタを移動するタスクの一部として、現在の vCenter サーバから新しい VCenter サーバへのストレージ クラスタの移動 （64 ページ）の手順を完了します。

（注）
- 複数の HX クラスタが同じ vCenter に登録されている場合、すべての HX クラスタが別の vCenter に完全に移行されるまで、この手順を実行しないでください。この手順を実行すると、vCenter に登録されている既存の HX クラスタに問題が生じます。

手順

ステップ 1 vSphere クライアントからの HX Data Platform ファイルの削除 （68 ページ）の手順を完了します。
ステップ 2 HX クラスタが vCenter から登録解除されていることの確認 （69 ページ）の手順を完了します。

次のタスク

新しい vCenter クラスタによるストレージ クラスタの登録 （69 ページ） に進みます。

EAM 拡張機能の登録解除および削除

HX Data Platform を部分的にインストールしているかアンインストールしている場合、または、当該の vSphere にインストールされている HX クラスタよりも多くのエージェンシーがある HX クラスタを登録解除している場合、HX Data Platform 拡張機能のための古い ESX Agent Manager（EAM）が残っている場合があります。Managed Object Browser（MOB）拡張マネージャを使用して、古い拡張機能を削除します。

始める前に

- まだダウンロードしていない場合は、vSphere ESX Agent Manager SDK をダウンロードします。
- 複数の HX クラスタが同じ vCenter に登録されている場合、すべての HX クラスタが別の vCenter に完全に移行されるまで、この手順を実行しないでください。この手順を実行すると、vCenter に登録されている既存の HX クラスタに問題が生じます。
- vSphere クラスタからデータセンターを削除します。

（注） HyperFlex リリース4.0 以降で新たに導入された HX クラスタは、HyperFlex ストレージ コントローラ VM の vSphere ESX Agent Manager (EAM) を利用できなくなりました。HX 4.0 より前に構築された HX クラスタは引き続き EAM を使用します。そのクラスタが新しい vCenter に移行された場合、EAM 連携は設定されません。

手順

ステップ 1 HX クラスタの UUID を指定します。

各エージェンシーには、基盤となる vSphere 拡張機能を参照するフィールド、`cluster_domain_id` があります。この拡張機能 ID には、Managed Object ID（moid）が使用されています。

HyperFlex クラスタが複数ある場合は、登録を解除する正しいクラスタ ID を選択することを確認します。

ストレージ コントローラ VM コマンド ラインから次のコマンドを実行します。

```
# hxcli cluster info | grep vCenterClusterId:
vCenterClusterId: domain-c26
```

ステップ 2 ストレージ クラスタの拡張機能を登録解除する：vCenter サーバ MOB 拡張機能マネージャにログインします。

まず、HyperFlex クラスタを登録解除します。

a) ブラウザで、パスとコマンドを入力します。

`https://vcenter_server/mob/?moid=ExtensionManager`

vcenter_server は、ストレージ クラスタが現在登録されている vCenter の IP アドレスです。

b) 管理者用のログイン クレデンシャルを入力します。

ステップ 3 クラスタ ID を持つ HX ストレージ クラスタ拡張機能を探します。**[プロパティ（Properties）]** > **[extensionList]** をスクロールして、次のストレージ クラスタ拡張機能を探します。

`com.springpath.sysmgmt.cluster_domain_id` および `com.springpath.sysmgmt.uuid.cluster_domain_id`。

クリップボードに、これらの文字列をそれぞれコピーします。文字列の端に二重引用符（”）がある場合、それを除外します。

ステップ 4 各ストレージ クラスタ拡張機能の登録を解除します。

a) [メソッド（Methods）] テーブルから `UnregisterExtension` をクリックします。

b) **[UnregisterExtension]** ポップアップに拡張機能のキー値である `com.springpath.sysgmt.cluster_domain_id` を入力します。

例：`com.springpath.sysgmt.domain-26`

c) **[メソッドの呼び出し（Invoke Method）]** をクリックします。

ステップ 5 古い EAM 拡張機能を削除する：vCenter サーバ MOB ESX エージェンシー拡張機能マネージャにログインします。

次に、HyperFlex クラスタに関連付けられていた古い EAM 拡張機能を削除します。

a) ブラウザで、パスとコマンドを入力します。

`https://vcenter_server/eam/mob/`

vcenter_server は、ストレージ クラスタが現在登録されている vCenter の IP アドレスです。

b) 管理者用のログイン クレデンシャルを入力します。

ステップ 6 当該のクラスタ ID を持つ古い HX ストレージ クラスタの ESX エージェンシー拡張機能を見つけます。

a) **[プロパティ（Properties）]** > **エージェンシー** > **[値（Value）]** までスクロールします。

b) エージェンシーの値をクリックします。

c) **[エージェンシー（Agency）]** ウィンドウで、**[プロパティ（Properties）]** > **[solutionID]** > **[値（Value）]** 拡張機能を確認します。正しい *cluster_domain_id* があることを確認します。

例：`com.springpath.sysgmt.domain-26`

ステップ 7 古い ESX エージェンシー拡張機能を削除します。

a) **[エージェンシー（Agency）]** ウィンドウの **[メソッド（Methods）]** テーブルからメソッドを選択します。

古い ESX エージェンシーは、`destroyAgency` または `uninstall` のいずれかを使用して削除できます。

b) ***[メソッド（method）]*** ポップアップで、**[メソッドの呼び出し（Invoke Method）]** をクリックします。

ステップ 8 **[ExtensionManager]** タブを更新し、**extensionList** エントリに `com.springpath.sysgmt.cluster_domain_id` という拡張機能が含まれていないことを確認します。

ステップ 9 vSphere クライアント サービスを再起動します。

vSphere クライアント サービスが再起動されると、HX Data Platform の拡張機能が削除されます。vSphere クライアント サービスを再起動すると、ブラウザを介した vCenter へのアクセスが一時的に無効になります。追加情報については、*VMware* のナレッジ ベース『*Stopping, starting, or restarting VMware vCenter Server Appliance 6.0 services*（*2109887*）』の記事を VMwear お客様コネクト サイトで参照してください。

vSphere クライアントからの HX Data Platform ファイルの削除

この作業は HX Storage Cluster を vCenter から登録解除するための手順です。

手順

VSphere クライアントから HX Data Platform ファイルを削除します。方法を選択します。

Linux vCenter

a) Linux vCenter サーバーに `ssh` を使用して、root ユーザーとしてログインします。

b) HX Data Platform Plug-in フォルダを含むフォルダに移動します。

vCenter 6.0 の場合

```
# cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
```

vCenter 5.5 の場合

```
# cd /var/lib/just/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
```

c) HX Data Platform Plug-in のフォルダとファイルを削除します。

```
# rm -rf com.springpath*
```

d) vSphere クライアントを再起動します。

```
# service vsphere-client restart
```

Windows vCenter

a) Remote Desktop Protocol（RDP）を使用して、Windows vCenter システム コマンド ラインにログインします。

b) HX Data Platform Plug-in フォルダを含むフォルダに移動します。

```
# cd "%PROGRAMDATA%\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity
```

c) HX Data Platform Plug-in のフォルダとファイルを削除します。

```
# rmdir /com.springpath*
```

d) サービス画面を開きます。

```
# services.msc
```

e) vCenter からログアウトして、vSphere Web クライアントを再起動します。

```
# serviceLogout
```

HX クラスタが vCenter から登録解除されていることの確認

この作業は HX ストレージ クラスタを vCenter から登録解除するための手順です。

HX クラスタが古い vCenter 上にないことを確認します。

始める前に

次の手順を実行します：vSphere クライアントからの HX Data Platform ファイルの削除 （68 ページ）

手順

ステップ 1 vCenter に再度ログインする前にキャッシュをクリアします。

ステップ 2 古い vCenter からログアウトします。

ステップ 3 古い vCenter に再度ログインし、HX Data Platform プラグインが削除されていることを確認します。

新しい vCenter クラスタによるストレージ クラスタの登録

始める前に

HyperFlexクラスタをvCenterに登録する前に、すべてのESXiホストでESXiロックダウンモードを無効にし、SSHサービスが有効で実行中であることを確認する必要があります。

vCenter サーバから別の vCenter サーバへストレージ クラスタを移動するタスクの一部として、vCenter クラスタからのストレージ クラスタの登録解除 （65 ページ）の手順を完了します。

手順

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 `stcli cluster reregister` コマンドを実行します。

例：

```
stcli cluster reregister [-h] --vcenter-datacenter NEWDATACENTER
 --vcenter-cluster NEWVCENTERCLUSTER --vcenter-url NEWVCENTERURLIP
[--vcenter-sso-url NEWVCENTERSSOURL] --vcenter-user NEWVCENTERUSER
```

必要に応じて、さらにリストされているオプションを適用します。

構文の説明

Option	必須またはオプション	説明
--vcenter-cluster NEWVCENTERCLUSTER	必須	新しい vCenter クラスタの名前。
--vcenter-datacenter NEWDATACENTER	必須	新しい vCenter データセンター名。
--vcenter-sso-url NEWVCENTERSSOURL	任意	新しい vCenter SSO サーバの URL。指定されない場合、`--vcenter url` から推測されます。
--vcenter-url NEWVCENTERURL	必須	新しい vCenter の URL、*<vcentername>*。ここで、*<vcentername>* には新しい vCenter の FQDN または IP を使用できます。
--vcenter-user NEWVCENTERUSER	必須	新しい vCenter 管理者のユーザー名。 プロンプトが表示されたら vCenter 管理者パスワードを入力します。

レスポンスの例：

```
Reregister StorFS cluster with a new vCenter ...
Enter NEW vCenter Administrator password:
Waiting for Cluster creation to finish ...
```

ストレージクラスタを再登録してから、コンピューティング専用ノードがEAMの登録に失敗したか、EAMクライアント内に存在しないか、vCenter のリソース プール内に存在しない場合は、下のコマンドを実行してコンピューティング専用ノードを再度追加します。

```
# stcli node add --node-ips <computeNodeIP> --controller-root-password <ctlvm-pwd> --esx-username
<esx-user> --esx-password <esx-pwd>
```

サポートが必要な場合は、TAC にお問い合わせください。

ステップ 3 スナップショット スケジュールを再入力します。

vCenter クラスタ間でストレージ クラスタを移動する場合、スナップ ショット スケジュールはストレージ クラスタと共に移動されません。

ステップ 4 （オプション）登録に成功したら、HyperFlexクラスタをvCenterに登録する前にESXiロックダウンモードを無効にします。

クラスタの名前変更

HX Data Platform ストレージ クラスタを作成した後、プロセスを中断することがなく名前を変更できます。

（注） 次の手順は vCenter クラスタの名前変更ではなく、HX クラスタに適用されます。

手順

ステップ 1 vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** の順に選択して名前変更します。

ステップ 2 **[クラスタの名前変更（Rename Cluster）]** ダイアログボックスを開きます。ストレージクラスタを右クリックするか、タブの上部にある **[アクション（Actions）]** ドロップダウンリストをクリックします。

ステップ 3 **[クラスタの名前変更（Rename Cluster）]** を選択します。

ステップ 4 テキスト フィールドにストレージ クラスタの新しい名前を入力します。

HX クラスタ名の最大文字数は 50 文字です。

ステップ 5 **[OK]** をクリックして、新しい名前を適用します。

自己署名証明書の置き換え

VCenter サーバで自己署名証明書を外部証明書へ置換

手順

vCenter の certMgmt モードを **[カスタム (Custom)]** に設定し、サードパーティ証明書を持つ ESXi ホストを vCenter に追加します。

（注） デフォルトでは、certMgmt モードは **vmsa** です。デフォルトの **[vmsa]** モードでは、自己署名証明書を持つ ESX ホストのみ追加できます。CA 証明書を持つ ESX を vCenter に追加する場合、CA 証明書が自己署名証明書に置換されない限り ESX ホストを追加できません。

certMgmt モードを更新するには：

a) ホストを管理する vCenter サーバを選択し、**[設定 (Settings)]** をクリックします。

b) **[詳細設定 (Advanced Settings)]** をクリックしてから、**[編集 (Edit)]** をクリックします。
c) **[フィルタ (Filter)]** ボックスに、**certmgmt** と入力し、証明書管理キーのみを表示します。
d) **vpxd.certmgmt.mode** の値を **custom** に変更して**[OK]** をクリックします。
e) vCenter サーバ サービスを再起動します。

サービスを再起動するには、ブラウザに次のリンクを入力して、**[Enter]** をクリックします。

```
https://<VC URL>:5480/ui/services
```

（注） vCenter のホスト追加動作は、証明書および certMgmt モードによって異なります。

- ホストに certMgmt モードの自己署名証明書がある場合、vCenter の **vmsa**デフォルト値に設定します。
  - 自己署名証明書を持つ ESX ホストのみ追加できます。
  - サードパーティ CA 証明書を持つ ESX の追加は許可されていません。
  - 自己署名証明書をサードパーティ CA 証明書に置換した後 ESX を vCenter に追加する場合、システムではサードパーティ CA 証明書を自己署名証明書に置換するように促します。CA 証明書を自己署名証明書に置換した後、ESX ホストを追加できます。
- ホストに certMgmt モードの自己署名証明書がある場合、vCenter の **custom** に設定します。
  - 自己署名証明書をサードパーティ CA 証明書に置換した後 ESX を vCenter に追加する場合、システムは次のエラーをスローします。`ssl thumbprint mismatch and add host fails.` この場合、次のことを実行して、サードパーティ CA s 証明書を自己署名証明書に置換します。
    1. ホストをメンテナンス モード (MM モード) に配置します。
    2. certified rui.crt and rui.key ファイルをバックアップしている以前のキーと証明書に置換します。
    3. hostd および vpxa service を再起動します。CA 証明書が新しいノードに表示されます。
    4. 右クリックして vCenter に接続します。ホストは CA 証明書を削除し、VMware の自己署名証明書に置換します。
- ホストに certMgmt モードのサードパーティ CA 証明書がある場合、vCenter の **vmsa**デフォルト値に設定します。
  - 自己署名証明書を持つ ESX ホストのみ追加できます。
  - サードパーティ CA 証明書を持つ ESX の追加は許可されていません。
- ホストに certMgmt モードのサードパーティ CA 証明書がある場合、vCenter の **custom** に設定します。
  - 自己署名証明書を持つ ESX ホストのみ追加できます。
  - ESX ホストの自己署名証明書を vCenter の CA 証明書に置換する必要があります。

ESXi ホスト サーバで自己署名証明書を外部証明書へ置換

手順

ステップ 1 ホスト証明書 (rui.crt) およびキー (rui.key) ファイルを生成し、ファイルを証明書機関に送信します。

（注） rui.key および rui.crt ファイルを生成している間に、ESX の適切なホスト名または FQDN が提供されていることを確認します。

ステップ 2 元のホスト証明書(rui)およびキー(rui)ファイルのバックアップを取得した後、各ESXiホストの/etc/vmware/sslディレクトリ内の認定ホスト証明書 (rui) およびキー (rui) ファイルを置き換えます。

（注） メンテナンス モードで 1 個のホストのみ配置してローリング傾向でホスト証明書 (rui.crt) およびキー(rui.key)ファイルを置き換えて、クラスタが正常になるまで待機して、それから別のノードの証明書を置き換えます。

a) 管理者権限を持つ SSH クライアントから ESXi ホストにログインします。
b) ホストをメンテナンス モード (MM モード) に配置します。
c) /etc/vmware/ssl/ ディレクトリの rui.bak ファイルに以前のキーおよび証明書のバックアップを作成します。
d) /etc/vmware/ssl/ ディレクトリに新しい認定 rui.crt および rui.key ファイルをアップロードします。
e) 次のコマンドを使用して、hostd および vpxa サービスを再起動して実行中のステータスを確認します。

```
/etc/init.d/hostd restart
/etc/init.d/vpxa restart
/etc/init.d/hostd status
/etc/init.d/vpxa status
```

f) ホストを vCenter に再接続し、メンテナンス モードを終了します。

（注） すべてのノードで同じ手順を繰り返します。Web でアクセスして各ノードの証明書を確認できます。

HyperFlex クラスタの再登録

認定ファイルを交換した後に vCenter にすべてのホストを追加した後、次のコマンドを使用して、HX クラスタを vCenter に再登録します。

```
hxcli license register
```

（注） HyperFlexクラスタをvCenterに登録する前に、すべてのESXiホストでESXiロックダウンモードを無効にし、SSHサービスが有効で実行中であることを確認する必要があります。登録が成功したら、ロックダウンモードを再度有効にすることができます。

自己署名証明書の再作成

外部 CA 証明書を交換した後にホスト証明書に問題が発生した場合は、次の手順を実行して自己署名証明書を再作成できます。

1. SSH クライアントから ESXi ホストにログインします。
2. /Etc/vmware/ssl/ ディレクトリから、rui.key および rui.crt ファイルを削除します。
3. 次のコマンドを使用して、ホストの自己署名証明書を再作成します。

   ```
   /sbin/generate-certificates
   ```

4. 次のコマンドを使用して、IPICS サービスを再起動します。

   ```
   /etc/init.d/hostd restart
   /etc/init.d/vpxa restart
   ```

ブースト モード

ブースト モードを使用すると、Cisco HyperFlex クラスタでは、ストレージ コントローラ VM の CPU リソースを 4 vCPU で増やしより高い IOP を実現できます。ブースト モードを有効にすると、HX データ プラットフォームのユーザ VM から追加の CPU リソースを取得します。追加の CPU の利点が、展開のサイジングによる影響を上回ると判断された場合にのみ有効にするべきです。ブースト モードでサポートされる CPU の詳細については、Cisco HyperFlex 仕様シートを参照してください。

ブースト モードの設定

ブースト モードを有効にする各クラスタに次の手順を実行します。

始める前に

ブースト モードのサポートは次の設定に制限されています。

- サポート対象ハードウェア：
  - すべての NVMe
  - All Flash C245
  - すべての Flash C240
  - All Flash C225
  - すべての Flash C220
- ハイパーバイザ：ESX のみ
- コントローラ VM vCPU のブースト モード番号：
  - すべての NVMe：16

- All Flash C245: 12
- すべての Flash C240：12
- All Flash C225: 12
- すべての Flash C220：12

- クラスタ拡張では、新しいノードに対してブースト モードを適用する必要があります。
- ブースト モードは Cisco HX リリース 4.0(2a) 以降でサポートされています。
- ブースト モードは、お客様の展開で追加の CPU からメリットが得られるとサポートが判断した場合にのみ、有効にしてください。

（注） CPU：多くの物理コアは、少なくともコントローラ vCPU の新しい数と等しくなければなりません。vSphere クライアントの物理コアの数を確認するには、**[ホスト (host)]** > **[設定 (Configure)]** > **[ハードウェア (Hardware)]** > **[プロセッサ (Processors)]** > **[ソケットあたりのプロセッサ コア (Processor cores per socket)]** をクリックします。

手順

ステップ 1 vCenter から、コントローラ VM と **[ゲスト OS をシャットダウンする (Shut Down Guest OS)]** を右クリックします。

ステップ 2 すべての NVMeに対してコントローラ VM vCPU の数を 16 に増やし、all flash C220 および all flash C240 に対しては 12 に増やします。vSphere クライアントで VM の **[設定の編集 (Edit Settings)]** をクリックし、最初の行にある CPU フィールドの値を変更します。

（注） コントローラ VM vCPU のブースト モード番号：

- すべての NVMe：16
- All Flash C245: 12
- すべての Flash C240：12
- All Flash C225: 12
- すべての Flash C220：12

ステップ 3 設定変更を適用するには、**[OK]** をクリックします。

ステップ 4 コントローラ VM の電源をオフにします。

ステップ 5 HX Connect にログインし、クラスタが正常になるまで待機します。

ステップ 6 クラスタ内の各ホストにプロセスを繰り返します。

ブースト モードの無効

ブースト モードを無効にするには、次の手順を実行します。

手順

ステップ 1 From the vCenter, right-click one controller VM and **Shut Down Guest OS**.

ステップ 2 すべての NVMeに対してコントローラ VM vCPU の数を 12 に減らし、all flash C220 および all flash C240 に対しては8 に減らします。vSphere クライアントで VM の **[設定の編集 (Edit Settings)]** をクリックし、最初の行にある CPU フィールドの値を変更します。

ステップ 3 設定変更を適用するには、**[OK]** をクリックします。

ステップ 4 コントローラ VM の電源をオフにします。

ステップ 5 HX Connect にログインし、クラスタが正常になるまで待機します。

ステップ 6 クラスタ内の各ホストにプロセスを繰り返します。

UEFI セキュア ブート モード

Unified Extensible Firmware Interface（UEFI）は、オペレーティング システムとプラットフォーム ファームウェア間のソフトウェア インターフェースを定義する仕様です。HX Data Platform は、UEFI を使用して BIOS ファームウェア インターフェイスを置換します。これにより、BIOS はレガシー サポートを提供する一方で UEFI で動作できるようになります。

HX Data Platform リリース 4.5（1a）以降、クラスタ内のコンバージド ノードとコンピューティング ノードのブート モードを Unified Extensible Firmware Interface（UEFI）セキュア ブートに無停止で変更する自動ワークフローを提供することで、ハイパーバイザ（ESXi）ブートセキュリティの強化が簡素化されています。信頼チェーンは、UCS ラックおよびブレード サーバに組み込まれたハードウェア トラストアンカー（つまり、Cisco Trust Anchor モジュール）によって固定されます。各ノードのセキュア ブート ステータスの UI および API ベースのクエリも許可するため、オンデマンドでクラスタのセキュリティポスチャを監査できます。

次の制限は、UEFI ブート モードに適用されます。

- HX Edge クラスタの場合、UEFI セキュア ブートは、Cisco IMC バージョン 4.1(2a) 以降を実行している HX Edge クラスタでのみ有効にする必要があります。以前のバージョンの Cisco IMC でセキュア ブートが有効になっている場合は、ファームウェアの更新中にセキュア ブートを一時的に無効にする必要があります。
- セキュア ブートのサポートは、HyperFlex ESXi M5/M6 サーバでのみ使用できます。
- vCenter による ESXi ホストのセキュア ブートのアテステーションはサポートされています。この機能を使用するには、コンバージド ノードまたはコンピューティング ノードに ESXi リリース 6.7 以降と TPM 2.0 モジュールが必要です。TPM および TXT パラメータは、TPM モジュールの使用を有効にするために必要であり、セキュア ブートを有効にす

る際に自動的に設定されます。アテステーションを使用するための手順は必要ありません。

- 工場で準備されたすべてのM.2 RAIDエッジノードは、HXDPサーバファームウェアバージョン4.1（2a）以降を実行します。顧客が現場でダウングレードするか、既存のセットアップを改良し、HXDPサーバファームウェアバージョンが4.1（2a）より前のM.2RAIDノードを含むクラスタを起動しようとすると、インストールが失敗し、UEFI ブート パラメータをレガシー ブート モード用に設定できません。HXDP サーバ ファームウェアをバージョン 4.1（2a）以降にアップグレードしてから、インストールを再試行する必要があります。

セキュア ブート モードの有効化

- セキュア ブートモードを有効にすると、ESXi ホストのブート モードをレガシー BIOS または UEFI (非セキュア) から UEFI セキュア ブートに変更できます。
- HyperFlex クラスタの一部である UCS サーバの UCS Manager または Cisco IMC のブートパラメータを手動で変更しないでください。HyperFlex はこのような変更を認識せず、自動的に修復しません。
- [セキュア ブート ステータスの確認]アクション（ステップ 4 を参照）を使用して、クラスタのセキュア ブート ステータスを監査します。ノードがコンプライアンス違反であることが判明した場合、セキュアブートモードのアップグレードタイプオプションが[アップグレード（Upgrade）]タブで使用可能になり、ユーザはセキュアブートを再度有効にできます。コンプライアンス違反のノードのみがリブートされ、ブートモードが変更されます。

始める前に

- **[セキュア ブート ステータスの確認（Check Secure Boot Status）]**を実行して、セキュアブートがすでに有効になっているかどうかを確認し、それに応じて続行します。ステップ 4 を参照してください。
- HX リリース 4.5（1a）以降では、HX リリース 4.5（1a） インストールの更新後、または既存のクラスタを HX 4.5（1a） にアップグレードした後、UEFI セキュアブートを別の 2 日目の操作として有効にする必要があります。
- プリフライト検証を実行して、セキュアブートを有効にするクラスタが準備完了状態であることを確認します。
- クラスタにレガシー、UEFI、およびUEFIセキュアブートノードが存在する場合、セキュアブート操作はクラスタのすべてのノードで有効になり、それ以降の拡張はセキュアブートに対応します。
- セキュア ブートを有効にするオプションは、ESXi クラスタでのみ使用できます。
- セキュア ブートを有効にするために ESXi ホストがローリング リブートするため、アクティビティはメンテナンス ウィンドウで計画します。

- セキュア ブートの有効化は、他のアップグレード アクティビティと組み合わせることができません。
- セキュア ブートがすでに有効になっている場合、**[セキュア ブートの有効化（Enable Secure Boot）]** オプションはグレー表示され、それ以上のアクションは必要ありません。
- **[セキュア ブートの有効化（Enable Secure Boot）]** ワークフローが失敗した場合は、vCenter から、ホストがまだ**メンテナンス モード**であるかどうかを確認します。その場合は、**セキュア ブートの有効化**を再試行する前に、**メンテナンス モード** を終了します。

手順

ステップ 1 HX Connect UI から、**[アップグレード (Upgrade)]** > **[アップグレード タイプの選択 (Select Upgrade Type)]** に移動します。

ステップ 2 **[アップグレード タイプの選択 (Select Upgrade Type)]** タブで、**[セキュア ブート モード (Secure Boot mode)]** チェックボックスをオンにします。

（注） セキュア ブートを有効にした後で、無効にすることはできません。

ステップ 3 vCenter と UCSM のクレデンシャル（**ユーザー名**と**管理者パスワード**）を入力し、**[アップグレード (Upgrade)]** をクリックします。

クラスタでセキュアブートを有効にすると、その後に追加された新しいコンバージドノードまたはコンピューティングノードでは、自動的にセキュアブートが有効になります。手動による作業は必要ありません。

ステップ 4 セキュア ブートのステータスを確認するには、**[システム情報]** > **[アクション]** ドロップダウン メニューに移動し、**[セキュア ブートのステータスの確認（Check Secure Boot Status）]** を選択します。

（注） すべてのノードが有効になっている場合は、**すべてのノードでセキュア ブートが有効になっている**というメッセージが表示されます。

自動セキュア ブート ノードでの ESXi 再展開後に hx_edge.py スクリプトが失敗する

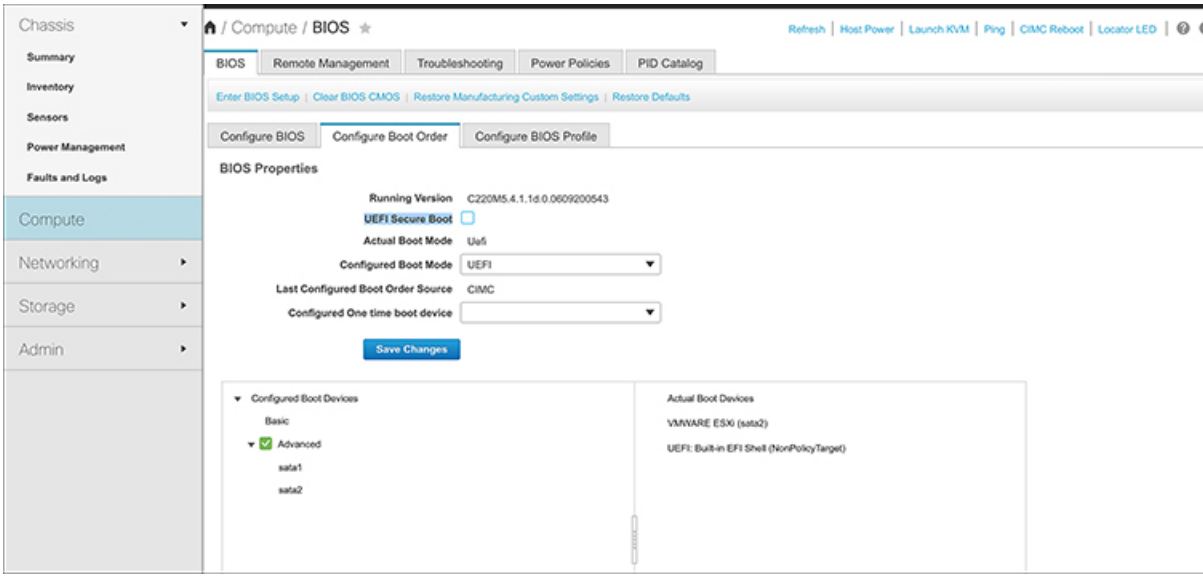
説明

Cisco UCS ツールは、従来のインストーラを使用した HyperFlex Edge 設定ではサポートされていません。従来のインストーラを使用した HX Edge の設定では、SOL for IP 設定を使用し、ESXi ログイン コンソールが受信されたかどうかを確認する必要があります。

次の手順を実行して、SOL セキュア ブートを有効にします。

アクション

1. [Compute Configure Boot Order] ページの[UEFI Secure Boot]チェックボックスをオフにして、ブートセキュリティを無効にします。 >



2. サーバの電源を再投入します。
3. ESXi をインストールします。
4. `hx_edge.py` スクリプトを実行します。

カタログの更新

互換性カタログ更新機能は、ESXiのCisco HyperFlexリリース4.5（1a）で導入されました。

カタログ更新では、クラスタで実行中のHXDPバージョンをアップグレードすることなく、新しいモデルのドライブのクラスタ作成、拡張、またはホットアド時にクラスタ全体でカタログバージョンを更新できます。

- 現在のカタログでサポートされていないドライブを明確に識別します。
- HXDPをアップグレードする必要がないため、クラスタノードに新しいドライブモデルを追加する際のオーバーヘッドが削減されます。
- HXインストーラ、HX Connect、およびIntersightでサポートされます。
- カタログはオンラインで更新され、実行中のクラスタには影響しません。

ガイドラインと制約事項

- 新しいドライブを追加する前に、HyperFlex リリース ノートを参照して、現在のHXDPバージョンが新しいドライブモデルをサポートしていることを確認します。

- カタログ更新では、ドライブがサポートされていることは保証されません。ハードウェアの問題とHXDPのバージョンによって、ドライブがHXDPで認識されないことがあります。
- より高いドライブ容量ポイントなど、カスタム設定にHXDPの調整が必要なドライブには、カタログアップグレードを使用しないでください。これには、完全なHXDPアップグレードが必要です。
- カタログバンドルを以前のバージョンにダウングレードすることはサポートされていません。

カタログの更新：HX インストーラ

カタログの更新：HX インストーラを使用したクラスタの作成

HX VM ベースのインストーラ（OVA）を使用してクラスタの作成中にカタログをアップグレードするには、次の手順を実行します。

始める前に

- CCO からカタログバンドルをダウンロードします。https://software.cisco.com/download/home/286305544/type/286305994/

手順

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 **[クラスタの作成]** ワークフローに従います。

ステップ 3 [サーバの選択（Server Selection）]ページで、インストーラはドライブのサポート可能性を検証し、サポートされていないドライブが見つかった場合は、サポートされていないドライブが特定され、**[カタログのアップグレード（Upgrade Catalog）]** ボタンが表示されます。

ステップ 4 **[カタログのアップグレード]** ボタンをクリックします。[カタログのアップグレード] ウィンドウが表示されます。

（注） ウィンドウに使用中のカタログバージョンが表示されます。

ステップ 5 ローカルに保存されたカタログファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
アップロード操作が完了しました。

ステップ 6 **[アップグレード]** をクリックしてアップグレードを完了するか、**[閉じる]** をクリックして [カタログのアップグレード] ウィンドウを終了します。

カタログのアップグレード後に、ドライブのサポート可能性チェックが再度実行されます。すべてのドライブに互換性のあるカタログがある場合、緑色の成功バナーが表示されます。

カタログの更新：HX インストーラを使用したクラスタ拡張

クラスタを拡張する場合、互換性カタログ機能は、インストーラのカタログがクラスタのカタログよりも低いかどうかを識別し、ドライブのサポート可能性の検証を実行します。HX VM ベースのインストーラ（OVA）を使用してクラスタ拡張中にカタログをアップグレードするには、次の手順を実行します。

始める前に

- CCO からカタログバンドルをダウンロードします。https://software.cisco.com/download/home/286305544/type/286305994/

手順

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 **Expand Cluster**） ワークフローに従います。

ステップ 3 [サーバの選択（Server Selection）]ページで、インストーラはドライブのサポート可能性を検証し、サポートされていないドライブが見つかった場合は、サポートされていないドライブが特定され、**[カタログのアップグレード（Upgrade Catalog）]** ボタンが表示されます。

ステップ 4 **[カタログのアップグレード]** ボタンをクリックします。[カタログのアップグレード] ウィンドウが表示されます。

（注） ウィンドウに使用中のカタログバージョンが表示されます。

ステップ 5 ローカルに保存されたカタログファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
アップロード操作が完了しました。

ステップ 6 **[アップグレード]** をクリックしてアップグレードを完了するか、**[閉じる]** をクリックして [カタログのアップグレード] ウィンドウを終了します。

カタログのアップグレード後に、ドライブのサポート可能性チェックが再度実行されます。すべてのドライブに互換性のあるカタログがある場合、緑色の成功バナーが表示されます。

カタログアップグレードの完了後に現在のカタログバージョンを表示するには、実行中のクラスタの HX Connect のアップグレードページに移動します。

HX インストーラ設定からのカタログの更新

HX VM インストーラ（OVA）のアウトオブバンド カタログアップグレードを実行するには、次の手順を実行します。

手順

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 任意のページの **[設定（Settings）]** 歯車アイコンをクリックします。

ステップ 3 **[カタログのアップグレード]** ボタンをクリックします。[カタログのアップグレード] ウィンドウが表示されます。

（注） ウィンドウに使用中のカタログバージョンが表示されます。

ステップ 4 ローカルに保存されたカタログ ファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
アップロード操作が完了しました。

ステップ 5 **[アップグレード]** をクリックしてアップグレードを完了するか、**[閉じる]** をクリックして [カタログのアップグレード] ウィンドウを終了します。

カタログ アップグレードの完了後に現在のカタログバージョンを表示するには、**[設定（Settings）]アイコン**>**[アップグレード カタログ（Upgrade Catalog）]** をクリックして、アップグレード カタログ ウィンドウに戻ります。

カタログの更新：HX Connect

HX Connect を使用したクラスタ カタログのアップグレード

新しいディスクが HX Connect で認識されない場合は、カタログの更新が必要である可能性があります。HX Connect を使用してカタログをアップグレードするには、次の手順を実行します。

始める前に

- CCO からカタログバンドルをダウンロードします。https://software.cisco.com/download/home/286305544/type/286305994/

（注） HXDP バージョンをアップグレードすると、クラスタ カタログが自動的にアップグレードされます。すでに更新されたカタログが含まれているバージョンに HXDP をアップグレードする場合は、カタログを手動で更新する必要はありません。

手順

ステップ 1 HX Connect の **[アップグレード（Upgrade）]** タブをクリックします。

ステップ 2 [アップグレードの選択（Select Upgrade）] タブの **[HX データ プラットフォーム（HX Data Platform）]** ボックスをオンにしてください。

（注） カタログアップグレードと他のタイプのアップグレードの組み合わせはサポートされていません。

ステップ 3 ローカルに保存されたカタログファイルをアップロードします。ファイルをターゲットにドラッグアンドドロップするか、ターゲットをクリックしてファイルの場所を参照します。
カタログファイルのアップロード操作が完了しました。

ステップ 4 アップグレードを完了するには、**[アップグレード（Upgrade）]** をクリックします。

a) HX ストレージクラスタのアップグレードタスクの進行状況をモニタするには、HX Connect の **[アクティビティ（Activity）]** ページをクリックします。

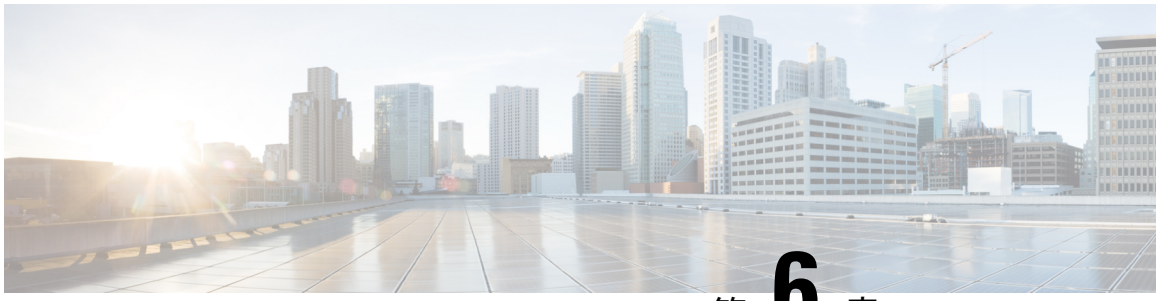
ステップ 5 **[システム情報（System Information）]** ページをクリックし、すべてのディスクが HXDP によって要求され、使用中であることを確認します。

カタログの更新：Intersight

Intersight を使用したカタログのアップグレード

HX インストーラ VM とは異なり、Intersight HX インストーラは最新の互換性カタログで自動的に最新の状態に維持されます。シスコは、Intersight HX インストーラのアップデートを定期的にリリースし、その標準プロセスの一部としてカタログのアップデートを含めています。

同様に、Intersight に接続されたクラスタは、HX Connect を介して手動でダウンロードおよびアップロードする必要なく、自動的に最新のカタログバージョンに更新されます。これらの自動更新を受信するには、HyperFlex クラスタが Intersight に接続されていることを確認します。



第 6 章

HX ストレージ クラスタのメンテナンスに向けた準備

ストレージ クラスタ メンテナンス操作の概要

Cisco HyperFlex (HX) Data Platform ストレージ クラスタのメンテナンス タスクは、ストレージ クラスタのハードウェア コンポーネントとソフトウェア コンポーネントの両方に影響します。ストレージクラスタのメンテナンス操作には、ノードやディスクの追加または削除と、ネットワーク メンテナンスが含まれます。

メンテナンス タスクの一部の手順は、ストレージクラスタ内のノードのストレージコントローラ VM から行います。ストレージコントローラ VM で発行される一部のコマンドは、ストレージ クラスタ内のすべてのノードに影響を与えます。

（注） **3 ノード ストレージ クラスタ。**3 ノード クラスタでノードを削除またはシャットダウンする必要があるタスクについては、テクニカル アシスタンス センター（TAC）までご連絡ください。3 ノード ストレージ クラスタでは、1 つのノードで障害が発生するか、または 1 つのノードが削除された場合、3 番目のノードが追加されてストレージ クラスタに参加するまで、クラスタは正常ではない状態になります。

ノードの追加。Cisco HX Data Platform ストレージ クラスタへのノードの追加は、HX Data Platform インストーラのクラスタ拡張機能を使用して実行されます。新しいノードはすべて、Cisco HX Data Platform のインストールおよび初期ストレージ クラスタの作成時と同じシステム要件を満たしている必要があります。クラスタ拡張機能の使用の要件と手順に関する完全なリストついては、適切な『Cisco HX Data Platform インストール ガイド』を参照してください。

オンライン メンテナンスとオフライン メンテナンスの比較

タスクによっては、ストレージクラスタをオンラインまたはオフラインのいずれかにする必要があります。通常、メンテナンス タスクを行うには、ストレージ クラスタ内のすべてのノードがオンラインであることが必要です。

ストレージクラスタのメンテナンスをオフライン モードで実行する場合、Cisco HX Data Platform はオフラインですが、ストレージ コントローラ VM は稼働しており、`stcli`コマンド ライン、HX Connect および HX Data Platform プラグインを使用して Cisco HX Data Platform 管理機能を表示できます。vSphere Web Client は、ストレージ I/O レイヤーについてレポートできます。`stcli cluster info` コマンドを発行すると、ストレージ クラスタ全体のステータスが`オフライン`であるという応答が返されます。

メンテナンス前のタスク

ストレージ クラスタのメンテナンスを行う前に、次のことを確認します。

- 実行するメンテナンス タスクを特定します。
- すべてのメンテナンス操作（リソースの取り外し/交換など）は、システム負荷が低いメンテナンス期間中に行われます。
- メンテナンス タスクの**実行前**に、ストレージ クラスタが正常で稼動している必要があります。
- HX Connect または HX Data Platform プラグイン ビーコン オプションを使用してディスクを識別します。

  HX ビーコン オプションは、ハウスキーピング 120 GB SSD には使用できません。サーバでハウスキーピング SSD の物理的な位置を確認します。
- 互いに同時に実行できないメンテナンス タスクのリストを確認します。これらのタスクの詳細情報については、シリアル操作とパラレル操作 （87 ページ） を参照してください。相互に順次一部のタスクのみ実行可能です。
- SSH がすべての ESX ホストで有効になっていることを確認します。

- ホストでメンテナンス タスクを実行する前に、ESX ホストを HXDP メンテナンス モードにします。HXDP メンテナンス モードは、vSphere 付属のホスト メンテナンス モードと比べて、より多くのストレージ クラスタ固有ステップを実行します。

メンテナンス後タスク

メンテナンス タスクが終了したら、HXDP メンテナンス モードを終了して、ストレージ クラスタを正常に保つ必要があります。加えて、Cisco HX ストレージ クラスタを変更した場合は、追加のメンテナンス後タスクが必要になります。たとえば、vNIC または vHBA を変更した場合は、PCI パススルーを再設定する必要があります。PCI パススルーを再設定する方法の詳細についての詳細は、vNIC または vHBA の変更後の PCI パススルーの設定 （107 ページ） を参照してください。

次の状態を確認してください。

- ホストでのメンテナンス タスクの完了後に、ESX ホストの HXDP メンテナンス モードが終了している。
- 取り外しまたは交換作業の完了**後**に、ストレージ クラスタが正常であり稼動している。
- Cisco HX ストレージ クラスタ内の特定の ESX ホストで vNIC または vHBA を追加、削除、または交換した場合は、PCI パススルーを再設定します。

シリアル操作とパラレル操作

操作によっては、複数の操作を同時に実行できない場合があります。次の操作は、（パラレルではなく）必ずシリアルで実行してください。

- ストレージ クラスタまたはノードのアップグレード。
- ストレージ クラスタの作成、再作成、または構成。
- ノードの追加または削除。
- ノードのシャットダウンが必要となるノード メンテナンス。これには、ディスクやネットワーク インターフェイス カード（NIC）の追加または取り外しが含まれます。
- ストレージ クラスタの起動またはシャット ダウン。
- vCenter でのストレージ クラスタの再登録。

クラスタ ステータスの確認

手順

ステップ 1 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。コントローラ VM コマンド ラインから、次にリストするコマンドを実行します。

ステップ 2 ストレージ クラスタが正常であることを確認します。

```
# hxcli cluster info
```

次の例の応答は、ストレージ クラスタがオンラインで正常であることを示します。

```
locale: English (United States)
state: online
upgradeState: ok
healthState: healthy
state: online
state: online
```

ステップ 3 ノード障害の数を確認します。

```
# stcli cluster storage-summary
```

レスポンスの例：

```
#of node failures tolerable to be > 0
```

ビーコンの設定

ビーコンは、ノード（ホスト）とディスクを探して特定するのに役立つ LED をオンにする方法です。ノードには、前面の電源ボタンの近くと背面にビーコン LED があります。ディスクには、前面にビーコン LED があります。

Cisco UCS Manager を通じてノード ビーコンを設定します。ディスク ビーコンは、Cisco HX Data Platform プラグインまたは HX Connect ユーザー インターフェイスを使用して設定します。

手順

ステップ 1 UCS Manager を使用してノードのビーコンをオンまたはオフにします。

a) UCS Manager の左側のパネルから、**[設備（Equipment）]** > **[サーバ（Servers）]** > **サーバ**を選択します。

b) UCS Manager の中央のパネルから、**[一般（General）]** > **[ロケータ LED をオンにする（Turn on Locator LED）]** を選択します。

c) サーバが見つかったら、ロケータ LED をオフにします。

UCS Manager の中央のパネルから、**[一般（General）]** > **[ロケータ LED をオフにする（Turn off Locator LED）]** を選択します。

ステップ 2 Cisco HX Data Platform プラグインを使用してディスク ビーコンをオンまたはオフにします。

a) vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex システム（Cisco HyperFlex Systems）]** > **[Cisco HX データ プラットフォーム（Cisco HX Data Platform）]** > ***[クラスタ（cluster）]*** > **[管理（Manage）]** の順に選択します。

b) **[管理（Manage）]** タブで、**[クラスタ（Cluster）]** > ***[クラスタ（cluster）]*** > ***[ホスト（host）]*** > **[ディスク（Disks）]** > ***[ディスク（disk）]*** の順に選択します。

c) オブジェクトの物理的な場所を探して、ビーコンをオンにします。

[操作（Actions）] ドロップダウン リストから、**[ビーコン ON（Beacon ON）]** を選択します。

d) ディスクが見つかったら、ビーコンをオフにします。

[操作（Actions）] ドロップダウン リストから、**[ビーコン OFF（Beacon OFF）]** を選択します。

ステップ 3 HX Connect を使用してディスク ビーコンをオンまたはオフにします。

a) HX Connect にログインします。

b) **[システム情報（System Information）]** > **[ディスク（Disks）]**を選択します。

c) ノードを選択し、**[ロケータ LED をオンにする（Turn On Locator LED）]** または **[ロケータ LED をオフにする（Turn Off Locator LED）]** をクリックします。

ハウスキーピング SSD とキャッシュ NVMe SSD を除いて、選択されているノード上のすべてのディスクのビーコン LED が切り替えられます。ハウスキーピング SSD またはキャッシュ NVMe SSD では、LED ビーコンは動作しません。

HX クラスタの vMotion 構成の確認

HX クラスタで HX メンテナンス操作を実行する前に、Cisco HyperFlex (HX) クラスタのすべてのノードが vMotion 用に設定されていることを確認します。vSphere Web クライアントから次の項目を確認します。

メモ vMotion でサポートされていない一部の VM は、ノードがメンテナンスモードになるのを防ぐため、シャットダウンする必要があります。

1. vMotion ポート グループが、クラスタのすべての ESXi ホスト間でアクティブ/スタンバイ構成の `vmnic3` と `vmnic7` で設定されていることを確認します。
2. ポート グループが vMotion 用に設定されていること、およびクラスタのすべての ESXi ホスト間で命名規則がまったく同じであることを確認します。

（注） 名前では、大文字と小文字が区別されます。

3. 各 vMotion ポート グループに静的 IP アドレスを割り当て済みであること、各 vMotion ポート グループの静的 IP アドレスが同じサブネットにあることを確認します。

（注） 静的 IP アドレスは、VMKernel インターフェイスとして定義されています。

4. クラスタ内の各 ESXi ホスト上で、vMotion ポート グループのプロパティで vMotion オプションがオンになっていること、他のポート グループ（Management など）でこのオプションがオンになっていないことを確認します。
5. 設定で、vMotion ポート グループが 9000 MTU に設定されており（ジャンボ フレームを使用している場合）、さらに VLAN ID が vMotion サブネットのネットワーク構成に一致していることを確認します。
6. vMotion の 1 つの ESXi ホストの vMotion ポート グループから他のホストの vMotion IP に ping できることを確認します。

   「 `vmkping -I vmk2 -d -s 8972 <近隣サーバの vMotion IP アドレス>`」と入力します。

ストレージ クラスタ ノードのメンテナンス モード

メンテナンス モードは、クラスタ内のノードに適用されます。ノードをデコミッションまたはシャットダウンする前に、メンテナンス モードですべての VM を他のノードに移行することにより、さまざまなメンテナンス タスク用にノードを準備できます。

メンテナンス モードには次の 2 つのタイプがあります。

- HXDP メンテナンス モード
- ホスト メンテナンス モード

HXDP メンテナンス モード

HXDP メンテナンス モードでは、ホスト メンテナンス モードの機能に加えて Cisco HX Data Platform に固有の機能も実行されます。最初のストレージ クラスタの作成後に、ストレージ クラスタ ノードで実行されるメンテナンス タスクには、ホスト メンテナンス モードではなく、必ず HXDP メンテナンス モードを選択してください。

クラスタ内の個々のノードに対して選択したタスクを実行するには、このメンテナンス モードが適切です。たとえば、

- ディスク交換などのメンテナンスを行うために、個々のホストをシャット ダウンする場合。

- ESX サーバ バージョンなど、ホスト上の選択したソフトウェアをアップグレードする場合。

Cisco HX メンテナンス モードに関する考慮事項

- HXDPメンテナンス モードを使用する前に、ストレージ クラスタ内のすべてのノード上の ESX で SSH が有効になっていることを確認してください。
- ESX ホストでタスクを実行できるように HXDP メンテナンス モードを開始した場合は、ESX ホストでのタスクが完了した後、必ず HXDP メンテナンス モードを終了してください。
- HXDP メンテナンス モードは、正常なクラスタ内のノードにのみ適用されます。クラスタが正常な状態でない場合（たとえば、ダウンしているノードの数が多すぎるなど）、またはクラスタをシャットダウンする場合には、ホスト メンテナンス モードを使用してください。
- クラスタからノードが追加または削除されると、ユーザー IO を提供するリソース数(コントローラ VM、キャッシングおよび永続階層デバイスなど) が変更されます。HXDP は最適に IO を提供するため利用可能なクラスタ リソースを使用するようにしています。各ノードはユーザー IO の一部を提供するために使用され、内部のブックキーピング アクティビティを行う責任があります。

  ノードがなくなると(メンテナンス モードに入ると)、実行中の IO はクラスタ内の他のノードに対してフェールオーバーする必要があります。内部ブックキーピング リソースとアクティビティに加えて、リソースとアクティビティもフェールオーバーする必要があります。この動作に必要な時間はノードによって提供されたデータに比例しています。これにより、実行中のユーザー IO にさらに遅延が生じます。

  ノードがメンテナンス モードから戻った際も同様のケースが発生します。
- 手順については、『Cisco HyperFrex のメンテナンス モードの開始』および HXDP メンテナンス モードの終了 （93 ページ） を参照してください。

ホスト メンテナンス モード

このモードは、Cisco HX Data Platform をインストールする場合や、クラスタに大幅な変更を適用する場合に使用されます。

vSphere メンテナンス モードを開始または終了するには、次のようにします。

- VCenter GUI で、目的の**ホスト** 選択し、右クリック メニューから **[メンテナンス モード（maintenance mode）]** を選択します。
- ESX コマンド ラインで、`esxcli system maintenanceMode` コマンドを使用します。

Cisco HyperFrex のメンテナンス モードの開始

Cisco HyperFlex (HX) Connect ユーザ インターフェイスの使用

1. Cisco HX Connect: *https://<cluster management ip>* にログインします。
2. メニューで **[システム情報（System Information）]** をクリックします。
3. **[ノード（Nodes）]** をクリックし、メンテナンス モードにするノードの行をクリックします。
4. **[HXDP メンテナンス モードの開始（Enter HXDP Maintenance Mode）]** をクリックします。
5. **[HXDP メンテナンス モードの確認（Confirm HXDP Maintenance Mode）]** ダイアログ ボックスで、**[HXDP メンテナンス モードの開始（Enter HXDP Maintenance Mode）]** をクリックします。

（注） すべてのメンテナンス タスクを完了した後、手動で HXDP メンテナンス モードを終了する必要があります。

vSphere Web クライアントの使用

1. vSphere Web クライアントにログインします。
2. **[ホーム（Home）]** > **[ホストおよびクラスタ（Hosts and Clusters）]** に移動します。
3. **[HX クラスタ（HX Cluster）]** が含まれている **[データセンター（Datacenter）]** を展開します。
4. **[HX クラスタ（HX Cluster）]** を展開し、ノードを選択します。
5. ノードを右クリックして、**[HXDP メンテナンス モード（HXDP Maintenance Mode）]** > **[HXDP メンテナンス モードの開始（Enter HXDP Maintenance Mode）]** を選択します。

コマンド ラインインターフェイス（CLI）

1. root 権限を持つユーザとして、ストレージ コントローラ クラスタのコマンド ラインにログインします。
2. ノードを HXDP メンテナンス モードに移動します。
   1. ノード ID と IP アドレスを特定します。

      ```
      # hxcli node list --summary
      ```

   2. ノードを HXDP メンテナンス モードにします。

```
# hxcli node maintenanceMode (--id ID | --ip IP Address) --mode enter
```

(`hxcli node maintenanceMode --help` も参照してください)

3. ルート権限を持つユーザーとして、このノードのESXiコマンドラインにログインします。
4. ノードが HXDP メンテナンス モードになったことを確認します。

```
# esxcli system maintenanceMode get
```

[メンテナンス モードに切り替える（Enter Maintenance Mode）] タスクの進捗を vSphere Web クライアントの **[モニタ（Monitor）]** > **[タスク（Tasks）]** タブでモニタできます。

操作が失敗すると、エラーメッセージが表示されます。原因となっている問題を修正して、もう一度メンテナンス モードを開始します。

HXDP メンテナンス モードの終了

Cisco HyperFlex (HX) Connect ユーザ インターフェイスの使用

1. HX Connect へのログイン：*https://<cluster management ip>*。
2. メニューで **[システム情報（System Information）]** をクリックします。
3. **[ノード（Nodes）]** をクリックし、メンテナンス モードを修了するノードの行をクリックします。
4. **[HXDP メンテナンス モードの終了（Exit HXDP Maintenance Mode）]** をクリックします。

vSphere Web クライアントの使用

1. vSphere Web クライアントにログインします。
2. **[ホーム（Home）]** > **[ホストおよびクラスタ（Hosts and Clusters）]** に移動します。
3. **[HX クラスタ（HX Cluster）]** が含まれている **[データセンター（Datacenter）]** を展開します。
4. **[HX クラスタ（HX Cluster）]** を展開し、ノードを選択します。
5. ノードを右クリックして、**[HXDP メンテナンス モード（HXDP Maintenance Mode）]** > **[HXDP メンテナンス モードの終了（Exit HXDP Maintenance Mode）]** を選択します。

コマンド ラインインターフェイス（CLI）

1. root 権限を持つユーザとして、ストレージ コントローラ クラスタのコマンド ラインにログインします。
2. ノードの HXDP メンテナンス モードを終了します。
   1. ノード ID と IP アドレスを特定します。

```
# hxcli node list --summary
```

2. ノードの HXDP メンテナンス モードを終了します。

```
# stcli node maintenanceMode (--id ID | --ip IP Address) --mode exit
```

（`stcli node maintenanceMode --help` も参照してください）

3. ルート権限を持つユーザーとして、このノードの ESXi コマンドラインにログインします。
4. ノードで HXDP メンテナンス モードが終了したことを確認します。

```
# esxcli system maintenanceMode get
```

[メンテナンス モードの終了（Exit Maintenance Mode）] タスクの進捗は、vSphere Web クライアントの **[モニタ（Monitor）]** > **[タスク（Tasks）]** タブで、モニタできます。

操作が失敗すると、エラーメッセージが表示されます。原因となっている問題を修正して、もう一度メンテナンス モードを終了します。

バックアップ操作の作成

HX ストレージ クラスタをシャット ダウンする前に、設定をバックアップします。ID の保護属性を持つフルステート バックアップとすべての設定タイプ バックアップの両方を実行します。

始める前に

1. UCS Manager にログインします。
2. バックアップ サーバの IPv4 アドレスおよび認証クレデンシャルを取得します。

（注） 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。

手順

ステップ 1 [ナビゲーション]ペインで、[管理者]をクリックします。

ステップ 2 **[すべて（All）]** ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域の [Backup Configuration] をクリックします。

ステップ 5 **[バックアップ設定（Backup Configuration）]** ダイアログボックスで、**[バックアップ操作の作成（Create Backup Operation）]** をクリックします。

ステップ 6 **[バックアップ操作の作成（Create Backup Operation）]** ダイアログボックスで、次のフィールドに入力します。

名前	説明
[管理状態（Admin State）] フィールド	次のいずれかになります。 • **[Enabled]**：**[OK]** をクリックするとすぐに、Cisco UCS Manager によってバックアップ操作が実行されます。 • **[Disabled]**：**[OK]** をクリックしても、Cisco UCS Manager によってバックアップ操作は実行されません。このオプションを選択すると、ダイアログボックスのすべてのフィールドが表示されたままになります。ただし、[バックアップ設定（Backup Configuration）] ダイアログボックスからバックアップを手動で実行する必要があります。

名前	説明
[Type] フィールド	バックアップ コンフィギュレーション ファイルに保存された情報。次のいずれかになります。 • [フル ステート（Full state）]：システム全体のスナップショットが含まれるバイナリ ファイル。このバックアップにより生成されたファイルを使用して、ディザスタ リカバリ時にシステムを復元できます。このファイルにより、元のファブリック インターコネクト上で設定を復元または再構築できます。また、別のファブリック インターコネクト上で設定を再現することもできます。このファイルは、インポートには使用できません。 （注） バックアップ ファイルのエクスポート元となったシステムと同じバージョンを実行しているシステムを復元するために使用できるのは、Full State バックアップ ファイルのみです。 • [All configuration]：すべてのシステム設定と論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。このファイルには、ローカル認証されたユーザのパスワードは含まれません。 • [System configuration]：ユーザ名、ロール、ロケールなどのすべてのシステム設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。 • [Logical configuration]：サービス プロファイル、VLAN、VSAN、プール、ポリシーなどのすべての論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。

名前	説明
[アイデンティティの保存（Preserve Identities）] チェックボックス	**[すべての構成（All configuration）]** および **[システム構成（System Configuration）]** に対しては、このチェックボックスがオンのままになり、次の機能を提供します。 • **[すべての構成（All configuration）]** : バックアップ ファイルに、vHBA、WWPN、WWNN、vNIC、MAC、UUID を含め、プールから取得したすべてのアイデンティティが 保持されます。また、シャーシ、FEX、ラック サーバと、シャーシ、FEX、ラック サーバ、IOM、およびブレード サーバのユーザ ラベルも保持されます。 （注） このチェック ボックスがオンになっていない場合、復元後にアイデンティティが再割り当てされ、ユーザ ラベルは失われます。 • **[システム構成（System Configuration）]**: バックアップ ファイルに、シャーシ、FEX、ラック サーバと、シャーシ、FEX、ラック サーバ、IOM、およびブレード サーバのユーザ ラベルが保持されます。 （注） このチェック ボックスがオンになっていない場合、復元後にアイデンティティが再割り当てされ、ユーザ ラベルは失われます。 このチェックボックスが **[論理構成（Logical Configuration）]** タイプのバックアップ操作に対してオンにされている場合、バックアップ ファイルには、vHBA、WWPN、WWNN、vNIC、MAC、UUID を含め、プールから取得したすべてのアイデンティティが保持されます。 （注） このチェック ボックスがオンになっていない場合、復元後にアイデンティティが再割り当てされ、ユーザ ラベルは失われます。

名前	説明
[バックアップファイルの場所（Location of the Backup File）] フィールド	バックアップ ファイルの保存場所。次のいずれかになります。 • **[リモートファイルシステム（Remote File System）]**：バックアップ XML ファイルはリモート サーバーに保存されます。Cisco UCS Manager GUI によって次に示すフィールドが表示され、リモート システムのプロトコル、ホスト、ファイル名、ユーザ名、パスワードを指定できます。 • **[ローカル ファイル システム（Local File System）]**：バックアップ XML ファイルはローカルに保存されます。 Java ベース Cisco UCS Manager GUI には、**[ファイル名（Filename）]** フィールドが、関連付けられた **[参照（Browse）]** ボタンとともに表示され、バックアップ ファイルの名前と場所を指定できます。 （注） **[OK]** をクリックした後、場所は変更できません。 HTML ベースの Cisco UCS Manager GUI に **[ファイル名（Filename）]** フィールドが表示されます。**<*filename*>.xml** 形式のバックアップ ファイルの名前を入力します。ファイルがダウンロードされ、ブラウザの設定に応じた場所に保存されます。
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。 • **FTP** • **TFTP** • **SCP** • **ステップ** • **[USB A]**：ファブリック インターコネクト A に挿入された USB ドライブ。 このオプションは特定のシステム設定でのみ使用できます。 • **[USB B]**：ファブリック インターコネクト B に挿入された USB ドライブ。 このオプションは特定のシステム設定でのみ使用できます。

名前	説明
[Hostname] フィールド	バックアップ ファイルが格納されている場所のホスト名または IP アドレス（IPv4）。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。 （注） IPv4 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が **local** に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が **global** に設定されている場合は、 Cisco UCS Central で DNS サーバを設定します。 （注） 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。
[Remote File] フィールド	バックアップコンフィギュレーションファイルのフルパス。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
[ユーザ] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP の場合、このフィールドは適用されません。
[パスワード（Password）] フィールド	リモート サーバのユーザ名のパスワード。プロトコルが TFTP の場合、このフィールドは適用されません。 Cisco UCS Manager では、このパスワードは保存されません。そのため、バックアップ操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。

ステップ 7 **[OK]** をクリックします。

ステップ 8 Cisco UCS Manager に確認ダイアログボックスが表示されたら、**[OK]** をクリックします。

Admin State を有効に設定する場合、Cisco UCS Manager によって、選択した構成タイプのスナップショットが取得され、ファイルがネットワークの場所にエクスポートされます。**[バックアップ設定（Backup Configuration）]** ダイアログボックスの **[バックアップ操作（Backup Operations）]** テーブルに、バックアップ操作が表示されます。

ステップ 9 （任意） バックアップ操作の進行状況を表示するには、次の操作を実行します。

a) **[プロパティ（Properties）]** 領域に操作が表示されない場合、**[バックアップ操作（Backup Operations）]** テーブルの操作をクリックします。

b) **[プロパティ（Properties）]** 領域で、**[FSM の詳細（FSM Details）]** バーの下矢印をクリックします。

[FSM の詳細（FSM Details）] 領域が展開され、操作のステータスが表示されます。

ステップ 10 **[OK]** をクリックし、**[バックアップ設定（Backup Configuration）]** ダイアログボックスを閉じます。

バックアップ操作は完了するまで実行し続けます。進捗を表示するには、**[バックアップ設定（Backup Configuration）]** ダイアログボックスを再度開きます。

Cisco HX ストレージ クラスタのシャットダウンと電源オフ

一部のストレージ クラスタ メンテナンス タスクでは、ストレージ クラスタをシャットダウンする必要があります。これは、ストレージクラスタをオフライン状態にすることとは異なります。また、ストレージ クラスタ内のノードをシャットダウンすることとも異なります。ストレージクラスタを電源オフにすると、クラスタのすべての物理コンポーネントに影響します。

- **電源がオフにされたクラスタ**では、そのすべての物理コンポーネントが電源から切り離されます。

  ストレージクラスタのすべてのコンポーネントを電源オフにする必要が生じることは非常にまれです。定期的なメンテナンスまたはアップグレード プロセスでは、ストレージ クラスタ全体を完全に電源オフにする必要はありません。

- **シャットダウン クラスタ**には、すべてのストレージ クラスタ プロセス（作業 VM、電源ダウンなど）があります。クラスタ内のノードを電源オフにしたり、vCenter や FI クラスタをシャットダウンしたりする操作は含まれません。

- **オフライン クラスタ**は、ストレージクラスタの動作ステータスの 1 つです。不明なエラーまたは特定のエラーが発生した場合や、ストレージクラスタがすでにシャットダウンされた場合には、ストレージ クラスタをオフラインにできます。

Cisco HX ストレージ クラスタをシャットダウンするには、次の手順を実行します。

始める前に

- ストレージ クラスタが正常な状態であることが必要です。
- シャットダウンする前に、HyperFlexクラスタに、HyperFlexの外部にある到達可能な外部NTPおよびDNSリソースが1つ設定されていることを確認します。
- ID の保護属性を持つフルステート バックアップとすべての設定タイプ バックアップの両方を実行します。バックアップ操作の作成 （94 ページ）を参照してください。

手順

ステップ 1 すべての Cisco HX データストアのすべてのワークロード VM のグレースフル シャットダウンを実行します。

あるいは、vMotion を使用してワークロード VM を別のクラスタに移行します。

（注） ストレージ コントローラ VM（stCtlVM）をシャットダウンまたは移動しないでください。

ステップ 2 Cisco HX ストレージ クラスタを正常にシャットダウンします。

a) 任意のコントローラ VM のコマンドラインから、コマンドを実行して、シェル プロンプトが戻るまで待機します。

（注） ネストされた vCenter があるクラスタでは、stcli クラスタ シャットダウンの実行には特定の制限があります。詳細については、『vCenter 導入による既知の制約』を参照してください。

```
# stcli cluster shutdown
```

b) クラスタ情報コマンドを実行します。ストレージ クラスタがオフラインであることを確認します。

```
# hxcli cluster info
```

コマンド応答テキストで、クラスタ サブセクションをチェックし、`healthstate` が `unknown` になっていることを確認します。

この Cisco HX クラスタ シャットダウン手順では、ESXi ホストはシャットダウンされません。

メンテナンス タスクまたはアップグレード タスクで物理コンポーネントを電源オフにする必要がない場合は、この手順を終了して「次の作業」に進みます。

ステップ 3 **HX ストレージ クラスタを電源オフにする**には、ステップ 2 とステップ 3 を完了した後、以下の残りのステップをすべて完了します。

ステップ 4 各ストレージ クラスタ ESX ホストで、コントローラ VM（`stCtlVM`）をシャット ダウンします。

方法を選択します。

vCenter シャットダウン ゲスト OS の使用

a) vCenter クライアントで、各 ESX ホスト上のコントローラ VM を見つけます。
b) controller_vm を右クリックするか、**[電源（Power）] > [ゲスト OS のシャットダウン（Shut Down Guest OS）]** を選択します。.

この方式では、ゲスト VM のグレースフル シャットダウンが行われます。

vCenter ESX Agent Manager を使用する場合

a) vCenter クライアントで、ESX Agent Manager コンソールを開きます。
b) 各 ESX ホストでコントローラ VM を見つけて、**[電源（Power）] > [ゲスト OS のシャットダウン（Shut Down Guest OS）]** の順に選択します。.

この方式では、エージェント VM のグレースフル シャットダウンが行われます。コントローラ VM はエージェント VM の 1 つです。

VCenter ホスト メンテナンス モードを使用する場合

a) vCenter クライアントで、各 ESX ホストを見つけます。
b) ESX ホストを右クリックし、**[メンテナンス モード（Maintenance Mode）] > [メンテナンス モードの開始（Enter Maintenance Mode）]** の順に選択します。

この方式では、コントローラ VM を含め、ESX ホスト内のすべての VM のハード シャットダウンが行われます。

ステップ 5 各ストレージ クラスタ ESX ホストをシャットダウンします。

a) vCenter クライアントで、ホストを見つけます。
b) ホストを右クリックし、**[電源（Power）] > [シャットダウン（Shut Down）]** の順に選択します。

ステップ 6 メンテナンス タスクで必要な場合は、FI を電源オフにします。

Cisco UCS FI は継続的に運用できるように設計されています。実稼働環境では、ファブリック インターコネクトをシャットダウン/再起動する必要はありません。そのため、UCS ファブリック インターコネクトには電源ボタンがありません。

Cisco UCS ファブリック インターコネクトを電源オフにするには、電源ケーブルを手動で引き抜きます。あるいは、FI 電源ケーブルがスマート PDU に接続されている場合は、リモート制御を使用して電源コンセントの電源をオフにします。

a) FI 上のすべてのストレージ クラスタ サーバで緑色の電源 LED が点灯していないことを確認します。
b) セカンダリ FI を電源オフにします。
c) プライマリ FI を電源オフにします。

これで、HX ストレージ クラスタが安全に電源オフになります。

次のタスク

1. ストレージ クラスタのシャットダウンまたは電源オフを必要となるタスクを完了します。たとえば、オフライン アップグレード、ストレージ クラスタの物理的移動、ノードでのメンテナンス作業などのタスクなどです。
   - アップグレード タスクについては、『Cisco HyperFlex Systems Upgrade Guide』を参照してください。
   - ハードウェア交換タスクについては、サーバ ハードウェアのガイドを参照してください。

   タスクによっては、ホストのシャットダウンが必要になることがあります。たとえば、VM の移行、HXDP メンテナンス モードの開始、サーバの電源オフなどです。これらのタスクについては、サーバ ハードウェア ガイドにある手順に従ってください。

（注） ほとんどのハードウェア メンテナンス タスクでは、Cisco HX クラスタをシャットダウンする必要がありません。

2. Cisco HX ストレージ クラスタを再起動するには、Cisco HX ストレージ クラスタの電源オンと起動 （103 ページ） に進んでください。

Cisco HX ストレージ クラスタの電源オンと起動

次の手順は、グレースフル シャットダウンや電源オフの後の Cisco HX ストレージ クラスタの再起動に使用します。通常、ストレージ クラスタでメンテナンス タスクが完了した後には、この手順を行います。

始める前に

Cisco HX ストレージ クラスタのシャットダウンと電源オフ （100 ページ）の手順を完了します。

手順

ステップ 1 FI の電源ケーブルを接続して電源投入します。

a) プライマリ FI の電源をオンにします。UCS Manager にアクセス可能になるまで待機します。

b) セカンダリ FI の電源をオンにします。UCS Manager でこれがオンラインになっていることを確認します。

まれに、ファブリック インターコネクトを再起動しなければならないことがあります。

1. SSH を使用して各ファブリック インターコネクトにログインします。
2. 次のコマンドを発行します。

```
FI# connect local-mgmt
FI# reboot
```

ステップ 2 すべての ESX ホストを FI に接続します。

a) 電源が自動的にオンにならない、ストレージ クラスタ内のノードの電源をオンにします。

通常、ノードは自動的に電源オンになり、ESX にブートするはずです。この正常な動作が行われないノードについては、UCS Manager に接続して UCS Manager からサーバ（ノード）を電源オンにする必要があります。

b) 各 ESX ホストが稼働中で、該当するサービス プロファイルに関連付けられていることを UCS Manager で確認します。

ステップ 3 すべての ESXi ホストがネットワークに到達可能であることを確認します。

すべての管理アドレスに ping します。

ステップ 4 各ノードのメンテナンス モードを終了します。

（注） これは **hxcli cluster start** コマンドによって自動的に実行されます。

ステップ 5 すべてのコントローラ VM の電源が自動でオンにならない場合は、次のいずれかの方法を使用して、すべてのコントローラ VM （stCtlVM）の電源をオンにします。

vSphere クライアントを使用します。

a) vSphere クライアントから、ストレージ コントローラ ホストを参照します。
b) StCtrlVM を右クリックし、**[電源（Power）] > [電源オン（Power On）]** の順に選択します。
c) 各ホストに対して、手順を繰り返します。

ESXi ホストのコマンド ラインを使用します。

a) ホストにログインします。
b) stCtlVM の VMID を特定します。

```
# vim-cmd vmsvc/getallvms
```

c) コントローラ VM の VMID 電源オンを使用する場合。

```
# vim-cmd vmsvc/power.on VMID
```

d) 各ホストに対して、手順を繰り返します。

ステップ 6 すべてのコントローラ VM が起動してネットワークで到達可能になるまで待ちます。その後、確認作業を行います。

各コントローラ VM の管理アドレスに対して ping を実行します。

ステップ 7 ストレージ クラスタが再起動できる状態であることを確認します。

a) SSH を使用して任意のコントローラ VM に接続し、次のコマンドを実行します。

```
# hxcli about
```

b) このコマンドから、ビルド番号を含む完全なストレージ クラスタ情報が返された場合、ストレージ クラスタは起動できる状態にあります。ストレージ クラスタの再起動に進みます。
c) このコマンドから完全なストレージ クラスタ情報が返されない場合は、ホスト上ですべてのサービスが起動するまで待ちます。

ステップ 8 ストレージ クラスタを起動します。

任意のコントローラ VM のコマンド ラインから、次のコマンドを実行します。

```
# hxcli cluster start
```

HX クラスタのシャットダウンしたときに行われたメンテナンス タスクまたはアップグレード タスクに応じて、ノードの HXDP メンテナンス モードやホスト メンテナンス モードが終了している可能性があります。不明なホスト例外に関するエラー メッセージは無視します。

ステップ 9 ストレージ クラスタがオンラインになって正常な状態に戻るまで待ちます。

a) 任意のコントローラ VM から、次のコマンドを実行します。

```
# hxcli cluster info
```

b) コマンドの応答テキストで、クラスタ サブセクションを調べて、`healthstate` が `online` になっていることを確認します。

これには最大で30分かかりますが、最後に既知であった状態によっては、時間が短くなることもあります。

ステップ 10 vCenter から、ESX がデータストアを再マウントしたことを確認します。

クラスタが利用可能になると、データストアは自動的にマウントされて利用可能になります。

ESX がデータストアを認識しない場合は、ESX コマンド ラインから次のコマンドを実行します。

```
# esxcfg-nas -r
```

ステップ 11 ストレージ クラスタが正常な状態になってデータストアが再マウントされたら、ワークロード VM を電源オンにします。

あるいは、vMotion を使用してワークロード VM を元のストレージ クラスタに戻します。

ファブリック インターコネクトの設定の復元

フル ステート バックアップ ファイルを使用して、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元することをお勧めします。同じリリース トレインを使用している場合もフル ステート バックアップを使用してシステムを復元できます。たとえば、リリース 4.5(1a) を実行しているシステムから取得したフル ステート バックアップを使用して、リリース 4.5(2a) を実行しているシステムを復元できます。

VSAN または VLAN 設定の問題を回避するために、バックアップの復元はバックアップ時にプライマリ ファブリック インターコネクトだったファブリック インターコネクト上で実行する必要があります。

始める前に

システム設定を復元するには、次の情報を取得します。

- ファブリック インターコネクト管理ポートの IPv4 アドレスおよびサブネット マスク
- デフォルト ゲートウェイの IPv4 アドレス

（注） すべての IP アドレスは IPv4 である必要があります。IPv6 アドレスはサポートされていません。

- バックアップ サーバの IPv4 アドレスおよび認証クレデンシャル
- Full State バックアップ ファイルの完全修飾名

（注） システムを復元するには、Full State コンフィギュレーション ファイルへのアクセスが必要です。その他のタイプのコンフィギュレーション ファイルやバックアップ ファイルでは、システムを復元できません。

手順

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 インターコネクトがオフの場合はオンにします。

ファブリック インターコネクトがブートする際、Power On Self-Test 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、次の情報を入力します。

- 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サブネット マスクまたはプレフィックス
- 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

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 起動ページで **[簡単設定（Express Setup）]** を選択します。

ステップ 7 **[簡単設定（Express Setup）]** ページで **[バックアップから復元（Restore From Backup）]** を選択し、**[送信（Submit）]**をクリックします。

ステップ 8 **[Cisco UCS Manager 初期設定（Cisco UCS Manager Initial Setup）]** ページの **[プロトコル（Protocol）]** 領域で、フル ステート バックアップ ファイルをアップロードするために使用するプロトコルを選択します。

- **SCP**
- **TFTP**
- **FTP**
- **SFTP**

ステップ 9 **[サーバ情報（Server Information）]** 領域で、次のフィールドに値を入力します。

名前	説明
サーバ IP	完全な状態のバックアップ ファイルがあるコンピュータの IPv4 アドレス。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。

名前	説明
バックアップ ファイル パス	フォルダ名やファイル名など、完全な状態のバックアップ ファイルがあるファイルのパス。 （注） バックアップ ファイルのエクスポート元となったシステムと同じバージョンを実行しているシステムを復元するために使用できるのは、Full State バックアップ ファイルのみです。
[ユーザ ID（User ID）]	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP の場合、このフィールドは適用されません。

ステップ 10 **[送信（Submit）]** をクリックします。

コンソールに戻ってシステム復元の進捗状況を確認できます。

ファブリック インターコネクトはバックアップ サーバにログインし、指定された完全な状態のバックアップ ファイルのコピーを取得し、システム設定を復元します。

クラスタ設定の場合、セカンダリ ファブリック インターコネクトを復元する必要はありません。セカンダリ ファブリック インターコネクトがリブートすると、Cisco UCS Manager はただちにその設定をプライマリ ファブリック インターコネクトと同期させます。

vNIC または vHBA の変更後の PCI パススルーの設定

説明

vNIC または vHBA を手動で Cisco HyperFlex (HX) サービス プロファイルまたはサービス プロファイル テンプレートに追加すると、PCI デバイスが再列挙され、VMware directpath I/O 設定が失われます。サービスプロファイルを変更すると、ホストハードウェアが更新されるため、PCI パススルーを再設定する必要があります。サービス プロファイルを変更した ESX ホストごとに次の手順を実行します。

変更した ESX ホストのストレージ コントローラ VM で次の手順を実行します。

アクション：ESX ホスト上で vSphere サービス プロファイルを更新する

手順

ステップ 1 ESX ホストを HXDP メンテナンス モードにします。

ステップ 2 サービス プロファイルで変更（ハードウェアの追加など）を行うか、変更を確認します。

ステップ 3 ESX ホストをリブートします。

このホストのダイレクト パス設定が失われます。

ステップ 4 vCenter にログインして、[DirectPath I/O 設定（DirectPath I/O Configuration）] ページを選択します。

vCenter クライアントで：***[ESX* ホスト（*ESX host*）*]*** > **[設定（Configuration）] タブ** > **[ハードウェア（Hardware）] ペイン** > **[詳細設定（Advanced Settings）]** > **[編集（Edit）]** の順に選択します。

vCenter Web クライアント：**[vCenter インベントリ（vCenter Inventory）]** で、**[リソース（Resources）]** > **[ホスト（Hosts）]** > ***ESX* ホスト** > **[管理（Manage）]** > **[設定（Settings）]** > **[ハードウェア（Hardware）]** > **[PCI デバイス（PCI Devices）]** > **[編集（Edit）]** の順に選択します。

ステップ 5 パススルー用の LSI カードを選択します。

a) [DirectPath I/O 設定（DirectPath I/O Configuration）] ページから、**[パススルーの設定（Configure Passthrough）]** を選択します。
b) [パススルー用のデバイスをマーク（Mark devices for passthrough）] リストから、パススルー用の LSI カードを選択します。
c) [OK] をクリックします。

ステップ 6 ESX ホストをリブートします。

ステップ 7 HX ストレージ コントローラ VM（StCtlVM）の設定を編集して、PCI デバイスを HX ストレージ コントローラ VM に再マップします。

a) 不明な PCI デバイスを見つけて削除します。

vCenter クライアント：***HX* ストレージ コントローラ *VM*** を右クリックして、**[設定の編集（Edit Settings）]** > **[PCI デバイス 0（PCI device 0）]** > **[削除（Remove）]** > **[OK]** の順に選択します。

vCenter Web クライアント：***HX* ストレージ コントローラ *VM*** を右クリックして、**[設定の編集（Edit Settings）]** > **[PCI デバイス 0 の削除（Remove PCI device 0）]** > **[OK]** の順に選択します。

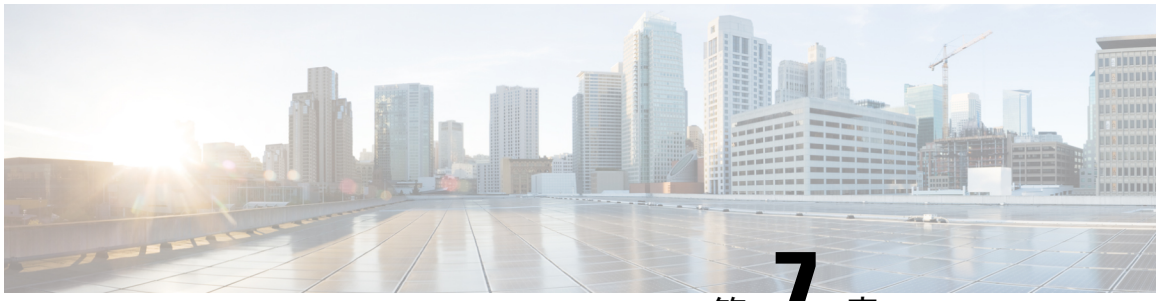
b) LSI ロジック PCI デバイスを見つけて追加し直します。

vCenter Web クライアント：***HX* ストレージ コントローラ *VM*** を右クリックして、**[設定の編集（Edit Settings）]** > **[PCI デバイス（PCI Device）]** > **[追加（Add）]** > **[LSI 論理 PCI デバイス（LSI Logic PCI device）]** > **[OK]** の順に選択します。

vCenter Web クライアント：***HX* ストレージ コントローラ *VM*** を右クリックして、**[設定の編集（Edit Settings）]** > **[PCI デバイス（PCI Device）]** > **[追加（Add）]** > **[LSI 論理 PCI デバイス（LSI Logic PCI device）]** > **[OK]** の順に選択します。

ステップ 8 ESX ホストの HXDP メンテナンス モードを終了します。

ホストが再びアクティブになると、HX ストレージ コントローラ VM が正常にブートして、ストレージ クラスタに再参加します。



第 7 章

暗号化の管理

SED 暗号化

自己暗号化ドライブの概要

自己暗号化ドライブ（SED）には、着信データの暗号化と発信データの復号化をリアルタイムで行う特殊なハードウェアが備わっています。ディスク上のデータは常に暗号化された形で保存されます。この暗号化と復号化は、メディア暗号キーによって制御されます。このキーがプロセッサやメモリに保管されることは決してありません。

メディア暗号キーの暗号化には、セキュリティキー（キー暗号キーまたは認証パスフレーズとも呼ばれます）が使用されます。SED を有効にするには、セキュリティ キーを提供する必要があります。ディスクがロックされていない場合、データを取得するために必要なキーはありません。

Cisco HyperFlex システムでは、セキュリティキーをローカルまたはリモートで設定できます。ローカルでキーを設定する場合は、キーを覚えておく必要があります。キーを忘れてしまった場合、そのキーを再取得することはできず、ドライフの電源再投入によってデータが失われます。キー管理サーバ (KMIP サーバとも呼ばれる) を使用すると、リモートでキーを設定できます。この方法により、ローカル管理でのキーの保管と取得に伴なう問題に対処することができます。

