



Cisco HyperFlex Data Platform リリース 3.0 アドミニストレーションガイド

初版：2018年4月24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/>

Full Cisco Trademarks with Software License

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとしません。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとしません。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとしません。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



目次

Full Cisco Trademarks with Software License iii

第 1 章

HX ストレージ クラスタの概要 1

- Cisco HX Data Platform の概要 1
- ストレージ クラスタの物理コンポーネントの概要 2
- HX Data Platform キャパシティの概要 3
 - キャパシティ削減の理解 5
 - ストレージ容量イベントメッセージ 6
- HX Data Platform のハイ アベイラビリティの概要 7
 - ストレージ クラスタ ステータス 7
 - 動作ステータスの値 8
 - 復元力ステータスの値 8
 - HX Data Platform クラスタの耐障害性 9
 - データ レプリケーション係数の設定 11
 - クラスタ アクセス ポリシー 11
 - ストレージ クラスタ ノード障害に対する応答 12
- HX Data Platform ReadyClone の概要 18
- HX Data Platform ネイティブ スナップショットの概要 18

第 2 章

HX Data Platform インターフェイスへのログイン 21

- HyperFlex クラスタ インターフェイスの概要 21
 - HX Data Platform ログイン クレデンシャルに関するガイドライン 22
 - HX Data Platform の名前、パスワード、文字 24

HX Connect へのログイン	28
コントローラ VM (stcli) コマンドラインへのログイン	30
ストレージコントローラパスワードの変更	32
Cisco HX データ プラットフォーム インストーラの導入	32
HX Data Platform REST API へのアクセス	33
Cisco HX Data Platform プラグインへのアクセス	34
Cisco TAC への連絡	35

第 3 章

HX ストレージ クラスタのモニタリング	37
HyperFlex クラスタのモニタリング	37
パフォーマンス チャートの表示	37
ストレージ クラスタのパフォーマンス チャート	38
ホスト パフォーマンスのチャート	38
データストア パフォーマンスのチャート	38
[Performance] ポートレット	39
[Datastore Trends] ポートレット	39
パフォーマンス チャートのカスタマイズ	40
パフォーマンス期間の指定	40
カスタム範囲の指定	41
パフォーマンス チャートの選択	41
HX Data Platform プラグイン インターフェイスの使用法	42
Cisco HX Data Platform プラグインと vSphere Web クライアントの統合	43
Cisco HX Data Platform プラグインと vSphere インターフェイス間のリンク	43
Cisco HX Data Platform プラグイン タブの概要	43
HX Connect を使用した HyperFlex クラスタのモニタリング	44
[Dashboard] ページ	44
[Activity] ページ	46
[System Information Overview] ページ	47
[Nodes] ページ	50
[Disks] ページ	51

第 4 章

HX ストレージ クラスタ メンテナンスの準備 55

- ストレージ クラスタのメンテナンス操作の概要 55
- シリアル操作とパラレル操作 57
- クラスタ ステータスの確認 58
- ビーコンの設定 58
- HX クラスタの vMotion の設定の確認 59
- ストレージ クラスタ ノードのメンテナンス モード 60
- Cisco HyperFlex のメンテナンス モードの開始 61
- Cisco HyperFlex のメンテナンス モードの終了 62
- バックアップ操作の作成 64
- HX ストレージ クラスタのシャットダウンと電源オフ 65
- HX ストレージ クラスタの電源オンと起動 67
- vNIC または vHBA の変更後の PCI パススルーの設定 69

第 5 章

HX ストレージ クラスタの管理 71

- クラスタ アクセス ポリシー レベルの変更 71
- クラスタの再調整 71
 - 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 72
- スペース不足エラーの処理 73
 - クリーナー スケジュールの確認 74
- vCenter 間でのストレージ クラスタの移動計画 74
 - 現在の vCenter Server から新しい vCenter Server へのストレージ クラスタの移動 75
 - vCenter クラスタからのストレージ クラスタの登録解除 75
 - EAM 拡張機能の登録解除および削除 76
 - vSphere クライアントからの HX Data Platform ファイルの削除 78
 - HX クラスタが vCenter から登録解除されたことの確認 79
 - 新しい vCenter クラスタへのストレージ クラスタの登録 79
 - クラスタの名前変更 80

第 6 章

暗号化の管理 83

自己暗号化ドライブの概要	83
HyperFlex クラスタが暗号化できることの確認	84
ローカル暗号化キーの構成	84
ローカル暗号化キーの変更	85
ローカルの暗号化キーの無効化	85
暗号化されたディスクを安全に消去する	86
リモート キー管理	86
証明書署名要求の生成	87
CSR（証明書署名要求）を使用したキー管理サーバの構成	88
自己署名証明書の生成	89
SSC（自己署名証明書）を使用したキー管理サーバの構成	91
暗号化のやり直し	92

第 7 章

データストアの管理	93
データストアの管理	93
データストアの追加	94
データストアの編集	94
データストアのマウント	95
データストアのマウント解除	96
データストアの削除	97
部分的にマウント解除されたデータストアの回復	97

第 8 章

ディスクの管理	99
クラスタ内のディスクの管理	99
ディスクの要件	100
自己暗号化ドライブ（SED）の交換	104
SSD の交換	106
NVMe SSD の交換	108
ハウスキーピング SSD の交換	109
ハードディスク ドライブの交換または追加	111

第 9 章

ノードの管理 113

ノードの管理 113

ノードメンテナンス方法の特定 115

DNS アドレスまたはホスト名による検索 118

ESXi ホスト ルート パスワードの変更 119

ノードソフトウェアの再インストール 119

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 120

ノードコンポーネントの交換 121

ノードの取り外し 123

ノード削除の準備 125

オンラインストレージクラスタからのノードの削除 127

オフラインストレージクラスタからのノードの削除 129

ノードの交換 131

第 10 章

HX コントローラ VM の管理 137

ストレージコントローラ VM の管理 137

ストレージコントローラ VM の電源のオン/オフ 137

第 11 章

ReadyClone の管理 139

HX Data Platform ReadyClone の概要 139

HX Data Platform ReadyClone の利点 140

サポート対象のベース VM 140

ReadyClone の要件 141

ReadyClone のベストプラクティス 141

HX 接続を使用して Readyclone を作成する 141

HX データプラットフォームプラグインを使用した ReadyClone の作成 143

HX Data Platform ReadyClone のカスタマイズの準備 145

vSphere Web クライアント内での Linux 向けカスタマイズ仕様の作成 145

vSphere Web クライアント内での Windows 向けカスタマイズ仕様の作成 146

カスタマイズ仕様を使用した ReadyClone の設定 146

仮想マシン ネットワーキングの管理 147

第 12 章

ネイティブ スナップショットの管理 149

HX Data Platform ネイティブ スナップショットの概要 149

HX Data Platform ネイティブ スナップショットの利点 150

ネイティブ スナップショットの考慮事項 151

ネイティブ スナップショットのベストプラクティス 153

SENTINEL スナップショットについて 154

ネイティブ スナップショットのタイムゾーン 155

スナップショットの作成 156

スナップショットのスケジューリングの概要 157

スナップショットのスケジューリング 158

スケジュール済みスナップショットの頻度の設定 159

スナップショット スケジュールの削除 159

スナップショットの復元 160

スナップショットの削除 161

第 13 章

異なる HXDP バージョンで動作するクラスタの管理 163

異なる HXDP バージョンで動作するクラスタの管理 163

シナリオ—HXDP 3.0 でサイト A および HXDP 2.6 でサイト B 163

シナリオ: HXDP 2.6 のサイト A および HXDP 3.0 のサイト B 165

機能の制限 167

第 14 章

仮想マシンのディザスタ リカバリの管理 169

データ保護の概要 169

レプリケーションとリカバリの考慮事項 170

レプリケーション ネットワークとペアリングの考慮事項 172

データ保護の用語 173

仮想マシンの保護の概要 174

データ保護のワークフロー 175

レプリケーション ペアの概要 176

レプリケーション ペアの作成	177
レプリケーション ペアの編集	179
レプリケーション ペアの削除	180
保護グループの作成	181
保護グループの編集	183
保護グループの削除	184
既存の保護グループでの仮想マシンの保護	184
新しい保護グループでの仮想マシンの保護	185
個別の仮想マシンの保護	188
仮想マシンの保護の解除	190
ディザスタ リカバリの概要	190
仮想マシンのリカバリのテスト	191
仮想マシンのリカバリ	193
保護グループの仮想マシンのリカバリ	194
計画された移行ワークフロー	195
未計画の移行ワークフロー	197
障害後の仮想マシンの保護	199
仮想マシンのフェールバック	199
レプリケーション メンテナンスの概要	200
レプリケーションの一時停止	200
レプリケーションの再開	201

第 15 章**ユーザの管理 203**

HyperFlex ユーザの管理の概要	203
ユーザ管理用語	205
AAA アカウンティングの監査ログ	205
HX データ プラットフォーム RBAC ユーザの作成	206
ユーザへの権限の割り当て	206



第 1 章

HX ストレージ クラスタの概要

- [Cisco HX Data Platform の概要 \(1 ページ\)](#)
- [ストレージ クラスタの物理コンポーネントの概要 \(2 ページ\)](#)
- [HX Data Platform キャパシティの概要 \(3 ページ\)](#)
- [HX Data Platform のハイ アベイラビリティの概要 \(7 ページ\)](#)
- [ストレージ クラスタ ステータス \(7 ページ\)](#)
- [HX Data Platform クラスタの耐障害性 \(9 ページ\)](#)
- [ストレージ クラスタ ノード障害に対する応答 \(12 ページ\)](#)
- [HX Data Platform ReadyClone の概要 \(18 ページ\)](#)
- [HX Data Platform ネイティブ スナップショットの概要 \(18 ページ\)](#)

Cisco HX Data Platform の概要

Cisco HyperFlex Data Platform (HX Data Platform) は、シスコ サーバをコンピューティングとストレージ リソースの単一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。ネットワークストレージの必要性が解消され、仮想環境でのコンピューティングとストレージ間のシームレスな相互運用が可能となります。Cisco HX Data Platform は、耐障害性の高い分散ストレージシステムを提供することで、データの整合性を維持し、仮想マシン (VM) ストレージのワークロードを最適化します。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。これには、Cisco ファブリック インターコネクタ (FI)、Cisco UCS Manager、Cisco HX 固有のサーバ、Cisco コンピューティング専用サーバ (VMware vSphere、ESXi サーバ、および vCenter)、Cisco HX Data Platform インストーラ、コントローラ VM、HX Connect、vSphere HX Data Platform Plug-in、および `stcli` コマンドが含まれます。

Cisco HX データ プラットフォームは、VMware vSphere などの仮想化プラットフォームにインストールされます。インストール時に、Cisco HyperFlex HX クラスタ名を指定した後、HX データ プラットフォームは、ノードごと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

ノードは、ストレージクラスタに追加してコンピューティング専用リソースを増やすことができます。

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の HX Data Platform によってモニタされます。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、ディスク領域、メモリ、データ処理、電源、ネットワーク I/O などのコンピューティングとストレージのリソースを提供します。

コンバージドノードがストレージクラスタに追加されると、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、関連付けられているドライブを介してストレージクラスタにストレージリソースを追加します。

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。 `stcli` 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がストレージクラスタに追加されると、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。 `stcli` 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。

ディスクが追加または取り外されると、HX Data Platform がストレージクラスタを再調整して、ストレージリソース内の変更を調節します。

コンバージドノードでのディスクの追加や取り外しは、HX Data Platform を介しては実行されません。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、サーバハードウェアガイドを参照してください。

- **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、HX Data Platform によって管理される、組み合わせての使用が可能な物理ストレージです。

データストアは、ストレージの使用とストレージリソースの管理のために HX Data Platform で使用される論理コンテナです。

データストアは、ホストが仮想ディスクファイルと他の VM ファイルを配置する場所です。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

HX Data Platform では、キャパシティの概念は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。値はベース 2 (GiB/TiB) で測定されますが、簡略化と一貫性のために、GB または TB というラベルが付けられます。

- **[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。このプロセスが完了した後、すべてのストレージクラスタデータストアの合計キャパシティは、メタデータを除いて、ストレージクラスタキャパシティの合計と同程度の範囲である必要があります。リストされているデータストアキャパシティは、通常は HX ストレージクラスタキャパシティと一致しません。cleaner コマンドに関する情報については、『*Cisco HX Data Platform Command Line Interface Reference guide*』を参照してください。
- **[Cluster capacity]** : ストレージクラスタ内のすべてのノード上の、すべてのディスクのすべてのストレージです。これには、クリーンアップされていないデータと各ディスクのメタデータのオーバーヘッドが含まれます。
クラスタの合計/使用/未使用キャパシティは、ストレージキャパシティの全体と、ストレージが使用されている量に基づいています。
- **[Condition]** : HX Storage Cluster が空間イベント状態になると、[Free Space Status] フィールドが表示されます。[Condition] フィールドには、空間イベント状態状態が表示されます。オプションは、[Warning]、[Critical]、および [Alert] です。
- **[Datastore capacity]** : オーバー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、これはストレージクラスタキャパシティに非常に近くなりますが、完全に一致するわけではありません。これには、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/未使用キャパシティは、データストアの (シン) プロビジョニングキャパシティに基づいています。データストアはシンプロビジョ

ニングされているため、プロビジョニングキャパシティ（データストア作成時に管理者が指定）は実際のストレージを超えることができます。

- **[Free Capacity, storage cluster]**：使用可能なキャパシティと同じです。ストレージクラスタの場合、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になります。
- **[Free Capacity, datastore]**：使用可能なキャパシティと同じです。すべてのストレージクラスタ データストアの場合、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になります。

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ていません。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ため、ストレージクラスタのキャパシティの可用性が低く示される一方で、**[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がより大きく示される場合があります。

- **[Multiple users]**：別個のデータストアに、それぞれ異なるキャパシティをプロビジョニングすることができます。いずれの時点においても、ユーザは割り当てられたデータストアキャパシティのすべてを使用しないでください。複数のユーザにデータストア キャパシティを割り当てる場合、各ユーザにプロビジョニングされたキャパシティが受け取られたかを確認するのは管理者の責任です。
- **[Over-provisioning]**：すべてのデータストアに割り当てられたストレージ キャパシティの量が、ストレージクラスタに使用できる量を超えると発生します。

最初は、オーバー プロビジョニングをするのが一般的です。これにより、管理者はまずキャパシティを割り当ててから、後で実際のストレージに合わせていくことができます。

値は、使用可能なキャパシティとプロビジョニングされたキャパシティとの差です。

有効な最大物理量よりも多くの領域が割り当てられない限り、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キャパシティを見直し、システムが領域不足の状態に達していないことを確認してください。

- **[Provisioned]**：ストレージ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、単独のストレージクラスタ データストアでの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が、同一のストレージキャパシティからプロビジョニングされたストレージになる場合があります。

- **[Space Needed]**：HX Storage Clusterが空間イベント状態になると、**[Free Space Status]** フィールドが表示されます。**[Space Needed]** は、リストされた **[Condition]** をクリアできるようにする必要があります、ストレージの量を示します。
- **[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るストレージキャパシティの量です。

HX Data Platform の内部メタデータにより、0.5% から 1% の領域が使用されます。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 Plug-in または HX Connect に [Used] ストレージの値が表示される場合があります。

ストレージの [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ています。

- [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の容量です。

キャパシティ削減の理解

[Summary] タブの [Capacity] ポートレットには、重複排除と、ストレージクラスタによる圧縮による削減量が表示されます。たとえば、全体的な削減量が 50% の場合、キャパシティが 6TB のストレージクラスタでは、実質 9 TB のデータを保存できます。

HX Data Platform システムで削減される合計のストレージキャパシティは、次の 2 つの要素で計算されます。

- **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。重複排除は、冗長データの削除によって記憶域を削減する手法です。重複のないデータのインスタンスが 1 つだけ保存されます。

重複排除と圧縮による削減は、同時に追加されるだけのものではありません。また、それぞれ独立した操作でもありません。これらは、次のような仕組みで関連しています。まず、原則として、ストレージで使用される固有のバイト量は重複排除を介して削減されます。そして、重複排除されたストレージの使用分が圧縮され、ストレージクラスタでさらに多くのストレージが使用できるようになります。

VM クローンをを使用する場合、重複排除と圧縮による削減は有用です。

削減量が 0% と表示される場合、ストレージクラスタは新規クラスタです。ストレージクラスタへの採取データの合計では、有意なストレージ削減量を判断するには不十分です。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ちます。

次に例を示します。

1. 初期値

100 GB の VM が 2 回クローニングされると仮定します。

Total Unique Used Space (TUUS) = 100GB

Total Addressable Space (TAS) = 100x2 = 200 GB

この例では次のようになります。

Total Unique Bytes (TUB) = 25 GB

2. 重複排除による削減

$$\begin{aligned}
 &= (1 - \text{TUUS}/\text{TAS}) * 100 \\
 &= (1 - 100\text{GB} / 200\text{GB}) * 100 \\
 &= 50\%
 \end{aligned}$$

3. 圧縮による削減

$$\begin{aligned}
 &= (1 - \text{TUB}/\text{TUUS}) * 100 \\
 &= (1 - 25\text{GB} / 100\text{GB}) * 100 \\
 &= 75\%
 \end{aligned}$$

4. 計算後の合計削減量

$$\begin{aligned}
 &= (1 - \text{TUB}/\text{TAS}) * 100 \\
 &= (1 - 25\text{GB} / 200\text{GB}) * 100 \\
 &= 87.5\%
 \end{aligned}$$

ストレージ容量イベントメッセージ

クラスタ ストレージ容量には、ストレージクラスタ内のすべてのノード上のすべてのディスクのすべてのストレージが含まれます。この使用可能な容量は、データの管理に使用されます。

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、HX Data Platform Plug-in の [Alarms] と [Events] ページに表示されます。



(注) 警告または重大なエラーが表示された場合：

容量を拡張するために新しいドライブまたはノードを追加します。加えて、未使用の仮想マシンとスナップショットの削除を検討します。ストレージ容量が減少するまで、パフォーマンスは影響を受けます。

- **SpaceWarningEvent**：問題とエラー。これは第 1 レベルの警告です。

クラスタ 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 Storage Clusterの容量合計の 70%）を下回るまで削減します。

- **SpaceAlertEvent**：問題とエラー。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発行されますが、まだ警告しきい値を上回っています。

クラスタ 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 Storage Clusterの容量合計の80%）を下回るまで削減し続けます。

- **SpaceCriticalEvent**：問題とエラー。これは重大レベルの警告です。

クラスタは、読み取り専用状態にあります。

使用されているストレージ容量がこの警告しきい値（HX Storage Clusterの容量合計の92%）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**：これは情報です。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す。

HX Data Platform のハイ アベイラビリティの概要

HX Data Platform のハイ アベイラビリティ（HA）機能においては、通常動作時で3つ以上のノードが完全に機能し、ストレージクラスタがすべてのデータの複製を少なくとも2つ維持できるようにします。

ストレージクラスタ内のノードまたはディスクで障害が発生すると、クラスタの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内のノード数とデータ レプリケーション係数やアクセス ポリシーの設定を加味して、ノード障害に起因するストレージクラスタの状態が決定されます。



- (注) HX Data Platform HA 機能を使用する前に、vSphere Web Client の DRS および vMotion を有効にします。

ストレージクラスタ ステータス

HX Data Platform ストレージクラスタのステータスに関する情報は、HX Connect、HX Data Platform Plug-in、ストレージコントローラ VM `stcli` コマンドを使用して利用されます。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**：一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、アプリケーションがI/Oを実行できるかどうかを示します。

動作ステータスのオプションを次に示します。

- **[Online]** : クラスタはI/Oに対応する準備ができています。
- **[Offline]** : クラスタはI/Oに対応する準備ができていません。
- **[Out of space]** : クラスタ全体でスペースが不足しているか、1つまたは複数のディスクでスペースが不足しています。どちらの場合も、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ができませんが、静的なクラスタ情報の表示は続行できます。
- **[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ができませんが、静的なクラスタ情報の表示は続行できます。
- **[Unknown]** : これは、クラスタがオンラインになるときの移行状態です。

クラスタのアップグレードまたは作成時には、その他の移行状態が表示されることがあります。

カラーコーディング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、現在の状態となっている原因を説明する理由メッセージなどの追加情報が表示されます。

復元カステータスの値

復元カステータスは、データ復元力のヘルス ステータスであり、ストレージクラスタの耐障害性を示すものです。

復元カステータスのオプションを次に示します。

- **[Healthy]** : データと可用性の点でクラスタは正常です。
- **[Warning]** : データまたはクラスタの可用性に対する悪影響が生じています。
- **[Unknown]** : これは、クラスタがオンラインになるときの移行状態です。

カラーコーディング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、現在の状態となっている原因を説明する理由メッセージなどの追加情報が表示されます。

HX Data Platform クラスタの耐障害性

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に影響するノード障害の数は次のように異なります。

- **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 インストール中に設定し変更できません。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。



注目 3 のデータ レプリケーション ファクタが推奨されます。

- **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。

障害ノード数を伴うクラスタの状態

次の表で、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。

障害ノード数を伴う 5 ノード以上のクラスタの状態

レプリケーション ファクタ	アクセス ポリ シー	障害発生ノードの数		
		読み取り/書き込み	Read-Only	シャットダウン
3	Lenient	2	--	3
3	strict	1	2	3
2	Lenient	1	--	2
2	strict	--	1	2

障害ノード数を伴う 3～4 ノードのクラスタの状態

レプリケーション ファクタ	アクセス ポリ シー	障害発生ノードの数		
		読み取り/書き込 み	Read-Only	シャットダウン
3	Lenient または Strict	1	--	2
2	Lenient	1	--	2
2	strict	--	1	2

ディスクで障害が発生したノード数を伴うクラスタの状態

次の表で、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。

サーバには、SSD と HDD という 2 種類のディスクがあります。次の表で複数のディスク障害について説明する際は、ストレージ容量に使用されてい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、別のノードの容量 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。

次の表で、最悪のシナリオと障害が発生したディスクの数を示します。これは、ストレージクラスタの3つ以上のノードに適用されます。例：自己修復中のレプリケーション係数が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、自己修復のサポートに使用可能な十分な容量があることです。この表内の最悪のシナリオは、HX が自動自己修復と再調整を実行している短期間のみ適用されます。

ディスクで障害が発生したノード数を伴う3ノード以上のクラスタの状態

レプリケー ションファ クタ	アクセス ポリ シー	ノード数に対する障害が発生したディスク数		
		読み取り/書き込み	Read Only	シャットダウン
3	Lenient	2	--	3
3	strict	1	2	3
2	Lenient	1	--	2
2	strict	--	1	2

データ レプリケーション係数の設定



(注) 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 と HDD の両方を含むサーバ) を使用している場合は、デフォルトが 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 のどちらかを明示的に選択する必要があります。

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 : データの冗長複製を 3 つ保持します。この場合、より多くのストレージリソースが使用され、ノード障害やディスク障害のイベント時にデータを最大限に保護します。

注目 データ レプリケーション係数 3 が推奨されているオプションです。

- データ レプリケーション係数 2 : データの冗長複製を 2 つ保持します。この場合、より少ないストレージリソースが使用され、ノード障害やディスク障害のイベント時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。2 つのクラスタ アクセス ポリシー オプションがあります。デフォルトは lenient です。これはインストール中には設定できませんが、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は変更できます。

- **Strict** : データ損失から保護するためのポリシーを適用します。

ストレージクラスタ内のノードまたはディスクで障害が発生すると、クラスタの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。厳密な設定により、同時障害発生時にデータが保護されます。

- **Lenient** : より長いストレージクラスタの可用性をサポートするためのポリシーを適用します。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 Plug-in 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。

クラスタの復元カステータスが [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。

オプションで、HX Connect および HX Data Platform Plug-in で関連付けられている [Cluster Status/Operational Status]、または [Resiliency Status/Resiliency Health] をクリックすると、現在の状態の原因を説明する理由メッセージが表示されます。

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 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ラ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。	<ol style="list-style-type: none"> 1. 1 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。 - 障害が発生した SSD 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 2. 1 台の HDD に障害が発生しているか削除されている場合、ディスクはすぐにブラックリストにリストされます。ストレージクラスタは、数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することはできません。 - 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

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
4 ノード	1	1 ノード。	<p>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。</p> <p>ノード障害を迅速に修復し、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。</p> <ol style="list-style-type: none"> 1. ノードが電源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。	<p>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。</p> <p>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。</p>

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 以上のノード	2	最大 2 ノード。	<p>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。</p> <p>ノード障害を迅速に修復し、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。</p> <ol style="list-style-type: none"> 1. ノードが電源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 <p>ストレージクラスタがシャットダウンする場合は、 「Troubleshooting, Two Nodes Fail Simultaneously Causes the Storage Cluster to Shutdown」の項を参照してください。</p>
5 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。	<p>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の正常性を復元します。</p>

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。	

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
			<p>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。</p> <p>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。</p> <p>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時間経過後に稼働しない場合、ストレージクラスタが障害発生ノードの修復を開始します。</p> <p>ノード障害を迅速に修復し、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。</p> <ol style="list-style-type: none"> 1. ノードが電源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。

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
			2. クラスタを再調整します

上の表を確認して、指定された操作を実行します。

HX Data Platform ReadyClone の概要

HX Data Platform ReadyClone は、ホスト VM からの複数のクローン VM の迅速な作成と、カスタマイズを可能とする草分け的なストレージ技術です。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。

ReadyClone (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、ReadyClone は別のゲスト VM となります。

ReadyClone に対して変更を行っても、ホスト VM には影響しません。ReadyClone 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。ReadyClone を実行すると、単一のインストールおよびコンフィギュレーションプロセスで、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 ネイティブスナップショットの概要

HX Data Platform ネイティブスナップショットは、動作している 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 をネイティブスナップショットに戻すことができます。

HX Data Platform Plug-in を使用して、VM のネイティブスナップショットを取得します。HX Data Platform ネイティブスナップショットオプションには、ネイティブスナップショットの作成、任意のネイティブスナップショットへの復元、ネイティブスナップショットの削除が含まれます。タイミングオプションには、毎時、日次、週次があり、15分単位で設定できます。

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。

VMが電源オン、オフ、またはサスペンド状態のときに、ネイティブスナップショットを取得できます。VMware スナップショットの追加情報については、次のリンクから VMware のナレッジベース『Understanding virtual machine snapshots in VMware ESXi and ESX (1015180)』の記事を参照してください。

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

[US&cmd=displayKC&externalId=1015180](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180)



第 2 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 \(21 ページ\)](#)
- [HX Connect へのログイン \(28 ページ\)](#)
- [コントローラ VM \(stcli\) コマンドラインへのログイン \(30 ページ\)](#)
- [Cisco HX データ プラットフォーム インストーラの導入 \(32 ページ\)](#)
- [HX Data Platform REST API へのアクセス \(33 ページ\)](#)
- [Cisco HX Data Platform プラグインへのアクセス \(34 ページ\)](#)
- [Cisco TAC への連絡 \(35 ページ\)](#)

HyperFlex クラスタ インターフェイスの概要

HyperFlex の各インターフェイスは、HX Storage Cluster についての情報とアクションを実行するための手段へのアクセスを提供します。HX Storage Cluster インターフェイスには次のものがあります。

- **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 readyclones のタスク。
- **HX Data Platform Plug-in**—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。
- **ストレージコントローラ VM コマンドライン**—HX Data Platform stcli コマンドの実行。
- **HyperFlex Systems RESTful API**—認証、複製、暗号化、モニタリング、およびオンデマンドステートレスプロトコルを介しての HyperFlex Systems の管理の有効化。

追加のインターフェイスには次のものが含まれます。

- **Cisco HX Data Platform インストーラ**—HX Data Platform のインストール、HX Storage Cluster クラスタの展開および拡張、ストレッチクラスタの展開、HYPER-V クラスタの展開。
- **Cisco UCS Manager**—HX Storage Cluster 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 Clientおよび vSphere クライアント：vCenter クラスタのすべての VMware ESXi サーバの管理。
- 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 ログインクレデンシャルに関するガイドライン

stcli コマンドは、ログインクレデンシャルを要求します。

定義済みユーザ admin および root のストレージコントローラ VM のパスワードは、HX Data Platform インストーラの実行時に指定します。インストール後は、stcli コマンドラインを使用してパスワードを変更できます。

コンポーネント	権限レベル	[Username]	[Password]	注意
HX Data Platform OVA	root	root	Cisco123	重要 システムは、デフォルトのパスワード [Cisco123] で出荷されますので、インストール中にこれを変更する必要があるあります。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。

コンポーネント	権限レベル	[Username]	[Password]	注意
HX Data Platform インストーラVM	root	root	Cisco123 重要 システムは、デフォルトのパスワード [Cisco123] で出荷されますので、インストール中にこれを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 Connect	管理者または読み取り専用	vCenter から定義されたユーザ。	vCenter から定義されたユーザ。	
		定義済みの admin または root ユーザ。	HX のインストール中に指定されます。	ログインの場合は、local/ を先頭に付ける必要があります。つまり、local/admin または local/root になります。

コンポーネント	権限レベル	[Username]	[Password]	注意
HX ストレージ コントローラ VM	root	HX のインストール中に定義されたユーザ。 vCenter から定義されたユーザ。 定義済みの admin または root ユーザ。	HX のインストール中に指定されます。 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する必要があります。 インストール後、パスワードを変更するときは <code>stcli</code> コマンドを使用します。
vCenter	admin	administrator@vsphere.local デフォルト。 SSO 有効。 設定に依存します。 MYDOMAIN\name または name@mydomain.com。	SSO 有効。 設定に依存します。	ESX サーバがバージョン 5.5 の場合は、vCenter クレデンシャルが vSphere 5.5 の要件を満たしていることを確認してください。 読み取り専用ユーザには HX Data Platform Plug-in へのアクセス権はありません。
ESXi サーバ	root	SSO 有効。 設定に依存します。	SSO 有効。 設定に依存します。	ストレージクラスタ内のすべての ESX サーバで一致する必要があります。
ハイパーバイザ	root	root	HX のインストール中に指定されます。	HX のインストール後にパスワードを変更するときは、vCenter または <code>esxcli</code> コマンドを使用します。
UCS Manager	admin	設定に依存します。	設定に依存します。	
ファブリック インターコネクト	admin	設定に依存します。	設定に依存します。	

HX Data Platform の名前、パスワード、文字

印刷可能な ASCII 文字と拡張 ASCII 文字のほとんどを名前とパスワードに使用することができます。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ない文字があります。フォルダとリソースプールには文字の例外はありません。

ただし、名前とパスワードを簡素化するために、特別な目的に使用されることの多い以下の特殊文字の使用を避けるようにしてください。

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、使用しているシェルを考慮してください。シェルごとに、大文字小文字を区別するかどうか異なります。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!')。

HX ストレージクラスタ名

HX クラスタ名は 50 文字以内です。

HX ストレージクラスタ ホスト名

HX クラスタ ホスト名は 15 文字以内です。

仮想マシンとデータストア名

仮想マシン名、コントローラ VM 名、またはデータストア名を構成する文字のほとんどが許容されます。エスケープされた文字は、仮想マシン名、コントローラ VM 名、またはデータストア名として許容されます。

最大文字数: 仮想マシン名には 15 文字まで使用できます。

除外される文字: スナップショットを有効にするユーザ仮想マシン名またはデータストア名に次の文字を使用しないでください。

- アクセント (´)

特殊文字: ユーザの仮想マシン、またはデータストア名に使用できる特殊文字は次のとおりです。

- 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 (\)、サーカムフレックス (^)、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

HX Data Platform コンポーネントに固有なユーザ名を使用できますが、UCS Manager 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 内で一意にする必要があります。
- 先頭を英字にする必要があります。
- 必須要素：英字（大文字または小文字）。
- 使用可能要素：数字。すべて数字にすることはできません。
- 許可される唯一の特殊文字：アンダースコア（_）、ダッシュ（-）、ドット（.）。

コントローラ VM のパスワードの要件

コントローラ VM の root および admin ユーザのパスワードには、次のルールが適用されます。



(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。コマンドは、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
- 1つ以上の大文字
- 1つ以上の小文字
- 1つ以上の数字
- 1つ以上の特殊文字
- 新しいパスワードの設定を試せる回数は最大3回

コントローラ VM のパスワードを変更するには、必ず `stcli` 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. `stcli` コマンドを実行します。

`stcli security password set [-h] [--user USER]`

変更は、HX クラスタ内のすべてのコントローラ VM に伝達されます。

UCS Manager と ESX のパスワードの形式と文字の要件

以下の項では、UCS Manager と VMware ESXi のパスワードの形式と文字の要件について簡単にまとめています。詳細については Cisco UCS Manager と VMware ESXi のマニュアル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。

- **文字の長さ** : 最小 6、最大 80

4 つすべての文字クラスの文字を含む場合は、6 文字以上が必要です。

3 つ以上の文字クラスの文字を含む場合は、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、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、2 桁の数字が必要です。

要件を満たしている例 :

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) 。 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) 。 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** : 最大 2。たとえば、hhh###555 は許容されません。

vSphere SSO ポリシーを介して、この値を設定できます。

- **除外される文字** :

UCS Manager のパスワードにエスケープ (\) 文字を含めることはできません。

ESX パスワードにこれらの文字を含めることはできません。

- ユーザ名やユーザ名を逆にしたものは使用できません。

- デクショナリに存在する単語を含めることはできません。

- エスケープ文字 (\) 、ドル記号 (\$) 、疑問符 (?) 、等号 (=) を含めることはできません。

- **辞書に載っている単語**:

辞書で使用されている単語は使用しないでください。

vSphere 5.5 のパスワードの例外

一部の文字は、vSphere 内の機能で処理されるときにエスケープされます。つまり、処理機能によって、特殊文字の前にエスケープ文字が付加されてから、指定された名前が処理されます。

許可される特殊文字は vSphere バージョン 5.5 または 6.0 以降に固有です。 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2060746 で、VMware KB の記事『*Installing vCenter Single Sign-On 5.5 fails if the password for administrator@vsphere.local contains certain special character (2060746)*』を参照してください。

除外される文字：vSphere 5.5 では次の文字を使用しないでください。

- 非 ASCII 文字。拡張 ASCII 文字。
- アクセント付きの文字。たとえば、アクセント、鋭アクセント、サーカムフレクス、ウムラウト、ティルダ、およびセディーユ (é, à, â, å, ø, ü, ö, œ, ç, æ) があります。
- vSphere 5.5 と SSO：アンパサンド (&)、アポストロフィ (')、バックスラッシュ (\)、サーカムフレクス (^)、二重引用符 (")、感嘆符 (!)、パーセント (%)、セミコロン (;)、スペース ()

VMware には、vSphere SSO パスワードポリシー設定オプションとユーザ名のアップグレードに関する検討事項があります。VMware のマニュアルで、「*How vCenter Single Sign-On Affects Upgrades*」と「*Edit the vCenter Single Sign-On Password Policy*」のトピックを参照してください。

- ロケーションベースの例外：名前の先頭に、アットマーク (@) と丸カッコ (()) を使用しないでください。

HX Connect へのログイン

Cisco HyperFlex Connect は、HX Storage Cluster モニタリングへの HTML5 ベースのアクセス、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を可能にします。

セッションの概要

HX Connect へのログインはそれぞれセッションです。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数には、次が含まれます。

- ユーザごとに 256 の同時セッション
- HX Storage Cluster 全体で 300 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に開きがありすぎる場合は、AAA 認証が失敗します。

ステップ 1 HX Storage Cluster 管理 IP アドレスを見つけます。

個々のストレージコントローラ 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 ブラウザに HX Storage Cluster の管理 IP アドレスを入力します。

ステップ 3 HX Storage Cluster のログイン クレデンシャルを入力します。

- **RBAC ユーザ** : Cisco HyperFlex Connect は、次のロールに基づくアクセス制御 (RBAC) ログインをサポートします。
 - **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 Storage Cluster 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 Storage Cluster を変更することはできません。

これらのユーザは、vCenter を介して作成されます。vCenter ユーザ名の形式は、<name>@domain.local です。例 : administrator@vsphere.local。

- **HX 事前定義ユーザ** : HX Data Platform の事前定義ユーザである 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 を使用して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には、local/root ではなくセッションのユーザが表示される可能性があります。たとえば、アラームで Acknowledged By might list com.springpath.sysmgmt.domain-c7 と表示される可能性があります。

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 に表示される内容を更新するには、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 からログアウトして、適切にセッションを閉じるには、[User] メニュー（右上）> [Logout] を選択します。

コントローラ VM (stcli) コマンドラインへのログイン

すべての stcli コマンドは、HX Cluster 情報を読み取るコマンドと HX Cluster を変更するコマンドに分かれています。

- 変更のコマンド：管理者レベルの権限が必要です。例：

```
stcli cluster create
stcli datastore create
```

- 読み取りのコマンド：管理者レベルまたは読み取り専用レベルの権限で使用できます。例：

```
stcli <cmd> -help
stcli cluster info
stcli datastore info
```

stcli コマンドを実行するには、HX データプラットフォーム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 stcli コマンドにも当てはまります。

以下の方法で、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ログインできます。

- ブラウザから
- 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：stcli 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：stcli cluster reregister

ステップ 1 コントローラ VM の DNS 名を探します。

1. [VM] > [Summary] > [DNS Name] を選択します。
2. [ホーム] > [VM およびテンプレート] > [vCenter サーバ] > [datacenter] > [ESX Agents] > [VVM] を選択します。
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 Clusterの作成時に定義。

- b) プロンプトに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。

例

- すべてのコントローラ VM の事前定義済みユーザ。

```
# ssh admin@<ipaddress_controllervm>
```

- vCenter を介して作成された RBAC ユーザ。vCenter ユーザ名の形式は、<name>@domain.local です。例：administrator@vsphere.local

```
# ssh vc-<username>@<ipaddress_controllervm>
```

```
# ssh vc-administrator@vsphere.local@<ipaddress_controllervm>
```

- 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 root@10.198.3.24
The authenticity of host '10.198.3.24 (10.198.3.24)' can't be established.
```

ストレージコントローラパスワードの変更

```
ECDSA key fingerprint is 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) プロンプトに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パスワードの変更

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

ステップ 1 ストレージコントローラ VM にログインします。

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

```
# stcli security password set
```

このコマンドによって、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) Unix のパスワード コマンドは使用しないでください。

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 データ プラットフォーム インストーラの導入

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。

ステップ 1 ブラウザに、HX Data Platform インストーラ がインストールされる VM の URL を入力します。

このアドレスは、前述の項「Deploying HX Data Platform インストーラの展開」から入手します。例：
http://10.64.4.254

ステップ2 次のクレデンシャルを入力します。

- ユーザ名 : *root*
- パスワード (デフォルト) : *Cisco123*

注目 システムは、デフォルトのパスワード [*Cisco123*] で出荷されますので、インストール中にこれを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。[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。[Login] をクリックします。

ステップ3 この HX Data Platform インストーラ ワークフローページには、ワークフローのオプションが 2 つ表示されます。

- **[クラスタの作成]** ドロップダウンリスト—標準のクラスタ、ストレッチクラスタ、または Hyper-V 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。

HX Data Platform REST API へのアクセス

Cisco HyperFlex HX-Series System は、コンピューティング、ストレージ、ネットワークの 3 つのレイヤすべてを強力な Cisco HX Data Platform のソフトウェア ツールと組み合わせた完全内包仮想サーバプラットフォームで、シングルポイントの接続性が得られ、シンプルな管理を実現できます。Cisco HyperFlex システムは、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。このハイパーコンバージドシステムでは、ワークロードのニーズに基づいて、統合されたリソースのプールが提供されます。

HTTP 動詞を使用した Cisco HyperFlex システム 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、モニタリング、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。

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。

Cisco HX Data Platform プラグインへのアクセス

vSphere Web Clientを介してHX Data Platform Plug-inにアクセスします。



- (注)
- HX Data Platform Plug-inは、英語以外の vCenter（日本語、韓国語、および簡体字中国語）で機能します。
 - Firefox ブラウザを使用している場合は、最新の Adobe Flash Player がインストールされていることを確認してください。
 - HX Data Platform Plug-inは、vSphere シック クライアントとも呼ばれる vSphere クライアント for Windows 経由では入手できません。HX Data Platform Plug-inのアクティビティについて生成されたイベントメッセージは、vSphere クライアント表示に含まれています。HX Data Platform Plug-inタスクは、Windows用のvSphereクライアントで実行することはできません。
 - 読み取り専用の権限を持つユーザは、設定関連のタスクを実行できません。状態の情報の表示のみが可能です。

ステップ 1 vSphere Web クライアントから、vCenter パネル上部にある [Home] アイコン（家）をクリックします。

ステップ 2 ナビゲータの [Home] ページで [vCenter Inventory Lists] を選択します。

ステップ 3 vCenter インベントリ リストの下部までスクロールして、HX Data Platform プラグインにアクセスします。

ステップ 4 [Cisco HyperFlex Systems] を展開し、[Cisco HX Data Platform] をクリックして HX Data Platform Plug-in内で使用可能な HX ストレージクラスタを表示します。

Cisco HXDP オブジェクトが HX ストレージクラスタの数の一覧であることに注意してください。

[Objects] タブでは次の操作を実行できます。

- ストレージクラスタ名を編集します。[edit] アイコン（鉛筆）をクリックするか、[Actions] メニューから [Rename Cluster] を選択します。

- ストレージクラスタ設定を表示します。[summary]アイコン（緑色の紙）をクリックするか、[Actions]メニューから [Summary] を選択します。

ステップ 5 [Navigator] ペインのリストから、[HX ストレージクラスタ] を選択します。

Cisco HX Data Platformの下にストレージクラスタのリストがあります。このリストからストレージクラスタを1つ選択します。

ステップ 6 [センター (center)] ペイン内のタブをクリックして、HX Data Platform Plug-inの情報とさまざまなアクションにアクセスします。

タブオプション	説明
使用する前に	概要の情報について読み、基本的なアクションにアクセスします。
Summary	HX Data Platform ストレージオブジェクトの基本ステータスと設定をモニタします。
Monitor	HX ストレージクラスタ、ホスト、およびデータストアのパフォーマンスとイベントをモニタします。
Manage	HX ストレージクラスタの詳細をモニタし、データストアの作成と管理、および情報のコピーとエクスポートを行います。

Cisco TAC への連絡

問題解決時間を短縮するために Cisco Technical Assistance Center (TAC) のケースをオープンして、Cisco PRIME コラボレーションアプリケーションから直接効率的なサポートを受けることができます。

シスコ サービス契約が有効なお客様、パートナー、リセラー、ディストリビュータは、Cisco Technical Support で受賞歴のあるテクニカル サポート サービスを 24 時間体制で受けることができます。Cisco Technical Support Web サイトでは、シスコ製品やシスコ テクノロジーに関する技術的な問題を解決するためのオンラインのドキュメントやツールをご利用いただけます。

<http://www.cisco.com/techsupport>

TAC Support Case Manager オンライン ツールを利用することで、最も素早く S3 および S4 のサポート ケースを開くことができます (S3 および S4 サポート ケースは、最小限のネットワーク障害の問題と製品情報リクエストから構成されます)。状況をご説明いただくと、TAC Support Case Manager が自動的に推奨する解決方法を提供します。推奨リソースを使っても問題を解決することができなかった場合、TAC Support Case Manager がお客様のサポート ケースを Cisco TAC のエンジニアに割り当てます。以下の場所から、TAC Support Case Manager にアクセスできます。

<https://mycase.cloudapps.cisco.com/case>

S1 または S2 のサポート ケースに関して、またはインターネット アクセスがない場合は、電話で Cisco TAC にご連絡ください (S1 または S2 サポート ケースは、著しいパフォーマンスの低下または停止などの製品のネットワークの問題から構成されています)。お客様の業務を円滑に続行できるように、S1 および S2 のサポート ケースは、迅速に Cisco TAC エンジニアに割り当てられます。

電話でサポート ケースを開く場合は、次のいずれかの電話番号をご利用ください。

- アジア太平洋地区 : +61 2 8446 7411
- オーストラリア : 1 800 805 227
- EMEA : +32 2 704 55 5555
- USA: 1 800 5532447

企業およびサービス プロバイダー製品に関する Cisco TAC の連絡先の一覧については、<http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html> を参照してください。

Cisco Small Business Support Center (SBSC) の連絡先の一覧については、<http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html> を参照してください。



第 3 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 \(37 ページ\)](#)
- [パフォーマンス チャートの表示 \(37 ページ\)](#)
- [HX Data Platform プラグイン インターフェイスの使用法 \(42 ページ\)](#)
- [HX Connect を使用した HyperFlex クラスタのモニタリング \(44 ページ\)](#)