SED の暗号化と復号化はハードウェアを介して行われます。したがって、システムの全体的なパフォーマンスには影響がありません。SED は、瞬間的な暗号化消去によってディスクの廃止コストや再配置コストを削減します。暗号化消去は、メディア暗号キーを変更することによって実行されます。ディスクのメディア暗号キーが変更されると、そのディスク上のデータは復号不能になるので、ただちにデータが使用不可になります。

SED ベースのクラスタでは、暗号化を任意に有効または無効にできます。いつでも 2 つの状態の間を自由に移動できます。詳細については、HX Hardening Guide を参照してください。

HyperFlex クラスタが暗号化に対応するかどうかの確認

を使用して確認する HX データ プラットフォーム プラグイン

1. HX データ プラットフォーム プラグインから vSphere Web クライアントにログインします。
2. **[Global Inventory Lists (グローバル インベントリ リスト)] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [Cluster_Name] > [Summary (概要)]** > の順に選択します。
3. HyperFlex クラスタに SED ドライブがあり、暗号化に対応している場合は、**[サマリー（Summary）]** タブの先頭に **[保管中のデータの暗号化可能（Data At Rest Encryption-Capable）]** と表示されます。

HX 接続 ユーザ インターフェイスを使用して確認する

1. HX 接続 UI で、**[暗号化（Encryption）]** を選択します。
2. HX クラスタに SED ドライブが含まれていて暗号化可能な場合は、**[Encryption]** ページに **[Data At Rest Encryption-Available]** が表示されます。

ローカル暗号キーの構成

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化（Encryption）] を選択します。

ステップ 2 暗号化ページで、**[暗号化の設定（Configure encryption）]** をクリックします。

ステップ 3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <*eng-fi12.eng.storvisor.com*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*admin*> password

[次へ（Next）] をクリックします。

ステップ 4 ローカルに生成/保管される暗号キーを使って HyperFlex クラスタを保護するには、[ローカル キー（Local Key）] を選択します。

[次へ（Next）] をクリックします。

ステップ 5 このクラスタの**暗号キー（パスフレーズ）**を入力します。

（注） 32 文字ちょうどの英数字を入力します。

ステップ 6 [暗号化を有効にする（Enable Encryption）] をクリックします。

ローカル暗号キーの変更

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化（Encryption）] を選択します。

ステップ 2 [暗号化（Encryption）] ページで、[鍵の再生成（Re-key）] をクリックします。

ステップ 3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	**基本的な情報**
[UCS Manager のホスト名（UCS Manager host name）] フィールド	たとえば、*10.193.211.120* とします。
[ユーザ名（User name）] フィールド	<管理者> ユーザ名。
[パスワード（Password）] フィールド	<*admin*> パスワード。

[次へ（Next）] をクリックします。

ステップ 4 クラスタの [既存の暗号化鍵（Existing Encryption Key）] と、[新しい暗号化鍵（New Encryption Key）] を入力します。

（注） 32 文字ちょうどの英数字を入力します。

ステップ 5 [鍵の再生成（Re-key）] をクリックします。

ローカル暗号キーの無効化

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化（Encryption）] を選択します。

ステップ 2 [暗号化（Encryption）] ページで、[設定の編集（Edit configuration）]ドロップダウン メニューから [暗号化を無効にする（Disable encryption）] を選択します。

ステップ 3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <*eng-fi12.eng.storvisor.com*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*admin*> password

[次へ（Next）] をクリックします。

ステップ 4 クラスタで暗号キーを無効にするには、クラスタに使用している**暗号キー**を入力します。

ステップ 5 [暗号化を無効にする（Disable encryption）] をクリックします。

ステップ 6 クラスタの暗号キーを無効にする操作を確定するには、[暗号化を無効にしますか?（Disableencryption?）] ダイアログボックスで、[はい、暗号化を無効にします（Yes, disable encryption）] をクリックします。

暗号化されたディスクの安全な消去

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、**[システム情報（System Information）]** を選択します。

ステップ 2 **[ディスク（Disks）]** タブで、ローカル キーを安全に消去する**ディスク**を選択します。

ステップ 3 **[安全に消去する（Secure erase）]** ボタンをクリックします。

ステップ 4 クラスタで暗号化されたディスクを安全に消去するには、クラスタで使用中の暗号化キーを入力します。

ステップ 5 **[安全に消去する（Secure erase）]** をクリックします。

ステップ 6 **[このディスクを消去しますか?（Erase this disk?）]** ダイアログボックスで、**[はい、このディスクを消去します。（Yes, erase this disk）]** をクリックし、暗号化されたディスクを安全に消去します。

リモート鍵管理

リモート KMIP 証明書の一般的な処理手順は、次のとおりです。

- 自己署名する場合は、構成でローカル認証局を指定し、ルート証明書を取得します。
- 信頼できるサードパーティ CA を使用する場合は、該当する CA を構成で指定し、そのルート証明書を使用します。
- クラスタ キーの入力を求める HX 暗号化フィールドに、ルート証明書を入力します。
- SSL サーバ証明書を作成し、証明書署名要求（CSR）を生成します。
- CSR に、使用中のルート証明書で署名を付けます。
- クライアント証明書を使用するよう KMIP サーバ設定を更新します。
- SSL 証明書とルート CA が利用可能になったら、選択したベンダーに固有の KMIP サービス構成に進みます。

SafeNet キー管理

SafeNet キー管理サーバを使用した暗号化キーの管理に関する詳細については、『SafeNet Admin Guide』を参照してください。

Vormetric キー管理

Vormetric キー管理サーバを使用した暗号キーの管理について詳しくは、「Vormetric support portal」ドキュメントのダウンロード] セクションを参照してください。

リモート暗号キーの構成

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、**[暗号化（Encryption）]** を選択します。

ステップ 2 暗号化ページで、**[暗号化の設定（Configure encryption）]** をクリックします。

ステップ 3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 *<eng-fi12.eng.storvisor.com>*

UI 要素	基本的な情報
[ユーザ名（User name）] フィールド	*<admin>* ユーザ名
[パスワード（Password）] フィールド	*<root>* パスワード

[次へ（Next）] をクリックします。

ステップ 4 キー管理（KMIP）サーバによって生成されるリモート セキュリティ キーを使って HyperFlex クラスタを保護するには、**[キー管理サーバ（Key Management Server）]** を選択します。

次の証明書のいずれかを使用して、クラスタ内の自己暗号化ドライブをサーバで構成できます。

- **[認証局署名証明書の使用（Use certificate authority signed certificates）]**：外部認証局によって署名された証明書署名要求（CSR）を生成します。
- **[自己署名証明書の使用（Use self-signed certificates）]**: 自己署名証明書を生成します。

[次へ（Next）] をクリックします。

ステップ 5

次のタスク

新しい証明書署名要求または自己署名証明書を生成できます。

証明書署名要求の生成

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、**[暗号化（Encryption）]** を選択します。

ステップ 2 暗号化ページで、**[暗号化の設定（Configure encryption）]** をクリックします。

ステップ 3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 *<eng-fi12.eng.storvisor.com>*
[ユーザ名（User name）] フィールド	*<admin>* ユーザ名

UI 要素	基本的な情報
[パスワード（Password）] フィールド	<*admin*> password

[次へ（Next）] をクリックします。

ステップ 4 **[キー管理サーバ（Key Management Server）]** > **[認証局署名証明書の使用（Use certificate authority signedcertificatess）]** を選択します。

[次へ（Next）] をクリックします。

ステップ 5 キー管理（KMIP）サーバを設定するためにリモート暗号化キーを生成するには、次の詳細を入力します。

UI 要素	基本的な情報
[電子メールアドレス（Email address）] フィールド	<管理者> 電子メール アドレス。
[組織名（Organization name）] フィールド	証明書を要求している組織。 32 文字以下で入力します。
[組織単位名（Organization unit name）] フィールド	組織ユニット 最大 64 文字まで入力できます。
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。 32 文字以下で入力します。
[状態（State）] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以下で入力します。
[国（Country）] フィールド	会社が存在する国。 2 文字のアルファベットを大文字で入力します。
[有効日数（Valid for (days)）] フィールド	証明書の有効期間。

ステップ 6 すべての HyperFlex ノードに対する証明書署名要求（CSR）を生成してダウンロードするには、**[証明書の生成（Generate certificates** をクリックします。

ステップ 7 証明書をダウンロードして、認証局の署名を取得します。[閉じる（Close）] をクリックします。

次のタスク

1. 署名された証明書をアップロードします。
2. KMIP サーバ （キー管理サーバ） を設定します。

CSR（証明書署名要求）を使用したキー管理サーバの構成

始める前に

まず、生成された CSR をローカル マシンに確実にダウンロードし、その CSR に認証局の署名を付け、Cisco HX Data PlatformUI を使ってアップロードして、KMIP（キー管理）サーバを構成します。

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[暗号化（Encryption）] を選択します。

ステップ 2 [暗号化（Encryption）] ページで、[設定の続行（Continue configuration）] をクリックします。

ステップ 3 [設定の続行（Continue configuration）] ドロップダウンリストから、[証明書の管理（Manage certificates）] を選択して CSR をアップロードします。

ステップ 4 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	**基本的な情報**
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <*eng-fi12.eng.storvisor.com*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[次へ（Next）] をクリックします。

ステップ 5 [認証局署名証明書のアップロード（Upload certificate authority signed certificates）] を選択します。**[次へ（Next）]** をクリックします。

ステップ 6 [新しい証明書のアップロード（Upload new certificate）] で、CA 署名付き証明書をアップロードします。**[アップロード（Upload）]** をクリックします。

ステップ 7 [設定の続行（Continue configuration）] ドロップダウン リストから、[キー管理サーバの設定（Configure key management server）] を選択して KMIP サーバを構成します。

ステップ 8 Cisco UCS Manager クレデンシャルを入力して、プライマリ キー管理（KMIP）サーバと、必要に応じてセカンダリ KMIP サーバを設定します。

UI 要素	**基本的な情報**
[プライマリ キー管理サーバ（Primary key management server）] フィールド	プライマリキー管理サーバのIPアドレスを入力します。

UI 要素	基本的な情報
（オプション）[セカンダリ キー管理サーバ（Secondary key management server）] フィールド	冗長性を確保するためにセカンダリ キー管理サーバをセットアップした場合は、ここで詳細情報を入力します。
[ポート番号（Port number）] フィールド	キー管理サーバに使用するポート番号を入力します。
[公開キー（Public key）] フィールド	KMIP サーバ構成中に生成された、認証局の公開ルート証明書を入力します。

ステップ 9 **[保存（Save）]** をクリックします。これで、リモート管理されるキーによってクラスタが暗号化されるようになります。

自己署名証明書の生成

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、**[暗号化（Encryption）]** を選択します。

ステップ 2 暗号化ページで、**[暗号化の設定（Configure encryption）]** をクリックします。

ステップ 3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <*eng-fi12.eng.storvisor.com*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[次へ（Next）] をクリックします。

ステップ 4 **[キー管理サーバ（Key Management Server）]** > **[自己署名証明書を使用（Use self-signed certificates）]** を選択します。

[次へ（Next）] をクリックします。

ステップ 5 キー管理（KMIP）サーバを設定するためにリモート暗号化キーを生成するには、次の詳細を入力します。

UI 要素	基本的な情報
[電子メールアドレス（Email address）] フィールド	<管理者> 電子メール アドレス。
[組織名（Organization name）] フィールド	証明書を要求している組織。 32 文字以下で入力します。
[組織単位名（Organization unit name）] フィールド	組織ユニット 最大 64 文字まで入力できます。
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。 32 文字以下で入力します。
[状態（State）] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以下で入力します。
[国（Country）] フィールド	会社が存在する国。 2 文字のアルファベットを大文字で入力します。
[有効日数（Valid for (days)）] フィールド	証明書の有効期間。

ステップ 6 すべての HyperFlex ノードの自己署名証明書を生成してダウンロードするには、**[証明書の生成（Generate certificates）]** をクリックします。

ステップ 7 署名付き証明書をアップロードし、KMIP サーバ（キー管理サーバ）を設定します。

SSC（自己署名証明書）を使用したキー管理サーバの構成

始める前に

KMIP（キー管理）サーバを構成するには、まず、生成された SSC をローカル マシンにダウンロードしたことを確認してください。

手順

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、**[暗号化（Encryption）]** を選択します。

ステップ 2 [暗号化（Encryption）] ページで、**[設定の編集（Edit configuration）]** をクリックします。

ステップ 3 **[設定の編集（Edit configuration）]** ドロップダウンリストから、**[証明書の管理（Manage certificates）]** を選択します。

ステップ 4 次の Cisco UCS Manager クレデンシャルを入力して、プライマリ キー管理（KMIP）サーバと、必要に応じてセカンダリ KMIP サーバを設定します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 <*eng-fi12.eng.storvisor.com*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*admin*> password

[次へ（Next）] をクリックします。

ステップ 5 プライマリおよびセカンダリ キー管理（KMIP）サーバのクレデンシャルを入力します。

UI 要素	基本的な情報
[プライマリ キー管理サーバ（Primary key management server）] フィールド	プライマリキー管理サーバのIPアドレスを入力します。
（オプション）[セカンダリ キー管理サーバ（Secondary key management server）] フィールド	冗長性を確保するためにセカンダリ キー管理サーバをセットアップした場合は、ここで詳細情報を入力します。
[ポート番号（Port number）] フィールド	キー管理サーバに使用するポート番号を入力します。
[公開キー（Public key）] フィールド	KMIP サーバ構成中に生成された、認証局の公開ルート証明書を入力します。

ステップ 6 **[保存（Save）]** をクリックします。これで、リモート管理されるキーによってクラスタが暗号化されるようになります。

暗号化の再起動

手順

Cisco UCS Manager クレデンシャルを入力して、キー管理サーバまたはローカル キーの設定を再起動し、HyperFlexクラスタを安全に暗号化します。

UI 要素	基本的な情報
[UCS Manager のホスト名（UCS Manager host name）] フィールド	Cisco UCS Manager クラスタ ホスト名。 IP アドレスまたは FQDN を入力します。 *<eng-fi12.eng.storvisor.com>*
[ユーザ名（User name）] フィールド	*<admin>* ユーザ名
[パスワード（Password）] フィールド	*<admin>* password

HyperFlex ソフトウェア暗号化

HyperFlex ソフトウェア暗号化を有効にする

以下の表は HyperFlex ソフトウェア暗号化の有効化ワークフローを要約しています。

ステップ	説明	参考資料
1.	[My Cisco Entitlements（MCE）] から HyperFlex ソフトウェア暗号化パッケージをダウンロードします。	My Cisco Entitlements
2.	管理 CIP にログインして、クラスタ内のすべてのコントローラー VM にパッケージをインストールします。	コマンド `priv install-se-core-package` を実行します。
3.	暗号化パッケージをインストールします。	HX ソフトウェア 暗号化 パッケージをインストールします：13 個以上のノードのあるクラスタ（122ページ）を参照してください。
4.	Intersight の有効化手順に従います。	Intersight HyperFlex ソフトウェア暗号化
5.	クラスタが暗号化されていることを確認してください。	コマンド `hxcli encryption info` を実行します。

（注） クラスタで VMware EVC が有効になっている場合は、EVC ベースラインが Advanced Encryption Standards New Instructions（AES-NI）を備えたノードをサポートしていることを確認してください。現在の EVC ベースラインが AES-NI をサポートしていない場合は、ソフトウェア暗号化を有効にする前に EVC 設定を変更してください。

HyperFlex ソフトウェア暗号化の注意事項と制限事項

HyperFlex ソフトウェア暗号化を有効にする前にこれらの注意事項を確認してください。

- 全ての HyperFlex クラスタ ノードが HXDP リリース 5.0(1b) 以降を実行している場合に HyperFlex ソフトウェア 暗号化を有効化することができます。
- HyperFlex ソフトウェア暗号化を使用した HyperFlex ストレッチ クラスタのサポートは、HXDP リリース 5.0(2a) で導入されました。
- SED HyperFlex 構成は、HyperFlex ソフトウェア暗号化でサポートされていません。
- HyperFlex ソフトウェア暗号化は、Vmware ESXi HyperFlex 構成でのみサポートされます。
- HyperFlex ソフトウェア暗号化パッケージを HX クラスタにインストールするには、AES-NI を有効にする必要があります。
- HyperFlex ソフトウェア暗号化は、既存のデータベースで有効にできません。
- HyperFlex ソフトウェア暗号化は、新しく作成されたデータベースにのみ有効にできます。
- HyperFlex ソフトウェア暗号化がクラスタ/データストアに対して有効化されると、クラスタまたはデータストアに対して無効にできません。
- Once HyperFlex ソフトウェア暗号化がクラスタに対して有効化されると、暗号化されたデータストアまたは暗号化されていないデータストアを作成できます。

HX ソフトウェア 暗号化 パッケージをインストールします：1 - 12 ノードのあるクラスタ

始める前に

[My Cisco Entitlements（MCE）] から HyperFlex ソフトウェア暗号化パッケージをダウンロードし、My Cisco Entitlements を参照してください。

（注） HyperFlex Software Encryption パッケージは独自のソフトウェア PID でライセンスされています。これはHyperFlex Data Platform と Intersight ソフトウェア ライセンスの追加です。詳細については、『Cisco HyperFlex Systems Ordering and Licensing Guide』を参照してください。

手順

ステップ 1 暗号化パッケージを HyperFlex cip ノード（クラスタ管理 IP を保持するノード）に SFTP で送信します。**[ユーザー名/パスワード（username/password）]** と winscp などのファイル 転送 アプリケーションに管理アカウントを使用します。これは、パッケージを /tmp または /home/admin directory にアップロードするはずです。

ステップ 2 クラスタのすべての使用可能なノードのパッケージをインストールするために、cip ノードに SSH を実行し、**priv install-package --cluster** オプションを使用します。

例：

```
priv install-se-core-package --cluster --path /tmp/storfs-se-core_<latest version>_x86_64.deb
```

（注） `--cluster` オプションを使用して暗号化パッケージをインストールするときは、すべてのノードが稼働しており、メンテナンス モードになっていないことを確認してください。

次のタスク

Intersight [HyperFlex ソフトウェア暗号化（HyperFlex Software Encryption）] に移動し、クラスタの暗号化を有効にします。

HX ソフトウェア 暗号化 パッケージをインストールします：13 個以上のノードのあるクラスタ

始める前に

[My Cisco Entitlements（MCE）] から HyperFlex ソフトウェア暗号化パッケージをダウンロードし、My Cisco Entitlements を参照してください。

（注） HyperFlex Software Encryption パッケージは独自のソフトウェア PID でライセンスされています。これはHyperFlex Data Platform と Intersight ソフトウェア ライセンスの追加です。詳細については、『Cisco HyperFlex Systems Ordering and Licensing Guide』を参照してください。

手順

ステップ 1 暗号化パッケージを各 HyperFlex ノードに SFTP で送信します。**[ユーザー名/パスワード（username/password）]** と winscp などのファイル 転送 アプリケーションに管理アカウントを使用します。これは、パッケージを /tmp または /home/admin directory にアップロードするはずです。

ステップ 2 12 個以上のノードのあるクラスタの場合、各ノードに SSH で接続し、`priv install-package -- local` オプションを使用します。

例：

```
priv install-se-core-package --local --path /home/admin/<package-filename>
```

（注） 次の手順に進む前にクラスタをシャットダウンしないでください。HyperFlex ソフトウェア暗号化が有効になります。クラスタをシャットダウンして再起動した場合は、暗号化パッケージを再インストールする必要があります。

次のタスク

Intersight HyperFlex ソフトウェア暗号化 に移動し、クラスタの暗号化を有効にします。

HyperFlex ソフトウェア暗号化の暗号化キーをバックアップする

暗号キーはクラスタに分散形式の複数のコピーで保管されます。クラスタ全体に影響を与える壊滅的な障害から保護するために、データ損失から保護するために暗号キーの帯域外バックアップを作成することをお勧めします。

（注） HX ソフトウェア暗号化が有効になった後で、キー変更のたびごとの DEK をバックアップすることをお勧めします。以前バックアップした DEK は、クラスタでキー変更を行った後で復元できません。

以前保存したバックアップから失ったり、破損したりした場合、クラスタに暗号化された DEK 構成を復元するには、TAC にお問い合わせください。

手順

ステップ 1 `hxcli encryption backup-keys -f <path to file name>` コマンドを実行します。

（注） ファイル名の先頭は **/home/admin/** でなければなりません。

ステップ 2 コマンドが実行されたときにプロンプトされた後で、パス フレーズを入力します。

すべてのパスワード ルールに合格した後で、コマンドは暗号化形式でファイルを正常に保存します。

（注） パスフレーズの長さは最低 8 文字で、少なくとも 1 個の小文字、少なくとも 1 個の大文字、少なくとも 1 個の数字、少なくとも 1 個の特殊文字（!@#$%^&*()_+{}? のいずれか）を含む必要があります。

HyperFlex ソフトウェア暗号化の安全なディスク消去

ディスクのベーシック（モード '0'）および標準（モード '1'/モード '2'）サニタイズを行うためのオプションを備えたソフトウェアベースのディスク消去ユーティリティです。分類は主に、サニタイズされるディスクの領域、データ消去の一部としてのドライブ上の上書きサイクルとパターンの数に基づいています。

安全な消去の操作を実施する前に、以下のことを考慮してください。

- 安全なディスク消去（secure disk erase）は破壊的で不可逆的であり、不適切な使用はデータの損失につながる可能性があります。
- 安全なディスク消去（secure disk erase）ユーティリティはデフォルトで、選択したディスクにデータの最後のコピーが含まれているかどうかをチェックします。このチェックはバイパスしてはなりません。
- 安全なディスク消去（secure disk erase）は、サニタイズのモードとドライブのサイズに応じて、時間のかかる操作になる場合があります。
- 管理者モードから安全な消去操作をトリガーできます。
- 複数のディスクを並行してサニタイズできます。

制限事項

- ブート ディスク/ハウスキーピング ディスクは、安全な消去が許可されていません。
- ディスクが安全に消去されると、ディスクを同じクラスタに再展開することはできません。
- 安全なディスク消去（secure disk erase）は、SED ドライブでサポートされていません。
- 安全なディスク消去（secure disk erase）が進行中のときに、完了するまで同じディスクで消去を実行できません。

手順

ステップ 1 secure_disk_erase コマンドを実行して、ターゲット ディスクの絶対パスを指定します。

例：

```
-d DISK_PATH, --disk-path DISK_PATH
```

ステップ 2 以下のさまざまな消去のモードから選択します。

ベーシック（デフォルト）モードの消去（例 モード '0'）：

例：

```
admin:~$ secure_disk_erase -d /dev/sdh -m 1

 THIS UTILITY WILL IRRECOVERABLY ERASE DATA FROM DRIVE.PROCEED WITH CAUTION.
 All data (including storfs) from the disk /dev/sdh will be destroyed, proceed [Y/N]:y
```

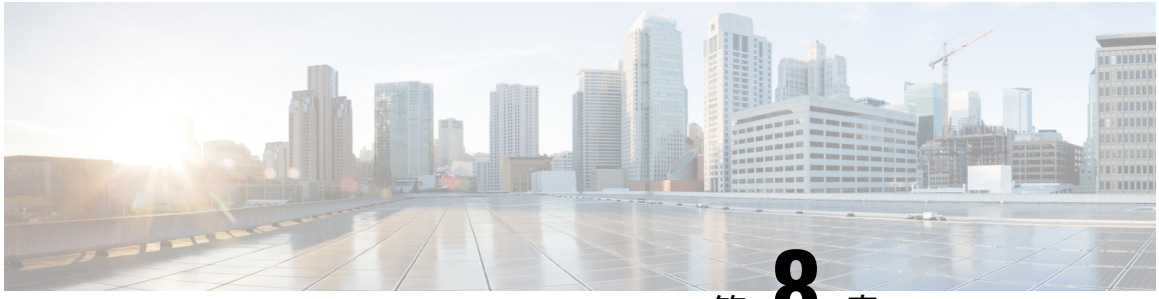
```
Successfully removed the disk from the system: '/dev/sdh'
Starting erase operation for disk '/dev/sdh'
    SEAGATE   ST1200MM0009      CN03   peripheral_type: disk [0x0]
      << supports protection information>>
      Unit serial number: WFK25FY70000C917H4GQ
      LU name: 5000c500a762ca2b

Successfully triggered secure erase operation for the disk: '/dev/sdh'
Please use following command to track the erase progress:
 secure_disk_erase -d /dev/sdh --progress
```

ステップ 3 以下のコマンドを使用して消去の進捗をチェックします。

例：

```
admin:~$ secure_disk_erase -d /dev/sdh --progress
 Fetching the secure erase progress:
 Progress indication: 80.15% don
```

ステップ 4 消去プロセスが完了した後で、ノードから消去したドライブを物理的に取り外してください。



第 8 章

データストアの管理

データストアの管理

データストアは、ストレージの使用状況およびストレージリソースを管理するために HX Data Platform によって使用される論理的コンテナです。ホストは、仮想ディスク ファイルやその他の VM ファイルをデータストアに配置します。データストアは、物理ストレージ デバイスの仕様を非表示にし、VM ファイルを格納するための統一モデルを提供します。

HX Connect UIまたは HX Data Platform プラグイン UI から、リストの追加や更新、名前とサイズの編集、データストアの削除、マウントおよびマウント解除を行うことができます。マウント解除された非ペア データストアの名前は変更できません。vCenter 管理者インターフェイスから HX データストアの名称を変更することはサポートされていませんし、行うべきでもありません。

開始する前に、次のサポート ノートを確認してください。

重要

- vCenter から HX データストアの名前を変更しないでください。HX Connect または Intersight および ESXi ホスト データストア （vCenter に表示される）に表示されるデータストア名は、同一である必要があります。また、大文字と小文字は区別されます。それらが同一でない場合、データストアの拡張、マウント/アンマウントなどの一部の操作に影響します。
- クラスタの暗号化を有効にすることは、データストア作成手順の間にのみ可能です。一度有効にすると、データストアの暗号化を無効にすることはできません。
- HX ネイティブ スナップショットは、複数のデータストアでサポートされていません。
- M5 / M6 ノードを使用する場合は、HyperFlex NFS またはローカルのスプリング パス データストアの残りのスペースをこれらの目的に使用できます。
- VM にフラット vmdk ファイルがあり、1 つはシン プロビジョニング、もう 1 つはシック プロビジョニングである場合、vCenter/ESXi および HX Connect によって報告されるすべてのフラット VMDK ファイルの合計ストレージ使用量は、vCenter および HX によって報告されるデータストアの使用量よりも多くなる可能性があります。接続します。これは、各 VM ファイルの ESXi および vCenter のスペースレポートが、VAAI API を介して拡張統計情報および属性の基盤となる NFS ストレージから送信される「uniqueBytes」属性を無視することが原因である可能性があります。
- VMware ESXi 環境の場合は、vCenter 内のすべての HyperFlex データストアでストレージ I/O が無効になっていることを確認します。この設定はデータストアごとの設定であり、これを有効にすると、予期しないパフォーマンスへの影響が発生する可能性があります。

手順

ステップ 1 インターフェイスを選択します。

- vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** > **[管理]** > **[データストア]** の順に選択します。
- HX Connect から **[データストア]** を選択します。

ステップ 2 データストアを新規作成するか、既存のデータストアを選択して、オプションを表示します。

- データストアの新規作成
- データストア リストの更新
- データストア名とサイズの編集
- データストアの削除
- ホストでのデータストアのマウント
- ホストからのデータストアのマウント解除

データストアの追加

データストアは、物理ストレージの具体的な仕様を隠し、統一モデルでVMファイルを保管できるようにする、ファイルシステムに似た論理コンテナです。また、データストアを使用してISOイメージとVMテンプレートを保存することもできます。

Procedure

ステップ1 インターフェイスを選択します。

- vSphere Webクライアントナビゲータから、**[vCenterインベントリリスト]**>**[Cisco HyperFlex Systems]**>**[Cisco HX Data Platform]**>***[クラスタ（cluster）]***>**[管理]**>**[データストア]**の順に選択します。
- HX Connectから**[データストア]**を選択します。

ステップ2 [データストアの作成（Create Datastore）]を選択します。

ステップ3 データストアの名前を入力します。vSphere Webクライアントではデータストア名に42文字の制限があります。各データストアに固有の名前を割り当ててください。

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。

ステップ5 データ ブロック サイズを指定します。HX 接続 で、**[8K]**または**[4K]**を選択します。デフォルトは8Kです。HXデータ プラットフォーム プラグインでは、デフォルト値が想定されています。VDIワークロードの場合、デフォルトは4kです。

ステップ6 データストアを暗号化するには、**[ソフトウェア暗号化]**チェック ボックスをクリックします。

クラスターでソフトウェア暗号化を有効にする方法の詳細については、HyperFlex ソフトウェア暗号化を有効にする, on page 120を参照してください。

ステップ7 **[OK]**をクリックして変更を確定するか、**[キャンセル（Cancel）]**をクリックしてすべての変更を取り消します。

ステップ8 データストアを確認します。必要に応じて、[更新（Refresh）]アイコンをクリックして新しいデータストアを表示します。

HXデータ プラットフォーム プラグインで、**[管理（Manage）]**>**[データストア（Datastores）]**>**[ホスト（Hosts）]**タブをクリックして、新しいデータストアのマウント ステータスを確認します。

vSphere クライアント アプリケーションを使用してデータストアを確認する場合は、***[ホスト]***>**[構成（Configuration）]**>**[データストア（Datastores）]**に移動すると、ドライブ タイプが `Unknown` としてリストされます。NFSデータベースを「不明」とリストすることは、vSphereの想定される動作です。

データストアの編集

HXデータプラットフォームデータストアは、編集（鉛筆）オプションを使用して変更できます。編集オプションは次のとおりです: 1 データストア名を変更するか、2 にします。データストアのストレージ割り当てを変更します。つまり、データストアのサイズです。

（注） HX リリース 5.0(2a) 以降、既存のデータストアのサイズを減らすことはサポートされていません。5.0(2a) 以降のリリースでデータストアのサイズを縮小しようとすると、次のエラーが表示されます: データ損失を防ぐためにデータストア サイズを縮小することは許可されていません。データストアが新しい場合は、削除して正しいサイズで再作成できます。

（注） コントローラ VM を使用してデータストアの名前を変更しないでください。

手順

ステップ 1 インターフェイスを選択します。

- vSphere Web クライアントナビゲータから、**[vCenter インベントリ リスト]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** > **[管理]** > **[データストア]** の順に選択します。
- HX 接続 から、[データストア（Datastores）] を選択します。

ステップ 2 データストア を選択します。

ステップ 3 データストアのマウントを解除します。

データストアのサイズを変更するだけの場合は、データストアのマウントを解除する必要はありません。このステップをスキップしてください。

ステップ 4 データストアの [編集（Edit）]（鉛筆アイコン）をクリックします。

ステップ 5 必要に応じて、データストア名やサイズを変更します。[OK] をクリックします。

ステップ 6 以前にマウントを解除した場合、データストアを再マウントします。

データストアのマウント解除

データストアのマウント解除の準備をします。

- データストアにVM、テンプレート、スナップショット、またはCD/DVDイメージは常駐していません。これはマウント解除中の最も一般的なエラーです。

- データストアのストレージ I/O 制御は無効です。
- データストアは vSphere HA ハートビートには使用されません。
- データストアは RDM メタデータ ファイルのホスティングには使用されません。RDM はサポートされていません。
- データストアはスクラッチのロケーションとしては使用されません。

データストアのマウントを解除します。

手順

ステップ 1 インターフェイスを選択します。

- vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** > **[管理]** > **[データストア]** の順に選択します。
- HX 接続 から、[データストア（Datastores）] を選択します。

ステップ 2 データストア を選択します。

ステップ 3 [マウント解除（Unmount）] をクリックします。

ステップ 4 データストアのマウント解除を確認して、[OK] をクリックします。

ステップ 5 **必要な場合、部分的なマウント解除から復旧します。**

a) 上記のチェックリストを確認し、いずれかの UI または CLI を使用して再度マウント解除または削除します。

b) データストアを再マウントするには UI または CLI を使用します。

一部のマウント解除の詳細または回復については、部分的にマウント解除されたデータストアの回復（133 ページ） を参照してください。

データストアの削除

データストアを削除するための準備をします。

- すべての VM の電源をオフにします。
- データストアのマウント ポイントで開いているすべてのシェルを閉じます。
- データストア上の HA を無効にします。
- データストアを使用するすべてのアプリケーションを閉じます。

データストアを削除します。

手順

ステップ 1 インターフェイスを選択します。

- vSphere Web クライアントナビゲータから、**[vCenter インベントリ リスト]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** > **[管理]** > **[データストア]** の順に選択します。
- HX 接続 から、[データストア（Datastores）] を選択します。

ステップ 2 データストア を選択します。

ステップ 3 [Delete] をクリックします。

ステップ 4 データストアの削除を確認して、[OK] をクリックします。

データストアの暗号化サポート

リモート プラグイン暗号化を有効にするには、次の手順を実行します。クラスターでソフトウェア暗号化を有効にする方法の詳細については、『Enabling HyperFlex Software Encryption Workflow』を参照してください。

手順

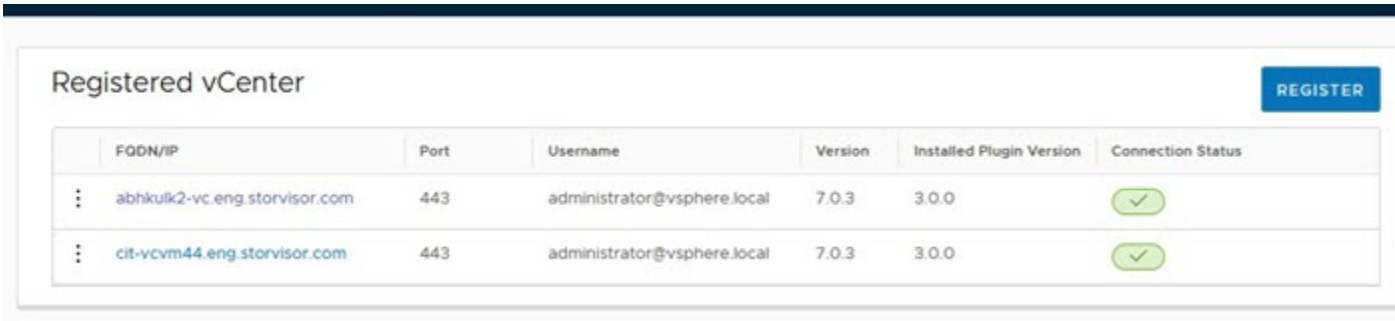
ステップ 1 暗号化するクラスタを選択します。

ステップ 2 **データストア**をクリックします。

ステップ 3 [Create] ボタンをクリックします。[データストア（Datastore）] ウィンドウが表示されます。

a) データストア名を入力します。
b) サイズを入力し、GB または TB を選択します。
c) ブロック サイズを選択し、4K または 8K を選択します。
d) **[ソフトウェア暗号化（Software Encryption）]** チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。新しいデータストアが作成され、データストアテーブル リストに追加されます。



新しいデータストアがリストに表示されない場合は、**[更新（Refresh）]** 矢印をクリックしてリストを再確認します。

部分的にマウント解除されたデータストアの回復

データストアをマウント、マウント解除、または削除すると、データストアが部分的にマウント解除される場合があります。この状態が発生した場合は、必要に応じて、次の手順を実行します。

手順

ステップ 1 試みているタスクに応じて、データストアのマウントの準備、データストアのマウント解除の準備、またはデータストアの削除の準備にある項目を実行します。

ステップ 2 もう一度、HX 接続または HX データ プラットフォーム プラグイン の UI または CLI を介して、データストアのマウント、マウント解除、削除を試します。

ステップ 3 データストアが、必要なマウント状態、マウント解除状態、または削除状態になっていない場合は、次の手順を実行します。

a) VM がデータストアで実行されていないことを確認します。

b) ESX ホストから、HX Data Platform のデータストアが VMware サービス `storageRM` で使用されているかどうかを確認します。

```
# ls -ltra /vmfs/volumes/stfs-ds1/ | grep -i iorm
```

サンプル応答

```
-rwxr-xr-x 1 root root 16511 Jan 20 20:05 .iormstats.sf
drwxr-xr-x 1 root root 1125 Jan 20 20:06 .iorm.sf
```

c) `storagerm` のステータスを確認します。

```
# /etc/init.d/storageRM status
```

サンプル応答

```
storageRM is running
```

d) `storagerm` サービスを停止します。

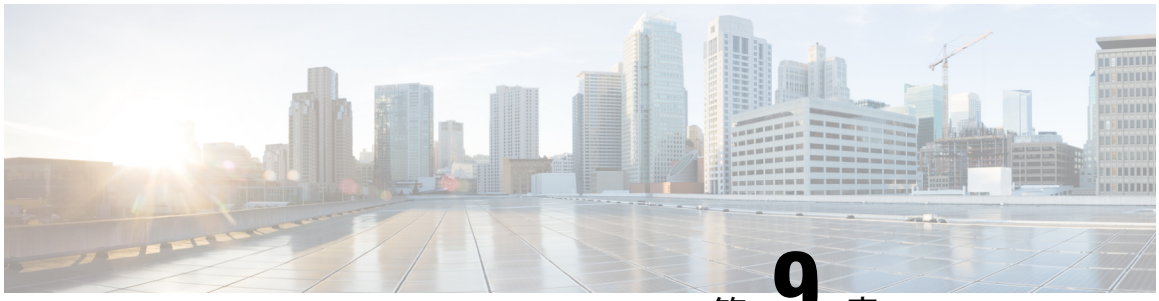
```
# /etc/init.d/storageRM stop
```

サンプル応答

```
watchdog-storageRM: Terminating watchdog process with PID 34096
storageRM stopped
```

e) もう一度、データストアのマウント、マウント解除、または削除を試みます。

f) これは考えられる解決策の 1 つです。これで問題が解決しない場合は、テクニカル アシスタンス センター（TAC）にお問い合わせください。



第 9 章

ディスクの管理

クラスタ内のディスクの管理

ディスク、SSD、または HDD で障害が発生することがあります。その場合、障害が発生したディスクを取り外して交換する必要があります。ホスト内のディスクの取り外しと交換については、サーバ ハードウェア ガイドの手順に従ってください。HX Data Platform は、SSD または HDD を識別しストレージ クラスタに組み込みます。

ストレージ クラスタのデータストア容量を増やすには、ストレージ クラスタ内の各コンバージド ノードに同じサイズとタイプの SSD または HDD を追加します。ハイブリッド サーバの場合は、ハードディスク ドライブ（HDD）を追加します。すべてのフラッシュ サーバでは、SSD を追加します。

（注） 異なるタイプの異なるベンダーから複数のドライブでホットプラグ引き出しおよび交換を実行する場合は、アクションとアクションの間を少し開けます（30秒間）。ドライブをプルし、約 30 秒間一時停止し、交換して、30 秒間一時停止します。それから、次のドライブを 30 秒間プルし、一時停止して、交換します。

場合によっては、ディスクを取り外しても、そのディスクがクラスタのサマリー情報に引き続き表示されることがあります。情報を更新するには、HX クラスタを再起動します。

（注） 1つのHXクラスタから機能ドライブを取り外し、別のHXクラスタに取り付けることはサポートされていません。

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。
- 同じディスク内のサーバ間で操作ディスクを移動する、または同じアクティブ クラスタ内で拡張ノードに移動することはサポートされていません。
- 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、[カタログ アップデート（Catalog Update）]を参照してください。

以下の表にリストされているディスクに加えて、すべての M5/M6 コンバージド ノードには、ESXi がインストールされた M.2 SATA SSD があります。

（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	ESXi のブートでサポートされている方法
• Cisco B200 M5/M6 • C240 M5/M6 • C220 M5/M6 • 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 バージョン4.5（1a）以降でサポートされるブート設定です。

SSD の交換

SSD の交換手順は SSD のタイプによって異なります。障害が発生した SSD を特定し、関連する手順を実行します。

（注） タイプやサイズの異なるストレージ ディスクを 1 台のサーバまたはストレージ クラスタ全体で混在させることはサポートされていません。

- すべて HDD、すべて 3.8 TB SSD、またはすべて 960 GB SSD を使用します。
- 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。
- 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、必ず元のディスクと同じタイプとサイズのものを使用します。

手順

ステップ 1 障害が発生した SSD を特定します。

- キャッシュまたは永続 SSD の場合、ディスク ビーコン チェックを実行します。ビーコンの設定 （88 ページ）を参照してください。

  キャッシュと永続 SSD のみビーコン要求に応答します。NVMe キャッシュ SSD とハウスキーピング SSD はビーコン要求に応答しません。

- キャッシュ NVMe SSD の場合、物理的チェックを実行します。これらのドライブは HX サーバのドライブ ベイ 1 にあります。
- HXAF240c または HX240c サーバのハウスキーピング SSD の場合、サーバ背面の物理的チェックを実行します。
- HXAF220c または HX220c のサーバのハウスキーピング SSD の場合、サーバのドライブ ベイ 2 の物理的チェックを実行します。

ステップ 2 **障害が発生した SSD がキャッシュまたは永続 SSD の場合**、ディスクのタイプに基づいて続行します。

- NVMe SSD については、NVMe SSD の交換 （139 ページ）を参照してください。
- その他すべての SSD の場合は、サーバのハードウェア ガイドに従って、ホスト内の障害が発生した SSD を取り外して交換する手順を実行します。

キャッシュまたは永続ドライブの交換後、HX Data Platform は、SDD をHX データ プラットフォーム識別してストレージ クラスタを更新します。

ノードにディスクが追加されると、ディスクはすぐに HX で使用できるようになります。

ステップ 3 Cisco UCS Manager の **[UCS Manager] > [Equipment (機器)] > [Server (サーバ)] > [Inventory (インベントリ)] > [Storage (ストレージ)]** タブに新しいディスクを含める Cisco UCS Manager には、サーバー ノードを再認識します。これにはキャッシュ ディスクと永続ディスクも含まれます。

（注） サーバーの再認識が中断します。実行する前に、サーバーを HXDP メンテナンス モードにします。

ステップ 4 SSD を交換して、*[*ディスク修復のスケジュールが正常終了しました（*Disk successfully scheduled for repair*）*]* というメッセージが表示された場合、ディスクは存在しますがまだ正しく機能していません。サーバー ハードウェア ガイドの手順に従ってディスクが正常に追加されたことを確認します。

NVMe SSD の交換

SSD の交換手順は SSD のタイプによって異なります。このトピックでは、NVMe キャッシュ SSD を交換するための手順について説明します。

（注） タイプやサイズの異なるストレージ ディスクを 1 台のサーバーまたはストレージ クラスタ全体で混在させることはサポートされていません。

NVMe ディスクを交換するときには常に元のディスクと同じタイプおよびサイズを使用します。

始める前に

HX クラスタ サーバーで NVMe SSD を使用する場合は、次の条件を満たしていることを確認します。

- NVMe Ssd は HX240 および HX220 オールフラッシュおよび All-NVMe サーバーでサポートされています。
- M5 および M6 サーバーのホットスワップ NVMe ドライブは、HX リリース 4.5(1a) 以降でサポートされます。
- NVMe SSD を HGST SN200 ディスクで交換するには HX データ プラットフォーム リリース 2.5(1a) 以降が必要です。
- All-Flash ノードに対して、NVMe SSD はサーバーのスロット 1 でのみ使用できます。その他のサーバー スロットでは NVMe SSD は検出されません。
- All-Flash ノードに対して、NVMe SSD はキャッシュにのみ使用されます。

（注） All-Flash ノードの容量またはハウスキーピング ドライブとして NVMe SSD を使用することはできません。

- M5 サーバーの場合：NVMe キャッシュ ドライブを非 NVMe ドライブに交換する場合（またはその逆に、非 NVMe キャッシュ ドライブを NVMe ドライブに交換する場合）、ケーブルを別の SAS ケーブルに交換する必要があります（たとえば、UCSC-RNVME-240M5 = HXAF240c M5 背面 NVMe ケーブル (1) または UCSC-RSAS-C240M5 = C240 背面 UCSC-RAID-M5 SAS cbl(1)）。これは、ドライブが正しく検出されるようにするために必要です。

（注） M6 サーバーの場合: 前面にあるスロットの配置のため、NVMe キャッシュ ドライブを非 NVMe キャッシュ ドライブに置き換えることはできません。

手順

ステップ 1 障害があるディスクが NVMe キャッシュ SSD であることを確認します。

物理的な検査を実行します。NVMe キャッシュ SSD とハウスキーピング SSD はビーコン要求に応答しません。

障害が発生した SSD が NVMe SSD でない場合は、このガイドの「SSD の交換」セクションを参照してください。

ステップ 2 ESXi ホストを HXDP メンテナンス モードにします。

a) HX Connect にログインします。

b) **[システム情報（System Information）]** > **[ノード（Nodes）]** > **ノード** > **[HXDP メンテナンス モードの開始（Enter HXDP Maintenance Mode）]** の順に選択します。

ステップ 3 サーバー ハードウェア ガイドを参照し、障害がある SSD の取り外しと交換の指示に従います。

（注） HGST NVMe ディスクを取り外すと、同じタイプのディスクを同じスロットに挿入するか、ホストをリブートするまでコントローラ VM に障害が発生します。

キャッシュまたは永続ドライブの交換後、HX Data Platform は、SDD をHX データ プラットフォーム識別してストレージ クラスタを更新します。

ノードにディスクが追加されると、ディスクはすぐに HX で使用できるようになります。

ステップ 4 ESXi ホストをリブートします。これにより、ESXi で NVMe SSD が検出できるようになります。

ステップ 5 ESXi ホストの HXDP メンテナンス モードを終了します。

ステップ 6 Cisco UCS Manager の **[UCS Manager]** > **[Equipment (機器)]** > **[Server (サーバ)]** > **[Inventory (インベントリ)]** > **[Storage (ストレージ)]** タブに新しいディスクを含める Cisco UCS Manager には、サーバー ノードを再認識します。これにはキャッシュ ディスクと永続ディスクも含まれます。

（注） サーバーの再認識が中断します。実行する前に、サーバーを HXDP メンテナンス モードにします。

ステップ 7 SSD を交換して、*[ディスク修復のスケジュールが正常終了しました（Disk successfully scheduled for repair）]* というメッセージが表示された場合、ディスクは存在しますがまだ正しく機能していません。サーバー ハードウェア ガイドの手順に従ってディスクが正常に追加されたことを確認します。

M5 および M6 サーバーのホットスワップ NVMe ドライブ

Cisco HyperFlex リリース 4.5(1a) 以降、VMD 対応の BIOS オプションがアクティブになっている M5 および M6 サーバーは、新規インストールで NVMe ドライブをホットスワップすること、および HX+ UCS アップグレードを組み合わせたアップグレードを実行することができます。VMD の有効化が BIOS で設定されているため、HXDP のメンテナンス モードや ESXi の再起動を必要とせずに、NVMe ドライブをホット スワップ可能にすることができます。

VMD が有効になっていることを確認するには、次の手順に従います。

始める前に

HX クラスタ サーバーで NVMe SSD を使用する場合は、NVMe SSD の交換 （139 ページ） の条件を満たしていることを確認します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで **[サーバー（Servers）]** をクリックします。

ステップ 2 Go to **[ポリシー（Policies）]** > **[ルート（Root）]** > **[BIOS ポリシー（BIOS Polices）]**に移動します。

ステップ 3 **[ルート（root）]** > **[サブ組織（Sub-Organizations）]** > **で、自身の組織**を展開します。

ステップ 4 hx-bios-af (M5 の場合) または hx-bios-m6-af (m6 の場合) を選択します。

ステップ 5 **[情報（Info）]** をクリックします。

ステップ 6 [BIOS ポリシー（BIOS Policy）] ウィンドウが表示されます。**[詳細（Advanced）] タブで、**>**[LOM]**>**[PCIe スロット（ PCIe Slots）]**を選択します。

ステップ 7 下にスクロールして **[VMD 有効（VMD Enable）]** 設定を確認し、**[有効（Enabled）]** になっているかチェックします。

Cisco HX リリース 5.0(2b)以降のハウスキーピング SSDs の交換

（注） この手順は、HXAF220c M5、HX220c M5、HXAF240c M5、HX240c M5、HXAF220c M6、HX220c M6、HXAF240c M6、および HX240c M6 サーバーのみに適用されます。

障害が発生したハウスキーピング SSD を特定し、関連する手順を実行します。

手順

ステップ 1 障害が発生したハウスキーピング SSD を特定します。

ハウスキーピング ドライブはビーコン チェックを通して表示されないため、SSD ドライブを物理的にチェックします。

ステップ 2 SSD を取り外し、同じサポートされている種類とサイズの新しい SSD に交換します。サーバ ハードウェア ガイドの手順に従います。

サーバ ハードウェア ガイドでは、SSD を交換するために必要な物理的手順について説明しています。

（注） ハードウェア手順を実行する前に、ノードを HXDP メンテナンス モードにします。ハードウェア手順を実行したら、ノードの HXDP メンテナンス モードを終了します。

ステップ 3 SSH を使用して、cip ノード（他の作業ノード）のストレージ コントローラ VM にログインし、次のコマンドを実行して **bootdev** パーティションを作成します。

```
priv createBootdevPartitions --target 10.20.24.69
```

サンプル応答

```
hxshell:~$ priv createBootdevPartitions --target 10.20.24.69
Enter the root password:
create Bootdev Partitions initiated on 10.20.24.69
```

（注） ターゲットは、影響を受けるノードのストレージ コントローラ VM IP である必要があります。

このコマンドは、影響を受けるノードを再起動します。

ステップ 4 ストレージ コントローラ VM が自動的に再起動するのを待ちます。

ステップ 5 ストレージ コントローラ VM の再起動が完了したら、新しく追加された SSD でパーティションが作成されていることを確認します。コマンドを実行します。

```
# df -ah
```

サンプル応答

```
...........
/dev/sdb1 63G 324M 60G 1%
/var/stv /dev/sdb2 24G 173M 23G 1% /var/zookeeper
```

ステップ 6 既存のストレージ クラスタにインストールされている HX Data Platform インストーラ パッケージのバージョンを確認します。

```
# hxcli cluster version
```

すべてのストレージクラスタ ノードに、同じバージョンがインストールされている必要があります。ストレージ クラスタ内の、新しい SSD を搭載したノード以外のノードのコントローラ VM で、このコマンドを実行します。

ステップ 7 **[ユーザー名（user name）]/[パスワード（password）]**の管理者アカウントと、**winscp** などのファイル転送アプリケーションを使用して、影響を受けるノードのストレージ コントローラ VM に HX データ プラットフォーム インストーラ パッケージを SFTP で送信します。これは、パッケージを `/tmp` にアップロードするはずです。パッケージを `/tmp` ディレクトリにコピーした後、解凍します。

```
# tar -zxvf storfs-packages-<version>.tgz
```

ステップ 8 SSH を使用して、cip ノード（他の作業ノード）のストレージ コントローラー VM にログインし、次のコマンドを実行します。

```
priv housekeeper-preinstall --target 10.20.24.69
```

サンプル応答：

```
hxshell:~$ priv housekeeping-preinstall --target 10.20.24.69
      Enter root password :
      Copied secure files
```

（注） /etc/springpath/secure/* フォルダのセキュア ファイルを、動作中の別のコントローラ マシンから該当するノードにこのコマンドは、コピーします。

ステップ 9 cip ノード（他の作業ノード）のストレージ コントローラ VM で次のコマンドを実行して、HX Data Platform インストーラ パッケージをインストールします。

プライベートハウスキーピングインストパッケージ – ターゲット 10.20.24.69

サンプル応答：

```
hxshell:~$ priv housekeeping-inst-packages –target 10.20.24.69
         Enter root password :
  Installed packages successfully
```

パッケージインストールに要する時間はおよそ 10 分 ー 15 分です。

ステップ 10 cip ノード（他の作業ノード）のストレージ コントローラ VM で次のコマンドを入力して、インストール後のタスクを実行します。

priv housekeeper-postinstall --target 10.20.24.69

サンプル応答：

```
hxshell:~$ priv housekeeping-postinstall --target 10.20.24.69
        Enter root password :
        Successfully done post install tasks
       Successfully installed SE core package on 10.20.24.69 (optional only when Software Encryption
 is enabled on the cluster
```

インストール後のタスクでは、次の手順を実行します。

a) SE コア パッケージをインストールします（クラスタで SE が有効になっている場合はオプション）。
b) CVM をリブートします。

この手順により、影響を受けるノードが再起動されます。ストレージ コントローラ VM が自動的に再起動するのを待ちます。

ステップ 11 **cip-monitor** および **stofs** が実行ステータスであることを確認するには、`priv service cip-monitor status` および `priv service storfs status` コマンドを実行します。

例：

```
hxshell:~$ priv service cip-monitor status
       cip-monitor start/running, process 18251

       hxshell:~$ priv service storfs status
       storfs start/running, process 22057
```

自己暗号化ドライブ（SED）の交換

Cisco HyperFlex System は、自己暗号化ドライブ（SED）とエンタープライズ キー管理サポートによる保管中データの保護を提供します。

- 保管中のデータ対応のサーバとは自己暗号化ドライブを備えたサーバを指します。
- 暗号化された HX クラスタ内のすべてのサーバは、保管中のデータ対応である必要があります。
- 暗号化は、クラスタが作成された後、HX Connect を使用して HX クラスタで設定されます。
- 自己暗号化ドライブを持つサーバは、ソリッド ステート ドライブ（SSD）またはハイブリッドのいずれかです。

重要 暗号化されたデータの安全性を引き続き確保するには、SED を取り外す前にドライブ上のデータが**安全に消去される**必要があります。

始める前に

HX クラスタに暗号化が適用されているかどうかを確認します。

- **暗号化が構成されていない**：SED の取り外しまたは交換を行うには暗号化に関連した前提条件の手順が必要です。SSD の交換 （138 ページ）または ハード ディスク ドライブの交換または追加 （147 ページ）とサーバのハードウェア ガイドを参照してください。
- **暗号化が構成されている**：次の点を確認してください。
  - SED を交換する場合は、メーカーの返品保証（RMA）を取得します。TAC に連絡します。
  - 暗号化のローカル キーを使用している場合は、キーを見つけます。その入力を求められます。
  - SED を取り外す前に、以下のステップを完了します。

手順

ステップ 1 HX クラスタが正常であることを確認します。

ステップ 2 HX クラスタにログインします。

ステップ 3 **[システム情報（System Information）] > [ディスク（Disks）]**ページを選択します。

ステップ 4 取り外すディスクを識別し、確認します。

1. [ロケータ LED をオンにする（Turn On Locator LED）] ボタンを使用します。
2. サーバ上のディスクを物理的に表示します。
3. [ロケータ LED をオフにする（Turn Off Locator LED）] ボタンを使用します。

ステップ 5 取り外すディスクに対応する **[スロット（Slot）]** 行を選択します。

ステップ 6 **[安全に消去する（Secure erase）]** をクリックします。このボタンは、ディスクを選択した後にのみ利用可能です。

ステップ 7 ローカルの暗号化キーを使用する場合は、フィールドに **[暗号化キー（Encryption Key）]** を入力して **[安全に消去する（Secure erase）]** をクリックします。

リモートの暗号化サーバを使用する場合、操作は必要ありません。

ステップ 8 このディスク上のデータを削除することを確認し、**[はい、このディスクを消去します（Yes, erase this disk）]** をクリックします。

警告 **これにより、ディスクからすべてのデータが削除されます。**

ステップ 9 選択した **[ディスク スロット（Disk Slot）]** の **[ステータス（Status）]** が **[削除できます（Ok To Remove）]** に変わるまで待ち、指示に従ってディスクを物理的に取り外します。

次のタスク

（注） 取り外したドライブは、元または別の HX クラスタ内の別のサーバーで再利用しないでください。取り外したドライブを再利用する必要がある場合は、TAC にお問い合わせください。

1. SED 上のデータを安全に消去した後、ディスク タイプ（SSD またはハイブリッド）に適したディスクの交換タスクに進みます。

   ディスク タイプの **[タイプ（Type）]** 列を確認します。

   - **ソリッドステート**（SSD）：SSD の交換（138 ページ） とサーバのハードウェア ガイドを参照してください。
   - **回転**（ハイブリッド ドライブ）：ハード ディスク ドライブの交換または追加（147 ページ） とサーバのハードウェア ガイドを参照してください。

2. 取り外しおよび交換された SED のステータスを確認します。

   SED を取り外した場合：

   - **[ステータス（Status）]**：**[削除できます（Ok To Remove）]** のままです。
   - **[暗号化（Encryption）]**：**[有効（Enabled）]** から **[不明（Unknown）]** に変わります。

SED を交換した場合、新しい SED は自動的に HX クラスタによって使用されるようになります。暗号化が適用されていない場合、ディスクは他の使用可能なディスクと同様に一覧表示されます。暗号化が適用されている場合、セキュリティ鍵が新しいディスクに適用されます。

- **[ステータス（Status）]**：**[無視（Ignored）]** > **[要求（Claimed）]** > **[使用可能（Available）]** と遷移します。
- **[暗号化（Encryption）]**：暗号化鍵が適用された後に、**[無効（Disabled）]** > **[有効（Enabled）]** と遷移します。

ハード ディスク ドライブの交換または追加

（注） タイプやサイズの異なるストレージ ディスクを 1 台のサーバまたはストレージ クラスタ全体で混在させることはサポートされていません。

- すべて HDD、すべて 3.8 TB SSD、またはすべて 960 GB SSD を使用します。
- 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。
- 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、必ず元のディスクと同じタイプとサイズのものを使用します。

手順

ステップ 1 サーバのハードウェア ガイドを参照して、ディスクの追加または交換手順に従います。

ステップ 2 ストレージ クラスタ内の各ノードに同じサイズの HDD を追加します。

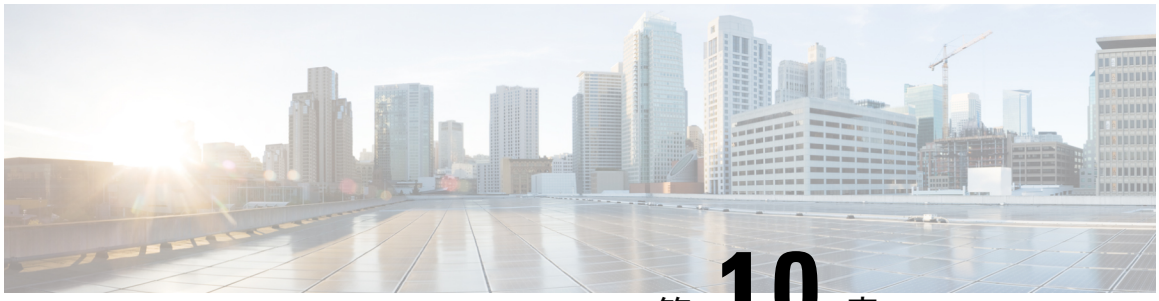
ステップ 3 妥当な時間内に、各ノードに HDD を追加します。

ストレージ クラスタで、ストレージの使用がすぐに開始されます。

[vCenter イベント（vCenter Event）] ログには、ノードへの変更を反映したメッセージが表示されます。

（注） ディスクをノードに追加すると、UCSM サーバ ノード インベントリにそれが表示されなくても、ディスクはすぐに HX で使用可能になります。これにはキャッシュおよび永続ディスクが含まれます。**[機器（Equipment）]** > **[マネージャー（Manager）]** > **[UCS（UCS）]** > **[機器（Equipment）]** > **[サーバー（Server）]** > **[インベントリ（Inventory）]** > **[ストレージ（Storage）]** タブにディスクを含めるには、サーバ ノードを再認識します。

（注） サーバーの再認識が中断します。実行する前に、サーバーを HXDP メンテナンス モードにします。



第 10 章

ノードの管理

ノードの管理

ノードは最初、HX Data Platform インストーラのクラスタの作成機能を使用してストレージ クラスタに追加されます。ノードを既存のストレージ クラスタに追加する場合は、HX Data Platformインストーラのクラスタの展開機能を使用します。ストレージクラスタに対してノードを追加または削除すると、HX Data Platform がそれに応じてストレージ クラスタのステータスを調整します。

- 障害が発生したノードのメンテナンスに関するタスク。
  - ESXi または HX ソフトウェアを再インストールする必要がある。
  - ノード コンポーネントを交換する必要がある。
  - ノードを交換する必要がある。
  - ノードを取り外す必要がある。
- 障害が発生していないノードのメンテナンスに関するタスク。
  - ノードをメンテナンス モードにする。
  - ESX パスワードを変更する。

ノードの管理

（注） 若干の違いはありますが、**サーバ**、**ホスト**、および**ノード**という用語が HyperFlex のマニュアルを通して区別されずに使われています。一般に、サーバは、特定の目的専用のソフトウェアを実行する物理ユニットです。ノードは、ソフトウェア クラスタやサーバのラックなどのより大きなグループ内のサーバです。シスコのハードウェア マニュアルでは、ノードという用語が使われる傾向があります。ホストは、仮想化または HyperFlex ストレージ ソフトウェアを実行しているサーバで、仮想マシンにとっての「ホスト」です。VMware のマニュアルでは、ホストという用語が使われる傾向があります。

手順

ステップ 1 クラスタ内のノードをモニタします。

HX ストレージ クラスタ、ノード、およびノード コンポーネントのステータスがモニタされ、HX Connect、HX Date Platform Plug-in、vCenter UI、およびさまざまなログに、動作ステータス（オンライン、オフライン）値と復元力ステータス値（正常、警告）として報告されます。

（注） 機能状態の区別は、HX Connect と HX Data Platform Plug-in のビューに表示されるストレージ クラスタの動作ステータスと復元力ステータスに影響しますが、それらのステータスとは別個のものです。データ レプリケーション係数（2 または 3）、クラスタ アクセス ポリシー（寛容（lenient）または厳格（strict））、およびストレージ クラスタ内の特定の数のノードごとに、障害が発生したノードの数またはノード内の障害が発生したディスクの数に応じて、ストレージ クラスタの状態が読み取りと書き込み、読み取り専用、またはシャットダウンの間で変化します。

（注） 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、実稼働環境で使用してはなりません。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 ノード障害を分析して、実行するアクションを決定します。

これには、HX Connect、HX Data Platform Plug-in, 、vCenter、または ESXi を介したノード状態のモニタリングと、サーバー ビーコンのチェック、ログの収集と分析が必要になります。

ステップ 3 特定されたタスクを実行します。

- ソフトウェアを再インストールまたはアップグレードします。

  ESXi または HX Data Platform を再インストールする手順については、『*VMware ESXi 用 Cisco HyperFlex システム インストール ガイド*』を参照してください。ソフトウェアのアップグレード手順については、『*Cisco HyperFlex Systems Upgrade Guide*』を参照してください。

- ノード内のコンポーネントを修理します。

  ノード コンポーネント（ソリッド ステート ドライブ（SSD）、ハード ディスク ドライブ（HDD）、電源装置（PSU）、ネットワーク インターフェイス カード（NIC）コンポーネントなど）は、HX

Connect または HX Data Platform Plug-in では設定できませんが、HX Data Platform はこれらのコンポーネントをモニタして、いずれかのアイテムの中断、追加、取り外し、または交換が発生すると、ストレージ クラスタ ステータスを調整します。

ディスクを追加または取り外す手順は、ディスクのタイプによって異なります。PSU や NIC などの現場交換可能ユニット（FRU）を交換するには、サーバ ハードウェア ガイドで説明される手順に従います。

- クラスタ内のノードを交換します。

  通常、ストレージクラスタ内のノードを交換する際は、TAC によるサポートが必要です。要件が満たされていれば、ストレージ クラスタがオンライン（5 ノード以上のクラスタのみ）中またはオフライン（4 ノード以上のクラスタ）中に、ノードを TAC の支援なしで交換できます。

- クラスタからノードを削除します。

  （注） ノードを削除する際は、使用可能なノードの数が最小数の 3 を下回らないようにしてください。3 を下回るとストレージ クラスタが正常に動作しなくなります。3 ノード クラスタ内のノードを削除する際は、常に TAC の支援が必要です。

  オフライン クラスタから最大 2 つのノードを削除できます。

ノードのメンテナンス方法の特定

ノード メンテナンス タスクには、ストレージ クラスタがオフラインのときに実行されるもの、クラスタがオンラインであり、ノードが HXDP メンテナンス モードであることだけが必要である場合に実行できるものがあります。

- **オンライン タスク**：タスク開始前にストレージ クラスタが正常な状態である必要があります。
- **オフライン タスク**：ストレージ クラスタをシャット ダウンする必要があります。

  2 つ以上のノードがダウンしている場合、ストレージ クラスタは自動的にオフラインになります。
- **TAC 支援によるタスク**：通常は、TAC 担当員によって実施される手順が必要になります。

次の表に、関連するノード メンテナンス タスクを実行するときに使用できる方法を示します。

ノード ソフトウェアの修復

ESX と HX Data Platform ソフトウェアは、ストレージ クラスタ内の各ノードにインストールされます。ノード障害分析後にいずれかのソフトウェア項目を再インストールする必要があることが判明した場合は、『*VMware ESXi 用 Cisco HyperFlex システム インストール ガイド*』を参照してください。ソフトウェアのアップグレード手順については、『*Cisco HyperFlex Systems Upgrade Guide*』を参照してください。

ノード ハードウェアの修復

ノード上の修理可能なアイテムで障害が発生した場合です。これには FRU やディスクが該当します。一部のノードコンポーネントにはTACの支援が必要です。たとえば、ノードのマザーボードの交換には TAC の支援が必要です。

クラスタ内のノードの数	クラスタ内の障害発生ノードの数	方法	注記
3	1 つ以上	TAC の支援によるノード修復のみ。	修復作業のためにノードを取り外す必要はありません。ノード上のディスクの交換が含まれます。
4-8	1	オンラインまたはオフラインでのノードの修復。	修復作業のためにノードを取り外す必要はありません。ノード上のディスクの交換が含まれます。

ノードの削除

ノード上の修理不可能なアイテムで障害が発生した場合です。取り外したノードのディスクは、ストレージ クラスタで再利用されません。

クラスタ内のノードの数	クラスタ内の障害発生ノードの数	方法	注記
4	1	オフラインでのノードの取り外し。	4 ノード クラスタで 2 つのノードがダウンしている場合は、TAC の支援が必要です。
5 つ以上	1	オンラインまたはオフラインでのノードの取り外し。	
5 つ以上	2	オフラインでの 2 ノードの取り外し。	5 ノード クラスタで 3 つのノードがダウンしている場合は、TAC の支援が必要です。

ノードの交換とストレージの廃棄

ノード上の修理不可能なアイテムで障害が発生した場合です。取り外したノードのディスクは、ストレージ クラスタで再利用されません。

クラスタ内のノードの数	クラスタ内の障害発生ノードの数	方法	注記
3	1	TAC の支援によるノード交換のみ。	クラスタを最小限の 3 ノードに戻すには、TAC の支援によってノードを交換する必要があります。 3 ノード クラスタで 1 つのノードがダウンしている場合は、TAC の支援が必要です。
4	1	オフラインでのノードの交換。 ディスクは再利用されません。	新しいノードを追加するにはクラスタ拡張を使用します。他のすべてのノードが稼働している必要があります。 4 ノード クラスタで 2 つのノードがダウンしている場合は、TAC の支援が必要です。
5 つ以上	1	オンラインまたはオフラインでのノードの交換。 ディスクは再利用されません。	新しいノードを追加するにはクラスタ拡張を使用します。他のすべてのノードが稼働している必要があります。
5 つ以上	2	オフラインでの 1 または 2 ノードの交換。 ディスクは再利用されません。	新しいノードを追加するにはクラスタ拡張を使用します。他のすべてのノードが稼働している必要があります。 最大 2 つのノードの交換がサポートされています。3つ以上のノードを交換するには、TAC の支援が必要です。

ノードの交換とストレージの再利用

ノード上の修理不可能なアイテムで障害が発生した場合です。取り外したノードのディスクをストレージ クラスタで再利用します。

クラスタ内のノードの数	クラスタ内の障害発生ノードの数	方法	注記
3以上	1 つ以上	TAC の支援のみ。	クラスタを最小限の 3 ノードに戻すには、TAC の支援によってノードを交換する必要があります。 (注) ディスクを再利用するには、古いノードの UUID を新しいノードに割り当てる必要があります。ディスク UUID とノード UUID の関係は固定されているため、再割り当てできません。これは、TAC 支援によるタスクです。

DNS アドレスまたはホスト名による検索

トラブルシューティングの目的では、DNS サーバアドレスまたは DNS サーバホスト名で検索できることが便利な場合があります。これはオプションのタスクです。

手順

ステップ 1 DNS 検索アドレスを割り当てます。

a) HX Data Platform インストーラ仮想マシンにログインします。`ssh` または vSphere コンソール インターフェイスを使用します。

b) `resolv.conf.d` ファイルを編集します。

```
# vi /etc/resolvconf/resolv.conf.d/base
```

c) 変更を確認します。

```
# resolvconf -u
# cat /etc/resolv.conf
```

d) DNS サーバが IP アドレスまたはホスト名から照会できることを確認します。

```
# nslookup ip_address
# nslookup newhostname
```

ステップ 2 DNS ホスト名を割り当てます。

a) HX Data Platform インストーラ仮想マシンにログインします。`ssh` または vSphere コンソール インターフェイスを使用します。

b) 編集のために hosts ファイルを開きます。

```
# vi /etc/hosts
```

c) 次の行を追加し、ファイルを保存します。

ip_address ubuntu *newhostname*

各ホストの *ip_address* に対して、ホストの *newhostname* を入力します。

a) *newhostname* を hostname に追加します。

```
# hostname newhostname
```

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。

手順

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。

ノード ソフトウェアの再インストール

既存のストレージ クラスタのメンバーであるノードでソフトウェアを再インストールするには、TAC にお問い合わせください。このタスクは TAC アシスタンスと共に実行する必要があります。

手順

ステップ 1 TAC からの指示に従って ESX を再インストールします。

サーバがホスト ESX サーバ設定要件に記載されている必要なハードウェアおよび設定を満たしていることを確認します。HX 構成の設定は HX Data Platform プロセス中に適用されます。

ステップ 2 TAC からの指示に従って HX Data Platform を再インストールします。

HX Data Platform の再インストールは常に ESX を再インストールした後で行う必要があります。

IP から FQDN への vCenter クラスタ内のノード識別フォームの変更

このタスクでは、vCenter によるクラスタ内のノードの識別方法を IP アドレスから完全修飾ドメイン名（FQDN）に変更する方法について説明します。

手順

ステップ 1 このタスクを実行するためのメンテナンス ウィンドウをスケジュールします。

ステップ 2 ストレージ クラスタが正常であることを確認します。

ストレージ クラスタのステータスを HX Connect、HX Data Platform プラグイン、またはストレージ コントローラ VM の `stcli cluster info` コマンドのいずれかにより確認します。

ステップ 3 ストレージ クラスタ内の各 ESXi ホストの FQDN を探します。

a) ESXi ホスト コマンド ラインから。

```
# cat /etc/hosts
```

この例では、FQDN は sjs-hx-3-esxi-01.sjs.local です。

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1         localhost.localdomain localhost
::1               localhost.localdomain localhost
172.16.67.157     sjs-hx-3-esxi-01.sjs.local  sjs-hx-3-esxi-01
```

b) ストレージ クラスタ内の各 ESXi ホストに対して繰り返します。

ステップ 4 各 ESXi ホストの FQDN を vCenter、他の ESXi ホストから互いに、およびコントローラ VM から解決できることを確認します。

a) vCenter のコマンド ラインから。

```
# nslookup <fqdn_esx_host1>
# nslookup <fqdn_esx_host2>
# nslookup <fqdn_esx_host3>
...
```

b) ESXi ホストから各 ESXi ホストに対して繰り返します。

c) 各コントローラ VM から各 ESXi ホストに対して繰り返します。

ステップ 5 FQDN 名が解決できない場合は、各 ESXi ホストと各コントローラ VM 上の DNS 設定を確認します。

a) コントローラ VM が DNS サーバの正しい IP アドレスを認識していることを確認します。

コントローラ VM のコマンド ラインから。

```
# stcli services dns show
10.192.0.31
```

a) ESXi ホストの DNS 設定がコントローラ VM と同じであることを確認します。

vCenter から、各 ESXi ホストを選択してから、**[構成（Configuration）]** > **[DNS サーバ（DNS Servers）]** を選択します。

ステップ 6 データセンター名とクラスタ名を探してメモします。

vCenter クライアントまたは Web クライアントから、データセンター名とクラスタ名が表示されるまでスクロールします。それらを書き留めておきます。これらは後の手順で使用します。

ステップ 7 vCenter から、**クラスタ**を削除します。

vCenter から、**データセンター** > **クラスタ**を選択します。**クラスタ**を右クリックし、**[削除（Delete）]** を選択します。

（注） **データセンター**は削除しないでください。

ステップ 8 vCenter で**クラスタ**を再作成します。

a) vCenter から、**データ センター**を右クリックします。**[新規クラスタ（New Cluster）]** を選択します。

b) 削除したクラスタとまったく同じ名前を **[クラスタ名（Cluster Name）]** に入力します。これは、ステップ 6 で書き留めた名前です。

ステップ 9 FQDN 名を使用して、**クラスタ**に ESXi ホスト（ノード）を追加します。すべての ESXi ホストに対してこの手順を繰り返します。

a) vCenter から、**データ センター** > **クラスタ**を右クリックします。**[ホストの追加（Add Host）]** を選択します。
b) FQDN を使用して ESXi ホストを選択します。
c) クラスタ内の各 ESXi ホストに対して繰り返します。

ステップ 10 クラスタを vCenter に再登録します。

```
#  #  stcli cluster reregister
--vcenter-datacenter <datacenter_name>
--vcenter-cluster <hx_cluster_name>
--vcenter-url <FQDN_name>
--vcenter-user <vCenter_username>
--vcenter-password <vCenter_Password>
```

HX バージョン 1.8.1c 以降では、SSO URL が必要ありません。クラスタの再登録の詳細については、新しい vCenter クラスタによるストレージ クラスタの登録 （69 ページ）を参照してください。

ステップ 11 インストール後のスクリプトを使用して、VMware クラスタ HA および DRS を有効にします。

a) admin として HX クラスタ IP にログインし、**# hx_post_install** コマンドを実行します。
b) [Option 1-"New / Existing Cluster"]を選択し、すべてのログイン クレデンシャルを入力します。
c) 新しいライセンス キーを入力する場合は「y」と入力します。
d) クラスタで HA と DRS を有効にするには、「y」と入力します。
e) 他のすべてのオプションで「n」を選択し、スクリプトを終了します。

ノード コンポーネントの交換

ノード上の選択したコンポーネントを交換できます。コンポーネントの中には、ノードが稼働中でも交換できるものがあります。一部のコンポーネントを交換するには、ノードをメンテナンス モードにするか、シャットダウンする必要があります。すべての現場交換可能ユニット（FRU）のリストについては、ご使用のサーバのハードウェア インストール ガイドを参照してください。コンポーネントによっては、交換できないものや、TAC の支援がある場合にのみ交換できるものもあります。次に示すのは、ノードで交換可能なコンポーネントの一般的なリストです。

（注） ディスクを取り外した場合、ディスクが物理的には存在しない状態でも、ディスク UUID が引き続きリストされます。同一クラスタ内の別のノードでディスクを再利用するには、TAC にサポートを依頼してください。

- ノードをシャットダウンする必要がないコンポーネント。これらはホットスワップ可能です。
  - HDD データ ドライブ。前面ベイ

ストレージ クラスタのタスクについては TAC にお問い合わせください。ハードウェアを中心とするタスクについては『ディスクの管理』を参照してください。このコンポーネントを交換するには、両方のタスクが必要です。

- SSD キャッシュ ドライブ。前面ベイ 1

  ストレージ クラスタのタスクについては TAC にお問い合わせください。ハードウェアを中心とするタスクについては『ディスクの管理』を参照してください。このコンポーネントを交換するには、両方のタスクが必要です。

- ファン モジュール

  このコンポーネントを交換するには、ハードウェア インストール ガイドを参照してください。

- 電源

  このコンポーネントを交換するには、ハードウェア インストール ガイドを参照してください。

- ノードをメンテナンス モードにしてシャットダウンする必要があるコンポーネント。

  次に示すすべてのコンポーネントについては、ハードウェア インストール ガイドを参照してください。

  - ハウスキーピング SSD

    このコンポーネントを交換するには、ストレージ クラスタ タスクとハードウェア中心のタスクの両方が必要です。

  - マザーボード上の RTC バッテリ

（注） マザーボード自体は交換可能コンポーネントではありません。ローカル ハードウェア ストアからバッテリを購入し、交換する必要があります。

  - DIMMS
  - CPU とヒートシンク
  - 内部 SD カード
  - 内部 USB ポート
  - モジュラ HBA ライザー（HX 220c サーバ）
  - モジュラ HBA カード
  - PCIe ライザー アセンブリ
  - PCIe カード

- トラステッド プラットフォーム モジュール
- mLOM カード
- RAID コントローラ
- 仮想インターフェイス カード（VIC）
- グラフィック処理ユニット（GPU）

ノードの削除

ノードの削除は、次のクラスタタイプでサポートされています。

表 *4:* ノードの削除をサポートするクラスタタイプ

クラスタ タイプ	コンバージド	コンピューティング
Standard	はい	○
ストレッチ	いいえ	はい
Edge	はい（注を参照） **（注）** ノード（コンピューティングまたはコンバージド）の削除は、3 ノードよりも大きなクラスタでのみサポートされます。4 ノードのエッジ クラスタの場合は、オフライン ノード削除プロセスに従います。5 つ以上のノードを持つエッジクラスタの場合、オンラインおよびオフラインのノード削除プロセスがサポートされています。ただし、オンライン ノード削除方法を**お勧めします。**	

クラスタ内のノードの数に応じて、クラスタがオンラインの場合、またはクラスタをオフラインにする必要がある場合に、ノードを削除できます。その前に、必要な準備手順が完了していることを確認する必要があります。

影響するコンテキストは、コンバージド ノードの数に基づきます。コンピューティング ノードの数は、ノード削除のプロセスに影響しません。

一度に 1 つのコンバージド ノードのみを削除できます。

4つのコンバージド ノードがあるクラスタの場合は、オフライン ノード削除プロセスに従います。5つ以上のコンバージド ノードを持つクラスタの場合は、オンライン ノード削除プロセスに従います。

（注） 3 ノード クラスタからのコンバージド ノードの削除はサポートされていません

（注） クラスタがオフラインのときにノードを削除すると、そのノードをクラスタに戻すことはできません。

論理アベイラビリティゾーン（LAZ）が設定された HyperFlex クラスタのノードを削除する前に、LAZ を無効にする必要があります。

LAZ が HyperFlex クラスタで使用される場合、LAZ を再有効化する前に、残りのノードの数が、LAZ のガイドラインと考慮事項に従って LAZ をサポートするバランスの取れた構成である必要があります。

ノードの削除の準備

ストレージ クラスタからノードを削除する前に、次の手順を実行します。

手順

ステップ 1 クラスタが正常であることを確認します。

```
# stcli cluster info
```

次の例の応答は、ストレージ クラスタがオンラインで正常であることを示します。

```
locale: English (United States)
state: online
upgradeState: ok
healthState: healthy
state: online
state: online
```

ステップ 2 SSH がストレージ クラスタ内のすべてのノード上の ESX で有効になっていることを確認してください。

ステップ 3 分散リソース スケジューラ（DRS）が有効になっていることを確認してください。

DRS は、電源がオンの VM だけを移行します。ネットワークで VM の電源がオフになっている場合は、削除されないストレージ クラスタ内のノードにこれらの VM を手動で移行する必要があります。

（注） DRS を使用できない場合は、仮想マシンをそのノードから手動で移動します。

ステップ 4 zkEnsemble をメモします。これには、コントローラ VM（CVM）のデータ IP が含まれます。

```
Example:
admin:~$ cat /etc/springpath/stMgr.cfg
{"0":"10.104.18.37:2181","1":"10.104.18.38:2181","2":"10.104.18.39", "3":"10.104.18.40:2181",
 "4":"10.104.18.41:2181"}
```

削除されたノードが ucs-308 で、その CVM データ IP が 10.104.18.40 の場合、ノードの削除後に上記のコマンドを実行すると、その CVM データ IP は表示されなくなります。

ステップ 5 削除するノードをメンテナンス モードにします。次の方法を選択します。vSphereGUI、コントローラVM コマンドライン（CLI）、または HyperFlex Connect システム情報パネル:

GUI

a) 各ホストを右クリックし、リストを下にスクロールし、**[メンテナンス モード（Cisco Maintenance Mode）] > [メンテナンス モードの開始（Enter Maintenance Mode）]** の順に選択します。

[vSphere メンテナンス モード（vSphere Maintenance Mode）] オプションは、ホストの右クリック メニューの上部にあります。リストの下部までスクロールし、[Maintenance Mode] を選択します。

b) HX Connectで、**[管理（MANAGE）] > [システム情報（System Information）] パネルの [ノード（Node）] タブ**からノードを選択し、**[HXDP メンテナンス モード（HXDP Maintenance Mode）]** ボタンをクリックします。

CLI

a) 管理ユーザーとしてコントローラ VM にログインします。

b) **stcli cluster info** 実行し、`stNodes: セクション` を探します。

```
# stcli cluster info

stNodes:
    ----------------------------------------
    type: node
    id: 689324b2-b30c-c440-a08e-5b37c7e0eefe
    name: ucs-305
    ----------------------------------------
    type: node
    id: 9314ac70-77aa-4345-8f35-7854f71a0d0c
    name: ucs-306
    ----------------------------------------
    type: node
    id: 9e6ba2e3-4bb6-214c-8723-019fa483a308
    name: ucs-307
    ----------------------------------------
    type: node
    id: 575ace48-1513-0b4f-bfe1-e6abd5ff6895
    name: ucs-308
    ----------------------------------------
    type: node
    id: 875ebe8-1617-0d4c-afe1-c6aed4ff6732
    name: ucs-309
```

`stNodes` セクションで、`id` がクラスタ内の各ノードがリストされます。削除する必要があるノード ID または名前を見つけます。

c) ESX ホストをメンテナンス モードに移行します。