HyperFlex クラスタのモニタリング

この章では、HX Storage Cluster 次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。

- HX Connect
- HX Data Platform Plug-in
- ストレージ コントローラ VM コマンドライン

パフォーマンス チャートの表示

[Monitor Performance] タブでは、ストレージ クラスタ、ホスト、データストアの読み込みと書き込みに関するパフォーマンスが表示されます。

- パフォーマンス チャートでは、ストレージ クラスタ、ホスト、データストアのパフォーマンスが図表形式で表示されます。
- システムは、20 秒ごとにパフォーマンス チャートを更新します。
- 個々のデータポイント上でマウスを移動することで、パフォーマンスのピークに関する情報やタイムスタンプが表示されます。
- 薄い青は書き込み操作を表し、濃い青は読み込み操作を表します。
- パフォーマンス チャート内のギャップは、データを使用できなかった期間を示します。ギャップは必ずしもパフォーマンスの低下を示すものではありません。

ストレージクラスタのパフォーマンス チャート

ステップ 1 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] > [Monitor] > [Performance] の順に選択します。

左側には、モニタ対象として選択できるオプションが3つあります ([Storage Cluster]、[Hosts]、および [Datastores])。

ステップ 2 [Storage Cluster] をクリックして、[Storage Cluster Performance] タブを表示します。

ステップ 3 [Hour]、[Day]、[Week]、[Month]、[Max]、[Custom] オプションをクリックして、ストレージクラスタのパフォーマンスを表示する時間帯を指定します。

ステップ 4 [IOPS]、[Throughput]、[Latency]、[Show] のチェックボックスをクリックして、選択したパフォーマンスとオブジェクトを表示します。

ホスト パフォーマンスのチャート

ステップ 1 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] > [Monitor] > [Performance] の順に選択します。

左側には、モニタ対象として選択できる3つのオプションが表示されます ([Storage Cluster]、[Hosts]、および [Datastores])。

ステップ 2 [Hosts] をクリックして、[hosts performance] タブを表示します。

ステップ 3 [Hour]、[Day]、[Week]、[Month]、[Max]、または [Custom] オプションをクリックして、ホストパフォーマンスを表示する時間帯を指定します。

ステップ 4 [IOPS]、[Throughput]、[Latency]、[Show] のチェックボックスをクリックして、選択したパフォーマンスとオブジェクトを表示します。

ステップ 5 個別のホストを除外したり表示したりするには、[host] をクリックします。コンピューティング ノードには、ストレージクラスタ パフォーマンス値はありません。

データストア パフォーマンスのチャート

ステップ 1 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] > [Monitor] > [Performance] の順に選択します。

左側には、モニタ対象として選択できるオプションが3つあります ([Storage Cluster]、[Hosts]、および [Datastores])。

ステップ 2 [Datastores] をクリックして、[datastores performance] タブを表示します。

- ステップ 3 [Hour]、[Day]、[Week]、[Month]、[Max]、[Custom] オプションをクリックして、データストア パフォーマンスを表示する時間帯を指定します。
- ステップ 4 [IOPS]、[Throughput]、[Latency]、[Show] のチェック ボックスをクリックして、選択したパフォーマンスとオブジェクトを表示します。

[Performance] ポートレット

[Performance] ポートレットには、HX Data Platform ストレージクラスタのパフォーマンスに関する詳細情報が表示されます。ここでは、20秒間隔でプロットされた、過去1時間のパフォーマンス データが表示されます。[Performance] ポートレットのチャートは、ストレージクラスタ全体のデータを示します。

ストレージクラスタ、データストア、ホスト レベルのパフォーマンス レポートに関する詳細については、[Monitor] タブを選択します。

- ステップ 1 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] > [Summary] の順に選択します。
- ステップ 2 [Performance] ポートレットにスクロールします。

オプション	説明
IOPS	1 秒当たりの入出力処理。
スループット	ストレージクラスタのデータ転送レート。単位は MBps です。
遅延	遅延は、1 つの I/O リクエストが完了するまでに要する時間の尺度です。これは、リクエストが発行され応答が受信されるまでの時間長です。msec 単位での測定値です。
Current	チャートの最新のデータ ポイントの値。
Past Hour	データ ポイントの最後の 1 時間のチャート。

[Datastore Trends] ポートレット

[Datastore Trends] ポートレットは、選択したデータストアの IO パフォーマンスのチャートです。

- ステップ 1 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] > [Manage] の順に選択します。

ステップ2 [table] リストから、[datastore] を選択します。[Summary] タブを更新して、選択したデータストアの情報を表示します。

ステップ3 スクロールして、[Trends] ポートレットを表示します。

タブでは、20分ごとにプロットされた IOPS を表示します。

ピーク値の上にマウス オーバーし、色分けされた読み取り IOPS と書き込み IOPS を取得します。

パフォーマンスチャートのカスタマイズ

パフォーマンスチャートを変更して、オプションの一覧の一部またはすべてを表示します。

カスタマイズされたアイテム	説明
Time period	[hour]、[days]、[week]、[month]、[all]、または [custom] から選択します。この章の「パフォーマンス期間の指定」のセクションを参照してください。
Cluster objects	ストレージクラスタ、ホスト、またはデータストアのリストから選択します。
Chart type	[IOPS]、[Throughput]、[Latency] から選択します。
Show objects	表示するオブジェクトのデータを一覧から選択します。この章の「パフォーマンスチャートの選択」のセクションを参照してください。

パフォーマンス期間の指定

ステップ1 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] > [Monitor] > [Performance] の順に選択します。

ステップ2 次のいずれかのタブをクリックして、ストレージクラスタ、ホスト、データストアのパフォーマンスを表示する時間を指定します。

パラメータ	説明
時間	過去の時間のパフォーマンスを表示
Day	過去の日付のパフォーマンスを表示
Week	過去の週のパフォーマンスを表示
Month	過去の月のパフォーマンスを表示

パラメータ	説明
すべて (All)	ストレージクラスタのパフォーマンスを作成された時点から表示
Custom	このタブを選択し、「カスタム範囲の指定」で説明されているようにカスタム範囲を指定します

カスタム範囲の指定

ステップ 1 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] > [Monitor] > [Performance]** の順に選択します。

ステップ 2 **[Custom]** タブをクリックして、**[Custom Range]** ダイアログボックスを表示します。

ステップ 3 **[Custom Range]** ダイアログボックスのメソッドを選択します。

- [Last]** をクリックして、分、時、日、月の数字を入力します。必要に応じて、上下の矢印を使用して数字を増やしたり減らしたりします。
- ドロップダウンリストをクリックして、分、時、日、週、月の数字を指定します。
- [From]** をクリックし、**[calendar]** アイコンをクリックして、パフォーマンスの測定を開始する日付を選択します。ドロップダウンリストをクリックして、時間を選択します。
- [To]** をクリックし、**[calendar]** アイコンをクリックして、パフォーマンスの測定を終了する日付を選択します。ドロップダウンリストをクリックして、時間を選択します。

ステップ 4 **[Apply]** をクリックし、次に **[OK]** をクリックして設定を適用します。

パフォーマンス チャートの選択

パフォーマンス チャートを選択して、ストレージクラスタ、ホスト、データストアを表示できます。

タブの下部の **[IOPS]**、**[Throughput]**、**[Latency]** に対応するチェックボックスを選択もしくは選択解除して、特定の情報を表示します。

たとえば、ストレージクラスタの IOPS パフォーマンスのみを表示するには、次の操作を行います。

- 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] > [Monitor] > [Performance]** の順に選択します。
- [Storage Cluster]**、**[Hosts]**、**[Datastores]** のチャート設定のいずれかをクリックします。**[Hosts]** テーブルでは、ストレージクラスタにストレージを提供しないように、コンピューティングノードは **[IOPS]**、**[Throughput]**、**[Latency]** の値を表示しません。
- チャートオプションの選択を解除します。

フィールド	説明
Chart types	<p>チェックボックスをクリックして、どのテーブル列を表示または隠すかを選択します。次のオプションがあります。</p> <ul style="list-style-type: none"> • IOPS • スループット • 遅延
Show	<p>各ストレージクラスタ、ホスト、データストアの場合、チェックボックスをクリックしてチャートに含むまたは除外する特定のオブジェクトを選択します。</p>
読み取り/書き込み	<p>チャートでの各オブジェクトの読み込みや書き込みの値の色分けを示します。</p>
Storage Cluster	<p>チャート内のストレージクラスタ名。</p>
ホスト	<p>チャート内のホスト名。これには、コンバージドノードとコンピューティングノードの両方が含まれます。</p>
Datstores	<p>チャート内のデータストア名。</p>
IOPS Read/Write	<p>1秒当たりの入出力処理の最新のデータポイント。</p>
Throughput Read/Write (Mbps)	<p>ストレージクラスタのデータ転送レートの最新のデータポイント。Mbpsで測定されます。</p>
Latency Read/Write (msec)	<p>1つのI/Oリクエストが完了するまでに要する時間の尺度である、[Latency]の最新のデータポイント。これは、リクエストが発行され応答が受信されるまでの時間長です。単位はmsecです。</p>

HX Data Platform プラグインインターフェイスの使用法

インターフェイス全体に適用されるいくつかのHX Data Platform プラグイン機能があります。これらについては、次の各項を参照してください。

Cisco HX Data Platform プラグインと vSphere Web クライアントの統合

HX Data Platform プラグインは VMware vSphere vCenter インターフェイスと緊密に統合されており、シームレスなデータ管理エクスペリエンスを提供します。vSphere Web クライアントまたは vSphere クライアント vSphere vCenter インターフェイスのいずれかを使用できます。このガイドのタスクの例のほとんどは、vSphere Web クライアント インターフェイスを参照します。

vSphere vCenter インベントリ リストから HX Data Platform プラグインにアクセスします。HX Data Platform プラグインから管理するストレージクラスタを選択します。HX Data Platform プラグインは、ストレージクラスタ固有のオブジェクト（データストアなど）をモニタおよび管理します。vSphere は、ストレージクラスタ内のオブジェクト（ESX サーバなど）をモニタおよび管理します。HX Data Platform プラグインと vSphere でタスクが重複します。

Cisco HX Data Platform プラグインと vSphere インターフェイス間のリンク

vSphere Web クライアントでは、HX Data Platform プラグインと vCenter の両方が、コンポーネントとクラスタのステータスに関する情報を提供します。一部のタブとパネルでは、HX Data Platform プラグインと vCenter の情報およびアクションの間に直接リンクがあります。

HX Data Platform プラグインまたは vCenter からのリンクをたどる場合、リンク元の位置に 1 回のクリックで戻ることができるリンクが存在するわけではない点に注意してください。

Cisco HX Data Platform プラグイン タブの概要

HX Data Platform プラグインのモニタリング情報と管理機能は、3 つのタブに分けられています。HX Data Platform プラグインのすべてのタブとパネルを次に示します。これらのタブとパネルには HX Data Platform ストレージクラスタ ステータスと、ストレージクラスタ管理タスクのオプションが表示されます。

[Summary] タブには、[Summary] エリアと [Portlets] エリアが表示されます。[Summary] タブのポートレットは、[Capacity]、[Performance]、[Status] です。

[Monitor] タブには 2 つのサブタブがあります。

- [Performance] タブ：ストレージクラスタ、ホスト、およびデータセンタの [Latency]、[Throughput]、および [IOPs] パフォーマンス チャートが表示されます。
- [Events] タブ：HX Data Platform イベントのリストと、選択されているイベントの詳細パネルが表示されます。

[Manage] タブには 2 つのサブタブがあります。

- [Cluster] タブ：ストレージクラスタ、ホスト、ディスク、PSU、および NIC が示されます。これには、クラスタとホストのリスト、選択されているクラスタまたはホストの詳細パネル、追加のサブタブ ([Hosts]、[Disks]、[PSU]、[NIC]) が含まれます。

- [Datastores] タブ：データストアの観点からのホストに関する情報を示します。これには、データストアのリストと、選択されているデータストアの追加のサブタブが含まれます。データストアのサブタブには、[Summary] タブと [Hosts] タブがあります。[Summary] タブには、[Details]、[Trends]、[Top VMs by Disk Usage] の各ポートレットが含まれています。

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

HX Connect ユーザ インターフェイスは、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 HX ストレージ クラスタに関する情報が含まれています。

- [Dashboard]：HX ストレージ クラスタ ステータスの概要です。
- [Alarms, Events, Activity]：詳細は、Cisco HyperFlex Systems Troubleshooting Guide を参照してください。
- [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。
- [System Information]：システムの概要、およびノードとディスクのステータスとタスク。
サポートバンドルを生成するには Cisco HyperFlex Systems Troubleshooting Guide、メンテナンス モードを起動および終了するには [ストレージ クラスタのメンテナンス操作の概要 \(55 ページ\)](#)、ノードまたはディスクのビーコンを設定するには [ビーコンの設定 \(58 ページ\)](#) を参照してください。
- [Datastores]：データストアに関連するステータスおよびタスク。
- [Virtual Machines]：仮想マシンの保護に関連するステータスおよびタスク。

追加の HX Connect ページでは、管理アクセスを提供します。

- [Encryption]：保管中のデータのディスクおよびノードの暗号化タスク。
- [Replication]：ディザスタ リカバリのための VM 保護タスク。

[Upgrade] ページは、HX Data Platform および Cisco UCS Manager ファームウェア アップグレード タスクへのアクセスを提供します。

[Dashboard] ページ



重要 読み取り専用ユーザには、ヘルプで利用可能なすべてのオプションが表示されるわけではありません。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。

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 にログインしたときに表示される最初のページです。

UI 要素	基本情報
[Operational Status] セクション	HX ストレージクラスタとアプリケーションパフォーマンスの機能の状態を示します。 [Information] (i) 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。
[Resiliency Health] セクション	データのヘルス ステータスと、HX ストレージクラスタの耐障害性を示します。 [Information] (i) 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。
[Capacity] セクション	ストレージの合計の内訳と、ストレージの使用量または未使用の容量が表示されます。 ストレージの最適化、圧縮、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。
[Nodes] セクション	HX ストレージクラスタ内のノード数と、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マウスを移動すると、そのノードの名前、IP アドレス、ノードの種類が表示され、容量、使用率、シリアル番号、およびディスクの種類のデータへのアクセスが可能なディスクがインタラクティブに表示されます。
[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 スナップショットを表示し、IOPS、スループット、および遅延データを表示します。 詳細については、[Performance] ページを参照してください。
[Cluster Time] フィールド	クラスタのシステム日付および時刻。

テーブル ヘッダーの共通のフィールド

HX Connect のいくつかのテーブルは、テーブルに表示される内容に影響を与える次の 3 つのフィールドのうち 1 つ以上を提供します。

UI 要素	基本情報
[Refresh] フィールドおよびアイコン	<p>HX Cluster の動的な更新のためにテーブルを自動的に更新します。タイムスタンプは、テーブルが更新された最終時刻を示します。</p> <p>コンテンツを今すぐ更新するには円形のアイコンをクリックします。</p>
[Filter] フィールド	<p>入力したフィルタ テキストに一致する項目のみテーブルに表示します。以下の表の現在のページに記載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。</p> <p>[Filter] フィールドに選択テキストを入力します。</p> <p>[Filter] フィールドを空にするには、[x] をクリックします。</p> <p>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。</p>
[Export] メニュー	<p>テーブルデータの現在のページのコピーを保存します。テーブルの内容は、選択したファイル形式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。</p> <p>エクスポート ファイルの形式を選択する下矢印をクリックします。ファイルの形式のオプションは、cvs、xls および doc です。</p> <p>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。</p>

[Activity] ページ

vSphere から収集された HX ストレージクラスタの最近のアクティビティのリストを表示します。Ready Clones、VM 電源オン/オフ、メンテナンス モードの入/切のように、HX ストレージクラスタで最新タスクの進捗をモニタできます。

UI 要素	基本情報
[Expand All] と [Collapse All] ボタン	<p>[Activity] 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。</p> <p>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。</p>

UI 要素	基本情報
[Activity] リスト	<p>次の詳細を含む最近のタスクの一覧が表示されます。</p> <ul style="list-style-type: none"> • ID • 説明 • VM 電源のオン/オフ/一時停止ステータス • タスク ステータス : <ul style="list-style-type: none"> • In Progress • Success • 不合格 <p>VM 電源の操作に失敗した場合は、[Existing State] フィールドと [Required State] フィールドも含まれます。</p> <ul style="list-style-type: none"> • 日付とタイムスタンプ • Progress bar <p>展開された [Activity] リストには、タスクのステップ名とステータスが表示されます。</p> <p>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。更新間隔は 5 分です。</p>

[System Information Overview] ページ

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、HX メンテナンス モードへのアクセスを提供します。

HX ストレージクラスタ構成データ

この HX ストレージクラスタの基本的な構成情報が表示されます。

UI 要素	基本情報
[HX storage cluster] フィールド	このストレージクラスタの名前です。

UI 要素	基本情報
[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を提供します。 <ul style="list-style-type: none"> • [Online] : クラスタの準備ができています。 • [Offline] : クラスタの準備ができていません。 • [Read Only] : クラスタでスペースが不足しています。 • [Unknown] : クラスタがオンラインになるときの移行状態です。
[vCenter] リンク	この HX ストレージクラスタに関連付けられた VMware vSphere へのセキュアな URL です。リンクをクリックして vSphere Web Client にリモートアクセスします。
[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です。
[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です。
[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のレプリカの数です。
[Uptime] フィールド	この HX ストレージクラスタがオンラインになっている時間の長さです。
[Total Capacity] フィールド	このクラスタの全体的なストレージサイズです。
[Available Capacity] フィールド	このクラスタの空きストレージの容量です。
DNS Server(s)	この HX ストレージクラスタの DNS サーバの IP アドレスです。
NTP Server(s)	この HX ストレージクラスタの NTP サーバの IP アドレスです。

ノードデータ

この HX ストレージクラスタ内の個々の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、[Nodes] ページに移動します。

UI 要素	基本情報
[Node] フィールド	このクラスタ上のノードの名前です。
[Model] フィールド	このノードの物理ハードウェアのモデル番号です。

UI 要素	基本情報
[Disks] フィールド	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。
[Node status] フィールド	<ul style="list-style-type: none"> • Online • Offline • In Maintenance • Healthy • 警告
[HXDP Version] フィールド	このノード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です。
[Type] フィールド	<ul style="list-style-type: none"> • Hyper Converged • コンピューティング
[Hypervisor Status] フィールド	<ul style="list-style-type: none"> • Online • Offline • In Maintenance • In Progress
[Hypervisor Address] フィールド	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。

ディスクのあるノードでは、ディスクのインタラクティブな表示が、次のポップアップデータとともに表示されます。

表 1: キャッシュ ディスク

UI 要素	基本情報
[Slot Number] フィールド	ドライブの場所です。
[Serial Number] フィールド	このディスクの物理シリアル番号です。
[Disk State] フィールド	<ul style="list-style-type: none"> • 準備
[Capacity] フィールド	ディスク サイズの合計です。
[Locator LED] フィールド	ディスクを探すために役立つホスト上の物理光を有効にします。オプションは、[On] と [Off] です。

表 2: 永続ディスク

UI 要素	基本情報
[Slot Number] フィールド	ドライブの場所です。
[Serial Number] フィールド	このディスクの物理シリアル番号です。
[Disk State] フィールド	<ul style="list-style-type: none"> • 準備 • Blacklisted • To Be Removed
[Used / Total Capacity] フィールド	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。
[Storage Usage] フィールド	使用されているディスク ストレージの割合です。
ロケータ LED	ディスクを探すために役立つホスト上の物理光を有効にします。オプションは、[On] と [Off] です。

[Nodes] ページ

8 列の表にこの 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。各列をデータの並べ替えに使用できます。

UI 要素	基本情報
[Enter HX Maintenance Mode] ボタン	このボタンにアクセスするには、ノードを選択します。 [Confirm HX Maintenance Mode] ダイアログボックスを開きます。
[Exit HX Maintenance Mode] ボタン	このボタンにアクセスするには、ノードを選択します。 すべてのメンテナンス タスクが完了したら、手動で HX メンテナンス モードを終了する必要があります。
[Node] カラム	この HX ストレージクラスタ上のノードの名前です。
[Hypervisor Address] カラム	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。
[Hypervisor Status] カラム	<ul style="list-style-type: none"> • Online • Offline • In Maintenance • In Progress

UI 要素	基本情報
[Controller Address] カラム	HX ストレージ コントローラ VM の IP アドレス。
[Controller Status] カラム	<ul style="list-style-type: none"> • Online • Offline • In Maintenance
[Model] カラム	このノードの物理ハードウェアのモデル番号です。
[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です。
[Disks] カラム	ノード内のディスクの数です。 数をクリックすると、選択したノード名でフィルタ処理した [Disks] ページが開きます。

[Disks] ページ

7列の表にこの HX の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。各列をデータの並べ替えに使用できます。

UI 要素	基本情報
[Node] カラム	ディスクが存在するノードの名前です。
[Slot] カラム	SED ドライブの場所です。これはメンテナンス作業のためのドライブを識別します。
[Capacity] カラム	ディスク サイズの合計です。

UI 要素	基本情報	
[Status] カラム		次の状態は無視できます。 <ul style="list-style-type: none">• Invalid• 標準• [Removed] : [Secure Erase] オプションを使用した後に SED ディスクが削除された状態です。• Time out• 不明 (Unknown)

UI 要素	基本情報
	<ul style="list-style-type: none"> • [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の状態です。また、他の状態のいずれかにディスクが移動するときの移行状態です。 • [Blacklisted] : 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、ディスクがまだ利用可能な場合、クラスタがディスクを修復しようとしており、[Repairing] の状態に移行する前の移行状態である可能性があります。 • [Claimed] : ディスクが認識され、使用中の状態です。 • [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。 • [Ok To Remove] : SED ディスクが [Secure Erase] オプションを使用して安全に消去されており、安全に削除できる状態です。 (注) Cisco HX Data Platform 2.5 では、[Ok To Remove] の状態になったディスクは、クラスタによって使用されません。 • [Repairing] : ブラックリスト登録済みディスクが現在修復され