```
# stcli node maintenanceMode (--id ID | --ip NAME) --mode enter
```

（`stcli node maintenanceMode --help` も参照してください）

たとえば、ノード ucs-308 を削除するには、次の手順を実行します。

```
Example:
stcli node maintenanceMode –id 575ace48-1513-0b4f-bfe1-e6abd5ff6895
or
stcli node maintenanceMode –ip 10.104.18.40
```

ステップ 6 2時間待機し、stcli cluster storage-summaryで修復情報をモニタします。「ストレージクラスタが正常です」と表示されるまで待機する必要があります。次の例に示すように、

Example:

```
admin:$ stcli cluster storage-summary | grep -i heali -A 8
healingInfo:
    inProgress: False
resiliencyInfo:
    messages:
        ----------------------------------------
        Storage node 10.104.18.40 is unavailable.
        ----------------------------------------
        Storage cluster is healthy.
        ----------------------------------------
```

Before the healing starts you will see following:

```
admin:$ date; stcli cluster storage-summary | grep -i heali -A 8
Thu Sep 30 12:33:57 PDT 2021
healingInfo:
inProgress: False
resiliencyInfo:
messages:
----------------------------------------
Storage cluster is unhealthy   .
----------------------------------------
Storage node 10.104.18.40 is unavailable   .
----------------------------------------
```

After 2 hours + you will see following:

```
admin:$ stcli cluster storage-summary | grep -i heali -A 8
healingInfo:
messages:
Space rebalanc   ing in progress, 83 % completed.
inProgress: True
percentComplete: 83
estimatedCompletionTimeInSeconds: 211
resiliencyInfo:
messages:
```

次のタスク

ノードの削除に進みます。ストレージクラスタ内のノードの数に基づいて、オンラインまたはオフラインの方法を選択します。

オンライン ストレージ クラスタからのノードの削除

導入環境をクリーンアップするか、またはストレージ クラスタからノードを削除するには、`stcli node remove` を使用します。

（注） 連続して複数のノードを削除できます。ただし、一度に1つのノードを削除する場合、および連続する各ノード削除の間にクラスタが正常な状態である場合に限り。また、ノードを削除するための準備に必要な手順を実行している必要があります。詳細については、ノードの削除の準備 （161 ページ） を参照してください。

（注） 論理アベイラビリティゾーン（LAZ）が設定された HyperFlex クラスタのノードを削除する前に、LAZ を無効にする必要があります。

LAZ が HyperFlex クラスタで使用される場合、LAZ を再有効化する前に、残りのノードの数が、LAZ のガイドラインと考慮事項に従って LAZ をサポートするバランスの取れた構成である必要があります。

（注） このタスクの手順を実行する前に、コントローラ VM またはその他の HX Data Platform コンポーネントを削除しないでください。

手順

ステップ 1 **stcli cluster info** コマンドを実行し、`stNodes: section` を探して、削除する必要があるノードを見つけます。この情報は、ノードをメンテナンスモードにした場合にも使用できます。

Example:

```
    ----------------------------------------
stNodes:
type: node
id: 689324b2-b30c-c440-a08e-5b37c7e0eefe
name: ucs305

type: node
id: 9314ac70-77aa-4345-8f35-7854f71a0d0c
name: ucs306

type: node
id: 9e6ba2e3-4bb6-214c-8723-019fa483a308
name: ucs307

type: node
id: 575ace48-1513-0b4f-bfe1-e6abd5ff6895
name: ucs308

type: node
id: 875ebe8-1617-0d4c-af
name: ucs 309
```

5 -ノード クラスタからノードを削除するには、 **stcli node remove** コマンドを次のように実行します。

- **stcli node remove –ip-1 ucs 308** または
- **stcli node remove –-id-1 575ace48-1513-0b4f-bfe1-e6abd5ff6895**

`stcli node remove` コマンドが正常に完了すると、システムにより、ストレージ クラスタの状態が [正常（Healthy）] になるまで、ストレージ クラスタの再調整が行われます。この期間中に障害テストを実行しないでください。ストレージ クラスタは引き続き正常です。

ストレージ クラスタ内にノードがないため、HXDP メンテナンス モードを終了する必要はありません。

（注） ストレージ クラスタ内のコンバージド ノードを取り外す場合は、TAC と一緒に作業することを強くお勧めします。取り外したコンバージド ノードやディスクは、元のクラスタで再利用しないでください。

（注） 削除したノードを別のストレージ クラスタ内で再利用するには、テクニカル アシスタンス センター（TAC）にご連絡ください。ノードを別のストレージクラスタで利用できるように準備するには、追加手順が必要です。

ステップ 2 ノードがストレージ クラスタから削除されていることを確認します。

a) ストレージ クラスタ情報を確認します。

```
# stcli cluster storage-summary
```

b) 応答の `ActiveNodes` エントリを調べ、クラスタのノード数が 1 つ少なくなっていることを確認します。

c) 削除されたノードが Ensemble の一部ではないことを確認します。次に例を示します。

Example:

```
admin:~$ cat /etc/springpath/stMgr.cfg
{"0":"10.104.18.37:2181","1":"10.104.18.38:2181","2":"10.104.18.39", "3":"10.104.18.40:2181",
 "4":"10.104.18.41:2181"}
```

たとえば、削除されたノードが ucs-308 で、その CVM データ IP が 10.104.18.40 の場合、上記のようにノード削除後に上記のコマンドを実行すると、その CVM データ IP は表示されなくなります。

.

5 つ以上のノードがあり、削除されたノードがアンサンブルの一部であった場合、新しいノード IP が `crmZKEnsemble` に表示されます。たとえば、クラスタに最初に 7 つのノード（10.104.18.37ー10.104.18.43）があり、`crmZKEnsemble` に 10.104.18.37:2181,10.104.18.38:2181,10.104.18.39:2181、10.104.18.40:2181、10.104.18.41 がある場合：2181、その後、10.104.18.40 の削除後、`crmZKEnsemble` は次のいずれかを持ちます。

10.104.18.37:2181,10.104.18.38:2181,10.104.18.39:2181、10.104.18.42:2181、10.104.18.41:2181 または

10.104.18.37:2181,10.104.18.38:2181,10.104.18.39:2181、10.104.18.43:2181、10.104.18.41:2181

ステップ 3 `hxcli disk list` コマンドを実行して、削除されたノードのディスクが表示されなくなったことを確認します。

```
admin:~$ hxcli disk list --no-loader
+-----------+------------------+------+----------+---------+------------+-------------+
| NODE NAME | HYPERVSIOR STATUS | SLOT | CAPACITY | STATUS | TYPE | USAGE |
+-----------+------------------+------+----------+---------+------------+-------------+
| ucs305 | ONLINE | 1 | 111.8 GB | Claimed | Solidstate | System |
| ucs305 | ONLINE | 2 | 894.3 GB | Claimed | Solidstate | Caching |
| ucs305 | ONLINE | 3 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 4 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 5 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 6 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 7 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE |8|0B| Unknown | | |
| ucs306 | ONLINE | 1 | 111.8 GB | Claimed | Solidstate | System |
| ucs306 | ONLINE | 2 | 894.3 GB | Claimed | Solidstate | Caching |
| ucs306 | ONLINE | 3 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 4 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 5 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 6 | 1.1 TB | Claimed | Rotational | Persistence |
```

```
| ucs306 | ONLINE | 7 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE |8|0B| Unknown | | |
| ucs307 | ONLINE | 1 | 111.8 GB | Claimed | Solidstate | System |
| ucs307 | ONLINE | 2 | 894.3 GB | Claimed | Solidstate | Caching |
| ucs307 | ONLINE | 3 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 4 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 5 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 6 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 7 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE |8|0B| Unknown | | |
| ucs309 | ONLINE | 1 | 111.8 GB | Claimed | Solidstate | System |
| ucs309 | ONLINE | 2 | 894.3 GB | Claimed | Solidstate | Caching |
| ucs309 | ONLINE | 3 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs309 | ONLINE | 4 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs309 | ONLINE | 5 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs309 | ONLINE | 6 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs309 | ONLINE | 7 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs309 | ONLINE |8|0B| Unknown | | |
+-----------+------------------+------+----------+---------+------------+-------------+
```

たとえば、ucs-308 を削除すると、そのディスクは表示されなくなります。

ステップ 4 VCenter の **[ホストおよびクラスタ（Hosts and Cluster）]** ビューからホストを削除します。

a) vSphere Web クライアント ナビゲータにログインします。vSphere インベントリの **[ホスト（Host）]** に移動します。

b) ホストを右クリックして、**[すべての vCenter アクション（All vCenter Actions）]** > **[インベントリから削除（Remove from Inventory）]** を選択しオンます。[はい（Yes）] をクリックします。

ステップ 5 すべてのノード関連データストアが削除されていることを確認します。たとえば、ESXiで次のコマンドを実行します。

```
[root@ucs308:~] esxcfg-nas -l
ds4 is 169.254.226.1:ds4 from 6894152532647392862-8789011882433394379 mounted available
ds3 is 169.254.226.1:ds3 from 6894152532647392862-8789011882433394379 mounted available
ds2 is 169.254.226.1:ds2 from 6894152532647392862-8789011882433394379 mounted available
ds5 is 169.254.226.1:ds5 from 6894152532647392862-8789011882433394379 mounted available
ds1 is 169.254.226.1:ds1 from 6894152532647392862-8789011882433394379 mounted available
```

（注） ノード関連データストアが表示されている場合は、それらのデータストアを手動でマウント解除して削除します。

オフライン ストレージ クラスタからのノードの削除

導入環境をクリーンアップするか、またはストレージ クラスタからノードを削除するには、`stcli node remove` を使用します。

（注） ストレージ クラスタ内のコンバージド ノードを取り外す場合は、TAC と一緒に作業することを強くお勧めします。

クラスタ内のノードの数	クラスタ内の障害が発生したノードの数	方法	注記
3	1	ノードを削除して交換するには、TACにご連絡ください。	-
4	1	オフラインでのノードの取り外し。 （注） 「ストレージクラスタマネージャが構成されていません（*storage cluster manager is not configured*）」というエラーが hxconnect で表示されるか、stcli cluster storage-summary | grep -i Heali -A 8 コマンドの一部として表示される場合は、TACにお問い合わせください。	4 ノード クラスタで 2 つのノードがダウンしている場合は、TAC の支援が必要です。
5 つ以上	1	クラスタをオフラインにする必要があります。	オンライン モードが推奨されます。
5 つ以上	2	クラスタをオンラインにすることができます。	5 ノード クラスタで 3 つのノードがダウンしている場合は、TAC の支援が必要です。

（注） このタスクの手順を実行する前に、コントローラ VM またはその他の HX Data Platform コンポーネントを削除しないでください。

手順

ステップ 1 ノードの削除を準備するプロセスに従います。詳細については、ノードの削除の準備 （161 ページ） を参照してください。

ステップ 2 (4 ノード クラスタのみ) シャットダウンの準備をしてから、ストレージ クラスタをシャットダウンします。

a) すべての HX データストアのすべての常駐 VM を正常にシャットダウンします。

任意で、VM を vMotion で移動します。

b) HX ストレージ クラスタ ノードの非 HX データソースですべての VM を正常にシャットダウンし、マウント解除します。

c) コントローラ VM コマンド ラインから `stcli cluster shutdown` コマンドを実行します。

```
# stcli cluster shutdown
```

ステップ 3 **stcli cluster info** コマンドを実行し、`stNodes: section` を探して、削除する必要があるノードを見つけます。この情報は、ノードをメンテナンスモードにした場合にも使用できます。

Example:

```
    ----------------------------------------
    type: node
    id: 569c03dc-9af3-c646-8ac5-34b1f7e04b5c
    name: example1
    ----------------------------------------
    type: node
    id: 0e0701a2-2452-8242-b6d4-bce8d29f8f17
    name: example2
    ----------------------------------------
    type: node
    id: a2b43640-cf94-b042-a091-341358fdd3f4
    name: example3
----------------------------------------
    type: node
    id: d2d43691-daf5-50c4-d096-941358fede374
    name: example5
```

ステップ 4 `stcli node remove` コマンドを使用して該当するノードを取り外します。

次に例を示します。

1 つのノードを削除するには

- **stcli node remove: ip-1 example5** または
- **stcli node remove –id-1 d2d43691-daf5-50c4-d096-941358fede374**

Response:

```
    Successfully removed node: EntityRef(type=3, id='', name='10.10.2.4')
```

このコマンドは、すべてのデータストアをマウント解除し、クラスタ アンサンブルから削除し、このノードの EAM をリセットし、すべてのサービス（ストア、クラスタ管理 IP）を停止し、すべてのファイアウォール ルールを削除します。

このコマンドは、vCenter からノードを削除しません。ノードは vCenter に残ります。このコマンドはまた、インストールされている HX Data Platform 要素（コントローラ VM など）を削除しません。

ストレージ クラスタ内にノードがないため、HXDP メンテナンス モードを終了する必要はありません。

（注） 削除したノードを別のストレージ クラスタ内で再利用するには、テクニカル アシスタンス センター（TAC）にご連絡ください。ノードを別のストレージクラスタで利用できるように準備するには、追加手順が必要です。

ステップ 5 クラスタを再起動します。

```
# hxcli cluster start
```

ステップ 6 クラスタが起動したら、ノードがストレージ クラスタクラスタから削除されていることを確認してください。

a) ストレージ クラスタ情報を確認します。

```
# stcli cluster storage-summary
```

b) 応答の `ActiveNodes` エントリを調べ、クラスタのノード数が 1 つ少なくなっていることを確認します。

c) 削除されたノードが Ensemble の一部ではないことを確認します。

```
Example:
admin:~$ cat /etc/springpath/stMgr.cfg
{"0":"10.104.18.37:2181","1":"10.104.18.38:2181","2":"10.104.18.39", "3":"10.104.18.40:2181",
 "4":"10.104.18.41:2181"}
```

たとえば、10.104.18.40 を削除した場合は表示されなくなります。

d) ノード数が 5 以下のクラスタでノード削除アクションが成功した場合、アンサンブルには 4 つの参加者ノードと 1 つのオブザーバ ノードが含まれている可能性があります。参加者ノードのみが stMgr.cfg で更新されます。オブザーバ ノードの詳細は更新されません。

例：

ノード削除後のアンサンブル server.0=10.107.16.111:2888:3888:participant;10.107.16.111:2181

server.1=10.107.16.107:2888:3888:participant;10.107.16.107:2181

server.2=10.107.16.108:2888:3888:participant;10.107.16.108:2181

server.4=10.107.16.110:2888:3888:participant;10.107.16.110:2181

server.5=10.107.16.109:2888:3888:observer;10.107.16.109:2181

version=10000558b

ステップ 7 `hxcli disk list` コマンドを実行して、削除されたノードのディスクが表示されなくなったことを確認します。

```
admin:~$ hxcli disk list --no-loader
+-----------+------------------+------+----------+---------+------------+-------------+
| NODE NAME | HYPERVSIOR STATUS | SLOT | CAPACITY | STATUS | TYPE | USAGE |
+-----------+------------------+------+----------+---------+------------+-------------+
| ucs305 | ONLINE | 1 | 111.8 GB | Claimed | Solidstate | System |
| ucs305 | ONLINE | 2 | 894.3 GB | Claimed | Solidstate | Caching |
| ucs305 | ONLINE | 3 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 4 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 5 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 6 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 7 | 1.1 TB | Ignored | Rotational | Persistence |
| ucs305 | ONLINE | 8 | 0 B | Unknown | | |
| ucs306 | ONLINE | 1 | 111.8 GB | Claimed | Solidstate | System |
| ucs306 | ONLINE | 2 | 894.3 GB | Claimed | Solidstate | Caching |
| ucs306 | ONLINE | 3 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 4 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 5 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 6 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 7 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs306 | ONLINE | 8 | 0 B | Unknown | | |
```

```
| ucs307 | ONLINE | 1 | 111.8 GB | Claimed | Solidstate | System |
| ucs307 | ONLINE | 2 | 894.3 GB | Claimed | Solidstate | Caching |
| ucs307 | ONLINE | 3 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 4 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 5 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 6 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 7 | 1.1 TB | Claimed | Rotational | Persistence |
| ucs307 | ONLINE | 8 | 0 B | Unknown | | |
+----------+------------------+------+----------+---------+------------+-------------+
```

たとえば、ucs-308 を削除すると、そのディスクは表示されなくなります。

ステップ 8 VCenter の **[ホストおよびクラスタ（Hosts and Cluster）]** ビューからホストを削除します。

a) vSphere Web クライアント ナビゲータにログインします。vSphere インベントリの **[ホスト（Host）]** に移動します。

b) ホストを右クリックして、**[すべての vCenter アクション（All vCenter Actions）] > [インベントリから削除（Remove from Inventory）]** を選択しオンます。[はい（Yes）] をクリックします。

ステップ 9 すべてのノード関連データストアが削除されていることを確認します。たとえば、ESXiで次のコマンドを実行します。

```
[root@ucs308:~] esxcfg-nas -l
ds4 is 169.254.226.1:ds4 from 6894152532647392862-8789011882433394379 mounted available
ds3 is 169.254.226.1:ds3 from 6894152532647392862-8789011882433394379 mounted available
ds2 is 169.254.226.1:ds2 from 6894152532647392862-8789011882433394379 mounted available
ds5 is 169.254.226.1:ds5 from 6894152532647392862-8789011882433394379 mounted available
ds1 is 169.254.226.1:ds1 from 6894152532647392862-8789011882433394379 mounted available
```

（注） ノード関連データストアが表示されている場合は、それらのデータストアを手動でマウント解除して削除します。

コンピューティング ノードの削除

手順

ステップ 1 削除する必要があるコンピューティング ノードからすべての VM を移行します。

ステップ 2 コンピューティング ノードからのデータストアをマウント解除します。

ステップ 3 次のコマンドを実行して、クラスタが健全な状態であることを確認します。

```
stcli cluster info --summary
```

ステップ 4 ESXi ホストを HXDP メンテナンス モードにします。

ステップ 5 CIMP (クラスタ IP アドレスのように Cisco HX Connect IP アドレスを使用) から `stcli node remove` コマンドを使用して、コンピューティング ノードを削除します。

```
stcli node remove --id-1
```

Or

```
stcli node remove --ip-1
```

IP は、削除されるノードの IP アドレスです。

ステップ 6 DVS が存在する場合、vCenter の EXSi ホストから DVS を削除します。

ステップ 7 vCenter から ESXi ホストを削除します。

ステップ 8 次のコマンドを実行して、クラスタが健全な状態であることを確認します。

```
stcli cluster info --summary
```

ステップ 9 `stcli cluster info` の情報出力に計算ノードの virtnode エントリーがまだ存在する場合は、次を実行します。

SCVM で `priv service stMgr restart` を使用して、stMgr 管理サービスを再起動します。

ステップ 10 Cisco HX Connect をログアウトし、Cisco HX Connect にログインして、コンピューティング ノードの古いエントリを消去します。

ステップ 11 高可用性 (HA) および分散リソース スケジューラ (DRS) サービスを無効にしてから再度有効にして、ノードを削除した後にサービスを再設定します。

同じクラスタ内で以前に削除されたノードを再利用する

以前に削除した同じクラスタ内のノードを再利用するには、次の手順を実行します。

始める前に

- 同じクラスタで再利用するには、HXDP 4.5(2b) 以降を実行しているクラスタでノードを削除する必要があります。
- HX ノードは、クラスタがオンラインのときに削除しなければなりません。クラスタがオフラインのときにノードを削除した場合、そのノードは同じクラスタ内で再利用できなくなる可能性があります。
- HX ノードの削除は、管理ガイドに記載されている stcli node コマンドを使用して実行する必要があります。ノードがクラスタから適切に削除されなかった場合、同じクラスタ内で再利用できなくなる可能性があります。
- 4 ノードクラスタの場合には、オフライン ストレージ クラスタからのノードの削除（166 ページ） のみ使用します。ノードの再利用は、4 ノードクラスタではサポートされていません。

手順

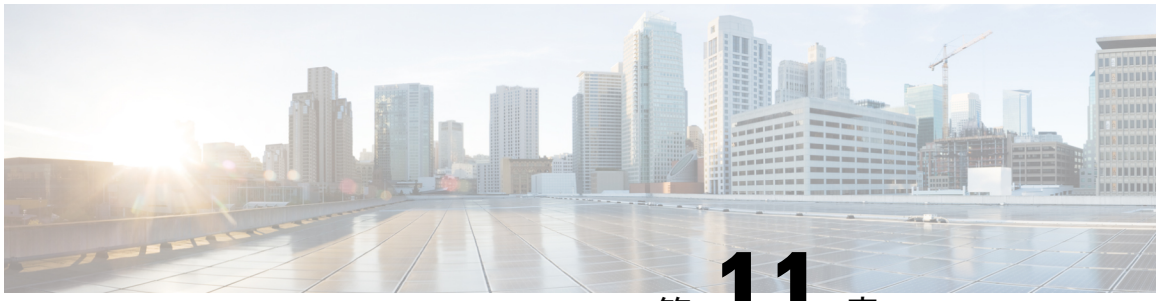
ステップ 1 vCenter Cluster インベントリから ESXi ホストを削除します。

ステップ 2 HX クラスタの残りの部分とマッチする、同一のバージョンの ESXi を再インストールします。

ステップ 3 この削除されたノードに以前に関連付けられていた UCS Manager から UCS サービス プロファイルのみを削除します。

ステップ 4 同じバージョンの HX インストーラを使用して、拡張ワークフローを実行します。

（注） 拡張ワークフロー中は、必ず **[ディスク パーティションをクリア（Clear Disk Partitions）]** ボックスをオンにしてください。



第 11 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 （195 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、M5/M6 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 SAN ブート、フロント アクセス対応 SSD/HDD、または単一の 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。

  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、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 5.0(1b) 以降では、Intersight を介して 2 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。

  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
- HX リリース 5.0(2b) 以降、375G WL キャッシュ ドライブを備えた新しいノードを、1.6TB キャッシュ ドライブ搭載のノードを備えた既存のクラスタに追加することはできません。
- 同じディスク内のサーバ間で操作ディスクを移動する、または同じアクティブ クラスタ内で拡張ノードに移動することはサポートされていません。

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/M6 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/M6 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。

M5/M6 クラスタを拡張する場合の前提条件

M5/M6 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。

混合クラスタ展開のガイドライン - Cisco HX リリース 5.5(x) 以降

一般的なガイドライン

- HX240c M6は、M5 ノードを持つクラスタで組み合わせた場合、追加のスロットを使用できません。
- すべてのサーバーは、クラスタのフォーム ファクタ（220/240）、タイプ（Hybrid/AF/NVME）、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。

混合クラスタ拡張オプション：サポート

- M6 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す。

- M5 または M6 コンバージド ノードを持つ既存の混合 M5/M6 クラスタの展開がサポートされています。
- 混合クラスタの作成では、拡張ワークフローのみがサポートされています（混合 M5/M6 サーバでの最初のクラスター作成はサポートされていません）。
- 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 5.0 またはそれ以降のインストーラを使用した M5、混合 M5/M6 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。

混合クラスタ拡張オプション：サポートされていません

- M5 コンバージド ノードを使用して既存の M6 クラスタを拡張する操作はサポートされません。
- Intel と AMD M6 の混在はサポートされていません。
- HX Edge は、混在 M5、M6 クラスタをサポートしません。
- 混在 M5/M6 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。

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 ノードの追加に関する前提条件

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（Hybrid、All FlashまたはNVME）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

手順

ステップ 1 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。

ステップ 2 HX ノードが工場出荷時に準備されたノードであることを確認します。

（注） 取り外したコンバージドノードやディスクは、元のクラスタで再利用しないでください。

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。

手順

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	

フィールド	説明
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。
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。
[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。	
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 クライアントでホストをvCenterクラスタに追加します。
- HX でデータ プラットフォーム 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 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。
- 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。

- 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、M5/M6 世代サーバ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（**Priority**）	**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）

コンピューティング専用ノードの準備

手順

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

手順

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専用ノードへの 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。

手順

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する必要があります。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。

Cisco HyperFlex Data Platform でサポートされているリリースの ESXi 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。

手順

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-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10-install-only.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 サーバーに対してステップ 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。

手順

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。

クラスタ拡張を実行するために、必要な設定データとともに *JSON* 構成ファイルをインポートすることもできます。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）

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. インポートした Cisco UCS Manager の値が異なる場合は、**[インポートされた値の上書き（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。

フィールド	説明
[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 **（M6 サーバーのみ）[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。それらを選択せずに、**[関連付けなし（Unassociated）]** タブでは、クラスタに追加するサーバーを選択します。

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。

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 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 マネージャの次の手順を完了します。

1. HX Data Platform 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。

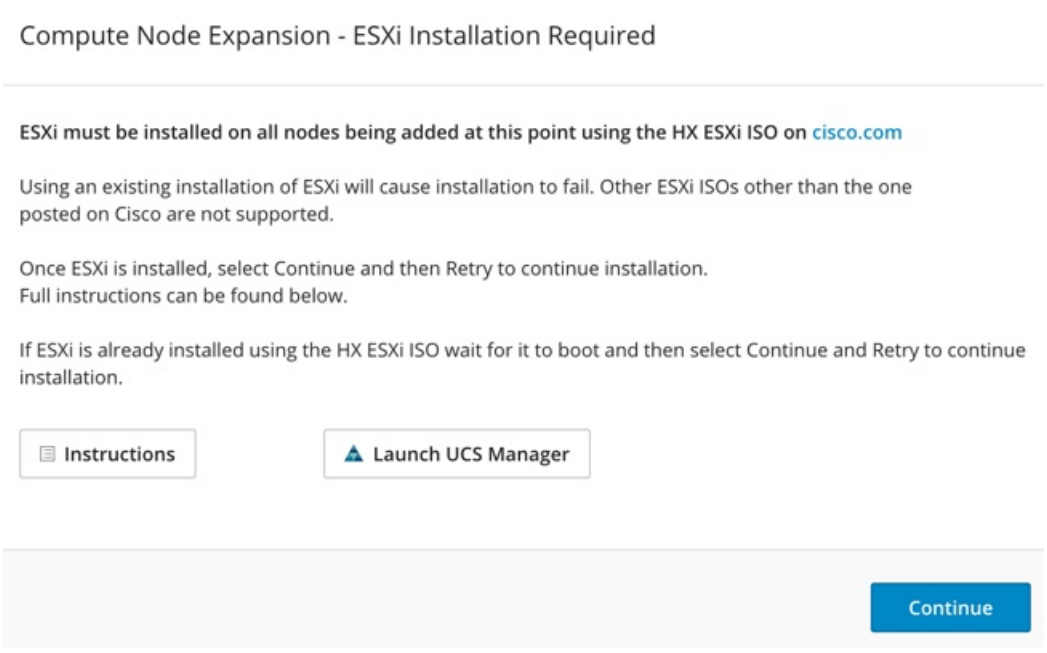
3. 作業中のペインで、**[ストレージ（Storage）]** タブをクリックします。**[ローカル ディスクの設定ポリシー（Local Disk Configuration Policy）]** サブ タブをクリックします。

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）」。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) vSphere Web クライアントでホストをvCenterクラスタに追加します。
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。

手順

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 ノードのクラスタでは、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
```

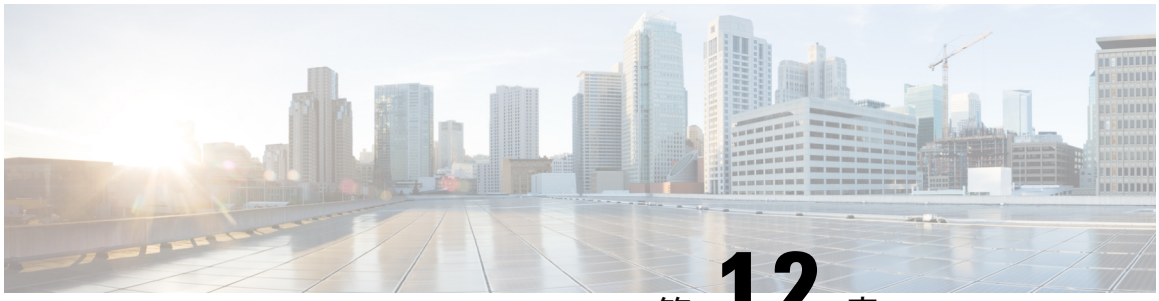
LAZ 関連コマンド

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 12 章

HX コントローラ VM の管理

ストレージ コントローラ VM の管理

ストレージコントローラ VM は、分散型 Cisco HX Data Platform に不可欠な機能を提供します。ストレージ クラスタ内のすべてのコンバージド ノードにストレージ コントローラ VM がインストールされます。ストレージ コントローラ VM には、ストレージ クラスタに対して `hxcli` コマンドを実行するためのコマンドライン インターフェイスがあります。

ストレージ コントローラ VM の電源のオン/オフ

vSphere Web クライアントまたは ESX コマンド ラインを介して VM の電源をオンまたはオフにすることができます。これはストレージ コントローラ VM にも適用されますが、通常はストレージ コントローラ操作によってストレージ コントローラ VM の電源のオンまたはオフが処理されます。

手順

ステップ 1 **vSphere Web クライアントを使用した** VM の電源のオンまたはオフ。

a) vSphere Web クライアントにログインします。

b) VM を特定します。

ナビゲータで **[Global Inventory Lists]** > **[Virtual Machines]** > ***[vm]*** を選択します。

ストレージ コントローラ VM の名前には、`stCtlVM` というプレフィックスが付きます。

c) 右クリックするか、または[アクション（Actions）]メニューから、**[電源（Power）]**>**[電源オン（Power On）]**または**[電源（Power）]**>**[ゲスト OS のシャットダウン（Shut Down Guest OS）]** を選択します。

ステップ 2 **ESX コマンド ラインを使用した** VM の電源のオンまたはオフ。

a) VM の ESX ホストのコマンド ラインにログインします。

b) VM `vmid` を特定します。

これは、ESX ホストに固有です。コマンドを実行します。

```
# vim-cmd vmsvc/getallvms
```

サンプル応答

```
Vmid   Name    File   Guest OS   Version   Annotation
1   stCtlVM-<vm_number>   [SpringpathDS-<vm_number>]  stCtlVM-<vm_number>/
stCtlVM-<vm_number>.vmx  ubuntu64Guest   vmx-11
3   Cisco HyperFlex Installer  [test]  Cisco HyperFlex Installer/Cisco
HyperFlex Installer.vmx   ubuntu64Guest   vmx-09
Retrieved runtime info
Powered off
```

ストレージ コントローラ VM の名前には、`stCtlVM` というプレフィックスが付きます。

c) VM の電源を入れます。VM の電源をオンにするように指定するコマンドを実行します。

```
# vim-cmd vmsvc/power.on 1
```

d) VM の電源を切ります。VM の電源をオフにするように指定するコマンドを実行します。

```
# vim-cmd vmsvc/power.shutdown 1
```

これらのオプションは、グレースフル シャットダウンと望ましくないハード シャットダウンの放棄アクションを実行します。

HX コントローラ VM での HA VM モニタリングの無効化

HX クラスタで All Paths Down (APD) 状態を開けるためには、vSphere Web クライアントを使用して、すべての HX コントローラ VM の HA VM モニタリングを無効にします。

手順

ステップ 1 vSphere Web クライアントにログインします。

ステップ 2 変更する HX クラスタを選択します。

ステップ 3 メニューから **[Configure (設定)]** > **[VM Overrides (VM オーバーライド)]** を選択します。

ステップ 4 [Add] をクリックします。

[Add VM Override Sandbox (VM オーバーライド サンドボックスの追加)] ウィンドウが、vCenter の VM リストとともに表示されます。

ステップ 5 w ウィンドウで利用可能なすべての HX Controller VMs を選択します。

（注） HX Controller VM の名前は、`stCtlVM-` から始まります。

ステップ 6 [Next] をクリックします。

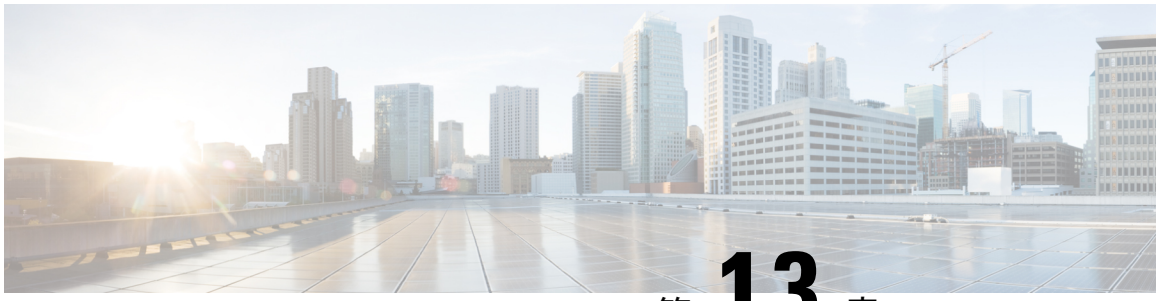
[Add VM Override (VM オーバーライドの追加)] ダイアログ ボックスが表示されます。

ステップ 7 **[vSphere HA - VM Monitoring]** おぷoption and select the following:

- **[Override (オーバーライド)]** チェックボックス
- ドロップダウン リストから **[Disabled (無効化)]** を選択します。

ステップ 8 **[Finish (終了)]** をクリックして、設定の変更を適用します。

HA VM Monitoring は、すべての HX controller VM で無効になります。



第 13 章

Ready Clone の管理

HX Data Platform Ready Clone の概要

HX Data Platform Ready Clones は、業界初のストレージ技術で、ホスト VM から複数のクローン VM をすぐに作成およびカスタムできます。スタンドアロン VM として使用可能な VM の複数のコピーを作成することができます。

Ready Clone（標準のクローンと同様に、既存の VM のコピーです）。既存の VM は、ホスト VM と呼ばれます。クローニング操作が完了すると、Ready Clone は別のゲスト VM となります。

Ready Clone に対して変更を行っても、ホスト VM には影響しません。Ready Clone の MAC アドレスおよび UUID は、ホスト VM の MAC アドレスおよび UUID とは異なります。

ゲスト オペレーティング システムとアプリケーションのインストールには、時間がかかることがあります。Ready Clone を実行すると、単一のインストールおよび設定プロセスで、多数の VM のコピーを作成できます。

クローンは、多数の同一の VM を 1 つのグループに配置する場合に役立ちます。

HX Data Platform Ready Clone の利点

HX Data Platform Ready Clone には次の利点があります。

- **同時に複数の VM クローンを作成**：VM を右クリックするだけで、Ready Clone 機能を使用して複数の VM のクローンを作成します。
- **高速クローニング**：HX Data Platform ReadyClone は、VMware vSphere® Storage APIs - Array Integration（VAAI）データ オフロードをサポートしており、VM の電源でサポートされているため、従来のクローニング操作よりも非常に高速です。VAAI はハードウェア アクセラレーションまたはハードウェア オフロード API とも呼ばれ、VMware vSphere ESXi ホストとストレージデバイス間の通信を可能にする API のセットです。HX Data Platform Ready Clone を使用して、分単位ではなく秒単位で VM のクローンを作成してください。
- **ゲスト VM のバッチ カスタマイズ**：HX Data Platform カスタマイズ仕様を使用すると、ホスト VM から複製される複数のゲスト VM 用の IP アドレス、ホスト名、VM 名などのパラメータを瞬時に構成できます。
- **複数の手順をワンクリック プロセスへと自動化**：HX Data Platform Ready Clone 機能が、各ゲスト VM 作成のタスクを自動化します。
- **VDI 導入サポート**：Ready Clone は、VMware ネイティブ テクノロジーを使用している VDI 導入のデスクトップ VM でサポートされます。
- **データストア アクセス**：クローン対象の VM がアクセス可能なマウントポイントにある限り、Ready Clone は部分マウント/アクセス可能なデータストアに対して機能します。

サポートされているベース VM

HX Data Platform では次のものがサポートされています。

- HX Data Platform データストアに保存されているベース VM
- HX Data Platform スナップショットを使用しているベース VM Powered-on VM の場合、Ready Clone ワークフローは HX スナップショットを取得し、そのスナップショットを使用してクローンを作成します。HX スナップショットが削除されると、同じワークフローが発生します。

（注） sentinel ベースの HX スナップショットの場合、sentinel スナップショットは Ready Clone の後に自動的に削除されません。sentinel ベースの HX スナップショットを使用することの意味については、HX ネイティブ スナップショットの概要 （19 ページ） を参照してください。

- Storage vMotion は、HX ネイティブ スナップショットのある VM ではサポートされていません。
- 1 つのベース VM から最大 2048 個の Ready Clone
- 一度に 1 つのバッチで作成された最大 256 の Ready Clone

HX Data Platform では次のものはサポートされません。

- 30 個を超えるスナップショットを使用した電源オン状態のベース VM
- redo ログ スナップショットを使用した電源オン状態のベース VM

Ready Clone の要件

- HX Data Platform ストレージ クラスタ内の VM である必要があります。HX Data Platform 以外の VM はサポートされていません。
- HX Data Platform データストア、VM フォルダ、およびリソース プール上に VM が存在している必要があります。

  HX Data Platform データストアに存在しない VM では、ReadyClone は失敗します。これは、VM レベル、VM フォルダ レベル、またはリソース プール レベルの Ready Clone にあてはまります。
- VM で持つことができるネイティブ スナップショットは 1 つだけです。Ready Clone は、redo ログを持つスナップショット（非ネイティブ スナップショット）を使用する VM からは作成できません。
- Ready Clone には単一の vNIC カスタマイズ テンプレートだけを使用してください。
- Cisco HX リリース 3.0 以降では、ストレージ クラスタ内のすべてのノードの ESX で SSH を有効にする必要はありません。
- HX Connect Ready Clones 操作が実行されていない場合、VM の移行がサポートされます。VM を別のデータストアに移動する必要がある場合は、最初にスナップショットを削除してください。

Ready Clone のベストプラクティス

- カスタマイズ仕様をプロファイルまたはテンプレートとして使用します。
- バッチ全体に適用されるプロパティがカスタマイズ仕様に含まれていることを確認してください。
- HX Data Platform Ready Clone の一括クローニングのワークフローで、ユーザ定義のパラメータを取得します。

- パターンを使用して、クローンごとに区別するための設定（VM のゲスト名など）を抽出します。
- ネットワーク管理者がゲスト名に静的IPアドレスを割り当てていることを確認し、クローンを作成する前にそれらのアドレスを確認します。
- 特定の時点で、1 ～ 256 個からなるバッチを作成できます。HX Data Platform プラグインでこれを確認することができます。
- （電源オンまたは電源オフ時に）同じ VM 上で複数のクローン バッチを同時に作成しないでください。そのようにすると、HX Data Platform プラグインのマスター タスク更新情報の誤表示や障害の原因となります。

HX 接続を使用して Ready clone を作成する

HX データ プラットフォーム Ready clone 機能を使用して、それぞれ異なる静的 IP アドレスを持つ、VM の複数のクローンを作成することにより、クラスタを設定します。

（注） VM の OVA 展開が進行中のときに VM を複製するために **[Ready Clone]** をクリックした場合は、エラー メッセージが表示されます。VM の展開が成功した後にのみ VM を複製できます。

手順

ステップ 1 管理者として HX 接続 にログインします。

ステップ 2 **[Virtual Machines (仮想マシン)]** ページから、***[virtual machine (仮想マシン)]*** を選択し、**[Ready Clones]** をクリックします。

ステップ 3 **[Ready Clone]** ダイアログのフィールドに入力します。

UI 要素	基本的な情報
Number of clones	作成する Ready Clones の数を入力します。特定の時刻に 1 ～ 256 個のクローンのバッチを作成できます。
Customization Specification	オプション フィールド。 ドロップダウンリストをクリックして、リストからクローン向けの [カスタマイズ仕様（Customization Specification）] を選択します（このリストには vCenter で使用可能なカスタマイズ仕様が含まれます）。 システムは、選択したホスト仮想マシンに関するカスタマイズ仕様をフィルタリングします。たとえば、選択したホスト仮想マシンでゲスト仮想マシン向けに Windows OS を使用している場合、ドロップダウンリストには Windows OS のカスタマイズ仕様が表示されます。

UI 要素	基本的な情報
Resource Pool	オプション フィールド。 HX ストレージ クラスタ ですでにリソース プールを定義している場合、選択された仮想マシンの Readyclone のうち保存するものを 1 つ選択できます。
VM 名プレフィックス	ゲスト仮想マシン名にプレフィックスを入力します。 このプレフィックスは、作成された各 Ready Clone の名前に追加されます。 （注） Ready Clone に名前を付けるために使用される VM 名のプレフィックスには、文字、数字、およびハイフン (-) のみを含める必要があります。名前は文字で始まる必要があり、数字またはハイフンのみを含めることはできません。
Starting clone number	クローンを開始するクローン番号を入力します。 各 Ready Clone は一意の名前を持ち、番号付けは名前の一意の要素を確認するために使用されます。
クローン番号の増分	ゲスト仮想マシンの名前の中で増えていく必要のあるクローンの番号を入力します。もしくは、デフォルト値の 1 のままにします。システムが、仮想マシン Ready Clones の名前に番号を追加します（clone1、clone2、clone3 など）。デフォルトでは、番号は 1 から始まります。この値は、任意の数値に変更できます。
ゲスト名に同じ名前を使用	このチェックボックスをオンにすると、vCenter VM のインベントリ名がゲスト ホスト仮想マシン名として使用されます。 このボックスをオフにすると、テキストボックスが使用可能になります。ゲストのホスト仮想マシン名として使用する名前を入力します。
Preview	必須フィールドを入力したら、 HX データ プラットフォーム により提案された Ready Clone の名前がリストされます。必須のフィールドの内容を変更すると、[**クローン名**] と [**ゲスト名**] フィールドが更新されます。
Power on VMs after cloning	クローニング プロセスの完了後、ゲスト仮想マシンをオンにするには、このチェックボックスをオンにします。

ステップ 4 [複製（Clone）] をクリックします。

HX データ プラットフォーム により、名前が付けられロケーションが指定された状態で Ready clone 番号を作成します。

HX データプラットフォームプラグインを使用した Ready Clone の作成

VMware のクローニング操作を使用した場合、VM から作成できるクローンは 1 つのみです。この操作は手動で、VM からの複数クローンをバッチ処理で作成する場合よりも時間がかかります。たとえば、VM のクローンを 20 個作成する場合、手動で何度もクローン操作を実行する必要があります。

（注） HX Data Platform Ready Clone を使用して、ワンクリックで VM のクローンを複数作成します。

たとえば、Windows VM から、異なる静的 IP アドレスを有したクローンを 10 個別々に作成できます。

手順

ステップ 1 vSphere Web クライアント ナビゲータから、**[Global Inventory Lists]** > **[Virtual Machines]** の順に選択します。vCenter 内の VM の一覧が表示されます。

ステップ 2 複製する VM を選択し、**[Actions (アクション)]** メニューを開きます。[VM information (VM 情報)] ポートレット内で、VM を右クリックするか **[Actions (アクション)]** メニューをクリックします。

必要に応じて、クラスタと関連 VM のリストを表示し、VM がストレージ クラスタ VM であることを確認します。

ステップ 3 **[Cisco HX Data Platform]** > **[Ready Clones]** の順に選択して、[Ready Clones] ダイアログ ボックスを表示します。

ステップ 4 [Ready Clones] ダイアログ ボックスに次の情報を指定します。

制御	説明
クローン数	作成するクローンの数を入力します。特定の時刻に 1 ～ 256 個のクローンのバッチを作成できます。
カスタマイズ仕様	ドロップダウンリストをクリックして、リストからクローン向けの [カスタマイズ仕様（Customization Specification）] を選択します（このリストには vCenter で使用可能なカスタマイズ仕様が含まれます）。 システムは、選択したホスト VM のカスタマイズ仕様をフィルタリングします。たとえば、選択したホスト VM がゲスト VM 向けに Windows OS を使用する場合、ドロップダウンリストには Windows OS のカスタマイズ仕様が表示されます。
VM 名のプレフィクス	ゲスト VM 名のプレフィックスを入力します。

制御	説明
	（注） Ready Clone に名前を付けるために使用される VM 名のプレフィックスには、文字、数字、およびハイフン (-) のみを含める必要があります。名前は文字で始まる必要があり、数字またはハイフンのみを含めることはできません。
最初のクローン数	開始クローンのクローン番号を入力します。
ゲスト名に同じ名前を使用	このチェックボックスをオンにすると、vCenter VM のインベントリ名がゲストのホスト VM 名として使用されます。このボックスをオフにすると、テキスト ボックスが表示されます。ゲストのホスト VM 名に使用する名前を入力します。 システムには、ダイアログボックス内の [ゲスト名（Guest Name）] 列にある、ゲスト VM の名前が表示されます。 [カスタマイズ仕様（Customization Specification）] 自体にも、同様のオプションがあります。この HX Data Platform Ready Clone のバッチのカスタマイゼーション プロセスでは、[Customization Specification] オプションで指定したオプションがオーバーライドされます。 • [カスタマイズ仕様（Customization Specification）] に静的ゲートウェイ、静的サブネット、または静的 IP アドレスに解決されるゲスト名を使用する NIC もしくはネットワーク アダプタが含まれる場合、システムはゲスト名に関連付けられた静的 IP アドレスをネットワーク アダプタに割り当てます。また、指定されたゲスト名にストレージ クラスタ名またはホスト名を設定します。 • [カスタマイズ仕様（Customization Specification）] に、DHCP を使用して IP アドレスを取得する NIC もしくはネットワーク アダプタが含まれる場合、システムはストレージ クラスタ名またはホスト名のみを指定されたゲスト名に設定します。
クローン番号を次の単位で増分	ゲスト VM 名に含まれるクローン番号の増分値を入力します。または、デフォルト値の 1 のままにします。システムによって、VM クローンの名前に番号が追加されます（clone1、clone2、clone3 など）。デフォルトでは、番号は 1 から始まります。この値は、任意の数値に変更できます。
クローニング後にVMの電源をオン	クローニング プロセスの完了後、ゲスト VM をオンにするには、このチェックボックスをオンにします。

ステップ 5 設定変更を適用するには、**[OK]** をクリックします。

[vSphere Web Client Recent Tasks] タブでは、Ready Clone のタスクのステータスに関するメッセージが表示されます。システムにより、次の内容が表示されます。

- イニシエータが vCenter ユーザとしてログインしている状態でのトップ レベルの進捗状況。
- イニシエータが vCenter ユーザとしてログインしている状態での導入ワークフローと HX Data Platform の拡張機能。

- ReadyClone ワークフローの一部として一時的なスナップショットが vCenter と HX Connect に表示されます。これは、Ready Clone の作成中のみ、余分な電源オフの VM として一時的に表示されます。

HX Data Platform Ready Clone のカスタマイズの準備

- VMware のドキュメントに従ってカスタマイズ仕様を作成します。

  以降のトピックで説明する Linux VM または Windows VM に固有のカスタマイズ設定を適用してください。

- 管理者から IP アドレスを取得します。たとえば、10.64.1.0 から 10.64.1.9 までの 10 個の IP アドレスを取得します。
- これらの IP アドレスのサブネットマスクなど、ネットワークに固有の情報を収集します。
- ベース VM が有効であること（切断されておらず、スナップショットや vMotion も実行中でないこと）を確認します。
- ゲスト ツールがベース VM にインストールされていることを確認します。必要に応じて更新します。
- [VM サマリー（VM Summary）] タブに移動し、ゲスト ツールが動作していることを確認します。

vSphere Web クライアントでの Linux 用カスタマイズ仕様の作成

[vSphere Web クライアント ゲストのカスタマイズ（vSphere Web Client Guest Customization）] ウィザードを使用すると、ゲスト オペレーティング システムの設定を仕様に保存し、仮想マシンのクローン作成時またはテンプレートからの展開時にそれを適用できるようになります。

次の点を考慮しながら、ウィザードを完了します。

- HX Data Platform Ready Clone の機能を使用して、カスタマイズ仕様の作成時に指定したゲスト名を上書きできます。
- HX Data Platform Ready Clone により、VM 名またはゲスト名におけるパターンの使用を有効にできます。
- HX Data Platform がサポートする NIC は 1 台のみです。
- カスタマイズされた Linux VM の NIC の編集

  - HX Data Platform Ready Clone のカスタマイズ プロセスでは、このアドレスが上書きされるため、仮の IP アドレスを使用できます。

  - HX Data Platform Ready Clone では、VM のゲスト名が静的 IP アドレスに解決され、クローニングされた VM 用に設定されます。

作成されたカスタマイズ仕様は、[カスタマイズ仕様マネージャ（Customization Specification Manager）] 内にリストされます。これを使用して、仮想マシンのゲスト オペレーティング システムをカスタマイズすることができます。

vSphere Web クライアントでの Windows 用カスタマイズ仕様の作成

[vSphere Web クライアント ゲストのカスタマイズ（vSphere Web Client Guest Customization）] ウィザードを使用すると、Windows ゲスト オペレーティング システムの設定を仕様に保存し、仮想マシンのクローン作成時またはテンプレートからの展開時にそれを適用できるようになります。

（注） カスタマイズ後、Windows Server 2008 用のデフォルト管理者パスワードは保存されません。カスタマイズの実行中、Windows Sysprep ユーティリティが Windows Server 2008 の管理者アカウントを削除して再作成します。カスタマイズ後、仮想マシンの初回起動時に管理者パスワードを再設定する必要があります。

次の考慮事項を確認し、ウィザードを完了させます。

- オペレーティング システムは、ネットワーク上で自身を認識するためにこの名前を使用します。Linux システムでは、これはホスト名と呼ばれます。
- HX Data Platform がサポートする NIC は 1 台のみです。
- カスタマイズされた Windows VM の NIC の編集

  HX Data Platform Ready Clone のカスタマイズ プロセスでは、IP アドレスが上書きされるため、仮の IP アドレスを使用できます。

作成されたカスタマイズ仕様は、[カスタマイズ仕様マネージャ（Customization Specification Manager）] 内にリストされます。これを使用して、仮想マシンのゲスト オペレーティング システムをカスタマイズすることができます。

カスタマイズ仕様を使用した Ready Clone の設定

スタティック IP アドレスを使用する場合、新しい VM に IP アドレスが正しく適用されるようにするには、カスタマイズ仕様を使用します。

たとえば Windows サーバの VM クローンを作成する場合、DHCP を使用すると、ゲスト VM には新しい IP アドレスが自動的に割り当てられます。しかし、スタティック IP アドレスを使用する場合は、ゲスト VM 内で IP アドレスが自動的に複製されません。これを解決するには、カスタマイズ仕様を使用して、HX Data Platform Ready Clone を設定します。

手順

ステップ 1 有効な DNS 名を取得し、有効な IP アドレスにそれらが解決されることを確認します。

たとえば、ゲスト名 userwinvm1 ～ userwinvm100 を使って 100 個の Windows VM をプロビジョニングするには、userwinvm1 から userwinvm100 までが有効な IP アドレスであることを確認します。

ステップ 2 ソース（クローン元）VM に、ゲスト VM ツールをインストールします。

ステップ 3 Ready Clone 機能を使用して、クローン元 VM をクローンします。クローンされたゲスト VM は、ソース VM のアイデンティティを取得します。

ステップ 4 カスタマイズ仕様を使用して、クローンされたすべての VM のアイデンティティを変更します。IP アドレス、ホスト名、VM 名などのパラメータを設定できます。

仮想マシン ネットワークの管理

ストレージクラスタに変更を行った後、クラスタ内のノードで仮想マシンのネットワーキングが正しく設定されていることを確認できます。仮想マシン ネットワークの詳細な情報については、UCS Manager のマニュアルを参照してください。

手順

ステップ 1 VLAN が正しく設定されていることを確認します。

Cisco UCS Manager ネットワーク管理ガイドhttps://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/4-1/b_UCSM_Network_Mgmt_Guide_4_1/b_UCSM_Network_Mgmt_Guide_4_1_chapter_0110.htmlの VLAN の章を参照してください。

ステップ 2 vNIC が正しく設定されていることを確認します。

『*Cisco UCS Manager Network Management Guide*』の vNIC テンプレートのトピックを参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/4-1/b_UCSM_Network_Mgmt_Guide_4_1/b_UCSM_Network_Mgmt_Guide_4_1_chapter_0110.html

ステップ 3 仮想ポート グループが正しく設定されていることを確認します。

vmware サイトで *VMware vSphere 7.0* ドキュメントの「仮想マシン ポート グループの追加」に関するトピックを参照してください。

第 14 章

HX ネイティブ スナップショットの管理

HX ネイティブ スナップショットの概要

HX ネイティブ スナップショットは、VM のバージョン（状態）を保存するバックアップ機能です。VM は、HX ネイティブ スナップショットを使用して、以前に保存したバージョンに戻すことができます。ネイティブ スナップショットはVMの複製で、ネイティブ スナップショットが作成された時点での、すべての VM ディスク上のデータの状態と VM の電源の状態（オン、オフ、またはサスペンド）が含まれます。保存した状態へ復元できるようにするには、ネイティブ スナップショットを取得して VM の現在の状態を保存します。

HX ネイティブ スナップショットの管理では、次の方法が使用されます。

- HTML 5 の vSphere クライアント プラグインでの HX ネイティブ スナップショットのサポートは、プラグイン バージョン 2.0.0 で導入されました。詳細については、今すぐスナップショットを作成 （420 ページ） を参照してください。
- HTML 5 の vSphere クライアント プラグインのスケジュール スナップショットのサポートは、プラグイン バージョン 2.1.0 で導入されました。詳細については、スナップショットのスケジュール （423 ページ）を参照してください。

- vSphere の「スナップショットの管理」機能は、特定の HX ネイティブ スナップショットに戻すことも、すべてのスナップショットを削除することもできます。
- Cisco HyperFlex Connect は、オンデマンドを作成し、HX ネイティブ スナップショットをスケジュールできます。
- HyperFlex コマンドライン ユーザー インターフェイスでは、HX ネイティブ スナップショットを作成できます。
- HX REST API は、HX ネイティブ スナップショットを作成および削除できます。
- Cisco HXDP リリース 5.5(x) 以降の重要な変更：
  - ESXi バージョン 6.5、6.7、および 7.0 U1 はサポートされていません。
  - Sentinel スナップショット作成ワークフローの代わりに、VMware VAAI スナップショット ワークフローが使用されます。

VMware スナップショットの詳細については、VMware Customer Connect サイトの「Overview of virtual machine snapshots in vSphere（KB 1015180）」を参照してください。

HX ネイティブ スナップショットの利益

HX Native スナップは次の利点を提供します。

- **登録済み VM の復元 ー** VM が登録されている場合、電源のオン/オフに関係なく、HX ネイティブ スナップショットと VM スナップショットは、スナップショットが作成された時点よりも前の状態を復元できます。
- **高性能** - HX ネイティブ スナップショットのプロセスは、I/O オーバーヘッドが発生しないため高速です。
- **VM のパフォーマンス** - HX ネイティブ スナップショットは、VM のパフォーマンスを低下させません。
- **クラッシュ整合** - HX ネイティブ スナップショットは、デフォルトでクラッシュ整合です。I/O のクラッシュ整合性においては、アプリケーションがクラッシュから正常に再起動できるように、書き込み操作の正しい順序を維持するように定義されています。
- **静止** - ゲスト ファイル システムを静止した状態で HX Native スナップショットを作成できます。静止オプションは、Cisco HyperFlex Connect、HyperFlex コマンドライン ユーザー インターフェイス、および HX REST API を使用する場合に使用できます。静止オプションを使用して HX ネイティブ スナップショットを作成する場合は、ゲスト VM に VMware ツールをインストールする必要があります。

  HyperFlex リリース 4.5（2a）および VMware ESXi 7.0 U2 以降の静止スナップショットのパフォーマンスと信頼性が向上しました。

  「ファイル システムの休止」とは、物理または仮想コンピュータのディスク上のデータをバックアップに適した状態にするプロセスを指します。このプロセスには、オペレーティ

ング システムのメモリ内キャッシュからディスクにダーティ バッファをフラッシュするなどの操作の他、アプリケーションに固有の高位レベルのタスクが含まれる場合があります。

休止ベースのスナップショットは、Windows2008R2 オペレーティング システムではサポートされていません。オペレーティング システムのサポート終了です。サポートされているオペレーティング システムの最新のリストについては、VMware のドキュメントを参照してください。VMware 互換性ガイド

システムに休止エラーが表示された場合は、VMware Customer Connect『*Troubleshooting Volume Shadow Copy（VSS）quiesce related issues (1007696)*』の記載を参照してください。

- **スケジュールされたスナップショットはノード障害に耐性があります** - スケジュールされたスナップショットは、HXDP メンテナンス モードや HX オンライン アップグレードなど、ノードのシャットダウンを必要とする管理操作に耐性があります。

  スケジュール済みスナップショットは、マルチ-クラスタ環境では他の HX クラスタで発生する障害に対して耐障害性があります。

- **詳細な進捗とエラー レポート**: これらのモニタリング タスクは、 VM レベルの HX Native スナップショットのタスク レベルで実行されます。。

- **瞬時のスナップショットの削除** - HX ネイティブ スナップショットと統合の削除は常に瞬時に行われます。

- **VDI 導入サポート。**スケジュール済み HX ネイティブ スナップショットは、VMware ネイティブ テクノロジーを使用する VDI 導入環境のデスクトップ VM でサポートされています。

- **データストア アクセス。**スナップショット対象の VM がアクセス可能なマウントポイントにある限り、スナップショットは部分マウントまたはアクセス可能なデータストアに対して機能します。

HX ネイティブ スナップショットの考慮事項

スナップショット パラメータ

注目 HX リリース 4.5（2a）以降では、VMware ESXi 7.0 U2 Sentinel スナップショットは適用されません。

- **HX ネイティブ スナップショット**ー最初の HX ネイティブ スナップショットを作成すると、HX ネイティブ スナップショットの前に HX SENTINEL スナップショットが作成されます。SENTINEL スナップショットは、後続のスナップショットが HX ネイティブ スナップショットであることを保証するベースライン スナップショットです。SENTINEL スナッ

プショットが存在する場合、vSphere を使用して追加のスナップショットを作成すると、HX ネイティブ スナップショットが作成されます。

（注） ネイティブスナップショットの作成時に、VMware スナップショット（非ネイティブ）が存在しないようにする必要があります。

- **HX スナップショットと VMware VAIO の互換性**-VMware VAIO が設定された HX スナップショットの作成はサポートされていません。HX スナップショットを作成しようとすると、VM の電源がオフになります。HX スナップショットは、vSphere API for IO Filtering（VAIO）が有効になっている仮想マシンと共存できません。VAIO フレームワークをバックアップ ソリューションで使用して、仮想マシンの継続的データ保護（CDP）を有効にすることができます。CDP でバックアップ ソリューションを使用するには、CDP 機能を有効にする前に既存の HX スナップショットを削除します。

  製品で VMware VAIO フレームワークが使用されているかどうかを確認するには、『VMware Compatibility Guide』で VMware サイトの認定ベンダーのリストを確認します。

- **保存スナップショットの最大数**：VMware における VM ごとのスナップショットの上限は、31 です。制限の合計は、すべての VMware 作成済みスナップショット、HX SENTINEL スナップショット、および HX ネイティブ スナップショットの合計に等しくなります。

  仮想マシンの `snapshot.maxSnapshots` プロパティで設定されている数字以上のスナップショットをユーザーが作成しようとすると、次のエラーメッセージでスナップショット操作が失敗します：スナップショット操作を実行できません。

- **スケジュール済みスナップショット**：VM とそのリソースプールで、スナップショットが重複してスケジュールされないようにしてください。

Performance

- **VMware vSphere ストレージ API アレイ統合（VAAI）**：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 以降にアップグレードします。

アップグレード プロセス中のスナップショット

- HX ネイティブ スナップショットは、HX、ESXi、または UCS のアップグレードが進行中の場合はサポートされていません。

VM

表 *7:* リリース固有の *VM* に関する考慮事項

リリース	検討
VMware ESXi 7.0 U2 以降を使用する HX リリース 4.5（2a）以降	統合時間は、仮想マシンの I/O 負荷に比例しなくなりました。 Sentinel スナップショットは作成されなくなりました。

次の注意事項は、すべてのさぽーとあれているリリースに適用されます。

- **VM ハードウェア バージョン**: HX Native スナップショットには、VM ハードウェア バージョン 9 以降が必要です。最新バージョンを使用することを推奨します。
- **削除された VM**：HX ネイティブ スナップショットのライフサイクルは、VM スナップショットと同様であり、仮想マシンに関連付けられています。VM が故意にまたは誤って削除されると、関連するすべての HX ネイティブ スナップショットも削除されます。HX ネイティブ スナップショットには、削除された VM から回復するメカニズムはありません。VM の削除から保護するには、バックアップ ソリューションを使用します。
- **HX Data Platform ストレージ コントローラ VM**: ストレージ コントローラ VM の HX Native スナップショットはスケジュールできません。
- **HX Data Platform に属していない VM（Non-HX Data Platform VMs）**：HX データストアに存在しない VM では、HX Native スナップショットは機能不全になります。HX データストアにまたがる VM の HX ネイティブ スナップショットには、VMware ESXi バージョン 7.0 U2 以降を備えた HXDP バージョン 4.5(2a) 以降が必要です。
- **中断状態の VM**: 最初の HX Native スナップショットおよび VM の HX SENTINEL スナップショットを中断状態から作成することはサポートされていません。
- **VM 名**： VM 名は、HX Native スナップショットの撮影に対して、vCenter ごとに固有である必要があります。
- **準備ができているストレージ クラスタ**: HX Native スナップショットを許可するには、ストレージクラスタが、十分なスペースがあり、オンラインである必要があります。VM が存在するデータストアにアクセスできる必要があります。VM が有効であり、移行状態（vMotion 実行中など）であってはなりません。

オンライン ノードが 1 つだけ残っているクラスタ

- HX Native スナップショットは、電源オン状態の CBT 対応 VM の単一オンライン ノードでは許可されません。VM の電源をオフにし、SENTINEL スナップショットを取得します。電源がオンになっている VM の後続のスナップショットがサポートされます。

vCenter

- **vMotion**：vMotion は、HX ネイティブ スナップショットのある VM でサポートされています。
- **Storage vMotion**：Storage vMotion は、HX ネイティブ スナップショットのある VM ではサポートされていません。VM を別のデータストアに移動する必要がある場合は、Storage vMotion を実行する前にスナップショットを削除してください。

名称

- **名前の重複**：HX Data Platform vCenter で、VM やリソース プールの名前の重複はサポートされておらず、HX ネイティブ スナップショットが失敗します。これには、ネストされたリソース プール内の親および子、別の vCenter クラスタ内のリソース プールが対象となります。
- **名前の文字**：特殊文字はサポートされていません。名前に特殊文字を使用すると、指定した名前とは異なる名前が表示されます。
- **スナップショット名の最大長** – 80 文字。

ディスクとデータストア

- **シック ディスク**ーソース ディスクがシック ディスクの場合、VM のディスクのスナップショットもシックになります。必要に応じて、スナップショットに対応するためデータストア サイズを大きくしてください。

（注） HyperFlex データストアで新しい仮想マシンディスクを作成し、シックプロビジョニングされたディスクの作成を有効にする場合、シックプロビジョニングされたディスクを作成するオプションはありません。これは、VMware の既知の問題です。詳細については、「Creating VMDK with NFS-backed storage does not allowthick-provisioning with vendor plugin」を参照してください。

（注） ESXi は、NFS データストア上のシックプロビジョニングの遅延ゼロ仮想ディスクとシックプロビジョニングの仮想ゼロディスクを区別できません。NFS データストアを使用する場合、vSphere クライアントでは、Thick Provision Lazy Zeroed（zeroedthick）または Thick Provision Eager Zeroed（eagerzeroedthick）形式の仮想ディスクを作成できます。ただし、[仮想マシンのプロパティ（Virtual Machine Properties）]ダイアログボックスでディスクタイプをオンにすると、[ディスクプロビジョニング（Disk Provisioning）]セクションに、ディスクフォーマットとして[シックプロビジョニング（Eager Zeroed）]が常に表示されます（ディスク作成時にどのフォーマットを選択しても）。

- **仮想ディスク タイプ**：VMware は、さまざまな仮想ディスク バッキング タイプをサポートします。最も一般的なタイプは FlatVer2 形式です。HX ネイティブ スナップショットはこの形式でサポートされています。

  その他の仮想ディスク形式には、Raw Device Mapping（RDM）、SeSparse、VmfsSparse（Redlog 形式）などがあります。これらの形式の仮想ディスクを含む VM は、HX ネイティブ スナップショットではサポートされていません。

ログイン アクセス

- **SSH**：SSH がストレージ クラスタ内のすべてのノード上の ESX で有効になっていることを確認してください。

制限

オブジェクト	最大数
HX ネイティブ スナップショット	VM あたり 30 VMware の上限は 31 です。1 つのスナップショットが HX SENTINEL スナップショットで使用されます。
データ ストア	ストレージ クラスタあたり 48
最大 VMDK サイズ	3 TB

HX ネイティブ スナップショットのベスト プラクティス

- 多数のスナップショットを作成する際には、次の点を考慮します。
  - データ トラフィックの低いことが予想される場合は、HX ネイティブ スナップショットを同時にスケジュールします。

- 多数の VM が同時にスナップショットされるようにスケジュールされないように、HX ネイティブ スナップショット スケジュールをずらします。

- ストレージ クラスタ内の VM で vCenter が稼働している場合は、vCenter VM の HX Native スナップショットを作成しないでください。詳細については、VMware サイトの『*VMware VirtualCenter Server service fails due to a quiesced snapshot operation on the vCenter Server database virtual machine (2003674)*』記事を参照してください。

HX ネイティブ スナップショットのベスト プラクティス HX リリース 4.5（1x）以前

HX リリース 4.5（2a）および ESXi 7.0 U2 で重要な更新が導入されました。次の推奨事項は、このリリースの前に導入されたリリースを使用しているユーザにのみ適用されます。

重要 **VM の最初のスナップショットを作成するためには、常に HX ネイティブ スナップショット機能を使用してください。これで、後続のスナップショットがすべてネイティブ形式になります。**

- VM の最初のスナップショットを作成するためには、VMware のスナップショット機能を使用しないでください。VMware スナップショットは redo ログ技術を使用するので、それが原因で元の VM でパフォーマンスが低下します。しかも、スナップショットが追加されるごとにパフォーマンスがさらに低下します。
  - 削除するべき redo ログ スナップショットがある場合は、redo ログ スナップショットが常駐する ESXi ホストで、`/etc/vmware/config` ファイルを編集して、`snapshot.asyncConsolidate="TRUE"` を設定します。

- HX ネイティブ スナップショットは、最初の HX ネイティブ スナップショットが作成された後の VM のパフォーマンスには影響しません。

- 最初の HX ネイティブ スナップショットを作成する前に、VM にすべての VMDK を追加します。

  VMDK が VM に追加されると、追加の SENTINEL スナップショットが取得されます。それぞれの追加の HX SENTINEL は、追加スペースを使用します。

  たとえば、HX Native スナップショットを持つ既存の VM に 2 つの新しい VMDK を追加すると、次にスケジュールされた HX Native スナップショットで 1 つの新しい HX SENTINEL が作成されます。1 つ以上の VMDK を追加する必要がある場合は、既存の HX Native スナップショット スケジュールの保持計画を確認し、保持されている HX Native スナップショットと HX SENTINEL スナップショットの合計数が合計値 31 を超えないようにしてください。

HX ネイティブ スナップショットのタイムゾーン

スナップショットのタイムスタンプとスケジュールを表示したり操作したりするオブジェクトは、次の 3 つです。

- vSphere と vCenter は UTC 時間を使用します。
- vSphere クライアント (HTML5) はブラウザのタイムゾーンを使用します。
- HX vSphere クライアント（HTML5）プラグイン、HX ストレージ クラスタ、HX ストレージ コントローラ VM は同じタイムゾーンを使用します。これは HX ストレージ クラスタ全体に適用されます。これらのエンティティで使用されるタイムゾーンは設定可能です。デフォルトは UTC です。

スケジュールの設定には HX ストレージ コントローラ VM の時刻が使用されます。HX ネイティブ スナップショットの作成には vSphere UTC 時刻が使用されます。ログとタイムスタンプは、その表示方法に応じて異なります。

HX vSphere クライアント（HTML5）を使用してスケジュールを作成すると、スケジュールされた時間は HX ストレージ コントローラ VM のタイムゾーンから UTC に変換されます。vSphere クライアント（HTML5） タスクでスケジュールを表示すると、ブラウザのタイムゾーンでタスクが表示されます。

これらを同じタイムゾーンに変換すると、同一時刻になります。たとえば、5:30pm PST、8:30PM EST、1:30AM UTC はすべて同じ時刻です。

[vSphere のスケジュールされたタスク] タブの場合、HX vSphere クライアント（HTML5）プラグイン内で作成したスケジュール済みのスナップショットと同じ時間を表示し、ストレージコントローラ VM を UTC に設定します。

ローカルのタイムゾーン設定に基づいて、スナップショットをスケジュールに沿って実行するには、ストレージ クラスタ用のタイムゾーンを設定します。デフォルトでは、ストレージ コントローラ VM は HX Data Platform のインストール中に設定された UTC のタイムゾーンを使用します。

vSphere とストレージ コントローラ VM が同じタイムゾーンを使用していない場合、[vSphere Scheduled tasks] タブでは [HX vSphere クライアント（HTML5）プラグイン] スケジュール スナップショット s ダイアログでスケジュールした時間とは異なる時間が表示される場合があります。

時間単位のスナップショットを設定すると、スナップショット スケジュールは特定の開始時間と終了時間の間で実行されます。[vSphere Task (vSphere タスク)] ウィンドウでは、タイムゾーンに基づき、スケジュールされたスナップショットが時間単位で指定された終了時刻の後で完了したというステータスを表示することがあります。

ストレージ コントローラ VM で使用されるタイムゾーンの識別と設定

1. ストレージコントローラ VM のコマンドラインから、タイムゾーンの設定を参照します。

```
$ hxcli services timezone show
```

2. ストレージ クラスタのタイムゾーンを変更します。

```
$ hxcli services timezone set --timezone timezone_code
```

関連トピック

スナップショットのスケジュール （423 ページ）

HX ネイティブ スナップショットの作成

HX ネイティブ スナップショットを作成するには、次の手順を実行します。

始める前に

HX ストレージ クラスタ内の VM の redolog スナップショットを削除します。この手順が完了していない場合は、VM がスナップショット統合中に機能しなくなる可能性があります。

Redo ログ スナップショットは、HX Native のスナップショット機能ではなく、VMware のスナップショット機能を介して作成されるスナップショットです。REDO ログ スナップショットが存在する ESXi ホスト設定を編集するには、

1. ESXi ホストのコマンド ラインにログインします
2. 編集するために `/etc/vmware/config` を探して開きます。
3. `snapshot.asyncConsolidate` パラメータを `TRUE` に設定します。

```
snapshot.asyncConsolidate="TRUE"
```

手順

ステップ 1 vSphere クライアント（HTML5）ナビゲータから、VM レベルで vCenter の VM のリストを表示します。**ホストとクラスタ**、**VM とテンプレート**、**ストレージ**、**ネットワーキング**、または**グローバル インベントリ リスト**のいずれかの方法で VM リストを表示します。

例：

グローバル インベントリ リスト > **VM**

ステップ 2 ストレージクラスタ VM を選択し、**[操作（Actions）]** メニューを開きます。[VM 情報（VM information）] ポートレット内で、VM を右クリックするか [操作（Actions）] メニューをクリックします。

（注） ストレージ クラスタのリソース プール上に HX Data Platform に属していないデータストアがないことを確認します。そうでない場合、スナップショットは失敗します。

ステップ 3 **[Cisco HX Data Platform]** > **[今すぐスナップショット（Snapshot Now）]** の順に選択して、[スナップショット（Snapshot）] ダイアログボックスを表示します。

ステップ 4 ダイアログボックスに入力します

表 *8 : [Take Snapshot]*ダイアログボックス

フィールド	説明と使用上の注意
名前	スナップショット名を入力します。スナップショット名の最大長は80文字です。
説明	スナップショットの説明を入力します。
[スナップショット オプション] チェックボックス	チェックボックスを使用して、**[仮想マシンのメモリのスナップショット（Snapshot the virtual machine's memory）]**または**[ゲスト ファイル システムの静止（Quiesce guest file system）]**を選択します（VMware Tools がインストールされている必要があります）。

ステップ 5 **[OK]** をクリックして、HX ネイティブ スナップショットを作成します。

[最近のタスク（Recent Tasks）] タブでは、次のステータス メッセージが表示されます。

```
Create virtual machine native snapshot.
 The first snapshot
```

関連トピック

今すぐスナップショットを作成 （420 ページ）

ESXi 7.0 U2 を使用した HX ネイティブ スナップショット

ESXi 7.0 U2 を使用してスナップショットを作成すると、次の機能が強化されます。

- Sentinel スナップショットは作成されません。
- VM 属性 `snapshot.alwaysAllowNative=TRUE.`を自動的に設定することで、VM のすべてのスナップショットの VAAI オフロードをサポートします。
- パフォーマンス、信頼性、および機能の向上。
- スパンされたデータストア上の VM のスナップショットをサポートします。
- 不要になった場合に自動的に識別し、sentinels を削除します。

HX Native スナップショットのスケジューリングの概要

スナップショットスケジュールをストレージクラスタオブジェクト（VM、VM リソースプールなど）に適用します。

（注） vCenterクラスタを再登録すると、HXNativeのスナップショット スケジュールは失われます。この場合は、HX Native スナップショット スケジュールを再設定します。

HX Native スナップショットをスケジュールする場合は、バックアップ要件を考慮してください。重要なデータについては、より頻繁な HX Native スナップショットを保持します。障害発生時には、直近の HX Native スナップショットを復元するか、カスタムのリアルタイム HX Native スナップショットを作成できます。重要度の低いデータの場合は、HX Native スナップショットの作成頻度を少なくすることを検討します。

HXNative スナップショット スケジューリングは、バックアップ コストの制御に役立ちます。ストレージ クラスタの各 VM で、時間単位、日単位、または週単位でスナップショットをスケジュールできます。個別の VM の最大頻度は、1 時間に 1 度です。時間単位の設定は 15 分の増分値で利用できます。

たとえば、HX Native スナップショットは、次の設定で毎日、取得されます。

VM 1 の時間単位のスナップショット、午後 10 時と午前 1 時の間の 15 分に実行。
VM 2 の時間単位のスナップショット、午後 8 時と午前 12 時の間の 30 分に実行。
VM 3 と 4 の時間単位のスナップショット、午前 6 時と午前 8 時の間の 45 分に実行。
VM 5 の日単位のスナップショット、午前 6 時に実行

これらのHXNative スナップショットは毎日、取得されます。最後のHXNative スナップショットが終了時:00 分より前になっていることに注意してください。

午前 6 時 — VM 5
午前 6 時 45 分 — VM 3、VM 4
午前 7 時 45 分 — VM 3、VM 4
午後 8 時 30 分 — VM2
午後 9 時 30 分 — VM2
午後 10 時 15 分 — VM1
午後 10 時 30 分 — VM2
午後 11 時 15 分 — VM1
午後 11 時 30 分 — VM2
午前 12 時 15 分 — VM1

24 時間で 1 時間ごとに HX Native スナップショットをスケジュールするには:

手順

ステップ 1 開始時刻を設定します

ステップ 2 開始時刻の 1 時間前に終了時刻を設定します。

例：

時間が 15 分の設定で、午後 4 時を開始にして午後 3 時を終了にします。

このタスクは、HX Native スナップショットを午後 4 時 15 分、午後 5 時 15 分 ... 午前 12 時 15 分、午前 1 時 15 分 ... 午後 2 時 15 分、午後 3 時 15 分に取得します。その後、24 時間のサイクルが再開されます。

（注） VM ごとの最大 HX Native スナップショット数は 31 です。1 つの HX SENTINEL スナップショットも必要です。したがって、1時間ごとにHX Nativeスナップショットを取得し、最新の 30 の HX Native スナップショットを保持することができます。

HX Native スケジュール スナップショットには、ストレージ コントローラ VM の現在のタイム ゾーン設定に基づく、スナップショットの設定時間が表示されます。そのため、HX Native スナップショットを午後 7 時 PST に設定し、ストレージ コントローラ VM のタイム ゾーンを EST に変更した場合、次に HX Native スケジューラのウィンドウを開くときには、設定時間は午後 10 時 EST に自動で更新されています。

関連トピック

スナップショットのスケジュール （423 ページ）

HX Native スナップショットのスケジューリング

重要 HXネイティブスナップショットをスケジュールするこの方法は、HXリリース4.0（x）以前でのみサポートされています。

始める前に

HXDP 4.5（x）以降を使用してHXネイティブスナップショットをスケジュールするには、最新のHTML5プラグインをインストールします。詳細については、VMware vCenter の Cisco HyperFlex HTML プラグイン （367 ページ）およびスナップショットのスケジュール （423 ページ）を参照してください。

手順

ステップ 1 vSphere クライアント（HTML5）のホームページから、VM またはリソース プール リストを選択します。

たとえば、**[vCenter インベントリ リスト（vCenter Inventory Lists）] > [仮想マシン（Virtual Machines）]** の順に選択し、vCenter 内での VM のリストを表示します。

ステップ 2 ストレージクラスタ VM またはリソースプールを選択し、**[アクション（Actions）]** メニューを開きます。

オブジェクトを右クリックするか、または [操作（Actions）] メニューをクリックします。

ステップ 3 [操作（Actions）] メニューから **[Cisco HX Data Platform] > [スケジュール スナップショット（Schedule Snapshot）]** の順に選択し、[スケジュール スナップショット（Schedule Snapshot）] ダイアログ ボックスを表示します。

ステップ 4 スナップショットの頻度を選択します。

時間単位、日単位、週単位の頻度を示すボックスをクリックし、開始日、開始時刻、および期間を設定します。

ステップ 5 保持するスナップショットの数を設定します。

最大数に達すると、新しいスナップショットの作成に伴って古いスナップショットが削除されます。

ステップ 6 必要に応じて、既存のスケジュール済み項目を選択解除します

以前のスケジュールが存在している場合は、項目を選択解除すると、今後のスケジュールからこれらの項目が削除されます。

ステップ 7 **[OK]** をクリックしてスケジュールを受け入れ、ダイアログを閉じます。

HX Native スケジュール済みスナップショットの頻度の設定

スナップショットを、毎時間（特定の時刻）、毎日（特定の時刻）または毎週（選択した曜日と時刻）作成します。

始める前に

VM またはリソース プールの [スナップショットのスケジューリング（Schedule Snapshot）] ダイアログボックスを開きます。

手順

ステップ 1 [スケジュール スナップショット（Schedule Snapshot）] ダイアログボックスで、[時間単位のスナップショットを有効にする（Enable Hourly Snapshot）]、[日単位のスナップショットを有効にする（Enable Daily Snapshot）]、または [週単位のスナップショットを有効にする（Enable Weekly Snapshot）] のチェックボックスをオンにします。

ステップ 2 ドロップダウン リストの **[開始（Start）]** をクリックし、開始時間を選択します。時間、15 分単位の分、午前または午後を選択します。

ステップ 3 スナップショット スケジュールを時間単位で設定するには、[終了日時（Until）] ドロップダウン リストをクリックして、終了時間を選択します。時間、15分単位の分、午前または午後を選択します。[開始（Start）] で選択した開始時間と同じ値に分を設定します。

HX Data Platform プラグインは、開始時間と終了時間の間で毎時間ごとに VM のスナップショットを作成します。

ステップ 4 対応するチェックボックスをオンにして、スナップショットを取得する曜日（[日（Days）]）を指定します。

ステップ 5 [保持（Retention）] で、数値を入力するか矢印ボタンを使用して、スケジュールごとに保持するコピーの最大数を指定します。

関連トピック

スナップショットのスケジュール （423 ページ）

HX Native スナップショット スケジュールの削除

手順

ステップ 1 HX vSphere クライアント (HTML5)、から、VM またはリソース プール リストを選択します。

たとえば、**[vCenter インベントリ リスト（vCenter Inventory Lists）]** > **[仮想マシン（Virtual Machines）]** の順に選択し、vCenter 内での VM のリストを表示します。

ステップ 2 ストレージクラスタ VM またはリソースプールを選択し、**[アクション（Actions）]** メニューを開きます。

オブジェクトを右クリックするか、または [操作（Actions）] メニューをクリックします。

ステップ 3 [アクション（Actions）] メニューから **[Cisco HX データ プラットフォーム（Cisco HX Data Platform）]** > **[スケジュール スナップショット（Schedule Snapshot）]** を選択し、[スケジュール HX Native スナップショット（Schedule HX Native Snapshot）] ダイアログ ボックスを表示します。

ステップ 4 不要になったスケジュール済みオプションをオフにします。

ステップ 5 **[OK]** をクリックして変更を受け入れ（変更には、以前に設定されていたスケジュールの削除が含まれます）、ダイアログを終了します。

ステップ 6 スケジュールが削除されたことを確認します。

ストレージ クラスタ VM またはリソース プールを選択します。HX vCenter のタブ、**[管理（Manage）]** > **[スケジュール済みタスク（Scheduled Tasks）]** をクリックします。これで、以前の HX Native スナップショット スケジュールが表示されなくなります。

HX ネイティブ スナップショットへの復帰

スナップショットに復帰すると、VM がスナップショットに保存されている状態に戻ります。スナップショットへの復帰は、一度に 1 つの VM で実行します。スナップショットへの復帰は、HX Data Platform プラグインではなく vCenter Snapshot Manager で実行されます。

始める前に

VM のスナップショットが存在している必要があります。

手順

ステップ 1 vSphere クライアント （HTML5） から、VM レベル、VM フォルダ レベル、またはリソース プール レベルを選択します。たとえば、**[vCenter インベントリ リスト（vCenter Inventory Lists）] > [仮想マシン（Virtual Machines）]** の順に選択し、vCenter 内の VM のリストを表示します。

ステップ 2 ストレージ クラスタ VM を選択し、**[操作（Actions）]** メニューを開きます。[VM 情報（VM information）] ポートレット内で、VM を右クリックするか [操作（Actions）] メニューをクリックします。

ステップ 3 **[スナップショット（Snapshots）] > [スナップショットの管理（Manage Snapshots）]** を選択し、vSphere Snapshot Manager を開きます。

ステップ 4 選択した VM のスナップショット階層から、復元するスナップショットを選択します。

ステップ 5 **[復帰（Revert to）] > [はい（Yes）] > [閉じる（Close）** の順にクリックします。

復帰された VM は VM リストに追加され、電源がオフになります。場合によっては、VM スナップショットから復帰した VM がすでに電源オンになっていることがあります。詳細については、次の表を参照してください。

表 *9 : HX VM* スナップショットの再起動後の *VM* 電源状態

HX VM スナップショット撮影後の VM 状態	**復元後の VM 状態**
電源がオンになっています（メモリが含まれます）。	HX VM スナップショットに戻した後、VM がオンになり実行中になります。
電源がオンになっています（メモリを含みません）。	HX VM スナップショットに戻した後、VM がオフになります。
電源がオフになっています（メモリを含みません）。	HX VM スナップショットに戻した後、VM がオンになり実行中になります。

ステップ 6 戻された VM がオフになる場合、VM を選択して、電源をオンにします。

HX Native スナップショットの削除

HX Native スナップショットの削除は、HX vSphere プラグインではなく vSphere インターフェイスで管理されます。

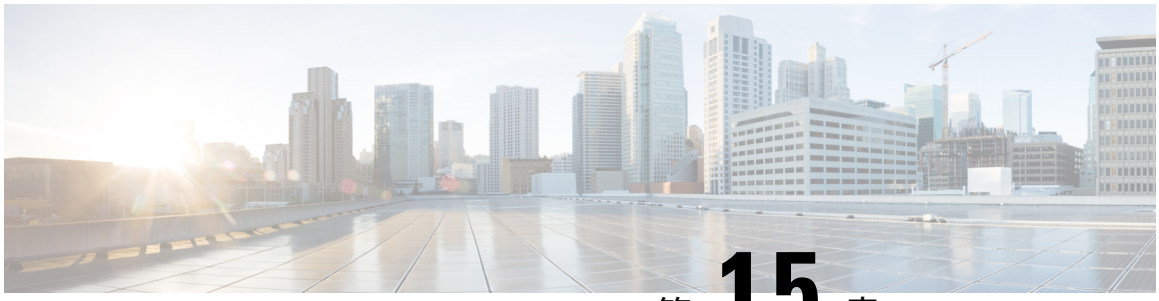
手順

ステップ 1 vSphere クライアント (HTML5) から、**[VM とテンプレート（VMs and Templates）]** > **[*vcenter_server*]** > **[スナップショット（Snapshots）]** > **[データセンター（*datacenter*）]** > **[*vm*]** の順序で選択します。

ステップ 2 ***[vm]*** を右クリックして、**[Snapshots]** > **[Manage Snapshots]** を選択します。

ステップ 3 HX Native スナップショットを選択し、**[削除（Delete）]** をクリックします。

（注） **[すべて削除（Delete All）]** オプションのみを使用して、HX SENTINEL スナップショットを削除します。HX SENTINEL スナップショットは個別に削除しないでください。



第 15 章

仮想マシンのディザスタ リカバリの管理

HX ディザスタ リカバリの概要

HyperFlex DR は、ネットワーク接続のクラスタのペアの間で実行中の VM のレプリケーションを設定することによって、災害からの仮想マシンの保護を有効にすることができます。VM のレプリケーションでは、一方のクラスで稼働中の保護対象の仮想マシンが、ペアとなっているもう一方のクラスタに複製されます。ペアにする 2 つのクラスタは通常、互いに離れたところに位置し、一方のクラスタが他方のクラスタで実行中の仮想マシンのディザスタ リカバリ サイトとして機能します。

保護が VM で設定されると、HX Data Platform はローカル クラスタで実行中の VM のデータ保護（DP）スナップショットを定期的に作成し、スナップショットをペアのリモート クラスタにレプリケート（コピー）します。ローカル クラスタで障害が発生すると、保護された各 VM の最も最近レプリケートされたスナップショットがリモート クラスタでが回復されることができます。他のクラスタのディザスタ リカバリ サイトとして機能する各クラスタは、障害の発生時に、通常のワークロードだけでなく新しく回復した VM を実行できるように、十分な予備リソースを含むサイズにする必要があります。

（注） 最後に複製された DP スナップショットのみが宛先クラスタに保持されます。追加の DP スナップショットの保持はサポートされていません。

レプリケーション間隔（スケジュール）を含む保護属性を割り当てることによって、各 VM を個別に保護できます。レプリケーション間隔を短くすると、レプリケートされたスナップショット データはより新しいものになる可能性があります。DP スナップショットの間隔は、5 分ごとから 24 時間ごとまでの範囲で設定できます。

保護グループとは、共通のDPスナップショット スケジュールおよび休止パラメータ値、および共通開始時間を持つ VM のグループです。

DP スナップショットの設定では、HX Data Platform バージョン リリースを現在実行している 2 つの既存のクラスタが必要です。クラスタは両方とも同じ HX Data Platform バージョンにある必要があります。HyperFlex Connect を使用してセットアップを完了します。。

まず、各クラスタのローカル レプリケーション ネットワークを設定します。HX Connect を使用して、リモート クラスタにレプリケートするローカル クラスタ ノードが使用する IP アドレスのセットを提供することが含まれます。HX Connect では、専用の ローカル レプリケーション ネットワークを使用するために UCS Manager で VLANを作成します。

（注） このオプションを HX Connect で選択すると、UCSM は UCS Manager とファブリック インターコネクトの両方が HyperFlex クラスタに関連付けられている場合にのみ設定されます。UCSM と FI が存在しない場合は、VLAN ID を入力し、HX Connect で UCSM 設定を選択する必要はありません。

2 つのクラスタ、およびそれに対応する既存の関連するデータストアを明示的にペアリングする必要があります。ペアリングのセットアップは、2つのクラスタのいずれかからHX Connectを使用して完了できます。これには、他方のクラスタの管理者クレデンシャルが必要です。

現在アクティブになっているクラスタでHX Connectを使用することで、仮想マシンを保護 (または、既存の保護属性を変更) することができます。

HX Connect を使用して、クラスタでの着信および発信の両方のレプリケーションのアクティビティをモニタすることができます。

障害の後、DP スナップショット リカバリ サイトとして機能するクラスタで、保護された VM を回復して実行できます。

レプリケーションとディザスタ リカバリ要件の考慮事項

（注） HyperFlex 機能の N:1 DR のドキュメントは、Intersight ヘルプ センターにあります。URL は https://www.intersight.com/help/saas/resources/replication_for_cisco_hyperFlex_clustersです。

仮想マシンのレプリケーションの構成時および仮想マシンのディザスタ リカバリの実行時には、以下にリストする要件および考慮事項があります。

- **データストアのマッピング解除の動作**：

  [他のDROデータストアペアのマッピング解除（Unmap Other DRO datastore pair）] は、いずれかのサイトでVMがアクティブ（保護）状態の場合にサポートされます。アクティブ以外の状態（たとえば、Recovered、Recovery_Failed、Migrate_Failed）のVMは、他のDROデータストアペアのマップ解除をサポートするために、アクティブ（保護）状態に移行する必要があります。

- **その他の DRO データストア削除操作**：

  次のガイドラインが適用されます。

  - 削除操作は、HXDP リリース 6.0(1a) へのアップグレード後にサポートされます。
  - スケジュールの追加と編集はサポートされていません。
  - DRO データストアのマッピング解除が並行して行われる場合、データストアのマッピングとマッピング解除はサポートされません。

- **[すべての保護されたVM（All Protected VMs）] タブの使用**：SRM（OtherDRO）VM の **[すべての保護された VM（All Protected VMs）]** タブから使用可能な DR アクションを実行しません。
- **HXDP 6.0(1a) アップグレード後のアクション**：

  HyperFlex が SRA/SRM ペアを作成して VM を保護すると、SRM は反対側のサイトに同じ名前のプレースホルダ VM を作成し、移行とリカバリ中に VM のリソースを予約します。HXDP 6.0(1a) にアップグレードした後は、プレースホルダ VM を削除することをお勧めします。このアクションの完了に失敗すると、反対側のサイトに同じ名前の VM が存在するため、DR ワークフローが失敗します。

⚠

注意 **SRM を介した操作**：SRM 内の VM であっても、環境は計画移行またはディザスタ リカバリの実行に使用できます。Cisco では、ユーザーが SRM を介してあらゆる種類の操作を実行することを推奨していません。

管理者ロールの要件

ローカル クラスタで管理者権限とともにすべてのレプリケーションおよびリカバリ タスクを実行できます。リモート クラスタに関連するタスクについては、ローカルとリモート ユーザの両方に管理者権限が必要です。各クラスタで vCenter SSO を使用して管理者権限を設定できます。

ネットワーキング要件

レプリケーション ネットワークが信頼でき、HyperFlex レプリケーション ネットワークで構成されている帯域幅と同じ最小の対称帯域幅が持続しあります。アップリンクまたはダウンリンク上の他のアプリケーションまたはトラフィックとネットワークを共有しないでください。その他の要件は次のとおりです。

表 *10 :* ネットワーキング要件

要件：	説明
最小および推奨帯域幅	サポートされる最小帯域幅は 10 Mbps です。推奨帯域幅は、レプリケーションに使用可能なネットワークリンク帯域幅の半分です。たとえば、使用可能なネットワークリンク帯域幅が 100 Mbps の場合、レプリケーション帯域幅を 50 Mbps に設定する必要があります。
適応帯域幅制御	レプリケーション ネットワークに変動があると、ネットワーク帯域幅も変動し、ネットワーク エラーが発生する可能性があります。レプリケーションの適応帯域幅制御は、エラーが検出された場合はレプリケーション速度を動的に調整してスケールダウンし、エラーがクリアされると、構成されたレプリケーション帯域幅制限までスケールアップします。 (注) 適応帯域幅制御は、レプリケーション ネットワークの帯域幅制限が有効になっており、ゼロ以外の数として構成されている場合にのみ有効です。レプリケーション ネットワークの帯域幅制限が有効になっていない場合、適応帯域幅制御は無効です（デフォルト）。レプリケーション帯域幅制限を有効にするには、10 ～ 100,000 Mbit/s の範囲で帯域幅値を入力する必要があります。管理者には、デフォルト設定を使用するのではなく、常に両方のクラスタでレプリケーション ネットワークの帯域幅制限を構成することをお勧めします。

要件：	説明

使用可能なレプリケーションネットワーク帯域幅の測定	iperf ユーティリティを使用して、2 つのサイト間の HyperFlex レプリケーションネットワークの帯域幅を測定できます。iperf ユーティリティを使用するための準備として、両方の HyperFlex クラスタでローカルレプリケーションネットワークを設定します。ローカルレプリケーションネットワークを設定したら、HyperFlex クラスタをペアリングできます。HyperFlex クラスタをペアリングしたら、ローカルデータストアの 1 つをリモート HyperFlex クラスタのデータストアにマッピングします。
	• マッピングされた両方のデータストアにユーザ VM を展開します。それぞれの HyperFlex レプリケーションネットワークで使用されているものと同じネットワークとゲートウェイでユーザ VM を設定します。HyperFlex ストレージコントローラ VM の Linux ディストリビューションに合わせて、VM を Ubuntu 16.04 にすることができます。
	（注） これらの VM は、ネットワーク帯域幅のテストのみを目的としています。テストが完了したら、削除できます。これらの VM を保護する必要はありません。
	• 次のコマンドを実行して、両方のユーザ VM に iperf ユーティリティをインストールします。
	`apt get install iperf`
	• 次のコマンドを実行して、サイト B に展開されたユーザ VM で iperf サーバを実行します。
	`iperf -s`
	`Example Output:`
	`------------------------------------------------------------`
	`Server listening on TCP port 5001`
	`TCP window size: 85.3 KByte (default)`
	`------------------------------------------------------------`
	ポート 5001 はサイト間で開いている必要があります。

要件：	説明
使用可能なレプリケーションネットワーク帯域幅の測定（続）	• サイト A のユーザ VM で次の iperf コマンドを実行します。 `iperf -c <server ip> -i <interval in secs> -t <time in seconds>` Example Output: Client connecting to a.b.c.d TCP port 5001 TCP window size: 85.0 KByte (default) -- local w.x.y.z port 47642 connected with a.b.c.d port 5001 0.0-10.0 sec 44.8 MBytes 37.6 Mbits/sec 10.0-20.0 sec 222 MBytes 187 Mbits/sec 20.0-30.0 sec 312 MBytes 261 Mbits/sec 30.0-40.0 sec 311 MBytes 261 Mbits/sec 40.0-50.0 sec 312 MBytes 262 Mbits/sec 50.0-60.0 sec 311 MBytes 261 Mbits/sec 60.0-70.0 sec 312 MBytes 262 Mbits/sec 70.0-80.0 sec 312 MBytes 262 Mbits/sec 80.0-90.0 sec 311 MBytes 261 Mbits/sec 90.0-100.0 sec 312 MBytes 262 Mbits/sec 100.0-110.0 sec 311 MBytes 261 Mbits/sec (注) 最初のペアのクラスタから 2番目のペアのクラスタへ、次に 2番目のペアのクラスタから最初のペアのクラスタへの両方向でテストを実行します。これが他のアプリケーションとの共有リンクである場合は、レプリケーションスケジュールの実行時にテストを実行します。このリンクが共有されると、複製に使用可能な帯域幅が影響を受け、複製ネットワークで輻輳が発生し、パケットがドロップされる可能性があります。HyperFlex レプリケーションエンジンはパケットドロップを監視し、必要に応じてレプリケーショントラフィックを抑制します。

要件：	説明

Maximum Latency	サポートされるレプリケーションネットワークの最大遅延は、2 つのペアクラスタ間で 75 ms です。一部のレプリケーションジョブでエラー状態が発生し、失敗する可能性がある状況があります。たとえば、複数のレプリケーションジョブが低いネットワーク帯域幅と高い遅延で同時に実行される場合に発生することがあります。このような状況が発生した場合、レプリケーションネットワークの帯域幅を増加するか、同時レプリケーションジョブの数をずらしてジョブの同時実行性を減少させます。この状況が続く場合、オペレーションを VM 保護しないと予想以上に時間がかかる場合があります。
	レプリケーションネットワーク遅延の測定
	サイト A とサイト B のストレージコントローラ VM のいずれかで ping コマンドを実行することで、平均レプリケーションネットワーク遅延を測定できます。
	サイト A から、次の例のように ping コマンドを実行します。
	`ping -I eth2 "Repl IP of any ctlvm on site B" -c 100`
	`Example Output:`
	`100 packets transmitted, 100 received, 0% packet loss, time 101243ms`
	`rtt min/avg/max/mdev = 0.112/0.152/0.275/0.031 ms`
	平均遅延は 75 ミリ秒以下である必要があります。
	（注） サイト A からサイト B、サイト B からサイト A の両方向で ping コマンドを実行します。

要件：	説明
ネットワークポート	HyperFlex 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。HyperFlex レプリケーションのポート/プロトコル要件（2021 年 9 月付けのバージョン 4.5.2a rev 3 以降）は、ICMP、TCP：9338、9339、3049、4049、4059、9098、8889、および 9350 です。 **ネットワークポートのテスト** HyperFlex クラスタの内部では、サイトのペアリング操作中に送信元と宛先のストレージコントローラ VM でファイアウォールエントリが作成され、HX データプラットフォームがシステムに双方向でアクセスできるようにします。各 HX ノード複製IP アドレスおよび管理CIP アドレスに対して、WAN ルータでこのトラフィックを許可する必要があります。 HyperFlex クラスタでローカルレプリケーションネットワークを設定する場合、**ローカルレプリケーションネットワークのテスト**アクションを手動で実行して、ローカルクラスタ上の各ストレージコントローラ VM のレプリケーション IP アドレス間の接続をテストできます。このテストには、ポート接続とファイアウォールのチェックが含まれます。2 つのクラスタがペアリングされている場合は、**リモートレプリケーションネットワークのテスト**アクションを手動で実行して、各ローカルストレージコントローラ VM と各リモートストレージコントローラ VM間の接続をテストできます。ポートの接続とファイアウォールのチェックが実行されます。 ポートの接続を確認する追加オプションとして、Linux の「netcat」ユーティリティを使用することもできます。

要件：	説明
ネットワーク損失	信頼性の高いデータ伝送により、2つのペアクラスタ間のレプリケーションが最適に機能します。2 つのペアクラスタ間のデータ伝送でパケット損失が発生すると、レプリケーションのパフォーマンスが低下する可能性があります。 **ドロップしたパケットの分析** パケットの損失が発生する可能性があるのは、ネットワーク輻輳と一時的なネットワークデバイスエラーの 2 つのケースです。 ネットワークの輻輳が原因でレプリケーションネットワークでドロップされたパケットが発生した場合、HyperFlex クラスタレプリケーションエンジンはレプリケーション帯域幅を自動的に調整します。レプリケーションネットワーク帯域幅をスロットリングすると、ネットワークの輻輳が軽減され、ドロップされたパケットが削減されます。極端な場合、レプリケーション帯域幅のスロットリングにより、レプリケーションジョブが予想よりも完了するまでに時間がかかることがあります。 一時的なネットワークデバイスのエラーが原因でレプリケーションネットワークでパケットがドロップされると、ランダムにまたは特定の時刻にレプリケーション障害が発生する可能性があります。 ドロップされたパケットは、HX Connect ユーザインターフェイスでは報告されません。 パケットドロップの発生は、HyperFlex ストレージコントローラのログに記録されます。レプリケーションジョブの延長やその他の障害が目立つ場合は、サポートに連絡してサポートを受けてください。

クラスタの要件

仮想マシン レプリケーションの設定および仮想マシンのディザスタ リカバリを設定するとき、次のクラスタ要件を満たしていることを確認してください。

ストレージ領域の要件

両方のクラスタに、複製された DP スナップショットの保持と処理に十分なスペースがあることを確認します。保護された VM ごとに、設定されたスケジュール間隔に基づいて DP スナップショットが作成され、複製されます。最近成功した複製された DP スナップショットが宛先 HyperFlex クラスタに保持されます。保護されたすべての VM について、ソースクラスタには最大 2 つの DP スナップショットが存在し、宛先クラスタには最大 2 つの DP スナップショットが存在することに注意してください。このアプローチにより、効率的な差分ベースの複製が容易になり、新しい DP スナップショットが複製プロセスを正常に完了できなかった場合に、最新の正常に複製された DP スナップショットを確実に回復できるようになります。ストレー

ジキャパシティの方法が適用されますが（重複、圧縮を含む）、複製された各仮想マシンが一部のストレージ スペースを消費します。

- **Redologスナップショットで保護されたVMによって消費される領域**：VMware redologスナップショットもあるVMを保護すると、VMのコンテンツ全体が複製されます。コンテンツ全体には、VMと保持されているVMware redologスナップショットが含まれます。これにより、ペアのHyperFlexクラスタの両方でストレージ領域の使用率が増加します。より多くのredologスナップショットが保持されると、ストレージ領域の消費量も増加します。

- **HX ネイティ ブスナップショットで保護されたVMによって消費される領域**：HX ネイティブ スナップショットもあるVMを保護する場合、最新のVMデータのみが複製されます。保持されたHXネイティブスナップショットデータは複製されません。通常、レプリケーション先のHyperFlexクラスタでHX ネイティブ スナップショットによって消費される領域を考慮する必要はありません。

- **削除されたVMによって消費された領域**：保護されたVMを削除しても、ペアになったHyperFlexクラスタデータストアの領域は再利用されません。正常に複製された最新のDPスナップショットは、VMを誤って削除しないように保持されます。保護されたVMによって消費された領域を再利用するには、まずVMを保護解除する必要があります。VMが保護されていない場合、関連付けられたDPスナップショットは、ペアになった両方のHyperFlexクラスタで削除されます。

- **スペース消費量の計算**：保護されたVMのサイズに加えて予測されるスペース消費量は、次のように表すことができます。

  VM の変更率と保持される *DP* スナップショットの数

  保持されるDPスナップショットの数は2です。保護されたVMにVMware redologスナップショットがある場合、計算は保持されるスナップショットの数に基づいて偏ります。

  スペースの計算では、保護されたVMがフェールオーバーしたとき、またはペアのサイトに移行したときに、ソースとターゲットの計算を逆にできることも考慮する必要があります。

- **差分ベースのレプリケーションとフルコピー レプリケーション**：一般的なレプリケーションデータ保護ライフサイクルでは、保護されたVMのフルコピーがDPスナップショットの形式で1回だけ複製されます。このフルコピー レプリケーション ジョブは、VMが最初に保護されるときに発生します。最初のレプリケーションジョブが完了すると、後続のレプリケーションジョブは効率的な差分ベースのテクノロジーを利用して、新規および変更されたデータのみを複製します。

  次の既知の状況では、差分ベースのテクノロジーを使用できません。

  - 保護されたVMには、HX ネイティブ スナップショットもあります。VMが保持されているHXネイティブスナップショットに戻されると、次にスケジュールされている保護ジョブは、差分ベースのレプリケーション ジョブではなく、フルコピー レプリケーションジョブを実行します。ペアになった両方のクラスタで、追加のフルコピーに相当する領域をバジェットする必要があります。

- 保護された VM はストレージ vMotion を実行し、別のデータストアに移行されます。宛先データストアがペアリングされたクラスタのデータストアにマッピングされている場合、次にスケジュールされている保護ジョブは差分ベースのレプリケーションジョブではなく、フルコピー レプリケーションジョブを実行します。ペアになった両方のクラスタで、追加のフルコピーに相当する領域をバジェットする必要があります。
- 保護された VM には、レプリケーション ジョブと一緒に作成された DP スナップショットがあります。これに続いて、HX Sentinel スナップショットも作成する最初の HX ネイティブ スナップショットが作成されます。次のスケジュールされた保護ジョブは、差分ベースの複製ジョブではなく、完全コピー複製ジョブを実行します。ペアになった両方のクラスタで、追加のフルコピーに相当する領域をバジェットする必要があります。
- 中間デルタ ディスクを作成した HX ネイティブ スナップショットワークフロー中に保護された VM Dp スナップショットが取得されると、差分ベースのレプリケーション ジョブではなく、次のスケジュールされた保護ジョブがフルコピー レプリケーション ジョブを実行します。ペアになった両方のクラスタで、追加のフルコピーに相当する領域をバジェットする必要があります。
- すでに保護されている VM に新しい VMDK を追加すると、その特定の VMDK がフルコピーされます。

リモート クラスタに十分なストレージ容量がないと、リモート クラスタで使用可能な最大容量に達する可能性があります。**スペース不足**エラーに気付いた場合は、「スペース不足エラーの処理」を参照してください。クラスタが適切に調節された状態でスペースが利用可能になるまで、すべてのレプリケーション スケジュールを一時停止します。クラスタ容量の消費量が常にスペース使用率の警告しきい値を下回るようにしてください。

サポートされる構成

ネイティブ レプリケーション（NRDR 1：1）でサポートされる構成は、2N / 3N / 4N Edge、FI と DC-no-FI ベースのクラスタから 2N / 3N / 4N Edge、FI と DC-no-FI ベースのクラスタ（ストレッチ クラスタを含む）であり、すべて HX Connect で管理されます。

HyperFlex ハードウェア アクセラレーション カード（PID：HX-PCIE-OFFLOAD-1）は、HX 4.5（1a）以降のネイティブレプリケーションでサポートされています。ペアの HyperFlex クラスタの両方で HX ハードウェア アクセラレーションを有効にする必要があります。

ノードの再起動

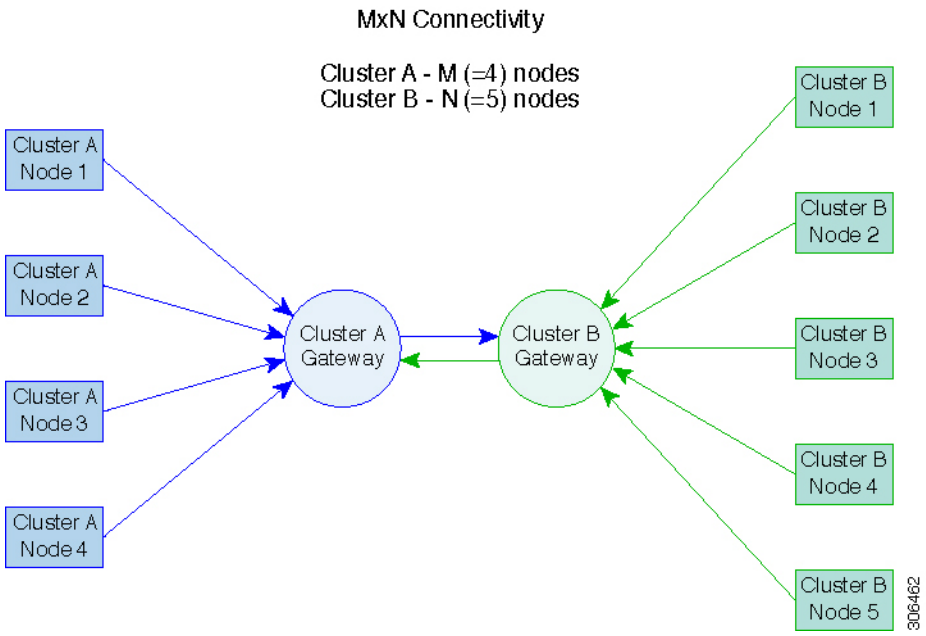
復元、レプリケーション、またはリカバリ操作中に、HX クラスタ内のノードを再起動しないでください。ノードのリブート操作は、アップグレードプロセスの一部として実行される場合があることに注意してください。アップグレード前にレプリケーション スケジューラを一時停止し、アップグレードの完了後に再開する必要があります。

レプリケーション ネットワークとペアリングの要件

データ保護（DP）スナップショットにレプリケーションを使用するHyperFlexクラスタ間にレプリケーションネットワークを確立する必要があります。各クラスタとサイト内の他のトラフィックから、クラスタ間レプリケーションのトラフィックを特定するために、レプリケーション ネットワークが作成されます。次の点も考慮してください。

表 *11* : レプリケーション ネットワークとペアリングの要件

コンポーネント	説明
HX Data Platform のバージョン	レプリケーションのためにペアリングされる HyperFlex クラスタが同じ HX Data Platform ソフトウェア バージョンを実行していることを確認します。異なるHX Data Platformバージョンの使用は、HX Data Platform のアップグレード中にのみサポートされることに注意してください。このシナリオでは、ペアになった HyperFlex クラスタのいずれかが、ペアになった両方のクラスタがアップグレードされるまでの間、異なるバージョンの HX Data Platform ソフトウェアを実行している可能性があります。サイト固有の制約に基づいて、最短時間内に、ペアになった両方のクラスタを同じ HX Data Platform バージョンにアップグレードしてください。また、ペアリングされたクラスタをアップグレードする場合、最大 1 つのメジャー HX Data Platform リリース バージョンの違いが許可されることに注意してください。また、アップグレード時にペアリングされたクラスタの両方が同じ HX Data Platform バージョンを実行していない場合、レプリケーション設定パラメータの変更はサポートされません。
ノードステータス	ローカル レプリケーション ネットワークを作成し、サイト ペアリング プロセスを実行する前に、すべての HyperFlex クラスタ ノードがオンラインであり、完全に動作していることを確認します。

コンポーネント	説明
ノード通信の要件	要件は次のとおりです。 • 効率的なレプリケーションをサポートするには、クラスタ間の N x M 接続図で示されるように、クラスタ A のすべての M ノードがクラスタ B のすべての N ノードと通信できるようにすることです。 • クラスタ間のレプリケーション トラフィックがサイトの境界を越えてインターネットを通過するためには、クラスタ A の各ノードがサイトの境界とインターネットを超えて、クラスタ B 上の各ノードと通信できるようにすることです。 • 分離レプリケーション トラフィックは、クラスタやデータ センター内の他のトラフィックからされるます。 詳細については、次の図を参照してください。
クラスタ間 M x N 接続  	

コンポーネント	説明
ノード障害	まれにしか発生しないノード障害のイベントでは、レプリケーションに影響が及ぶ可能性があります。たとえば、レプリケーション CIP アドレスを持つノードが動作不能状態になると、進行中のレプリケーション ジョブが停止します。レプリケーション CIP アドレスがクラスタ内の別のノードによって要求された時点で、レプリケーションジョブが自動的に再開されます。同様に、レプリケーション CIP アドレスを持つノードでリカバリ ジョブが実行されていた場合、そのノードは失敗します。複製CIP アドレスは、その後クラスタ内の別のノードによって要求されます。障害が発生したら操作を再試行してください。
vCenter の推奨事項	- 2 つのペアの HyperFlex クラスタのそれぞれが一意の vCenter インスタンスによって管理されていることを確認します。また、ディザスタ リカバリ シナリオでの可用性のために、vCenter が別の障害ドメインに展開されていることを確認します。

レプリケーションとディザスタ リカバリ仮想マシンの考慮事項

VM の考慮事項は次のとおりです。

表 *12 :* 仮想マシンの考慮事項

検討	説明
シン プロビジョニング	保護された VM は、元されていた仮想マシンでのディスクの指定方法に関係なく、シンプロビジョニングされたディスクでリカバリされます。
VM デバイスの制限	個別に保護された VM として、または保護グループ内で、接続された ISO イメージまたはフロッピーで VM を保護しないでください。[接続済み（Connected）]状態を無効にして、設定済みの CD または DVD ドライブを[クライアントデバイス（Client Device）]に設定できます。VM設定からデバイスを削除する必要はありません。ISO イメージを一時的にマウントする必要がある場合は、CD または DVD ドライブを[クライアントデバイス（Client Device）]に設定してから切断すると、VM の保護を解除して再度保護できます。

検討	説明
保護された仮想マシンのスケーラビリティ	HX リリース 4.5(1a) 以降： • すべてのノード上で保護された VM の合計が、単一方向設定でクラスタあたり最大2000の保護されたVM、双方向設定の場合 1000 の保護された VM の上限を超えないようにする必要があります。 • 1 つの保護グループに設定可能な VM の最大数は 64 です。 • 最大 100 個の保護グループがサポートされます。
非HX データストア	HX データストア上にストレージが含まれている VM を保護している場合、この VM での定期的なレプリケーションは失敗します。障害を回避するには、VM の保護を解除するか、VM から非 HX ストレージを削除します。保護された VM を HX データストアから非 HX データストアに移動しないでください。vMotion を使用する前に、ストレージの vMotion を通じて非 HX データストアに VM を移動する場合、VM の保護を解除します。
テンプレート	テンプレートはディザスタ リカバリをサポートしていません。テンプレートを保護しようとしないでください。
スナップショットがある仮想マシンのリカバリ	VMware redolog スナップショットを持つ保護された VM をリカバリすると、VM がリカバリされ、以前のすべてのスナップショット redolog スナップショットが保持されます。
データ保護スナップショット	複製された DP スナップショットは、ペアになっているクラスタのマッピングされたデータストアに保存されます。サポートされていないため、DP スナップショットの手動削除は実行しないでください。スナップショットディレクトリまたは個別ファイルを削除すると、HX データ保護とディザスタ リカバリが損なわれる可能性があります。 （注） DP スナップショットを手動で削除しないようにするには、VMware が管理者ユーザーによるデータストアの操作を制限しないことに注意してください。VMware 環境と同様に、vCenterブラウザを介して管理ユーザがアクセスするか、または ESXi ホストにログインすることによって、データストアにアクセスできます。このため、スナップショットディレクトリとコンテンツは参照可能で、管理者がアクセスできます。

検討	説明
VM の命名	vCenter から保護済み VM の名前を変更すると、HyperFlex は以前の名前フォルダで回復しますが、復元側で新しい名前を使用して VM を登録します。次に、この状況の制限事項の一部を示します。 • VMware を使用すると、任意の場所にある VMDK を VM に接続できます。このような場合、HyperFlex は VM フォルダ内の VM を回復しますが、元の場所にマップされている場所ではありません。また、VMDK がパスによって virtualmachine name.vmx ファイルで明示的に参照されている場合、復元が失敗することがあります。データは正確に復元していますが、vCenter への VM の登録に問題がある可能性があります。このエラーを修正するには、virtualmachine name.vmx ファイル名を新しいパスで更新します。 • VM の名前が変更され、その後に VMDK が追加された場合、新しい VMDK は [sourceDs] newVm/newVm.vmdk で作成されます。HyperFlex は、この VMDK を以前の名前で復元します。その場合、VMDK がパスによって virtualmachine name.vmx ファイルで明示的に参照されている場合、復元が失敗することがあります。データは正確に復元していますが、仮想センターへの VM の登録に問題がある可能性があります。このエラーを修正するには、virtualmachine name.vmx ファイル名を新しいパスで更新します。
HyperFlex ソフトウェア暗号化	暗号化されたデータストア上のVMを保護できるようにするには、ペアになっている両方のデータストアのクラスタでソフトウェア暗号化を有効にする必要があります。

ストレージ レプリケーション アダプタの概要

VMware vCenter Site Recovery Manager (SRM) の Storage Replication Adapter (SRA) は、VMware vCenter サーバのストレージ ベンダー特有のプラグインです。アダプタは、ストレージ仮想マシン (SVM) レベルとクラスタ レベル設定で。SRM とストレージ コントローラ間の通信を可能にします。アダプタは SVM と通信して、複製されたデータストアを検出します。

SRM のインストールと設定の詳細については、SRM リリース バージョンに従って次のリンクを参照してください。

- SRM 8.1 のインストール:https://docs.vmware.com/en/Site-Recovery-Manager/8.1/srm-install-config-8-1.pdf

- SRM 6.5 のインストール:https://docs.vmware.com/en/Site-Recovery-Manager/6.5/srm-install-config-6-5.pdf
- SRM 6.0 のインストール:https://docs.vmware.com/en/Site-Recovery-Manager/6.0/srm-install-config-6-0.pdf

保護および復元サイトの両方で、Site Recovery Manager サーバ ホストに適切な SRA をインストールする必要があります。複数のタイプのストレージアレイを使用する場合は、両方の Site Recovery Manager サーバ ホストで、各タイプのアレイに SRA をインストールする必要があります。

SRA をインストールする前に、SRM および JDK 8 以降のバージョンが、保護および復元サイトの Windows マシンにインストールされていることを確認します。

SRA をインストールするには、次の手順を実行します。

1. VMware サイトから SRA をダウンロードします。

   https://my.vmware.com/web/vmware/downloads ページで、VMware Site Recovery Manager を検索し、**[Download Product (製品のダウンロード)]** をクリックします。**[Drivers & Tools (ドライバおよびツール)]** をクリックし、**[Storage Replication Adapters (ストレージ複製アダプタ)]** を展開し、**[Go to Downloads (ダウンロードに進む)]** をクリックします。

2. SRA Windows インストーラを、保護および復元サイトの両方で SRM Windows マシンにコピーします。
3. インストーラをダブルクリックします。
4. インストーラの [Welcome (ようこそ)] ページで **[Next (次へ)]** をクリックします。
5. EULA に同意して、**[Next (次へ)]** をクリックします。
6. **[完了（Finish）]** をクリックします。

（注） SRM プログラム フォルダ内に SRA がインストールされます。

```
C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra
```

SRA のインストール後に、SRM リリース バージョンに従って次のガイドを参照し、SRM 環境の設定を行います。

- SRM 8.1 の設定:https://docs.vmware.com/en/Site-Recovery-Manager/8.1/srm-admin-8-1.pdf
- SRM 6.5 の設定:https://docs.vmware.com/en/Site-Recovery-Manager/6.5/srm-admin-6-5.pdf
- SRM 6.0 の設定:https://docs.vmware.com/en/Site-Recovery-Manager/6.0/srm-admin-6-0.pdf

設定後、SRM は SRA と連携してアレイを検出し、複製およびエクスポートされたデータストアを検出し、フェールオーバーまたはフェールオーバーのデータストアをテストします。

SRA により、SRM が次のワークフローを実行できるようにします。

- 複製されたストレージの検出
- 複製データの書き込み可能コピーを使用した中断フェールオーバー テストの復元
- 緊急または計画されたフェールオーバー復元
- フェールバックの一部としてフェールオーバー後に複製を戻す
- 実稼働テストの一環として、フェールオーバー後の複製を復元する

データ保護の用語

間隔：レプリケーション スケジュール設定の一部。保護された VM の DP スナップショットを取得してターゲット クラスタにコピーする頻度を指定するために使用します。

ローカル クラスタ：VM レプリケーション クラスタ ペアで、HX Connect を通じて現在ログインしているクラスタ。ローカル クラスタから、ローカル上に存在する VM にレプリケーション保護を設定できます。VM はペアリング済みのリモート クラスタにレプリケートされます。

移行—VM の最近のレプリケーション スナップショットのコピーが稼働中の VM になる場合、定期的なシステム メンテナンスと管理タスク。ソースおよびターゲット クラスタのレプリケーション ペアは変更されません。

プライマリ クラスタ—VM ディザスタ リカバリのソース クラスタの別の名前。

保護された仮想マシン—レプリケーションが設定されている VM。保護された VM は、レプリケーション ペアのローカル クラスタのデータストアに存在します。保護された VM には個別または保護グループを通じて設定されたレプリケーション スケジュールがあります。

保護グループ：同じレプリケーション構成を VM のグループに適用する方法です。

リカバリ プロセス：ソース クラスタに失敗または障害が発生した場合に、保護された VM を回復するための手動プロセス。

リカバリ テスト：災害時にリカバリ プロセスを成功させるためのメンテナンス タスクです。

リモート クラスタ：VM レプリケーション クラスタ ペアの 1 つ。リモート クラスタは、ローカル クラスタの保護された VM からレプリケーション スナップショットを受信します。

レプリケーション ペア：ローカル クラスタ VM のレプリケートされた DP スナップショットを格納するリモートのクラスタ ロケーションを提供するためにまとめられた 2 つのクラスタです。

レプリケーション ペアのクラスタは、リモート クラスタまたはローカル クラスタの両方になることが可能です。レプリケーション ペアの両方のクラスタは、レジデント VM を持つことができます。各クラスタは、自身のレジデント VM に対してローカルです。各クラスタは、ペアリング相手のローカル クラスタに存在する VM に対してリモートです。

DP スナップショット：レプリケーション保護メカニズムの一部。保護された VM の取得されたスナップショットのタイプで、ローカル クラスタからリモート クラスタにレプリケートされます。

セカンダリ クラスタ：VM ディザスタ リカバリ内のターゲット クラスタの別名。

ソース クラスタ：VM レプリケーション クラスタ ペアの 1 つ。ソース クラスタは、保護された VM が置かれる場所となります。

ターゲット クラスタ：VM レプリケーション クラスタ ペアの 1 つ。ターゲット クラスタは、ソース クラスタの VM からレプリケートされた DP スナップショットを受信します。ソース クラスタで障害が発生した場合、VM を回復するためにターゲット クラスタが使用されます。

データ保護とディザスタ リカバリのベスト プラクティス

保護対象の環境に基づく効果的なデータ保護およびディザスタリカバリ戦略の要件は、過大評価することはできません。設計されて展開されるソリューションは、実稼働 VM のリカバリ ポイント目標 (RPO) とリカバリ時間の目標 (RTO) の両方のビジネス要件を満たしている必要があります。次に、この戦略を設計する際に考慮する必要があるポイントの一部を示します。

- ミッション クリティカル、ビジネス クリティカル、および重要な VM を含む可能性のある、さまざまな種類の生産ワークロードに準拠するために必要なサービスレベル契約(SLA)の数。
- 各 SLA の詳細な構造。これには、RPO、RTO、保存されたリカバリ ポイント数、データのオフサイト コピー要件、および異なるメディア タイプにバックアップ コピーを保存するための要件が含まれます。異なる場所、異なるハイパーバイザ、異なるプライベート/パブリック クラウドなど、異なる環境に復元する機能などには、追加の要件がある場合があります。
- ソリューションが設計されたビジネス要件を満たしていることを証明するために機能する各 SLA の継続的なテスト戦略。

バックアップとバックアップ コピーは、保護される HyperFlex クラスタの外部に保存する必要があることに注意してください。たとえば、HyperFlex クラスタ上の VM を保護するために実行されるバックアップは、同じ HyperFlex クラスタでホストされているバックアップ リポジトリまたはディスク ライブラリには保存しないでください。

内蔵 HyperFlex データ保護機能は、次のカテゴリに一般化されています。

- **データ レプリケーション ファクタ**: HyperFlex クラスタ内のデータの冗長コピー数を示します。データ レプリケーション ファクタ 2 または 3 は、データプラットフォームのインストール時に設定できますが、変更することはできません。データ レプリケーション ファクタの利点は、クラスタで許容される障害の数に関係します。データ レプリケーション ファクタの詳細については、「HX Data Platform クラスタで許容される障害 （12 ページ）」の項を参照してください。

（注） データ レプリケーション ファクタ単独では、クラスタの障害が発生した場合や、サイトの拡張が停止した場合に、リカバリの要件を満たすことができない場合があります。また、データ レプリケーション ファクタは、ポイント インタイム リカバリ、複数のリカバリ ポイントの保持、またはクラスタ外部のデータのポイント インタイム コピーの作成を促進することはありません。

- **HX Native スナップショット**: 個々の VM ベースで動作し、一定期間 VM のバージョン保存を有効にします。HX SENTINELスナップショットを含め、最大合計 31 のスナップショットを保持できます。

（注） HX Native スナップショット単独では、珍しいクラスタの障害が発生した場合や、サイトの拡張が停止した場合に、リカバリの要件を満たすことができない場合があります。また、HX Native スナップショットは、クラスタの外部にあるデータのポイントインタイム コピーを作成する機能を促進するものではありません。さらに重要な点として、VM を意図せずに削除すると、削除された VM に関連付けられているデータ プラットフォームの HX Native スナップショットも削除されます。

- **非同期レプリケーション —** HX Data Platform ディザスタ リカバリ機能とも呼ばれ、ネットワークに接続された HyperFlex クラスタのペア間で仮想マシンのスナップショットを複製することにより、仮想マシンの保護を可能にします。VM のレプリケーションでは、一方のクラスで稼働中の保護対象の仮想マシンが、ペアとなっているもう一方のクラスタに複製されます。ペアにする 2 つのクラスタは通常、互いに離れたところに位置し、一方のクラスタが他方のクラスタで実行中の仮想マシンのディザスタ リカバリ サイトとして機能します。

（注） リモート クラスタで複数のポイント インタイム コピーを保持する必要がある場合、非同期レプリケーションのみリカバリの要件を満たしていない可能性があります。特定の VM の最新のスナップショット レプリカのみがリモート クラスタに保持されます。また、非同期レプリケーションは、いずれかのクラスタ外部にあるデータのポイント インタイム コピーを作成する機能を促進するものではありません。

まず、環境における固有のビジネス要件を理解し、これらの要件を満たすかそれらを超える包括的なデータ保護とディザスタ リカバリ ソリューションを展開することをお勧めします。

仮想マシンの保護の概要

仮想マシン (VM) を保護するには、次の保護属性を指定します。

- レプリケーションの DP スナップショットが作成されるレプリケーション間隔。
- 開始時刻（次の 24 時間以内で、VM に対して最初にレプリケーションを試行する時刻の指定）
- VM を停止した状態で DP スナップショットを取得するかどうかを指定します。静止オプションを適切に使用するには、保護されている VM に VMware ツールがインストールされている必要があります。
- ディザスタ リカバリの静止スナップショット用の VMware ゲスト ツールがサポートされています。最新の VMware ゲスト ツール サービスをインストールするか、既存のサービスが最新であることを確認します。

（注） サードパーティ製ゲスト ツール（open-vm-tools）の使用は許可されています。

保護属性を作成し、保護グループに割り当てることができます。VM に保護属性を割り当てるには、保護属性を保護グループに追加します。

たとえば、ゴールド、シルバー、ブロンズの 3 つの異なる SLA があります。各 SLA に保護グループを設定し、レプリケーション間隔を、金は 5 ～ 15 分、銀は 4 時間、銅は 24 時間と設定します。VM のほとんどは、作成済みの 3 つの保護グループのいずれかに追加するだけで保護できます。

VM を保護する方法を次の中から選択できます。

（注） 複数の VM を選択する場合、それらを保護グループに追加する必要があります。

- **Independently**：VM を 1 つ選択し、保護を設定します。特定の VM のレプリケーション スケジュールおよびVMwareの休止オプションを設定します。レプリケーション設定の変更は、個別に保護された VM にのみ影響を与えます。VM は保護グループに含まれません。
- **既存の保護グループ**：1 つ以上の VM を選択し、それらを既存の保護グループに追加します。スケジュールおよび VMware の休止オプション設定は、保護グループ内のすべての VM に適用されます。保護グループの設定を変更する場合、保護グループのすべての VM に変更が適用されます。
- **新しい保護グループ**：2 つ以上の VM を選択し、新しい保護グループを作成することを選択します。保護グループの名前、スケジュール、およびVMwareの休止オプション設定を

定義します。これらの設定は、保護グループ内のすべての VM に適用されます。保護グループの設定を変更する場合、保護グループのすべての VM に変更が適用されます。

データ保護のワークフロー

レプリケーションを使用して VM とそのデータを保護するには、次の手順を実行します。

- レプリケーション ネットワーク アクティビティをサポートするように、2つのクラスタを設定し、お互いがペアになるようにします。
- ソース クラスタに DP のスナップショットを作成して、ターゲット クラスタにそれらをレプリケートする頻度（間隔）を設定する VM のレプリケーション スケジュールを割り当てます。個々の VM と保護グループにレプリケーション スケジュールを割り当てることができます。

レプリケーション ワークフロー

1. HX データ プラットフォーム をインストールし、2 つのクラスタを作成します。
2. 各クラスタに 1 つ以上のデータストアを作成します。
3. HX 接続 にログインします。
4. レプリケーション ネットワークを作成する前に、レプリケーション ネットワークに使用される IP アドレス、サブネット マスク、VLAN、ゲートウェイ、および IP 範囲を確認します。複製ネットワークの作成後は、このレプリケーション ネットワークを介して、クラスタ内の接続を検証します。
5. デフォルトの MTU 値は 1500 です。HyperFlex クラスタが OTV またはその他のトンネリング メカニズムを使用する場合は、サイト間またはクラスタ間の接続で機能する MTU を必ず選択します。Cisco HyperFlex リリース 5.0(2a) 以降、MTU フィールドは編集可能です。
6. 各クラスタでクラスタ レプリケーション ネットワークを設定します。レプリケーション ネットワーク情報は、各クラスタで一意です。

   レプリケーション ネットワーク専用のサブネット、ゲートウェイ、IP アドレスの範囲、帯域幅制限を指定します。HX データ プラットフォーム は UCS Manager を介して両方のクラスタの VLAN を設定します。
7. クラスタ間のネットワーク テストは、レプリケーション ネットワークの設定後、クラスタのノード間の接続を検証するために実行されます。クラスタ間のネットワーク テストが失敗した場合、レプリケーション ネットワーク設定がロールバックされます。問題を修正した後、レプリケーション ネットワークを再設定します。
8. レプリケーション ペアを作成する前に、このペアをサポートする社内ネットワークが更新されていることを確認します。

9. 1 つのクラスタから別のクラスタへのレプリケーション ペアを作成し、2 つのクラスタを接続します。レプリケーションペアを作成した後、クラスタ間ペア ネットワークのテストを実行し、クラスタ間の双方向接続を検証します。両方のクラスタからのデータストア マッピングを設定します。
10. オプションで、保護グループを作成できます。
    - スケジュールを設定します。各保護グループにスケジュールが 1 つ必要です。
    - 異なる VM 用にさまざまなレプリケーション間隔（スケジュール）がある場合は、複数の保護グループを作成します。VM は、1 つの保護グループにのみ属することができます。
11. 個々の VM または保護グループに割り当てられた仮想マシンとして、保護する VM を選択します。
12. 保護を設定し、次の手順を実行します。
    1. 1つ以上の VM を選択します。[Protect] をクリックします。
    2. [VM の保護] ウィザードでのオプションは次のとおりです。
       - 既存の保護グループを通じて 1 つの VM を保護します。
       - 1 つの VM を個別に保護します。

         スケジュールを設定します。
       - 既存の保護グループを通じて複数の VM を保護します。
       - 新しい保護グループで複数のVMを保護します。

         新しい保護グループを作成して、スケジュールを設定します。

HX Connect でレプリケーション ネットワークを設定する

レプリケーション ペアを構成するには、その前に、ローカル/リモートの両方のクラスタでレプリケーション ネットワークが構成されている必要があります。ローカル クラスタで設定を完了してから、リモート クラスタにログインして、そこで構成を完了します。

始める前に

複製ネットワークを設定する前に、次の前提条件を満たしていることを確認します

- 少なくとも N + 1 個の IP アドレスが必要です（N はコンバージド ノードの数）。また、これらの新しい IP アドレスにまたがる IP サブネット、ゲートウェイ、およびこのサブネットに関連付けられた VLAN も必要です。
- 将来のクラスタ拡張に対応するには、今後使用できる十分な数の IP アドレスがサブネットに存在することを確認してください。展開されたクラスタ内の新しいノードには、複製

用の IP アドレスも割り当てる必要があります。前の手順で指定したサブネットは、潜在的な新しい IP 範囲にまたがっている必要があります。

- 後で IP プール範囲をネットワークに追加することはできますが、レプリケーション ネットワークですでに設定されている IP プールを変更することはできません。
- レプリケーション ネットワークに使用する IP アドレスが、他のシステムでまだ使用されていないことを確認してください。
- レプリケーション ネットワークを作成する前に、レプリケーション ネットワークに使われる IP アドレス、サブネット、VLAN、ゲートウェイを確認します。

手順

ステップ 1 管理者権限のユーザーとして HX Connect にログインします。

ステップ 2 **[Replication]** > **[Replication Configuration]** > **[Configure Network]** を選択します。

（注） レプリケーション ネットワークを構成できるのは 1 回のみです。構成後は、使用可能な IP アドレスとネットワーク帯域幅を編集できます。

ステップ 3 **[レプリケーション ネットワークの構成（Configure Replication Network）]** ダイアログボックスの **[VLAN ネットワークの構成（Configure VLAN Network）]** タブで、ネットワーク情報を入力します。

UI 要素	基本的な情報
[既存の VLAN の選択（Select an existing VLAN）] オプション ボタン	このラジオ ボタンをクリックして、既存の VLAN を追加します。 レプリケーション ネットワークで使用するために VLAN を Cisco UCS Manager を通じて手動で設定した場合、その VLAN ID を入力します。
[新しい VLAN の作成] ラジオ ボタン	このラジオ ボタンをクリックして、新規 VLAN を作成します。 （注） Edge クラスタでレプリケーション ネットワークを構成している場合は、**[VLAN の作成]** オプションを使用しないでください。既存の VLAN オプションを使用して、同じ手順に従います。

UI 要素	基本的な情報
[VLAN ID] フィールド	上矢印または下矢印をクリックして VLAN ID の番号を選択するか、フィールドに番号を入力します。 これは、HXデータ プラットフォーム管理トラフィック ネットワークおよびデータ トラフィック ネットワークとは別のものです。 **重要** レプリケーション ペアを構成する HX ストレージ クラスタごとに、異なる VLAN ID を必ず使用してください。 レプリケーションは、2 つの HX ストレージ クラスタ間で行われます。各 HX ストレージ クラスタには、レプリケーション ネットワーク専用の VLAN が必要です。 たとえば、*3* です。 値を追加すると、デフォルトの VLAN 名が更新されて追加の ID が組み込まれます。VLAN ID の値は、手動で入力される VLAN 名には影響を与えません。
[VLAN名（VLAN Name）] フィールド	**[Create a new VLAN]** ラジオ ボタンを選択した場合、このフィールドにはデフォルトの VLAN 名が入力されます。VLAN ID は名前に紐づけられます。
ストレッチ クラスタの場合は、プライマリおよびセカンダリ FI（サイト A とサイト B ）の Cisco UCS Manager ログイン情報を入力します。通常のクラスタの場合は、単一の FI の Cisco UCS Manager ログイン情報を入力します。	
[UCS Manager のホスト IP または FQDN（UCS Manager host IP or FQDN）] フィールド	Cisco 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。
[ユーザ名（Username）] フィールド	Cisco UCS Manager の管理ユーザー名を入力します。
[パスワード（Password）]フィールド	Cisco UCS Manager の管理パスワードを入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 **[IP & Bandwidth Configuration]** タブで、ネットワーク パラメータとレプリケーション帯域幅を設定します。

UI 要素	基本的な情報

[サブネット（Subnet）] フィールド	レプリケーション ネットワークで使用するサブネットを、ネットワーク プレフィックス表記で入力しますサブネットは HX データ プラットフォーム 管理トラフィック ネットワーク およびデータ トラフィック ネットワーク とは別です。
	`Format example:`
	`x.x.x.x/<number of bits>`
	`1.1.1.1/20`

[ゲートウェイ（Gateway）]フィールド	複製ネットワークで使用するゲートウェイ IP アドレスを入力します。ゲートウェイは、HX データ プラットフォーム 管理トラフィック ネットワーク および データ トラフィック ネットワーク で異なります。 たとえば、*1.2.3.4* と指定します。 （注） 障害復旧が flat ネットワーク用に設定されている場合でも、ゲートウェイ IP アドレスにアクセスできる必要があります。
[IP範囲（IP Range）] フィールド	レプリケーション ネットワークで使用する IP アドレス範囲を入力します。 • 必要な IP アドレスの最小数は、HX Storage クラスタのノード数プラス 1 です。 たとえば、4 ノードのHX ストレージ クラスタの場合、少なくとも 5 つの IP アドレスを含むように範囲を入力します。 • **[開始（from）]** の値には、**[終了（to）]** の値より小さい値を指定する必要があります。 たとえば、*From 10.10.10.20 To 10.10.10.30* とします。 • クラスタにノードを追加する計画がある場合は、追加ノードに対応するのに十分な数の IP アドレスを含めます。IP アドレスはいつでも追加できます。 （注） IP アドレス範囲には、コンピューティング専用ノードは含まれません。
[IP 範囲の追加（Add IP Range）] ボタン	クリックすると、**[IP 範囲（IP Range）]** の `[開始（From）]` および `[終了（To）]` フィールドに入力した IP アドレス範囲が追加されます。

UI 要素	基本的な情報
[Set Replication Bandwidth Limit] チェック ボックス	チェックボックスをオンにして、レプリケーション帯域幅制限の設定を有効にします。複製ネットワークが着信および発信トラフィックに使用できる最大のネットワーク帯域幅を入力します。これは、10 ～ 100,000 Mbps の範囲内の値です。 レプリケーション帯域幅制限を有効にしないと、適応帯域幅制御が無効になります。レプリケーションネットワークの変動により、帯域幅関連のレプリケーションエラーが発生する可能性があるため、これは推奨されません。 レプリケーション帯域は、このローカルHXストレージクラスタからペアリング相手のリモートHXストレージクラスタにレプリケーション スナップショットをコピーする際に使用されます。 （注） • 低帯域幅 (通常、50 Mbps 以下) では、複数の VM を複製すると、データ転送レートが高くなりすぎてしまい、複製プロセスを実行することなく終了する可能性があります。この問題を克服するには、帯域幅を増やすか、VM 複製のスケジュールを調整して、VM が同じウィンドウで複製されないようにします。 • 帯域幅設定は、リンク速度に近い必要があります。ペア内のクラスタの帯域幅設定は同じである必要があります。 • 設定された帯域幅は、帯域幅が設定されているクラスタの着信および発信トラフィックにのみ適用されます。たとえば、帯域幅制限を 100 Mb に設定すると、100 Mb が着信トラフィックに対して設定され、100 Mb が発信トラフィックに設定されていることを意味します。 • 帯域幅制限の設定は、物理帯域幅を超えないようにする必要があります。 • 設定された帯域幅は、障害復旧環境の両方のサイトで同じである必要があります。 • 許容される低帯域幅は 10Mb で、10Mb でサポートされる最大遅延は 75ms です。ネットワークの損失や不安定なHXクラスタが原因でVMの初期レプリケーションが失敗した場合は、新しいレプリケーション ジョブとして次のスケジュールでVM レプリケーションが再度開始されます。この場合、VM を保護するために、スケジュールのサイズを調整する必要があります。

UI 要素	基本的な情報
[Set non-default MTU] チェックボックス	デフォルトの MTU 値は 1500 です。 レプリケーション ネットワークのカスタム MTU サイズを設定するチェック ボックスを選択します。MTU は 1024 ～ 1500 の範囲で設定できます。 （注） • ペアの HX クラスタの両方で同じ MTU 値を使用します。 • HXDP リリース 5.0（2a）以降では、クラスタの設定後に MTU 値を編集できます。古いバージョンの HXDP では、既存のレプリケーション ネットワーク構成を削除する必要があります。レプリケーション ネットワークは、正しい MTU 値で設定できます。

（注） 複製ネットワークに既存の VLAN を使用すると、複製ネットワークの設定が失敗します。Cisco UCS マネージャーの管理 vNIC テンプレートに、自分で作成したレプリケーション VLAN を追加する必要があります。

ステップ 6 [Next] をクリックします。

ステップ 7 **[Test Configuration]** タブで、複製ネットワーク構成を確認します。

ステップ 8 [構成] をクリックします。

次のタスク

- レプリケーション ペアの両方の HX ストレージ クラスタにレプリケーション ネットワークを構成してください。
- 複製ネットワークがクラスタ上に作成された後、クラスタ上の各統合ノードは、eth2 インターフェイス上の IP アドレスで構成されます。
- *'arping'* を使用して重複 IP 割り当てを確認してください。

```
For example:arping -D -b -c2 -I ethX $replicationIP` (replace ethX and $replicationIP
 with actual values).
```

重複 IP 割り当てがある場合は、複製ネットワーク割り当てを削除する必要があります。

ローカル レプリケーション ネットワークのテスト

クラスタ間のレプリケーション ネットワーク テストを実行するには、次の操作を実行します。

手順

ステップ 1 HX Connect にログインします。

a) ブラウザで、HX ストレージ クラスタ管理 IP アドレスを入力します。
https://<storage-cluster-management-ip> に移動します。
b) 管理者ユーザのユーザ名とパスワードを入力します。
c) **[Login]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、[レプリケーション（Replication）] をクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン リストから、[ローカルレプリケーションネットワークのテスト（Test Local Replication Network）] を選択します。

ステップ 4 [テストを実行（Run Test）] をクリックします。

ステップ 5 [アクティビティ（Activity）]ページで、[レプリケーションネットワークのテスト（Test Replication Network）] タスクの進行状況を表示できます。

レプリケーション ネットワークの編集

構成済みのレプリケーションがあるHXクラスタを展開するときは、レプリケーションネットワークに使用できる十分なIPアドレスがあることを確認します。レプリケーションネットワークでは、クラスタ内の各ノード 1 台に 1 つに加えてもう 1 つ専用の IP アドレスが必要です。例えば、3 ノードのクラスタでは 4 つの IP アドレスが必要です。ノードをもう 1 つクラスタに追加する場合は、少なくとも 5 つの IP アドレスが必要です。

IP アドレスを追加するためにレプリケーション ネットワークを編集するには、次のタスクを実行します。

手順

ステップ 1 管理者として HX 接続 にログインします。

ステップ 2 ナビゲーション ペインで、[レプリケーション（Replication）] を選択します。

ステップ 3 [アクション（Actions）] ドロップダウンリストから、[レプリケーションネットワークの編集（Edit Replication Network）] を選択します。

ステップ 4 [ネットワーク設定の編集（Edit Network Configuration）] ダイアログ ボックスで、使用する IP の範囲を編集して、レプリケーション トラフィックのレプリケーション帯域幅制限を設定することができます。レプリケーション ネットワーク サブネットおよびゲートウェイは参照用にのみ表示され、編集できません。

UI 要素	基本的な情報

[レプリケーション ネットワーク サブネット（Replication Network Subnet）]フィールド	レプリケーション ネットワークのサブネット。レプリケーション ネットワーク用に設定されているサブネット（ネットワーク プレフィックス表記）。この値は編集できません。
	`Format example:`
	`p.q.r.s/<length>`
	`209.165.201.0/27`

[ゲートウェイ（Gateway）]フィールド	レプリケーション ネットワーク用に設定されているゲートウェイ。この値は編集できません。

UI 要素	基本的な情報
[IP範囲（IP Range）] フィールド	レプリケーション ネットワークで使用する IP アドレス範囲を入力します。 • 必要な IP アドレスの最小数は、HX Storage クラスタのノード数プラス 1 です。 たとえば、HX ストレージ クラスタに 4 つのノードがある場合、IP 範囲は少なくとも 5 つの IP アドレスである必要があります。 • **[開始（from）]** の値には、**[終了（to）]** の値より小さい値を指定する必要があります。 たとえば、*From 10.10.10.20 To 10.10.10.30* とします。 • ただし IP アドレスはいつでも追加できます。 • クラスタにノードを追加する計画がある場合は、追加ノードをカバーするのに十分な数の IP アドレスを含めます。 （注） IPアドレス範囲には、コンピューティング専用ノードは含まれません。
[IP 範囲の追加（Add IP Range）] フィールド	クリックして、**[IP 範囲（IP Range）]** の [開始（From）] および [終了（To）] フィールドに入力した範囲の IP アドレスを追加します。
[レプリケーション帯域幅制限の設定（Set replication bandwidth limit）] チェックボックス（オプション）	レプリケーションネットワークが発信トラフィックに使用できる最大のネットワーク帯域幅を入力します。 有効な範囲：10ー10,000。デフォルトは unlimited で、使用可能なレプリケーションネットワークの合計に最大ネットワーク帯域幅を設定します。 レプリケーション帯域幅は、このローカル HX ストレージ クラスタから、ペアになっているリモート HX ストレージ クラスタ に DP スナップショットをコピーするのに使用されます。
[Set non-default MTU] チェックボックス	デフォルトの MTU 値は 1500 です。 レプリケーション ネットワークのカスタム MTU サイズを設定するチェック ボックスを選択します。MTU は 1024 ～ 1500 の範囲で設定できます。 （注） • ペアの HX クラスタの両方で同じ MTU 値を使用します。 • HXDP リリース 5.0（2a）以降では、クラスタの設定後に MTU 値を編集できます。古いバージョンの HXDP では、既存のレプリケーション ネットワーク構成を削除する必要があります。レプリケーションネットワークは、正しい MTU 値で設定できます。

ステップ 5 **[Save Changes]**をクリックします。

これでレプリケーションネットワークが更新されます。追加したレプリケーションネットワーク IP アドレスは、ストレージ クラスタに追加された場合に新しいノードで使用できるようになります。レプリケーショントラフィックは、帯域幅制限に対する変更に合わせて調整されます。

レプリケーション ペアの概要

レプリケーション クラスタ ペアの作成は、レプリケーション用 VM の設定の前提条件です。2 つの HX クラスタをペアリングした後、リモート クラスタのデータストアをローカル クラスタのデータストアにマッピングします。

HX クラスタ 1 のデータストア A を HX クラスタ 2のデータストア B にマッピングすると、データストア A に常駐し、HX クラスタ 2 のデータストア B にレプリケートされるように設定された HX クラスタ 1 上のすべての VM が有効になります。同様に、データストア B に常駐するクラスタ 2 上の任意の VM では、レプリケーションの対象として設定される場合、HX 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。

マッピングは厳密な 1対1 の関係です。ペアになっている HX クラスタ上の 1 つのデータストアは、他の HX クラスタ上の 1 つのデータストアのみマッピングできます。複数のマッピングされたデータストアが存在する可能性があることに注意してください。たとえば、HX クラスタ 1 のデータストア A は HX クラスタ 2 のデータストア B にマッピングされ、HX クラスタ 1 のデータストア C は HX クラスタ 2 のデータストア D にマッピングされます。

レプリケーション ペアの作成

レプリケーション ペアは、保護ネットワークの半分を 2 つ定義します。ログインしている HX クラスタはローカルクラスタで、ペアの最初の片方です。このダイアログによって、ペアのもう片方であり、リモート クラスタである、もう 1 つの HX クラスタを識別します。複製ペアが設定され、少なくともデータストアの 1 つのペアがマップされたら、仮想マシンを保護できるようになります。[Virtual Machines] タブを参照してください。以下は、レプリケーション ペアを作成するための前提条件と手順です。

（注） HX クラスタをペアリングするときに、クラスタ ステータスまたはログで考えられる解決策を確認する というエラーが表示されたら、次のコマンドを実行してペアリングが成功したかどうかを確認します。

```
stcli dp peer list
```

ペアリングが成功しない場合は、ログで解決策を確認してください。

始める前に

- ローカル クラスタとリモート クラスタの両方でデータストアを作成します。
- リモート クラスタで暗号化されたデータストアを作成して、ローカル サイトの暗号化されたデータストアを保護します。

（注） 暗号化されたデータストア上のVMを保護できるようにするには、ペアになっている両方のデータストアのクラスタでソフトウェア暗号化を有効にする必要があります。

- レプリケーション ネットワークを構成します。

手順

ステップ 1 HX 接続 から、管理者権限を持つユーザーとしてローカルまたはリモート HX クラスタのいずれかにログインし、次のうちいずれかを実行します。

a) 始めてクラスタ ペアリングを行う場合、**[Replication (レプリケーション)]** > **[Pair Cluster (クラスタのペアリング)]** を選択します。

b) **[Replication (レプリケーション)]** > **[Create Replication Pair (レプリケーション ペアの作成)]** を選択します。

[Create Replication Pair (複製ペアの作成)] オプションは、すべての VM の保護を解除し、すべての依存関係を削除した後に、既存の複製ペアを削除するときにのみ有効です。

ステップ 2 レプリケーション ペアの [Name] を入力し、[Next] をクリックします。

2つの HX ストレージ クラスタ間のレプリケーション ペアリングの名前を入力します。この名前は、ローカル クラスタとリモート クラスタの両方に設定されます。この名前は変更できません。

ステップ 3 **[リモート接続（Remote Connection）]** の ID を入力し、**[ペア（Pair）]** をクリックします。

UI 要素	基本的な情報
[管理 IP または FQDN（Management IP or FQDN）] フィールド	リモートの管理ネットワークの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。たとえば、*10.10.10.10* とします。
[ユーザ名（User Name）] および **[パスワード（Password）]** フィールド	リモート HX クラスタの vCenter シングル サインオンまたはクラスタ固有の管理者クレデンシャルを入力します。

HX データ プラットフォーム はリモート HX クラスタを確認し、レプリケーション ペア名を割り当てます。

クラスタ ペアのテスト ジョブが成功したら、次の手順に進むことができます。[アクティビティ（Activity）] ページで、クラスタ ペアのテスト ジョブの進行状況を表示できます。

（注） 保護される仮想マシンは、レプリケーション ペアのデータストアのいずれか 1 つに存在している必要があります。

ステップ 4 [Next] をクリックします。

[Create New Replication Pair (新規複製ペアの作成)] ダイアログ ボックスが表示されます。

ステップ 5 HX データ プラットフォーム 障害復旧機能を使用して VM を保護するには、**[Native Protection (ネイティブ保護)]** をクリックし、次を行います。

a) **[Local Datastore (ローカル データストア)]** 列には、ローカル HX ストレージ クラスタに設定されているデータストアのリストが表示されます。1 つのローカル データストアを 1 つのリモート データストアにマップします。

b) **[Remote datastore (リモート データストア)]** プルダウン メニューから、ローカル データストアとペアリングする必要があるデータストアを選択します。

c) **[Map Datastore (データストアのマッピング)]** をクリックします。

[**キャンセル (cancel)]**をクリックしてデータストアマッピングをキャンセルすることを選択した場合は、[レプリケーション (Replication)] ダッシュボードで [**データストア (datastore**)] にマッピングされている**マップデータストア**を使用して、データストアを後でマッピング

ローカル データストアの選択を変更するには:

1. **[Remote Datastore (リモート データストア)]** プルダウン メニューから、**[Do not map this datastore (このデータストアにマップしない)]** を選択して、現在のローカル データストアからマッピングを削除します。
2. **[Remote datastore (リモート データストア)]** プルダウン メニューから、ローカル データストアとペアリングするデータストアを選択します。

（注）
- 選択したデータストア上に、保護する仮想マシンが存在している必要があります。レプリケーション ペア用に構成されたデータストアから仮想マシンを移動すると、その仮想マシンの保護も解除されます。
- ペアリングされた別のデータストアへの仮想マシンの移動は、サポートされています。VM がペアリングされていないデータストアに移動されると、レプリケーション操作が失敗します。

（注） ローカルデータストアがリモートデータストアにマップされると、対応するローカルデータストアが **[Other DRO Protection (その他の DRO 保護)]** に表示されません。

ステップ 6 Disaster recovery orchestrator (DRO) で SRM を使用して VM を保護するには、**[Other DRO Protection (その他の DRO 保護)]** をクリックし、次の手順を実行します。

a) **[Local Datastore (ローカル データストア)]** 列には、ローカル HX クラスタに設定されているペアリングされていない設定済みのデータストアのリストが表示されます。1 つのローカル データストアを 1 つのリモート データストアにマップします。

b) **[Remote datastore (リモート データストア)]** プルダウン メニューから、ローカル データストアとペアリングする必要があるデータストアを選択します。
c) **[Direction (方向)]** プルダウン メニューから、マップされたデータストアの VM 移動の方向として **[Incoming (着信)]** または **[Outgoing (発信)]** を選択します。
d) **[Protection Schedule (保護スケジュール)]** プルダウン メニューから、データストアですべての VM を保護するスケジュールを選択します。
e) **[Map Datastore (データストアのマッピング)]** をクリックします。

[**キャンセル (cancel)**]をクリックしてデータストアマッピングをキャンセルすることを選択した場合は、[レプリケーション (Replication)] ダッシュボードで [**データストア (datastore)**] にマッピングされている**マップデータストア**を使用して、データストアを後でマッピング

（注） 新しい VM が保護データストアに追加されると、新しく追加された VM も Cisco HyperFlex によって保護されます。

（注） **[Other DRO Protection (その他の DRO 保護)]** の下で編集された複製ペアは、SRM に表示されます。

次のタスク

仮想マシンの保護ステータスを確認するには、次のいずれかを実行します。

- **[Virtual Machines (仮想マシン)]**をHX 接続からクリックします。これにより、保護ステータスとともにローカル クラスタ上の仮想マシンのリストが表示されます。VM が SRM によって保護されている場合、ステータスは **[Protected (by other DRO) (保護済み (その他の DRO))]** として表示されます。

（注） **[Virtual Machine (仮想マシン)]** ページでは、SRM によって保護された VM のステータスが、最初の自動保護サイクルが完了するまで**非保護**として表示されます。その後、これらの VM を手動で保護することは推奨されません。

- **[Replication (複製)]** をHX 接続からクリックします。
- **[Local VMs (ローカル VM)]** タブの **[Protected Group (保護グループ)]** をクリックして、保護グループ内で保護されている VM を表示します。**[Local VMs (ローカル VM)]** の **[Other DRO (その他の DRO)]** をクリックして、SRM によって保護されている VM を表示します。
- **[Replication (複製)]** をHX 接続からクリックします。**[Replication Activity (複製アクティビティ)]** をクリックして、保護された VM の複製アクティビティのステータスを表示します。VM が SRM によって保護されている場合、ステータスは **[Protected (by other DRO) (保護済み (その他の DRO))]** として表示されます。

リモート レプリケーション ネットワークのテスト

リモート レプリケーション ネットワークのクラスタ間でペアリングをテストするには、次の操作を実行します。

手順

ステップ 1 HX Connect にログインします。

a) ブラウザで、HX ストレージ クラスタ管理 IP アドレスを入力します。
https://<storage-cluster-management-ip> に移動します。
b) 管理者ユーザのユーザ名とパスワードを入力します。
c) **[Login]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、[レプリケーション（Replication）] をクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン リストから、[リモートレプリケーションネットワークのテスト（Test Remote Replication Network）] を選択します。

フィールド	説明
MTUテスト値（MTU Test Value）	デフォルトの MTU 値は 1500 です。MTU は 1024 ～ 1500 の範囲で設定できます。 （注） • HXDP バージョン 5.0（2a）以降では、クラスタの設定後に MTU 値を編集できます。古いバージョンの HXDP では、既存のレプリケーション ネットワーク構成を削除する必要があります。レプリケーション ネットワークは、正しい MTU 値で設定できます。

ステップ 4 [テストを実行（Run Test）] をクリックします。

ステップ 5 [アクティビティ（Activity）] ページで、[レプリケーションペアネットワークのチェック（Replication Pair Network Check）] タスクの進行状況を表示できます。

マップされたデータストア レプリケーション ペアの編集

レプリケーションペアを編集すると、レプリケーションペアのデータストアが変更されます。

（注） 同じ暗号化プロパティをもつデータストアをマッピングできます。

手順

ステップ 1 管理者として HX 接続 にログインします。

ステップ 2 **[Replication (複製)]** > **[Replication Pairs (複製ペア)]** を選択します。

ステップ 3 編集する必要がある複製ペアを選択し、**[Edit (編集)]** をクリックします。

[Edit Replication Pair (複製ペアの編集)] ダイアログ ボックスが表示されます。

ステップ 4 HX データ プラットフォーム 障害復旧機能を使用して VM を保護するには、**[Native Protection (ネイティブ保護)]** をクリックし、次を行います。

a) **[Local Datastore (ローカル データストア)]** 列には、ローカル HX ストレージ クラスタ に設定されているデータストアのリストが表示されます。1 つのローカル データストアを 1 つのリモート データストアにマップします。

b) **[Remote datastore (リモート データストア)]** プルダウン メニューから、ローカル データストアとペアリングする必要があるデータストアを選択します。

c) **[Map Datastore (データストアのマッピング)]** をクリックします。

ローカル データストアの選択を変更するには:

1. **[Remote Datastore (リモート データストア)]** プルダウン メニューから、**[Do not map this datastore (このデータストアにマップしない)]** を選択して、現在のローカル データストアからマッピングを削除します。
2. **[Remote datastore (リモート データストア)]** プルダウン メニューから、ローカル データストアとペアリングするデータストアを選択します。

（注） ローカルデータストアがリモートデータストアにマップされると、対応するローカルデータストアが **[Other DRO Protection (その他の DRO 保護)]** に表示されません。

ステップ 5 Disaster recovery orchestrator (DRO) で SRM を使用して VM を保護するには、**[Other DRO Protection (その他の DRO 保護)]** をクリックし、次の手順を実行します。

a) **[Local Datastore (ローカル データストア)]** 列には、ローカル HX クラスタに設定されているペアリングされていない設定済みのデータストアのリストが表示されます。1 つのローカル データストアを 1 つのリモート データストアにマップします。

b) **[Remote datastore (リモート データストア)]** プルダウン メニューから、ローカル データストアとペアリングする必要があるデータストアを選択します。

c) **[Direction (方向)]** プルダウン メニューから、マップされたデータストアの VM 移動の方向として **[Incoming (着信)]** または **[Outgoing (発信)]** を選択します。

d) **[Protection Schedule (保護スケジュール)]** プルダウン メニューから、データストアですべての VM を保護するスケジュールを選択します。

e) **[Map Datastore (データストアのマッピング)]** をクリックします。

（注） 保護されたデータストアに追加された新しい VM も保護されます。

（注） **[Other DRO Protection (その他の DRO 保護)]** の下で編集された複製ペアは、SRM に表示されます。

次のタスク

仮想マシンの保護ステータスを確認するには、次のいずれかを実行します。

- **[Virtual Machines (仮想マシン)]**をHX 接続からクリックします。これにより、保護ステータスとともにローカル クラスタ上の仮想マシンのリストが表示されます。VM が SRM によって保護されている場合、ステータスは **[Protected (by other DRO) (保護済み (その他の DRO))]** として表示されます。

（注） **[Virtual Machine (仮想マシン)]** ページでは、SRM によって保護された VM のステータスが、最初の自動保護サイクルが完了するまで**非保護**として表示されます。その後、これらの VM を手動で保護することは推奨されません。

- **[Replication (複製)]** をHX 接続からクリックします。
- **[Local VMs (ローカル VM)]** タブの **[Protected Group (保護グループ)]** をクリックして、保護グループ内で保護されている VM を表示します。**[Local VMs (ローカル VM)]** の **[Other DRO (その他の DRO)]** をクリックして、SRM によって保護されている VM を表示します。
- **[Replication (複製)]** をHX 接続からクリックします。**[Replication Activity (複製アクティビティ)]** をクリックして、保護された VM の複製アクティビティのステータスを表示します。VM が SRM によって保護されている場合、ステータスは **[Protected (by other DRO) (保護済み (その他の DRO))]** として表示されます。

ピア クラスタの削除

何らかの理由でペアリング関係を削除するための推奨される方法は、HxConnect を使用することです。**stcli dp peer delete** コマンドを使用してクラスタのペアリングを解除する必要がある場合。**stcli dp peer delete** コマンドは 2 クラスタ操作であり、両方のクラスタからペアリングを削除します。

クラスタ A と B がペアリングされていて、クラスタ B が永続的にダウンしているか、長期間使用できない状況では、クラスタ A のペアリング関係を削除する必要がある場合があります。適切な解決策は、クラスタ A で **stcli dp peer forget --pair-name** を使用することです。

stcli dp peer delete を使用してピア クラスタを削除するには：

手順

ペアのいずれかのクラスタで **stcli dp peer delete** を実行して、ペアの両方のクラスタからペアリング関係が削除されていることを確認します。

成功すると、両方のクラスタをデータ保護の新しい構成に使用できるようになります。

レプリケーション ペアの削除

ローカル クラスタとリモート クラスタでレプリケーション ペアを削除します。

[レプリケーション（Replication）] > [レプリケーション ペア（Replication Pairs）] > [削除（Delete）] を選択します。

始める前に

ローカルおよびリモートの両方のHXクラスタで、レプリケーションペアから依存関係を削除します。

ローカルおよびリモートのHXストレージクラスタにログインして、次の手順を実行します。

- すべての仮想マシンの保護を解除します。仮想マシンを保護グループから削除します。
- 保護グループを削除します。保護グループにVMがない場合、保護グループの削除は必要ありません。

手順

ステップ 1 管理者として HX 接続 にログインします。

ステップ 2 レプリケーション ペア内のデータストアをマップ解除します。

a) **[レプリケーション（Replication）] > [レプリケーション ペア（Replication）] > [編集（Edit）]**を選択します。

クラスタ ペアのテスト ジョブが成功したら、次の手順に進むことができます。[アクティビティ（Activity）] ページで、クラスタ ペアのテスト ジョブの進行状況を表示できます。

b) [レプリケーションペアの編集（Edit Replication Pair）] ダイアログボックスで、[リモート データ ストア（Remote Datastore）] メニューから [このデータストアをマップしない（Do not map this datastore）] を選択します。

UI 要素	基本的な情報
[ローカル データストア（Local Datastore）] カラム	このクラスタ、ローカルHXクラスタであるこのクラスタに構成されたデータストアの一覧です。 1 つのローカルデータストアを 1 つのリモートデータストアにマップします。 （注） データストア名の横にあるロック/ロック解除アイコンは、データストアの暗号化が有効か無効かを示します。 • ロック アイコン：暗号化が有効 • ロック解除アイコン：暗号化が無効 暗号化されたローカル データストアが選択されている場合、暗号化されたリモートデータストア情報のみが表示されます。
[リモート データストア（Remote Datastore）] カラム	HX クラスタ間でデータストアをペアリングします。 **1.** ローカルデータストアの選択を変更するには、現在のローカルデータストアへのマッピングを削除します。 **[Remote Datastore (リモート データストア)]** 列のプルダウン メニューで、**[Do not map this datastore (このデータストアをマップしない)]** を選択します。 **2.** 該当する **[ローカル データストア（Local Datastore）]** 行で、**[リモート データストア（RemoteDatastore）]** プルダウン メニューからデータストアを選択します。これにより、単一の操作でリモートとローカルの両方のデータストアが選択されます。

c) すべての可能なリモートデータストアが、[このデータストアをマップしない（Do not map this datastore）] に設定されていることを確認します。

d) [Finish] をクリックします。

ステップ 3 **[レプリケーション（Replication）]** > **[レプリケーション ペア（Replication Pairs）]** > **[削除（Delete）]** を選択します。

ステップ 4 リモート クラスタの管理者の資格情報を入力し、[削除（Delete）] をクリックします。

UI 要素	基本的な情報
[ユーザ名（User Name）] フィールド	リモート HX ストレージ クラスタの管理者ユーザ名を入力します。

UI 要素	基本的な情報
[パスワード（Password）] フィールド	リモートHXストレージクラスタの管理者パスワードを入力します。

保護グループの作成

保護グループは、同じレプリケーション スケジュールと VMware ツール休止設定の VM のグループです。

保護グループは、管理ユーザーがログオンしているHXクラスタに作成されます。保護グループは、特定の保護グループのメンバーである VM を保護します。保護グループがリモート クラスタにレプリケートする仮想マシンを保護している場合、これらの保護グループはHXConnectにリストされます。

（注） 保護グループの管理は、作成されたローカル クラスタからのみ実行できます。

始める前に

- レプリケーション ネットワークおよびレプリケーション ペアが構成されていることを確認します。
- 最新の Vmware ゲスト ツール サービスをインストールするか、既存のサービスが最新であることを確認します。

手順

ステップ 1 HX Connect に管理者としてログインします。

ステップ 2 **[レプリケーション（Replication）] > [保護グループ（Protection Groups）] > [保護グループの作成（Create Protection Group）]** を選択します。

ステップ 3 ダイアログボックスのフィールドに情報を入力します。

UI 要素	基本的な情報
[保護グループ名（Protection Group Name）] フィールド	この HX クラスタの新しい保護グループの名前を入力します。 保護グループは、HX クラスタに一意です。名前はリモート クラスタで参照されますが、リモート HX クラスタでは編集できません。各 HX クラスタには複数の保護グループを作成できます。