UI 要素	基本情報	
	<p>ている状態です。</p> <ul style="list-style-type: none"> • [To Be Removed] : ディスクが RMA にスケジュールされているときの状態です。 	
[Encrypted] カラム	<ul style="list-style-type: none"> • [Enabled] : この保管中データ対応ディスクには暗号化が設定されています。 • [Disabled] : この保管中データ対応ディスクには暗号化は設定されていません。これは、新しいディスクが存在するが、キーがまだ適用されていない場合に発生します。 • Locked • 不明 (Unknown) 	
[Type] カラム	<ul style="list-style-type: none"> • 不明 (Unknown) • [Rotational] : ハイブリッド ドライブ • [Solid State] : SSD ドライブ 	
[Usage] カラム	<ul style="list-style-type: none"> • 不明 (Unknown) • Cache • 永続 	
[Turn On Locator LED] および [Turn Off Locator LED] ラジオ ボタン	<p>ラジオ ボタンにアクセスするには、ディスクを選択します。</p> <p>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。</p>	
(省略可能) [Secure Erase] ボタン	<p>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化を使用して暗号化されている場合にのみ表示されます。</p> <p>ボタンにアクセスするには、ディスクを選択します。</p> <p>クラスタで使用中の暗号化キーを入力し、[Secure Erase] をクリックしてから [Yes, erase this disk] をクリックし、ローカルの暗号化キーを安全に消去します。</p>	



第 4 章

HXストレージクラスタメンテナンスの準備

- ストレージクラスタのメンテナンス操作の概要 (55 ページ)
- シリアル操作とパラレル操作 (57 ページ)
- クラスタ ステータスの確認 (58 ページ)
- ビーコンの設定 (58 ページ)
- HX クラスタの vMotion の設定の確認 (59 ページ)
- ストレージクラスタ ノードのメンテナンス モード (60 ページ)
- Cisco HyperFlex のメンテナンス モードの開始 (61 ページ)
- Cisco HyperFlex のメンテナンス モードの終了 (62 ページ)
- バックアップ操作の作成 (64 ページ)
- HX ストレージクラスタのシャットダウンと電源オフ (65 ページ)
- HX ストレージクラスタの電源オンと起動 (67 ページ)
- vNIC または vHBA の変更後の PCI パススルーの設定 (69 ページ)

ストレージクラスタのメンテナンス操作の概要

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 から実行されます。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します。



(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するか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ると、3番目のノードが追加され、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。

vSphere 5.5 から 6.0 へのアップグレード。ESX サーバまたは vCenter サーバのいずれかを 5.5 から 6.0 にアップグレードする場合は、事前に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。

ノードの追加。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、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ついては、『Cisco HX Data Platform Getting Started Guide』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 もオフラインですが、ストレージコントローラ VM は起動されており、Cisco HX データプラットフォーム管理は `stcli` コマンドライン、HX Connect、HX Data Platform Plug-in から表示できます。vSphere Web クライアントは、ストレージ I/O 層に関する報告が可能です。`stcli cluster info` コマンドは、ストレージクラスタ全体のステータスが `offline` であることを返します。

メンテナンス前タスク

ストレージクラスタのメンテナンスを行う前に、次の点を確認します。

- 実行するメンテナンスタスクを特定します。
参照先
- 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、システムロード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あり稼動しています。
- HX Connect または HX Data Platform Plug-in ビーコン オプションを使用してディスクを特定します。

HX ビーコン オプションは、ハウスキーピング 120GB 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。

- 並列して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。順次に行うことだけが可能なタスクがあります。
- 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 HX メンテナンスモードにします。HX メンテナンスモードは、ESX メンテナンスモードでの vSphere よりも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、ノードのメンテナンスモードを終了して、ストレージクラスタを再起動する必要があります。加えて、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。

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 HX 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働している。
- 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

特定の操作は同時に実行することができません。次の操作は、（パラレルではなく）シリアルで実行するようにしてください。

- 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、設定。
- ノードの追加または削除。
- ノードをシャットダウンする必要があ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開始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

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。リストされているコマンドをコントローラ VM のコマンドラインから実行します。

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。

```
# 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3 ノード障害の数を確認します。

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

応答の例：

```
#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。

ノードビーコンは Cisco UCS Manager から設定します。ディスク ビーコンは、HX Data Platform Plug-in または HX Connect ユーザインターフェイスから設定します。

ステップ1 ノード ビーコンは、UCS Manager を使用してオンまたはオフにします。

- UCS Manager の左側のパネルから、**[Equipment] > [Servers] > [server]** を選択します。
- UCS Manager の中央のパネルから、**[General] > [Turn on Locator LED]** を選択します。
- 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、**[General] > [Turn off Locator LED]** を選択します。

ステップ2 ディスク ビーコンは、HX Data Platform Plug-in を使用してオンまたはオフにします。

- 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] > [Manage]** の順に選択します。
- [Manage] タブで、**[Cluster] > [cluster] > [host] > [Disks] > [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。
[Actions] ドロップダウン リストから、[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。
[Actions] ドロップダウン リストから、[Beacon OFF] を選択します。

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

- a) HX Connect にログインします。
- b) [System Information] > [Disks] の順に選択します。
- c) ノードを選択し、[Turn On Locator LED] または [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 を除く、選択しているノード上のすべてのディスクのビーコン LED が切り替わります。ハウスキーピング SSD またはキャッシュ NVMe SSD には、機能する LED ビーコンはありません。

HX クラスタの vMotion の設定の確認

HX クラスタで HX メンテナンス操作を実行する前に、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。

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 vmnic6 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、および命名規則が、クラスタのすべての ESXi ホストの間で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ていること、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。
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)、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 <vMotion IP address of neighboring server>`」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。このモードでは、ノードのデコミッションまたはシャットダウンの前にすべてのVMを他のノードに移行することによって、さまざまなメンテナンス タスク用にノードが準備されます。

メンテナンス モードには次の2種類があります。

- Cisco HX メンテナンス モード
- VMware ESX メンテナンス モード

Cisco HX メンテナンス モード

Cisco HX メンテナンス モードは ESX メンテナンス モードに加えて HX Data Platform 固有の機能を実行します。最初のストレージクラスタの作成後に行うストレージクラスタ ノードのメンテナンスタスクでは、必ず、ESX メンテナンス モードではなく Cisco HX メンテナンスモードを選択してください。

このモードは、クラスタ内の個別のノードで選択されたタスクを実行するための優先メンテナンスモードです。次のようなものがあります。

- ディスクの交換などのメンテナンスのために個々のホストをシャットダウンする場合。
- ESX Server のバージョンなど、ホスト上で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 モードの留意点

- HX 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ます。
- ESX ホストでタスクを実行できるように HX メンテナンスモードを開始した場合は、ESX ホストでのタスクの完了後に必ず HX メンテナンス モードを終了してください。
- Cisco HX メンテナンス モードは、正常なクラスタのノードのみに適用されます。たとえば、非常に多くのノードがダウンしている、またはクラスタをシャットダウン中など、クラスタが正常でない場合は ESX メンテナンス モードを使用します。
- 手順については、「*Cisco HyperFlex* メンテナンス モードの開始」と「*Cisco HyperFlex* メンテナンス モードの終了」を参照してください。

VMware ESX メンテナンス モード

このモードは、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、次の手順を実行します。

- vCenter GUI で *[host]* を選択してから、メニューを右クリックして *[maintenance mode]* を選択します。
- ESX コマンドラインで `esx maintenance mode` コマンドを使用します。

Cisco HyperFlex のメンテナンス モードの開始



- (注) レプリケーションを設定している場合は、アップグレード、拡張、クラスタの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ます。アップグレードや拡張、または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。

HX Storage Clusterがオフラインの場合は、VMware メンテナンス モードを使用してください。

HX Connect ユーザ インターフェイスの使用



- (注) リリース 2.5(1a)/2.5(1b) 以降のリリースでのみサポートされています。

1. HX Connect : `https://<cluster management ip>` にログインします。
2. メニューで *[System Information]* をクリックします。
3. *[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. *[Enter HX Maintenance Mode]* をクリックします。
5. *[Confirm HX Maintenance Mode]* ダイアログボックスで、*[Enter HX Maintenance Mode]* をクリックします。



- (注) すべてのメンテナンス タスクが完了したら、手動で HX 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 の Web クライアントにログインします。
2. [Home] > [Hosts and Clusters] に移動します。
3. [HX Cluster] が含まれている [Datacenter] を展開します。
4. [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、[Cisco HX Maintenance Mode] > [Enter HX Maintenance Mode] の順に選択します。

コマンドラインインターフェイスの使用

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 HX メンテナンス モードにします。
 1. ノード ID と IP アドレスを特定します。


```
# stcli node list --summary
```
 2. ノードを HX メンテナンス モードにします。


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

 (stcli node maintenanceMode --help も参照してください)
3. root 権限を持つユーザとして、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 HX 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
```

vSphere Web クライアントの [Monitor] > [Tasks] タブで [Enter Maintenance Mode] タスクの進行状況をモニタできます。

操作に失敗した場合はエラーメッセージが表示されます。根本的な問題を修正してからもう一度メンテナンスモードに入ります。問題を解決できない場合は、Cisco TAC までお問い合わせください。

Cisco HyperFlex のメンテナンス モードの終了



- (注) レプリケーションを設定している場合は、アップグレード、拡張、クラスタの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ます。アップグレード、拡張、クラスタのメンテナンスの完了後、再開してください。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。

HX Connect ユーザ インターフェイスの使用



(注) リリース 2.5(1a)/2.5(1b) 以降のリリースでのみサポートされています。

1. HX Connect : `https://<cluster management ip>` にログインします。
2. メニューで [System Information] をクリックします。
3. [Nodes] をクリックし、メンテナンス モードから移動するノードの行をクリックします。
4. [Exit HX 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. [Home] > [Hosts and Clusters] に移動します。
3. [HX Cluster] が含まれている [Datacenter] を展開します。
4. [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、[Cisco HX Maintenance Mode] > [Exit HX Maintenance Mode] を選択します。

コマンドライン インターフェイスの使用

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 HX 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。

```
# stcli node list --summary
```

2. ノードの HX 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. root 権限を持つユーザとして、このノードの ESXi コマンドラインにログインします。
4. ノードの HX 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
```

vSphere Web クライアントの [Monitor] > [Tasks] タブで [Exit Maintenance Mode] タスクの進行状況を監視できます。

操作に失敗した場合はエラーメッセージが表示されます。根本的な問題を修正してから、もう一度メンテナンスモードを終了します。問題を解決できない場合は、Cisco TAC までお問い合わせください。

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。Preserve Identities 属性を使用して、Full-State タイプと All Configuration タイプの両方のバックアップを実行します。

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 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [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 [Backup Configuration] ダイアログボックスで、[Create Backup Operation] をクリックします。

ステップ 6 [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。

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] フィールドをイネーブルに設定すると、Cisco UCS Manager によって、選択した設定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。[Backup Configuration] ダイアログボックスの [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) [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。
- b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[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、[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、[Backup Configuration] ダイアログボックスを再度開きます。

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の電源をオフにすると、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の電源をオフにする必要があるのは非常に稀なことです。ストレージクラスタ全体の電源をオフにしなければならない定期メンテナンスやアップグレードプロセスはありません。

- **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。これには、クラスタ内のノードの電源ダウンや、vCenter または FI クラスタのシャットダウンは含まれません。
- **オフライン クラスタ**は、ストレージクラスタの動作状態の 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、またはストレージクラスタがシャットダウンされた場合に、ストレージクラスタがオフラインになることがあります。

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。
- **Preserve Identities** 属性を使用して、**Full-State** タイプと **All Configuration** タイプの両方のバックアップを実行します。[バックアップ操作の作成 \(64 ページ\)](#) を参照してください。

ステップ 1 HX ストレージ クラスタをシャットダウンするには、次の 2 つのステップを実行します。

ステップ 2 すべての 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 3 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。

```
# 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になっていることを確認します。

```
# stcli 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offlineになっていることを確認します。

この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。

メンテナンスまたはアップグレードタスクで物理コンポーネントの電源を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4 HXストレージクラスタの電源をオフにするには、ステップ2とステップ3を実行してから、残りの手順を実行します。

ステップ5 各ストレージクラスタESXホスト上で、コントローラVM (stCt1VM) をシャットダウンします。

方法を選択します。

vCenter VM 電源オフを使用する

- a) vCenterクライアントから、各ESXホスト上のコントローラVMを特定します。
- b) コントローラVMを右クリックして、[Power] > [Power Off] を選択します。

この方法は、グレースフルゲストVMシャットダウンを実行します。

vCenter ESX Agent Manager を使用する

- a) vCenterクライアントから、ESX Agent Manager コンソールを開きます。
- b) 各ESXホスト上でコントローラVMを特定して、[Power] > [Power Off] を選択します。

この方法は、エージェントVMのグレースフルシャットダウンを実行します。コントローラVMはエージェントVMです。

vCenter ESX メンテナンスモードを使用する

- a) vCenterクライアントから、各ESXホストを特定します。
- b) ESXホストを右クリックして、[Maintenance Mode] > [Enter Maintenance Mode] を選択します。

この方法は、コントローラVMを含むESXホスト内のすべてのVM上でハードシャットダウンを実行します。

ステップ6 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クライアントから、ホストを特定します。
- b) ホストを右クリックして、[Power] > [Shut Down] を選択します。

ステップ7 メンテナンスタスクで必要な場合は、FIの電源をオフにします。

Cisco UCS FIは、連続運用向け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タをシャットダウンまたは再起動する必要がありません。そのため、UCSファブリックインターコネクタには電源ボタンが付いていません。

Cisco UCS ファブリックインターコネクタの電源をオフにするには、電源ケーブルを手で引き抜きます。または、FIの電源ケーブルがスマートPDUに接続されている場合は、付属のリモコンを使用して電気コンセントからの電力をオフにします。

- 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が付いていないことを確認します。

- b) セカンダリ FI の電源をオフにします。
- c) プライマリ FI の電源をオフにします。

これで、HX ストレージ クラスタの電源が安全にオフになりました。

次のタスク

1. ストレージ クラスタをシャットダウンまたは電源オフする必要があるタスクを実行します。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、またはノード上でのメンテナンスの実行です。

- 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 ガイドを参照してください。

これらのタスクでは、ホストのシャットダウンが必要な場合があります。サーバハードウェア ガイドの手順に従って、VM の移行、HX メンテナンス モードの開始、およびサーバの電源オフを実行します。



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

2. HX ストレージ クラスタを再起動するには、[HX ストレージ クラスタの電源オンと起動 \(67 ページ\)](#) に進んでください。

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 HX ストレージ クラスタの再起動に使用します。通常、この手順は、ストレージ クラスタ上でメンテナンス タスクが完了してから実行されます。

始める前に

[HX ストレージ クラスタのシャットダウンと電源オフ \(65 ページ\)](#) の手順を完了します。

ステップ 1 コンセントにつないで FI の電源を入れます。

- a) プライマリ FI の電源をオンにします。UCS Manager にアクセスできるよう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。それが UCS Manager 内でオンラインになっていることを確認します。

稀に、ファブリック インターコネクタをリブート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 インターコネクタにログインします。
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。
ノードは、自動的に電源がオンになって、ESX にブートするはずですが、どのノードもそうならない場合は、UCS Manager に接続して、UCS Manager からサーバ（ノード）の電源を入れます。
- b) 各 ESX ホストがアップし、UCS Manager 内のそれぞれのサービス プロファイルに関連付けられていることを確認します。

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なことを確認します。

すべての管理アドレスに ping します。

ステップ 4 すべてのコントローラ VM (stCtrlVM) の電源をオンにします。

方法を選択します。

vSphere クライアントを使用する。

- 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 を右クリックして、**[Power] > [Power On]** を選択します。
- c) 各ホストに対して、手順を繰り返します。

ESX ホストのコマンドラインを使用する。

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

```
# vim-cmd vmsvc/getallvms
```
- c) VMID を使用して、コントローラ VM の電源をオンにします。

```
# 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 5 すべてのコントローラ VM がブートして、ネットワークに到達可能になるまで待機します。その後で、確認します。

コントローラ VM のそれぞれの管理アドレスを ping します。

ステップ 6 ストレージクラスタが再起動する準備ができていることを確認します。

- a) 任意のコントローラ VM に SSH して、次のコマンドを実行します。

```
# stcli about
```
- b) コマンドがビルド番号を含むすべてのストレージクラスタ情報を返した場合は、ストレージクラスタが開始する準備ができています。ストレージクラスタの再起動に進みます。

- c) コマンドがすべてのストレージクラスタ情報を返さなかった場合は、ホスト上ですべてのサービスが開始するまで待機します。

ステップ 7 必要に応じて、各ノードのメンテナンス モードを終了します。

これは、`stcli cluster start` コマンドによって自動的に実行されます。

ステップ 8 ストレージクラスタを再起動します。

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。

```
# stcli cluster start
```

HX クラスタがシャットダウン中に実行されたメンテナンス タスクまたはアップグレードタスクによっては、ノードの HX メンテナンス モードまたは ESX メンテナンス モードが終了する場合があります。不明なホスト例外に関するエラー メッセージは無視してください。

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機します。

- 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。

```
# stcli cluster info
```

- b) 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 `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。最後の既知の状態によってはもう少し短くなる可能性があります。

ステップ 10 vCenter から、ESX によりデータストアが再マウントされたことを確認します。

クラスタが使用可能になると、データストアが自動的にマウントされ、使用可能になります。

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で、データストアが再マウントされたら、ワークロード VM の電源をオンにします。

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

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 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

ステップ 1 ESX ホストを HX 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 Configuration] ページを選択します。

vCenter クライアントで、[*ESX host*] > [Configuration] タブ > [Hardware] ペイン > [Advanced Settings] > [Edit] の順に選択します。

vCenter Web クライアントの [vCenter Inventory] で、[Resources] > [Hosts] > [*ESX host*] > [Manage] > [Settings] > [Hardware] > [PCI Devices] > [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。

- [DirectPath I/O Configuration] ページから、[Configure Passthrough] を選択します。
- [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。
- [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。

- 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 storage controller VM*] を右クリックし、[Edit Settings] > [PCI device 0] > [Remove] > [OK] の順に選択します。

vCenter Web クライアント : [*HX storage controller VM*] を右クリックし、[Edit Settings] > [Remove PCI device 0] > [OK] の順に選択します。

- LSI ロジック PCI デバイスを見つけて再度追加します。

vCenter クライアント : [*HX storage controller VM*] を右クリックし、[Edit Settings] > [Add] > [PCI Device] > [LSI Logic PCI device] > [OK] の順に選択します。

vCenter Web クライアント : [*HX storage controller VM*] を右クリックし、[Edit Settings] > [PCI Device] > [Add] > [LSI Logic PCI device] > [OK] の順に選択します。

ステップ 8 ESX ホストの HX 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 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 (71 ページ)
- クラスタの再調整 (71 ページ)
- スペース不足エラーの処理 (73 ページ)
- vCenter 間でのストレージクラスタの移動計画 (74 ページ)
- クラスタの名前変更 (80 ページ)

クラスタ アクセス ポリシー レベルの変更

ステップ 1 ストレージクラスタは、クラスタ アクセス ポリシーを「strict」に変更する前にヘルシー状態である必要があります。

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}
```

クラスタの再調整

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に応じて保存データの配布を再調整し、ストレージクラスタの正常性を復元するために使用されます。ストレージクラスタ内のノードを追加または削除する場合、`stcli rebalance` コマンドを使用して、ストレージクラスタの再調整を手動で開始できます。



(注) 再調整は、障害の発生しているノードやディスクで使用されているディスクのキャパシティによって、時間がかかる場合があります。

ステップ 1 ストレージ クラスタの再調整を開始します。

- a) ストレージ クラスタ内のコントローラ VM にログインします。
- b) 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。

```
# stcli rebalance start --force
```

ステップ 2 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) 進捗をモニタするには、次のコマンドを再入力します。

```
# stcli rebalance status
rebalanceStatus:
percentComplete: 0
rebalanceState: cluster_rebalance_not_running
rebalanceEnabled: True
```

- c) プロセスの完了を確認するには、次のコマンドラインを再入力します。

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

この例では、rebalance が有効になっており、再調整の実行準備が整っていますが、現在はストレージ クラスタが再調整されていないことを示しています。

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 クラスタの再調整は、定期的なスケジュールと、クラスタ内の使用可能なストレージの容量が変化した場合に実行されます。再調整は、使用可能なストレージの量が変化した場合にもトリガーされます。これは自動自己修復機能です。

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。

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] > [Summary]** の順に選択します。
[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。

[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）が表示されます。

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 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、現在ストレージクラスタで再調整が実行されていないことを示します。

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

HX Data Platform プラグインの [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 [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。

[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。

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] > [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) [Summary] > [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) [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 [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] > [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) **[Summary]** > **[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) **[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。

クリーナー スケジュールの確認

stcli cleaner コマンドは通常、バックグラウンドで継続的に実行されます。cleaner は、不要になるとスリープモードに入り、ポリシーにより定義されている条件に一致すると起動します。たとえば、ストレージクラスタで ENOSPC 状態が発生している場合には、クリーナーは自動的に高優先度で実行されます。

クリーナーの実行中には、クラスタを展開しないでください。クリーナースケジュールを確認するか、必要に応じてスケジュールを調整します。

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。リストされているコマンドをコントローラ VM のコマンドラインから実行します。

ステップ 2 クリーナーのスケジュールを表示します。

```
# stcli cleaner get-schedule --id ID | --ip NAME
```

パラメータ	説明
--id ID	ストレージクラスタ ノードの ID
--ip NAME	ストレージクラスタ ノードの IP アドレス

vCenter 間でのストレージクラスタの移動計画

vCenter データセンターまたは vCenter クラスタの名前を変更する場合は、HX ストレージクラスタを再登録する必要があります。

ある vCenter クラスタから別のクラスタにストレージクラスタを移動するには、一連の手順を実行する必要があります。詳細については、次のトピックを参照してください。

1. このタスクの前提条件を満たしてください。 [現在の vCenter Server から新しい vCenter Server へのストレージクラスタの移動 \(75 ページ\)](#) を参照してください。
2. 古い vCenter からクラスタを削除し、新しい vCenter に新しいクラスタを作成します。同じクラスタ名を使用します。 [現在の vCenter Server から新しい vCenter Server へのストレージクラスタの移動 \(75 ページ\)](#) を参照してください。
3. vCenter 拡張マネージャを使用して HX Data Platform の登録を解除します。参照先 [vCenter クラスタからのストレージクラスタの登録解除 \(75 ページ\)](#)

4. `stcli cluster reregister` コマンドを使用して、HX Storage Cluster を新しい vCenter に関連付けます。[新しい vCenter クラスタへのストレージクラスタの登録 \(79 ページ\)](#) を参照してください。

現在の vCenter Server から新しい vCenter Server へのストレージクラスタの移動

始める前に

- HX Cluster が 1.8(1c) よりも古いバージョンの HX Data Platform を実行している場合は、新しい vCenter に再登録する前にアップグレードしてください。
- このタスクは、メンテナンス期間中に実行してください。
- クラスタが正常な状態で、アップグレード状態が [OK] と [Healthy] であることを確認します。状態は、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表示できません。

```
# stcli cluster info
```