UI 要素	基本的な情報
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	ペアになっているクラスタに仮想マシンをレプリケートする頻度を選択します。 プルダウン メニュー オプション: 5 分、15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間デフォルト値は 1 時間です。
[仮想マシンの保護をすぐに開始（Start protecting the virtual machines immediately）] オプション ボタン	この保護グループに最初の仮想マシンを追加した後、すぐに最初のレプリケーションを開始するには、このオプション ボタンを選択します。
[仮想マシンの保護の開始時間（Start protecting the virtual machines from）] オプション ボタン	最初のレプリケーション操作を開始する特定の時間を設定する場合は、このラジオ ボタンを選択します。 レプリケーションを開始する前に、次のことを確認してください。 • 少なくとも 1 つの仮想マシンが保護グループに追加されている。 • スケジュールされた開始時刻に達している。 保護の開始時間を指定するには、次の手順に従います。 1. **[仮想マシンの保護の開始時間（Start protecting the virtual machines from）]** オプション ボタンをオンにします。 2. [時刻（time）]フィールドをクリックし、時間と分を選択します。時刻を選択した後、フィールドの外をクリックします。 **[クラスタのタイムゾーン（Cluster time zone）]** と **[クラスタの現在時刻（Current time on cluster）]** を参照すると、適切なレプリケーションの開始時刻を選択するのに役立ちます。開始時間は、ローカル クラスタの時計に基づいています。次に例を示します。 クラスタの現在時刻が午後 1:56:15 である場合、「現在から 10 時間 3 分後」は、午後 11:59:00 に最初のレプリケーションが発生することを意味します。 *[現在からの時間と分（hours, minutes from now）]* は、最初のレプリケーションがいつ行われるかを示します。これは、[時刻（time）] フィールドの設定値を変更すると更新されます。
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェックボックス	静止 DP スナップショットを作成するには、このチェックボックスをオンにします。このチェックボックスをオフのままにすると、一貫性のある DP スナップショットがクラッシュします。 この設定は、VMware ツールがインストールされている仮想マシンにのみ適用されます。

ステップ 4 **[保護グループの作成（Create Protection Group）]** をクリックします。

HX データ プラットフォームで **[保護グループ（Protection Group）]** タブに新しいグループが追加されます。この保護グループは、このクラスタ上の仮想マシンを保護するために利用可能です。

ステップ 5 **[レプリケーション（Replication）]** > **[保護グループ（Protection Groups）]** の順にクリックして新しい保護グループを表示または編集します。

VM の数を 0 にする場合は、仮想マシンをこの新しい保護グループに追加し、この保護グループに設定されたレプリケーション スケジュールを適用します。

休止の概要

休止とは、物理または仮想コンピュータのディスク上のデータをバックアップに適した状態にするプロセスを指します。このプロセスには、オペレーティング システムのメモリ内キャッシュからディスクにダーティ バッファをフラッシュするなどの操作の他、アプリケーションに固有の高位レベルのタスクが含まれる場合があります。

HX データ保護（DP）スナップショットは、ゲスト ファイル システムを休止した状態で作成できます。**休止** オプションは、Cisco HyperFlex Connect、HyperFlex コマンド ライン ユーザー インターフェイス（UI）、および HX REST API を使用する場合に選択できます。**休止**オプションを使用して HX DP スナップショットを作成する場合は、ゲスト VM に VMware ツールをインストールする必要があります。VMware については、次の VMware の Web サイトにアクセスしてください。

- VMware 互換性ガイド
- VMware ツールのドキュメント
- 仮想マシン ツール、バージョン、およびステータス。
- VMware ゲスト オペレーティング システム インストール ガイド

HXDP ソフトウェア リリース 5.0(2a) 以前は、次のゲスト状態をサポートしています。

- guestToolsCurrent
- guestToolsUnmanaged

静止データ保護スナップショットが失敗すると、**DataProtectionVmError** が発生し、HX イベントと HX アラームが表示されます。

保護グループの編集

保護グループで仮想マシンのレプリケーション間隔（スケジュール）を変更します。保護グループを編集するには、次の手順を実行します。

手順

ステップ 1 管理者として HX 接続 にログインします。

ステップ 2 **[複製（Replication）] > [保護グループ（Protection Groups）] > [スケジュールの編集（Edit Schedule）]** を選択します。

ステップ 3 ダイアログ フィールドの情報を編集します。

UI 要素	基本的な情報
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	プルダウン リストを使用して、仮想マシンがペアになっているクラスタにレプリケートされる頻度を選択します。 リストの値: 5 分、15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェック ボックス	停止した DP スナップショットを作成するには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。チェックボックスをオフのままにすると、クラッシュの整合性のある DP スナップショットが取得されます。 これは、VMware ツールがインストールされている仮想マシンにのみ適用されます。

ステップ 4 **[変更を保存（Save Changes）]** をクリックして、保護グループの間隔と VMware ツールの静止設定を保存します。間隔の頻度を確認するには、[保護グループ（Protection Groups）] タブを参照してください。

保護グループの削除

始める前に

保護グループからすべての仮想マシンを削除します。

手順

ステップ 1 **[レプリケーション（Replication）] > [保護グループ（Protection Groups）] > *protection_group_name*** を選択します。

ステップ 2 **[削除（Delete）]** をクリックします。確認ポップアップで、[削除（Delete）] をクリックします。

既存の保護グループでの仮想マシンの保護

このタスクでは、既存の保護グループを使用して複数の仮想マシンを保護する方法について説明します。

既存の保護グループを使用する：1 つまたは複数の仮想マシンを選択し、既存の保護グループに追加します。スケジュールおよびVMwareの休止オプション設定は、保護グループ内のすべ

ての仮想マシンに適用されます。保護グループの設定を変更すると、保護グループのすべての仮想マシンに変更が適用されます。

始める前に

レプリケーション ネットワークおよびレプリケーション ペアが構成済みとなっています。

仮想マシンを追加する前に保護グループを作成します。

手順

ステップ 1 管理者権限で HX 接続 にログインし、**[仮想マシン（Virtual Machines）]** を選択します。

これによりローカル HX クラスタ上の仮想マシンが一覧表示されます。

ステップ 2 一覧から 1 つまたは複数の保護されていない VM を選択します。

仮想マシンの行をクリックして選択します。仮想マシンの行をクリックすると、対応する仮想マシンのチェック ボックスが選択されます。

ステップ 3 **[保護（Protect）]** をクリックします。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、**[保護グループ（Protection Group）]** ページが表示されます。

ステップ 4 **[既存の保護グループに追加（Add to an existing protection group）]** ラジオ ボタンをクリックします

UI 要素	基本的な情報
[保護パラメータの設定（Set the protection parameters）] テーブル	**[名前（Name）]** で、選択した仮想マシンを確認します。 **[プロビジョニング済みのストレージ（Storage Provisioned）]** と **[使用済みのストレージ（Storage Used）]** を使用して、リモート HX クラスタに利用可能な十分なリソースがあることを確認します。
[既存の保護グループに追加（Add to an existing protection group）] オプション ボタン	プルダウン リストから既存の保護グループを選択します。 保護グループの間隔とスケジュールの設定が、選択済みの VM に適用されます。
[新しい保護グループの作成（Create a new protection group）] オプション ボタン	このローカル クラスタの新しい保護グループの名前を入力します。 保護グループは、各クラスタに固有です。名前はリモート クラスタで参照されますが、リモート クラスタでは編集できません。各クラスタには複数の保護グループを作成できます。

ステップ 5 プルダウンリストから保護グループを選択し、**[次へ（Next）]** をクリックします

選択した保護グループに、必要なスケジュール間隔が設定されていることを確認します。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、**[サマリー（Summary）]** ページが表示されます。

ステップ 6 **[サマリー（Summary）]** ページの情報を確認し、**[保護グループに追加（Add to Protection Group）]** をクリックします。

選択した VM が保護グループに追加されます。**[レプリケーション（Replication）]** または **[仮想マシン（Virtual Machines）]** ページを表示して、1 つまたは複数の VM が保護グループに追加されていることを確認します。

新しい保護グループでの仮想マシンの保護

このタスクでは、新しい保護グループを作成することで複数の仮想マシンを保護する方法について説明します。

新しい保護グループ ー VM を選択し、新しい保護グループを作成することを選択します。保護グループの名前、スケジュール、開始時間、およびVMwareの休止オプション設定を定義します。これらの設定は、保護グループ内のすべての仮想マシンに適用されます。保護グループの設定を変更すると、保護グループのすべての仮想マシンに変更が適用されます。

始める前に

レプリケーション ネットワークおよびレプリケーション ペアが構成済みとなっています。

手順

ステップ 1 管理者権限で HX 接続 にログインし、**[仮想マシン（Virtual Machines）]** を選択します。

これによりローカル HX クラスタ上の仮想マシンが一覧表示されます。

ステップ 2 一覧から 1 つまたは複数の保護されていない VM を選択します。

仮想マシンの行をクリックして選択します。仮想マシンの行をクリックすると、対応する仮想マシンのチェックボックスが選択されます。

ステップ 3 **[保護（Protect）]** をクリックします。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、**[保護グループ（Protection Group）]** ページが表示されます。

ステップ 4 **[新しい保護グループを作成（Create a new protection group）]** ラジオ ボタンをクリックして、保護グループの名前を追加し、**[次へ（Next）]** をクリックします。

[保護スケジュール（Protection Schedule）] ウィザード ページが表示されます。

ステップ 5 必要に応じて、スケジュールと VMware 休止オプションを入力し、**[次へ（Next）]** をクリックします。

UI 要素	基本的な情報
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	ペアになっているクラスタに仮想マシンをレプリケートする頻度を選択します。デフォルト値は 1 時間ごとです。
[仮想マシンの保護をすぐに開始（Start protecting the virtual machines immediately）] オプション ボタン	この保護グループに最初の仮想マシンを追加した後、すぐに最初のレプリケーションを開始するには、このオプション ボタンを選択します。
[仮想マシンの保護の開始時間（Start protecting the virtual machines from）] オプション ボタン	最初のレプリケーションを開始する具体的な時間を設定するには、このラジオボタンを選択します。レプリケーションを開始するには、次の要件が満たされる必要があります。 • 少なくとも 1 つの仮想マシンが保護グループに追加されている。 • スケジュールされた開始時刻に達している。 保護の開始時間を指定するには、次の手順に従います。 1. **[仮想マシンの保護の開始時間（Start protecting the virtual machines from）]** オプション ボタンをオンにします。 2. [時刻（time）] フィールドをクリックし、時間と分を選択します。時刻を選択した後、フィールドの外をクリックします。 *[現在からの時間と分（hours, minutes from now）]* は、最初のレプリケーションがいつ行われるかを示します。これは、[時刻（time）] フィールドの設定値を変更すると更新されます。 **[クラスタのタイムゾーン（Cluster time zone）]** と **[クラスタの現在時刻（Current time on cluster）]** を参照すると、適切なレプリケーションの開始時刻を選択するのに役立ちます。開始時間は、ローカルクラスタの時計に基づいています。次に例を示します。 クラスタの現在時刻が午後 1:56:15 である場合、「現在から 10 時間 3 分後」は、午後 11:59:00 に最初のレプリケーションが発生することを意味します。
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェックボックス	静止 DP スナップショットを取得するには、チェックボックスをオンにします。チェックボックスをオフにすると、クラッシュ整合性のある DP スナップショットが作成されます。このチェックボックスは、デフォルトでオフになっています。 この設定は、VMware ツールがインストールされている仮想マシンにのみ適用されます。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、**[サマリー（Summary）]** ページが表示されます。

ステップ 6 **[サマリー（Summary）]** ページの情報を確認し、**[保護グループに追加（Add to Protection Group）]** をクリックします。

サマリーの内容を確認し、選択した仮想マシンに適用する設定を確定します。

- 保護グループの名前
- 保護する仮想マシンの数
- 仮想マシンの名前
- 各仮想マシンのプロビジョニング済みストレージ
- 各仮想マシンの使用（消費）済みストレージ

選択した VM が保護グループに追加されます。**[レプリケーション（Replication）]** または **[仮想マシン（Virtual Machines）]** ページを表示して、VM が保護グループに追加されていることを確認します。

個別の仮想マシンの保護

このタスクでは、仮想マシン（VM）を保護する方法について説明します。

- **[Independently]**：1 つの VM を選択し、保護を設定します。特定の VM のレプリケーション スケジュールおよび VMware ツールの休止オプションを設定します。

  レプリケーション設定の変更は、個別に保護された VM にのみ影響を与えます。VM は保護グループのメンバーではありません。

- **既存の保護グループ** ー 1 つ以上の VM を選択し、それらを既存の保護グループに追加します。スケジュールおよびVMwareの休止オプション設定は、保護グループ内のすべての VM に適用されます。保護グループの設定を変更する場合、保護グループのすべての VM に変更が適用されます。

始める前に

レプリケーション ネットワークおよびレプリケーション ペアを構成します。

手順

ステップ 1 管理者権限で HX 接続 にログインし、**[仮想マシン（Virtual Machines）]** を選択します。

ステップ 2 一覧から 1 つの保護されていない仮想マシンを選択します。仮想マシンの行をクリックして選択します。

仮想マシンの行をクリックして選択します。仮想マシンの行をクリックすると、対応する仮想マシンのチェック ボックスが選択されます。

ステップ 3 **[保護（Protect）]** をクリックします。

[仮想マシンの保護（Protect Virtual Machine）] ダイアログボックスが表示されます。

ステップ 4 必要に応じてフィールドに入力します。

UI 要素	基本的な情報
[既存の保護グループに追加（Add to an existing protection group）] オプション ボタン	プルダウン リストから既存の保護グループを選択します。 その保護グループの間隔とスケジュールの設定が、この仮想マシンに適用されます。 追加の構成は必要ありません。**[仮想マシンの保護（Protection Virtual Machine）]** をクリックします。
[この仮想マシンを個別に保護（Protect this virtual machine independently）] オプション ボタン	この VM の保護を定義するため、間隔、スケジュール オプション、および VMware ツール オプションを有効にします。
[この仮想マシンを次の間隔で保護（Protect this virtual machine every）] フィールド	プルダウン リストから、ペアになっているクラスタに仮想マシンをレプリケートする頻度を選択します。 リストの値: 5 分、15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間
[仮想マシンの保護をすぐに開始（Start protecting the virtual machines immediately）] オプション ボタン	この保護グループに最初の仮想マシンを追加した後、すぐに最初のレプリケーションを開始するには、このオプション ボタンを選択します。

UI 要素	基本的な情報
[仮想マシンの保護の開始時間（Start protecting the virtual machines from）] オプション ボタン	最初のレプリケーションを開始する具体的な時間を設定するには、このラジオボタンを選択します。レプリケーションを開始するには、次の要件が満たされる必要があります。 • 少なくとも 1 つの VM が保護グループに追加されます。 • スケジュールされた開始時刻に達している。 保護の開始時間を指定するには、次の手順に従います。 1. **[仮想マシンの保護の開始時間（Start protecting the virtual machines from）]** オプション ボタンをオンにします。 2. [時刻（time）]フィールドをクリックし、時間と分を選択します。時刻を選択した後、フィールドの外をクリックします。 *[現在からの時間と分（hours, minutes from now）]* は、最初のレプリケーションがいつ行われるかを示します。これは、[時刻（time）]フィールドの設定値を変更すると更新されます。 **[クラスタのタイムゾーン（Cluster time zone）]** と **[クラスタの現在時刻（Current time on cluster）]** を参照すると、適切なレプリケーションの開始時刻を選択するのに役立ちます。開始時間は、ローカルクラスタの時計に基づいています。次に例を示します。 クラスタの現在時刻が午後 1:56:15 である場合、「現在から 10 時間 3 分後」は、午後 11:59:00 に最初のレプリケーションが発生することを意味します。
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェックボックス	静止 DP スナップショットを取得するには、チェックボックスをオンにします。チェックボックスをオフにすると、クラッシュ整合性のある DP スナップショットが作成されます。このチェックボックスは、デフォルトでオフになっています。 この設定は、VMware ツールがインストールされている仮想マシンにのみ適用されます。

ステップ 5 **[仮想マシンの保護（Protect Virtual Machine）]** をクリックします。

仮想マシンの状態は、**[仮想マシン（Virtual Machine）]** ページと **[レプリケーション（Replication）]** ページで更新されます。[レプリケーション（Replication）] ページで、個々の VM として保護されている VM の保護グループが表示されないことに注意してください。

この VM のレプリケーションが有効になりました。

仮想マシンの保護の解除

（注） クラスタのアクティビティのレプリケーションを一時停止するためには、VMの保護を解除する必要はありません。レプリケーションの一時停止 （296 ページ）を参照してください。

手順

ステップ 1 HX 接続 に管理者としてログインします。

ステップ 2 [仮想マシン（Virtual Machines）] を選択します。

ステップ 3 一覧から保護されている仮想マシンを選択します。仮想マシンの行をクリックします。

VM は一度に 1 つの VM で保護解除できます。

ステップ 4 **[保護を解除（Unprotect）]** をクリックし、クリックして確認します。

仮想マシンの状態が、**[保護（protected）]** から **[非保護（unprotected）]** に変わります。

ディザスタ リカバリの概要

ディザスタ リカバリは、ソース サイトが到達不能で、VM および保護グループをターゲット クラスタにフェールオーバーする必要があるときに実行されます。リカバリのプロセスは、ターゲットクラスタ上のVMを回復します。仮想マシンのリカバリでは、リカバリ（ターゲット）クラスタから最新のレプリケーション スナップショットが復元されます。

暗号化されたデータストア上のVMを保護できるようにするには、ペアになっている両方のデータストアのクラスタでソフトウェア暗号化を有効にする必要があります。

VMリカバリのテストーレプリケーションを破損することがなく、リカバリをテストする機能を提供します。ターゲットのVMワークロードを表示し、VMのコンテンツを確認できます。

仮想マシンのリカバリーターゲット (リカバリ) クラスタから最新のレプリケーション スナップショットが復元されます。リカバリを開始すると、すべてのスケジュール済みのレプリケーションが停止されます。

計画的移行ー計画的移行を実行すると、レプリケーション スケジュールが一時停止され、DP スナップショットが作成および複製され、ターゲットで回復されます。ソースからターゲットに所有権をスイッチし、新しいソースになったターゲットでレプリケーションを再開します。

計画されていない移行および再保護—ターゲットのVMを復元し、ソースからターゲットに所有権をスイッチし、新しいソースになったターゲットでレプリケーションを再開します。

障害後に VM を保護する —障害が発生した場合、ソース サイトをいっぺんに失う可能性があります。リカバリの実行後、新しいクラスタに回復した VM を保護できます。

リカバリ設定

リカバリ設定では、リカバリ サイト間でのリソースのグローバル リカバリ パラメータとマッピングを定義できます。リカバリ中に使用されるフォルダ、ネットワーク、またはリソースプールのパラメータを設定し、リカバリおよび移行操作を実行できます。グローバル リカバリ設定が設定されていない場合は、リカバリ時に個々のVMを明示的にマッピングする必要があります。

手順

ステップ 1 管理者として HX 接続 にログインし、次のいずれかを実行します。

a) リカバリ設定を初めて設定する場合は、**[Replication (レプリケーション)]** > **[Configure (設定)]** を選択します。

b) **[Replication (レプリケーション)]** を選択し、**[Recovery Settings (リカバリ設定)]** の横にある **[Actions (アクション)]** をクリックします。**[Actions (アクション)]** ドロップダウン リストから、**[Edit (編集)]** を選択します。

ステップ 2 **[Recovery Settings (リカバリ設定)]** ダイアログ ボックスで、次のフィールドに値を入力します。

フィールド	説明
[Virtual Machine Power State (仮想マシンの電力状態)] オプション ボタン	デフォルトでは、このオプションは **[Off (オフ)]** になっています。選択したオプションに従って、回復したVMの電源がオンになります。
[Test Virtual Machine Name Prefix (仮想マシン名のプレフィックス テスト)]フィールド	テスト リカバリ後に仮想マシンに追加するプレフィックスを入力します。プレフィックスは、リソースのタイプとコンテキストを識別するのに役に立ちます。
[Notification Setting (通知設定)] オプション ボタン	リカバリ、テスト リカバリ、または移行時に設定の概要を確認するプロンプトを表示するには、**[通常モード（Normal Mode）]** を選択します。確認プロンプトを表示しないようにするには、**[サイレント モード（Silent Mode）]** を選択します。サイレント モードを選択すると、サイレント モードのデフォルトの動作について説明する確認ウィンドウが表示されます。サイレントモードのデフォルトの動作に同意する場合は、**[OK]** をクリックします。

フィールド	説明
[Resource Pool (リソース プール)] 領域	リカバリ、テスト リカバリ、移行操作のために、保護されたサイトのリソースをリモート サイトのリソースにマッピングします。 テスト リカバリ設定のリカバリ設定のリソース マッピングを使用するには、**[Same As Recovery configuration (リカバリ設定と同じ)]** チェックボックスをオンにします。 **[Add Rule (ルールの追加)]** をクリックして、もう 1 つのリソース プール マッピングを追加します。ルールを削除するには、アイコンをクリックします。ルールを編集するには、ルールを削除し、更新されたルールを新しいルールとして追加します。
[Folder (フォルダ)] 領域	リカバリ、テスト リカバリ、移行操作のために、保護されたサイトのフォルダをリモート サイトのフォルダにマッピングします。 テスト リカバリ設定のリカバリ設定のフォルダ マッピングを使用するには、**[Same As Recovery configuration (リカバリ設定と同じ)]** チェックボックスをオンにします。 **[Add Rule (ルールの追加)]** をクリックして、もう 1 つのフォルダ プール マッピングを追加します。ルールを削除するには、アイコンをクリックします。ルールを編集するには、ルールを削除し、更新されたルールを新しいルールとして追加します。
[Network (ネットワーク)] 領域	リカバリ、テスト リカバリ、移行操作のために、保護されたサイトのネットワークをリモートサイトのネットワークにマッピングします。 テスト リカバリ設定のリカバリ設定のネットワーク マッピングを使用するには、**[Same As Recovery configuration (リカバリ設定と同じ)]** チェックボックスをオンにします。 **[Add Rule (ルールの追加)]** をクリックして、もう 1 つのネットワーク プール マッピングを追加します。ルールを削除するには、アイコンをクリックします。ルールを編集するには、ルールを削除し、更新されたルールを新しいルールとして追加します。

ステップ 3 **[Save（保存）]** をクリックします。
リカバリ設定が正常に保存されると、**[Replication (レプリケーション)]** ページの **[recovery settings (リカバリ設定)]** フィールドに、通知設定モードとともに次のいずれかのステータスが表示されます。

- **部分的に設定**: このステータスは、いずれかのリソースに対してリカバリ マッピングを設定していない場合、または設定されているマッピングのいずれかが無効な場合に表示されます。
- [**設定済み**: このステータスは、すべてのリカバリ設定が有効になっている場合に表示されます。

（注） **[RECOVERY SETTINGS (復元設定)]** フィールドには、最後に検証された結果が表示されます。リカバリのためにルールが作成されると、定期的な自動検証は行われません。ただし、検証ジョブを実行して、リカバリ設定に存在するルールの有効性を確認することができます。

[Activity (アクティビティ)] ページの検証ジョブの概要で、**[Recovery Settings (リカバリ設定)]** ページの検証結果を確認するようにユーザーに通知します。

リカバリ設定を構成した後、**[Actions (アクション)]** ドロップダウン リストから **[Validate Recovery Settings (リカバリ設定の検証)** を選択して、リカバリ設定を確認できます。リカバリ設定検証メッセージが正常に開始されたことが表示されます。**[RECOVERY SETTINGS (リカバリ設定)]** フィールドには、最後の検証のタイムスタンプが表示されます。検証の進行状況をモニタするには、**[Activity (アクティビティ)]** タブをクリックします。通常の通知設定モードでは、仮想マシンのリカバリ、リカバリ テスト、移行中に、設定されたリカバリ設定が表示されます。

[Modify recovery configuration for current operation (現在の動作のリカバリ設定を変更する)] チェック ボックスをオンにすることで、リカバリ設定を表示し、必要に応じて編集できます。ただし、リカバリ設定の変更は現在の操作にのみ適用され、変更はグローバル リカバリ設定では更新されません。

ディザスタ リカバリ操作の互換性

レプリケーション ネットワークとペアリングの要件セクションで前述したように、異なる HX データ プラットフォーム バージョンの使用は、HX データ プラットフォームのアップグレード中にのみサポートされます。ペアになっている両方のクラスターがアップグレードされるまでの期間中、レプリケーション構成パラメーターの変更はサポートされません。テスト リカバリ、リカバリ、再保護、および計画された移行操作は、ペアになっているクラスタの両方がアップグレードされるまでの間、機能することが期待されます。場合によっては、再保護および計画された移行操作を完了するために、コマンド ライン ユーザー インターフェイスの使用が必要になることがあります。

仮想マシンのリカバリのテスト

VM リカバリのテストにより、レプリケーションを破損することなく、リカバリをテストできます。ターゲットの VM ワークロードを表示し、VM のコンテンツを確認できます。

（注）
- リカバリ テストを行っても実行中のクラスタが中断することはありません。テストの目的は、実際の障害が発生した場合に VM が回復可能であるか確認することです。
- HX Connect ユーザー インターフェイスを使用し VM をテストして、以前に送信されたタスクが完了するのを待たずに、シーケンス内で最大 10 つの再保護タスクを実行できます。

始める前に

VM リカバリ プロセスのテストを開始する前に、次のことを確認します。

- ターゲット クラスタは稼働しており状況は良好です。
- 保護された VM は、ターゲット クラスタへの最近のレプリケーションを完了しました。レプリケートされた VM は、ターゲット クラスタで DP スナップショットとして保存されています。

重要 その時点で作成可能なのは、回復した VM のテストのコピー 1 つのみです。別のテストで回復した VM が必要な場合、以前に作成された VM を削除してください。

テスト VM リカバリ プロセスに対して、次の手順を実行します。

手順

ステップ 1 管理者として、ターゲット クラスタの HX Connect にログインします。

ステップ 2 **[レプリケーション（Replication）]** > **[リモート VM（Remote VMs）] タブ** > ***[protected_vm]*** の順に移動します。

ステップ 3 リカバリ プロセスをテストするには、**[リカバリのテスト（Test Recovery）]** ボタンをクリックします。

（注） リカバリ設定を構成すると、次のフィールドが自動的に入力されます。

UI 要素	基本的な情報
[リソース プール] ドロップダウン リスト	保管するテスト VM のロケーションを選択します。
[フォルダ（Folders）] ドロップダウン リスト	保管するテスト VM のロケーションを選択します。例： • 検出された仮想マシン • HX テスト リカバリ
[電源オン/オフ（Power On/Off）] ラジオ ボタン	デフォルトでは、**[電源オン（Power ON）]** オプションが選択されています。回復した VM は、選択したオプションに応じて、作成した後に電源がオンになるかオフのままになります。
[VM名（VM Name）] フィールド	作成されたテスト VM に新しい名前を入力します。

UI 要素	基本的な情報
[テスト ネットワーク（Test Networks）] ラジオ ボタン	レプリケーション スナップショットからデータを転送するために使用する HX ストレージ クラスタ ネットワークを選択します。 ネットワークのオプションの例。 • ストレージ コントローラのデータ ネットワーク • ストレージ コントローラの管理ネットワーク • ストレージ コントローラ レプリケーション ネットワーク • VM ネットワーク
[ネットワークのマップ（Map Networks）] ラジオ ボタン	ソースとターゲット クラスタ ネットワークの間にマップを作成する場合に選択します。 • ソース ネットワーク：VM が接続されているソース側のネットワーク名。 • ターゲット ネットワーク：ドロップダウン リストから、VM を接続する必要があるターゲット ネットワークを選択します。

ステップ 4 **[VM を回復する（Recover VM）]** をクリックします。

ステップ 5 保護グループの一部である VM の場合、グループ内の各 VM でテスト リカバリを実行します。

ステップ 6 回復した VM の内容を確認します。

仮想マシンのリカバリ

VM のリカバリでは、ターゲット (リカバリ) クラスタから最新のレプリケーション スナップショットが復元されます。

注目

- リカバリ中に使用されるフォルダ、ネットワーク、またはリソース プールのパラメータを設定し、リカバリおよび移行操作を実行できます。グローバル リカバリ設定が設定されていない場合は、リカバリ時に個々の VM を明示的にマッピングする必要があります。
- VM のリカバリは異なる vSphere バージョン間ではサポートされていません。ターゲットが以前のバージョンの vSphere 環境で、プライマリの保護される VM のハードウェア バージョンをサポートしていない場合、VM のテスト リカバリやリカバリは失敗する可能性があります。保護される各 VM にテスト リカバリを実行して、ターゲット サイトでサポートを確認することをお勧めします。

  ターゲット環境をアップグレードして、保護される VM のリカバリを可能にします。
- リカバリプロセスのキャンセル（ロールバック）はサポートされていません。リカバリプロセスをキャンセルしようとすると、保護されていない「リカバリ準備完了」状態のすべてのVMが変更されます。
- VM でリカバリを実行する場合、VM をリカバリする際に明示的なネットワーク マッピングを指定して、リカバリされる VM への意図しないネットワーク接続を回避できます。

  次の場合、ネットワーク マッピングの指定をスキップできます。
  - ソース VM が vSphere 標準スイッチを使用し、回復側のすべての ESXi ホストに同じ名前の標準スイッチ ネットワークがある場合。
  - ソース VM が vSphere 分散スイッチ (vDS) ポート グループを使用し、回復サイトに同じ名前の vDS ポート グループがある場合。
- ネットワーク マッピングを指定する場合は、VM ネットワークの名前とタイプの両方がソースとターゲットの間で一致することを確認してください。
- 個別に保護された、または、別の保護グループに属している仮想マシンで回復を実行する場合、クラスタでの同時回復操作の最大数は 20 です。

始める前に

次の状態を確認してください。

- ターゲット クラスタは稼働しており状況は良好です。
- 保護された VM は、ターゲット クラスタへの最近のレプリケーションを完了しました。レプリケートされた VM は、ターゲット クラスタで DP スナップショットとして保存されています。

ターゲット クラスタで、ディザスタ リカバリを行うには、次を実行します。

手順

ステップ 1 HX Connect に管理者としてログインします。

ステップ 2 **[レプリケーション（Replication）]** > > **[リモート VM（Remote VMs）] タブ** > > ***[protected_vm]*** を選択し、**[回復（Recover）]** をクリックします。

ステップ 3 VM を回復し、ローカル クラスタに新しい VM を構築するには、**[VM の回復 (Recover VM)]** ボタンをクリックします。

（注） リカバリ設定を構成すると、次のフィールドが自動的に入力されます。

UI 要素	基本的な情報
[リソース プール] ドロップダウン リスト	新しい VM を格納する場所を選択します。
[フォルダ（Folders）] ドロップダウン リスト	新しい VM を格納する場所を選択します。
[電源オン/オフ（Power On/Off）] ラジオ ボタン	デフォルトでは、[電源オン（Power ON）] オプションが選択されています。回復した VM は、選択したオプションに応じて、作成した後に電源がオンになるかオフのままになります。
ネットワークのマッピング	ソースとターゲット クラスタ ネットワークの間にマップを作成する場合に選択します。 • ソース ネットワーク：VM が接続されているソース側のネットワーク名。 • ターゲット ネットワーク：ドロップダウン リストから、VM を接続する必要があるターゲット ネットワークを選択します。 ネットワークのオプションの例。 • ストレージ コントローラのデータ ネットワーク • ストレージ コントローラの管理ネットワーク • ストレージ コントローラ レプリケーション ネットワーク • VM ネットワーク

ステップ 4 **[VM を回復する（Recover VM）]** をクリックします。

ステップ 5 回復が完了するまで待ちます。ターゲット vCenter で回復した VM を表示します。

保護グループ内の仮想マシンのリカバリ

手順

ステップ 1 [protected-vm] を選択して、[回復（Recover）] をクリックします。

すべての VM は保護グループから移動され、選択した VM は回復されます。回復された VM では保護ステータスが [回復済み（Recovered）] と表示され、残り（保護グループ）の VM では保護ステータスが [回復中（Recovering）] と表示されます。保護グループは [回復済み（Recovered）] 状態になり、再利用できません。プライマリ サイトからこれを削除できます。

（注） グループ内の VM で **[回復 (Recover)]** をクリックすると、**[回復済み (Recovered)]** 状態 (実際に回復が行われた) になります。一方、スタンドアロン リスト内の残りの VM は、**[回復準備完了 (Ready for Recovery)]** 状態になっています。

回復された VM は **[スタンドアロンの保護VM (Standalone Protected VMs)]** サブペインに表示されます。

ステップ 2 保護グループに含まれていた残りの仮想マシンを [スタンドアロンの保護VM（Standalone Protected VMs）] サブペインから回復します。詳細については、仮想マシンのリカバリ （285ページ）を参照してください。

計画された移行

計画された移行の実行によりレプリケーション スケジュールを一時停止し、最新のコピーをレプリケートして、ターゲット上で回復し、所有権をソースからターゲットに切り替えて、新しいソースのターゲットでレプリケーションを再開します。

計画移行を実行するには、次の手順を実行します。

注目 このプロセスは戻すことができません。

手順

ステップ 1 ターゲット クラスタの HX Connect にログインします。ターゲット クラスタは、レプリケーション DP スナップショットのコピー先となっていたクラスタです。

ステップ 2 ターゲット クラスタで、**[レプリケーション（Replication）] > [リモートVM（Remote VMs）] タブ > *[protected_vm]*** を選択します。

ステップ 3 [移行（Migrate）] をクリックします。

（注） ここに記載されているすべてのフィールドはオプションです。

UI 要素	基本的な情報
[リソース プール] ドロップダウン リスト	新しい VM を格納する場所を選択します。
[フォルダ（Folders）] ドロップダウン リスト	新しい VM を格納する場所を選択します。
[電源オン/オフ（Power On/Off）] ラジオ ボタン	デフォルトでは、[電源オン（Power ON）] オプションが選択されています。回復した VM は、選択したオプションに応じて、作成した後に電源がオンになるかオフのままになります。
ネットワークのマッピング	ソースとターゲット クラスタ ネットワークの間にマップを作成する場合に選択します。 • ソース ネットワーク：VM が接続されているソース側のネットワーク名。 • ターゲット ネットワーク：ドロップダウン リストから、VM を接続する必要があるターゲット ネットワークを選択します。 ネットワークのオプションの例。 • ストレージ コントローラのデータ ネットワーク • ストレージ コントローラの管理ネットワーク • ストレージ コントローラ レプリケーション ネットワーク • VM ネットワーク

ステップ 4 [アクティビティ（Activity）] ページで進行状況をモニターします。

低帯域幅および一時的なパケット損失：VM移行操作が「THRIFT_EAGAIN（タイムアウト）」を含むエラーメッセージで失敗する場合は、VM移行を再試行します。タイムアウト エラーは、帯域幅の飽和または基礎となるネットワーク パケット損失が原因の一時的なネットワーク輻輳が原因です。

単一 vCenter 展開の計画移行

単一の vCenter 展開の計画移行を実行するには、次の手順を実行します。

注目 このプロセスは戻すことができません。

手順

ステップ 1 Web CLI を使用して、以下のコマンドを実行しソースでのフェールオーバーに備えます。

```
# stcli dp vm prepareFailover --vmid <VMID>
```

（注） `stcli dp vm list --brief` コマンドを使用して、保護された VM の VMID を判別できます。

タスク ID が返されます。

ステップ 2 プライマリ サイトの vSphere Web クライアント ナビゲータにログインし、プライマリ サイトから VM を削除して VM を登録解除します。

仮想マシンを右クリックして、**[すべてのvCenterアクション（All vCenter Actions）]** > **[インベントリから削除（Remove from Inventory）]** を選択します。

ステップ 3 セカンダリ サイトの HX Connect にログインします。**[レプリケーション（Replication）]** > **[リモートVM（Remote VMs）] タブ** > ***[protected_vm]*** を選択します。**[移行（Migrate）]** をクリックします。

ステップ 4 移行タスクが正常に完了したら、セカンダリ サイトの vSphere Web クライアントにログインして、VM を手動で登録します。

a) vSphere Web クライアント ナビゲータにログインします。**[構成（Configuration）]** > **[ストレージ（Storage）]** を選択します。

b) 適切なデータストアを右クリックして、**[データストアの参照（Browse Datastore）]** をクリックします。

virtualmachine name.vmx ファイルに移動し、ファイル上で右クリックして、**[インベントリに追加（Add to Inventory）]** をクリックします。ウィザードに従って、VM を手動で登録します。

低帯域幅および一時的なパケット損失：VM移行操作が「THRIFT_EAGAIN（タイムアウト）」を含むエラーメッセージで失敗する場合は、VM移行を再試行します。タイムアウト エラーは、帯域幅の飽和または基礎となるネットワーク パケット損失が原因の一時的なネットワーク輻輳が原因です。

保護グループの仮想マシンの移行

HX Connect ユーザー インターフェイスを使用し VM を移行して、以前に送信されたタスクが完了するのを待たずに、シーケンス内で最大 4 つの再保護タスクを実行できます。

手順

ステップ 1 [protected-vm] を選択して、[移行（Migrate）] をクリックします。

これですべての VM が保護グループから移動し、[スタンドアロンの保護VM（Standalone Protected VMs）] サブペインに表示されます。回復するのは選択した VM のみです。

ステップ 2 保護グループに含まれていた残りの仮想マシンを [スタンドアロンの保護VM（Standalone Protected VMs）] サブペインから移行します。詳細については、計画された移行 （288 ページ）を参照してください。

ディザスタ リカバリと再保護

ディザスタ リカバリを実行するとターゲットの VM が回復され、ソースからターゲットに所有権がスイッチされ、新しいソースになったターゲットでレプリケーションが再開されます。ディザスタ リカバリは通常、障害が発生したときや保護の方向を反対にするときに実行されます。

注目

- このプロセスは戻すことができません。

  1. プライマリ サイトの vSphere Web クライアント ナビゲータにログインし、プライマリ サイトから VM を削除して VM を登録解除します。

     仮想マシンを右クリックして、**[すべてのvCenterアクション（All vCenter Actions）]** > **[インベントリから削除（Remove from Inventory）]** を選択します。

  2. セカンダリ サイトの HX Connect にログインします。**[レプリケーション（Replication）]** > **[リモートVM（Remote VMs）] タブ** > ***[protected_vm]*** を選択します。[回復（Recover）] をクリックします。

  3. プライマリ サイトが復帰したら、セカンダリ サイトの HX Connect にログインします。**[レプリケーション（Replication）]** > **[リモートVM（Remote VMs）] タブ** > ***[非保護（unprotected）]*** を選択します。[再保護（Re-protect）] をクリックします。

  4. 再保護が正常に完了したら、セカンダリ サイトの vSphere Web クライアントにログインして、VM を手動で登録します。

     1. vSphere Web クライアント ナビゲータにログインします。**[構成（Configuration）]** > **[ストレージ（Storage）]** を選択します。

     2. 適切なデータストアを右クリックして、**[データ ストアの参照（Browse Data store）]** をクリックします。

        virtualmachine name.vmx ファイルに移動し、ファイル上で右クリックして、**[インベントリに追加（Add to Inventory）]** をクリックします。ウィザードに従って、VM を手動で登録します。

- HX Connect ユーザー インターフェイスを使用して、以前に送信されたタスクが完了するのを待たずに、シーケンス内で最大 5 つの再保護タスクを実行できます。

手順

ステップ 1 ソースとターゲットの HX 接続にログインします。ターゲット クラスタは、レプリケーション DP スナップショットのコピー先となっていたクラスタです。ソース クラスタは、VMが存在しているクラスタです。

ステップ 2 リモート VM のリストから VM を選択します。このクラスタの VM ワークフローで VM の回復を実行します。

（注） ターゲットとソースの両方のクラスタが同じ vCenter にある場合は、ソース クラスタの VM の登録を解除します。これにより、vCenter に VM のレコードがなくなり、VM の管理が停止することになりますが、VM のデータは保持します。

ステップ 3 **[レプリケーション（Replication）] > > [リモート VM（Remote VMs）] タブ > > *[非保護（unprotected）]*** を選択し、**[回復（Recover）]** をクリックします。

ステップ 4 ターゲット VM を回復し、ローカル クラスタに新しい VM を構築するには、**[VM の回復（Recover VM）]** ボタンをクリックします。

[このクラスタの VM を回復する（Recover VM on this cluster）] ダイアログボックスで、次のフィールドに入力します。

UI 要素	基本的な情報
[リソース プール] ドロップダウン リスト	新しい VM を格納する場所を選択します。
[フォルダ（Folders）] ドロップダウン リスト	新しい VM を格納する場所を選択します。
[電源オン/オフ（Power On/Off）] ラジオ ボタン	デフォルトでは、**[電源オン（Power ON）]** オプションが選択されています。回復した VM は、選択したオプションに応じて、作成した後に電源がオンになるかオフのままになります。

UI 要素	基本的な情報
ネットワークのマッピング	ソースとターゲット クラスタ ネットワークの間にマップを作成する場合に選択します。 • ソース ネットワーク：VM が接続されているソース側のネットワーク名。 • ターゲット ネットワーク：ドロップダウン リストから、VM を接続する必要があるターゲット ネットワークを選択します。 ネットワークのオプションの例。 • ストレージ コントローラのデータ ネットワーク • ストレージ コントローラの管理ネットワーク • ストレージ コントローラ レプリケーション ネットワーク • VM ネットワーク

ステップ 5 **[VM を回復する（Recover VM）]** をクリックします。

ステップ 6 ターゲット クラスタで、**[レプリケーション（Replication）]** > **[リモートVM（Remote VMs）] タブ** > ***[非保護（unprotected）]*** を選択します。

ステップ 7 [再保護（Re-protect）] をクリックします。

注目
- ターゲット クラスタとソース クラスタの両方が同じ vCenter 上にある場合、ソース クラスタに手動で VM を登録します。
- 再保護タスクが失敗し、HX Connect UI で [再保護（Re-protect）] タブが使用できない場合は、*stcli reverseprotect* を実行して再保護操作を完了します。

VM の保護ステータスとして [保護済み（Protected）] と表示されます。

ステップ 8 元のプライマリが復帰した後、プライマリに移行するには次の手順を実行します。

a) ターゲット クラスタで、**[レプリケーション（Replication）]** > **[リモートVM（Remote VMs）] タブ** > ***[非保護（unprotected）]*** を選択します。

b) [移行（Migrate）] をクリックし、ターゲット VM を登録解除して、VM の所有権を元のプライマリに移します。
VM の保護ステータスとして [保護済み（Protected）] と表示されます。

障害後の仮想マシンの保護

障害発生時、ソース サイトも一緒に失われる可能性があります。リカバリの実行後、新しいクラスタに回復した VM を保護できます。

重要な使用ガイド: Cisco HyperFlex リリース 5.0(2b) 以降のユーザーは、続行する前に次の使用例を確認する必要があります。

stcli dp peer forget --pair-name 操作は単一のクラスタ操作であり、コマンドが実行されるクラスタにのみ影響します。**stcli dp peer delete** は 2 クラスタ操作であり、両方のクラスタからペアリングを削除します。

クラスタ A と B がペアリングされていて、クラスタ B が永続的にダウンしているか、長期間使用できない状況では、クラスタ A のペアリング関係を削除する必要がある場合があります。適切な解決策は、クラスタ A で **stcli dp peer forget --pair-name** を使用することです。

手順

ステップ 1 仮想マシンを回復します。スタンドアロン リカバリ（VM の回復）またはグループ リカバリ（保護グループでの VM の回復）を実行します。詳細については、仮想マシンのリカバリ （285 ページ）を参照してください。

ステップ 2 既存のペアリングをクリアするには、HX 接続 WebCLI で次のコマンドを実行します。

```
stcli dp peer forget --all
```

これで、クラスタは元の送信元にペアリングされなくなります。

ステップ 3 すべてのローカルおよびリモートの VM の保護を解除します。詳細については、仮想マシンの保護の解除（280 ページ）を参照してください。

ステップ 4 STCLIを使用して、保護グループデータをクリーンアップします。

```
Remove Protection group (if any)
stcli dp group list
stcli dp group delete --groupid <groupUUID>
```

（注） GroupUUIDは、group listコマンドのvmGroupEr.idです。

グループ削除は、リモートクラスタのHX接続ではサポートされていません。stcliを使用します。

ステップ 5 （オプション）必要に応じて、**stcli drnetwork cleanup** コマンドを使用して DR ネットワークを変更します。詳細については、お使いのリリースに対する『Cisco HyperFlex Data Platform CLI ガイド』を参照してください。

ステップ 6 新しいクラスタにペアリングします。詳細については、レプリケーション ペアの作成 （261 ページ）セクションを参照してください。

ステップ 7 仮想マシンを保護します。

自動保護されたクラスタ VM からの保護の削除

vCLS VM が [仮想マシン（Virtual Machines）] ページに表示されないが、自動保護されている場合は、次の手順を実行して、自動保護されたクラスタ VM から保護を削除できます。

始める前に

- VSphere Cluster Services（vCLS）VM は、バックアップまたは DR/SRM データストアに配置しないでください。
- 1:1 DR または N:1 バックアップ機能を目的とした HX データストアに vCLS VM を配置しないでください。

手順

ステップ 1 `stcli dp vm delete <vmid>` cli を使用して VM の保護を解除します。

ステップ 2 VCenter を使用して、VM を別のデータストアに VMotion で保存します。

レプリケーション メンテナンスの概要

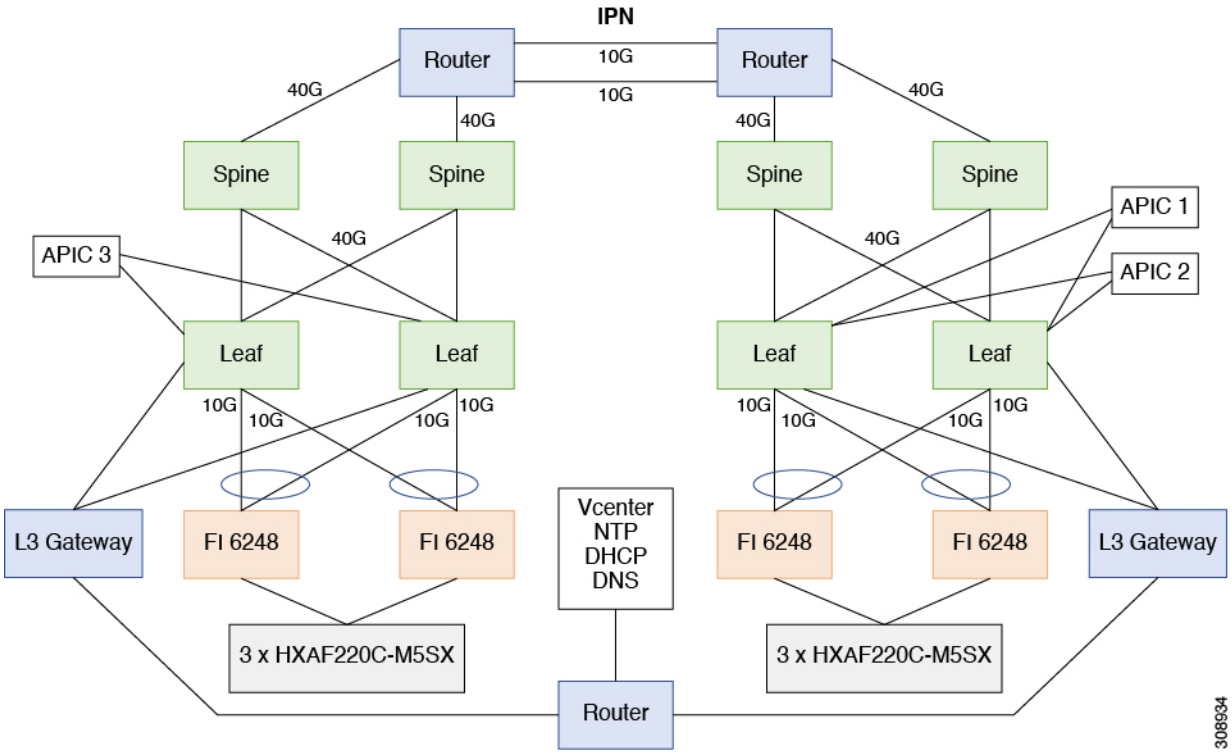
レプリケーションは、設定されている場合、定義されているスケジュールに従ってバックグラウンドで実行されます。レプリケーションのメンテナンス タスクは、次のとおりです。

- **リカバリのテスト**：リカバリ手法が機能しているかどうかテストします。詳細については、仮想マシンのリカバリのテスト （283 ページ）を参照してください。
- **レプリケーションの一時停止**ーHX クラスタのアップグレードを行うための準備をする際にレプリケーションが構成済みの場合は、レプリケーションアクティビティを一時停止する必要があります。

  `stcli dp schedule pause` コマンドを使用します。
- **レプリケーションの再開** ー HX クラスタのメンテナンス アクティビティが完了したら、レプリケーション スケジュールを再開します。

  それには、`stcli dp schedule resume` コマンドを使用します。
- **移行**：1 つのソース クラスタからレプリケーション ペアのターゲット クラスタに VM を移行し、ターゲット クラスタを移行後の VM の新しいソース クラスタにするには、このタスクを実行します。

次の図は、大規模な ACI 設定で展開する場合に HyperFlex のディザスタ リカバリに使用される設定を示しています。



レプリケーションの一時停止

storfs またはプラットフォームのアップグレードを行う前に、レプリケーションが設定されると、レプリケーション アクティビティは一時停止する必要があります。

手順

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 コマンド ラインから stcli dp schedule pause コマンドを実行します。
ステップ 3 アップグレード タスクを実行します。
ステップ 4 レプリケーション スケジュールを再開します。

レプリケーションの再開

レプリケーションが設定された HX ストレージ クラスタ が正常にアップグレードされたら、次の操作を実行してレプリケーション スケジュールを再開します。

始める前に

HX クラスタ レプリケーションが一時停止され、メンテナンスまたはアップグレードタスクが完了していることを確認します。

手順

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 コマンド ラインから `stcli dp schedule resume` コマンドを実行します。

保護されたすべての仮想マシンに以前設定されたレプリケーション スケジュールが開始されます。

[レプリケーション（Replication）] ページ

レプリケーション設定、ローカル保護、およびリモート保護に関連する概要情報と詳細情報へのリンクを表示します。

レプリケーション設定のリボン

UI 要素	基本的な情報
[レプリケーション設定（REPLICATION CONFIGURATION）] フィールド	レプリケーション ネットワーク設定の状態を表示します。 • **レプリケーション ネットワークが設定されていません Replication network not configured**：レプリケーション ネットワークが設定されていません。 **[設定（Configure）]** をクリックして開始します。 • **ネットワーク設定済み**：レプリケーション ネットワークが設定されています。 **[編集（Edit）]** をクリックして、レプリケーション ネットワークの IP範囲または帯域幅制限を調整します。

UI 要素	基本的な情報
[帯域幅制限（BANDWIDTH LIMIT）] フィールド	着信および発信レプリケーション データの送信に許可されている設定済み帯域幅を表示します。 • **空白**：レプリケーション ネットワークは設定されていません。 • **# Mbps**：メガビット/秒（Mbps）単位の設定。 • **最大（Maximum）**：デフォルト設定。レプリケーション ネットワークが使用可能なネットワーク帯域幅の合計を使用できるようにします。 帯域幅制限を変更するには、**[編集（Edit）]** をクリックします。
帯域幅チャート	この HX ストレージ クラスタ とペアリングされた HX ストレージクラスタの間で複製されるデータに使用される帯域幅を表示します。垂直軸は帯域幅、水平軸は時間です。 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。
[アクション（Actions）] ドロップダウン リスト	HX ストレージ クラスタ をクリックして、レプリケーション ネットワークを作成または編集し、レプリケーション ネットワークをテストします。 • **ローカル レプリケーション ネットワークのテスト**：<define> • **レプリケーションネットワークの編集**：IP範囲を編集し、レプリケーション帯域幅制限を設定します。

リカバリ設定 リボン

UI 要素	基本的な情報
[クラスタ ペアリング（Cluster Pairing）] フィールド	クラスタのペアの名前を表示します。 • クラスタペアリングが完了していないときに表示される **[ペア クラスタ（Pair Cluster）]** をクリックして、クラスタ ペアリングを開始します。 • **[ペアの作成（Create Pair）]** をクリックして、クラスタ ペアリングを開始します。**[Create Replication Pair (複製ペアの作成)]** オプションは、すべての VM の保護を解除し、すべての依存関係を削除した後に、既存の複製ペアを削除するときにのみ有効です。

UI 要素	基本的な情報
[データストア マッピング（DATASTORE MAPPED）] フィールド	マッピングされたデータストアの数を表示します。 • データストアのマッピングが完了していないときに表示される **[データストア ペアのマッピング（Map Datastore Pairs）]** をクリックして、1 つのローカル データストアを 1 つのリモート データストアにマッピングします。
リカバリ設定 リボン	リカバリ設定コンフィギュレーションの状態を表示します。 • リカバリ設定を行っていないときに表示される **[設定（Configure）]** をクリックして、リカバリ中またはテスト リカバリ中にネットワークを既知の動作状態に戻すように設定します。
[アクション（Actions）] ドロップダウン リスト	レプリケーション ネットワーク、リカバリ設定、およびデータ ストアマッピングに対して特定の操作を実行するアクションのいずれかを選択します。 • **リモート レプリケーション ネットワークのテスト**：リモート レプリケーション ネットワークのクラスタ間のペアリングをテストします。 • **リカバリ設定の検証**：設定されたリカバリ設定を検証します。 • **リカバリ設定の編集**：リカバリ設定を編集します。 • **データストア マッピングの編集**：ローカルとリモートのデータストア間のマッピングを編集します。

ローカル/リモート保護の概要のリボン

UI 要素	基本的な情報
[VM] フィールド	ローカル クラスタまたはリモート クラスタで保護用に設定された仮想マシンの合計数を表示します。個々の仮想マシンおよび保護グループ内の仮想マシンの詳細を表示します。 フィールドをクリックすると、保護された仮想マシンのリストが **[ローカル VM（Local Vms）]** タブまたは **[リモート VM（Remote Vms）]** タブに表示されます。

UI 要素	基本的な情報
[保護（Protection）] フィールド	レプリケーションスナップショットが作成された仮想マシンの合計数を表示します。 フィールドをクリックすると、保護された仮想マシンのリストが **[ローカル VM（Local Vms）]** タブまたは **[リモート VM（Remote Vms）]** タブに表示されます。
[間隔超過（Exceeds Interval）] フィールド	設定された間隔よりも完了に時間がかかったレプリケーションの数を表示します。 たとえば、仮想マシンの間隔が 15 分ごとであり、ローカルクラスタからリモートクラスタへのスナップショットの複製に 20 分かかった場合、複製はこの間隔を超えました。 フィールドをクリックすると、**[ローカル VM（Local Vms）]** タブまたは **[リモート VM（Remote Vms）]** タブに、間隔が超過した仮想マシンのリストが表示されます。
[現在のレプリケーションの障害（Current Replication Failures）] フィールド	完了しなかったレプリケーションの現在の数を表示します。 **[ローカル VM（Local Vms）]** タブまたは **[リモート VM（Remote Vms）]** タブに、このフィールドをクリックして、レプリケーションに失敗した仮想マシンのリストを表示します。
[保護グループ（Protection Group）] フィールド	この HX ストレージ クラスタ のために設定された保護グループの総数を表示します。 **[ローカル VM（Local Vms）]** タブまたは **[リモート VM（Remote VMs）]** タブの **[保護グループ（Protection Groups）]** セクションに、保護グループとその関連VM のリストを表示するフィールドをクリックします。

[レプリケーション（Replication）] ページの表には、**[ローカル VM（Local VMs）]**、**[リモート VM（Remote Vms）]**、**[レプリケーション、[レプリケーション アクティビティ（Replication Activity）]**、および **[レプリケーション ペア（Replication Pairs）]** の 4 つのタブがあります。これらの各タブには、レプリケーション保護の設定オプションがあります。

[レプリケーション アクティビティ（Replication Activity）] タブ

UI 要素	基本的な情報
[仮想マシン（Virtual Machine）] カラム	HX ストレージ クラスタ のレプリケーションによって保護されている仮想マシンの名前。
[リモート クラスタ（Remote Cluster）] カラム	保護された仮想マシンに関連付けられた対応するリモート クラスタの名前。これは、リストされている仮想マシンのリカバリクラスタです。

UI 要素	基本的な情報
[ステータス（Status）] カラム	このクラスタの仮想マシン保護の現在のステータスを表示します。 • **[成功（Success）]**：リモート クラスタへの仮想マシンとそのデータのスケジュールされたレプリケーションが完了しました。 • **[開始（Starting）]**：レプリケーション タスクを開始しています。 • **[進行中（In progress）]**：レプリケーション タスクが進行中です。 • **[失敗（Failed）]**：スケジュールされたレプリケーション タスクは完了しませんでした。 • **[削除済み（Deleted）]**：レプリケーション タスクが削除されます。 • **[一時停止（Paused）]**：レプリケーション タスクが一時停止されます。
[開始時間（Start Time）] カラム	最後に開始されたレプリケーションプロセスのタイムスタンプを表示します。
[終了時間（End Time）] カラム	最後に完了したレプリケーション プロセスのタイムスタンプを表示します。
[保護グループ（Protection Status）] カラム	関連付けられた仮想マシンが保護グループに属している場合は、保護グループ名が表示されます。保護グループがない場合、フィールドには **[なし（None）]** と表示されます。
[Direction (ディレクション)] カラム	複製された仮想マシンの方向。方向は、ローカル クラスタを基準にしています。ログイン中のクラスタは、常にローカル クラスタとしてのログインになります。次のオプションがあります。 • **[受信（Incoming）]**：仮想マシンはリモート クラスタに存在します。リモート クラスタからローカル クラスタに複製されます。 • **[発信（Outgoing）]**：仮想マシンはリモート クラスタに存在します。ローカル クラスタからリモート クラスタに複製されます。

UI 要素	基本的な情報
[データ転送（Data Transferred）] カラム	複製される仮想マシンのサイズ（バイト単位）。レプリケーションが進行中の場合、完了した量が表示されます。レプリケーションが完了すると、転送されたデータの量がバイト単位で表示されます。

[レプリケーション ペア（Replication Pairs）] タブ

UI 要素	基本的な情報
[名前（Name）] カラム	このローカル クラスタの名前。
[リモート クラスタ（Remote Cluster）] カラム	リモート クラスタのホスト名と IP アドレス。
[リモート クラスタ ステータス（Remote Cluster Status）] カラム	リモート クラスタのステータス。オプションには、オンライン、オフラインがあります
[VM 発信（VMs Outgoing）] カラム	このローカル HX ストレージ クラスタ からリモート HX ストレージクラスタ へのレプリケーション用に設定された仮想マシンの数。このローカル クラスタの保護グループの数が含まれます。 **[仮想マシン（Virtual Machines）]** ページに VM レプリケーションを表示するには、フィールドをクリックします。
[レプリケーションの発信（Replications Outgoing）] カラム	このローカル HX ストレージ クラスタ からリモート HX ストレージクラスタ に複製され、データを転送する仮想マシンの数。
[VM 受信（VMs Incoming）] カラム	リモート HX ストレージ クラスタ からこのローカル HX ストレージクラスタ へのレプリケーション用に設定された仮想マシンの数。リモート クラスタ上の保護グループの数が含まれます。 **[仮想マシン（Virtual Machines）]** ページに VM レプリケーションを表示するには、フィールドをクリックします。
[レプリケーション受信（Replications Incoming）] カラム	リモート HX ストレージ クラスタ からこのローカル HX ストレージクラスタ に複製され、データを転送している仮想マシンの数。
[マッピングされたデータストア ペア（Mapped Datastore Pairs）] カラム	ローカルクラスタのレプリケーションに使用されるデータストアの数。 フィールドをクリックすると、**[データストア（Datastores）]** ページにデータストアのリストが表示されます。

UI 要素	基本的な情報
レプリケーション ペアの作成	このボタンは、レプリケーションペアがこのローカルクラスタに設定されていない場合にのみ使用できます。ボタンをクリックし、**[レプリケーション ペアの作成（Create Replication Pair）]** ダイアログ ボックスを完了します。
[Edit（編集）] ボタン	レプリケーション ペアを選択し、**[編集（Edit）]** をクリックして、レプリケーションに使用するローカルまたはリモートデータストアを変更します。**[レプリケーション ペアの削除（Delete Replication Pair）]** ダイアログ ボックスで必要な値を入力します。
[削除（Delete）] ボタン	レプリケーション ペアを選択し、**[削除（Delete）]** をクリックします。操作を確認します。 この操作は、このローカルクラスタのペアリングをリモートクラスタから削除する場合に実行します。 （注） 両方のクラスタのすべての VM のレプリケーション設定が失われます。VM に保護を適用するには、新しいレプリケーションペアの作成を含むすべての保護手順を完了する必要があります。

[ローカル仮想マシン（Local Virtual Machines）] ページ

ローカル仮想マシンに関連する詳細情報を表示します。

UI 要素	基本的な情報
保護グループ サブ テーブル	**[+ グループの作成（+ Create Group）]** ボタン：**[保護グループの作成（Create Protection Group）]** ダイアログ ボックスを開きます。 ローカル クラスタで作成された保護グループを一覧表示します。**すべての保護された VM** または**スタンドアロンの保護された VM** で仮想マシンをフィルタリングできます。 次の保護グループデータを表示します。 • グループ名 • グループ内の VM の数 • VM のステータス：保護、リカバリ、リカバリ、リカバリ失敗 • レプリケーション間隔時間、ツールチップには最後のレプリケーションの時間が表示されます • スケジュールを編集するには、ペン アイコンをクリックします。保護グループを削除するには、ゴミ箱アイコンを使用します。
[一時停止（Pause）] ボタン	発信レプリケーションを一時停止すると、すべての動作中の仮想マシンと新しい仮想マシンがターゲットサイトで保護されなくなります。
[仮想マシン名（Virtual Machine Name）] カラム	HX ストレージ クラスタ のレプリケーションによって保護されている仮想マシンの名前を一覧表示します。

UI 要素	基本的な情報
[保護ステータス（Protection Status）] カラム	このクラスタで保護されている仮想マシンの現在のステータスを表示します。 • **[リカバリ中（Recovering）]**：仮想マシンは、リモート クラスタのレプリケーション スナップショットから最近復元されました。 VM の状態：フェールオーバーの準備が開始され、フェールオーバーの準備が完了しました • **[リカバリに失敗（Recovery Failed）]**：仮想マシンは、リモートクラスタのレプリケーション スナップショットからの復元に失敗しました。 VM状態：フェールオーバーの準備失敗、フェールオーバー失敗 • **[リカバリ済み（Recovered）]**：仮想マシンは、リモート クラスタのレプリケーション スナップショットから最近復元されました。 VM状態：フェールオーバー完了 • **[保護中（Protecting）]**：その仮想マシンに対して開始されたリバース保護。 VM の状態：リバース保護の開始の準備、リバース保護の準備の完了、リバース保護の開始 • **[保護失敗（Protection Failed）]**：仮想マシンのリバース保護に失敗しました。 VM の状態：Prepare Reverse Protect Failed、Reverse Protect Failed • **[保護（Protected）]**：仮想マシンには、リカバリに使用できるスナップショットが少なくとも 1 つあります。 VM の状態：成功 • **[アクティブ（Active）]**：保護は設定されていますが、スナップショットは使用できません。 VM状態：アクティブ • **[超過間隔（Exceed Interval）]**：最後のレプリケーションプロセスは、設定された間隔よりも長くかかりました。
[前回の保護時刻（Last Protection Time）] カラム	最後に完了したレプリケーション プロセスのタイムスタンプを表示します。

UI 要素	基本的な情報
[Direction (ディレクション)] カラム	複製された仮想マシンの方向を、ローカルクラスタを基準にして表示します。ログイン中のクラスタは、常にローカル クラスタとしてのログインになります。 • **[受信（Incoming）]**：仮想マシンはリモート クラスタに存在します。リモートクラスタからローカルクラスタに複製されます。 • **[発信（Outgoing）]**：仮想マシンはリモート クラスタに存在します。ローカルクラスタからリモートクラスタに複製されます。
[保護グループ（Protection Status）] カラム	関連付けられた仮想マシンが保護グループに属している場合は、保護グループ名が表示されます。保護グループがない場合、フィールドには **[なし（None）]** と表示されます。
[間隔（Interval）] カラム	各レプリケーションの開始間の時間の長さを表示します。各レプリケーションを完了するのに十分な間隔を選択します。 たとえば、[間隔時間（Interval time）] が 1 時間ごとの場合、VM のレプリケーションは 1 時間ごとに開始されます。
[スケジュールの編集（Edit Schedule）] ボタン	個別に保護された VM を選択し、**[スケジュールの編集（Edit Schedule）]** をクリックしてレプリケーション間隔を変更します。
[グループから削除（Remove from Group）] ボタン	同じ保護グループから 1 つ以上の VM を選択し、**[グループから削除（Remove from Group）]** をクリックして、選択した VM をグループから削除します。 選択した VM は、保護グループと同じレプリケーションスケジュールで引き続き個別に保護されます。 **[保護グループから削除（Remove from Protection Group）]** をクリックして確認します。
[グループに追加（Add to Group）] ボタン	保護されている仮想マシンをグループに追加する場合にクリックします。VM スケジュールがグループスケジュールに変更されます。

UI 要素	基本的な情報
[保護解除（Unprotect）] ボタン	VM からレプリケーション保護を削除するには、個別に保護された VM を選択し、**[保護解除（Unprotect）]** をクリックします。保護を解除すると、レプリケーション スナップショットが開始されなくなります。 **[保護解除（Unprotect）]** をクリックして確定します。 VM がリストから削除されます。 （注） 保護を解除すると、選択した VM の保護が解除されます。VM を保護するには、レプリケーション設定を再適用する必要があります。

[リモート仮想マシン（Remote Virtual Machines）] ページ

リモート仮想マシンに関連する詳細情報を表示します。

UI 要素	基本的な情報
保護グループ サブ テーブル	**[+ グループの作成（+ Create Group）]** ボタン：[保護グループの作成（Create Protection Group）] ダイアログ ボックスを開きます。 リモート クラスタで作成された保護グループを一覧表示します。**すべての保護された VM** または**スタンドアロンの保護された VM** で仮想マシンをフィルタリングできます。 次の保護グループデータを表示します。 • グループ名 • グループ内の VM の数 • VM のステータス：保護、リカバリ、リカバリ、リカバリ失敗 • レプリケーション間隔時間。ツールチップには、最後のレプリケーションの時間が表示されます。
[仮想マシン名（Virtual Machine Name）] カラム	HX ストレージ クラスタ のレプリケーションによって保護されている仮想マシンの名前を表示します。

UI 要素	基本的な情報
[保護ステータス（Protection Status）] カラム	このクラスタの仮想マシン保護の現在のステータスを表示します。 • **[リカバリ中（Recovering）]**：仮想マシンは、リモート クラスタのレプリケーション スナップショットから最近復元されました。 VM の状態：フェールオーバーの準備が開始され、フェールオーバーの準備が完了しました • **[リカバリに失敗（Recovery Failed）]**：仮想マシンは、リモートクラスタのレプリケーション スナップショットからの復元に失敗しました。 VM状態：フェールオーバーの準備失敗、フェールオーバー失敗 • **[リカバリ済み（Recovered）]**：仮想マシンは、リモートクラスタのレプリケーション スナップショットから最近復元されました。 VM状態：フェールオーバー完了 • **[保護中（Protecting）]**：その仮想マシンに対して開始されたリバース保護。 VM の状態：リバース保護の開始の準備、リバース保護の準備の完了、リバース保護の開始 • **[保護失敗（Protection Failed）]**：仮想マシンのリバース保護に失敗しました。 VM の状態：Prepare Reverse Protect Failed、Reverse Protect Failed • **[保護（Protected）]**：仮想マシンには、リカバリに使用できるスナップショットが少なくとも 1 つあります。 VM の状態：成功 • **[アクティブ（Active）]**：保護は設定されていますが、スナップショットは使用できません。 VM状態：アクティブ • **[超過間隔（Exceed Interval）]**：最後のレプリケーション プロセスは、設定された間隔よりも長くかかりました。
[前回の保護時刻（Last Protection Time）] カラム	最後に完了したレプリケーション プロセスのタイムスタンプを表示します。

UI 要素	基本的な情報
[Direction (ディレクション)] カラム	複製された仮想マシンの方向を、ローカルクラスタを基準にして表示します。ログイン中のクラスタは、常にローカル クラスタとしてのログインになります。 • **[受信（Incoming）]**：仮想マシンはリモート クラスタに存在します。リモートクラスタからローカルクラスタに複製されます。 • **[発信（Outgoing）]**：仮想マシンはリモート クラスタに存在します。ローカルクラスタからリモートクラスタに複製されます。
[保護グループ（Protection Status）] カラム	関連付けられた仮想マシンが保護グループに属している場合は、保護グループ名が表示されます。保護グループがない場合、フィールドには **[なし（None）]** と表示されます。
[間隔（Interval）] カラム	各レプリケーションの開始間の時間の長さを表示します。各レプリケーションを完了するのに十分な間隔を選択します。 たとえば、間隔が 1 時間ごとの場合、VM のレプリケーションは 1 時間ごとに開始されます。
[Recover (リカバリ)] ボタン	VM を選択し、**[リカバリ（Recover）]** をクリックして、VM の最新のレプリケーション スナップショットを取得し、ローカル クラスタに新しい VM を構築します。リモート クラスタ上の VM が使用できないことを確認します。 VM を回復するには、**保護解除**後にこの手順を実行します。
[移行（Migrate）] ボタン	保護された VM をソースからターゲットに移行するには、VM を選択して**[移行（Migrate）]**をクリックします。
[保護解除（Unprotect）] ボタン	VM からレプリケーション保護を削除するには、個別に保護された VM を選択し、**[保護解除（Unprotect）]** をクリックします。保護を解除すると、レプリケーション スナップショットが開始されなくなります。 VM を回復するには、**[クラスタでリカバリ（Recover on Cluster）]** の前にこの手順を実行します。
[再保護（Re-protect）] ボタン	個別に保護されていない VM を選択し、**[再保護（Re-protect）]** をクリックして VM を再保護します。
[リカバリのテスト（Test Recovery）] ボタン	VM を選択し、**[リカバリのテスト（Test Recovery）]** をクリックして、VM の最新のレプリケーション スナップショットを取得し、ローカル クラスタに新しいVMを構築します。

仮想マシンの保護の準備アラート

仮想マシンが保護される前に、レプリケーション ネットワークおよびレプリケーション ペアを設定する必要があります。

次のタスクを実行するには、管理者権限を持つユーザとしてログインする必要があります。

1. ローカル クラスタとリモート ストレージ クラスタでデータストアを作成します。各クラスタの **[データストア（Datastores）]** タブで、**[データストアの作成（Create Datastore）]** ボタンをクリックします。

   ローカル クラスタに1つ以上のデータストアを作成し、リモート クラスタにログインして、そこにデータストアを作成します。

2. ローカル クラスタとリモート クラスタの両方でレプリケーション ネットワークを構成します。各クラスタの **[レプリケーション（Replication）]** タブで、**[設定（Configure）]** ボタンをクリックします。

   ローカル クラスタで設定を完了してから、リモート クラスタにログインして、そこで構成を完了します。

3. ローカルとリモートのストレージクラスタ間のレプリケーションペアを設定します。**[レプリケーション（Replication）]** > **[ペア クラスタ（Replication Pair Cluster）]** を選択します。

   ローカルとリモートのストレージ クラスタ間でデータストアをマッピングします。データストアのマッピングは、ローカルまたはリモートのストレージ クラスタから実行できます。

[レプリケーション ネットワークの設定/編集（Configure/Edit Replication Network）] ダイアログボックス

レプリケーションネットワークの設定

（注） このタスクを実行するには、管理者権限を持つユーザとしてログインする必要があります。

仮想マシンを保護するには、まずレプリケーション ネットワークとレプリケーション ペアを構成する必要があります。

ローカルクラスタとリモートクラスタの両方でレプリケーションネットワークを構成します。最初にローカル クラスタでレプリケーション ネットワークを構成した後、リモート クラスタにログインして構成を完了します。

1. **[Replication]** > **[Configure Network]** を選択します。
2. **[VLAN 構成（VLAN Configuration）]** タブで、次のフィールドに値を入力します。

UI 要素	基本的な情報
[既存の VLAN の選択（Select an existing VLAN）] オプション ボタン	このラジオボタンをクリックして、既存の VLAN を追加します。 レプリケーション ネットワークで使用するために VLAN を Cisco UCS Manager を通じて手動で設定した場合、その VLAN ID を入力します。
[新しい VLAN の作成] ラジオ ボタン	このラジオボタンをクリックして、新規 VLAN を作成します。 （注） Edge クラスタでレプリケーション ネットワークを構成している場合は、**[VLAN の作成]** オプションを使用しないでください。既存の VLAN オプションを使用して、同じ手順に従います。
[VLAN ID] フィールド	上矢印または下矢印をクリックして VLAN ID の番号を選択するか、フィールドに番号を入力します。 これは、HX データ プラットフォーム管理トラフィック ネットワークおよびデータ トラフィック ネットワークとは別のものです。 **重要** レプリケーションペアを構成する HX ストレージ クラスタごとに、異なる VLAN ID を必ず使用してください。 レプリケーションは、2 つの HX ストレージ クラスタ間で行われます。各 HX ストレージ クラスタには、レプリケーション ネットワーク専用の VLAN が必要です。 たとえば、*3* です。 値を追加すると、デフォルトの VLAN 名が更新されて追加の ID が組み込まれます。VLAN ID の値は、手動で入力される VLAN 名には影響を与えません。
[VLAN名（VLAN Name）] フィールド	**[Create a new VLAN]** ラジオ ボタンを選択した場合、このフィールドにはデフォルトの VLAN 名が入力されます。VLAN ID は名前に紐づけられます。
ストレッチ クラスタの場合は、プライマリおよびセカンダリ FI（サイト A とサイト B）の Cisco UCS Manager ログイン情報を入力します。通常のクラスタの場合は、単一の FI の Cisco UCS Manager ログイン情報を入力します。	
[UCS Manager のホスト IP または FQDN（UCS Manager host IP or FQDN）] フィールド	Cisco 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。

UI 要素	基本的な情報
[ユーザ名（Username）] フィールド	Cisco UCS Manager の管理ユーザー名を入力します。
[パスワード（Password）] フィールド	Cisco UCS Manager の管理パスワードを入力します。

[次へ（Next）] をクリックします。

3. **[IP と帯域幅の設定（IP & Bandwidth Configuration）]** タブで、次のフィールドに値を入力します。

[IP と帯域幅の設定（IP & Bandwidth Configuration）] タブ

UI 要素	基本的な情報

[レプリケーション ネットワーク サブネット（Replication Network Subnet）]フィールド	レプリケーション ネットワークで使用するサブネットを、ネットワーク プレフィックス表記で入力しますこれは、HX データ プラットフォーム 管理トラフィック ネットワーク および データ トラフィック ネットワーク とは別です。
	`Format example:`
	`p.q.r.s/<length>`
	`209.165.201.0/27`

[ゲートウェイ（Gateway）] フィールド	レプリケーション ネットワークで使用するゲートウェイを入力します。これは、HX データ プラットフォーム 管理トラフィック ネットワーク および データ トラフィック ネットワーク とは別です。 たとえば、*1.2.3.4* とします。
[IP範囲（IP Range）] フィールド	レプリケーション ネットワークで使用する IP アドレス範囲を入力します。 • 必要な IP アドレスの最小数は、HX ストレージ クラスタ内のノード数プラス 1 です。 たとえば、4 ノード HX ストレージ クラスタの場合、少なくとも 5 つの IP アドレスを含む範囲を入力します。 • **[開始（from）]** の値には、**[終了（to）]** の値より小さい値を指定する必要があります。 たとえば、*From 10.10.10.20 To 10.10.10.30* とします。 • クラスタにノードを追加する計画がある場合は、追加ノードに対応するのに十分な数の IP アドレスを含めます。IP アドレスはいつでも追加できます。

UI 要素	基本的な情報
[IP 範囲の追加（Add IP Range）] ボタン	クリックすると、**[IP 範囲（IP Range）]** の [開始（From）] および [終了（To）] フィールドに入力した IP アドレス範囲が追加されます。
[レプリケーション帯域幅制限の設定（Set replication bandwidth limit）] チェックボックス	レプリケーション ネットワークが発信トラフィックに使用できる最大のネットワーク帯域幅を入力します。可能な値は、10 ～ 10,000 です。 デフォルト値は [無制限（unlimited）] です。この場合、最大ネットワーク帯域幅はネットワークで使用可能な合計帯域幅に設定されます。 レプリケーション帯域幅は、このローカル HX ストレージ クラスタからペアリング相手のリモート HX ストレージ クラスタにレプリケーション スナップショットをコピーする際に使用されます。

4. [構成（Configure）] をクリックします。

レプリケーションネットワークの編集

（注） このタスクを実行するには、管理者権限を持つユーザとしてログインする必要があります。

構成されるレプリケーション ネットワークに、利用可能な IP アドレスを追加します。ストレージ クラスタ内のノードごとに 1 つの IP アドレスと、管理用にもう 1 つの IP アドレスが必要です。ストレージ クラスタを拡張すると、利用可能な IP アドレスが使用されます。

1. **[Replication]** > **[Actions]** ***[drop-down list]*** > **[Edit Configuration]**を選択します。
2. [ネットワーク設定の編集（Edit Network Configuration）] ダイアログボックスで、使用する IP の範囲を編集して、レプリケーション トラフィックのレプリケーション帯域幅制限を設定することができます。レプリケーション ネットワークのサブネット、ゲートウェイ、および VLAN ID は参照用にのみ表示され、編集できません。

[ネットワーク設定の編集（Edit Network Configuration）] ダイアログボックス

UI 要素	基本的な情報
[レプリケーション ネットワーク サブネット（Replication Network Subnet）]フィールド	レプリケーション ネットワークのサブネット。レプリケーション ネットワーク用に設定されているサブネット（ネットワーク プレフィックス表記）。この値は編集できません。 Format example: p.q.r.s/<length> 209.165.201.0/27

UI 要素	基本的な情報
[ゲートウェイ（Gateway）] フィールド	レプリケーション ネットワーク用に設定されているゲートウェイ。この値は編集できません。
[IP範囲（IP Range）] フィールド	レプリケーション ネットワークで使用する IP アドレス範囲を入力します。 • 必要な IP アドレスの最小数は、HX Storage クラスタのノード数プラス 1 です。 たとえば、HX ストレージ クラスタ に 4 つのノードがある場合、IP 範囲は少なくとも 5 つの IP アドレスである必要があります。 • **[開始（from）]** の値には、**[終了（to）]** の値より小さい値を指定する必要があります。 たとえば、*From 10.10.10.20 To 10.10.10.30* とします。 • ただし IP アドレスはいつでも追加できます。 • クラスタにノードを追加する計画がある場合は、追加ノードをカバーするのに十分な数の IP アドレスを含めます。 （注） IP アドレス範囲には、コンピューティング専用ノードは含まれません。
[IP 範囲の追加（Add IP Range）] フィールド	クリックして、**[IP 範囲（IP Range）]** の [開始（From）] および [終了（To）] フィールドに入力した範囲の IP アドレスを追加します。
[レプリケーション帯域幅制限の設定（Set replication bandwidth limit）] チェックボックス（オプション）	レプリケーション ネットワークが発信トラフィックに使用できる最大のネットワーク帯域幅を入力します。 有効な範囲：10ー10,000。デフォルトは `unlimited` で、使用可能なレプリケーション ネットワークの合計に最大ネットワーク帯域幅を設定します。 レプリケーション帯域幅は、このローカル HX ストレージ クラスタ から、ペアになっているリモート HX ストレージ クラスタ に DP スナップショットをコピーするのに使用されます。

UI 要素	基本的な情報
[Set non-default MTU] チェック ボックス	デフォルトの MTU 値は 1500 です。 レプリケーション ネットワークのカスタム MTU サイズを設定するチェック ボックスを選択します。MTU は 1024 ～ 1500 の範囲で設定できます。 （注） • ペアの HX クラスタの両方で同じ MTU 値を使用します。 • HXDP リリース 5.0（2a）以降では、クラスタの設定後に MTU 値を編集できます。古いバージョンの HXDP では、既存のレプリケーション ネットワーク構成を削除する必要があります。レプリケーションネットワークは、正しいMTU値で設定できます。

3. **[Save Changes]**をクリックします。

   これでレプリケーション ネットワークが更新されます。追加した IP アドレスは、ストレージ クラスタに追加されたときに新しいノードで使用できるようになります。レプリケーション トラフィックは、帯域幅制限に対する変更に合わせて調整されます。

グループ リカバリの準備ダイアログ ボックス

注意 災害発生時にのみ、このアクションを完了してください。

グループ リカバリの準備により、保護グループ内のすべての仮想マシンのレプリケーション スケジュールが停止します。すべての VM のレプリケーション スケジュールが停止したら、[スタンドアロン VM（Standalone VM）] タブに進み、各 VM を回復します。

このクラスタ上で VM を回復します

VM を回復し、ローカル クラスタに新しい VM を構築するには、**[VM の回復 (Recover VM)]** ボタンをクリックします。

（注） ここに記載されているすべてのフィールドはオプションです。

UI 要素	基本的な情報
[リソース プール] ドロップダウン リスト	新しい VM を格納する場所を選択します。

UI 要素	基本的な情報
[フォルダ（Folders）] ドロップダウン リスト	新しい VM を格納する場所を選択します。
[電源オン/オフ（Power On/Off）] ラジオ ボタン	回復した VM の電源をオンにするか、作成後に電源をオフにする必要があるかを選択します。
ネットワークのマッピング	ソースとターゲット クラスタ ネットワークの間にマップを作成する場合に選択します。 • ソース ネットワーク—VM 複製スナップショットを持つクラスタ上のネットワーク。 • ターゲット ネットワーク—新しい VM が作成されるクラスタ上のネットワーク。 ネットワーク オプションには次のものが含まれます。 • ストレージ コントローラのデータ ネットワーク • ストレージ コントローラの管理ネットワーク • ストレージ コントローラ レプリケーション ネットワーク • VM ネットワーク