応答で以下を確認します。

```
upgradeState: ok  
healthState: healthy
```

- vCenter が起動して稼働している必要があります。
- 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しません。

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を作成したときに指定した vCenter クラスタです。

ステップ 2 新しい vCenter で、同じストレージ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内の新しい 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 \(75 ページ\)](#) 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 には HX Data Platform Plug-in の登録のみを残すようにしてください。

始める前に

ある vCenter サーバから別の vCenter サーバにストレージクラスタを移動するタスクでは、[現在の vCenter Server から新しい vCenter Server へのストレージクラスタの移動 \(75 ページ\)](#) の手順を実行します。



- (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。

ステップ 1 [EAM 拡張機能の登録解除および削除 \(76 ページ\)](#) の手順を完了します。

これは、HX クラスタを古い vCenter サーバから削除（登録解除）するための手順です。

また、当該の vSphere サーバにインストールされている HX クラスタよりも多くの ESX エージェントが存在する場合、クリーンアップが必要な古い EAM 構成がある可能性があります。

ステップ 2 [vSphere クライアントからの HX Data Platform ファイルの削除 \(78 ページ\)](#) の手順を完了します。

ステップ 3 [HX クラスタが vCenter から登録解除されたことの確認 \(79 ページ\)](#) の手順を完了します。

次のタスク

[新しい vCenter クラスタへのストレージクラスタの登録 \(79 ページ\)](#) 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トがある 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、古い拡張を削除します。

始める前に

- まだの場合、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。

ステップ 1 HX クラスタの UUID を指定します。

各エージェントには、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、登録を解除するための正しいクラスタ ID を選択してい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。

```
# stcli 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資格情報を入力します。

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。[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.sysgmt.cluster_domain_id および com.springpath.sysgmt.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) [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) [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 エージェント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資格情報を入力します。

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 エージェント拡張機能を見つけます。

a) [Properties] > [agency] > [Value] をスクロールします。

b) エージェントの値をクリックします。

- c) [Agency] ウィンドウで、[Properties] > [solutionID] > [Value] の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 エージェント拡張機能を削除します。

- a) [Agency] ウィンドウの [Methods] テーブルからメソッドを選択します。

古い ESX エージェントは、`destroyAgency` または `uninstall` のいずれかを使用すると削除できます。

- b) [method] ポップアップで、[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、ブラウザから 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 \(2109887\)](#)』を参照してください。

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

このタスクは、HX Storage Cluster の vCenter からの登録解除に含まれる手順です。

vSphere クライアントから HX Data Platform ファイルを削除します。メソッドを選択します。

Linux vCenter

- a) ルートユーザとして `ssh` を使用して Linux vCenter サーバにログインします。
b) HX Data Platform Plug-in フォルダが含まれているフォルダに変更します。

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 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) リモートデスクトッププロトコル (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 フォルダが含まれているフォルダに変更します。
cd "%PROGRAMDATA%\VMware\vsphere Web Client\vc-packages\vsphere-client-serenity
- c) HX Data Platform Plug-in フォルダとファイルを削除します。
rmdir /com.springpath*
- d) [Service] 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 から登録解除されたことの確認

このタスクは、HX Storage Clusterの vCenter からの登録解除に含まれる手順です。
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

次の項に記載の手順を実行します。

- [EAM 拡張機能の登録解除および削除 \(76 ページ\)](#)
- [vSphere クライアントからの HX Data Platform ファイルの削除 \(78 ページ\)](#)

ステップ 1 古い vCenter からログアウトします。

ステップ 2 古い vCenter に再度ログインし、HX Data Platform Plug-inが削除されていることを確認します。

新しい vCenter クラスタへのストレージクラスタの登録

始める前に

vCenter Server 間でストレージクラスタを移動するタスクでは、[vCenter クラスタからのストレージクラスタの登録解除 \(75 ページ\)](#) の手順を実行します。

ステップ 1 コントローラ VM にログインします。

ステップ 2 `stcli cluster reregister` コマンドを実行します。

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

必要に応じて、リストされている追加オプションを適用します。

構文の説明	オプション	必須またはオプション	説明
	--vcenter-cluster NEWVCENTERCLUSTER	必須	新しい vCenter クラスタ名。
	--vcenter-datacenter NEWDATACENTER	必須	新しい vCenter データセンター名。
	--vcenter-ssso-url NEWVCENTERSSSOURL	任意	新しい vCenter SSO サーバの URL。指定されていない場合、これは --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 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。

応答の例：

```
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、リソースプール内に存在しない場合は、TAC にコンピューティングノードの再登録を依頼します。

ステップ 3 クラスタ上にコンピューティングノードが存在する場合は、再登録の完了後に、コンピューティングノードを再追加します。

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

ステップ 4 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しません。

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ら、他のプロセスを中断せずにこのクラスタの名前を変更できます。



(注) これらの手順は HX Cluster の名前変更の手順であり、vCenter クラスタの名前変更の手順ではありません。

-
- ステップ 1** 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] (名前を変更するクラスタ) の順に選択します。
- ステップ 2** [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、またはタブ上部にある [Actions] ドロップダウンリストをクリックします。
- ステップ 3** [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 クラスタ名は 50 文字以内です。
- ステップ 5** [OK] をクリックして新しい名前を適用します。
-



第 6 章

暗号化の管理

- [自己暗号化ドライブの概要 \(83 ページ\)](#)
- [HyperFlex クラスタが暗号化できることの確認 \(84 ページ\)](#)
- [ローカル暗号化キーの構成 \(84 ページ\)](#)
- [ローカル暗号化キーの変更 \(85 ページ\)](#)
- [ローカルの暗号化キーの無効化 \(85 ページ\)](#)
- [暗号化されたディスクを安全に消去する \(86 ページ\)](#)
- [リモート キー管理 \(86 ページ\)](#)
- [証明書署名要求の生成 \(87 ページ\)](#)
- [CSR \(証明書署名要求\) を使用したキー管理サーバの構成 \(88 ページ\)](#)
- [自己署名証明書の生成 \(89 ページ\)](#)
- [SSC \(自己署名証明書\) を使用したキー管理サーバの構成 \(91 ページ\)](#)
- [暗号化のやり直し \(92 ページ\)](#)

自己暗号化ドライブの概要

自己暗号化ドライブ (SED) には、リアルタイムで着信データを暗号化し、送信データを復号化する特殊なハードウェアが搭載されています。ディスク上のデータは常に暗号化された形式で格納されます。メディア暗号化キーがこの暗号化と復号化を制御します。このキーは、プロセッサやメモリに格納されることはありません。

セキュリティキー (キー暗号化キーまたは認証パスフレーズとも呼ばれます) を使用して、メディア暗号化キーを暗号化します。SED を有効にするには、セキュリティ キーを入力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、データをフェッチするのにキーは必要ありません。

Cisco HyperFlex Systems を使用して、ローカルまたはリモートのセキュリティ キーを構成できます。ローカルでキーを設定した場合、そのキーを覚えておく必要があります。キーを忘れた場合はそれを取得することはできず、ドライブの電源が再投入されると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) を使用して、キーをリモートから設定できます。この方法で、ローカル管理でのキーの保管と取得に関する問題に対処します。

SEDの暗号化と復号化は、ハードウェアを通じて実行されます。したがって、全体的なシステムパフォーマンスに影響しません。SEDは瞬時に暗号を消去することで、ディスクの使用停止や再展開のコストを削減します。メディア暗号化キーを変更することで、暗号消去が実行されます。ディスクのメディア暗号化キーを変更すると、そのディスク上のデータは復号化できず、すぐに使用できない状態になります。

HyperFlex クラスタが暗号化できることの確認

HX Data Platform Plug-inを使用しての確認

1. HX Data Platform Plug-inから vSphere Web Clientにログインします。
2. [Cisco HX Data Platform] > [hx_cluster] > [Summary] を選択します。
3. HyperFlex 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、[Summary] タブの上部に [Data At Rest Encryption-Capable] が表示されます。

HX Connect ユーザ インターフェイスを使用しての確認

1. HX Connect UI から、[Encryption] を選択します。
2. HX HyperFlex 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。

ローカル暗号化キーの構成

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

ステップ2 [Encryption] ページで、[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	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[Next] をクリックします。

ステップ 4 ローカルで生成され、保存された暗号化キーを使用して HyperFlex クラスタを保護するには、[Local Key] を選択します。

[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）を入力してください。

（注） ちょうど 32 文字の英数字で入力します。

ステップ 6 [Enable Encryption] をクリックします。

ローカル暗号化キーの変更

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

ステップ 2 [Encryption] ページで、[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	基本情報
[UCS Manager host name] フィールド	たとえば <i>10.193.211.120</i> と入力します。
[User name] フィールド	<admin> ユーザ名。
[Password] フィールド	<root> パスワード。

[Next] をクリックします。

ステップ 4 クラスタの [Existing Encryption Key] と [New Encryption Key] を入力します。

（注） ちょうど 32 文字の英数字で入力します。

ステップ 5 [Re-key] をクリックします。

ローカルの暗号化キーの無効化

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

ステップ 2 [Encryption] ページの [Edit configuration] ドロップダウンメニューから、[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	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[Next] をクリックします。

ステップ 4 クラスタで暗号化キーを無効にするには、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 [Disable encryption] をクリックします。

ステップ 6 クラスタで暗号化キーを無効にすることを確認するために [Disable encryption?] ダイアログボックスで、[Yes, disable encryption] をクリックします。

暗号化されたディスクを安全に消去する

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

ステップ 2 [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 [Secure Erase] ボタンをクリックします。

ステップ 4 クラスタ上の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 [Secure erase] をクリックします。

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

リモート キー管理

リモート KMIP 証明書 の処理の一般的な手順は次のとおりです。

- 自己署名する場合は、設定でローカルの認証局を指定し、ルート証明書を取得します。
- 信頼されたサードパーティの CA を使用する場合は、設定でそれを指定し、そのルート証明書を使用します。
- クラスタ キーを尋ねる 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。

- 使用しているルート証明書で CSR に署名します。
- クライアント証明書を使用する KMIP サーバ設定を更新します。
- SSL 証明書とルート CA が利用可能な状態で、選択したベンダーに固有の KMIP サービス設定で続行します。

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、『[HyperFlex Encryption and SafeNet Key Management TechNote](#)』および『[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化キーの管理に関する詳細は、[Vormetric サポートポータル](#)のマニュアルダウンロードセクションを参照してください。

証明書署名要求の生成

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

ステップ 2 [Encryption] ページで、[Configure encryption] をクリックします。

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

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

[Next] をクリックします。

ステップ 4 [Key Management Server] > [Use certificate authority signed certificates] を選択します。

[Next] をクリックします。

ステップ 5 キー管理 (KMIP) サーバを構成するためのリモート暗号化キーを生成するには、次の情報を入力します。

UI 要素	基本情報
[Email address] フィールド	<admin> 電子メールアドレス
[Organization name] フィールド	証明書を要求している組織。 32 文字まで入力します。

UI 要素	基本情報
[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 文字まで入力します。
[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 文字まで入力します。
[Country] フィールド	会社が存在する国。 2 つの英字を大文字で入力します。
[Valid for (days)] フィールド	証明書の有効期間。

ステップ 6 HyperFlex のすべてのノードのための証明書署名要求（CSR）を生成してそれらをダウンロードするには、[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、認証局による署名を受けます。[Close] をクリックします。

次のタスク

- 署名付き証明書をアップロードします。
- 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

KMIP（キーマネージメント）サーバを構成するために、ローカルマシン上で生成された CSR をダウンロードし、それが認証局によって署名され、Cisco HX Data Platform UI 経由でアップロードされていることを確認してください。

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

ステップ 2 [Encryption] ページで、[Continue configuration] をクリックします。

ステップ 3 [Continue configuration] ドロップダウンリストから、[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	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-f12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[Next] をクリックします。

ステップ 5 [Upload certificate authority signed certificates] を選択します。[Next] をクリックします。

ステップ 6 [Upload new certificate] で CA 署名証明書をアップロードします。[Upload] をクリックします。

ステップ 7 [Continue configuration] ドロップダウン リストから [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 の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	基本情報
[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。
(省略可能) [Secondary key management server] フィールド	冗長化のためのセカンダリ キー管理サーバを設定した場合は、ここで詳細情報を入力します。
[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。
[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 [Save] をクリックしてクラスタをリモート管理キーで暗号化します。

例

自己署名証明書の生成

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

ステップ 2 [Encryption] ページで、[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	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[Next] をクリックします。

ステップ 4 [Key Management Server] > [Use self-signed certificates] を選択します。

[Next] をクリックします。

ステップ 5 キー管理 (KMIP) サーバを構成するためのリモート暗号化キーを生成するには、次の情報を入力します。

UI 要素	基本情報
[Email address] フィールド	<admin> 電子メール アドレス
[Organization name] フィールド	証明書を要求している組織。 32 文字まで入力します。
[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 文字まで入力します。
[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 文字まで入力します。
[Country] フィールド	会社が存在する国。 2 つの英字を大文字で入力します。
[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 ノードのために自己署名証明書を生成してそれらをダウンロードするには、[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、認証局による署名を受けます。[Close] をクリックします。

次のタスク

1. 署名付き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。

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 マネージメント）サーバを構成するためにローカル マシン上で生成された SSC がダウンロードされていることを確認してください。

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

ステップ 2 [Encryption] ページで、[Edit configuration] をクリックします。

ステップ 3 [Edit configuration] ドロップダウン リストから、[Manage certificates] を選択します。

ステップ 4 次の Cisco UCS Manager のクレデンシアルを入力して、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	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[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アルを入力します。

UI 要素	基本情報
[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。
(省略可能) [Secondary key management server] フィールド	冗長化のためのセカンダリ キー管理サーバを設定した場合は、ここで詳細情報を入力します。
[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。

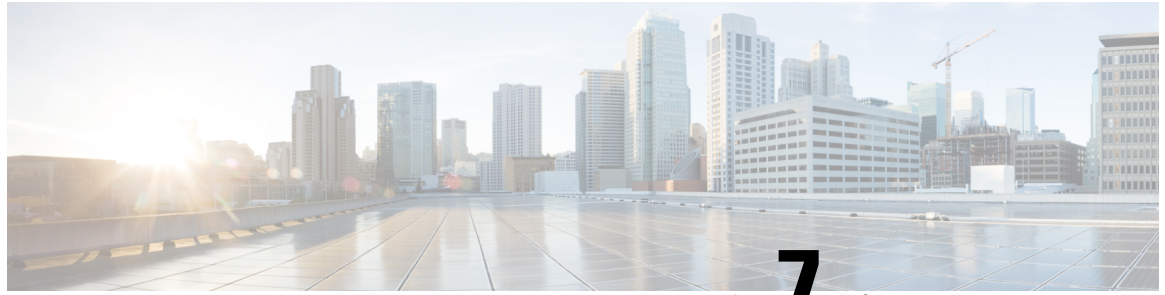
UI 要素	基本情報
[Public key] フィールド	KMIP サーバ構成中に生成された認証局の公開ルート証明書を入力します。

ステップ 6 [Save] をクリックしてクラスタをリモート管理キーで暗号化します。

暗号化のやり直し

HyperFlex クラスタを安全に暗号化するには、Cisco UCS Manager の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 キーの構成を再度開始します。

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



第 7 章

データストアの管理

- [データストアの管理 \(93 ページ\)](#)
- [データストアの追加 \(94 ページ\)](#)
- [データストアの編集 \(94 ページ\)](#)
- [データストアのマウント \(95 ページ\)](#)
- [データストアのマウント解除 \(96 ページ\)](#)
- [データストアの削除 \(97 ページ\)](#)
- [部分的にマウント解除されたデータストアの回復 \(97 ページ\)](#)

データストアの管理

データストアは、ストレージの使用とストレージリソースの管理のために HX Data Platform で使用される論理コンテナです。データストアは、ホストが仮想ディスク ファイルと他の VM ファイルを配置する場所です。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 または HX Data Platform Plug-in の UI から、データストアの追加、リストの更新、名前とサイズの編集、削除、マウントおよびマウント解除ができます。

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 Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [cluster] > [Manage] > [Datastores]** の順に選択します。
- HX Connect から **[Datastores]** を選択します。

ステップ 2 新しいデータストアを作成するか、または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。

- 新しいデータストアの作成
- データストアのリストの更新
- データストア名とサイズの編集
- データストアの削除
- ホスト上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

論理コンテナ内のデータストアは、ファイルシステムと同様に、物理ストレージ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。ISO イメージと VM テンプレートを保存するためにデータストアを使用することもできます。

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 Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [cluster] > [Manage] > [Datastores] の順に選択します。
- HX Connect から [Datastores] を選択します。

ステップ 2 データストアを作成するように選択します。

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ます。

ステップ 4 データストア 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 データのブロックサイズを指定します。HX Connect から、[8K] または [4K] を選択します。デフォルトは 8K です。HX Data Platform Plug-in では、デフォルトが想定されます。VDI ワークロードの場合、デフォルトは 4K です。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更を取り消します。

ステップ 7 データストアを確認します。必要に応じて [Refresh] ボタンをクリックし、新しいデータストアを表示します。

HX Data Platform Plug-in で、[Manage] > [Datastores] > [Hosts] タブをクリックして、新しいデータストアのマウント状態を確認します。

vSphere クライアントアプリケーションを介してデータストアを確認する場合、[host] > [Configuration] > [Datastores] で、[Drive Type] が `Unknown` として表示されます。この vSphere の動作はあらかじめ見込まれており、NFS データストアを不明としてリストするためのものです。

データストアの編集

HX のデータプラットフォームのデータストアは、編集（鉛筆）オプションを使用して変更できます。編集には以下のオプションがあります。

- データストア名を変更します。



(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。

- データストアのストレージの割り当ての変更。つまり、データストアのサイズ変更。

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 Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [cluster] > [Manage] > [Datastores] の順に選択します。
- HX Connect から [Datastores] を選択します。

ステップ 2 [datastore] を選択します。

ステップ 3 データストアをマウント解除します。

データストアのサイズだけを変更した場合は、データストアをマウント解除する必要はありません。このステップをスキップします。

ステップ 4 データストアの [Edit] (鉛筆アイコン) をクリックします。

ステップ 5 データストアの名前および/またはサイズを必要に応じて変更します。[OK] をクリックします。

ステップ 6 以前マウント解除した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

データストアのマウント準備。

- VM、テンプレート、スナップショット、CD/DVD イメージはデータストアには存在しません。これは、マウント解除時の最も一般的なエラーです。
- ストレージ I/O 制御はデータストアでは無効です。
- 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、ホスト RDM メタデータ ファイル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。

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 Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [cluster] > [Manage] > [Datastores] の順に選択します。
- HX Connect から [Datastores] を選択します。

ステップ2 [datastore] を選択します。

ステップ3 [Mount] をクリックします。

ステップ4 データストアのマウントを確認し、[OK] をクリックします。

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。

- VM、テンプレート、スナップショット、CD/DVD イメージはデータストアには存在しません。これは、マウント解除時の最も一般的なエラーです。
- ストレージ I/O 制御はデータストアでは無効です。
- 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、ホスト RDM メタデータ ファイル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解除。

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 Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [cluster] > [Manage] > [Datastores] の順に選択します。
- HX Connect から [Datastores] を選択します。

ステップ2 [datastore] を選択します。

ステップ3 [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、[OK] をクリックします。

ステップ5 必要に応じて部分的なマウント解除から回復。

- a) 上記のチェックリストに従って、UI または CLI のいずれかを使用してマウント解除するか削除します。
- 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。

データストアの削除

データストアを削除する準備をします。

- すべての VM の電源をオフにします。
- データストア マウント ポイント上のすべてのオープン シェルを閉じます。
- データストアの 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。

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 Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [cluster] > [Manage] > [Datastores] の順に選択します。
- HX Connect から [Datastores] を選択します。

ステップ 2 [datastore] 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、[OK] をクリックします。

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。

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 Connect または HX Data Platform Plug-in 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、削除を試みます。

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) 可能なソリューションはこれ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 8 章

ディスクの管理

- クラスタ内のディスクの管理 (99 ページ)
- ディスクの要件 (100 ページ)
- 自己暗号化ドライブ (SED) の交換 (104 ページ)
- SSD の交換 (106 ページ)
- NVMe SSD の交換 (108 ページ)
- ハウスキーピング SSD の交換 (109 ページ)
- ハードディスク ドライブの交換または追加 (111 ページ)

クラスタ内のディスクの管理

ディスク、SSD または HDD では、障害が発生する可能性があります。この場合、障害が発生したディスクを取り外し、交換する必要があります。ホスト内で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の指示手順に従ってください。HX Data Platform は SDD 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ョンノードに同じサイズとタイプの SSD を追加します。ハイブリッドサーバでは、ハードディスク ドライブ (HDD) を追加します。オールフラッシュサーバでは、SSD を追加します。



(注) 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)。ドライブを引き出して交換し、少し間を開けて、次のドライブを引き出して交換します。

ディスクを取り外しても、そのディスクが引き続きクラスタ概要情報に表示される場合があります。これを更新するには、HX クラスタを再起動します。

ディスクの要件

ディスクの要件は、コンバージドノードとコンピューティング専用ノード間で異なります。使用可能な CPU およびメモリ容量を拡大するには、必要に応じてコンピューティング専用ノードを使用して既存のクラスタを拡張します。これらのコンピューティング専用ノードを使用すると、ストレージのパフォーマンスを向上させたり、ストレージ容量を拡大したりすることができます。

あるいはコンバージドノードを追加することで、CPU およびメモリ リソースを拡大するとともに、ストレージのパフォーマンスを向上させ、ストレージ容量を拡大できます。

ソリッドステートディスク (SSD) のみが搭載されたサーバは、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) の両方が搭載されたサーバは、ハイブリッドサーバです。

以下は、HyperFlex クラスタ内のすべてのディスクに適用されます。

- ストレージクラスタ内のすべてのディスクには、同量のストレージ容量が必要です。ストレージクラスタ内のすべてのノードには、同数のディスクが必要です。
- すべての **SSD** は TRIM をサポートする必要があるため、TRIM が有効になっている必要があります。
- すべての **HDD** は、SATA または SAS タイプのいずれかです。ストレージクラスタ内のすべての SAS ディスクは、パススルーモードにする必要があります。
- ディスクパーティションは、SSD および HDD から削除する必要があります。パーティションが設定されたディスクは無視され、HX ストレージクラスタに追加されません。
- オプションで、ディスク上の既存のデータを削除またはバックアップできます。提供されたディスク上の既存のデータはすべて上書きされます。