[VM を回復する（Recover VM）] をクリックします。

[リカバリ パラメータのテスト（Test Recovery Parameters）] ダイアログ ボックス

リカバリ プロセスをテストするには、**[VM を回復する（Recover VM）]** ボタンをクリックします。

（注） ここに記載されているすべてのフィールドはオプションです。

UI 要素	基本的な情報
[リソース プール] ドロップダウン リスト	保管するテスト VM のロケーションを選択します。
[フォルダ（Folders）] ドロップダウン リスト	保管するテスト VM のロケーションを選択します: • 検出された仮想マシン • ESX エージェント • HX テスト リカバリ

UI 要素	基本的な情報
[電源オン/オフ（Power On/Off）] ラジオ ボタン	ボタンをクリックします。回復した VM は、作成した後、電源がオンになるかオフのままになります。
[VM名（VM Name）] フィールド	作成されたテスト VM に新しい名前を入力します。
[テスト ネットワーク（Test Networks）] ラジオ ボタン	レプリケーション スナップショットからデータを転送するために使用する HX ストレージ クラスタ ネットワークを選択します。 ネットワーク オプションには次のものが含まれます。 • ストレージ コントローラのデータ ネットワーク • ストレージ コントローラの管理ネットワーク • ストレージコントローラ レプリケーション ネットワーク • VM ネットワーク
[ネットワークのマップ（Map Networks）] ラジオ ボタン	ソースとターゲット クラスタ ネットワークの間にマップを作成する場合に選択します。 ソース—VM レプリケーション スナップショットのあるクラスタ。 ターゲット —テスト VM が作成されたクラスタ。

[VM を回復する（Recover VM）] をクリックします。

[仮想マシンの保護（Protect Virtual Machines）] タブ

仮想マシンの保護ステータスを表示します。保護スケジュールを編集したり、仮想マシンの保護を解除したりできます。保護する仮想マシンを選択するには、**[仮想マシン（Virtual Machines）]** ページを参照してください。

仮想マシンの保護アクション

UI 要素	基本的な情報
[スケジュールの編集（Edit Schedule）] ボタン	選択した仮想マシンのレプリケーションのレプリケーション間隔またはVMwareツールの休止設定を変更します。 仮想マシンを選択して、**[スケジュールの編集（Edit Schedule）]** をクリックします。

UI 要素	基本的な情報
[保護解除（Unprotect）] ボタン	仮想マシンの保護を解除するには： 1. **[レプリケーション（Replication）]** > **[保護済み仮想マシン（Protected Virtual Machines）]** タブを選択します。. 2. 発信保護が設定されたローカルクラスタに存在する1つ以上の仮想マシンを選択します。 個別に保護された仮想マシンは、1つずつ選択する必要があります。選択した複数の仮想マシンを同じ保護グループから選択する必要があります。 3. 仮想マシンを選択し、**[保護解除（Unprotect）]** をクリックします。 4. 別の保護グループ内の仮想マシンまたは独立して保護されている仮想マシンについて、この手順を繰り返します。 ある保護グループから別の保護グループに仮想マシンを移動するには、次の手順を実行します。 1. 仮想マシンの保護を解除します。 **[レプリケーション（Replication）]** > **[保護済み仮想マシン（Protected Virtual Machines）]** タブから、仮想マシンを選択し、**[保護解除（Unprotect）]** をクリックします。 これにより、仮想マシンのすべての保護が解除されます。 2. 新しい保護グループを選択して、仮想マシンを再保護します。 **[仮想マシン（Virtual Machines）]** から、仮想マシンを選択し、**[保護（Protect）]** をクリックします。

保護済み仮想マシンのテーブル

UI 要素	基本的な情報
# selected カラム	テーブルから選択された仮想マシンのチェックボックスの数。実行されたアクションは、選択したすべての仮想マシンに適用されます。
[仮想マシン名（Virtual Machine Name）] カラム	HX ストレージ クラスタ のレプリケーションによって保護されている仮想マシンの名前。

UI 要素	基本的な情報

[保護ステータス（Protection Status）] カラム	仮想マシン保護の最新の保護アクション。ステータスの矢印は、データ送信の方向を示します。
	方向矢印はデータ伝送を示します。
	• **[左から右（Left to Right）]**：ローカル クラスタからリモート クラスタに複製されます。
	• **[右から左（Right to Left）]**リモート クラスタからローカル クラスタに複製されます。
	保護ステータスのオプションは次のとおりです。
	• **[アクティブ（Active）]**：仮想マシンはレプリケーション用に設定され、定義された間隔でレプリケーションが実行されます。追加情報が表示される場合があります。
	  • **[保護済み（Protected）]**：仮想マシンにレプリケーション スケジュールがあります。
	  • **[一時停止（Paused）]**：仮想マシンのレプリケーションスケジュールは一時的に停止しています。これはクラスタのメンテナンス時に使用されます。
	  • **[無効（Invalid）]**：仮想マシンのレプリケーション設定にエラーがあります。
	  • **[進行中（In Progress）]**：仮想マシンのスケジュールされたレプリケーションが進行中です。
	  • **[エラー（Error）]**：この仮想マシンのレプリケーション タスクは完了しませんでした。
	  • **[削除済み（Deleted）]**：レプリケーション スナップショットがリモート クラスタから削除されました。
	  • **[なし（None）]**：この仮想マシンのレプリケーションはスケジュールされていません。
	• **[超過間隔（Exceeds Interval）]**：最後のレプリケーションプロセスが、設定された間隔より長くかかりました。
	• **[停止（Halted）]**：仮想マシンのレプリケーションスケジュールは停止しています。これにより、破損した可能性のある仮想マシン（ディザスタ リカバリの状態）がリモート クラスタに複製されるのを防ぎます。
	• **[リカバリ済み（Recovered）]**：仮想マシンは、リモート クラスタのレプリケーション スナップショットから最近復元されました。

UI 要素	基本的な情報
[前回の保護時刻（Last Protection Time）] カラム	最新の仮想マシン レプリケーション プロセスが開始されたときのタイムスタンプ。
[Direction (ディレクション)] カラム	複製された仮想マシンの方向。方向は、ローカル クラスタを基準にしています。ログイン中のクラスタは、常にローカル クラスタとしてのログインになります。次のオプションがあります。 • **[受信（Incoming）]**：仮想マシンはリモート クラスタに存在します。リモート クラスタからローカル クラスタに複製されます。 • **[発信（Outgoing）]**：仮想マシンはリモート クラスタに存在します。ローカル クラスタからリモート クラスタに複製されます。
[保護グループ（Protection Status）] カラム	関連付けられた仮想マシンが保護グループに属している場合は、保護グループ名が表示されます。保護グループがない場合は、フィールドに-と表示されます。.
[間隔（Interval）] カラム	仮想マシンを複製するために設定された間隔設定。これを変更するには、仮想マシンの行を選択し、**[スケジュールの編集（Edit Schedule）]** をクリックします。

[保護仮想マシン スケジュールの編集（Edit Protected Virtual Machine Schedule）] ダイアログボックス

選択した仮想マシンのレプリケーションのレプリケーション間隔またはVMwareツールの休止設定を変更します。

[レプリケーション（Replication）] > **[保護仮想マシン（Protected Virtual Machines）]** > **[スケジュールの編集（Edit Schedule）]** を選択します。

UI 要素	基本的な情報
[この仮想マシンを次の間隔で保護（Protect this virtual machine every）] フィールド	ペアになっているクラスタに仮想マシンをレプリケートする頻度を選択します。デフォルトは、1 時間ごとです。プルダウン メニューには次のオプションがあります。 15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェックボックス	レプリケーション スナップショットを取る前に、HX データ プラットフォームで仮想マシンを休止するには、このチェックボックスをオンにします。 この設定は、VMware ツールがインストールされている仮想マシンにのみ適用されます。

[変更の保存（Save Changes）]をクリックします。

HX データ プラットフォーム により、間隔と保護グループの Vmware ツール静止設定を更新します。新しい間隔頻度を表示するには**[保護グループ（Protection Groups）]** タブを参照してください。

保護グループ

[保護グループの作成（Create Protection Group）] ダイアログボックス

[レプリケーション（Replication）] > **[保護グループ（Protection Groups）]** > **[新規グループの追加（+ New Group）]** の順に選択します。

[保護グループの作成（Create Protection Group）] ダイアログボックス

UI 要素	基本的な情報
[保護グループ名（Protection Group Name）] フィールド	この HX クラスタの新しい保護グループの名前を入力します。 保護グループは、HX クラスタに一意です。名前はリモート クラスタで参照されますが、リモート HX クラスタでは編集できません。各 HX クラスタには複数の保護グループを作成できます。
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	ペアになっているクラスタに仮想マシンをレプリケートする頻度を選択します。 プルダウン メニュー オプション: 5 分、15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間デフォルト値は 1 時間です。
[仮想マシンの保護をすぐに開始（Start protecting the virtual machines immediately）] オプション ボタン	この保護グループに最初の仮想マシンを追加した後、すぐに最初のレプリケーションを開始するには、このオプション ボタンを選択します。

UI 要素	基本的な情報
[仮想マシンの保護の開始時間（Start protecting the virtual machines from）] オプション ボタン	最初のレプリケーション操作を開始する特定の時間を設定する場合は、このラジオ ボタンを選択します。 レプリケーションを開始する前に、次のことを確認してください。 • 少なくとも 1 つの仮想マシンが保護グループに追加されている。 • スケジュールされた開始時刻に達している。 保護の開始時間を指定するには、次の手順に従います。 1. **[仮想マシンの保護の開始時間（Start protecting the virtual machines from）]** オプション ボタンをオンにします。 2. [時刻（time）] フィールドをクリックし、時間と分を選択します。時刻を選択した後、フィールドの外をクリックします。 **[クラスタのタイムゾーン（Cluster time zone）]** と **[クラスタの現在時刻（Current time on cluster）]** を参照すると、適切なレプリケーションの開始時刻を選択するのに役立ちます。開始時間は、ローカル クラスタの時計に基づいています。次に例を示します。 クラスタの現在時刻が午後 1:56:15 である場合、「現在から 10 時間 3 分後」は、午後 11:59:00 に最初のレプリケーションが発生することを意味します。 *[現在からの時間と分（hours, minutes from now）]* は、最初のレプリケーションがいつ行われるかを示します。これは、[時刻（time）] フィールドの設定値を変更すると更新されます。
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェック ボックス	静止 DP スナップショットを作成するには、このチェックボックスをオンにします。このチェックボックスをオフのままにすると、一貫性のある DP スナップショットがクラッシュします。 この設定は、VMware ツールがインストールされている仮想マシンにのみ適用されます。

[保護グループの作成（Create Protection Group）] をクリックします。

HX データ プラットフォーム で **[保護グループ（Protection Group）]** タブに新しいグループが追加されます。VM の数はゼロ（0）であることに注意してください。仮想マシンをこの新しい保護グループに追加し、この保護グループに設定されたレプリケーション スケジュールを適用する必要があります。

[保護グループのスケジュールの編集（Edit Protection Group Schedule）] ダイアログボックス

保護グループ内の仮想マシンのレプリケーション間隔を変更します。

[複製（Replication）] > [保護グループ（Protection Groups）] > [スケジュールの編集（Edit Schedule）] を選択します。

UI 要素	基本的な情報
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	プルダウン リストを使用して、仮想マシンがペアになっているクラスタにレプリケートされる頻度を選択します。 リストの値: 5 分、15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェックボックス	停止した DP スナップショットを作成するには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。チェックボックスをオフのままにすると、クラッシュの整合性のある DP スナップショットが取得されます。 これは、VMware ツールがインストールされている仮想マシンにのみ適用されます。

[変更を保存（Save Changes）] をクリックして、保護グループの間隔と VMware ツールの静止設定を保存します。間隔の頻度を確認するには、[保護グループ（Protection Groups）] タブを参照してください。

保護グループ ダイアログ ボックスへの追加

UI 要素	基本的な情報
[既存の保護グループに追加（Add to an existing protection group）] ドロップダウン リスト	保護グループを選択し、保護グループに保護されている仮想マシンを追加する場合にクリックします。

[Save Changes]をクリックします。

[レプリケーション ペア（Replication Pairs）] タブ

[レプリケーション ペア（Replication Pairs）] タブから、ローカル クラスタとリモート クラスタのデータストアを選択してレプリケーションペアを作成、編集、または削除し、レプリケーションペアのステータスを表示できます。レプリケーションペアを展開して、このレプリケーション ペアによって保護されている仮想マシンのリストを表示することもできます。

レプリケーション ペアは、保護ネットワークの半分を 2 つ定義します。ログインしている HX ストレージ クラスタ はローカル クラスタで、ペアの片方です。レプリケーション ペアを設定する場合は、ペアのもう片方である別の HX ストレージ クラスタ を指定します。ストレージ コンポーネントを確保するために、レプリケーションペアを各 HX ストレージクラスタ のデー

タストアにマップします。レプリケーションペアを設定したら、仮想マシンの保護を開始できます。**[仮想マシン（Virtual Machines）]** タブを参照してください。

レプリケーション ペアのアクション

UI 要素	基本的な情報
レプリケーション ペアの作成	ローカル ストレージ クラスタとリモート ストレージ クラスタ間の接続を確立します。 **前提条件**：ローカル クラスタとリモート クラスタの両方でデータストアを作成します。ローカルクラスタとリモートクラスタの両方でレプリケーション ネットワークを構成します。 **[レプリケーション ペアの作成（Create Replication Pair）]** をクリックし、ウィザードを完了します。
[Edit（編集）] ボタン	レプリケーション ペア名を割り当てらてたデータストアを変更します。 レプリケーション ペアを選択し、**[編集（Edit）]** をクリックします。
[削除（Delete）] ボタン	ローカルクラスタとリモートクラスタ間のレプリケーション ペアを削除します。 **前提条件**：すべての依存関係を削除：すべての仮想マシンから保護を削除します。データストアのマッピングを削除します。 レプリケーション ペアを選択し、**[削除（Delete）]** をクリックします。

レプリケーション ペアのテーブル

UI 要素	基本的な情報
[名前（Name）] カラム	このクラスタのレプリケーション ペア名。
[リモート クラスタ（Remote Cluster）] カラム	このレプリケーション ペアのリモート クラスタ名。

UI 要素	基本的な情報
[リモート クラスタ ステータス（Remote Cluster Status）] カラム	リモート クラスタの現在のステータスを表示します。これは、一般的なクラスタステータスとは異なります。次のオプションがあります。 • **オンライン** • **オフライン** • **Upgrading** • **スペース不足** • **シャットダウン** • **不明（Unknown）**
[VM 発信（VMs Outgoing）] カラム	保護されている仮想マシンの数とローカル クラスタ上の保護グループの数。番号をクリックして発信**ローカル VM** を表示します。
[レプリケーションの発信（Replications Outgoing）] カラム	ローカルクラスタからリモートクラスタに複製される保護対象の仮想マシンの複製スナップショットの数。
[VM 受信（VMs Incoming）] カラム	リモートクラスタ上の保護された仮想マシンの数と保護グループの数。番号をクリックして発信**リモート VM** を表示します。
[レプリケーション受信（Replications Incoming）] カラム	リモートクラスタからローカルクラスタに複製されている保護された仮想マシンのスナップショットの数。
[マッピングされたデータストア ペア（Mapped Datastore Pairs）] カラム	このレプリケーション ペアにマッピングされたデータストアの数。番号をクリックして **[データストア（Datastores）]** ページを表示します。

[レプリケーション ペア（Replication Pairs）] の詳細テーブル

レプリケーション ペアの **[名前（Name）]** をクリックして、詳細テーブルを表示します。

UI 要素	基本的な情報
[仮想マシン名（Virtual Machine Name）] カラム	HX ストレージ クラスタ のレプリケーションによって保護されている仮想マシンの名前。

UI 要素	基本的な情報
[保護ステータス（Protection Status）] カラム	

UI 要素	基本的な情報

	仮想マシン保護の最新の保護アクション。ステータスの矢印は、データ送信の方向を示します。
	
	方向矢印はデータ伝送を示します。
	
	• **[左から右（Left to Right）]**：ローカル クラスタからリモート クラスタに複製されます。
	
	• **[右から左（Right to Left）]**リモート クラスタからローカル クラスタに複製されます。
	
	保護ステータスのオプションは次のとおりです。
	
	• **[アクティブ（Active）]**：仮想マシンはレプリケーション用に設定され、定義された間隔でレプリケーションが実行されます。追加情報が表示される場合があります。
	
	  • **[保護済み（Protected）]**：仮想マシンにレプリケーション スケジュールがあります。
	
	  • **[一時停止（Paused）]**：仮想マシンのレプリケーションスケジュールは一時的に停止しています。これはクラスタのメンテナンス時に使用されます。
	
	  • **[無効（Invalid）]**：仮想マシンのレプリケーション設定にエラーがあります。
	
	  • **[進行中（In Progress）]**：仮想マシンのスケジュールされたレプリケーションが進行中です。
	
	  • **[エラー（Error）]**：この仮想マシンのレプリケーション タスクは完了しませんでした。
	
	  • **[削除済み（Deleted）]**：レプリケーション スナップショットがリモート クラスタから削除されました。
	
	  • **[なし（None）]**：この仮想マシンのレプリケーションはスケジュールされていません。
	
	• **[超過間隔（Exceeds Interval）]**：最後のレプリケーションプロセスが、設定された間隔より長くかかりました。
	
	• **[停止（Halted）]**：仮想マシンのレプリケーションスケジュールは停止しています。レプリケーションスケジュールを停止することにより、（ディザスタ リカバリの状態にある）破損した可能性のある仮想マシンがリモート クラスタに複製されるのを防ぎます。
	
	• **[リカバリ済み（Recovered）]**：仮想マシンは、リモート クラスタのレプリケーション スナップショットから最近

UI 要素	基本的な情報
	復元されました。
[前回の保護時刻（Last Protection Time）] カラム	最新の仮想マシン レプリケーション プロセスが開始されたときのタイムスタンプ。
[Direction (ディレクション)] カラム	複製された仮想マシンの方向。方向は、ローカル クラスタを基準にしています。ログイン中のクラスタは、常にローカル クラスタとしてのログインになります。次のオプションがあります。 • **[受信（Incoming）]**：仮想マシンはリモート クラスタに存在します。リモート クラスタからローカル クラスタに複製されます。 • **[発信（Outgoing）]**：仮想マシンはリモート クラスタに存在します。ローカル クラスタからリモート クラスタに複製されます。
[保護グループ（Protection Status）] カラム	関連付けられた仮想マシンが保護グループに属している場合は、保護グループ名が表示されます。保護グループがない場合、フィールドには **[なし（None）]** と表示されます。
[間隔（Interval）] カラム	仮想マシンを複製するために設定された間隔設定。間隔を変更するには、仮想マシンの行を選択し、**[スケジュールの編集（Edit Schedule）]** をクリックします。

[新しいレプリケーション ペアの作成（Create New Replication Pair）] ウィザード

レプリケーション ペアは、保護ネットワークの半分を 2 つ定義します。ログインしている HX ストレージ クラスタ はローカル クラスタで、ペアの片方です。レプリケーション ペアを設定する場合は、ペアのもう片方である別の HX ストレージ クラスタ を指定します。ストレージ コンポーネントを確保するには、複製ペアを作成し、最初にデータストアの半分をペアのもう半分にマッピングします。複製ペアが設定され、データストアがマップされたら、仮想マシンを保護できるようになります。**[仮想マシン（Virtual Machines）]** タブを参照してください。

前提条件

- DRO 保護を有効にするには、HXDP リリース 5.5(1a) 以前を使用している必要があります。
- ローカル クラスタとリモート クラスタの両方でデータストアを作成します。
- レプリケーション ネットワークを構成します。

[レプリケーション ペア（Replication）] ウィザードを開始します。

管理者権限を持つユーザーとしてローカルまたはリモート クラスタのいずれかにログインし、次のうちいずれかを実行します。

- 始めてクラスタ ペアリングを行う場合、**[Replication (レプリケーション)]** > **[Pair Cluster (クラスタのペアリング)]** を選択します。
- **[Replication (レプリケーション)]** > **[Create Replication Pair (レプリケーション ペアの作成)]** を選択します。

  [Create Replication Pair (複製ペアの作成)] オプションは、すべての VM の保護を解除し、すべての依存関係を削除した後に、既存の複製ペアを削除するときにのみ有効です。

[名前（Name）] ページ

UI 要素	基本的な情報
[レプリケーションペアの名前（Replication Pair Name）] フィールド	2 つの HX ストレージ クラスタの間のレプリケーション ペアの名前を入力します。この名前は、ローカルおよびリモートの両方のクラスタに設定されます。この名前は変更できません。

[次へ（Next）] をクリックします。

[リモート接続（Remote Connection）] ページ

UI 要素	基本的な情報
[管理 IP または FQDN（Management IP or FQDN）] フィールド	リモートの管理ネットワークの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。たとえば、*10.10.10.10* とします。
[ユーザ名（User Name）] および **[パスワード（Password）]** フィールド	リモート HX クラスタの vCenter シングル サインオンまたはクラスタ固有の管理者クレデンシャルを入力します。

[ペアリング（Pair）]をクリックします。

HX データ プラットフォーム はリモート HX ストレージ クラスタ を確認し、レプリケーション ペア名を割り当てます。

（注） 保護される仮想マシンは、レプリケーション ペアのデータストアのいずれか 1 つに存在している必要があります。

[Create New Replication (新しい複製の作成)] ページ > データストアのマップ: ネイティブ保護

（注）
- 選択したデータストア上に、保護する仮想マシンが存在している必要があります。レプリケーションペア用に構成されたデータストアから仮想マシンを移動すると、その仮想マシンの保護も解除されます。
- ペアリングされた別のデータストアへの仮想マシンの移動は、サポートされています。ペアリングされていないデータストアに VM を移動すると、レプリケーション スケジュールが失敗します。

To protect VMs using the HX データ プラットフォーム 障害復旧機能を使用して VM を保護するには、**[Native Protection (ネイティブ保護)]** をクリックし、次を行います。

UI 要素	基本的な情報
[ローカル データストア（Local Datastore）] カラム	このクラスタ（ローカル HX ストレージ クラスタ）で構成されているデータストアのリスト。 1 つのローカル データストアを 1 つのリモート データストアにマップします。
[リモート データストア（Remote Datastore）] カラム	HX ストレージ クラスタ 間でデータストアをペアリングします。 該当する **[ローカル データストア（Local Datastore）]** 行で、**[リモート データストア（RemoteDatastore）]** プルダウン メニューからデータストアを選択します。これにより、単一の操作でリモートとローカルの両方のデータストアが選択されます。

[Map Datastore] をクリックします。

[Create New Replication (新しい複製の作成)] ページ > データストアのマップ: その他の DRO 保護

前提条件

- HXDP リリース 5.5(1a) 以前を使用している必要があります。

Disaster recovery orchestrator (DRO) で SRM を使用して VM を保護するには、**[Other DRO Protection (その他の DRO 保護)]** をクリックし、次の手順を実行します。

UI 要素	基本的な情報
[ローカル データストア（Local Datastore）] カラム	このクラスタ（ローカル HX ストレージ クラスタ）で構成されているデータストアのリスト。 1 つのローカル データストアを 1 つのリモート データストアにマップします。

UI 要素	基本的な情報
[リモート データストア（Remote Datastore）] カラム	HX ストレージ クラスタ 間でデータストアをペアリングします。 該当する **[ローカル データストア（Local Datastore）]** 行で、**[リモート データストア（RemoteDatastore）]** プルダウン メニューからデータストアを選択します。これにより、単一の操作でリモートとローカルの両方のデータストアが選択されます。
[Direction (ディレクション)] カラム	マップされたデータストア ペアの VM の移動方向に従って、**[Incoming (受信)]** または **[Outgoing (送信)]** を選択します。
[Protection Schedule (保護スケジュール)] カラム	データストアですべての VM を保護するスケジュールを選択します。

[Map Datastore] をクリックします。

（注）
- 他の DRO の下にあるデータストア内の VM は、SRM によって保護されます。
- 新しい VM が他の DRO によって保護されているデータストアに追加されると、新しく追加された VM は Cisco HyperFlex によって自動的に保護されます。ネイティブ DRO を使用して保護されたデータストアに VM を追加する場合は、VM を保護する必要があります。

  [Other DRO Protection (その他の DRO 保護)] の下で編集された複製ペアは、SRM に表示されます。

[レプリケーションペアの編集（Edit Replication Pair）] ダイアログボックス

レプリケーション ペアのデータストアの変更

ローカル クラスタとリモート クラスタでレプリケーション ペアに使用するデータストアを変更します。レプリケーション ペアを作成した後、その名前を変更することはできません。

（注） レプリケーションペアで使用されているデータストアを変更すると、ローカルおよびリモートクラスタの両方ですべての仮想マシンから保護が削除されます。

このタスクを行うユーザには、管理者権限が必要です。

1. 保護されたすべての仮想マシンの保護を解除します。これには、個別に保護された仮想マシンと保護グループを通して保護された仮想マシンの両方が含まれます。ローカル クラスタとリモート クラスタの両方で、保護の解除操作を行います。

   [Replication (複製)] > **[Local VMs (ローカル VM)]** > ***[virtual_machine (仮想マシン)]*** > **[Unprotect (保護しない)]** を選択します。

2. **[Replication]** > **[Replication Pairs]** > ***[replication_pair]*** > **[Edit]** を選択します。

   HX データ プラットフォーム ディザスタ リカバリ機能によって保護されている複製ペアを編集するには、**[Native Protection (ネイティブ保護)]** タブをクリックし、次の手順を実行します。

UI 要素	基本的な情報
[ローカル データストア（Local Datastore）] カラム	このクラスタ、ローカル HX クラスタであるこのクラスタに構成されたデータストアの一覧です。 1 つのローカル データストアを 1 つのリモート データストアにマップします。 （注） データストア名の横にあるロック/ロック解除アイコンは、データストアの暗号化が有効か無効かを示します。 • ロック アイコン：暗号化が有効 • ロック解除アイコン：暗号化が無効 暗号化されたローカル データストアが選択されている場合、暗号化されたリモート データストア情報のみが表示されます。
[リモート データストア（Remote Datastore）] カラム	HX クラスタ間でデータストアをペアリングします。 1. ローカル データストアの選択を変更するには、現在のローカル データストアへのマッピングを削除します。 **[Remote Datastore (リモート データストア)]** 列のプルダウン メニューで、**[Do not map this datastore (このデータストアをマップしない)]** を選択します。 2. 該当する **[ローカル データストア（Local Datastore）]** 行で、**[リモート データストア（RemoteDatastore）]** プルダウン メニューからデータストアを選択します。これにより、単一の操作でリモートとローカルの両方のデータストアが選択されます。

Disaster recovery orchestrator (DRO) で SRM を使用して VM を保護するには、その他の DRO 保護を有効にするに [1] で、**[Other DRO Protection (その他の DRO 保護)]** タブをクリックし、次の操作を行います。

[1] HXDP リリース 5.5(1a) 以前を使用する必要があります。

UI 要素	基本的な情報
[ローカル データストア（Local Datastore）] カラム	このクラスタ、ローカル HX クラスタであるこのクラスタに構成されたデータストアの一覧です。 1 つのローカル データストアを 1 つのリモート データストアにマップします。 （注） データストア名の横にあるロック/ロック解除アイコンは、データストアの暗号化が有効か無効かを示します。 • ロック アイコン：暗号化が有効 • ロック解除アイコン：暗号化が無効 暗号化されたローカル データストアが選択されている場合、暗号化されたリモート データストア情報のみが表示されます。
[リモート データストア（Remote Datastore）] カラム	HX クラスタ間でデータストアをペアリングします。 **1.** ローカル データストアの選択を変更するには、現在のローカル データストアへのマッピングを削除します。 **[Remote Datastore (リモート データストア)]** 列のプルダウン メニューで、**[Do not map this datastore (このデータストアをマップしない)]** を選択します。 **2.** 該当する **[ローカル データストア（Local Datastore）]** 行で、**[リモート データストア（RemoteDatastore）]** プルダウン メニューからデータストアを選択します。これにより、単一の操作でリモートとローカルの両方のデータストアが選択されます。
[Direction (ディレクション)] カラム	マップされたデータストア ペアの VM の移動方向に従って、**[Incoming (受信)]** または **[Outgoing (送信)]** を選択します。
[Protection Schedule (保護スケジュール)] カラム	データストアですべての VM を保護するスケジュールを選択します。

3. [Finish] をクリックします。
4. 再度、仮想マシンを保護します。**[Virtual Machines]** > **[virtual_machines]** > **[Protect]** を選択します。

[ペア クラスタ ネットワークのテスト（Test Pair Cluster Network）] ダイアログ ボックス

UI 要素	基本的な情報
[MTU] フィールド	デフォルト値は1500 です。 テストを実行するレプリケーションネットワークのMTUを入力します。 • HXDP リリース 5.0（2a）以降では、クラスタの設定後にMTU 値を編集できます。古いバージョンの HXDP では、既存のレプリケーション ネットワーク構成を削除する必要があります。レプリケーション ネットワークは、正しい MTU 値で設定できます。

[テストの実行（Run Test）] をクリックして、リモート レプリケーション ネットワーク内のクラスタ間のクラスタ ペアリングをテストします。

[レプリケーションペアの削除（Delete Replication Pair）] ダイアログボックス

レプリケーションのペアを削除する際の前提条件

レプリケーション ペアから依存関係を削除します。ローカル クラスタとリモート クラスタの両方の前提条件を満たします。

1. 保護されたすべての仮想マシンの保護を解除します。これには、個別に保護された仮想マシンと保護グループを通して保護された仮想マシンの両方が含まれます。ローカル クラスタとリモート クラスタの両方で、次の手順に従います。

   [レプリケーション（Replication）] > [保護された仮想マシン（Protected Virtual Machines）] > *[virtual_machine]* > [保護の解除（Unprotect）] の順に選択します。

2. ローカル クラスタとリモート クラスタのいずれかから、データストア マッピングを削除します。

   1. **[レプリケーション（Replication）] > [レプリケーション ペア（Replication Pairs）] > *[replication_pair]* > [編集（Edit）]** の順に選択します。
   2. [リモート データストア（Remote Datastore）] プルダウン メニューから、[このデータストアをマッピングしない（Do not map this datastore）] を選択します。
   3. [Finish] をクリックします。

レプリケーションペアの削除

ローカル クラスタとリモート クラスタでレプリケーション ペアを削除します。

このタスクを行うユーザには、管理者権限が必要です。

1. **[レプリケーション（Replication）] > [レプリケーション ペア（Replication Pairs）] > *[replication_pair]* > [削除（Delete）]** の順に選択します。

2. [レプリケーションペアの削除（Delete Replication Pair）] ダイアログボックスで必要な値を入力します。

UI 要素	基本的な情報
[ユーザ名（User Name）] フィールド	リモート HX ストレージ クラスタの管理者ユーザ名を入力します。
[パスワード（Password）] フィールド	リモート HX ストレージ クラスタの管理者パスワードを入力します。

3. レプリケーション ペアの削除を確定して [削除（Delete）] をクリックします。

[リカバリ設定（Recovery Settings）] ダイアログ ボックス

リカバリ設定の編集

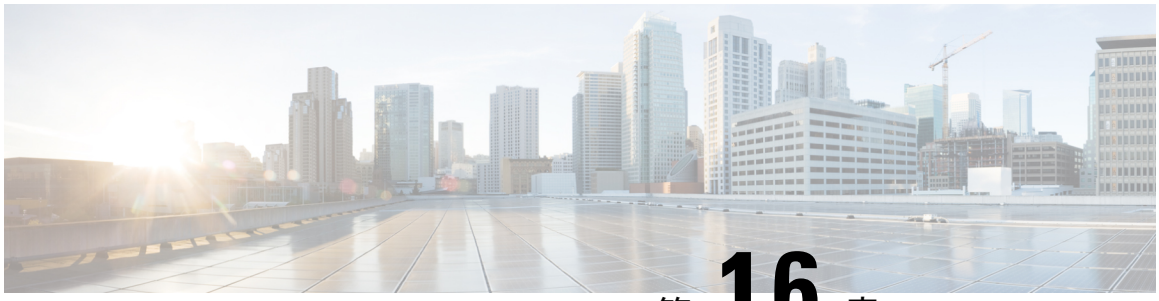
（注） このタスクを実行するには、管理者権限を持つユーザとしてログインする必要があります。

1. **[ネットワーク設定の編集（Edit Network Configuration）]** ダイアログ ボックスのフィールドに記入します。

UI 要素	基本的な情報
[仮想マシンの電力状態（Virtual Machine Power State）] オプション ボタン	ネットワークが既知の動作状態に戻るときのリソースの電源状態を指定します。
[仮想マシン名のプレフィックス テスト（Test Virtual Machine Name Prefix）] フィールド	（オプション）リソースのタイプとコンテキストを識別する共通プレフィックスを使用します。
[通知設定（Notification Setting）] オプション ボタン	回復イベント後に送信される通知プロンプトのタイプを選択します。 • リカバリ、テストリカバリ、または移行時に設定の概要を確認するプロンプトを表示するには、**[通常モード（Normal Mode）]** を選択します。 確認プロンプトを表示しないようにするには、**[サイレント モード（Silent Mode）]** を選択します。

UI 要素	基本的な情報
[リカバリ マッピング（Recovery Mappings）] フィールド	リカバリおよびテストリカバリ操作中に使用されるフォルダ、ネットワーク、またはリソース プール パラメータによって、グローバル リカバリ パラメータとリカバリ サイト全体のリソースのマッピングを定義します。パラメータ タイプをクリックして、設定フィールドを表示します。次の手順を実行します。 **リカバリ設定** • **ルール**：設定されているリカバリルールの数。この値は編集できません。 • **[ロケール（Locale）]** ドロップダウン リスト • **[リモート（Remote）]** ドロップダウン リスト **リカバリ設定のテスト** • **[リカバリ設定と同じ]** チェックボックス • **[ロケール（Locale）]** ドロップダウン リスト • **[リモート（Remote）]** ドロップダウン リスト
[ルールの追加（Add Rule）] ボタン	クリックして追加ルールを追加します。デフォルト値は 0 です。
[ごみ箱（Trash）] アイコン	[ごみ箱（Trash）] アイコンをクリックして削除します。

2. **[Save Changes]**をクリックします。



第 16 章

ユーザーの管理

Cisco HyperFlex ユーザー管理の概要

HX Data Platform でアクションを実行したり、コンテンツを表示できるユーザーのタイプには次のものがあります。

- **admin**：Cisco HX Data Platform に含まれている定義済みユーザー。パスワードは HX Data Platform の作成時に設定されます。同じパスワードが `root` にも適用されます。このユーザには読み取り権限と変更権限が付与されます。
- **root**：Cisco HX Data Platform に含まれている定義済みユーザー。パスワードは HX Data Platform の作成時に設定されます。同じパスワードが `admin` にも適用されます。このユーザには読み取り権限と変更権限が付与されます。
- ***administrator***：作成された Cisco HX Data Platform ユーザー。このユーザは vCenter で作成され、RBAC ロール `administrator` がこれに割り当てられます。このユーザには読み取り権限と変更権限が付与されます。パスワードは、ユーザの作成時に設定されます。
- ***read-only***：作成された Cisco HX Data Platform ユーザー。このユーザは vCenter で作成され、RBAC ロール `read-only` がこれに割り当てられます。このユーザには読み取り権限だけが付与されます。パスワードは、ユーザの作成時に設定されます。
- ***diag***：Cisco HX Data Platform に含まれている定義済みユーザー。パスワードは HX Data Platform の作成時に設定されます。同じパスワードが admin にも適用されます。このユーザには読み取り権限と変更権限が付与されます。

HX インターフェイス	admin	root	*hx_admin*	*hx_readonly*	*diag*
HX Data Platform インストーラ	必須	無効	無効	無効	無効
HX 接続	ほとんどの HX タスクを実行できます。	無効	ほとんどの HX タスクを実行できます。 優先されるユーザです。	モニタリング情報のみを表示できます。 HX のタスクを実行することはできません。 優先されるユーザです。	無効
ストレージ コントローラ VM の `hxcli` コマンド ライン	ほとんどの HX タスクを実行できます。	ほとんどの HX タスクを実行できます。	ログインする際は、`local/` プレフィックスが必要です。例： `vc-hx_admin`	HX のタスクを実行することはできません。 ログインする際は、`local/` プレフィックスが必要です。例： `vc-hx_readonly`	ほとんどの HX タスクを実行できます
vCenter を介した HX Data Platform プラグイン	ほとんどの HX タスクを実行できます。	無効	無効	無効	無効
HX REST API	ほとんどの HX タスクを実行できます。	無効	無効	無効	無効

ユーザ管理の用語

- **認証**：ログイン クレデンシャルに関する処理。これらのプロセスは、通常、ユーザ名とパスワードに基づいて、指定されたユーザのユーザ クレデンシャルを確認します。一般に、認証によってユーザ クレデンシャルを確認し、認証されたユーザにセッションを関連付けます。

- **承認**：アクセス権限に関する処理。これらのプロセスでは、ユーザのアイデンティティに基づき、ユーザ/クライアントアプリケーションに対して、管理対象エンティティの作成、読み取り、更新、削除、あるいはプログラムの実行などのアクションを許可します。承認により、認証済みユーザがサーバ上で何を実行できるかが定義されます。
- **アカウンティング**：ユーザ アクションの追跡に関する処理。これらのプロセスでは、レコードを保持し、ログインセッションおよびコマンドの実行を含むユーザ操作を追跡します。情報はログに保存されます。これらのログは、Cisco HX 接続 または他の Cisco HX データ プラットフォーム インターフェイスを通じて生成することができるサポート バンドルに含まれます。
- **アイデンティティ（ID）**：ユーザ個人にアイデンティティが与えられ、特定の権限を持つロールがそれに割り当てられます。
- **権限**：リソースを使用するためにロールに与えられる設定。これは、ロールと、リソースおよびリソースによって公開される機能との間のリンクです。たとえば、データストアはリソースであり、変更ロールにはデータストアをマウントする権限が付与されますが、読み取り専用ロールでは単にそのデータストアの存在を表示できるだけです。
- **特権**：アイデンティティとアプリケーションの間のリンク。アプリケーションとの特定のインタラクションのコンテキストで使用されます。例：仮想マシンの電源をオンにする、データストアを作成する、データストアの名前を変更する。
- **リソース**：Cisco HX プラットフォーム全体であり、その機能および管理制御は、GET、POST、PUT、DELETE、HEAD などの HTTP 動詞を使用して HTTP 経由で公開されています。データストア、ディスク、コントローラ ノード、クラスタ属性はすべて、REST API を使ってクライアント アプリケーションに公開されるリソースです。
- **ロール**：権限レベルを定義します。各アプリケーション機能は、1 つまたは複数のロールによって実行される可能性があります。例：管理者、仮想マシン管理者、リソース プール管理者。ロールは特定の ID に割り当てられます。

AAA アカウンティングの監査ログ

AAA アカウンティングをサポートするため、Cisco HX データ プラットフォーム ではユーザ アクティビティの監査ログを実装しています。これらのログは、生成されたサポートバンドルに含まれます。

Cisco HX データ プラットフォーム を含む HX 接続 インターフェイスを介したサポート バンドルの生成については、『*Cisco HyperFlex システム トラブルシューティング ガイド*』を参照してください。

- **stMgrAudit.log**：`stcli` アクティビティの監査記録を含みます。

  サンプル エントリ。キーワード `Audit` に注意してください。

```
2017-03-27-22:10:02.528 [pool-1-thread-1] INFO Audit - 2017-03-27-03.10.02 127.0.0.1
 --> 127.0.0.1 POST /stmgr 200 : root 27ms
```

このファイルには、その他の情報も含まれます。監査イベントに絞り込むには、スクリプトを使用して単語 `Audit` をフィルタリングします。

- **audit.log**：REST API アクティビティの監査レコードが格納されます。

  サンプル エントリ。ユーザ名 `administrator@vsphere.local` に注意してください。

  ```
  2017-03-29-01:47:28.779 - 127.0.0.1 -> 127.0.0.1 - GET /rest/clusters 200;
  administrator@vsphere.local 454ms
  ```

Cisco HX データ プラットフォーム RBAC ユーザーの作成

Cisco HX は、管理者および読み取り専用の 2 種類のユーザーを HX データ プラットフォーム サポートしています。VMware vCenter インターフェイスを介して HX Data Platform の新しいユーザが作成されます。

始める前に

ユーザを作成するには、管理者特権が必要です。

手順

ステップ 1 vSphere Web クライアントに vCenter 管理者としてログインします。

ステップ 2 **[ナビゲーション ホーム（Navigator Home）]** から、**[管理（Administration）]** > **[ユーザとグループ（Users and Groups）]** > **[ユーザ（Users）]**。

ステップ 3 **[追加（Add）]**（+）アイコンをクリックして、ユーザを追加します。**[ユーザの新規作成（New User）]** の情報を入力し、**[OK]** をクリックします。

新しいユーザのユーザ名およびパスワードを指定します。

パスワードには、エスケープ文字（\）、ドル記号（$）、疑問符（?）、等号（=）を使用しないでください。ユーザ名に使用できる特殊文字は、アンダースコア（_）、ダッシュ（-）、ドット（.）のみです。ユーザー名とパスワードの要件に関する情報は、HX Data Platform の名前、パスワード、文字 （23 ページ） を参照してください。

次のタスク

RBAC ロール グループにユーザを追加します。「ユーザへの権限の割り当て （341 ページ）」を参照してください。

ユーザへの権限の割り当て

vCenterで、RBACを介してユーザーに特権が割り当てられます。特権を割り当てるには、ユーザを管理者グループまたは読み取り専用グループに追加します。

始める前に

ユーザを作成します。

手順

ステップ1 Cisco vSphere Web Client で、**[Navigator Home (ナビゲーション ホーム)]** > **[Administration (管理)]** > **[Global Permissions (グローバル権限)]** > **[Manage (管理)]** の順に選択します。

ステップ2 **[追加（Add）]**（+）アイコンをクリックし、ロールを割り当てます。

ステップ3 **[ロールの割り当て（Assigned Role）]** を選択します。

[グローバル権限ルート - 権限の追加（Global Permission Root - Add Permission）] ダイアログボックスで、**[ロールの割り当て（Assigned Role）]** ドロップダウン メニューから選択します。次のいずれかを選択します。

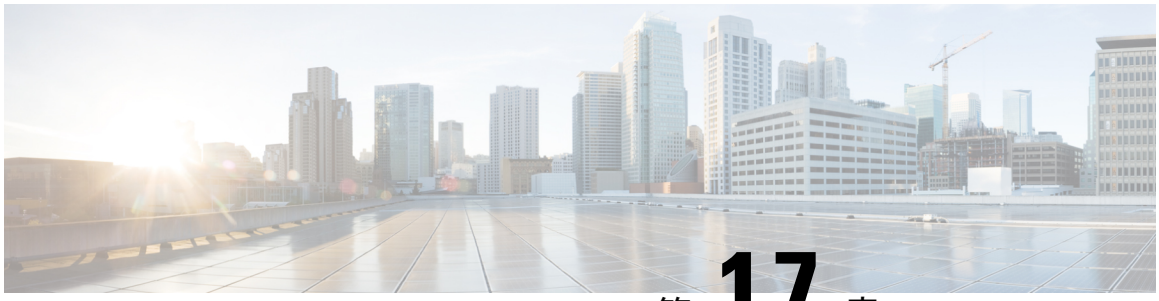
- **管理者**
- **読み取り専用（Read only）**

ステップ4 **[ユーザとグループ（Users and Groups）]** 領域で、**[追加（Add）]** をクリックします。

ステップ5 **[ユーザ/グループの選択（Select Users/Groups）]** ダイアログボックスで、*user_name* を選択し、**[追加（Add）]** をクリックします。

ステップ6 **[名前の確認（Check names）]** ボタンをクリックしてユーザ名を確認します。

ステップ7 **[OK]** をクリックして各ダイアログボックスを閉じます。



第 17 章

iSCSI の管理

（注） iSCSI 機能は、Cisco HyperFlex リリース 4.5（x）以降でサポートされています。

HyperFlex iSCSI ターゲット サービスの概要とサポートされる使用例

HyperFlex iSCSI ターゲット サービスは、HyperFlex 4.5（1a）で導入されます。HX iSCSI ターゲット サービスでサポートされる使用例は次のとおりです。

- Microsoft SQL Server や など、可用性の高い共有ストレージを必要とするアプリケーションに対して、Microsoft Failover Clusters などのフェールオーバ クラスタリングをサポートします。
- 外部コンピューティング ホスト上の Oracle データベースや Oracle RAC の展開など、HyperFlex クラスタの内部または外部で実行されているアプリケーションにブロック ストレージを提供します。
- iSCSI を介した Microsoft Exchange 展開のサポート

- HyperFlex Container Storage Interface for Kubernetes を使用した Kubernetes の永続ボリュームのプロビジョニング
- Edge および DC-No-FI への HX iSCSI サポートのサポートは、Cisco HX リリース 5.0(2a) で導入されました。

イニシエータは現在、Windows Server 2016、Windows Server 2019、Ubuntu 18.04 および 20.04、Oracle Linux 7、Red Hat Enterprise Linux 8.2、Red Hat Enterprise Linux 7 でサポートされています。

（注） HyperFlex iSCSI ターゲット サービスは、Stretched、 クラスタではサポートされません。

HyperFlex iSCSI のベスト プラクティス

HyperFlex で iSCSI を有効にする場合は、[ブースト モード（Boost Mode）] も有効にすることをお勧めします。ブースト モードを使用すると、Cisco HyperFlex クラスタでは、ストレージ コントローラの VMCPU リソースを 4vCPU 増やすことで、より高い IOP を実現し、iSCSI のパフォーマンスへの影響を軽減できます。ブースト モードの有効化または設定の詳細については、ブースト モード （75 ページ） を参照してください。

iSCSI 設定の概要

iSCSIターゲットサービスを設定するプロセスは次のとおりです。

- iSCSI ネットワークの作成
- iSCSI イニシエータ グループの作成
- iSCSI ターゲットの作成
- iSCSI イニシエータ グループをターゲットにリンク
- iSCSI LUN の作成
- iSCSI イニシエータの設定（Windows）
- iSCSI LUN のクローン作成

iSCSIのスケールとサポート

次に、iSCSIサポートの推奨事項について説明します。記載されている値は、シスコがテストしたもの、および最適なパフォーマンスを提供するものに基づいています。これらを「最大サポート」ガイドラインとして使用することを強く推奨します。

表 *13 : iSCSI*のスケールとサポートに関する推奨事項

スケール項目	HXDP のサポート
HyperFlexクラスタごとのiSCSI LUN	32,640
HyperFlex クラスタごとの iSCSI イニシエータ グループ	128
HyperFlexクラスタごとのiSCSIターゲット	128
ターゲットあたりのiSCSI LUN	255
最大iSCSI LUNサイズ	64 TB
コントローラVMあたりのiSCSIセッションの最大数	64
iSCSIセッションごとのiSCSI IOイニシエータキューの深さ	256
コントローラごとのiSCSI IOターゲット側キューの深さ	2,048

[iSCSI ネットワーク（iSCSI Network）] ページ

iSCSI ネットワークの設定情報を表示します。

iSCSI ネットワークデータ

iSCSI ネットワークをすでに設定している場合は、基本的なネットワーク情報が表示されます。

表 *14 : iSCSI* ネットワークデータ

UI 要素	説明
iSCSIの設定	iSCSI ネットワーク設定のステータス。設定されている場合、ステータスは「ネットワーク設定済み（Network Configured）」と表示されます。
LUN	作成された LUN の数。
使用済み容量	使用済み容量（GB単位）。
クラスタのキャパシティ使用率	LUN およびその他で使用されているクラスタ容量、および空きの割合。
ターゲット	iSCSI ターゲットのリストおよび設定情報。
イニシエータ グループ	iSCSI イニシエータ グループのリストおよび設定情報。

iSCSI ネットワークの作成

注意 新しい VLAN 設定には、IP アドレス範囲が必要です。この範囲は、クラスタにすでに存在していてはなりません。この要件に従わないと、クラスタが停止する可能性があります。

iSCSI ネットワークを作成するには、次の手順を実行します。

1. iSCSI ネットワークに必要な情報（**iSCSI ネットワーク**、**サブネット**、**ゲートウェイ**、**IP範囲**、**iSCSI ストレージ IP**、**デフォルト以外の MTU の設定**、および **VLAN設定**）を入力します。入力したら **[次へ]** をクリックします。
2. **[設定]** をクリックします。変更をキャンセルするには、**[キャンセル]** をクリックします。
3. **[確認]** をクリックして、iSCSI ネットワークを作成することを確認します。または、**[キャンセル]** をクリックして変更をキャンセルします。

（注） iSCSI ネットワークの作成を確認すると、一部の iSCSI ネットワーク パラメータについては、TAC の支援なしでは変更できなくなります。

（注） 1500 MTU（ジャンボ フレームなし）で hx-storage-data ネットワークを構成したが、（iSCSI ネットワークで推奨されているように）ジャンボ フレームを利用する場合は、9000MTU に HyperFlex クラスター内のすべての ESXi ホストで個別に hx-storage-datanetworkvswitch を編集する必要があります。

iSCSI ネットワーク設定データ

iSCSI ネットワークを作成するには、次の情報が必要です。

表 *15 : iSCSI* ネットワーク設定データ

UI 要素	説明
iSCSI ネットワーク	iSCSI ネットワークの設定情報を表示します。
サブネット	有効なサブネットを入力してください
ゲートウェイ	有効なゲートウェイを入力してください
IP範囲	有効な IP 範囲を入力します（この範囲は、iSCSI ストレージ IP を含んではなりません）

UI 要素	説明
iSCSI ストレージ IP	iSCSI ストレージの有効な IP アドレスを入力します（この IP アドレスは、IP 範囲フィールドで使用されたアドレスであってはなりません）
非デフォルト MTU の設定	MTU（メッセージトランスポートユニット）の手動設定を有効にするチェックボックス。MTU は、ネットワーク全体で 1 回のデータ伝送で送信できるネットワークフレームの最大サイズを定義します。デフォルト MTU サイズは 9000 です。 ジャンボ フレームを無効にするには、**[非デフォルト MTU を設定]**チェックボックスをクリックし、プルダウンを使用して値を 1500 に変更します。 （注） イニシエータのいずれかがルータを通過する場合、ルータはジャンボフレームを許可する必要があります。
VLAN 設定	**[新しい VLAN の作成**（推奨）] または **[既存の VLAN を選択]** のチェックボックスをクリックします。 新しい VLAN を作成するには、VLAN ID、VLAN 名、UCS Manager ホスト IP または FQDN、ユーザ名（UCS での認証のためのユーザ名）、パスワード（UCS での認証のためのパスワード）を指定する必要があります。 既存の VLAN を選択するには、VLAN ID を指定する必要があります。 （注） UCS-M で VLAN を手動で設定するには、[VLAN の作成] メニュー オプションを使用します。[Create VLANs] ウィンドウで、チェックボックスをそのままにします。HX の vNIC テンプレートで、VLAN を「vNIC Template storage-data-a」および「vNIC Template storage-data-b」に接続します。この設定は中断されません。

iSCSI ネットワークの編集

iSCSI ネットワーク設定を編集するには、次の手順を実行します。

1. **[アクション（Actions）]** メニューに移動し、**[ネットワークの編集（Edit Network）]** を選択します。<クラスタ名> に対応したネットワークの編集ウィンドウが表示されます。
2. iSCSIネットワークのIP範囲を追加します。
3. **[変更の保存（Save Changes）]** をクリックするか、変更を **[キャンセル（Cancel）]** します。

iSCSI ネットワークの削除

クラスタ上の iSCSI LUN、イニシエータ グループ、およびターゲットを保持したまま、iSCSI ネットワーク構成を削除および再構成できます。

iSCSIネットワーク設定を削除するには、以下の手順に従います。

1. **[アクション（Actions）]** メニューに移動し、**[ネットワークの削除（Delete Network）]** を選択します。[ネットワーク構成の削除（Delete Network Configuration）] ウィンドウが表示され、[ネットワーク構成を削除しますか?（Are you sure you want to delete Network Configuration?）] というプロンプトが表示されます。
2. [確認（Confirm）] をクリックするか、変更を[キャンセル（Cancel）] します。

（注） 「`hxcli iscsi network delete`」コマンドまたはAPIを使用すれば、iSCSI ネットワークを削除しながら、自分が設定したオブジェクトを保持するオプションを選択できます。詳細については、『CLI 参照ガイド』を参照してください。

iSCSI イニシエータ グループ

iSCSI イニシエータ グループの設定情報を表示します。

iSCSI イニシエータ グループのデータ

iSCSI イニシエータ グループを作成するには、次の情報が必要です。

表 16 : iSCSIイニシエータ グループのデータ

UI 要素	説明
名前	イニシエータ グループの名前。
イニシエータ IQN	イニシエータの iSCSI 修飾名（IQN）です。 IQN 形式は `iqn.yyyy-mm.naming-authority:unique name` の形式を取ります。

iSCSI イニシエータ グループの作成

iSCSI イニシエータ グループを作成するには、次の手順を実行します。

始める前に

iSCSI イニシエータ グループを作成する前に、iSCSI ネットワークの作成を作成しておく必要があります。

手順

ステップ 1 **[イニシエータ グループ]** タブに移動し、**[作成]** をクリックします。

[iSCSI イニシエータ グループの作成] ウインドウが表示されます。

ステップ 2 **[名前]** フィールドに、イニシエータ グループの名前を入力します。

ステップ 3 フィールドに **[イニシエータ IQN]** を入力します。イニシエータ IQN がわからない場合は、サーバから取得できます。

a) Windows の場合、Windows マシンにログインします。[サーバ マネージャ] に移動し、**[SCSI イニシエータ]** をクリックします。[設定（Configuration）] タブに移動します。イニシエータ IQN は **[イニシエータ名]** フィールドで徳k亭されます。

b) Linux の場合は、「`sudo cat /etc/iscsi/initiatorname.iscsi`」コマンドを入力します。イニシエータ IQN は **[イニシエータ名]** フィールドで徳k亭されます。

```
Cisco-Ubuntu:~$ sudo cat /etc/iscsi/initiatorname.iscsi
## DO NOT EDIT OR REMOVE THIS FILE!
## If you remove this file, the iSCSI daemon will not start.
## If you change the InitiatorName, existing access control lists
## may reject this initiator.  The InitiatorName must be unique
## for each iSCSI initiator.  Do NOT duplicate iSCSI InitiatorNames.
InitiatorName=iqn.2020-08.local.hx.green:Ubuntu-1

Cisco-Ubuntu:~$
```

イニシエータ名はファイル内にあり、適切な権限で変更できます。

ステップ 4 **[イニシエータの追加（Add Initiator）]** をクリックします。

（注） iSCSI VLAN サブネット外のイニシエータへのアクセスを許可するには、`hxcli iscsi allowlist` コマンドを使用します。次に例を示します。

```
hxcli iscsi allowlist add --ips 192.168.101.3
```

詳細については、お使いのリリースの『CLI ガイド、4.5』を参照してください。

ステップ 5 同じイニシエータ グループに参加する複数の IQN を追加するには、上記の手順を繰り返します。

ステップ 6 **[イニシエータ グループの作成（Create Initiator Group）]** をクリックします。

[イニシエータ グループ（Initiator Groups）] タブにイニシエータ グループが表示されます。

iSCSI イニシエータ グループの編集

iSCSI イニシエータ グループを編集するには、次の手順を実行します。

手順

ステップ 1 **[作成（Create）]** ボタンの横にある **[編集（Edit）]**（鉛筆）アイコンをクリックします。

[iSCSI イニシエータ グループの編集（Edit Initiator Group）] ウインドウが表示されます。

ステップ 2 iSCSI イニシエータ グループのデータを編集します。

ステップ 3 **[変更の保存（Save Changes）]** をクリックするか、変更を **[キャンセル（Cancel）]** します。

iSCSI イニシエータ グループの削除

iSCSI イニシエータ グループを削除するには、次の手順を実行します。

（注） ターゲットにリンクされている場合、iSCSIイニシエータグループは削除できません。

手順

ステップ 1 [イニシエータ グループの作成（Create Initiator Group）] ボタンの横にある [削除（Delete（X））]アイコンをクリックします。[iSCSI イニシエータ グループの削除（Delete Initiator Group）] ウインドウが表示されます。

ステップ 2 [Delete]をクリックします。 [Cancel]をクリックして変更をキャンセルします。

iSCSI イニシエータ グループをターゲットにリンク

iSCSI イニシエータ グループをリンクするには、次の手順を実行します。

始める前に

iSCSI イニシエータ グループの作成と iSCSI ターゲットの作成を作成したことを確認します。

手順

ステップ 1 **[ターゲット（Targets）]** タブに移動し、イニシエータ グループをリンクするターゲットの名前を選択します。

ステップ 2 **[リンクされたイニシエータ グループ（Linked Initiator Groups）]** タブで、**[リンク]** チェックボックスをオンにします。

[イニシエータ グループをリンク（Link Initiator Groups）] ウインドウが表示されます。

ステップ 3 ターゲットをリンクするイニシエータ グループを選択します。

ステップ 4 **[イニシエータ グループをリンク（Link Initiator Groups）]**をクリックします。

次のタスク

イニシエータ グループをターゲットにリンクした後、次の手順に従います。

- iSCSI LUN の作成
- iSCSI イニシエータの設定（Windows）
- iSCSI LUN のクローン作成

iSCSI イニシエータ グループのリンク解除

iSCSI イニシエータ グループのリンクを解除するには、次の手順を実行します。

手順

ステップ 1 **[ターゲット（Targets）]** タブに移動し、イニシエータ グループのリンクを解除するターゲットの名前を選択します。

ステップ 2 **[イニシエータ グループのリンク（Link Initiator Groups）]** タブで、チェックボックスをクリックして、ターゲットへのリンクを解除するイニシエータ グループを選択します。

ステップ 3 **[イニシエータ グループのリンク解除]** ボタンをクリックします。

ステップ 4 **[イニシエータ グループのリンク解除（Unlink Initiator Group（s））]** をクリックして続行するか、**[キャンセル（Cancel）]** をクリックします。

iSCSI のターゲット ページ

ターゲットの設定情報を表示します。

ターゲット データ

ターゲットを作成するには、次の情報が必要です。

表 *17* : ターゲット作成データ

UI 要素	説明
名前	ターゲットの名前です。

UI 要素	説明
CHAP 認証の有効化	クリックして、CHAP 認証を有効にします。 （注） HXDP は一方向の CHAP 認証をサポートします。
ユーザ名	CHAP 認証のユーザ名
秘密	CHAP 認証の秘密

ターゲットが作成されると、次の情報が表示されます。

表 *18 :* ターゲット情報データ

UI 要素	説明
IQN	イニシエータ向けターゲット iSCSI 認定名。
アクティブ イニシエータ数	アクティブなイニシエータの合計数。。
Total Capacity	使用され利用可能な LUN のストレージ総容量（Tb および Gb）。
CHAP 認証	CHAP 認証が有効になっているかどうかを示します。
LUN	ターゲットの LUNを作成、編集、複製、削除、表示できます。
リンクされたイニシエータ グループ	ターゲットの LUN を作成および表示できるタブです。

iSCSI ターゲットの作成

iSCSI ターゲットを作成するには、次の手順に従います。

始める前に

iSCSI ターゲットを作成する前に、iSCSI ネットワークの作成を作成しておく必要があります。iSCSI イニシエータ グループの作成を作成することも推奨されます。

手順

ステップ 1 **[ターゲット]** タブに移動し、**[作成]** をクリックします。
[ターゲットの作成] ウィンドウが表示されます。

ステップ 2 **[ターゲット名]** フィールドに、ターゲットの名前を入力します。

ステップ 3 （オプション）CHAP 認証を有効にする場合は、**[CHAP 認証の有効化]** チェックボックスをクリックします。[ユーザ名] および [シークレット] のフィールドが表示されます。[ユーザ名] と [シークレット] を入力します。

（注） Windows の場合、シークレットは 12ー16 文字にする必要があります。

（注） CHAP ベースの認証は、iSCSI 検出フェーズではサポートされません。

HXDPは一方向のCHAP認証をサポートします。

（注） CHAP を使用し、SAN（iSCSI LUN）から起動する場合は、UCS の上部イニシエータ領域で CHAP ユーザ/パスワードを設定する必要があります（たとえば、UCS マネージャで、[Boot Policy]、[Set iSCSI Boot Parameters]、[Authentication Profile]）。

ステップ 4 **[ターゲットの作成（Create Target）]** をクリックします。

[ターゲット（Targets）] タブにターゲットが表示されます。

次のタスク

iSCSI ターゲットを作成したら、次の手順を実行します。

- iSCSI イニシエータ グループをターゲットにリンク
- iSCSI LUN の作成
- iSCSI イニシエータの設定（Windows）

iSCSI ターゲットの編集

iSCSI ターゲットを編集するには、次の手順を実行します。

手順

ステップ 1 **[作成（Create）]** ボタンの横にある **[編集（Edit）]**（鉛筆）アイコンをクリックします。

[ターゲットの編集（Edit Target）] ウィンドウが表示されます。

ステップ 2 ターゲットのデータを編集します。

ステップ 3 **[変更の保存（Save Changes）]** をクリックするか、変更を **[キャンセル（Cancel）]** します。

iSCSI ターゲットの削除

ターゲットを削除するには、次の手順に従います。

手順

ステップ 1 [ターゲットの作成（Create Target）]ボタンの横にある[削除（Delete（X））]アイコンをクリックします。

[ターゲットの削除（Delete Target）] ウィンドウが表示されます。

ステップ 2 **[ターゲットの削除（Delete Target）]** をクリックします。**[キャンセル（Cancel）]** をクリックして変更をキャンセルします。

（注） ターゲットにリンクされているイニシエータグループがある場合は、ターゲットを削除できません。

（注） LUN が作成されている場合は、ターゲットを削除できません。ターゲットを削除する場合は、まず、そのターゲット用に作成されたすべての LUN を削除する必要があります。

iSCSI ターゲットのリンク

iSCSI ターゲットをリンクするには、次の手順を実行します。

始める前に

iSCSI ターゲットをリンクする前に、iSCSI イニシエータ グループの作成を作成して設定する必要があります。イニシエータ グループをまだ作成していない場合は、iSCSI ターゲットにリンクする前に作成する必要があります。詳細については、iSCSI イニシエータ グループの作成（348 ページ） を参照してください。

手順

ステップ 1 **[イニシエータ グループ（Initiator Groups）]** タブに移動し、ターゲットにリンクするイニシエータ グループの名前を選択します。

ステップ 2 **[リンクされたターゲット（Linked Targets）]** タブで、**[リンク（Link）]** ボタンをクリックします。

[ターゲットのリンク（Link Target）] ウィンドウが表示されます。

ステップ 3 イニシエータ グループにリンクするターゲットを選択します。

ステップ 4 **[ターゲットのリンク（Link Target）]** をクリックします。

選択したリンク済みターゲットが、[リンクされたターゲット（Linked Targets）] タブに表示されます。

次のタスク

iSCSI ターゲットをリンクした後、次の手順に従います。

- iSCSI LUN の作成
- iSCSI イニシエータの設定（Windows）
- iSCSI LUN のクローン作成

iSCSI ターゲットのリンク解除

iSCSI ターゲットのリンクを解除するには、次の手順を実行します。

手順

ステップ 1 **[イニシエータ グループ（Initiator Groups）]** タブに移動し、ターゲットのリンクを解除するイニシエータグループの名前を選択します。

ステップ 2 **[リンクされたターゲット（Linked Targets）]** タブで、チェックボックスをクリックして、リンクを解除するターゲットを選択します。

ステップ 3 **[リンク解除（Unlink）]** ボタンをクリックします。

ステップ 4 **[リンク解除（Unlink）]** をクリックします。または、**[キャンセル（Cancel）]** をクリックして変更をキャンセルします。

[iSCSI LUN] ページ

iSCSI LUN の設定情報を表示します。

iSCSI LUN データ

LUN を作成するには、次の情報が必要です。

表 19 : iSCSI LUN データ

UI 要素	説明
名前	LUN の名前。
サイズ（Size）	LUN の合計容量サイズ（GB）。 （注） 最大 LUN サイズは 64TB です。

LUN が作成されると、次の情報が表示されます。

表 *20 : LUN* 情報データ

UI 要素	説明
名前	LUN の名前。
LUN ID	LUN の一意の ID
シリアル番号（Serial No.）	LUN のシリアル番号
サイズ（Size）	LUN の合計容量サイズ（GB）。
使用済み（Used）	使用されているLUNの合計キャパシティ（GB）。
使用可能（Available）	使用可能な LUN の合計容量（GB）。

iSCSI LUN の作成

iSCSI LUN を作成するには、次の手順を実行します。

手順

ステップ 1 **[ターゲット（Targets）]** タブに移動し、LUN を作成するターゲットの名前を選択します。

ステップ 2 **[LUN の作成（Create LUN）]** チェックボックスをクリックします。

[LUN] ウィンドウが表示されます。

ステップ 3 **[LUN（LUN ）]** フィールドに名前を入力します。

ステップ 4 **[サイズ (Size)]** フィールドに LUN のサイズと単位を入力します。

（注） 最大LUNサイズは64 TBです。

ステップ 5 **[LUN の作成（Create LUN）]** をクリックします。

ターゲットの [LUN] タブに LUN が表示されます。

（注） ターゲットごとに公開できるLUNの数には制限があります。Linuxシステムでは、ターゲットあたりの LUN の上限は 255 です。Windows システムでは、ターゲットあたりの LUN 数は 254 です。

（注） CHAP で保護されたボリュームを作成できます。ターゲットごとに 1 つのストレージクラスで作成できるボリューム（永続的なボリューム要求）は最大 255 です。

次のタスク

iSCSI LUN を作成したら、iSCSI イニシエータの設定（Windows）できます。

。

iSCSI LUN の編集

iSCSI LUN を編集するには、次の手順を実行します。

手順

ステップ 1 **[ターゲット（Targets）]** タブに移動し、LUN を編集するターゲットの名前を選択します。

ステップ 2 [LUN] タブで、チェックボックスをクリックして編集する LUN を選択します。

ステップ 3 [LUN の作成（Create LUN）] ボタンの横にある [編集（Edit）] アイコンをクリックします。[LUN] ウィンドウが表示されます。

ステップ 4 LUN のデータを編集します。

（注） 最大 LUN サイズは 64TB です。

ステップ 5 **[LUN の編集]** をクリックするか、変更を **[キャンセル]** します。

iSCSI LUNの削除

iSCSI LUNを削除するには、次の手順を実行します。

手順

ステップ 1 [ターゲット（Targets）] タブに移動し、LUN を削除するターゲットの名前を選択します。

ステップ 2 [LUN] タブで、チェックボックスをクリックして、削除する LUN を選択します。

ステップ 3 [LUN のクローン（Clone LUN）] ボタンの横にある[削除（Delete）（X）]アイコンをクリックします。LUN の削除（Delete LUN）] ウィンドウが表示されます。

ステップ 4 [Delete]をクリックします。 [キャンセル（Cancel）]をクリックして変更をキャンセルします。

iSCSI イニシエータの設定（Windows）

この手順では、Windows マシンを iSCSI イニシエータとして設定する方法について説明します。これは、LUN を複製する前に、iSCSI LUN でボリュームを初期化、オンライン、および作成するために実行する必要があります。

（注） HXDP は一方向の CHAP 認証をサポートします。2 方向 CHAP 認証がサポートされていません。

手順

ステップ 1 iSCSI イニシエータとして設定する Windows マシンにログインします。

ステップ 2 **[サーバ マネージャ（Server Manager）]** に移動し、**[iSCSI イニシエータ（iSCSI Initiator）]** をクリックします。**[はい（Yes）]** をクリックして続行します。

ステップ 3 [ターゲット（Target）] タブにターゲットのホスト名または IP アドレスを入力し、**[クイック接続（Quick Connect）]** をクリックします。

検出されたターゲットは「HX クラスタ IP（CIP）」として表示され、ターゲットの IQN とターゲットのステータスが表示されます。

ステップ 4 **[完了（Done）]** をクリックします。

ステップ 5 ターゲットを選択し、[ターゲット（Target）] タブで **[接続（Connect）]** をクリックします。

ステップ 6 **[詳細設定（Advanced）]** をクリックします。

ステップ 7 [CHAP ログオンを有効にする（Enable CHAP log on）] をクリックして、HyperFlex のユーザ名とパスワードを指定します。**[OK]** をクリックします。

設定に問題がない場合は、ステータスが更新され、「接続済み（Connected）」であることを示します。

ステップ 8 ディスク管理ツールで iSCSI LUN が接続されていることを確認します。

これで、iSCSI LUN でボリュームを初期化、オンライン、および作成できるようになりました。

iSCSI イニシエータの設定（Linux）

この手順では、Linux で iSCSI イニシエータを設定する方法について説明します。これは、LUN を複製する前に、iSCSI LUN でボリュームを初期化、オンライン、および作成するために実行する必要があります。

手順

ステップ 1 `iscsiadm` コマンドが存在することを確認します。

ステップ 2 `sudo apt-get install open-iscsi` コマンドを実行します。

ステップ 3 ターゲットを検出します。これを行うには、`sudo iscsiadm -m discovery -t sendtargets -p <HX iSCSI CIP>` マンドを実行します。

ステップ 4 ターゲットにログインします。これを行うには、`sudo iscsiadm -m discovery -t sendtargets -p <HX iSCSI CIP> -l` コマンドを実行します。

（注） `lsblk -scsi` を使用すると、どのデバイスがターゲットであるかを確認できます。これで、gdisk でパーティションを作成し、HX iSCSI ドライブをフォーマットできます。

iSCSI LUN のクローン作成

LUN のアプリケーションの整合性が必要な場合は、LUN を複製できます。LUN の複製は、Windows および Linux ホストでサポートされています。ただし、アプリケーション整合性のある LUN クローンは、VSS 経由の Windows でのみサポートされます。

Windows マシンで iSCSI LUN を複製するには、最初に HX Windows エージェントをインストールする必要があります。詳細については、HX Windows Agent for iSCSI Clone LUN のインストール （361 ページ） を参照してください。

iSCSI クローンを成功させるには、特定のターゲットで 250 LUN 未満にすることをお勧めします。255 を超える LUN を持つ LUN のクローンを作成すると、内部サービス エラーが発生します。

iSCSI LUN を複製するには、次の手順を実行します。

始める前に

各イニシエータに HX Windows エージェントをインストールします。HX Windows エージェントのインストールの詳細については、HX Windows Agent for iSCSI Clone LUN のインストール （361 ページ） を参照してください。

手順

ステップ 1 **[ターゲット（Targets）]** タブに移動し、LUN を複製するターゲットの名前を選択します。

ステップ 2 [LUN] タブで、チェックボックスをクリックして、複製する LUN を選択します。

ステップ 3 [LUN の編集] ボタンの横にある **[クローンの複製]** アイコンをクリックします。[LUN のクローン（Clone LUN）] ウィンドウが表示されます。

ステップ 4 **[アプリケーション整合性]** チェックボックスをクリックして有効にします。Windows マシンの管理者アカウント（ローカルまたはAD）のユーザ名とパスワードを指定して、VSSユーザを確認および認証します。

（注） [アプリケーション整合性（Application Consistent）] チェックボックスをオンにしない場合、iSCSI クローン LUN はクラッシュ整合性になります。

ステップ 5 **[新しい宛先ターゲット名（New destination target name）]** フィールドに、新しい宛先ターゲットの名前を入力します。

ステップ 6 CHAP 認証を有効にする場合は、**[CHAP 認証を有効にする（Enable CHAP Authentication）]** チェックボックスをオンにします。ソース LUN ごとに、**[Destination LUN Name]** フィールドに宛先 LUN 名を入力します。

（注） CHAPベースの認証は、iSCSI検出フェーズではサポートされません。

ステップ 7 **[クローン（Clone）]** をクリックします。または、**[キャンセル（Cancel）]**をクリックして変更をキャンセルします。

（注） HX Windows エージェントは、他のアプリケーション（SQL Server、Exchange など）に関係する LUN を識別しません。複製に必要な LUN を選択する必要があります。

次のタスク

複製された LUN にアクセスするには、宛先ターゲットをイニシエータグループにリンクし、[イニシエータ]ウィンドウから iSCSI ターゲットを更新して LUN を検出します。宛先 LUN のディスク/ボリュームプロパティを変更するには、`HxWinAgentUtils.exe` を使用します。

HX Windows エージェントの制限事項

HX Windows エージェントには、次の制限が適用されます。

- iSCSI LUN は、vCenter Server \ ESXi ホストに展開された Windows 仮想マシンのゲスト内イニシエータを使用して追加する必要があります。
- Microsoft フェールオーバー クラスタによって管理されていない Windows マシン上の共有ディスクは、ISCSI クローン LUN 操作ではサポートされていません。
- HX Connect からは、新しい宛先ターゲットでのみ ISCSI LUN を複製できます。
- アプリケーション整合性のある ISCSI クローン LUN の場合は、アプリケーションで使用されているすべての LUN（SQL Server、Oracle など）を選択してください。
- Cluster Shared Volume（CSV）とクラスタ ディスク/スタンドアロン ディスクの組み合わせのクローンはサポートされていません。クローン操作では、SCV LUNのみ、またはスタンドアロン/クラスタ化されたディスクの組み合わせがサポートされます。
- HyperFlex VSS Hardware Provider サービスは、HyperFlex Windows エージェントによってのみ呼び出すことができます。サードパーティのバックアップ ベンダーが HX LUN のクロー

ンを作成しようとすると、「Microsoft ソフトウェア シャドウ コピー」プロバイダーが呼び出されます。

- HX Windows エージェントのアップグレードとパッチ適用がサポートされています。
- HyperFlex のアップグレードでは、HX Windows エージェントはアップグレードされません。HX Windows エージェントを手動でアップグレードする必要があります。
- HyperFlex クラスタノードを再起動するか電源をオフにすると、ISCSI クローン LUN 操作は失敗します。

HX Windows Agent の前提条件

HX Windows Agent を実行するには、次の前提条件を満たしている必要があります。

- Windows 2016 以降（ホスト マシンの基本設定を満たしていること）。
- Windows Server でポート 10152 および 9347 を開く必要があります。
- HX コントローラ VM でポート 10151 および 9347 が開いている必要があります。
- HyperFlex Windows Agent および HyperFlex VSS Hardware Provider サービスが Windows マシンにインストールされていることを確認します。
- HyperFlex Windows Agent が実行状態であることを確認します。
- iSCSI イニシエータとして公開されているすべての Windows マシンに、HyperFlex Windows Agent と HyperFlex VSS ハードウェア プロバイダの両方のサービスがインストールされていることを確認します。
- Application Consistent ISCSI Clone LUN ワークフローをトリガーする際に、管理者または AD のログイン情報を入力します。
- 複製するソース LUN が検出され、ボリューム ラベルを持ったボリュームが Windows マシンで作成されていることを確認します。

HX Windows Agent for iSCSI Clone LUN のインストール

この手順では、iSCSI クローン LUN の HX Windows Agent をインストールする方法について説明します。

始める前に

Microsoft Windows Server 2016 以降を、VM\ベア メタル上の基本設定で実行していることを確認します。インストーラは、10152 ポートでの着信を許可するルールを追加します。サードパーティのファイアウォールまたはアンチウイルス ソフトウェアを使用している場合には、ポート 10152 が開いていることを確認してください。

手順

ステップ 1 Administrator または AD のログイン情報を使用して、Windows マシンにログインします。

ステップ 2 `HxWindowsAgentIscsiClone-v4.5.1a-39020.exe` をダブルクリックして、Windows HX Agentインストール実行可能ファイルを実行します。

（注） `HxWindowsAgentIscsiClone-v4.5.1a-39020.exe` から抽出されたエージェントログとファイルは、ファイルのプロパティにビルド番号 `4.5.1a.38547` で表示されます。これは、機能に影響を与えないバージョン表示の問題であり、無視できます。

ステップ 3 **[次へ (Next)]** をクリックします。

ステップ 4 使用許諾契約書の条項に同意し、**[次へ（Next）]** をクリックします。

ステップ 5 インストールディレクトリとして `<Program File>\Cisco\HxWindowsAgent` を確認し、**[次へ（Next）]** をクリックします。

ステップ 6 **[インストール（Install）]** をクリックします。

ステップ 7 **[終了]** をクリックします。

これにより、HyperFlex Windows Agent および HyperFlex VSS Hardware Provider サービスがインストールされます。その他のインストールに関する注意事項は次のとおりです。

- HyperFlex Windows エージェントおよび HyperFlex VSS ハードウェア プロバイダー サービスは、Windows でサービスとして表示されます。HyperFlex Windows エージェントは実行状態、HyperFlex VSS ハードウェア プロバイダーは停止状態にあると表示されるはずです。HyperFlex VSS ハードウェア プロバイダーは、ユーザが LUN のクローンまたはバックアップをリクエストすると、開始されます。
- MSI インストーラによるインストールおよびその他のインストールの詳細は、`%appdata%\HxWinAgentMsiInstall.log` ファイルに記録されます。
- インストールディレクトリで、いくつかの依存dllに気付くことがあります。これらの依存関係は削除または更新しないでください。削除した場合は、インストーラの修復オプションを使用して復元する必要があります。
- サービス ログは `C:\HxWindowsAgent\Logs\ HxAgentService_<DateTime>.log` にあります。Windowsレジストリの場所は HKEY_LOCAL_MACHINE\SOFTWARE\HyperFlex です。このエントリには、サービスログの場所が含まれます。
- エージェントのバージョンを確認するには、インストール ディレクトリに移動し、`HxWinAgentService.exe` を右クリックして、**[プロパティ]** を選択します。**[詳細（Details）]** タブで、製品のバージョンを確認してください。
- インストール時および運用時のイベントは、イベント ビューアのサービス ログで、ソースを「HxVssHardwareProvider」および「HxWindowsAgent」として表示できます。着信ルールの名前はポート 10152 の「Hx Windows Agent」で、Windows firewall のすべての IP アドレスで有効にされます。

iSCSI Clone LUN のための（インストール前依存関係が設定された）HX Windows Agent のインストール

ここでは、依存関係がある場合に、HX Windows エージェントをインストールして、iSCSI Clone LUN for HyperFlex を有効にする方法について説明しいます。依存関係としては、Microsoft .NET framework 4.5 (バージョン : 4.5.50709 以降)、Microsoft Visual C++ 2017 Redistributable (x64) (バージョン 14.10.25017 以降）、および Microsoft Visual C++ 2017 Redistributable (x86) (バージョン 14.10.25017 以降）のプログラムが、Windows マシンにすでにインストールされていることが要求されている場合などが例となります。

手順

ステップ 1 Administrator または AD のログイン情報を使用して、Windows マシンにログインします。

ステップ 2 `HxWindowsAgentIscsiClone-v4.5.1a-39020.msi` ファイルをダブルクリックします。

（注） `HxWindowsAgentIscsiClone-v4.5.1a-39020.msi` を使用してエージェントをアンインストールすることはできません。

（注） `HxWindowsAgentIscsiClone-v4.5.1a-39020.exe` から抽出されたエージェントログとファイルは、ファイルのプロパティにビルド番号 `4.5.1a.38547` で表示されます。これは、機能に影響を与えないバージョン表示の問題であり、無視できます。

ステップ 3 **[次へ (Next)]** をクリックします。

ステップ 4 使用許諾契約書の条項に同意し、**[次へ（Next）]** をクリックします。

ステップ 5 インストール ディレクトリを選択します。デフォルトの場所は、`<Program File>\Cisco\HxWindowsAgent` です。

ステップ 6 **[インストール（Install）]** をクリックします。

ステップ 7 **[完了（Finish）]** をクリックします。

iSCSI クローン LUN の HX Windows Agent のアンインストール

この手順では、iSCSIクローンLUNのHX Windows Agent をアンインストールする方法について説明します。

手順

ステップ 1 Administrator または AD のログイン情報を使用して、Windows マシンにログインします。

ステップ 2 `HxWindowsAgentIscsiClone-v4.5.1a-39020.exe` ファイルをダブルクリックします。

（注） HxWindowsAgentIscsiClone-v4.5.1a-39020.exe から抽出されたエージェントログとファイルは、ファイルのプロパティにビルド番号 4.5.1a.39020 で表示されます。これは、機能に影響を与えないバージョン表示の問題であり、無視できます。

ステップ 3 **[次へ (Next)]** をクリックします。

ステップ 4 [削除（Remove）]を選択して、**[次へ (Next)]** をクリックします。

ステップ 5 **[削除（Remove）]** をクリックします。

ステップ 6 **[終了（Finish）]** をクリックします。

- 完了すると、アンインストーラは HyperFlex Windows Agent および HyperFlex VSS Hardware Provider サービスを削除します。
- アンインストーラは、ポート 10152 を持つ Hx Windows Agent という名前のインバウンドルールを Windows ファイアウォールから削除します。
- アンインストーラによって、Microsoft .NET framework 4.5（バージョン：4.5.50709 以降）、Microsoft Visual C++ 2017 Redistributable (x64)（バージョン：14.10.25017 以降）、Microsoft Visual C++ 2017 Redistributable (x86)（バージョン：14.10.25017 以降）プログラムが削除されることはありません。
- アンインストーラは、C:\HxWindowsAgent\Logs\ HxAgentService_<DateTime>.log と、Installation directory\HxCAInstallLogMsi.txt".からファイルとフォルダを削除しません。
- HKEY_LOCAL_MACHINE\SOFTWARE\HyperFlex レジストリ エントリは保持されます。

iSCSI HX Windows Agent のログ

HX Windows Agent の次のログを使用できます。

表 *21 : HX Windows Agent* ログ

ログ ファイル	説明
hxCloneSvcMgr.log	格納場所：/var/log/springpath
hxApplicationConsistentSvcMgr.log	格納場所：/var/log/springpath
HxAgentService_ <日付時刻> .log	格納場所： %SystemDrive%\HxWindowsAgent\Logs このファイルには、VSS リクエスタに固有の Windows エージェントのログが含まれています。
HxVSSProvider_ <日付時刻> .log	格納場所： %SystemDrive%\HxWindowsAgent\Logs このファイルには、VSS ハードウェア プロバイダーに固有の Windows エージェントログが含まれています。