(注) 新規のファクトリサーバは適切なディスクパーティションの設定で出荷されます。新規の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いでください。

- シスコから直接購入され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) が搭載されたサーバでは、キャッシュドライブと永続ストレージ (キャパシティ) ドライブの両方が SED に対応している必要があります。これらのサーバは、保管中データの暗号化 (DARE) をサポートします。

コンバージドノード

次の表に示すディスクに加えて、すべての M4 コンバージドノードは、ESX がインストールされたミラー設定で 2 枚の 64 GB SD FlexFlash カードを備えています。すべての M5 コンバージドノードには、ESXi 搭載の M.2 SATA SSD が内蔵されています。



- (注) サーバ上またはストレージ クラスタ全体でストレージ ディスクのタイプや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つのサーバでは、すべて HDD またはすべて SSD とし、ドライブのサイズを統一してください。
 - ハイブリッド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。
 - すべてのノードで同じサイズと同じ数量の SSD を使用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。

次の表に、HX サーバタイプごとの互換性のあるドライブを示します。ドライブは、指示がない限り、サーバの前面スロットに取り付けられます。複数のドライブが示されている場合、それらはオプションです。1つのドライブ サイズをサーバあたりのキャパシティとして使用してください。ドライブの最小数と最大数は、コンポーネントごとに記載されています。

HX240 M5 サーバ

コンポーネント	数量	Hybrid	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
キャッシュ SSD	1 (背面)	1.6 TB SSD	1.6 TB NVMe 400 GB SSD	1.6 TB SSD	800 GB SSD
永続	6 ~ 23	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX240 M4 サーバ

コンポーネント	数量	Hybrid	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD
キャッシュ SSD	1	1.6 TB SSD	1.6 TB NVMe 400 GB SSD	1.6 TB SSD	1.6 TB NVMe 800 GB SSD
永続	6 ~ 23	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX220 M5 サーバ

コンポーネント	数量	Hybrid	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
キャッシュ SSD	1	480 GB SSD 800 GB SSD	1.6 TB NVMe 400 GB SSD	800 GB SSD	800 GB SSD
永続	6 ~ 8	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX 220 M4 サーバ

コンポーネント	数量	Hybrid	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD
キャッシュ SSD	1	480 GB SSD	400 GB SSD	800 GB SSD	800 GB SSD
永続	6	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

エッジクラスタ用 HX220 M5 サーバ

コンポーネント	数量	Hybrid	すべてフラッシュ	ハイブリッドSED	オールフラッシュ SED
ハウスキーピング SSD	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
キャッシュ SSD	1	480 GB SSD 800 GB SSD	1.6 TB NVMe 400 GB SSD	800 GB SSD	800 GB SSD
永続	3 ~ 8	1.2 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

エッジクラスタ用 HX 220 M4 サーバ

コンポーネント	数量	Hybrid	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD
キャッシュ SSD	1	480 GB SSD	400 GB SSD	800 GB SSD	800 GB SSD
永続	3 ~ 6	1.2 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

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対しサポートされているコンピューティング専用ノードの設定を示します。コンピューティング専用ノードのストレージは、ストレージクラスタのキャッシュまたは容量に含まれていません。



(注) HyperFlex 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。サーバ関連のポリシーについては、『Cisco UCS Manager Server Management Guide』を参照してください。

サポートされ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
<ul style="list-style-type: none"> • Cisco B200 M3/M4/M5 • B260 M4 • B420 M4 • B460 M4 • C240 M3/M4/M5 • C220 M3/M4/M5 • C460 M4 • C480 M5 • B480 M5 	<p>方法を選択します。</p> <p>重要 ESXi インストールの際は、ブートメディアの形式が1つだけサーバに通知されるようにしてください。ローカルまたはリモートのディスクの追加は、インストール後に実行できます。</p> <p>USB ブートは HX コンピューティング専用のノードに対してサポートされていません。</p> <ul style="list-style-type: none"> • ESXi がインストールされているミラー設定での 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。

自己暗号化ドライブ (SED) の交換

Cisco HyperFlex システムは、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は、自己暗号化ドライブを備えたサーバを参照します。
- 暗号化された HX Cluster 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、クラスタの作成後に、HX Connect を使用して、HX Cluster に構成されます。
- 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 を削除する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 Cluster に暗号化が適用されているかどうかを判定します。

- 暗号化が構成されていない：SEDを削除または交換するためには、暗号化に関連した前提条件の手順は不要です。[SSDの交換（106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（111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：次を確認します。
 1. SEDを交換する場合は、メーカーの返品承認（RMA）を取得します。TACに連絡します。
 2. 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。
 3. データの損失を防ぐために、ディスク上のデータがデータの最後のプライマリコピーではないことを確認します。
必要な場合は、クラスタ上のサーバにディスクを追加します。開始するか、またはリバランスが完了するまで待機します。
 4. SEDを削除する前に、以下のステップを完了します。

ステップ 1 HX Clusterが正常であることを確認します。

クラスタが正常でない場合、SEDを削除または交換するにはTACにお問い合わせください。

ステップ 2 HX Connect にログインします。

ステップ 3 [System Information] > [Disks] ページを選択します。

ステップ 4 削除するディスクを識別し、確認します。

1. [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. [Turn Off Locator LED] ボタンを使用します。

ステップ 5 削除するディスクに対応する [Slot] 行を選択します。

ステップ 6 [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 [Encryption Key] を入力して [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、[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 [Disk Slot] の [Status] が [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、元の、または別の HX Cluster 内のドライブ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 [Type] 列を確認します。

- [Solid State] (SSD) : [SSD の交換 \(106 ページ\)](#) およびお使いのサーバのハードウェア ガイドを参照してください。
- [Rotational] (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 \(111 ページ\)](#) およびお使いの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

- [Status] : [Ok To Remove] のままです。
- [Encryption] : [Enabled] から [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 Cluster 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 キーが新しいディスクに適用されます。

- [Status] : [Ignored] > [Claimed] > [Available] に遷移します。
- [Encryption] : 暗号化キーが適用された後に、[Disabled] > [Enabled] に遷移します。

SSD の交換

SSD の交換手順は、SSD の種類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) サーバ上またはストレージクラスタ全体でストレージディスクのタイプまたはサイズを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、すべてのフラッシュサーバではすべてフラッシュ 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。

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的な SSD では、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 \(58 ページ\)](#) を参照してください。

キャッシュと永続的な SSD のみが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 の場合は物理的な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 サーバ上のハウスキーピング SSD の場合は、サーバの背面で物理的なチェックを実行します。
- HXAF220c または HX220c サーバ上のハウスキーピング SSD の場合は、サーバのドライブ ベイ 2 で物理的なチェックを実行します。

ステップ 2 失敗した SSD がハウスキーピング SSD の場合は、サーバの種類に基づいて続行してください。

- HXAF220c または HX220c サーバの場合は、手順 3 に進みます。
- HXAF240c または HX240c サーバの場合は、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。

ステップ 3 故障した SSD がキャッシュまたは永続 SSD の場合は、ディスクのタイプに基づいて続行してください。

- NVMe SSD については、[NVMe SSD の交換 \(108 ページ\)](#) 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、ホスト内の故障した 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的なドライブを交換後、HX Data Platform は SDD を識別し、ストレージクラスタを更新します。

ノードに追加したディスクは、すぐに HX で使用できるようになります。

- ステップ 4** Cisco UCS Manager の [UCS Manager Server Inventory Storage] タブに新しいディスクを含めるには、サーバ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。
- ステップ 5** SSD を交換して、「*Disk successfully scheduled for repair*」のメッセージが表示された場合、ディスクは存在しているが正常に機能していないということを意味します。サーバ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 の種類によって異なります。ここでは、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) サーバ上またはストレージクラスタ全体でストレージディスクのタイプまたはサイズを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際は、必ず、元のディスクと同じタイプとサイズを使用してください。

始める前に

HX Cluster サーバで NVMe の SSD を使用する場合、次の条件を満たすことを確認します。

- NVMe の SSD は、HX240 および HX220 のオールフラッシュサーバでサポートされます。
- NVMe SSD を HGST SN200 ディスクに置き換えるには、HX Data Platform バージョン 2.5.1a 以降が必要です。
- NVMe の SSD は、サーバのスロット 1 にのみ搭載できます。他のサーバスロットは NVMe の SSD を検出しません。
- NVMe の SSD はキャッシュにのみ使用されます。
 - 永続的なストレージでの使用はサポートされていません。
 - ハウスキーピングのドライブとしての使用はサポートされていません。
 - ハイブリッドサーバでの使用はサポートされていません。

- ステップ 1** 故障したディスクが 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。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。

故障した SSD が NVMe SSD でない場合は、[SSD の交換 \(106 ページ\)](#) を参照してください。

- ステップ 2** ESXi ホストを HX 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) **[System Information] > [Nodes] > [node] > [Enter HX Maintenance Mode]** を選択します。

ステップ 3 サーバのハードウェア ガイドに従って、ホスト内の故障した SSD を取り外して交換する手順を実行します。

(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再挿入するか、ホストをリブートするまで、コントローラ VM が正常に機能しません。

キャッシュまたは永続的なドライブを交換後、HX Data Platform は SDD を識別し、ストレージクラスタを更新します。

ノードに追加したディスクは、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。これで ESXi は NVMe SSD を検出できます。

ステップ 5 ESXi ホスト の HX 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 Server Inventory Storage] タブに新しいディスクを含めるには、サーバ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。

ステップ 7 SSD を交換して、「*Disk successfully scheduled for repair*」のメッセージが表示された場合、ディスクは存在しているが正常に機能していないということを意味します。サーバハードウェア 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。

ハウスキーピング SSD の交換



(注) この手順は、HXAF220c または HX220c サーバにのみ適用されます。HXAF240c または HX240c 上のハウスキーピング SSD を交換するには、Cisco TAC にお問い合わせください。

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。

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、種類とサイズが同じ新しい 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ます。

(注) ハードウェア手順を実行する前に、ノードを Cisco HX 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 Cisco HX 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、影響を受けた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ます。

```
# /usr/share/springpath/storfs-appliance/config-bootdev.sh -r -y
```

このコマンドは新しいディスクを使用し、そのディスクをストレージコントローラに追加します。

サンプル応答

```
Creating partition of size 65536 MB for /var/stv ...
Creating ext4 filesystem on /dev/sdg1 ...
Creating partition of size 24576 MB for /var/zookeeper ...
Creating ext4 filesystem on /dev/sdg2 ...
Model: ATA INTEL SSDSC2BB12 (scsi)
Disk /dev/sdg: 120034MB
Sector size (logical/physical): 512B/4096B
Partition Table: gpt ....
discovered. Rebooting in 60 seconds
```

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。

```
# stcli 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 HX Data Platform インストーラ パッケージを、/tmp フォルダ内のストレージコントローラ VM にコピーします。

```
# scp <hxdp_installer_vm_ip>:/opt/springpath/packages/storfs-packages-<hxdp_installer>.tgz /tmp
# cd /tmp
# tar zxvf storfs-packages-<hxdp_installer>.tgz
```

ステップ 8 HX Data Platform インストーラ導入スクリプトを実行します。

```
# ./inst-packages.sh
```

HX Data Platform のインストールに関する追加情報については、『*Cisco HX Data Platform Getting Started Guide*』を参照してください。

ステップ 9 パッケージのインストール後、HX Data Platform は自動的に起動します。ステータスを確認します。

```
# status storfs
```


サンプル応答

```
storfs running
```

新しい SSD を搭載したノードが既存のクラスタに再接続し、クラスタが正常な状態に戻ります。

ハードディスク ドライブの交換または追加



- (注) サーバ上またはストレージクラスタ全体でストレージディスクのタイプまたはサイズを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、すべてのフラッシュサーバではすべてフラッシュ 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。

ステップ 1 ご使用のサーバのハードウェア ガイドを参照し、ディスクの追加または交換の手順に従います。

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 妥当な時間内で各ノードに HDD を追加します。

ストレージは、すぐにストレージクラスタによって使用され始めます。

[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、ディスクはすぐに HX で使用できるようになりますが、UCSM サーバ ノード インベントリには表示されません。これには、キャッシュ ディスクと永続ディスクが含まれます。UCS Manager サーバの [Inventory 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。



第 9 章

ノードの管理

- ノードの管理 (113 ページ)
- ノードメンテナンス方法の特定 (115 ページ)
- DNS アドレスまたはホスト名による検索 (118 ページ)
- ESXi ホストルートパスワードの変更 (119 ページ)
- ノードソフトウェアの再インストール (119 ページ)
- 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 (120 ページ)
- ノードコンポーネントの交換 (121 ページ)
- ノードの取り外し (123 ページ)
- ノードの交換 (131 ページ)

ノードの管理

ノードを初めて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 Create Cluster 機能を使用します。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 Expand Cluster 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。



(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ほとんど区別されずに使われています。一般に、サーバは、特定の目的に特化された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。

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 Data Platform Plug-in、vCenter UI、およびさまざまなログに動作ステータス (online、offline) 値と復元力ステータス値 (healthy、warning) として報告されます。

(注) 機能状態の区別は、HX Connect および HX Data Platform Plug-in 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あります。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 (lenient または 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 Read と Write、Read Only、または Shutdown の間で変化します。

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、サーバ ビーコンのチェック、ログの収集と分析、および TAC との連携が必要になります。

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 の再インストール手順については、TAC 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 や 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、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。

ストレージクラスタ内のノードを交換する際は、常に 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。3 ノードクラスタ内のノードを交換する際は、常に TAC の支援が必要です。

- クラスタからノードを取り外します。

(注) ノードを削除する場合、使用可能なノードの数が最小数の 3 を下回ってはなりません。これは、3 を下回るとストレージクラスタが正常ではなくなるためです。3 ノードクラスタ内のノードを取り外す際は、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 HX 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、および TAC によるサポートが必要なものがあります。

- **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 サポートタスク**：一般に、TAC 担当員が実行する操作を必要とします。



(注) 3 ノードクラスタ内のノードを交換する際は、常に TAC によるサポートが必要です。

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、TAC にお問い合わせください。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

ノードの修理可能なアイテムで障害が発生しました。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	方式	注
3	1つ以上	TACはノードの修理だけをサポートします。	修理のためにノードを取り外す必要はありません。ノードのディスクの交換を含みます。
4-8	1	オンラインまたはオフラインでのノード修理。	修理のためにノードを取り外す必要はありません。ノードのディスクの交換を含みます。

ノードの取り外し

ノードの修理不可能なアイテムで障害が発生しました。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できません。

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	方式	注
4	1	オフラインノードの取り外し。	4ノードクラスタで2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ノードの取り外し。	
5つ以上	2	オフライン2ノードの取り外し。	5ノードクラスタで3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

ノードの修理不可能なアイテムで障害が発生しました。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できません。

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	方式	注
3	1	TAC はノードの交換だけをサポートします。	クラスタを最小限の 3 ノードに戻すには、TAC によりサポートされるノードの交換が必要です。 3 ノードクラスタで 1 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	ノードのオフライン交換。 ディスクを再利用しない。	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。その他のすべてのノードが稼動している必要があります。 4 ノードクラスタで 2 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ノードの交換。 ディスクを再利用しない。	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。その他のすべてのノードが稼動している必要があります。
5 つ以上	2	1 または 2 ノードのオフライン交換。 ディスクを再利用しない。	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。その他のすべてのノードが稼動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 つ以上のノードの交換には 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

ノードの修理不可能なアイテムで障害が発生しました。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	方式	注
3 つ以上	1 つ以上	TAC によるサポートのみ。	<p>クラスタを最小限の 3 ノードに戻すには、TAC によりサポートされるノードの交換が必要です。</p> <p>(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 からノード UUID への関係は固定であり、再割り当てできません。これは TAC サポート タスクです。</p>

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。

ステップ 1 DNS 検索アドレスを割り当てます。

- 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。
- resolv.conf.d ファイルを編集します。

```
# vi /etc/resolvconf/resolv.conf.d/base
```
- 変更を確認します。

```
# resolvconf -u
# cat /etc/resolv.conf
```
- DNS サーバが IP アドレスまたはホスト名から問い合わせることが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。

- 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。
- hosts ファイルを編集用に開きます。

```
# vi /etc/hosts
```
- 次の行を追加して、ファイルを保存します。


```
ip_address ubuntu newhostname
```

ホスト `ip_address` ごとに、ホスト `newhostname` を入力します。

a) `newhostname` を `hostname` に追加します。

```
# hostname newhostname
```

ESXi ホストルートパスワードの変更

インストール後のデフォルトの ESXi ルートパスワードを変更するには、次の手順を実行します。



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

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

ステップ 2 ルート権限を取得します。

```
su -
```

ステップ 3 現在のルートパスワードを入力します。

ステップ 4 ルートパスワードを変更します。

```
passwd root
```

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

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

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ーのメンバーであるノード上の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 の支援を得て実行する必要があります。

ステップ 1 TAC 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 サーバの設定要件に記載されている必要なハードウェアおよび構成を満たしていることを確認します。HX の構成時の設定は、HX Data Platform プロセス中に適用されます。

ステップ 2 TAC の指示に従って HX Data Platform を再インストールします。

HX Data Platform は、必ず、ESX の再インストール後に再インストールする必要があります。

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。

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。

HX Connect、HX Data Platform Plug-in、またはストレージコントローラ VM 上の `stcli clsuter info` コマンドから、ストレージクラスタのステータスをチェックします。

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 ホストの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 が vCenter、相互 ESXi ホスト、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、**[Configuration] > [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。それらを書き留めます。この名前は、後のステップで使用します。

ステップ 7 vCenter から **cluster** を削除します。

vCenter から、**[datacenter] > [cluster]** を選択します。**[cluster]** を右クリックして、**[Delete]** を選択します。

(注) **[datacenter]** は削除しないでください。

ステップ 8 vCenter で **[cluster]** を再作成します。

- a) vCenter から、**[datacenter]** を右クリックします。**[New Cluster]** を選択します。

- b) 削除したクラスタと全く同じ名前を **[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、**[cluster]** 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、**[datacenter] > [cluster]** を右クリックします。**[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 <vCenter_IP>
--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 クラスタへのストレージクラスタの登録 \(79 ページ\)](#) を参照してください。

ノードコンポーネントの交換

ノードの一部のコンポーネントは交換可能です。ノードの稼動中に交換できるコンポーネントがあります。一部のコンポーネントを交換する場合に、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。一部のコンポーネントは、TAC の支援がなければ交換することができません。次に、ノードで交換可能なコンポーネントの一般的なリストを示します。



(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。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本ガイドを参照し、ハードウェアを中心とするタスク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。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 ドライバ。前面ベイ 1

ストレージクラスタのタスクについては本ガイドを参照し、ハードウェアを中心とするタスク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。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。

• 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

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ハードウェア インストール ガイド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。

• 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なコンポーネントではありません。TAC に問い合わせるサポートを受けてください。

• DIMMS

• CPU およびヒートシンク

• 内蔵 SD カード

- 内蔵 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)
- GPU (Graphic Processing Unit)

ノードの取り外し

ノードメンテナンスタスクによっては、クラスタがオンラインかオフラインかに関係なく、ノードを取り外すことができます。ノードを取り外す前に準備手順が完了していることを確認してください。



- (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、元のクラスタや別のクラスタで再利用しないでください。

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、ノードの交換ワークフローに影響しません。

表 3: ノードの取り外しワークフロー

クラスタ サイズ	取り外すノード	ワークフロー
3 ノード クラスタ	1 つ以上	ワークフローには TAC の支援が必要です。

クラスタ サイズ	取り外すノード	ワークフロー
4 ノード クラスタ	1	<ol style="list-style-type: none"> 1. クラスタは正常です。 2. Cisco HX メンテナンス モードで影響を受けたノード。 3. クラスタをシャットダウンします (クラスタをオフラインにします)。 <code>stcli cluster shutdown</code> コマンドを使用します。 4. ノードを取り外します。 <code>stcli node remove</code> コマンドを使用します。 5. クラスタを再起動します。 <code>stcli cluster start</code> コマンドを使用します。
4 ノード クラスタ	2 つ以上	ワークフローには TAC の支援が必要です。
5 ノード クラスタ	1	<ol style="list-style-type: none"> 1. クラスタは正常です。 2. Cisco HX メンテナンス モードで影響を受けたノード。 3. クラスタはオンラインのままです。 4. ノードを取り外します。 <code>stcli node remove</code> コマンドを使用します。
5 ノード クラスタ	2	<ol style="list-style-type: none"> 1. クラスタは正常です。 2. Cisco HX メンテナンス モードで影響を受けたノード。 3. クラスタをシャットダウンします (クラスタをオフラインにします)。 <code>stcli cluster shutdown</code> コマンドを使用します。 4. ノードを取り外します。 <code>stcli node remove</code> コマンドを使用します。 両方のノードを指定します。 5. クラスタを再起動します。 <code>stcli cluster start</code> コマンドを使用します。
5 ノード クラスタ	3 つ以上	ワークフローには TAC の支援が必要です。

ノード削除の準備

ストレージクラスタからノードを削除する前に、クラスタがオンラインまたはオフラインのいずれであっても、次の手順を実行します。



(注) すべての3ノードクラスタで、ノードの準備、削除、交換のサポートを TAC に依頼してください。

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 ストレージクラスタを再調整します。

これにより、ノードに関連付けられたすべてのデータストアが削除されることが保証されます。

rebalance コマンドは、使用可能なストレージの変更に応じて保存データの配布を再調整し、ストレージクラスタの正常性を復元するために使用されます。ストレージクラスタ内のノードを追加または削除する場合、stcli rebalance コマンドを使用して、ストレージクラスタの再調整を手動で開始できます。

(注) 再調整は、障害の発生しているノードやディスクで使用されているディスクのキャパシティによって、時間がかかる場合があります。

- a) ストレージクラスタ内のコントローラ VM にログインします。
- b) 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。

```
# stcli rebalance start --force
```

ステップ5 削除するノードを Cisco HX メンテナンス モードにします。操作方法 (vSphere GUI またはコントローラ VM コマンドライン (CLI)) を選択します。

GUI

- a) vSphere Web クライアントから、[Home] > [Hosts and Clusters] > [Hosts] > [host] の順に選択します。

- b) 各ホストを右クリックし、リストを下にスクロールし、**[Cisco HX Maintenance Mode] > [Enter HX Maintenance Mode]** の順に選択します。

[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、**[Cisco HX Maintenance Mode]** を選択します。

CLI

- a) ESX ホストで、root 権限を持つユーザとしてコントローラ VM にログインします。
b) ノードを識別します。