ログ ファイル	説明
HxWinAgentMsiInstall.log	格納場所：`%appdata%`。 このファイルには、Windowsエージェントのインストールログが含まれています。

iSCSI HX Windows Agent ログの転送

HXWindowsエージェントログを含む有用なサポート情報をWindowsマシンからコントローラVMに転送するには、コントローラVMマシンから次のコマンドを実行します。

bash-4.2# hxWindowsAgentLogging

（注） このコマンドは、ログを取得するために必要なWindows IP、ユーザ名、およびパスワードを含む入力パラメータを受け入れます。

ログはコントローラ VM マシンの次の場所に転送されます。：`:/var/log/springpath/<WindowsIP>` 「`HXLogs.zip`」という名前のファイルに保存されます。`HXLogs.zip` ファイルには、HX Windows Agent ログ、HxDiskInfo.log のディスクの詳細、および HxSystem.log のシステム情報が含まれています。

サーバ ログの場所の変更

この手順では、サービス ログの場所の変更方法について説明します。

手順

ステップ 1 Administrator または AD のログイン情報を使用して、Windows マシンにログインします。
ステップ 2 レジストリ エディタを開きます。
ステップ 3 `HKEY_LOCAL_MACHINE\SOFTWARE\HyperFlex` を開きます。
ステップ 4 TargetDirectory の **[Data]** フィールドを右クリックして、**[Modify]** を選択します。
ステップ 5 ログ ファイルの場所を編集します。
ステップ 6 Windows サービスから Hx Windows Agent サービスを再起動します。

宛先ターゲット上の複製された LUN へのアクセス

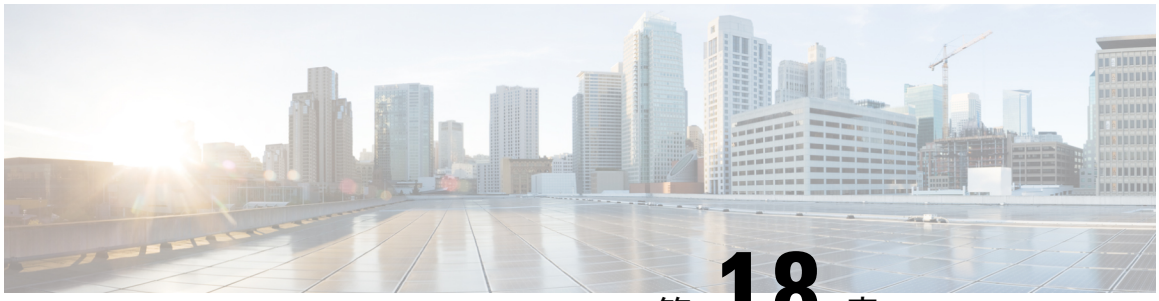
[iSCSIイニシエータ（iSCSI Initiator）] ウィンドウを使用して、次の手順に従って宛先ターゲット上の宛先 LUN を検出します。HX Windows Agent インストール ディレクトリにある `HxWindowsAgentUtils.exe` を使用することもできます。

手順

ステップ 1 diskmgmt.msc に移動し、必要な Disk <Disk ID> を「オンライン」として右クリックします。
ステップ 2 管理者としてコマンド プロンプトを開きます。diskpart.exe を実行します。
ステップ 3 コマンド List Disk を実行します。
ステップ 4 コマンド Select Disk <Disk ID> を実行します。（適切なディスクを選択します）。
ステップ 5 コマンド Detail Disk を実行します。
ステップ 6 ディスク属性「Read-only」が「Yes」の場合、「No」「attributes disk clear readonly」に設定します。
ステップ 7 ボリュームの選択 <Volume ID>（詳細ディスクの一部として表示されるボリュームを選択）
ステップ 8 次のコマンドを実行します。

- attributes volume clear READONLY
- attributes volume clear SHADOWCOPY
- attributes volume clear NODEFAULTDriveLETTER
- attributes volume clear HIDDEN

これで、ボリュームにアクセス可能なディスクと、読み取り/書き込み権限を持つボリューム ラベルが作成されました。



第 18 章

VMware vCenter の Cisco HyperFlex HTML プラグイン

VMware vCenter の Cisco HyperFlex Local 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。vSphere Web Client Navigator から Cisco HyperFlex vCenter プラグインに直接アクセスします。

ここでは、Cisco HyperFlex HTML5 プラグインを使用して VMware vCenter から HyperFlex クラスタを管理および監視する方法について説明します。

VMware vCenter の Cisco HyperFlex HTML5 プラグイン

Cisco HyperFlex Local 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。vSphere Web Client Navigator から Cisco HyperFlex vCenter プラグインに直接アクセスします。

ここでは、Cisco HyperFlex HTML5 プラグイン バージョン 2.0.0, 2.1.0 および 2.2.0 を使用して VMware vCenter から HyperFlex クラスタを監視および管理する方法について説明します。

Cisco HyperFlex HTML5 プラグインの前提条件

Cisco HyperFlex HTML5 プラグインには、次のハードウェアおよびソフトウェアの前提条件が適用されます。

- **ブラウザの互換性**：Cisco HyperFlex HTML プラグインは、Chrome、Firefox、および IE で動作します。
- 管理者権限がユーザーとロールを管理するために必要です。
- インストール ワークフローは、単一の vCenter でもリンク モードの vCenter インスタンスのどちらでも同じです。
- HX リリース 5.0(1a) 以降では、完全な HTML5 プラグイン機能を使用するには、ライセンス ステータスが In-compliance である必要があります。
- HXDP リリース および 5.0(x) 以降のリリースでは、Cisco HyperFlex Flash プラグイン（元のプラグイン）をサポートしていません。
- VMWare vCenter サポートの Cisco HyperFlex HTML5 プラグインが Cisco HX リリース 4.0(2a) と vCenter 6.5U2 に導入されました。
- Cisco HyperFlex HTML5 プラグイン 2.2.0 は、サポートされる最小バージョンです。実行中のバージョンが 2.1.0 または 1.0.1 の場合は、最新バージョンにアップグレードします。
- HTML-Plugin v2.2 は、vCenter リンク モードをサポートします。

vCenter HTML5 プラグインのインストールと登録

VMware vSphere Web クライアントで Cisco HyperFlex HTML5 プラグインをインストールします。プラグインのインストールプロセス中に、HX リリースに一致する必要な情報を入力します。

HX リリース 4.5（1a）	**HX リリース 4.5(2a) 以降**
vCenter Server FQDN/IP	HX ストレージ コントローラ VM 管理者パスワード
vCenter サーバのユーザー名とパスワード	vCenter ユーザ名とパスワード
HX Controller VM のパスワード	-
ストレージ コントローラ VM ルート パスワード	-
ストレージ コントローラ VM 管理者パスワード	-

表 *22 : CLI* 引数

Option	必須またはオプション	説明
-h, --help	任意	指定されているコマンドに関連するヘルプメッセージを表示して終了します。
-u, --unregister	任意	Cisco HyperFlex vCenter プラグインの登録を解除します。
-s, --show	任意	HTML5 vCenter プラグインの詳細を表示します。
-v, --verbose	任意	操作をより詳細にします。

始める前に

- vCenter とコントローラ VM 間の HTTP (ポート 80) と HTTPS (ポート 443) の接続を確認します。
- Cisco HX リリース 4.5 以降を使用する展開では、セキュア管理シェル機能を確認します。
- HTML-Plugin v2.2 は、vCenter リンク モードをサポートします。
- インストール ワークフローは、単一の vCenter でもリンク モードの vCenter インスタンスのどちらでも同じです。

手順

ステップ 1 Cisco ソフトウェア ダウンロード サイトから VMware vCenter 用の Cisco HYPERFLEX HTML プラグインをダウンロードします。

ステップ 2 `HyperFlex-VC-HTML-Plugin-2.2.0.zip` ファイルを、コントローラ VM のいずれかの一時ディレクトリにコピーし、解凍します。

a) ファイル転送は、sftp cliまたはwinscpやfilezillaなどのファイル転送アプリケーションを使用して完了できます。

ファイル転送アプリケーションを介してsftp転送を使用するには、HX管理者アカウントを使用してSCVMの/ tmpフォルダにファイルをコピーします。

b) そのSCVMにSSH接続し、adminアカウントでログインします。

c) コマンド「`cd/tmp`」を使用して`/tmp` ディレクトリに移動します。

例：

```
"cd /tmp"
```

d) コマンド unzip を使用して、プラグイン ファイル `HyperFlex-VC-HTML-Plugin-2.2.0.zip` を解凍します。

例：

```
unzip HyperFlex-VC-HTML-Plugin-2.2.0.zip
```

ステップ 3 シェルで `install_vc_plugin` コマンドを実行し、次のように入力します。

- vCenter FQDN/IP アドレス
- vCenter サーバの管理者のユーザー名とパスワード
- ストレージ コントローラ VM 管理者パスワード

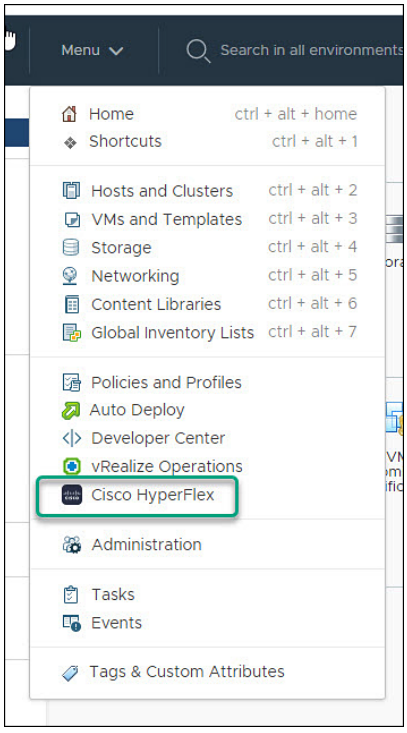
（注） セキュア シェルを使用する Cisco HX 4.5（x）以降では、デフォルトのストレージコントローラ VM ルート パスワードはストレージ コントローラ VM 管理者パスワードと同じです。

ストレージ コントローラ VM ルート パスワードの入力を求められた場合、デフォルトのルート パスワードは、セットアップ時にコントローラ VM に割り当てられた最初のパスワードです。

- ストレージ コントローラ VM 管理者パスワード

ステップ 4 vCenter にログオンすると、新しいプラグインがインストールされたことを確認するために、青色のメッセージ バナーが表示されます。

ステップ 5 vCenter からログアウトし、再度ログインするすると、HTML5 プラグインの Cisco HyperFlex メニューが表示されます。



vSphere クライアントからの Cisco HyperFlex HTML5 プラグインのインストールの確認

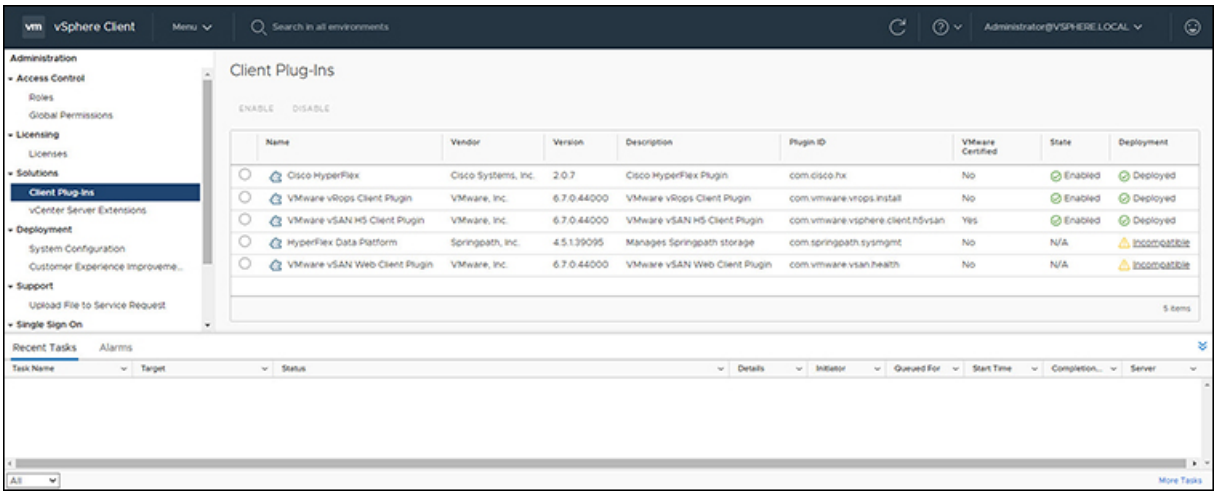
vSphere Client UI から Cisco HyperFlex プラグインのインストールを確認します。

始める前に

HTML5 プラグインを vCenter サーバにインストールする必要があります。

手順

vSphereクライアントを起動し、**[メニュー]**> **[管理]**> **[ソリューション]** >**[クライアント プラグイン]** を選択します。



Cisco HyperFlex HTML5 プラグインのアンインストール

HX Data Platform HTML5 プラグインをアンインストールするには、次の手順を実行します。

手順

ステップ 1 シェルでアンインストール コマンド `install_vc_plugin -u` を実行し、次のクレデンシャルを入力します。

- vCenter FQDN/IP アドレス
- vCenter サーバの管理者のユーザー名とパスワード

ステップ 2 vCenter サーバの vSphere UI サービスを再起動します。

HTML5 プラグインのアップグレード

最新の HTML プラグインにアップグレードするとき、Cisco ソフトウェア ダウンロード サイトから VMware vCenter 用の Cisco HyperFlex HTML プラグインをダウンロードします。

始める前に

このタスクは、vCenter サーバにインストールされている HTML プラグインのバージョンが 2.2.x より前の場合にのみ使用します。

手順

ステップ 1 Cisco ソフトウェア ダウンロード サイトから VMware vCenter 用の Cisco HYPERFLEX HTML プラグインをダウンロードします。

ステップ 2 `HyperFlex-VC-HTML-Plugin-2.2.x.zip` ファイルを、コントローラ VM のいずれかの一時ディレクトリにコピーし、解凍します。

a) ファイル転送は、sftp cliまたはwinscpやfilezillaなどのファイル転送アプリケーションを使用して完了できます。

ファイル転送アプリケーションを介してsftp転送を使用するには、HX管理者アカウントを使用してSCVMの/ tmpフォルダにファイルをコピーします。

b) そのSCVMにSSH接続し、adminアカウントでログインします。

c) /tmp ディレクトリに移動します "cd /tmp"

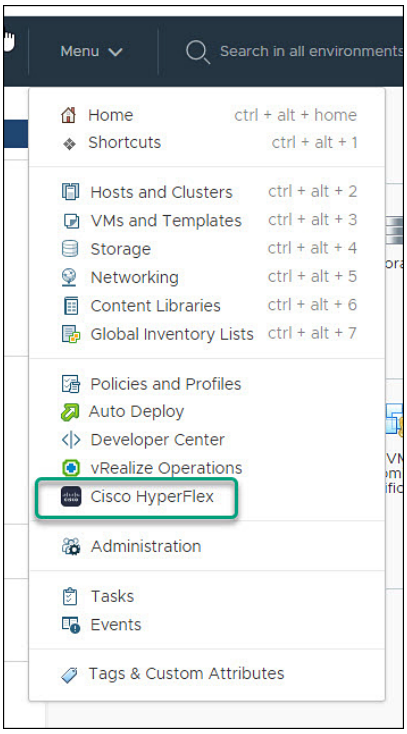
d) プラグイン ファイル `HyperFlex-VC-HTML-Plugin-2.2.x.zip` を解凍します

ステップ 3 シェルで `install_vc_plugin` コマンドを実行し、次のように入力します。

- vCenter FQDN/IP アドレス
- vCenter サーバの管理者のユーザー名とパスワード

ステップ 4 コントローラ ルートおよび admin パスワードを使用してアップグレード プロセスを続行するには、**[Y]** を選択します。

ステップ 5 ログアウトし、vCenter に再度ログインして、vCenter メニューに Cisco HyperFlex を表示します。



Cisco HyperFlex HTML5 プラグインの使用

次の表に、プラグインバージョンごとの機能サポートを定義します。

表 *23 : HTML5* ローカル プラグイン機能のサポート

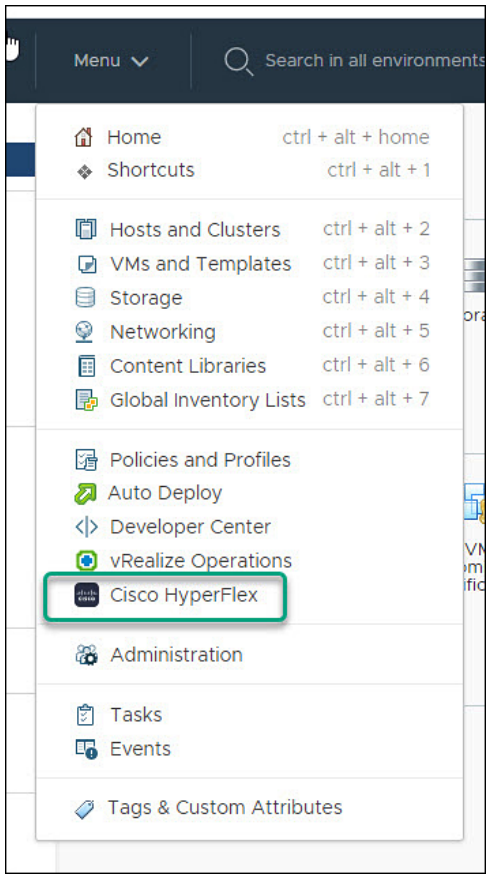
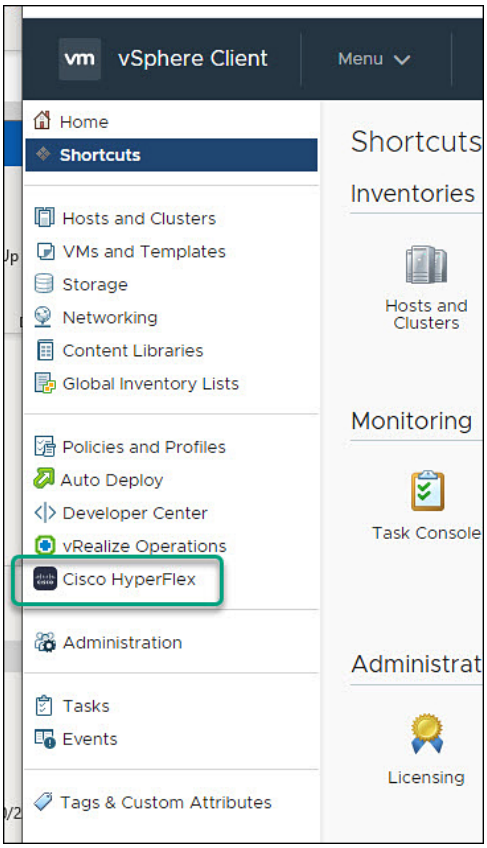
特長	プラグインバージョン 2.0.0	プラグインバージョン 2.1.0	プラグインバージョン 2.2.0
登録済み HX クラスタの検出	✓	✓	✓
クラスタの名前変更 [2]	-	✓	✓
HX クラスタ サマリーの表示	✓	✓	✓
クラスタおよびデータストアのパフォーマンス チャートの表示	✓	✓	✓
ディスク ビュー	✓	✓	✓
ノード ビュー	✓	✓	✓
HX データストア管理	✓	✓	✓

VM サマリーと上位 VM コンシューマ	✓	✓	✓
ネットワーク管理	-	✓	✓
iSCSI 管理 [3]	-	✓	✓
イベントおよびアラーム	✓	✓	✓
管理タスク	-	✓	✓
仮想マシン レベルでの HX スナップショットとクローン	-	✓	✓
スナップショットのスケジュール [4]	-	✓	✓
HX クラスタへのユーザーとアクセスの管理	✓	✓	✓
アップグレードのための HX Connect の相互起動	✓	✓	✓
ホストおよびクラスタ レベルでの組み込み vCenter サーバ アクション	✓	✓	✓
HTML 5 ライセンスステータス [5]	-	-	✓
リンク モード	-	-	✓

[2] HXDP リリース 4.5（x）以降が必要です。
[3] HXDP リリース 4.5（x）以降が必要です。
[4] HXDP リリース 4.5（x）以降が必要です。
[5] HXDP リリース 5.0（x）以降が必要です。

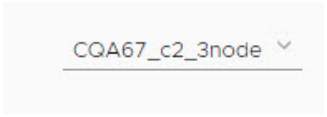
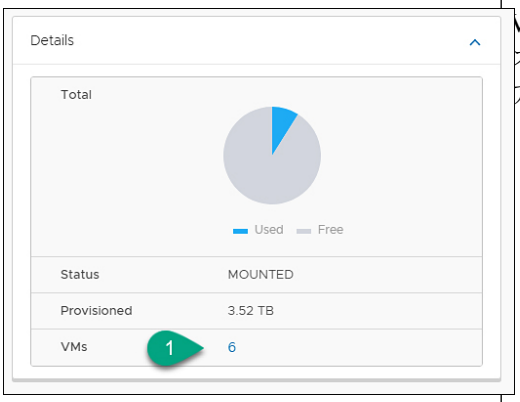
HTML5 プラグインの操作

Cisco HyperFlex HTML5 プラグインへのアクセスは、vSphere メニューまたはショートカット リストから簡単にアクセスできます。

vSphere メニュー	vSphere ショートカット リスト
	

Cisco HyperFlex HTML5 プラグインには、プラグイン全体で共通の機能があります。ここでは、アイコンとその使用方法について説明します。

アイコン	使用法
	Cisco HyperFlex プラグイン。インストールすると、このアイコンは[メニュー（Menu）]および[ショートカット（Shortcuts）] リストに表示されます。
	ビューを更新します。 （注） クラスタリストは動的関数ロードを使用し、[クラスタのスキャン（Scanning Clusters）]アイコンは、クラスタリストが完成したことを示します。
	クラスタテーブルにまだデータが入力されていることを示します。クラスタリストが完了すると、アイコンが消えます。

アイコン	使用法
	ブラウザに表示されるコンテンツをフィルタリングします。
	内容を展開または折りたたみます。
	クラスタ間を移動します。
	[VC クラスタ（VC Cluster）] ボタンを使用して、HyperFlex イベントまたはアラーム ビューから vCenter イベントまたはアラーム ページに移動します。
	VM の数（数値）をクリックすると、そのデータストアのすべての VM をリストする [データストア（Datastore）] ページに直接移動します。

クラスタの管理

HX Cluster へのユーザーおよびアクセスの管理

vCenterプラグインでは、ユーザーが管理者権限をもつ必要があります。ユーザーを作成し、クラスタ レベルの **[権限（Permissions）]** タブからそのユーザーに管理者ロールを割り当てることができます。

ユーザーとHXクラスタへのアクセスを管理するには、そのユーザーのすべてのクラスタに**No Access** ロールを割り当てます。

（注） 管理者権限がユーザーとロールを管理するために必要です。

登録済み HX クラスタの検出

HX クラスタを検出し、展開内の vSphere 管理対象オブジェクトをマッピングするには、次の手順を実行します。

手順

ステップ 1 vSphere Web クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex] を選択します**

ステップ 3 **[再スキャン（Rescan）]** をクリックして、表示された HX クラスタのリストを更新します。
登録されたクラスタは、クラスタの詳細の概要とともに HyperFlex クラスタ テーブルに表示されます。

ステップ 4 新しい HX クラスタを vCenter サーバに追加し、それらがクラスタリストに表示されない場合は、クラスタリスト グリッドの上部にある **[再スキャン（Rescan）]** アイコンをクリックして、HyperFlex からクラスタリストをリロードします。**[クラスタのスキャン（Scanning Cluster）]** アイコンは、クラスタ テーブルにまだデータが入力されていることを示します。クラスタリストが完了すると、アイコンが消えます。

クラスタの名前変更

クラスタの名前変更は、HX リリース 4.5 で導入されました。クラスタの名前を変更するには、次の手順を実行します。

手順

ステップ 1 vSphere Web クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex] を選択します**
[HyperFlex クラスタ] リストが表示されます。

ステップ 3 名前を変更するクラスタの行をクリックします。
サポートされているクラスタの **[名前変更]** ボタンが表示されます。

（注） クラスタ名変更機能は、HXDP リリース 4.5 以降でサポートされています。

ステップ 4 **[名前の変更]** ボタンをクリックします。
[クラスタの名前変更] ウィンドウが表示されます。

ステップ 5 **[クラスタ名：]** 行に新しい名前を入力します。

ステップ 6 **[OK]** をクリックして名前変更を確定します。

HX クラスタ サマリーの表示

展開内の HX クラスタの概要を表示するには、次の手順を実行します。

手順

ステップ 1 vSphere Web クライアントにログインします。

ステップ 2 **[メニュー（Menu）] > [Cisco HyperFlex] を選択します**

ステップ 3 サマリーを表示するには、検出された HX クラスタ名をクリックします。

ステップ 4 **[概要（Summary）]**をクリックして、合計ノード、データストア、HyperFlex リリース、モデル、vCenter クラスタ、ESXi バージョン、および稼働時間に関する詳細を表示します。

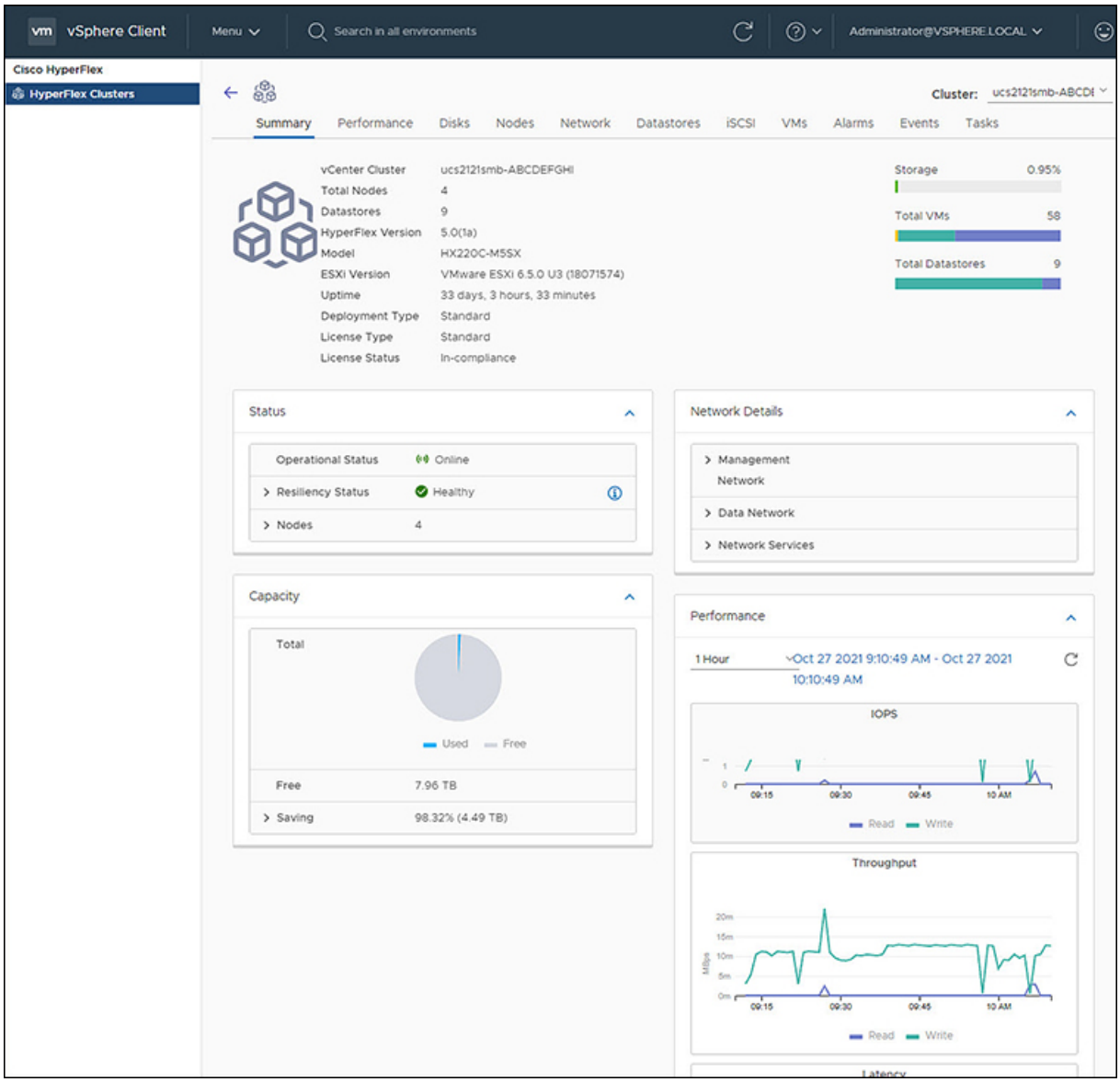


表 *24* : クラスタ概要ビューの詳細

フィールド名	その他の情報
vCenter クラスタ	vCenter クラスタ名
Total Nodes	ノードの合計数
Datastore	クラスタに接続されたデータストア
HyperFlex リリース	クラスタ上の HyperFlex のバージョン
モデル	モデル名

フィールド名	その他の情報
ESXi バージョン	ESXi バージョン
Uptime	クラスタが起動し実行された時間の長さ。
クラスタ タイプ	クラスタの種類
展開タイプ	クラスタ展開のタイプ。有効なオプションは[標準（Standard）]と[エッジ（Edge）]です。
[6]ライセンス タイプ	ライセンスのタイプ。有効なオプションには、評価、標準、およびエンタープライズがあります。 （注） 新しいユーザは、ライセンスを登録するために90日間の猶予期間を利用できます。90日が経過すると、「ライセンスが準拠していません」と表示され、製品の機能が制限されます。
[7]ライセンスのステータス	ライセンスのステータス。ステータスには、コンプライアンス違反、コンプライアンス違反、ライセンスが *x* 日以内に期限切れ、クラスタがシスコライセンスに登録されていません。クラスタがシスコのライセンスに登録されていません。
ストレージ容量バー	使用されている合計ストレージの割合のグラフ表示。バーにカーソルを合わせると、使用されているストレージの量が表示されます。
VM合計バー	クラスタ内のVMの合計数のグラフィカル表示。
合計データストアバー	クラスタに接続されたデータストアの数。バーにカーソルを合わせると、マウントされているデータストアとマウント解除されているデータストアの数が表示されます。

[6] HX release 5.0(x) で追加された
[7] HX リリース 5.0(x) で追加された

a) サマリー ビューには、クラスタに関する追加の詳細情報（ステータス、ネットワークの詳細、キャパシティ、パフォーマンス）をもつ 4 つのポートレットが含まれています。

矢印を使用して、ポートレットの内容を折りたたんだり展開したりします。

表 *25 : [Status]* ポートレット

フィールド名	その他の情報
運用ステータス	オンラインまたはオフライン

フィールド名	その他の情報
Resiliency Status	警告または正常 矢印をクリックして、[レジリエンス ステータス（Resiliency Status）] の詳細を折りたたんだり展開したりします。 • **ホストの障害許容度** ー 許容されるホスト障害の数 • **レプリケーション係数** - コピー数 • **作成時間** - クラスタ作成時間 • **永続的デバイス障害許容** - デバイス障害の許容数 • **キャッシングデバイス障害許容** - キャッシングデバイス障害の許容数
ノード	クラスタ内のノードの数。 矢印をクリックして、追加のノードの詳細を折りたたむか、展開します。 • ノードのタイプ • バージョン

表 *26 : [*容量（*Capacity***）*]* ポートレット**

フィールド名	その他の情報
Total	使用済み容量と空き容量（%）
合計容量（Total Capacity）	利用可能容量
Used	Used Capacity
Free	Free Capacity
保存中	節約された合計容量 [圧縮と重複排除（Compression and Deduplication）] で保存されたスペースの詳細を折りたたんだり展開したりするには、矢印をクリックします。データは、% で表されます。

表 *27 :* ネットワーク詳細ポートレット

フィールド名	その他の情報
管理ネットワーク	管理ネットワークの詳細 矢印をクリックして、次の管理ネットワークの詳細を表示します。 • 管理 IP アドレス/ FQDN • VLAN • デフォルト ゲートウェイ
Data Network	データ ネットワークの詳細 矢印をクリックして、次のデータ ネットワークの詳細を表示します。 • データ IP アドレス / FQDN • VLAN • デフォルト ゲートウェイ
ネットワーク サービス	ネットワーク サービスの詳細 矢印をクリックして、次のネットワーク サービスの詳細を表示します。 • DNS サーバ • NTP サーバ

表 *28 : [Performance]* ポートレット

フィールド名	その他の情報
全般的な使用率 • パフォーマンス チャートは、ライセンス ステータスが **[準拠中（In-compliance）]** の場合に表示されます。[8]. • [時間間隔（Time Interval）] リストをクリックして、パフォーマンス チャートに表示される時間の長さを選択します。 • 特定の時間の合計を表示するには、チャートの線にカーソルを合わせます。 • 表示を更新するには、[最新表示（Refresh）] をクリックします。 • [クラスタのスキャン（Scanning Cluster）]アイコンは、クラスタテーブルにまだデータが入力されていることを示します。クラスタリストが完了すると、アイコンが消えます。 • タイムゾーンを変更するには、現在の時間間隔をクリックし、[時間範囲（Time Range）] ポップアップに入力して、**[OK]** をクリックします。表示される時間は、ブラウザの時間を反映しています。	
IOPS	IOPS パフォーマンス チャートの表示
スループット	スループット パフォーマンス チャートの表示
遅延	遅延パフォーマンス チャートの表示

[8] HX リリース 5.0(1a) 以降でサポートされます。

ライセンスの登録

新規ユーザは、ライセンスを登録するための 90 日間の猶予期間があります。90 日間は、すべての機能にフルアクセスできます。機能の完全なセットを引き続き使用するには、次の手順を実行して製品内リンクを使用してライセンスを登録します。

始める前に

HX リリース 5.0（1a）以降、完全な HTML プラグイン機能を使用するには、ライセンスステータスがコンプライアンス違反である必要があります。[Summary]ページでライセンスタイプとステータスを確認します。ライセンスを登録する必要がある場合は、このタスクを実行します。

ライセンス コンプライアンスの例

図 *1*: 遵守状態のライセンス：

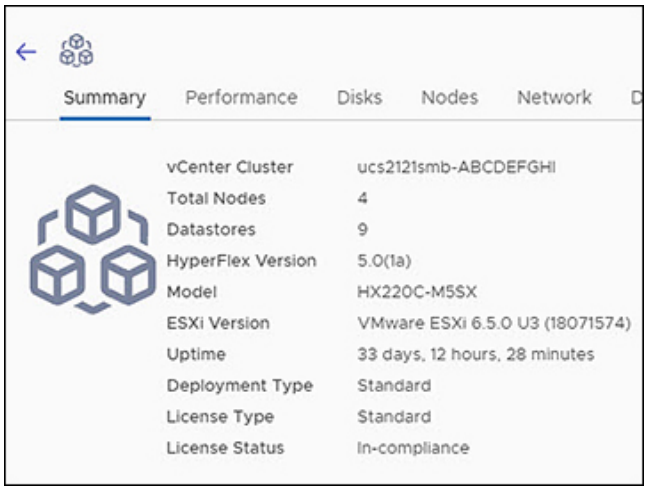
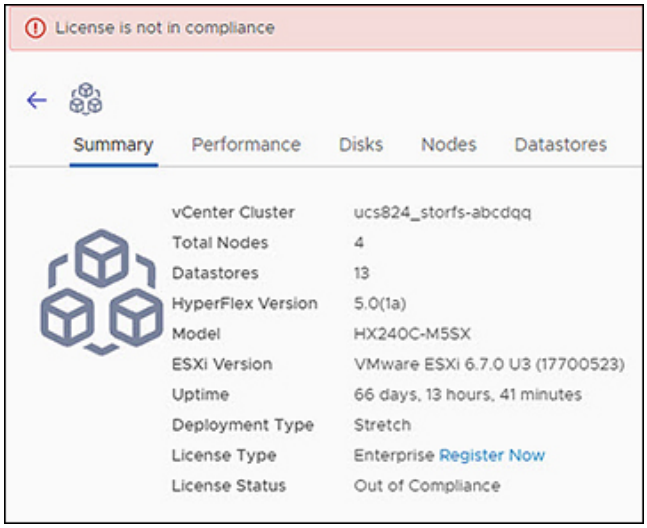


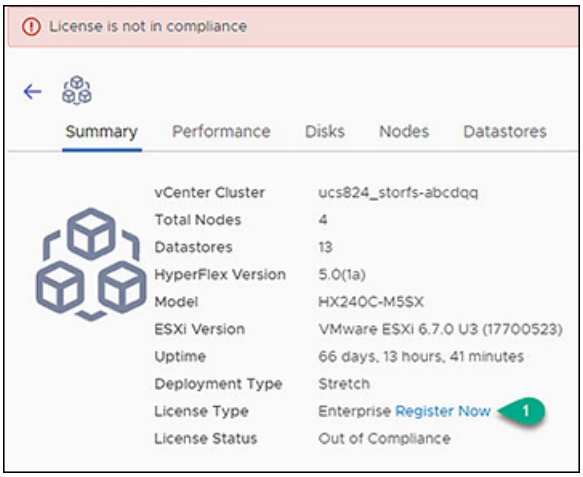
図 *2*: 違反状態のライセンス：



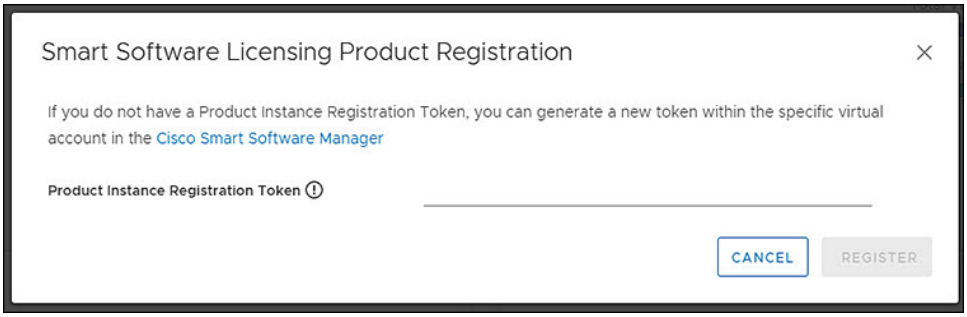
手順

ステップ 1 vSphere Web クライアントの **[サマリー]** ページで開始し、検出された HX クラスタ名をクリックしてその概要を表示します。

ステップ 2 [ライセンス タイプ] サマリーで、**[今すぐ登録]** リンクをクリックします。[スマート ソフトウェア ライセンシング製品の登録] ウィンドウが表示されます。



ステップ 3 提供されたフィールドに製品インスタンス登録トークンを入力します

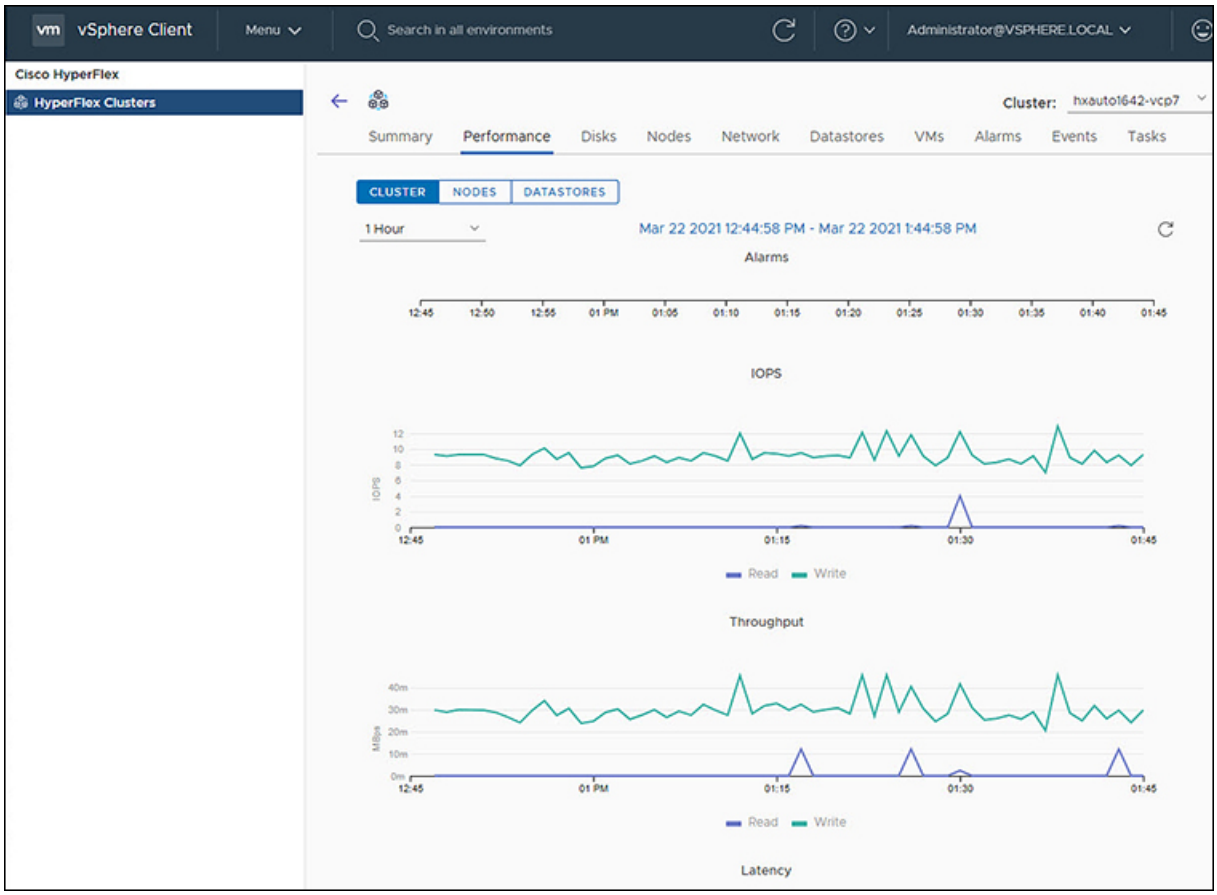


（注） 登録トークンが使用できない場合は、**[Cisco Smart Software Manager]** リンクをクリックして新しいトークンを生成し、プロンプトに従います。

ステップ 4 **[アクション]** をクリックして、登録を完了します。

クラスタおよびデータストアのパフォーマンス チャートの表示

[パフォーマンス（Performance）] タブには、1 時間前のクラスタとデータストアの両方のパフォーマンスの詳細が表示されます。



全般的な使用率:

- [時間間隔（Time Interval）] リストをクリックして、パフォーマンス チャートに表示される時間の長さを選択します。

（注） [アラーム（Alarms）] チャートは、1 ヵ月以下の時間間隔を選択して表示されます。

- 右上のドロップダウン クラスタ リストを使用して、クラスタ間を移動します。
- 特定の時間の合計を表示するには、チャートの線にカーソルを合わせます。
- 表示を更新するには、[最新表示（Refresh）] をクリックします。
- タイムゾーンを変更するには、現在の時間間隔をクリックし、[時間範囲（Time Range）] ポップアップに入力して、**[OK]** をクリックします。表示される時間は、ブラウザの時間を反映しています。

始める前に

HX リリース 5.0（1a）以降、パフォーマンスチャートはライセンス ステータスが [In-compliance] の場合にのみ表示されます。

手順

ステップ 1 vSphere Web クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex]** を選択します。

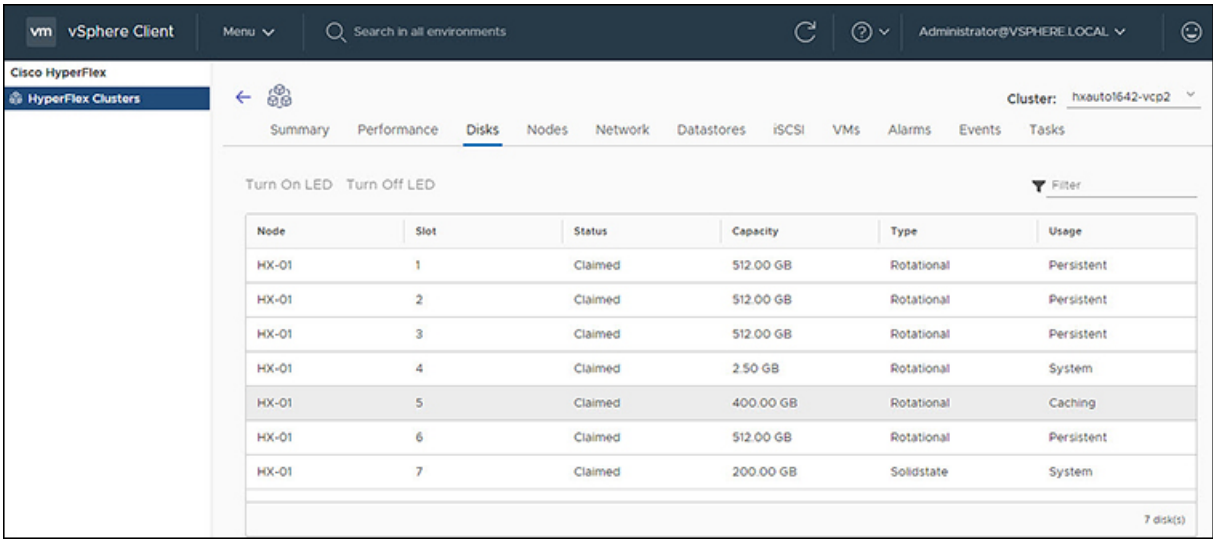
ステップ 3 確認する HX クラスタをクリックします。

ステップ 4 **[パフォーマンス（Performance）]** タブを選択します。Alarms、IOPS、ThroughPut、および Latency チャートが表示されます。

ステップ 5 [時間間隔（Time Interval）] リストをクリックして、パフォーマンス チャートに表示されるタイム スパンを選択します。

ディスク

[ディスクの詳細] ページを表示するには、次の手順を実行します。



手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex]** を選択します

ステップ 3 表示するクラスタ名をクリックします。

ステップ 4 [クラスタ サマリ] タブを使用して、**[ディスク]** をクリックします。
[ディスクの詳細] ビューが表示されます。

表 *29 :* ディスクの詳細

フィールド名	その他の情報
ノード	ノード名
スロット	スロット番号
ステータス	スロット ステータス。有効な値：Available または Claimed
容量	スロットの合計容量
タイプ	ディスクのタイプ。有効な値は次のとおりです。回転、ソリッドステート
使用方法	ディスクの使用方法。有効な値は次のとおりです。Caching、Persistence、System

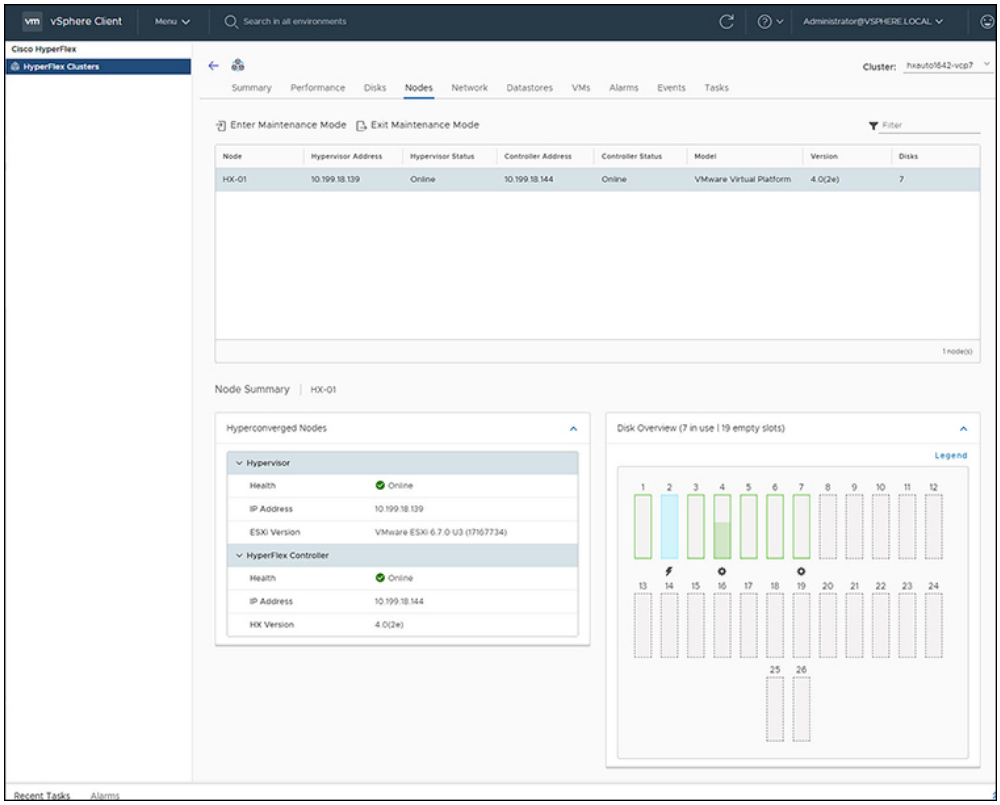
ステップ 5 （オプション）**[LED をオンにする]** ボタンを使用して物理サーバを特定します。

（注） HX リリース 5.0（1a）以降、オン/オフ LED ボタン機能では、ライセンスステータスが In-compliance である必要があります。

a) **オン LED** ボタンをクリックして、関連する物理サーバの LED ライトを点灯させます。
b) 完了したら、**[オフ LED]** ボタンをクリックして LED ライトをオフにします。

ノード

クラスタ、ホスト、および ノード に固有の VM の詳細を表示するには、次の手順を実行します。



手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）] > [Cisco HyperFlex] を選択します**

ステップ 3 表示するクラスタ名をクリックします。

ステップ 4 [クラスタ サマリ] タブを使用して、**[ノード]** をクリックします。
[ノード] リストが表示されます。

表 *30* : ノード リストの詳細

フィールド名	その他の情報
ノード	ノード名。
ハイパーバイザ アドレス	ハイパーバイザの IP アドレス。
ハイパーバイザ ステータス	ハイパーバイザ ステータス。有効な値は、Online と Offline です。
コントローラ アドレス	コントローラの IP アドレス。

フィールド名	その他の情報
コントローラのステータス	コントローラのステータス。有効な値は、Online と Offline です。
モデル	ノードのタイプ。
バージョン	使用中の HXDP バージョン。
ディスク	ノードに関連付けされたディスクの数です。
サイト	列は、エッジ展開の場合にのみ表示されます。

ステップ 5 詳細を表示するノード名をクリックします。[Node Summary]ポートレットが[Nodes]リストの下に表示されます。

a) [ノード サマリー] ビューには、ノードに関する追加の詳細情報を持つ 2 つのポートレット（ハイパーコンバージド ノードとディスクの概要）が含まれています。

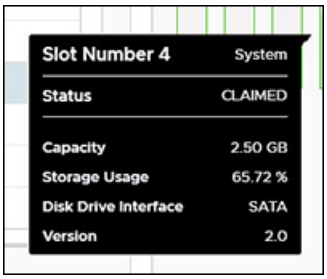
矢印を使用して、ポートレットの内容を折りたたんだり展開したりします。

表 *31* : ハイパーコンバージド ノード ポートレット

フィールド名	その他の情報
ハイパーバイザ	**ヘルス**：オンラインまたはオフライン **IP アドレス**：ハイパーバイザの IP アドレス **ESXi バージョン**：インストールされた ESXi バージョン
HyperFlex コントローラ	**ヘルス**：オンラインまたはオフライン **IP アドレス**：HyperFlex コントローラの IP アドレス **HX バージョン**：インストールされている HyperFlex リリース

表 *32* : ディスク概要ポートレット

フィールド名	その他の情報
ディスクの概要	使用中のスロットの数と空の数を記録します。
凡例（Legend）	ディスクグラフィックスで使用されるアイコンと色の凡例。

フィールド名	その他の情報
ディスクグラフィック	ディスクにカーソルを合わせると、そのディスクの詳細が表示されます。  詳細には次の情報が含まれます。 • スロット番号と使用タイプ • ディスクステータス：請求済みまたは未請求 • 容量 • ストレージ使用率（パーセンテージ）。 • ディスク ドライブ インターフェイス • バージョン

ステップ 6 （オプション）**メンテナンス モードを開始または終了します**

a) メンテナンス モードを開始するか、終了するノード名をクリックします。

b) **[メンテナンス モードの開始]** または **[メンテナンス モードの終了]** をクリックします。

（注） HX リリース 5.0（x）以降では、ライセンス ステータスが [In-compliance] の場合、[メンテナンス モードの開始または終了] ボタン機能が有効になります。

（注） 3 ノードまたは 4 ノードのクラスタがある場合、1 つのノードのみがメンテナンス モードになります。

ネットワーク

ネットワーク：新しいVLANの作成

[ネットワーク（Network）] ページでは、UCS を経由せずに VLAN を作成できます。vSphere クライアントから VLAN を作成するには、次の手順を実行します。

手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）] > [Cisco HyperFlex] > [VLAN の作成]**を選択します

ステップ 3 [VLAN の作成] ウィンドウが表示されます。
[VLAN の作成] ウィンドウのフィールドに入力します。

表 *33 : VLAN* の作成

フィールド名	その他の情報
VLAN ID	1 つの VLAN を作成するには、単一の数値 ID を入力します。VLAN ID には次の値を入力できます。 • 1 ～ 3967 • 4049 ～ 4093
VLAN 名	この名前には、1～32 文字の英数字を使用できます。スペースや特殊記号を使用できません。また、オブジェクトを保存した後はこの名前を変更できません。
UCS Manager のホスト IP または FQDN	UCS Manager の FQDN または IP アドレス たとえば、10.193.211.120 とします
UCS ユーザ名	<管理者> ユーザ名。 たとえば、sample_user1
UCS パスワード	<root> パスワード。

ステップ 4 **[OK]** をクリックします。
VLAN が作成されます。

（注） VLAN の作成は一方向の操作です。HTML プラグインで VLAN を表示することはできません。新しく作成された VLAN を確認するには、UCS に移動し、ESXi vSwitch で新しく作成された vLAN を確認します。

ネットワーク： iSSCI ネットワークの設定

[Network] ページでは、iSCSI ネットワークを設定できます。vSphere クライアントから iSCSI ネットワークを作成するには、次の手順を実行します。

始める前に

iSCSI 機能は、Cisco HyperFlex リリース 4.5（x）以降でサポートされています。

手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー]** > **[Cisco HyperFlex]** > **[ネットワーク設定]** > **[設定]** を選択します

ステップ 3 [Create iSCSI Network] ウィンドウが表示されます。
[Create iSCSI Network] ウィンドウのフィールドに入力します。

フィールド名	その他の情報
サブネット	有効なサブネットを入力してください
ゲートウェイ	有効なゲートウェイを入力してください
IP範囲	有効な IP 範囲を入力してください **[編集（Edit）]**ボタンを使用して、IP範囲を変更します。その他すべてのフィールドも無効になります。
iSCSI ストレージ IP	iSCSI ストレージの有効な IP アドレスを入力してください
VLAN 設定	**[新しい VLAN の作成（推奨）（Create a new VLAN（Recommended））]** または **[既存の VLAN を選択（Select an existing VLAN）]** のチェックボックスをクリックします。 新しい VLAN を作成するには、VLAN ID、VLAN 名、UCS Manager ホスト IP または FQDN、ユーザ名（UCS での認証のためのユーザ名）、パスワード（UCS での認証のためのパスワード）を指定する必要があります。 既存の VLAN を選択するには、VLAN ID を指定する必要があります。 （注） UCS-M で VLAN を手動で設定するには、[Create VLAN]メニューオプションを使用します。[Create VLANs]ウィンドウで、チェックボックスをそのままにします。HX の vNIC テンプレートで、VLAN を「vNIC Template storage-data-a」および「vNIC Template storage-data-b」に接続します。この設定は中断されません。

フィールド名	その他の情報
非デフォルト MTU の設定	MTU（メッセージトランスポートユニット）の手動設定を有効にするチェックボックス。MTU は、ネットワーク全体で 1 回のデータ伝送で送信できるネットワークフレームの最大サイズを定義します。デフォルト MTU サイズは 9000 です。 ジャンボ フレームを無効にするには、**[非デフォルト MTU を設定]** チェックボックスをクリックし、プルダウンを使用して値を 1500 に変更します。 （注） イニシエータのいずれかがルータを通過する場合、ルータはジャンボフレームを許可する必要があります。

ステップ 4 **[OK]** をクリックします。
iSCSI ネットワークが作成されます。

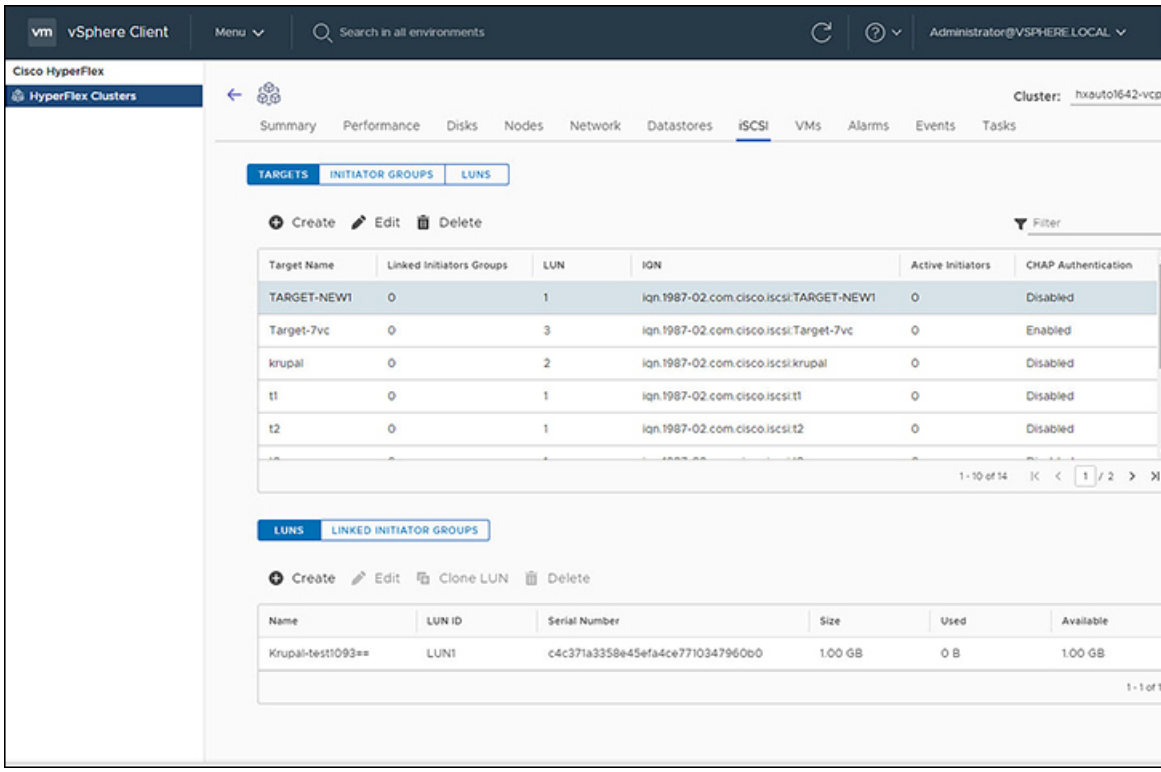
ステップ 5 [タスク（Tasks）]ページで、iSCSI ネットワークが作成されたことを確認します。

iSCSI

iSCSI: ターゲット

iSCSI ネットワークが作成されると、iSCSI ページがナビゲーションタブのリストに表示されます。デフォルト ビューは **[ターゲット（Targets）]** で、**[Create]**、**[Edit]**、**[Delete]**、および **[Clone LUN]** ボタンを使用して iSCSI ターゲットを管理します。

（注） iSCSI ページは、iSCSI ネットワークが設定されているクラスタのナビゲーションタブにのみ表示されます。



始める前に

- iSCSI 機能は、Cisco HyperFlex リリース 4.5（x）以降でサポートされています。
- HX リリース 5.0（1a）以降では、ライセンス ステータスが [In-compliance] の場合、[Create] および [Delete] ボタンが有効になります。
- iSCSI ネットワークの作成ネットワーク： iSSCI ネットワークの設定 （392 ページ）

手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）] > [Cisco HyperFlex] を選択します**
クラスタのリストが表示されます。

ステップ 3 iSCSI ネットワークが設定されているクラスタを選択します。
[iSCSI Network] ページが表示され、**[Targets]**、**[Initiator Groups]**、および **[LUNs]** ボタンが表示されます。
ビュー間を移動するには、ボタンを使用します。

ステップ 4 **[Targets]** ボタンをクリックして、ターゲットのリストを **[Create]**、**[Edit]**、**[Clone LUN]**および**[Delete]** ボタンとともにテーブルに入力します。

表 *34* : ターゲット リスト

フィールド名	その他の情報
ターゲット名（Target Name）	iSCSI サーバ上の iSCSI ストレージ リソースの名前。
リンクされたイニシエータ グループ（Linked Initiators Groups）	クラスタ上のリンクされたイニシエータグループの数。
LUN	イニシエータ グループ内の LUN の数。
IQN	イニシエータの修飾名（IQN）です。 IQN は `iqn.yyyy-mm.naming-authority:unique name` の形式を取ります。
アクティブなイニシエータ数（Active Initiators Count）	アクティブなイニシエータの合計数。。
CHAP 認証	共有秘密とチャレンジ メッセージを使用してリモート クライアントの ID を検証する認証方式。

ステップ 5 リストからターゲットを選択すると、選択したターゲットに関連付けられているすべてのLUNが表示されます。ターゲット リストの下のポートレットに表示されます。**[Create]**、**[Edit]**、**[Clone LUN]**、および **[Delete]** ボタンを使用して、選択したターゲットで LUN を作成、編集、複製、または削除します。

表 *35* : *LUN* 詳細ポートレット

フィールド名	その他の情報
名前	LUN 名
LUN ID	LUN の一意の ID
シリアル番号	LUN のシリアル番号
サイズ	LUN の合計容量サイズ（GB）
使用済み（Used）	使用されているLUNの合計キャパシティ（GB）
使用可能（Available）	使用可能な LUN の合計容量（GB）

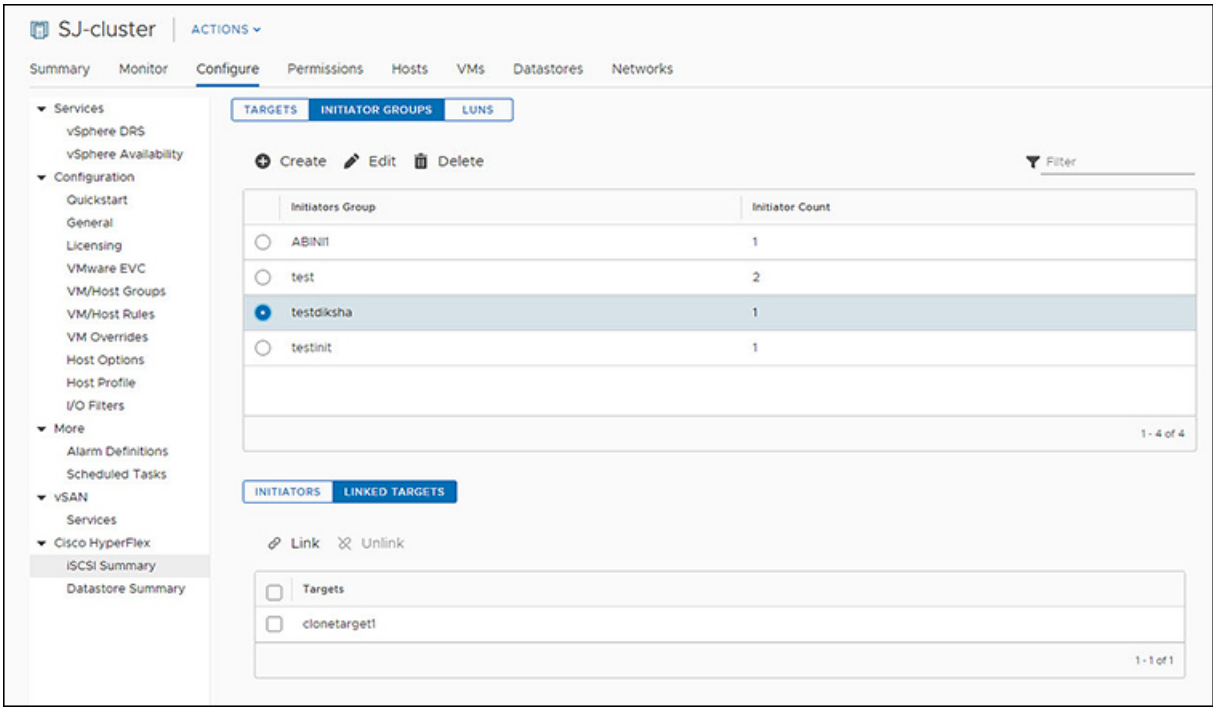
関連トピック

[iSCSI LUN] ページ （355 ページ）
iSCSI LUN の作成 （356 ページ）
iSCSI LUN の編集 （357 ページ）

iSCSI LUN のクローン作成 （359 ページ）
iSCSI LUNの削除 （357 ページ）
[Configure]タブからのiSCSIおよびデータストアの概要の表示 （418 ページ）

iSCSI : イニシエータ グループ

[iSCSI] ページの **[イニシエータ グループ（Initiator Groups）]** ボタンを使用して、イニシエータ グループを作成、編集、および削除します。



始める前に

- iSCSI 機能は、Cisco HyperFlex リリース 4.5（x）以降でサポートされています。
- HX リリース 5.0（1a）以降では、ライセンス ステータスが [In-compliance] の場合、[Create] および [Delete] ボタンが有効になります。

手順

ステップ 1 vSphere クライアントにログインします。

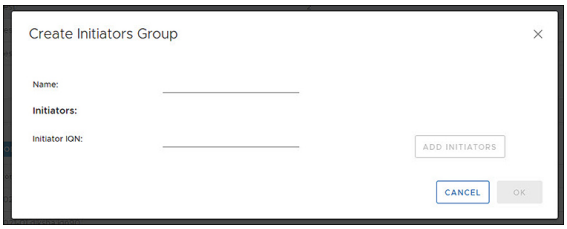
ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex]** > **[iSCSI]**を選択します
[iSCSI Network] ページが表示され、**[Targets]**、**[Initiator Groups]**、および **[LUNs]** ボタンが表示されます。ビュー間を移動するには、ボタンを使用します。

ステップ 3 **[イニシエータ グループ（Initiator Groups）]** ボタンをクリックし、**[作成（Create）]**、**[編集（Edit）]**、および **[削除（Delete）]** ボタンとともに、イニシエータ グループのリストをテーブルに入力します。

表 *36*：イニシエータ グループ リスト

フィールド名	その他の情報
イニシエータ グループ	クラスタ上の指定された LUN にアクセスできるホストを指定するグループのリスト。
イニシエータ	グループ内のイニシエータの数。

表 *37*：イニシエータ グループ アクション ウィンドウの例

アクション ウィンドウ名	例
イニシエータ グループの作成	
イニシエータ グループの編集	

ステップ 4 リストからイニシエータ グループを選択すると、リストの下の詳細ポートレットにイニシエータのリストが表示されます。

ステップ 5 **[イニシエータ（Initiators）]** ボタンをクリックして、グループ内の個々のイニシエータを表示します。

ステップ 6 **[リンクされたターゲット（Linked Targets）]** ボタンをクリックして、選択したグループに関連付けられているターゲットを表示します。

ステップ 7 **[リンク（Link）]** および **[リンク解除（Unlink）]** ボタンを使用して、ターゲットをグループにリンクおよびリンク解除します。

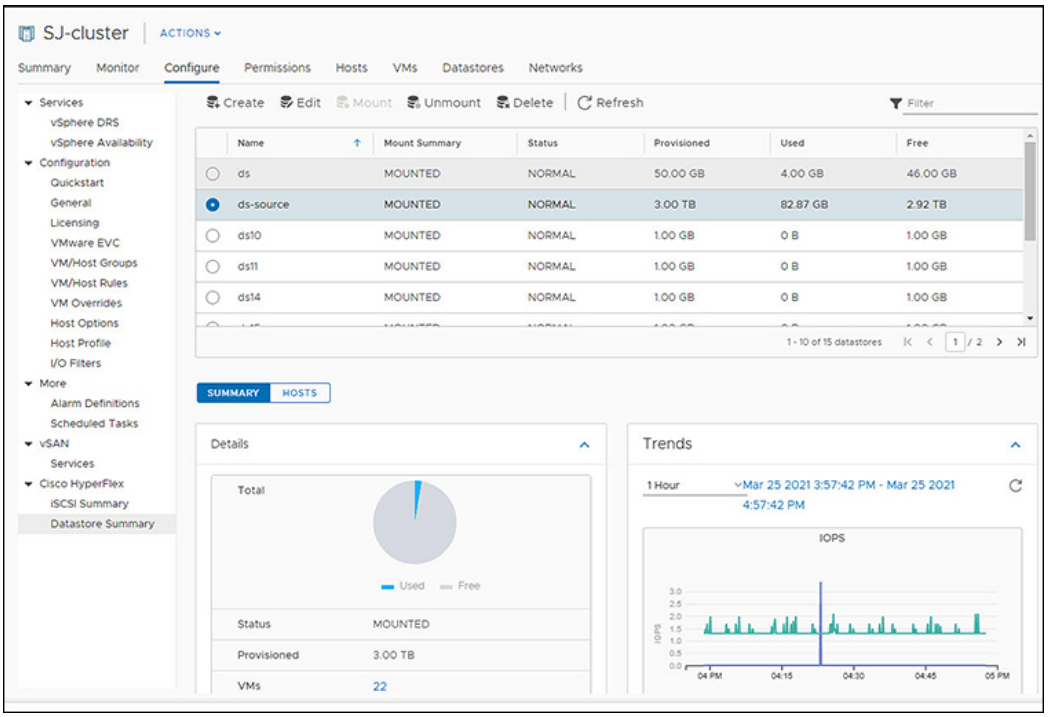
関連トピック

iSCSI イニシエータ グループ （348 ページ）
iSCSI イニシエータ グループの作成 （348 ページ）
iSCSI イニシエータ グループの編集 （349 ページ）
iSCSI イニシエータ グループの削除 （350 ページ）
iSCSI イニシエータ グループをターゲットにリンク （350 ページ）
iSCSI イニシエータ グループのリンク解除 （351 ページ）

[Configure]タブからのiSCSIおよびデータストアの概要の表示 （418 ページ）

iSCSI: LUNs

LUNを作成するには、[LUNS]ボタンを使用し、[LUN]ボタンを使用してLUNを管理します。



始める前に

- iSCSI 機能は、Cisco HyperFlex リリース 4.5（x）以降でサポートされています。
- HX リリース 5.0（1A）以降では、ライセンス ステータスが [In-compliance] の場合、[Create]、[Delete]、および [Clone LUN] ボタンが有効になります。

手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex]** > **[iSCSI]**を選択します

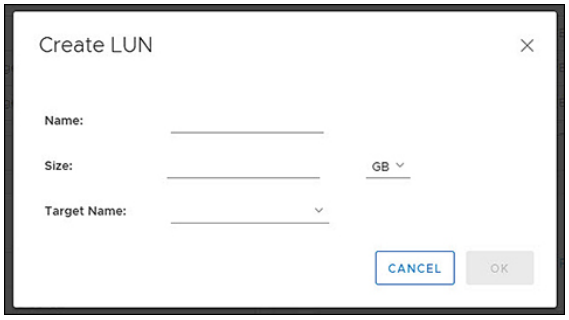
ステップ 3 **[LUNS]**ボタンをクリックして、**[作成（Create）]**、**[編集（Edit）]**、**[クローンLUN（CloneLUN）]**、および **[削除（Delete）]** ボタンとともに LUN のリストをテーブルに入力します。

表 *38 : LUN* 詳細ポートレット

フィールド名	その他の情報
名前	LUN 名

フィールド名	その他の情報
LUN ID	LUN の一意の ID
シリアル番号	LUN のシリアル番号
サイズ	LUN の合計容量サイズ（GB）
使用済み（Used）	使用されているLUNの合計キャパシティ（GB）
使用可能（Available）	使用可能な LUN の合計容量（GB）

表 *39 : iSCSI LUN* アクション ウィンドウの例

アクション ウィンドウ名	例
LUN の作成	
LUN の編集	
クローン LUN	

ステップ 4 リストで LUN を選択すると、LUN リストの下に [詳細ポートレット（Details Portlet）] と [パフォーマンス チャート（Performance Charts）] が表示されます。

関連トピック

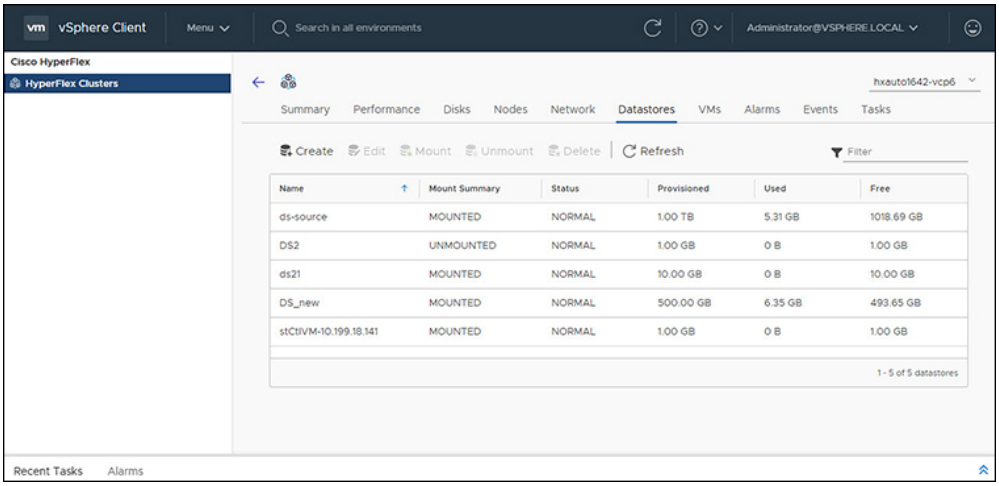
[Configure]タブからのiSCSIおよびデータストアの概要の表示 （418 ページ）

HX データストア管理

データストアの管理

[データストア（Datastore）] ページでは、データストアの詳細の表示、クラスタ上のデータストアの作成、編集、マウント、アンマウント、または削除ができます。

（注） HX リリース 5.0（1a）以降、ライセンス ステータスが [In-compliance] の場合、[Create and Store Datastore] ボタンが有効になります。



手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）] > [Cisco HyperFlex] を選択します**

ステップ 3 該当するクラスタをクリックします。

ステップ 4 **データストア**をクリックします。
[データストア詳細テーブル（Datastore Detail Table）] が表示されます。矢印を使用して、データストアの次または前のページ、および最初または最後のページに進みます。

表 *40* : データストアテーブルの詳細

フィールド名	その他の情報
名前	データストア名
マウント サマリー	マウントまたはアンマウント
ステータス	データストアのステータス：有効な値は次のとおりです：正常
プロビジョニング	プロビジョニングされたスペースの量

フィールド名	その他の情報
Used	使用領域
Free	使用可能なスペースの量

ステップ 5 テーブル内のデータストア名をクリックすると、データストアの追加の詳細が表示されます。
[詳細（Details）] ポートレットと [トレンド（Trends）] ポートレットがテーブルの下に表示されます。

表 *41 :* 詳細ポートレット

フィールド名	その他の情報
Total	プロビジョニングされ使用されているスペースのグラフ
Status	マウントまたはアンマウント
プロビジョニング	プロビジョニングされたスペースの量
VM	データストア内で作成された VM の数 VM の数（数値）をクリックすると、そのデータストアのすべての VM をリストする [データストア（Datastore）] ページに直接移動します。

表 *42 :* トレンド ポートレット

フィールド名	その他の情報
全般的な使用率: • [時間間隔（Time Interval）] リストをクリックして、パフォーマンス チャートに表示される時間の長さを選択します。 • 特定の時間の合計を表示するには、チャートの線にカーソルを合わせます。 • 表示を更新するには、[最新表示（Refresh）] をクリックします。 • [クラスタのスキャン（Scanning Cluster）]アイコンは、クラスタテーブルにまだデータが入力されていることを示します。クラスタリストが完了すると、アイコンが消えます。 • タイムゾーンを変更するには、現在の時間間隔をクリックし、[時間範囲（Time Range）] ポップアップに入力して、**[OK]** をクリックします。表示される時間は、ブラウザの時間を反映しています。	
IOPS	IOPS パフォーマンス チャートの表示
スループット	スループット パフォーマンス チャートの表示
遅延	遅延パフォーマンス チャートの表示

表 *43* : ホストポートレット

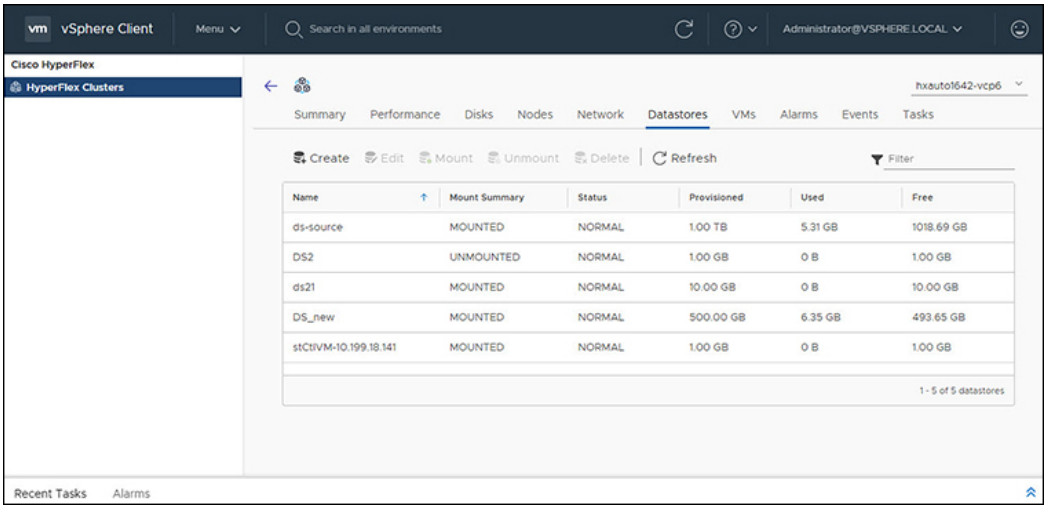
フィールド名	その他の情報
ホスト名	選択したデータストアのホストの IP アドレスを表示します。
Mount Status	ホストがマウントされているかマウント解除されているかを指定します。
アクセス可能	ホストがアクセス可能かどうかを指定します。

関連トピック

[Configure]タブからのiSCSIおよびデータストアの概要の表示 （418 ページ）

新しいデータストアの作成

新しいデータストアを作成するには:



始める前に

- HX リリース 5.0（1a）以降、ライセンス ステータスが [In-compliance] の場合、[Create Datastore] ボタンが有効になります。
- vSphere クライアントにログインし、**[メニュー]** > **[Cisco HyperFlex]** を選択します。

手順

ステップ 1 該当するクラスタをクリックします。

ステップ 2 **データストア**をクリックします。

ステップ 3 [Create] ボタンをクリックします。[データストア（Datastore）] ウィンドウが表示されます。

a) データストア名を入力します
b) [サイズ（Size）] を入力し、[GB] または [TB] を選択します。
c) ブロック サイズを選択し、4K または 8K を選択します。

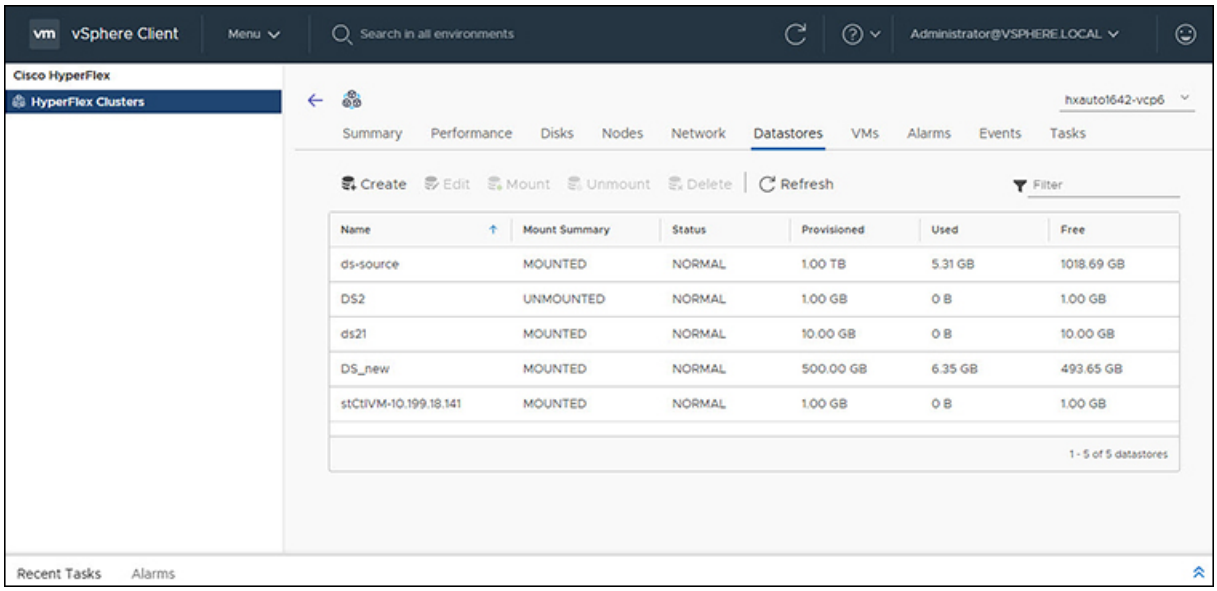
ステップ 4 [OK] をクリックします。新しいデータストアが作成され、データストアテーブルリストに追加されます。