```
# stcli node info

stNodes:
-----
type: node
id: 689324b2-b30c-c440-a08e-5b37c7e0eefe
name: 192.168.92.144
-----
type: node
id: 9314ac70-77aa-4345-8f35-7854f71a0d0c
name: 192.168.92.142
-----
type: node
id: 9e6ba2e3-4bb6-214c-8723-019fa483a308
name: 192.168.92.141
-----
type: node
id: 575ace48-1513-0b4f-bfe1-e6abd5ff6895
name: 192.168.92.143
-----
```

[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。

- 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)

ステップ 6 コマンド シェルを開き、ストレージコントローラ VM にログインします。たとえば ssh を使用します。

```
# ssh root@controller_vm_ip
```

プロンプトでパスワード (Cisco123) を入力します。

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の状態に応じてオンラインまたはオフラインの方式を選択します。結果が [Managing Nodes] に表示されます。

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。コンバージド ノードまたはコンピューティング ノードを削除する場合も同じ手順に従います。

ストレージ クラスタがオンライン中にそのクラスタからノードを取り外す場合は、クラスタがオフライン中にノードを取り外す場合と要件が若干異なります。



(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。

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、ノードの交換ワークフローに影響しません。

クラスタ内のノードの数	方式
3 ノード クラスタ	ノードを取り外して交換するには、TAC を参照してください。
4 ノード クラスタ	クラスタをオフラインにする必要があります。 オフラインストレージクラスタからのノードの削除 (129 ページ) を参照してください。
5 ノード クラスタ、2 ノードを取り外す	クラスタをオフラインにする必要があります。 オフラインストレージクラスタからのノードの削除 (129 ページ) を参照してください。
5 ノード クラスタ、正常なクラスタから1 ノードを取り外す	クラスタをオンラインにすることができます。ここに記載されている手順を続行します。



(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。

ステップ 1 「メンテナンス操作の準備」 および 「ノード削除の準備」 の手順を実行します。次の内容が含まれていません。

a) クラスタが正常であることを確認します。

3 ノード クラスタの場合、3 ノード クラスタでノード障害が発生すると、クラスタが正常ではなくなるため、TAC にご連絡ください。

b) DRS が有効であることを確認するか、またはノードから VM を手動で移動します。

c) ストレージ クラスタを再調整します。

- d) 削除するノードを HX メンテナンス モードにします。
- e) 削除しないノードのコントローラ VM にログインします。

ステップ 2 ストレージクラスタを再調整します。

- a) `rebalance` コマンドを実行します。

```
# stcli rebalance start -f
```

- b) 再調整が完了するまで待ち、完了したことを確認します。

ステップ 3 `stcli node remove` コマンドを使用して該当するノードを削除します。

```
stcli node remove [-h] [--id-1 ID1 | --ip-1 NAME1] [--id-2 ID2 | --ip-2 NAME2] [-f]
```

構文の説明	オプション	必須またはオプション	説明
	--id-1 ID1	セットのいずれかが必要。	ストレージクラスタ ノードの固有 ID 番号。ID は <code>stcli cluster info</code> コマンドで、 <code>stNode</code> のフィールド <code>id</code> に表示されます。
	--ip-1 NAME1	セットのいずれかが必要。	ストレージクラスタ ノードの IP アドレス。IP は <code>stcli cluster info</code> コマンドで、 <code>stNode</code> のフィールド <code>name</code> に表示されます。
	--id-2 ID2	オプション。	ストレージクラスタ ノードの固有 ID 番号。ID は <code>stcli cluster info</code> コマンドで、 <code>stNode</code> のフィールド <code>id</code> に表示されます。
	--ip-2 NAME2	オプション。	ストレージクラスタ ノードの IP アドレス。IP は <code>stcli cluster info</code> コマンドで、 <code>stNode</code> のフィールド <code>name</code> に表示されます。 --ip オプションは現在サポートされていません。
	-f, --force	オプション。	ストレージクラスタ ノードを強制的に削除します。

次に例を示します。

```
# stcli node remove --name-1 esx.SVHOST144A.complab
```

Response

```
Successfully removed node: EntityRef(type=3, id='', name='esx.SVHOST144A.complab')
```

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。

このコマンドでは次の操作は実行されません。

- vCenter からのノードの削除。ノードは vCenter に残ります。

- 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）の削除。

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 [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、HX 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 4 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 info
```

- 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。

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。

- (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。コンバージドノードまたはコンピューティングノードを削除する場合も同じ手順に従います。



- (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。

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、ノードの交換ワークフローに影響しません。

クラスタ内のノードの数	方式
3 ノードクラスタ	ノードを取り外して交換するには、TAC を参照してください。
4 ノードクラスタ	クラスタをオフラインにする必要があります。
5 ノードクラスタ、2 ノードを取り外す	クラスタをオフラインにする必要があります。

クラスタ内のノードの数	方式
5ノードクラスタ、正常なクラスタから1ノードを取り外す	クラスタをオンラインにすることができます。 オンラインストレージクラスタからのノードの削除 (127 ページ) を参照してください。



(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。

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。

ステップ1 「メンテナンス操作の準備」および「ノード削除の準備」の手順を実行します。次の内容が含まれていません。

a) クラスタが正常であることを確認します。

3ノードクラスタの場合、3ノードクラスタでノード障害が発生すると、クラスタが正常ではなくなるため、TACにご連絡ください。

b) DRS が有効であることを確認するか、またはノードから VM を手動で移動します。

c) ストレージクラスタを再調整します。

d) 削除するノードを HX メンテナンス モードにします。

e) 削除しないノードのコントローラ VM にログインします。

ステップ2 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。

このステップは、次の条件のいずれかにのみ必要です。

- クラスタは5ノード未満である。

- 5ノードクラスタから2ノードを取り外す。

a) すべての HX データストアのすべての常駐 VM をグレースフル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 をグレースフルシャットダウンし、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 node remove` コマンドを使用して該当するノードを削除します。

たとえば、削除するノードは IP アドレスまたはドメイン名によって指定できます。

```
# stcli node remove --ip-1 10.10.2.4 --ip-2 10.10.2.6
```

または

```
# stcli node remove --name-1 esx.SVHOST144A.complab --name-2 esx.SVHOST144B.complab.lab
```

(注) 5つ以上のノードからなるストレージクラスタで2番目のノードを削除する場合は、2番目のIPアドレスを入力します。

Response

```
Successfully removed node: EntityRef(type=3, id='', name='10.10.2.4' name='10.10.2.6')
```

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。

このコマンドでは次の操作は実行されません。

- vCenterからのノードの削除。ノードはvCenterに残ります。
- 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）の削除。

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[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の正常性は引き続き[Average]です。

ストレージクラスタ内にノードがないため、HX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4 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 info
```

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。

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。

(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。

ステップ6 クラスタを再起動します。

```
# stcli cluster start
```

ノードの交換

ノードの交換では、障害が発生したノードを取り外してから、Expand Clusterを使用して交換用ノードを追加します。ノードの交換は、要件が満たされていれば、HXストレージクラスタ

がオンライン中またはオフライン中に実行できます。ストレージクラスタ内のコンバインドノードを交換する際は、常に TAC によるサポートが必要です。



(注) ストレージクラスタ内のノードを交換する場合は、TAC と一緒に作業することを強くお勧めします。

TAC の支援を得てコンバインドノードを交換するための条件。

• 3 ノード クラスタ

3 ノード クラスタでは TAC の支援を得てノードを交換する必要があります。クラスタメンテナンス中にノードを交換します。

• 4 ノード クラスタ

- ストレージクラスタが異常です。
- ノードが削除された場合、ストレージクラスタは正常ではなくなります。
- 2 つ以上のノードで障害が発生しています。
- 交換したノードのディスクは再利用されます。

ノードがストレージクラスタに追加されると、HX Data Platform は各ディスク UUID をノード UUID に関連付けます。この関連付けは、ストレージクラスタの存続期間中にわたって変更されません。ディスクを異なる UUID のノードに再割り当てすることはできません。TAC と共同で、古いノードの UUID を新しいノードに割り当て、ディスク UUID とノード UUID の関連付けを維持します。

- ノードの交換中にストレージクラスタをオンラインのままにします。

• 5 ノード クラスタ

- ストレージクラスタが異常です。
- ノードが削除された場合、ストレージクラスタは正常ではなくなります。
- 3 つ以上のノードで障害が発生しています。
- 交換したノードのディスクは再利用されます。

ノードがストレージクラスタに追加されると、HX Data Platform は各ディスク UUID をノード UUID に関連付けます。この関連付けは、ストレージクラスタの存続期間中にわたって変更されません。ディスクを異なる UUID のノードに再割り当てすることはできません。TAC と共同で、古いノードの UUID を新しいノードに割り当て、ディスク UUID とノード UUID の関連付けを維持します。

- 2 ノードの交換中にストレージクラスタをオンラインのままにします。
- ストレージクラスタをオンラインのままにし、クラスタは最初から 3 または 4 ノードでした。

ストレージクラスタの初期構成が3または4ノードだった場合は、ノードを追加して全部で5ノードにすることで、3+2 クラスタまたは 4+1 クラスタを維持します。ノードの交換中にクラスタをオンラインのままにするには、TAC の支援が必要です。

ノードの交換ワークフロー

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、ノードの交換ワークフローに影響しません。

クラスタ サイズ	交換するノード	ワークフロー
3 ノード クラスタ	1 つ以上	ワークフローには TAC の支援が必要です。
4 ノード クラスタ	1	<ol style="list-style-type: none"> 1. クラスタは正常です。 2. Cisco HX メンテナンス モードで影響を受けたノード。 3. クラスタをシャットダウンします (クラスタをオフラインにします)。 stcli cluster shutdown コマンドを使用します。 4. ノードを取り外します。 stcli node remove コマンドを使用します。 5. クラスタを再起動します。 stcli cluster start コマンドを使用します。 6. クラスタがオンラインになって正常になるまで待機します。 7. [HX Installer] > [Expand Cluster] を使用して、交換用ノードを追加します。 <p>(注) 取り外したノード、そのクラスタ内のディスク、または他のクラスタ内のディスクは再利用しないでください。</p>
4 ノード クラスタ	2 つ以上	ワークフローには TAC の支援が必要です。

クラスタ サイズ	交換するノード	ワークフロー
5 ノード クラスタ	1	<ol style="list-style-type: none"> 1. クラスタは正常です。 2. Cisco HX メンテナンス モードで影響を受けたノード。 3. クラスタはオンラインのままです。 4. ノードを取り外します。 stcli node remove コマンドを使用します。 5. クラスタを再起動します。 stcli cluster start コマンドを使用します。 6. クラスタがオンラインになって正常になるまで待機します。 7. [HX Installer] > [Expand Cluster] を使用して、交換用ノードを追加します。 <p>(注) 取り外したノード、そのクラスタ内のディスク、または他のクラスタ内のディスクは再利用しないでください。</p>

クラスタ サイズ	交換するノード	ワークフロー
5 ノード クラスタ	2	<ol style="list-style-type: none"> 1. クラスタは正常です。 2. Cisco HX メンテナンス モードで影響を受けたノード。 3. クラスタをシャットダウンします（クラスタをオフラインにします）。 <code>stcli cluster shutdown</code> コマンドを使用します。 4. ノードを取り外します。 <code>stcli node remove</code> コマンドを使用します。 両方のノードを指定します。 5. クラスタを再起動します。 <code>stcli cluster start</code> コマンドを使用します。 6. クラスタがオンラインになって正常になるまで待機します。 7. [HX Installer] > [Expand Cluster] を使用して、交換用ノードを追加します。 <p>(注) 取り外したノード、そのクラスタ内のディスク、または他のクラスタ内のディスクは再利用しないでください。</p>
5 ノード クラスタ	3 つ以上	ワークフローには TAC の支援が必要です。

ノードの交換と障害発生ノードのディスクの廃棄。

ステップ 1 古いノードを削除します。該当するトピック内の手順に従います。

- オンラインストレージクラスタからのノードの削除

この方法は、HX クラスタが最初から 5 ノード以上で構成され、現在も 5 ノード以上である場合にのみ使用します。

- オフラインストレージクラスタからのノードの削除

この方法は、TAC の支援が要らないノード取り外しに使用します。

- (注) ノードとその関連ディスクを削除しても、HX Data Platform はディスクの UUID を記憶しています。ログとレポートの生成時に、ディスクが存在するが検出できないことを示すメッセージが出力されます。これらのメッセージは無視してください。

ステップ 2 HX Data Platform インストーラの拡張オプションを使用して新しいノードを追加します。『*Cisco HyperFlex Systems Getting Started Guide*』を参照してください。



第 10 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 \(137 ページ\)](#)
- [ストレージコントローラ VM の電源のオン/オフ \(137 ページ\)](#)

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、Cisco HX Distributed Data プラットフォームに重要な機能を提供します。ストレージコントローラ VM は、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インストールされます。ストレージコントローラ VM は、ストレージクラスタ上で `stcli` 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を備えています。

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、多くの場合、ストレージコントローラ VM の電源をオンまたはオフにするストレージコントローラ操作を介して、ストレージコントローラ VM にも適用されます。

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。

- vSphere Web クライアントにログインします。
- VM を探します。
ナビゲータから、**[vCenter 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。
- 右クリックメニューまたは **[Actions]** メニューから、**[Power] > [Power On]** または **[Power] > [Power Off]** 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。

- VM の ESX ホストのコマンドラインにログインします。
- VM `vmid` を探します。

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 の電源をオンにするには、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 の電源をオフにするには、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.off 1
```



第 11 章

ReadyClone の管理

- [HX Data Platform ReadyClone の概要 \(139 ページ\)](#)
- [HX Data Platform ReadyClone の利点 \(140 ページ\)](#)
- [サポート対象のベース VM \(140 ページ\)](#)
- [ReadyClone の要件 \(141 ページ\)](#)
- [ReadyClone のベストプラクティス \(141 ページ\)](#)
- [HX 接続を使用して ReadyClone を作成する \(141 ページ\)](#)
- [HX データプラットフォームプラグインを使用した ReadyClone の作成 \(143 ページ\)](#)
- [HX Data Platform ReadyClone のカスタマイズの準備 \(145 ページ\)](#)
- [カスタマイズ仕様を使用した ReadyClone の設定 \(146 ページ\)](#)
- [仮想マシン ネットワーキングの管理 \(147 ページ\)](#)

HX Data Platform ReadyClone の概要

HX Data Platform ReadyClone は、ホスト VM からの複数のクローン VM の迅速な作成と、カスタマイズを可能とする草分け的なストレージ技術です。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。

ReadyClone (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、ReadyClone は別のゲスト VM となります。

ReadyClone に対して変更を行っても、ホスト VM には影響しません。ReadyClone 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。ReadyClone を実行すると、単一のインストールおよびコンフィギュレーションプロセスで、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 ReadyClone の利点

HX Data Platform ReadyClone 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、ReadyClone 機能を使用して複数の VM のクローンを作成します。
- **ラピッドクローニング**：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 ReadyClone 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 の一括カスタマイズ**：HX Data Platform カスタマイゼーション仕様を使用して、IP アドレス、ホスト名、ホスト VM からクローニングした複数のゲスト VM 用の VM 名などのパラメータを瞬時に設定します。
- **複数の手順をワンクリック プロセスへと自動化**：HX Data Platform ReadyClone 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**：ReadyClone 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、ReadyClone 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。

サポート対象のベース VM

HX Data Platform は次をサポートします。

- HX Data Platform データストア上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
- 1 つのベース VM から最大 2048 の ReadyClone
- 一度に 1 つのバッチで作成された最大 256 の ReadyClone

HX Data Platform では次のものはサポートされません。

- Win2008 および Win2012 サーバゲストを使用している電源の入ったベース VM
- 30 未満のスナップショットを使用している電源の入ったベース VM
- redo ログのスナップショットを使用している電源の入ったベース VM

ReadyClone の要件

- VM が、HX Data Platform ストレージクラスタ内にある必要があります。HX Data Platform に属さない VM はサポートされません。
- VM が、HX Data Platform のデータストア、VM フォルダ、およびリソース プールに存在する必要があります。

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 ReadyClone 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。ReadyClone 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。
- SSH は、ストレージクラスタ内のすべてのノード上の ESX で有効にする必要があります。
- ReadyClone 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。

ReadyClone 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。
- バッチ全体に適用するプロパティが、カスタマイズ仕様であることを確認します。
- HX Data Platform ReadyClone 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。
- VM のゲスト名など、クローンごとに区別するための設定を、パターンを使用して抽出します。
- 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、クローニングする前にそれらのアドレスを確認します。
- 特定の時刻に、1 ~ 256 のバッチを作成できます。HX Data Platform プラグインを使用して、その確認ができます。
- HX Data Platform プラグインのマスター タスクの更新情報の誤表示や障害の発生要因につながる恐れがあるため、（電源オン、または電源オフ時に）同じ VM 上で、複数の一括クローニングが同時に生成されないようにしてください。

HX 接続を使用して Readyclone を作成する

HX データ プラットフォーム Readyclone 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。

ステップ 1 管理者として HX Connect にログインします。

ステップ 2 [仮想マシン] ページから、[仮想マシン] を選択し、[Readyclone] をクリックします。

ステップ 3 [ReadyClone] ダイアログ フィールドに記入します。

UI 要素	基本情報
[クローン数] フィールド	作成する ReadyClones の数を入力します。特定の時刻に 1 ~ 256 のクローンのバッチを作成できます。
[カスタマイズ仕様] フィールド	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 [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、選択したホスト仮想マシンがゲスト仮想マシン向けに 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。
[リソース プール] フィールド	オプション フィールド。 HX Storage Cluster 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] フィールド	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 ReadyClone の名前に追加されます。
[番号のクローンの開始] フィールド	クローンを開始するクローン番号を入力します。 各 ReadyClone 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。
[クローン番号を増加する手段] フィールド	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 ReadyClones 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 から開始されます。この値は、任意の番号に変更できます。
[ゲスト名に同じ名前を使用する] チェックボックス	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仮想マシン名として使用されます。 このチェック ボックスをオフにすると、テキスト ボックスが有効化されます。ゲストのホスト仮想マシンに使用する名前を入力します。

UI 要素	基本情報
[プレビュー] フィールド	必須フィールドを入力したら、HX Data Platform により提案された Readyclone 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。
[クローン後に VM を起動] チェックボックス	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 [Clone] をクリックします。

HX Data Platform により、名前を付けロケーションを指定した状態で複数の Readyclone 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 ReadyClone の作成

VMware のクローニング操作を使用すると、VM から単一のクローンのみを作成できます。この操作は手動で、VM からの複数クローンのバッチ処理よりも遅くなります。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 ReadyClone 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。

ステップ 1 vSphere Web クライアントナビゲータから、[vCenter 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 ストレージクラスタ VM を選択し、[Actions] メニューを開きます。[VM information] ポートレット内で、VM を右クリックするか [Actions] 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] > [ReadyClones] の順に選択して、[ReadyClones] ダイアログボックスを表示します。

ステップ 4 [ReadyClones] ダイアログボックスで次の情報を指定します。

Control	説明
Number of clones	作成するクローンの数を入力します。特定の時刻に 1 ~ 256 のクローンのバッチを作成できます。

Control	説明
Customization Specification	<p>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 [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）。</p> <p>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。</p>
VM name prefix	ゲスト VM 名のプレフィックスを入力します。
Starting clone number	開始クローンのクローン番号を入力します。
Use same name for 'Guest Name'	<p>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。このチェック 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。</p> <p>システムには、ダイアログ ボックス内の [Guest Name] 列にある、ゲスト VM の名前が表示されます。</p> <p>[Customization Specification] 自体にも、同様のオプションがあります。この HX Data Platform ReadyClone 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。</p> <ul style="list-style-type: none"> • [Customization Specification] に静的ゲートウェイ、静的サブネット、または静的 IP アドレスに転換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名またはホスト名を設定します。 • [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。
Increment clone number by	ゲスト VM 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、VM クローン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 から開始されます。この値は、任意の番号に変更できます。
Power on VMs after cloning	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、ReadyClone 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。システムが次を表示します。

- 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 HXConnect に表示されます。これは、ReadyClone 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 ReadyClone のカスタマイズの準備

- VMware のドキュメンテーションに従って、カスタマイズの仕様を作成します。
以降の項で説明する Linux または Windows VM に固有のカスタマイズ設定を適用します。
- 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、使用しているネットワークに固有の情報を収集します。
- ベース VM が有効であることを確認します（切断されておらず、スナップショットや vMotion の実行中でもないことを確認）。
- 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てください。
- [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 クライアント内での Linux 向けカスタマイズ仕様の作成

[vSphere Web Client Guest Customization] ウィザードを使用して、仮想マシンのクローニングまたはテンプレートからの展開時に適用可能な仕様で、ゲスト オペレーティング システムの設定を保存します。

次の考慮事項を確認し、ウィザードを完了させます。

- HX Data Platform ReadyClone 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 ReadyClone 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 ReadyClone 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 ReadyClone 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、[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 クライアント内での Windows 向けカスタマイズ仕様の作成

[vSphere Web Client Guest Customization] ウィザードを使用して、仮想マシンのクローニングまたはテンプレートからの展開時に適用可能な仕様で、Windows のゲスト オペレーティング システムの設定を保存します。



(注) カスタマイズの後、デフォルトの管理者パスワードは、Windows Server 2008 用に保存されません。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リセット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 ReadyClone 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、[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 ReadyClone の設定

カスタマイズ仕様を使用して、スタティック IP アドレスを使用する場合に IP アドレスが新しい VM に適用されるようにします。

たとえば、Windows サーバの VM クローンを作成し、DHCP を使用した場合、ゲスト VM には自動的に新しい IP アドレスが割り当てられます。ただし、静的 IP アドレスを使用する場合は、IP アドレスはゲスト VM 内で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 ReadyClone を設定します。

ステップ 1 有効な DNS 名を取得し、有効な IP アドレスに転換されることを確認します。

たとえば、100 個の Windows VM のゲスト名を userwinvm1 から userwinvm100 にした状態でプロビジョニングするには、userwinvm1 から userwinvm100 に有効な IP アドレスがあることを確認します。

ステップ 2 クローン元となる VM に、ゲスト VM ツールをインストールします。

ステップ 3 ReadyClone 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、クローン元 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、すべてのクローン 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 ネットワーキングの管理