ステップ 5 新しいデータストアがリストに表示されない場合は、**[更新（Refresh）]** 矢印をクリックしてリストを再確認します。

データストアの編集

既存のデータストアを編集するには、次の手順を実行します。

（注） データストアの名前は、アンマウントされた後にのみ変更できます。



始める前に

vSphere クライアントにログインし、**[メニュー]** > **[Cisco HyperFlex]** を選択します。

手順

ステップ 1 該当するクラスタをクリックします。

ステップ 2 **[データストア（Datastore）]** をクリックし、[編集（Edit）] アクションの [データストア（Datastore）] を選択します。

ステップ 3 [Edit] ボタンをクリックします。[データストアの編集（Edit Datastore）] ウィンドウが表示されます。

ステップ 4 データストアの詳細を編集します。

ステップ 5 [OK] をクリックして変更を保存します。データストア情報が更新されます。

データストアのマウントまたはアンマウント

[Mount] ボタンと [Unmount] ボタンは、データストアの現在のステータスに基づいてアクティブになります。マウントされたデータストアには、データストアをマウント解除するオプションがあり、マウントされていないデータストアには、データストアをマウントするオプションがあります。データストアのマウントまたはアンマウント:

始める前に

- マウント解除アクションを開始する前に、データストアに作成または登録されたVMを削除します。
- vSphere クライアントにログインし、**[メニュー]** > **[Cisco HyperFlex]** を選択します。

手順

ステップ 1 該当するクラスタをクリックします。

ステップ 2 **[Datastore]** をクリックし、[Datastore for Mount（Unmount）] アクションを選択します。

ステップ 3 **[Mount]**（**[Unmount]**）ボタンをクリックします。

[データストアをマウント（マウント解除）しますか？（Do you want to mount（Unmount）the datastore？）] という確認の質問が [データストアをマウント（アンマウント）] ウィンドウが表示されます。

ステップ 4 **[OK]** をクリックして [Mount（Unmount）] アクションを続行するか、**[Cancel]** をクリックして [Mount（またはUnmount）Datastore] ウィンドウを終了します。データストアのステータスが [マウント済み（Mounted）] から [マウント解除（Unmounted）] または [マウント解除済み（Unmounted）] から [マウント済み（Mounted）] に変更されます。

データストアの削除

データストアの削除

始める前に

- HXリリース5.0（1a）以降、ライセンスステータスが[In-compliance]の場合、[Delete Datastore] ボタンが有効になります。
- [データストアの削除（Delete Datastore）]アクションを開始する前に、データストアに作成または登録されたVMを削除し、データストアをマウント解除します。
- vSphere クライアントにログインし、**[メニュー]** > **[Cisco HyperFlex]** を選択します。

手順

ステップ 1 該当するクラスタをクリックします。

ステップ 2 **[データストア（Datastore）]** をクリックし、[削除（Delete）] アクションのための [データストア（Datastore）] を選択します。

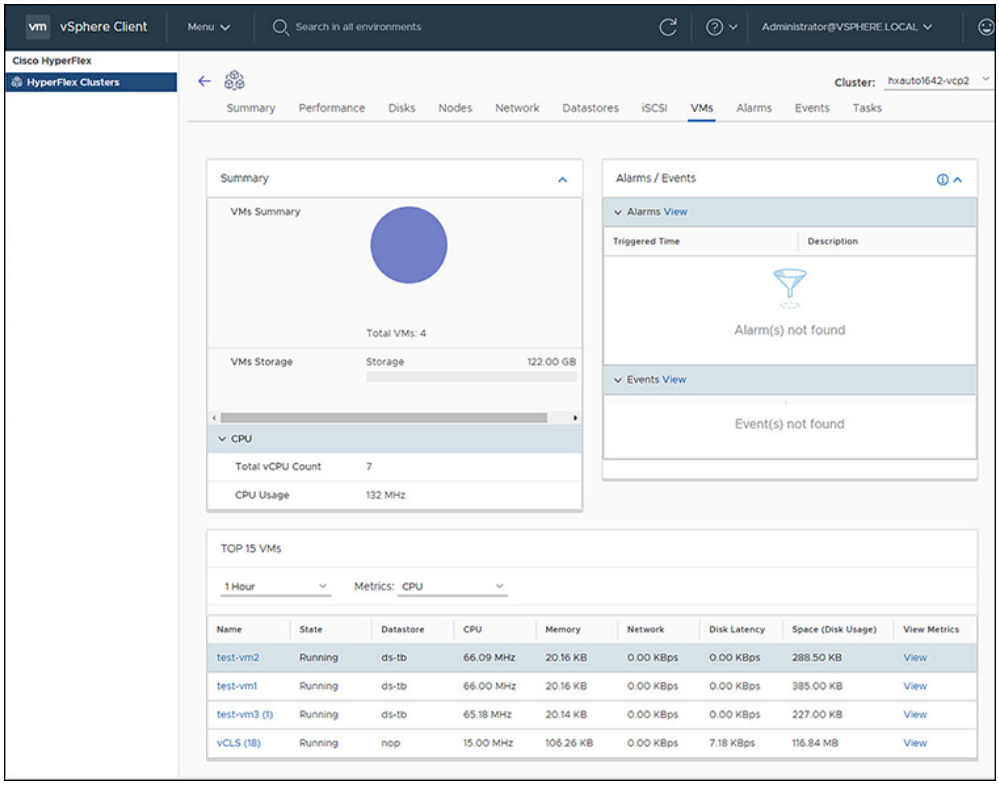
ステップ 3 **[削除（Delete）]** ボタンをクリックします。

[データストアの削除（Delete Datastore）] ウィンドウに「Do you want to delete the datastore？」という確認の質問が表示されます。

ステップ 4 **[OK]** をクリックして削除アクションを続行するか、**[キャンセル（Cancel）]** をクリックして [データストアの削除（Delete Datastore）] ウィンドウを終了します。
選択したデータストアがデータストア テーブル リストから削除されます。

VM

クラスタ、ホスト、および VM に固有の VM の詳細を表示するには、次の手順を実行します。



手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex] を選択します**

ステップ 3 表示するクラスタ名をクリックします。

ステップ 4 [クラスタ サマリ（Cluster Summary）] タブを使用して、**[VM]** をクリックします。
[VM の詳細（VM Detail）]には、[概要（Summary）]、[アラーム/イベント（Alarms / Events）]、および [上位 15 個（Top 15）] の 3 つのポートレットが表示されます。

表 *44* : サマリーポートレット

フィールド名	その他の情報
VM の概要	使用中のユーザ VM の使用状況図。カーソルを合わせると、実行中、一時停止中、オフの VM の数が表示されます。 Total VMs：すべてのユーザ VM の合計数。 （注） コントローラ VM はサマリーに含まれません。
VM ストレージ	すべてのユーザ VM ストレージの合計。すべてのユーザ VM の合計ストレージ容量がイメージの上に表示されます。グラフィックにカーソルを合わせると、現在使用されているストレージの量が表示されます。
VM メモリ	ポイントインタイムメモリの量。合計メモリ容量が表示されます。グラフィックの上にカーソルを合わせると、現在のメモリ使用量が表示されます。
CPU	**Total vCPU Count**：クラスタ内のすべての VM の合計 CPU 数。 **CPU 使用率**：特定の CPU が使用している 1秒あたりのサイクル数。

表 *45* : アラーム/イベントポートレット

フィールド名	その他の情報
アラーム	過去 1週間（7 日間）の VM のアラームを表示します。 [アラームの詳細（Alarms Details）]ビューに移動するには、**[表示（View）]**をクリックします。 • **トリガ時刻**：アラームの発生時刻。 • **説明**：アラームの説明。

フィールド名	その他の情報
イベント	先週（7 日間）の VM のイベントを表示します。 **[表示（View）]** をクリックして、[Events Details] ビューに移動します。 • **日時**：イベントが発生した日付と時刻。 • **説明**：イベントの説明。

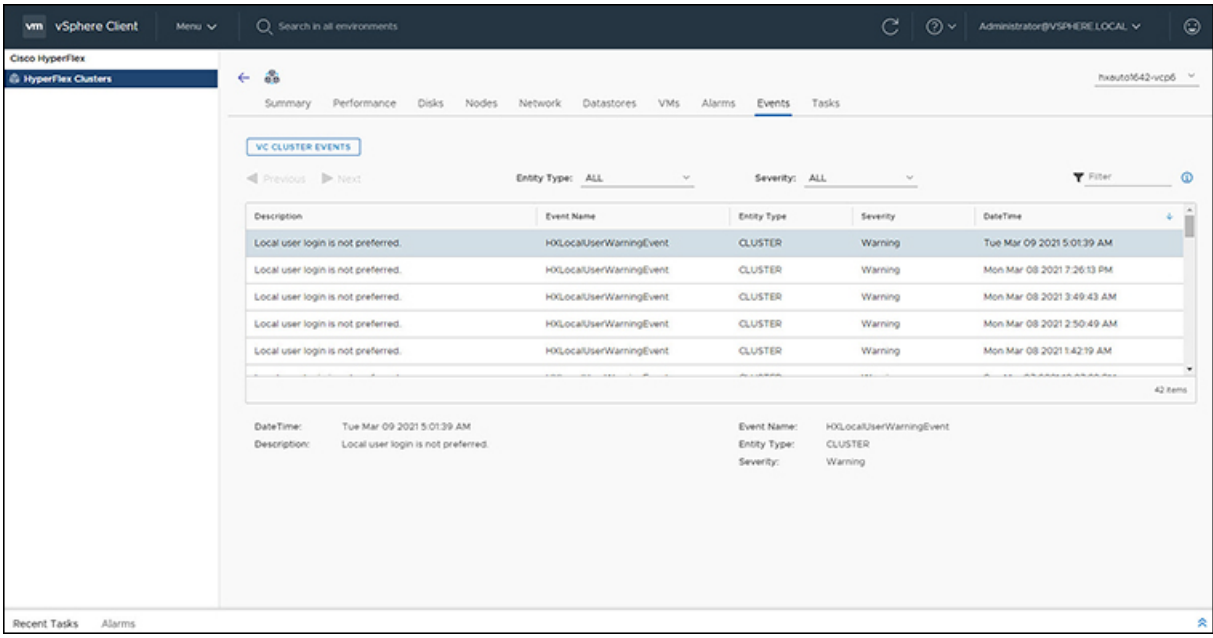
表 *46* : 上位 *15* の *VM* ポートレット

フィールド名	その他の情報
時間リスト	上位 15 の VM を表示する時間の測定値を指定します。リストのオプションには、1 時間、1 日、または 1週間があります。
メトリックリスト	テーブルの入力に使用するメトリックタイプを選択します。オプションには、CPU、メモリ、ディスク遅延、ネットワーク、およびスペースがあります。 • CPU、メモリ、ディスク遅延、ネットワーク-実行状態の VM のメトリックのみをレポートします。スイッチがオフになっている VM は含まれません。 • スペース：状態に関係なくすべての VM をカウントします。
名前	VM 名：VM 名をクリックすると、vCenter で表示されている VM のグラフまたはモニタリングページにユーザがリダイレクトされます。
状態	VM の現在の状態。有効な値は、Running、Off、および Suspended です。
データストア	データストア名（Datastore Name）
CPU	間隔に使用されるメガヘルツ単位の CPU 使用率。
メモリ	ゲスト物理メモリページのバックアップに消費されたホスト物理メモリの量。
ディスク遅延	ホストが使用するすべてのディスクで最大の遅延値
ネットワークスループット	間隔中のネットワーク使用率（送信レートと受信レートの組み合わせ）。
スペース（ディスク使用量）	VM が使用しているディスク容量

フィールド名	その他の情報
メトリックを表示	指定したVMのCPU、メモリ、ディスク遅延、およびネットワークスループットのパフォーマンステーブルを表示するためのリンク。表示される使用率の値は、すべての5分間の平均値です。 ホバー機能を使用して、マトリックスを同時に表示し、データ内の目に見えるスパイクを評価します。

イベント

クラスタ、ノード、ホスト、VM、またはディスクに固有のイベントを表示するには、次の手順を実行します。



手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex]を選択します。**

ステップ 3 表示するクラスタ名をクリックします。

ステップ 4 [クラスタ サマリ（Cluster Summary）]タブを使用して、**[イベント（Events）]** をクリックします。
[イベント詳細（Events Detail）] ビューが表示されます。

表 *47 : Event Details*

フィールド名	その他の情報
説明	テキストによるイベントの説明。
イベント名	イベント名
エンティティ タイプ	影響を受けるエンティティ。値には、All、Cluster、Node、Virtual Machine、および Disk が含まれます。
シビラティ（重大度）	イベントのシビラティ（重大度）レベル有効な値は、All、Info、Warning、Error、および Critical です。
日時（DateTime）	イベントの発生日時

ステップ 5 （オプション）イベント テーブルに表示される結果を制限するには、フィルタを使用します。

Filter	フィルタ オプション
エンティティ タイプ	All、Cluster、Node、Virtual Machine、および Disk
シビラティ（重大度）	All、Info、Warning、Error、および Critical
Filter	[フィルタ（Filter）] オプションにキーワードを入力して、ブラウザに表示されるテーブルの内容をフィルタリングします。

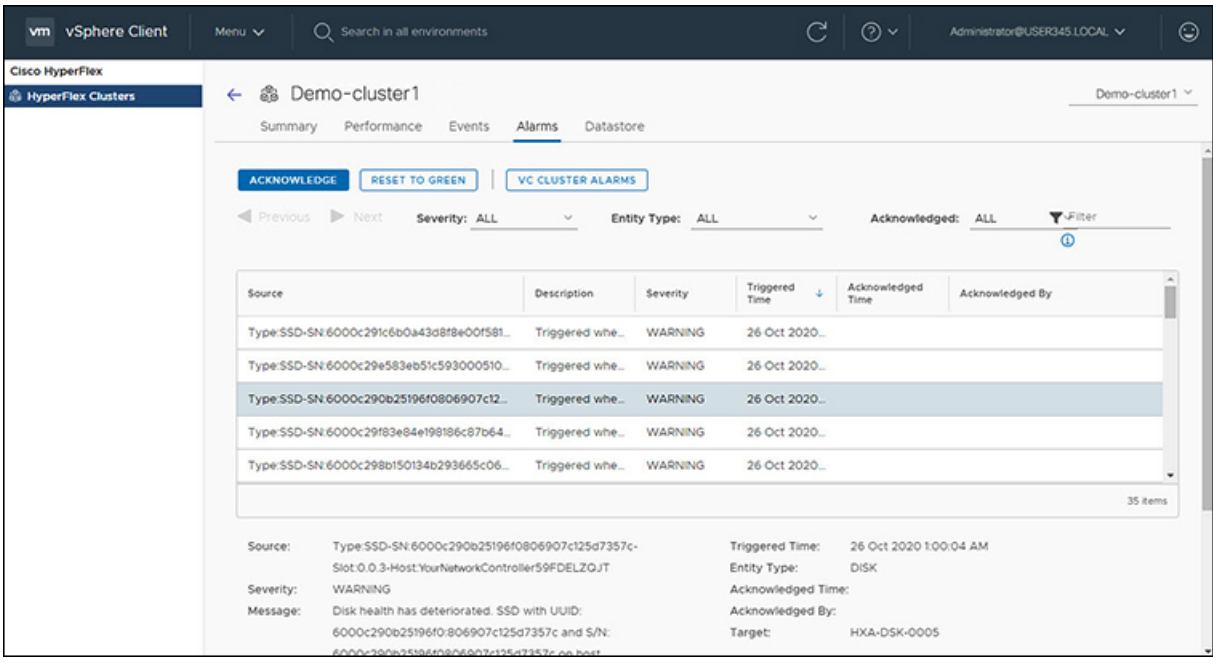
ステップ 6 イベントのリストで、詳細情報が必要なイベント名をクリックします。
[イベント（Events）] テーブルの下に詳細が表示されます。詳細には次の情報が含まれます。

- 説明
- イベント名
- エンティティ タイプ
- シビラティ（重大度）
- 日時（DateTime）

アラーム

クラスタ、ホスト、およびVMに固有のアラームを表示するには、次の手順を実行します。

（注） HX Connect または HTML プラグインの確認済みアラームは、同等の vCenter アラームを確認しません。



手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex]** を選択します

ステップ 3 表示するクラスタ名をクリックします。

ステップ 4 [クラスタ サマリ（Cluster Summary）]タブを使用して、**[アラーム（Alarms）]** をクリックします。[アラームの詳細（Alarms Detail）]ビューが表示されます。

表 *48* : アラームの詳細

フィールド名	その他の情報
送信元	アラームのテキストによる説明。
説明	アラーム名
シビラティ（重大度）	アラームのシビラティ（重大度）レベル有効な値は、All、Info、Warning、および Error です。
Triggered Time	アラームの発生日時。 矢印を使用して、テーブルの結果をソートおよび再ソートします。
承認時刻（Acknowledged Time）	アラームが確認された時刻
確認者:	アラームを確認したユーザーの自動入力

ステップ 5 （オプション）フィルタを使用して、[アラーム テーブル（Alarms Table）]に表示される結果を制限します。

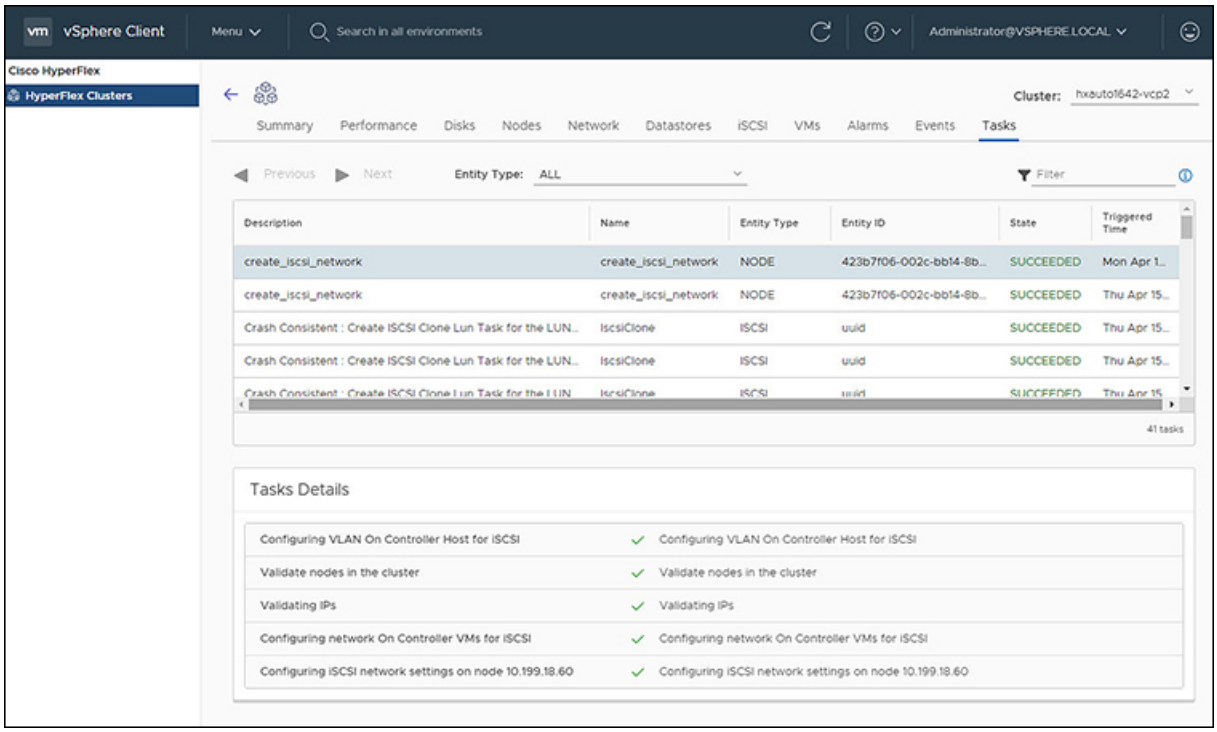
Filter	フィルタ オプション
シビラティ（重大度）	All、Info、Warning、および Error
エンティティ タイプ	All、クラスタ、ノード、仮想マシン、ディスクおよびデータストア
承認済み	All、True, および False
Filter	[フィルタ（Filter）] オプションにキーワードを入力して、ブラウザに表示されるテーブルの内容をフィルタリングします。

ステップ 6 **[確認済み（Acknowledged）]** ボタンをクリックして、アラームが表示されたことを確認します。
[確認済み（Acknowledged）] ボタンをクリックすると、**[確認者（Acknowledged by）]** フィールドにアラームを確認したユーザーが自動的に入力されます。

ステップ 7 リストからアラームを削除するには、**[グリーンにリセット（Reset To Green）]** ボタンをクリックします。

タスク

メンテナンスを検証するためにプラットフォームで発生している非同期タスクを表示するには、次の手順を実行します。



手順

ステップ 1 vSphere クライアントにログインします。

ステップ 2 **[メニュー（Menu）]** > **[Cisco HyperFlex]** > **[タスク]**を選択します

ステップ 3 表示するタスクをクリックします。
サブタスクは、タスクリストの下の表に表示されます。

表 *49* : タスクリスト

フィールド名	その他の情報
説明	タスクの説明
名前	タスク名（Task Name）
エンティティ タイプ（Entity Type）	タスクのタイプ。有効な値は、NODE、DP_Summary、Virtual Machine、Disk、および Datastore です。
エンティティ ID（Entity ID）	デバイス ID 番号
状態	タスクの成功または失敗を示します。
トリガ時刻	タスクの発生日時。

表 *50* : 作業内容

フィールド名	その他の情報
サブタスク名	タスクの名前。
成功通知	アクションの説明と、タスクが完了したときのステータス。説明の前にあるチェックアイコンは、タスクが成功したことを示します。このリストを確認して、タスクが失敗した場所を特定します。

ステップ 4 （オプション）**[エンティティタイプ（Entity Type）]** リストを使用して、テーブルの結果をフィルタリングします。

vCenter：HyperFlex プラグインの組み込みアクション

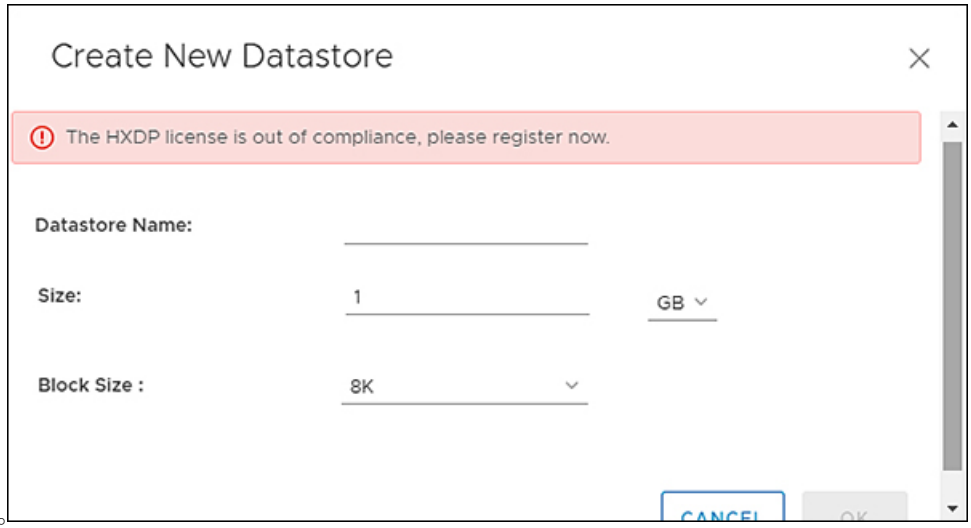
ホストおよびクラスタ レベルでの vCenter Server アクション

新しいデータストアの作成

[ホストおよびクラスタ（Hosts & Clusters）] レベルから新しいデータストアを作成するには、次の手順を実行します。

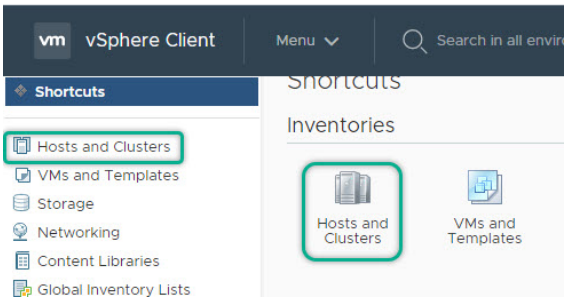
始める前に

HX リリース 5.0（1a） 以降、この機能はライセンスステータスが [In-compliance] の場合に有効になります。



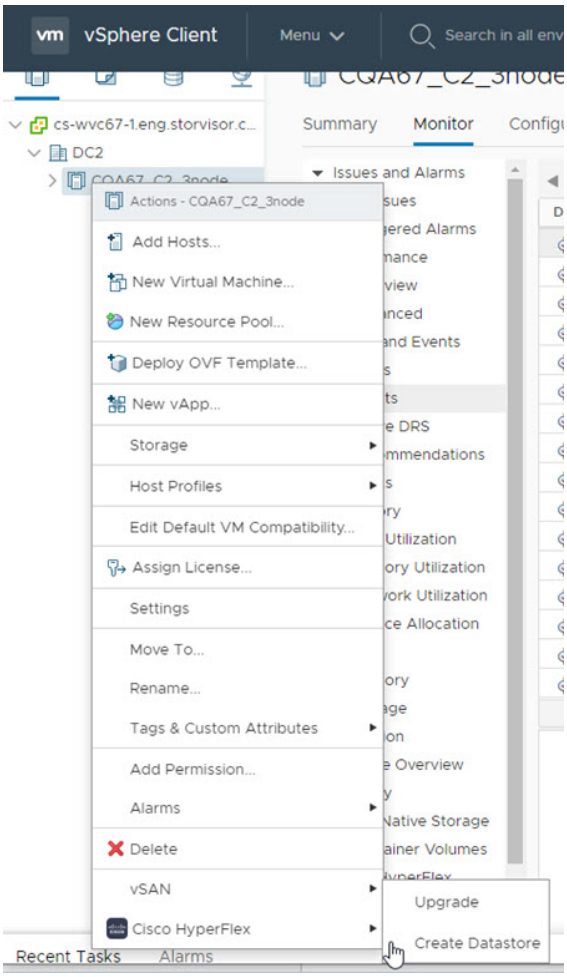
手順

ステップ 1 vSphere メニューまたは[ショートカット（Shortcut）] リンクから **[ホストおよびクラスタ（Hosts & Clusters）]** にアクセスします。



ステップ 2 クラスタを右クリックし、**[Cisco HyperFlex]** > **[アップグレード（Upgrade）]** を選択します。**アップグレード** HyperFlex Connect を起動し、アップグレード ページに直接移動してアップグレード プロセスを完了します。

ステップ 3 クラスタを右クリックし、**[Cisco HyperFlex]** > **[データストアの作成（Create Datastore）]** を選択します。



[データストア（Datastore）] ウィンドウが表示されます。

ステップ 4 [新しいデータストア] ウィンドウのフィールドに入力します。

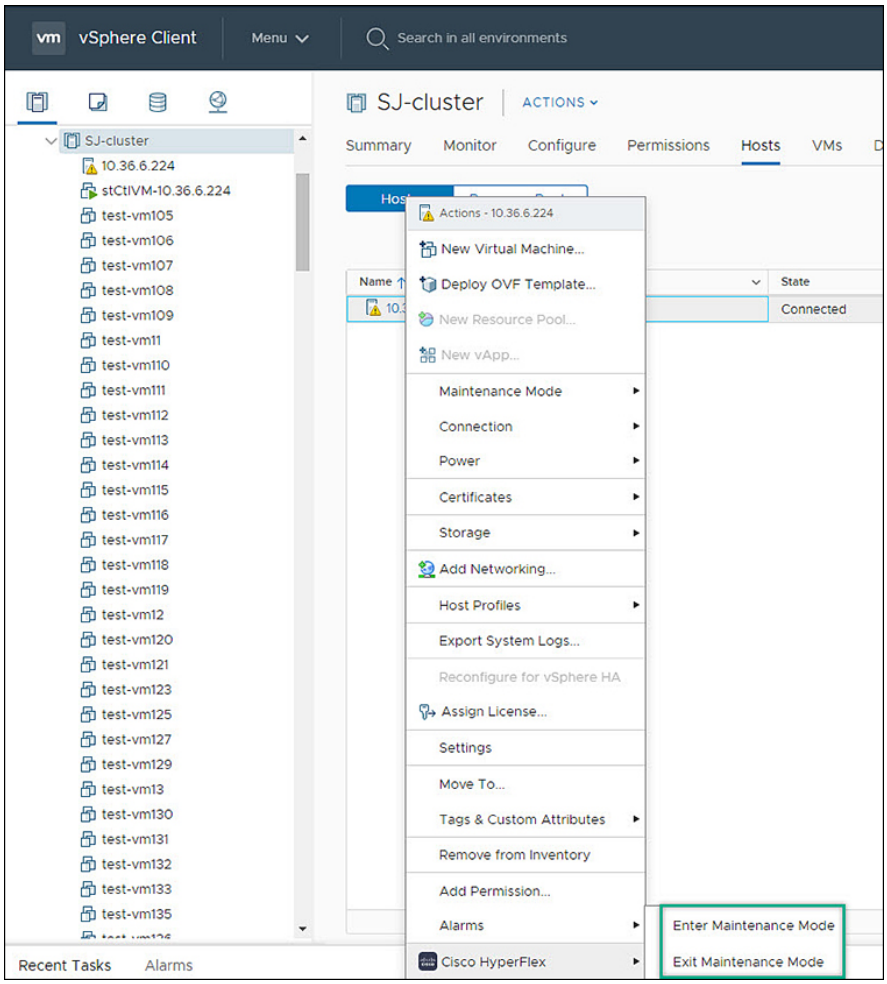
- データストア名を入力します
- [サイズ（Size）] を入力し、[GB] または [TB] を選択します。
- ブロック サイズを選択し、4K または 8K を選択します。
- **[OK]** をクリックします。

関連トピック

新しいデータストアの作成 （403 ページ）

メンテナンス モードを開始または終了します

vSphere Web UI からホスト レベルのメンテナンス モードを開始または終了するには、次の手順を実行します。



始める前に

HX リリース 5.0（1a）以降、スケジュール スナップショット機能は、ライセンス ステータスが [In-compliance] の場合に有効になります。

手順

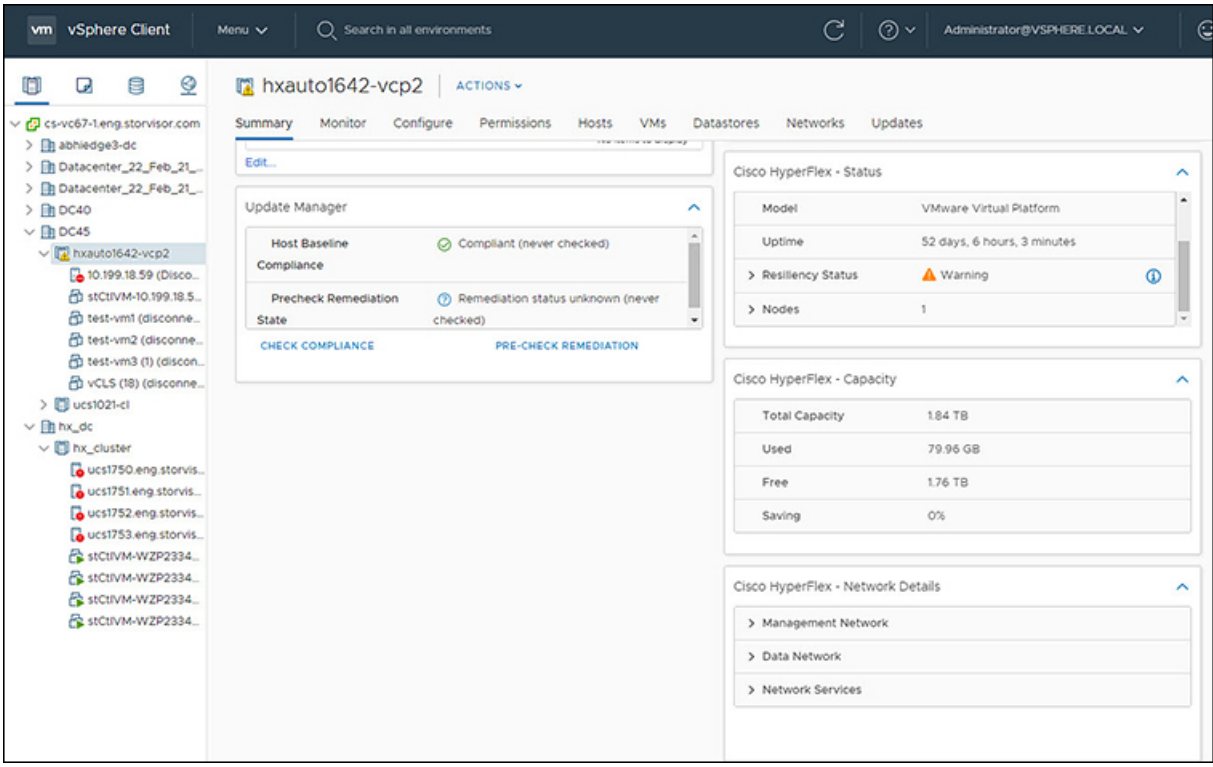
ステップ 1 vSphere メニューまたはショートカット リンクから **[ホストおよびクラスタ]** にアクセスします。

ステップ 2 クラスタ名をクリックし、**[ホスト（Hosts）]** タブを選択します。
[サマリー] ページが表示されます。

ステップ 3 ホストを右クリックし、**[Cisco HyperFlex ＞ ＞ Maintenance Mode] ＞ [Enter（or Exit）MainenanceMode]** を選択して、HyperFlex メンテナンスモードを開始または終了します。

[サマリー] タブからの HTML5 プラグイン ポートレットの表示

vSphere Web UI から Cisco HyperFlex HTML5 プラグイン ポートレットを表示するには、次の手順を実行します。



手順

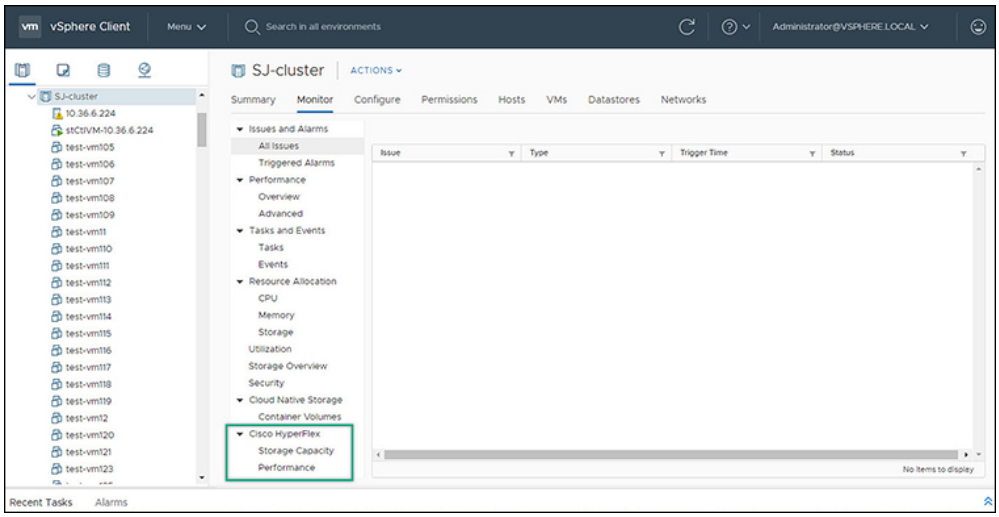
ステップ 1 vSphere メニューまたはショートカット リンクから **[ホストおよびクラスタ]** にアクセスします。
ステップ 2 クラスタ名をクリックし、**[サマリー]** タブを選択します。[サマリー] ページが表示されます。
ステップ 3 下にスクロールし、各ポートレットの矢印を使用して、ポートレットの詳細を表示または非表示にします。

関連トピック

HX クラスタ サマリーの表示 （378 ページ）

[モニタ（Monitor）]タブからの HTML5 プラグインポートレットの表示

vSphere Web UI から Cisco HyperFlex HTML5 プラグイン ポートレットを表示するには、次の手順を実行します。



手順

ステップ 1 vSphere メニューまたはショートカット リンクから **[ホストおよびクラスタ]** にアクセスします。

ステップ 2 クラスタ名をクリックし、**[モニタ（Monitor）]** タブを選択します。

ステップ 3 [モニタ（Monitor）] ナビゲーション パネルを下にスクロールし、**[Cisco HyperFlex]** を見つけます。

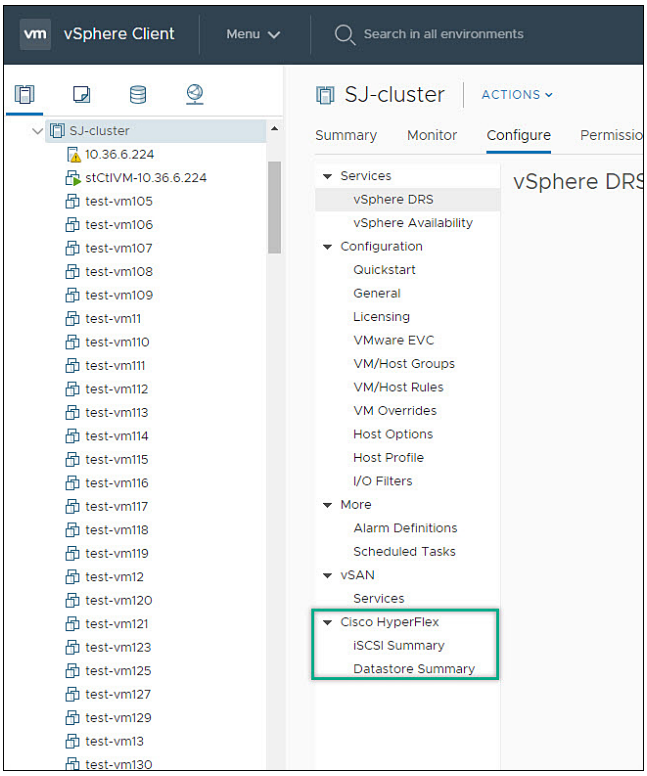
ステップ 4 **[ストレージ容量（Storage Capacity）]** または **[パフォーマンス（Performance）]** をクリックして、関連する Cisco HyperFlex HTML5 プラグイン チャートを表示します。

関連トピック

クラスタおよびデータストアのパフォーマンス チャートの表示 （385 ページ）

[Configure]タブからのiSCSIおよびデータストアの概要の表示

vSphere Web UI から iSCSI およびデータストアのサマリー ページを表示するには、次の手順を実行します。



始める前に

iSCSI 機能は、Cisco HyperFlex リリース 4.5（x）以降でサポートされています。

手順

ステップ 1 vSphere メニューまたはショートカット リンクから **[ホストおよびクラスタ]** にアクセスします。

ステップ 2 クラスタ名をクリックし、**[設定]** タブを選択します。

ステップ 3 [モニタ] ナビゲーション パネルを下にスクロールし、**[Cisco HyperFlex]** を見つけます。

ステップ 4 **[iSCSI Summary]** または **[Datastore Summary]** をクリックして、関連する[Cisco HyperFlex HTML5 Plugin] ページを表示します。

ステップ 5 ボタンを使用して、関連項目で定義されているすべてのメンテナンスタスクを実行します。

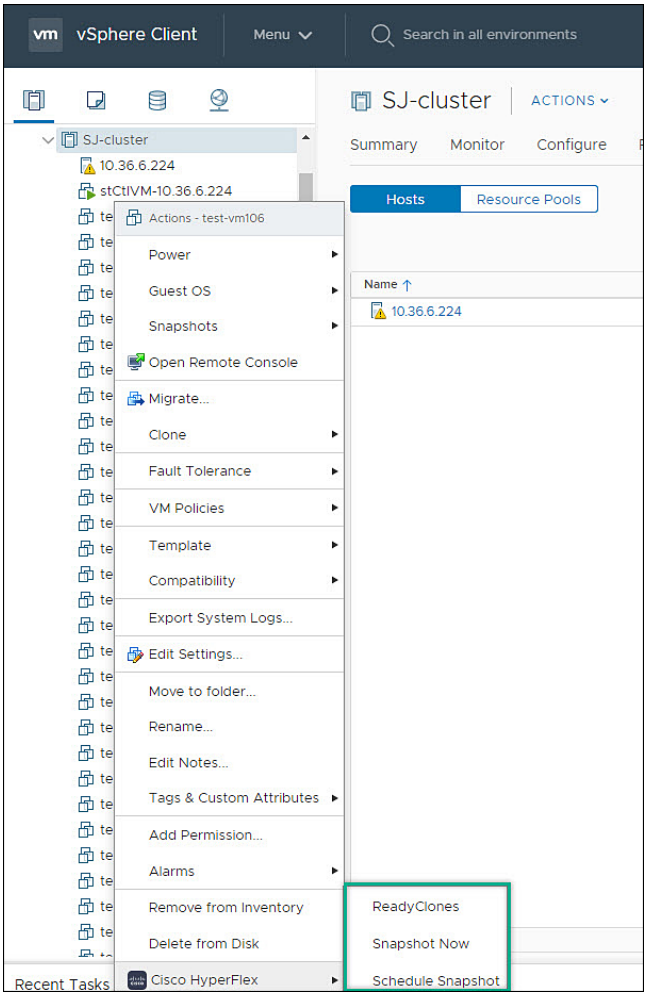
関連トピック

データストアの管理 （401 ページ）
新しいデータストアの作成 （403 ページ）
データストアの編集 （404 ページ）
データストアのマウントまたはアンマウント （405 ページ）
データストアの削除 （405 ページ）
iSCSI: ターゲット （394 ページ）

iSCSI : イニシエータ グループ （397 ページ）
iSCSI: LUNs （399 ページ）

仮想マシンレベルでの vCenter Server アクション

今すぐスナップショットを作成



始める前に

vSphere メニューまたはショートカット リンクのいずれかから **VM およびテンプレート** にアクセスします。

手順

ステップ 1 仮想マシンを右クリックします。**[Cisco HyperFlex]** > **[今すぐスナップショット（Snapshot Now）]**を選択します。

ステップ 2 **[VM Native スナップショットを取得（Take VM Native Snapshot）]** ウィンドウが表示されます。次のフィールドに入力します。

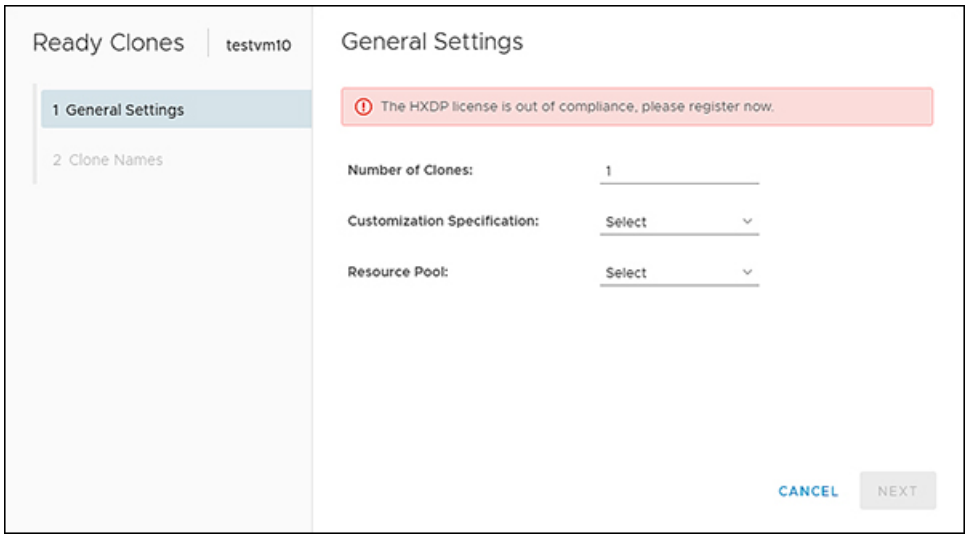
- **名前 —** スナップショット名
- **説明** - スナップショットの説明
- **[ゲスト ファイル システムの休止]** - チェックボックス

ステップ 3 **[OK]** をクリックして、VM スナップショットを作成します。バックグラウンドでアクティブなスナップショット タスクが表示されます。スナップショットが完了すると、スナップショット マネージャにリストされます。

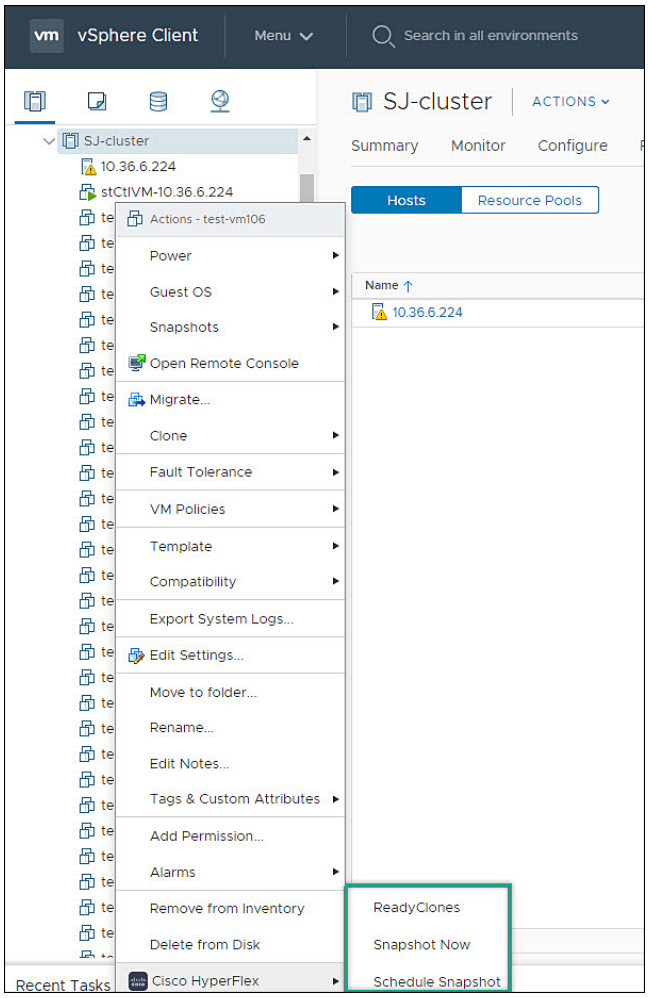
ReadyClone

始める前に

- HX リリース 5.0（1a）以降では、ライセンス ステータスが [In-compliance] の場合に ReadyClone 機能が有効になります。



- vSphere メニューまたはショートカット リンクのいずれかから **VM およびテンプレート** にアクセスします。



手順

ステップ 1 仮想マシンを右クリックします。**[Cisco HyperFlex]** > **[ReadyClone]** を選択します。

ステップ 2 **[クローン準備完了（Ready Clones）]** ウィンドウが表示されます。[一般設定（General Settings）] フィールドに入力します。

- **クローン数** - 有効なエントリ 1 ー 256
- **カスタマイズ仕様**: 設定されている場合は、リストから選択します
- **リソース プール**: 設定されている場合は、リストから選択します。

ステップ 3 [クローン名（Clone Name）] フィールドに入力します。

- **クローン後に VM を起動**: チェックボックス
- **[VM プレフィックスの名前（Name of VM Prefix）]** - VM プレフィックスを入力します。

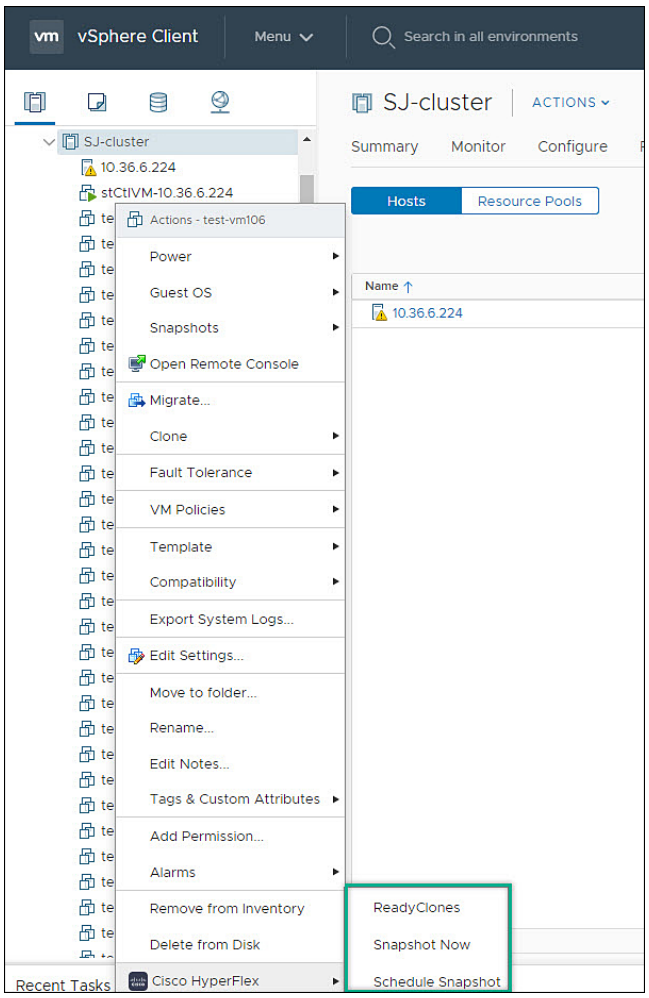
- **開始クローン番号** - デフォルトは 1 です
- **クローン番号増分値** - デフォルトは 1 です
- **ゲスト名に同じ名前を使用** — ゲスト名を指定する場合はオフにします

スナップショットのスケジュール

始める前に

- スナップショットのスケジュール機能は、Cisco HyperFlex リリース 4.5（x）以降でサポートされています。
- HX リリース 5.0（1a）以降、スケジュール スナップショット機能は、ライセンスステータスが [In-compliance] の場合に有効になります。
- 一時停止状態の VM でのスケジュールスナップショットはサポートされていません。

- vSphere メニューまたはショートカット リンクのいずれかから **VM およびテンプレート** に

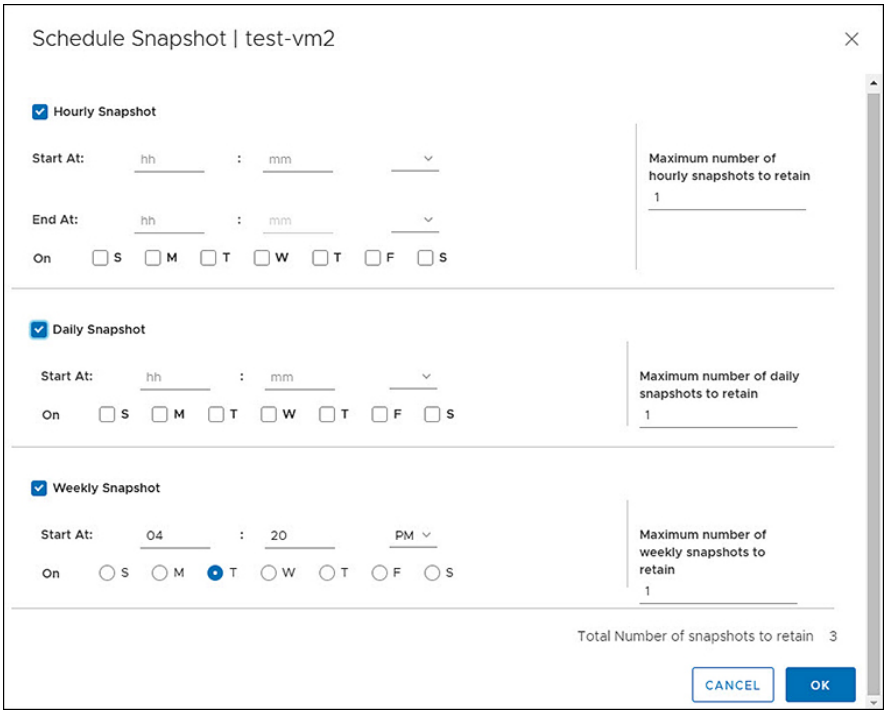


アクセスします。

手順

ステップ 1 仮想マシンを右クリックします。**[Cisco HyperFlex]** > **[スケジュールのスナップショット]**を選択します。**[スケジュールのスナップショット]** ウィンドウが表示されます。

ステップ 2 チェックボックスを使用して、スナップショットの頻度を選択します



ステップ 3 選択したスケジュールスナップショットのフィールドに入力します。

表 *51 : 1* 時間あたりのスナップショット:

開始時刻:	有効な開始時刻入力します。 • 時間：有効な値は 1ー24 です。 • 分：有効な値は 1ー60 です • AM/PM：リストから 1 つ選択します。
終了日：	有効な開始時刻入力します。 • 時間：有効な値は 1ー24 です。 • 分：有効な値は 1ー60 です • AM/PM：リストから 1 つ選択します。
オン	チェックボックスを使用して、スナップショットを取得する曜日を選択します
1 時間あたりのスナップショットの最大保持数	1ー30 の値を入力または選択します。

表 *52 :* 日次スナップショット*:*

開始時刻:	有効な開始時刻入力します。 • 時間：有効な値は 1ー24 です。 • 分：有効な値は 1ー60 です • AM/PM：リストから 1 つ選択します。
オン	チェックボックスを使用して、スナップショットを取得する曜日を選択します
1 時間あたりのスナップショットの最大保持数	1ー30 の値を入力または選択します。

表 *53 :* 週次スナップショット*:*

開始時刻:	有効な開始時刻入力します。 • 時間：有効な値は 1ー24 です。 • 分：有効な値は 1ー60 です • AM/PM：リストから 1 つ選択します。
オン	チェックボックスを使用して、週次スナップショットの開始日を選択します。
1 時間あたりのスナップショットの最大保持数	1ー30 の値を入力または選択します。

ステップ 4 **[OK]**をクリックして、スナップショットスケジュールを確認します。

ストレージ レベルでの vCenter Server アクション

データストアの編集

データストア レベルから、ユーザーは既存のデータストアを編集できます。

始める前に

vSphere メニューまたは [ショートカット（Shortcut）] リンクから**データストア**にアクセスします。

手順

ステップ 1 データストア名を右クリックします。

ステップ 2 **[Cisco HyperFlex]** > **[データストアの編集（Edit Datastore）]**を選択します。
[データストアの編集（Edit Datastore）] ウィンドウが表示されます。

ステップ 3 データストアの詳細を編集します。

ステップ 4 **[OK]** をクリックして変更を保存します。

関連トピック

データストアの編集 （404 ページ）

データストアの削除

データストア レベルから、ユーザーは既存のデータストアを削除できます。

始める前に

vSphere メニューまたは [ショートカット（Shortcut）] リンクから**データストア**にアクセスします。

手順

ステップ 1 データストア名を右クリックします。

ステップ 2 **[Cisco HyperFlex]** > **[データストアの削除（Delete Datastore）]**を選択します
[データストアの削除（Delete Datastore）] ウィンドウが表示されます。

ステップ 3 **[削除（Delete）]** ボタンをクリックします。
[データストアの削除（Delete Datastore）] ウィンドウに「Do you want to delete the datastore？」という確認の質問が表示されます。

ステップ 4 **[OK]** をクリックして削除アクションを続行するか、**[キャンセル（Cancel）]** をクリックして [データストアの削除（Delete Datastore）] ウィンドウを終了します。

関連トピック

データストアの削除 （405 ページ）

VMware vCenter 用 Cisco HyperFlex リモート プラグイン

vSphere 8.0.0 以降、vSphere リリースでサポートされているアーキテクチャはリモート プラグインのみです。

リモート プラグインは、vCenter アプライアンスから独立した独自のアプライアンスで実行されます。この自律性により、vCenter のパフォーマンスが向上し、ユーザー エクスペリエンスが向上します。

前提条件

VMware 用リモート プラグインを使用するには、次のものが必要です。

- **サポートされる Cisco HyperFlex リリース**：5.0(2a) 以降（ESXi 6.7 U3 以降）。

Cisco HyperFlex リモート プラグインの使用

次の表に、プラグインバージョンごとの機能サポートを定義します。

表 *54 : HTML5* リモート プラグイン機能のサポート

特長	プラグイン バージョン 3.0.0
登録済み HX クラスタの検出	✓
クラスタの名前変更 [9]	✓
HX クラスタ サマリーの表示	✓
クラスタおよびデータストアのパフォーマンス チャートの表示	✓
ディスク ビュー	✓
ノード ビュー	✓
HX データストア管理	✓
VM サマリーと上位 VM コンシューマ	✓
ネットワーク管理	✓
iSCSI 管理 [10]	✓
イベントおよびアラーム	✓
管理タスク	✓
仮想マシン レベルでの HX スナップショットとクローン	✓
スナップショットのスケジュール [11]	✓
HX クラスタへのユーザーとアクセスの管理	✓

アップグレードのための HX Connect の相互起動	✓
ホストおよびクラスタ レベルでの組み込み vCenter サーバ アクション	✓
HTML 5 ライセンスステータス [12]	✓
リンク モード	✓

[9] HXDP リリース 4.5（x）以降が必要です。
[10] HXDP リリース 4.5（x）以降が必要です。
[11] HXDP リリース 4.5（x）以降が必要です。
[12] HXDP リリース 5.0（x）以降が必要です。

（注） リモート プラグインとローカル プラグインの構成と機能は同じです。詳細については、このガイドの VMware vCenter の Cisco HyperFlex HTML5 プラグイン （367 ページ） セクションを参照してください。

リモートプラグインのインストール、登録、およびアップグレード

リモート プラグインのインストールと登録

リモート プラグインをインストールして登録するには、次の手順を実行します。

始める前に

アクティブなファイアウォールを使用しているユーザーは、ポート 433、9443、および 22 が開いており、トラフィックの送受信を許可していることを確認する必要があります。

デフォルト アプライアンス ログイン情報

- **ユーザー名**：vcp-admin
- **パスワード**：C^scohxplugin@1984

手順

ステップ 1 Cisco ソフトウェア ダウンロード サイトから VMware vCenter 用の Cisco HyperFlex HTML プラグインをダウンロードします。

ステップ 2 vCenter にログインし、リモート プラグイン アプライアンスを展開するホストを選択します。

ステップ 3 ホストを右クリックし、**[OVFテンプレートの展開（Deploy OVF Template）]** をクリックします。適切な静的/DHCP IP 設定を使用して、vCenter に OVA を展開します。

ステップ 4 Cisco ソフトウェア ダウンロード サイトから移動して local OVF を選択します。

リモート プラグイン アプライアンスの推奨構成設定：

- RAM：4G
- コア数：2
- データストア：50 GB の最小容量を備えた 1 つ
- 有効なネットワーク アダプタ

ステップ 5 ウィザードに従って展開プロセスを完了します。

（注） 静的/DHCP IP の割り当ては、スクリプトによってサポートされます。次の操作を行ってください。

1. アプライアンス VM コンソールを開き、デフォルトのログイン情報を使用してアプライアンスにログインします。
2. **hx-ip-address-change** と入力し、**Enter** を押してスクリプトを開始します。
3. アプライアンスの MAC アドレスの **静的** IP 構成または **DHCP IP** 設定をセットするかを選択します。

   ヒント 仮想アプライアンスに静的 IP アドレスを設定するか、MAC バインド IP で DHCP を使用することをお勧めします。

4. 静的 IP 割り当てを選択するかどうかを尋ねられたら、[IPアドレス（IP address）]、[サブネットマスク（Subnet mask）]、[ゲートウェイ（Gateway）]、および [DNS] フィールドに有効な値を入力します。DHCP IP 割り当てを選択した場合は、DNS の詳細を指定する必要はありません。
5. 静的/DHCP IP を表示するには、**ifconfig** コマンドを使用します。後で使用するために、これらを書き留めておきます。

ステップ 6 アプライアンスの IP アドレスをコピーして、ブラウザ ウィンドウに貼り付けます。

例：

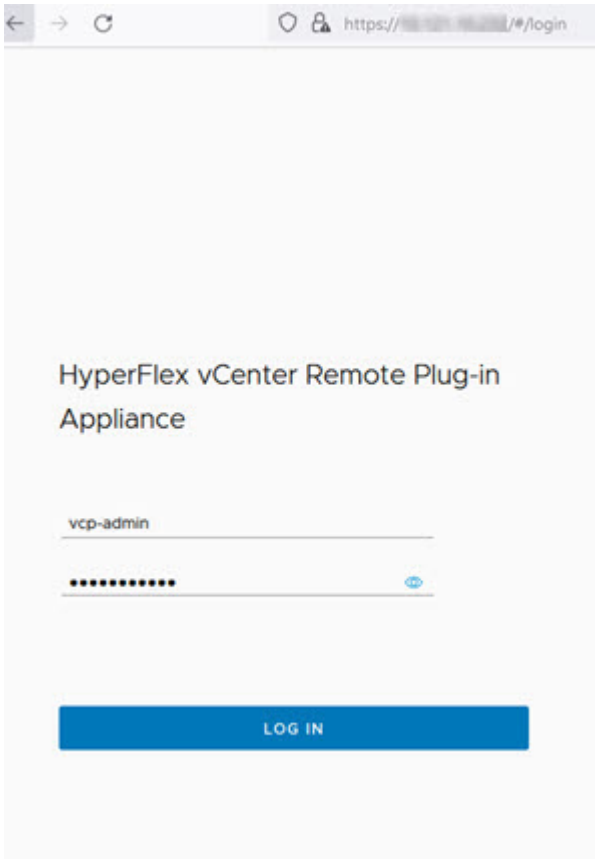
https://<appliance_ip>
UI が開きます。

ステップ 7 次の手順を使用して、コマンドラインからデフォルトのユーザー（vcp-admin）パスワードをリセットします。

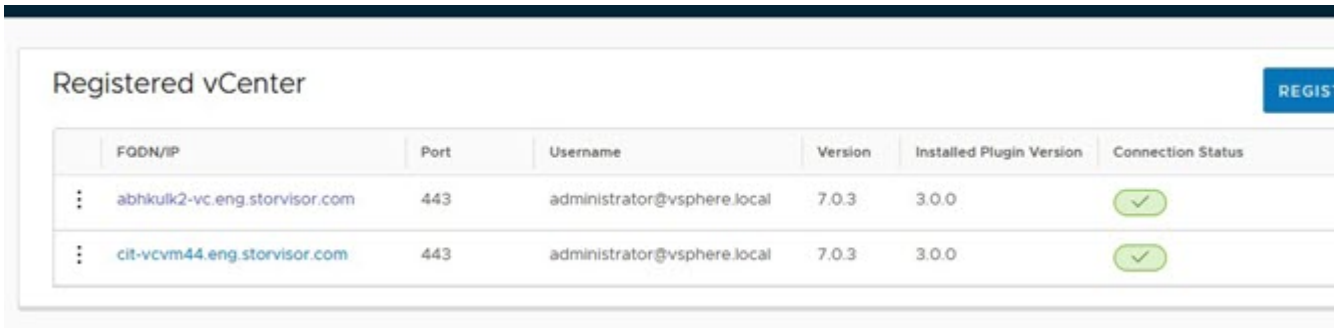
a) アプライアンス VM コンソールを開き、デフォルトのログイン情報を使用してアプライアンスにログインします。
b) **passwd vcp-admin** と入力し、**Enter** を押します。

c) UI の指示に従って古いパスワードと新しいパスワードを入力し、パスワードのリセット プロセスを完了します。

ステップ 8 新しいログイン情報を使用して HX vCenter リモート プラグイン アプライアンスにログインします。



ステップ 9 リモートプラグインを vCenter に登録するには、**[登録（Register）]** ボタンをクリックします。**[vCenter の追加（Add vCenters）]** ウィンドウが表示されます。



ステップ 10 **[vCenter の追加（Add vCenters）]** ウィンドウで **[追加（Add）]** ボタンをクリックし、指定されたフィールドに vCenter IP/FQDN、ポート番号、ユーザー名、およびパスワードを入力します。**[次へ（Next）]** をクリックします。

vCenter に到達可能で、ログイン情報が有効な場合、UI は **[プラグインの登録（Register Plugin）]** ページに進みます。

ステップ 11 **[登録（Register）]** をクリックして、登録プロセスを完了を待ちます。

ステップ 12 登録 UI に表示されるハイパーリンクを使用して、vCenter にログオンします。

ステップ 13 vSphere UI で Cisco HyperFlex HTML5 プラグイン オプションを表示するには、ログアウトして vCenter に再度ログインします。

vCenter から HyperFlex Remote プラグインのインストールと登録解除

vCenter から HX Remote プラグインをアンインストールして登録解除するには、次の手順を実行します。

手順

ステップ 1 プラグイン アプライアンス UI に移動します。

ステップ 2 有効なログイン情報でログインします。

ステップ 3 リストから登録解除する vCenter を選択し、vCenter FQDN/IP の前にあるアクション ボタンをクリックします。[登録解除（Unregister）] をクリックします。

ステップ 4 vCenter のログイン情報を指定し、vCenter からリモート プラグインを登録解除/アンインストールすることを確認します。

ステップ 5 vCenter からログアウトし、数分待ってから再度ログインします。

CLI を使用したリモート プラグイン アプリケーション 3.0.0 のアップグレード

リモートプラグインのアップグレードは2段階のプロセスです。アップグレードを完了するには、次の手順を実行します。

手順

ステップ 1 Cisco ソフトウェア ダウンロードサイトから vCenter リモート プラグインの新しいバージョンをダウンロードします。.

ステップ 2 プラグイン アプライアンス VM の /tmp ディレクトリにコピーします。

ステップ 3 **hx-plugin-upgrade <UpgradePackagePath>** コマンドを使用してアップグレード スクリプトを実行します。

ステップ 4 メッセージを慎重に確認し、**[Y]** を選択してアップグレードプロセスを続行します。

ステップ 5 vCenter アプリケーションのアップグレードが完了したら、プラグイン サーバーに登録されている各 vCenter で vCenter 拡張機能を最新バージョンに更新します。

a) **vCenter 拡張機能のアップグレード**：プラグイン アプライアンス UI にログインし、**vCenter** を選択します。

b) **[更新（Update）]** をクリックしてログイン情報を入力し、**[更新（Update）]** ボタンをクリックします。

暗号化のサポート

Remote Plugin Encryption Support

To enable remote plugin encryption, perform the following steps, For more information on enabling Software Encryption on your cluster, see Enabling HyperFlex Software Encryption Workflow.

Procedure

ステップ 1 Select the cluster you want to encrypt.

ステップ 2 Click **Datastore**.

ステップ 3 Click the **Create** button. The Create New Datastore window appears.

a) Type the Datastore Name.

b) Type the size and select GB or TB.

c) Select the Block Size, Select 4K or 8K.

d) Check the Software Encryption check box.

ステップ 4 Click OK. A new Datastore is created and added to the Datastore table list

If the new Datastore does not appear in the list, click the **Refresh**arrow and recheck the list.

サポート バンドルの生成

プラグイン サポート バンドルの生成

現在、この機能はコマンドラインを介して使用できます。これにより、アプライアンスと vCenter から必要なすべてのログ ファイルを含むサポート バンドルをユーザーがダウンロードできます。

コマンド ラインを使用して vCenter アプライアンスからサポート バンドルを生成する手順：

始める前に

vCenter のサポート バンドルを生成するには、ルート ユーザーのログイン情報が必要です。ルート ログイン情報が使用できない場合は、https://<VC_IP/FQDN>:5480（管理者のログイン情報を使用）からダウンロードします。

手順の概要

1. 事前設定されたユーザー ログイン情報を使用して vCenter アプライアンスにログインします。
2. **hx-plugin-supportbundle** コマンドを入力します。これにより、サポート バンドルを生成する vCenter の入力を求められます。
3. ルート ログイン情報を入力するか、vCenter ログをスキップして、vCenter アプライアンス ログのサポート バンドル生成を続行します。
4. デフォルトのサポート バンドルのダウンロード場所は、/var/log/plugin_support/ です。

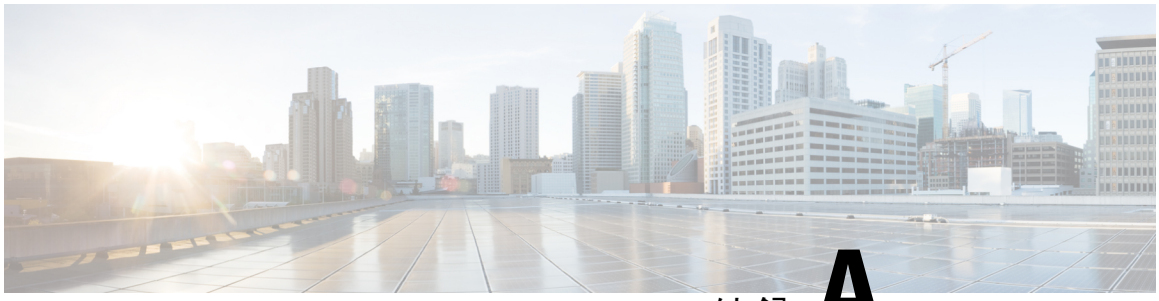
手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	事前設定されたユーザー ログイン情報を使用して vCenter アプライアンスにログインします。	
ステップ 2	**hx-plugin-supportbundle** コマンドを入力します。これにより、サポート バンドルを生成する vCenter の入力を求められます。	
ステップ 3	ルート ログイン情報を入力するか、vCenter ログをスキップして、vCenter アプライアンス ログのサポート バンドル生成を続行します。	

	コマンドまたはアクション	目的
ステップ 4	デフォルトのサポートバンドルのダウンロード場所は、/var/log/plugin_support/ です。	サポートバンドルをダウンロードするためのカスタム ディレクトリの指定がサポートされています。

サポート バンドル生成ツールのヘルプ サポートは、**hx-plugin-supportbundle -help** または **hx-plugin-supportbundle -h** です。



付録 A

付録

HX サーバ用の VLAN の作成

手順

ステップ 1 Web ブラウザを開き、Cisco UCS Manager の IP アドレスを入力します。ログイン クレデンシャルを入力します。

ステップ 2 **[LAN] タブ** > **[LAN]** > **[LAN Cloud]** > **[VLANS]** に移動します。

ステップ 3 次の表に示すように、右クリックして [Create VLANs] を選択します。

VLAN 名	**説明**	マルチキャスト ポリシー名	**VLAN ID**（デフォルト）
hx-inband-mgmt	次で使用されます。 • ESX 管理 • ストレージ コントローラ VM への SSH • HX クラスタ管理 IP：マルチキャスト トラフィックを使用 • HX データ プラットフォーム プラグイン用の HyperFlex VM への vCenter 接続	HyperFlex	3091

VLAN 名	説明	マルチキャスト ポリシー名	VLAN ID（デフォルト）
hx-storage-data	次で使用されます。 • ESX NFS クライアント（IOvisor） • HyperFlex レプリケーション/クラスタ • クラスタ データ VIP	HyperFlex	3092
hx-vmotion	次で使用されます。 • VM およびストレージ vMotion、FT、iSCSI	HyperFlex	3093
insert existing vlan name	次で使用されます。 • VM データ トラフィック	HyperFlex	任意*

（注）

- 設定オプションは [Common/Global] です。これは、両方のファブリックに適用され、いずれの状況でも同じ設定パラメータが使用されます。
- *VM データ VLAN に関する特別な推奨事項はありません。VM データ トラフィック用の独自の VLAN を作成できます。デフォルトでは、HXDP インストーラは VM データ トラフィック用の VLAN を作成しません。
- インストーラは、デフォルトで 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。

MAC アドレス プールの作成

MAC アドレスの重複を避けるために、デフォルトの MAC アドレスのブロックを変更できます。各ブロックには、デフォルトで 100 個の MAC アドレスが含まれており、UCS システムごとに最大 100 の HX サーバを展開できます。トラブルシューティングを容易にするために、vNIC ごとに 1 つの MAC プールを使用することを推奨します。

（注） 8 桁目は A または B に設定します。「A」は、ファブリック インターコネクト A にピン接続された vNIC で設定されます。「B」は、ファブリック インターコネクト B にピン接続された vNIC で設定されます。

手順

ステップ 1 Web ブラウザを開き、Cisco UCS Manager の IP アドレスを入力します。ログイン クレデンシャルを入力します。

ステップ 2 Cisco UCS Manager で **[LAN] タブ** > **[プール（Pools）]** > **[root]** > **[Sub-org]** > **[hx-cluster]** > **[MAC プール（MAC Pools）]** に移動します。

ステップ 3 [MAC Pools] を右クリックし、[Create MAC Pool] を選択します。

ステップ 4 [Create MAC Pool] ウィザードの [Define Name and Description] ページで、次に示すように必須フィールドに入力します。

MAC プール名	説明	割り当て順序	MAC アドレス ブロック
hv-mgmt-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:01:01-64
hv-mgmt-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:02:01-64
storage-data-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:03:01-64
storage-data-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:04:01-64
vm-network-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:05:01-64
vm-network-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:06:01-64
hv-vmotion-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:07:01-64
hv-vmotion-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:08:01-64

ステップ 5 [Next] をクリックします。

ステップ 6 [Create MAC Pool] ウィザードの [Add MAC Addresses] ページで、[Add] をクリックします。

ステップ 7 [Create a Block of MAC Addresses] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[First MAC Address] フィールド	ブロック内の最初の MAC アドレス。
[Size] フィールド	ブロック内の MAC アドレス数。

ステップ 8 [**OK**] をクリックします。

ステップ 9 **[終了]** をクリックします。

MAC アドレスの変更後、以前に設定されたように ESXi が再設定されます。管理 IP には DHCP が割り当てられる場合、IP が変わります。

MAC アドレス変更に対する製造プロセスの影響

- 特に顧客が UCS ファブリック インターコネクトがない HyperFlex サーバを発注する場合、製造プロセスと顧客サイトの間で MAC アドレスが変わります。
- MAC アドレスは、サービス プロファイルの関連付けの際に設定されます。サービス プロファイルの関連付けの解除の間は、設定されません。
- 製造プロセスの最後で、サービス プロファイルの関連付けが解除されます。つまり、MAC アドレスが未設定になります。
- HyperFlex サーバを導入する場合は、MAC アドレス プールを上記のように設定します。
- VMWare は Consistent Device Naming（CDN）をサポートしていますが、5.5.SR が公開されて以来、問題が報告されています。

vSwitch の設定

VMware ESX および ESXi ホストの両方で、GUI またはコマンド ラインから vSwitch を設定できます。

CLI 設定は、複数の ESX サーバをインストールして、vSwitch 設定のスクリプトを構築する際に非常に便利です。

ESX のインストール後、次の手順で ESX ホストの vSwitch を設定します。

手順

ステップ 1 各 ESX サーバのコマンド ラインにログインします。

ステップ 2 リストされた名前を使用して、各 ESX サーバで 3 つの vSwitch を作成します。

- **vswitch-hx-storage-data**

  スイッチで MTU を 9000 に設定します。

- **vmotion**

  スイッチで MTU を 9000 に設定します。

- **vswitch-hx-vm-network**

ステップ 3 次の CLI コマンドを使用して、3 つの新しい vSwitch を作成します。

```
# esxcli network vswitch standard add -v vswitch-hx-storage-data
# esxcli network vswitch standard set -v vswitch-hx-storage-data -mtu= 9000
# esxcli network vswitch standard add -v vswitch-vmotion
# esxcli network vswitch standard set -v vswitch-vmotion -mtu=9000
```

```
# esxcli network vswitch standard add -v vswitch-hx-vm-network
```

ステップ 4 ESXi のインストール時に作成されるデフォルトの vSwitch **vSwitch0** は、Hx データ プラットフォーム ノードのセットアップ スクリプトが機能するように、「**vswitch-hx-inband-mgmt**」に名前を変更する必要があります。次のコマンドを使用してスイッチの名前を変更してから、vmkernel がコンフィギュレーション ファイルを再度読み取り、新しい名前を使用するように、ホストを再起動します。

```
# sed -i 's/vSwitch0/vswitch-hx-inband-mgmt/g' /etc/vmware/esx.conf
```

```
# reboot
```

ステップ 5 次のコマンドを使用して、ホストの再起動後に、vSwitch の作成と名前の変更が確認できます。

```
# esxcli network vswitch standard list
```

前述の 4 つの vSwitch がコマンド出力に表示されていることを確認します。switch-hx-inband-mgmt vSwitch だけがアップリンクおよびポート グループをリストアップします。HX Data Platform インストーラ スクリプトは、残りのネットワーク構成を実行します。

仮想分散スイッチ（VDS）または Cisco Nexus 1000v（N1Kv）への vMotion ネットワークの移行

（注）
- HX に依存しない以下の特定のネットワークでは、VMware DVS または Cisco Nexus 1000v を使用して HX Data Platform を設定できます。

  vMotion ネットワーク

  仮想マシン ネットワーク
- 詳細については、Cisco Nexus 1000v のドキュメントを参照してください。

HX に依存しない vSwitch と関連するポート グループを DVS ネットワークまたは N1Kv ネットワークに移行するには、次の手順を実行します。

手順

ステップ 1 vCenter から、DVS スイッチおよびポート グループを作成します。

a) **[vCenter Inventory Lists] > [Datacenters] > [datacenter] > [Related Objects] > [Distributed Switches]** の順に選択します。[Add Distributed Switch] アイコンをクリックします。

b) [New Distributed Switch] ウィザードを完了します。2 つのアップリンクを使用して各 DVS スイッチを作成します。

例：VM ネットワークと vmotion pg

- DVSwitch-VMNetwork：DVPortGroup-VMNetwork
- DVSwitch-Vmotion：DVPortGroup-Vmotion

ステップ 2 vSwitch、VMNetwork を移行します。VMNetwork を、従来の vSwitch から DVS に移行するには、次の手順を実行します。

a) **[vCenter Inventory Lists]** > **[Datacenters]** > **[datacenter]** > **[Related Objects]** > **[Distributed Switches]** の順に選択します。

b) [DVSwitch-VMNetwork vSwitch] を選択します。[Add and Manage Hosts] アイコンをクリックします。**[Add and Manage Hosts (ホストの追加と管理)]** ウィザードが起動します。

c) [Select task] ページで、[Add Hosts] を選択します。[Next] をクリックします。

d) [Select hosts] ページで、[Add New Hosts] をクリックします。クラスタ内のすべてのホストを選択します。[Next] をクリックします。

e) [Select network adapter tasks] ページで、[Manage physical adapters] と [Migrate virtual machine networking] を選択します。[Next] をクリックします。

f) [Manage physical network adapters] ページで、vswitch-hx-vm-network：VM ネットワークの一部である物理アダプタが DVSwitch-VMNetwork に割り当てられます。

g) **[On other switches/unclaimed list (他のスイッチ/要求解除リスト)]** で、**スイッチで使用中の** vswitch-hx-vm-network に対応する vmnic を選択します。

h) **[Assign (割り当て)]** アップリンクをクリックします。

i) [自動割り当て] を選択します。

j) **[OK]** をクリックします。ページが更新され、新しく割り当てられた vmnic が [On this switch] にリストされます。

k) [Analyze impact] ページに、この移行による影響が表示されます。影響がすべてグリーンであることを確認します。[Next] をクリックします。

l) [Migrate VM networking] ページで、新しいネットワーク DVPortGroup-VMNetwork に移行する VM を選択します。

Next

すべてのホストから、コントローラ VM、stCtlVM を除くすべての VM を選択します。[DVPortGroup-VMNetwork] を選択します。[Next] をクリックします。

（注） 各ホストの VM のリストには、コントローラ VM を含むすべての VM が含まれています。コントローラ VM は選択しないでください。コントローラ VM を移行すると、ストレージ クラスタが中断されます。

m) [Ready to complete] ページで、移行の概要を確認します。[Finish] をクリックします。

（注） 移行後のシステムによって、複数のネットワーク関連のアラームが生成されます。アラームを確認し、クリアします。

ステップ 3 vmotion pg に vSwitch を移行します。vmotion pg を、従来の vSwitch から DVS に移行するには、次の手順を実行します。

a) **[vCenter Inventory Lists]** > **[Datacenters]** > **[datacenter]** > **[Related Objects]** > **[Distributed Switches]** の順に選択します。

b) [DVSwitch-Vmotion vSwitch] を選択します。[Add and Manage Hosts] アイコンをクリックします。**[Add and Manage Hosts (ホストの追加と管理)]** ウィザードが起動します。

c) [Select task] ページで、[Add Hosts] を選択します。[Next] をクリックします。

d) [Select hosts] ページで、[Add New Hosts] をクリックします。クラスタ内のすべてのホストを選択します。[Next] をクリックします。

e) [Select network adapter tasks] ページで、タスク [Manage physical adapters] と [Manage VMkernel adapters] を選択します。[Next] をクリックします。

f) **[Manage physical network adapters (物理ネットワーク アダプタの管理)]** ページで、vmotion:vmotion pg の物理アダプタ部分が DVSwitch-Vmotion に割り当てられます。

[On other switches/unclaimed (他のスイッチ/要求解除)] リストで、スイッチで使用中の vmotion に対応する vmnic を選択します。[Assign uplink] をクリックし、[Auto-assign] を選択して [OK] をクリックします。ページが更新され、新しく割り当てられた vmnic が [On this switch] にリストされます。[Next] をクリックします。

g) **[Manage VMkernel network adapters (VMkernel ネットワーク アダプタの管理)]** ページで、VMkernel アダプタをポート グループ DVPortGroup-Vmotion に移行します。

各ホストに対し、**[On other switches (他のスイッチ)]** で、**スイッチで使用中**の vmotion に対応する VMKernel アダプタを選択します。[Assign port group] をクリックします。宛先ポート グループ、DVPortGroup-Vmotion を選択します。[OK] をクリックします。ページが更新され、VMkernel ネットワーク アダプタが再度割り当てられ、送信元ポート グループと宛先ポート グループがリストされます。

h) 新しいネットワーク、DVPortGroup-Vmotion に移行するホストを選択します。[Next] をクリックします。

i) [Ready to complete] ページで、移行の概要を確認し、[Finish] をクリックします。

ステップ 4 移行後の手順：IO、ネットワークの接続性、および VM の移行について、VM に影響がないことを確認します。

付録

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。