ストレージクラスタを変更したら、クラスタ内のノード上の仮想マシンのネットワークが正しく設定されていることを確認できます。完全な仮想マシンネットワーク情報については、UCS Manager のマニュアルを参照してください。

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。

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/3-1/b_UCSM_Network_Mgmt_Guide_3_1/b_UCSM_Network_Mgmt_Guide_3_1_chapter_0110.html で、『Cisco UCS Manager Network Management Guide』の「VLANs」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。

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/3-1/b_UCSM_Network_Mgmt_Guide_3_1/b_UCSM_Network_Mgmt_Guide_3_1_chapter_0111.html#d24564e315a1635 で、『Cisco UCS Manager Network Management Guide』の「Configuring vNIC Templates」のトピックを参照してください。

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。

次のリンクから、『VMware vSphere 6.0 Documentation』の「Add a Virtual Machine Port Group」のトピックを参照してください。 <http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-004E2D69-1EE8-453E-A287-E9597A80C7DD.html>



第 12 章

ネイティブスナップショットの管理

- [HX Data Platform ネイティブスナップショットの概要 \(149 ページ\)](#)
- [HX Data Platform ネイティブスナップショットの利点 \(150 ページ\)](#)
- [ネイティブスナップショットの考慮事項 \(151 ページ\)](#)
- [ネイティブスナップショットのベストプラクティス \(153 ページ\)](#)
- [SENTINEL スナップショットについて \(154 ページ\)](#)
- [ネイティブスナップショットのタイムゾーン \(155 ページ\)](#)
- [スナップショットの作成 \(156 ページ\)](#)
- [スナップショットのスケジューリングの概要 \(157 ページ\)](#)
- [スナップショットのスケジューリング \(158 ページ\)](#)
- [スケジュール済みスナップショットの頻度の設定 \(159 ページ\)](#)
- [スナップショットスケジュールの削除 \(159 ページ\)](#)
- [スナップショットの復元 \(160 ページ\)](#)
- [スナップショットの削除 \(161 ページ\)](#)

HX Data Platform ネイティブスナップショットの概要

HX Data Platform ネイティブスナップショットは、動作している 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 をネイティブスナップショットに戻すことができます。

HX Data Platform Plug-in を使用して、VM のネイティブスナップショットを取得します。HX Data Platform ネイティブスナップショットオプションには、ネイティブスナップショットの作成、任意のネイティブスナップショットへの復元、ネイティブスナップショットの削除が含まれます。タイミングオプションには、毎時、日次、週次があり、15 分単位で設定できます。

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。

VM が電源オン、オフ、またはサスペンド状態のときに、ネイティブスナップショットを取得できます。VMware スナップショットの追加情報については、次のリンクから VMware のナ

レッジベース『Understanding virtual machine snapshots in VMware ESXi and ESX (1015180)』の記載を参照してください。

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

HX Data Platform ネイティブスナップショットの利点

HX Data Platform ネイティブスナップショットは、ネイティブ技術を使用します。ネイティブスナップショットには、次のような利点があります。

- **登録済みVMの復元。** VMが登録されている場合、電源のオン/オフに関係なく、ネイティブスナップショット（VMスナップショットと同一）を使用して、スナップショットが作成された時点の状態を復元できます。
- **高性能。** HX Data Platform 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 I/O に依存しない。** HX Data Platform ネイティブスナップショットの作成時間は、VMでのI/Oに依存しません。
- **VMのパフォーマンス。** HX Data Platform 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 コンシステント。** HX Data Platform の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 コンシステントである。I/O クラッシュ整合は、書き込み操作の正しい順序を維持するように定義されます。これにより、アプリケーションはクラッシュから正しく再起動できます。
- **アプリケーション コンシステント。** HX Data Platform CLI で `stcli vm snapshot` コマンドの `quiesce` オプションを選択して HX Data Platform ネイティブスナップショットをアプリケーションコンシステントにすることができます。ゲストVM内のアプリケーションは、ホストVMで実行されているのと同様に透過的に実行されます。詳細については、『Cisco HX Data Platform Command Line Interface Reference CLI Reference』を参照してください。

ファイルシステムの休止は、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です。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、ディスクまたはその他の高レベルのアプリケーション固有のタスクにバッファをフラッシュするなどのアクションが含まれる場合があります。

システムに休止エラーが表示された場合は、次のリンクから、VMwareのナレッジベース『*Troubleshooting Volume Shadow Copy (VSS) quiesce related issues (1007696)*』の記載を参照してください。

http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1007696

- **ノード障害に強いスケジュール済みスナップショット。** スケジュール済みスナップショットは、ノードのシャットダウンが必要な管理操作（HM 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）に対して耐障害性があります。

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。

- **統一されたインターフェイス。** VMware snapshot manager™ を使用して、HX Data Platform プラグインを介して作成されたネイティブ スナップショットを管理できます。
- **個別にまたはグループで。** ネイティブ スナップショットは、VM レベル、VM フォルダレベル、またはリソース プール レベルで取得できます。
- **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、リソース プール、フォルダ、および VM レベルの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。** 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。
- **パラレル バッチ スナップショット。** パラレル バッチ スナップショットでは、リソース プールまたはフォルダで最大 255 の VM がサポートされます。
- **VDI 導入サポート。** HX のスケジュール済み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。
- **回復可能な VM。** スナップショットが失敗しても、VM は常に回復可能です。
- **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/アクセス可能なデータストアに対して機能します。

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

- **ネイティブ スナップショット：** HX Data Platform プラグインを使用して最初のネイティブ スナップショットを作成した後、vSphere Web クライアントでさらにスナップショットを作成する場合は、これらも同様にネイティブであると見なされます。ただし、HX Data Platform プラグインではなく vSphere Web クライアントを使用して最初のスナップショットを作成する場合は、vSphere Web クライアントのスナップショットは非ネイティブであると見なされます。
- **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、現在、31 です。この上限は、VMware で作成されたスナップショット、HX Data Platform の SENTINEL スナップショット、HX Data Platform のネイティブ スナップショットを含んだ合計になります。

詳細については、次のリンクから VMware のナレッジ ベース『*Committing snapshots in vSphere when more than 32 levels of snapshots are present fails with the error: Too many levels of redo logs (1004545)*』を参照してください。 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKc&externalId=1004545

- **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。

VM

- **削除されたVM**：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、関連するすべてのスナップショットも削除されます。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**：HX Data Platform データストアに存在しないVMでは、スナップショットは失敗します。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スナップショットにあてはまります。スナップショットを作成するには、VMはHX Data Platform ストレージクラスタ内のHX Data Platform データストアに存在する必要があります。
- **中断状態のVM**：最初のネイティブスナップショット（SENTINELスナップショット）を中断状態のVMから作成することはサポートされていません。

vCenter

- **準備ができているストレージクラスタ**：ネイティブ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、オンラインであるなど、正常な状態である必要があります。データストアにアクセス可能である必要があります。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。
- **vMotion**：vMotionは、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、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。

名前付け

- **名前の重複**：HX Data Platform vCenterで、VMやリソースプールの名前が重複しないようにしてください。そうしない場合、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。
- **名前に含まれる文字**：スナップショットを有効にするすべてのゲスト/ユーザーVM名に特殊文字、ドット（.）、ドル記号（\$）、またはアクセント（'）を使用しないでください。

ディスクとデータストア

- **VMデータストア**：ネイティブスナップショットを作成する前に、すべてのVM（VMDK）ディスクが同じデータストアにあることを確認します。これはHXスナップショットにすぐに適用され、またHXスケジュール済みスナップショットにも適用されます。

- **シック ディスク** : 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。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。
- **仮想ディスク タイプ** : VMware は、さまざまな仮想ディスク バックアップ 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。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が含まれている VM は、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。

制限事項

オブジェクト	最大数
スナップショット	ストレージ クラスタあたり 30 VMware の上限は 31 です。1 つのスナップショットが SENTINEL 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 8
VM	ホストあたり 1024
電源をオンにした VM	ホストあたり 100
VM あたりの vDisk 数	VM あたり 60

ネイティブ スナップショットのベスト プラクティス



重要 VM のスナップショットを初めて作成する場合は、常に HX Data Platform のスナップショット機能を使用します。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。

- 最初のスナップショットを作成するときには VMware のスナップショット機能を使用しないでください。

VMware のスナップショットは redo ログ技術を使用するため、オリジナルの VM でパフォーマンスが低下する要因となる可能性があります。このパフォーマンスは、追加されたそれぞれのスナップショットでさらに低下します。

ネイティブ形式のスナップショットは、最初の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。

redo ログスナップショットを取る場合は、redo ログスナップショットを保存する VMware 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。

- 最初の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 SENTINEL は、追加スナップショット向けの領域を使用します。

たとえば、既存の VM があって新しく 2 つの VMDK を追加する場合、次のスナップショットのスケジュールで新しい SENTINEL が 1 つ作成されます。スナップショットスケジュールの保持数を確認して、十分なスナップショットスロットが使用可能であることを確認してください。1 つは新しい SENTINEL 向けで、1 つはスナップショット向けです。

- 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、スナップショットを同時にスケジュールします。
 - 単一のリソースプールまたは VM フォルダではなく、VM グループに複数のリソースプールまたは VM フォルダを使用します。そして、グループごとにスナップショットのスケジュールをずらします。

たとえば、`resourcePool1` のスナップショットスケジュールを 00 分、`resourcePool2` のスナップショットスケジュールを 15 分、`resourcePool3` のスナップショットスケジュールを 30 分にスケジュールします。
- 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 のネイティブスナップショットを作成しないでください。これは、VMware KB 「VMware VirtualCenter Server service fails due to a quiesced snapshot operation on the vCenter Server database virtual machine (2003674)」に関連しています。 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003674

SENTINEL スナップショットについて

[Snapshot Now] または [Scheduled Snapshot] を介して VM のスナップショットを初めて作成する場合、HX Data Platform プラグインは SENTINEL スナップショットと呼ばれるベースのスナップショットを作成します。SENTINEL スナップショットにより、後続のスナップショットがすべてネイティブスナップショットであることが保証されます。

SENTINEL スナップショットは、復元された VM が、VMware の redo ログをベースにした仮想ディスクを保持することを防ぎます。redo ログをベースにした仮想ディスクが生じるのは、オリジナルのスナップショットが削除され、VM が 2 番目に古いスナップショットから復元される時です。

SENTINEL スナップショットは、復元可能なネイティブ スナップショットに追加されるものです。VMware ごとに使用可能なスナップショットには、合計で 31 という制限があり、SENTINEL スナップショットは、そのうちの 1 つを使用します。

SENTINEL スナップショットの使用

- SENTINEL スナップショットは削除しないでください。
- VM を、SENTINEL スナップショットに復元しないでください。

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の内容と表示に関するオブジェクトが 3 つあります。

- vSphere と vCenter は UTC 時間を使用します。
- vSphere Web クライアントはブラウザのタイムゾーンを使用します。
- HX Data Platform プラグイン、ストレージクラスタ、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。これはストレージクラスタ全体に適用されます。これらに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ストレージコントローラ VM の時刻が使用されます。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。

スケジュールの作成時に、スケジュール時刻が UTC に変換されます。HX Data Platform プラグインでスケジュールを表示すると、コントローラ VM の時刻が表示されます。作成されたスナップショットを vCenter イベント ログで表示すると、UTC 時刻が表示されます。

各オブジェクトに複数のタイムゾーンを適用することが可能であるため、HX Data Platform プラグインと vCenter ログに表示されるイベントメッセージとスケジュールが同期していないように見えることがあります。ただし、これは各表示オプションに割り当てられているタイムゾーンによる表面上の結果に過ぎません。同一タイムゾーンに変換すると、同一時刻に変換されます。たとえば、5:30pm PST、8:30PM EST、1:30AM UTC はすべて同じ時刻です。

[vSphere Scheduled Task] タブの場合、HX Data Platform 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 のスケジュールされたタスクのリスト。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 Data Platform

Schedule Snapshot] 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。

vSphere のタスク完了リスト。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] ウィンドウでは、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に完了したというステータスを表示することがあります。このメッセージは、vSphere がスナップショットのシーケンスの完了を確認したことを示しています。

指定された時間に、vSphere はスナップショットを作成する必要があるか、終了時間外であるかを調べ、スナップショットが不要であることを確認した上で、より大きなタスク（毎時間の一連のスナップショットの取得）が完了したことを示すステータス メッセージをポストします。

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。

```
$ stcli 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。

```
$ stcli services timezone set --timezone timezone_code
```

タイムゾーンのコードに関する詳細については、

https://en.wikipedia.org/wiki/List_of_tz_database_time_zones などからタイムゾーンのリファレンスを参照してください。

スナップショットの作成

始める前に

HX ストレージクラスタ内の VM に関する redo ログ スナップショットを取る場合は、redo ログ スナップショットを保存する ESXi ホストの設定を編集します。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 Data Platform 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。

1. ESXi ホストのコマンドラインにログインします。
2. ファイル /etc/vmware/config を探して編集用に開きます。
3. snapshot.asyncConsolidate パラメータを TRUE に設定します。

```
snapshot.asyncConsolidate="TRUE"
```

ステップ 1 vSphere Web クライアントナビゲータから、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 Inventory Lists] > [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、[Actions] メニューを開きます。[VM information] ポートレット内で、VM を右クリックするか [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] > [Snapshot Now] を選択して、[Snapshot] ダイアログボックスを表示します。

ステップ 4 [snapshot] ダイアログボックスにスナップショットの名前を入力します。

ステップ 5 スナップショットの説明を入力します。

ステップ 6 [OK] をクリックして設定内容を確定します。

[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

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) に適用します。



(注) vCenter クラスタを再登録すると、HX Data Platform 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、スナップショットスケジュールを再設定します。

スナップショットをスケジュールして、バックアップ要件を調整できます。たとえば、重要なデータについてはより頻繁にスナップショットを保持できます。障害発生時には、直近のスナップショットの復元か、カスタムのリアルタイムスナップショットを作成できます。重要度の低いデータに関しては、頻繁なスナップショットの作成やバックアップコピーの保持は必要ありません。

スナップショットのスケジューリングで、バックアップに要するコストを制御できます。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 分単位です。

たとえば、次の設定の場合、スナップショットは毎日取得されます。

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、午後 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

これらのスナップショットは毎日取得されます。

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

最後のスナップショットの終了時間が 00 分より前になるように注意してください。

24 を超える単位でスナップショットをスケジュールするには、開始時間を設定し、その後終了時間を 1 時間前に設定します。たとえば、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、スナップショットを午後 4 時 14 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 時間のサイクルで再起動します。注：VM ごとの最大スナップショット数は 32 です。そのため、取得可能な時間単位のスナップショットは最大 32 時間です。

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、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。

スナップショットのスケジューリング

ステップ 1 vSphere Web クライアント ナビゲータ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 Inventory Lists] > [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 [Actions] メニューをクリックします。

ステップ 3 [Actions] メニューから [Cisco HX Data Platform] > [Schedule Snapshot] を選択し、[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。

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開きます。

ステップ 1 [Schedule Snapshot] ダイアログボックスで [Enable Hourly Snapshot]、[Enable Daily Snapshot]、または [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 [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、[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。時間で、[Start] 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 ([Days]) を指定します。

ステップ 5 [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。

スナップショット スケジュールの削除

ステップ 1 vSphere Web クライアント ナビゲータ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 Inventory Lists] > [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] 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 [Actions] メニューをクリックします。
- ステップ 3** [Actions] メニューから **[Cisco HX Data Platform] > [Schedule Snapshot]** を選択し、[Schedule Snapshot] ダイアログ ボックスを表示します。
- ステップ 4** 今後不要なスケジュール 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などがあります）、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。vCenter のタブ、[Manage] > [Scheduled Tasks] をクリックします。これで、以前のスナップショット スケジュールが表示されなくなります。

スナップショットの復元

スナップショットを復元すると、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。スナップショットの復元は、一度に 1 つの VM で実行します。これはリソース プール レベルまたは VM フォルダでは実行されません。スナップショットの復元は、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。

- ステップ 1** vSphere Web クライアント ナビゲータのホームページから、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 Inventory Lists] > [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 を選択し、[Actions] メニューを開きます。[VM information] ポートレット内で、VM を右クリックするか [Actions] メニューをクリックします。
- ステップ 3** [Snapshots] > [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** [Revert to] > [Yes] > [Close] の順にクリックします。
復元された 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元した VM がすでに電源オンになっていることがあります。
- ステップ 6** 復元した VM を選択し、電源をオンにします。

スナップショットの削除

スナップショットの削除は、HX Data Platform 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。

ステップ 1 vSphere Web クライアント ナビゲータから、[VMs and Templates] > [vcenter_server] > [Snapshots] > [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 スナップショットを選択し、[Delete] をクリックします。

(注) [Delete All] オプションのみを使用して、SENTINEL スナップショットを削除します。SENTINEL スナップショットは個別に削除しないでください。



第 13 章

異なる HXDP バージョンで動作するクラスタの管理

- 異なる HXDP バージョンで動作するクラスタの管理 (163 ページ)
- シナリオ—HXDP 3.0 でサイト A および HXDP 2.6 でサイト B (163 ページ)
- シナリオ: HXDP 2.6 のサイト A および HXDP 3.0 のサイト B (165 ページ)
- 機能の制限 (167 ページ)

異なる HXDP バージョンで動作するクラスタの管理

シナリオ—HXDP 3.0 でサイト A および HXDP 2.6 でサイト B

次の用語および略称が使用されます。

- サイト A —ソース クラスタ
- サイト B —ターゲット クラスタ
- `dr_cleanup` ツール —Cisco TAC に連絡し、3.0 内部サポート パッケージで利用可能なこのツールを入手します。

前提条件

- アップグレードの前に、[回復済み] または [中止] 状態の VM またはグループがないことを確認します。
- VM が [中止] 状態の場合、VM またはグループをリカバリおよび保護を解除します。
- VM が [回復済み] 状態の場合、VM またはグループの保護を解除します。

ステップ	サイト A	サイト B	結果
1.	HXDP バージョン 2.6 または以降。	HXDP バージョン 2.6 または以降。	—
2.	HXDP 3.0 へアップグ レードします。	—	<ul style="list-style-type: none"> • 進行中のレプリケーションが続行されます。 • VM の計画済みの移行がサポートされていません。 • 詳細については、機能の制限 (167 ページ) を参照してください。
3.	サイト B をアップグ レードする前に、サイ ト A で障害が発生した 場合。	<ol style="list-style-type: none"> 1. コマンドを実行し ます。 <i>#stcli dp peer forget</i> 2. 必要な VM を回復 します。 3. dr_cleanup ツール を実行して、ディ ザスタリカバリ データベースから すべての VM 情報 を削除します。 	ワークロードは現在サ イト B で実行されてい ます。
4.	サイト A を復元しま す。 サイト A を復元したら 以下を行います。 <ol style="list-style-type: none"> 1. コマンドを実行し ます。 <i>#stcli dp peer forget</i> 2. dr_cleanup ツール を実行して、ディ ザスタリカバリ データベースから すべての VM 情報 を削除します。 	—	サイトがペアリングさ れていません。

ステップ	サイト A	サイト B	結果
5.	—	HXDP 3.0 へアップグレードします。	—
6.	サイトをペアリングします。	—	サイト A とサイト B が再度ペアリング可能になり、ワークロードを保護することができます。

シナリオ: HXDP 2.6 のサイト A および HXDP 3.0 のサイト B

次の用語および略称が使用されます。

- **サイト A** —ソース クラスタ
- **サイト B** —ターゲット クラスタ
- **dr_cleanup ツール** —Cisco TAC に連絡し、3.0 内部サポート パッケージで利用可能なこのツールを入手します。

前提条件

- アップグレードの前に、[回復済み] または [中止] 状態の VM またはグループがないことを確認します。
- VM が [中止] 状態の場合、VM またはグループをリカバリおよび保護を解除します。
- VM が [回復済み] 状態の場合、VM またはグループの保護を解除します。

ステップ	サイト A	サイト B	結果
1.	HXDP バージョン 2.6 または以降。	HXDP バージョン 2.6 または以降。	—

ステップ	サイト A	サイト B	結果
2.	—	HXDP 3.0 へアップグレードします。	<ul style="list-style-type: none"> • 進行中のレプリケーションが継続されます。 • VM の計画済みの移行がサポートされていません。 • 詳細については、機能の制限 (167 ページ) を参照してください。
3.	サイト A をアップグレードする前に、サイト A で障害が発生した場合。	<ol style="list-style-type: none"> 1. コマンドを実行します。 <i>#stcli dp peer forget</i> 2. 必要な VM を回復します。 3. Dr_cleanup ツールを実行して、ディザスタリカバリデータベースからすべての VM 情報を削除します。 	<ul style="list-style-type: none"> • すべてのリカバリオプションを使用できるわけではありません。 • 詳細については、機能の制限 (167 ページ) を参照してください。 • ワークロードは現在サイト B で実行されています。
4.	<p>サイト A を復元します。</p> <p>サイト A を復元したら以下を行います。</p> <ol style="list-style-type: none"> 1. コマンドを実行します。 <i>#stcli dp peer forget</i> 2. Dr_cleanup ツールを実行して、ディザスタリカバリデータベースからすべての VM 情報を削除します。 	—	サイトがペアリングされていません。

ステップ	サイト A	サイト B	結果
5.	サイト A を HXDP 3.0 にアップグレードします。	—	—
6.	—	サイトをペアリングします。	サイト A とサイト B が再度ペアリング可能になり、ワークロードを保護することができます。

機能の制限

リリース 3.0 の新しい機能は、ソースクラスタとターゲットクラスタの両方が同じ HXDP バージョンにある場合にのみサポートされます。ソースとターゲットの両方が同じバージョンであるため、アップグレードの際に時間がかかることがあります。次の機能の制限事項を確認してください。

- ターゲットクラスタが 2.6、ソースクラスタが 3.0 のピアサイトのバージョンが一致していない場合、VM の計画された移行はサポートされません。
- ソースがアップグレードされると、リリース 3.0 の新しい機能 (グループ VM の `movein` や `moveout` など) は、ピアがアップグレードされるまでソースクラスタ上でブロックされません。
- ターゲットクラスタのみがアップグレードされている場合、**HX Connect UI** では、[リカバリ (Recovery)] ダイアログボックスの [ネットワーク マッピング (Network Mapping)] オプションは、ソースクラスタをアップグレードするまで使用できません。



第 14 章

仮想マシンのディザスタリカバリの管理

- [データ保護の概要 \(169 ページ\)](#)
- [仮想マシンの保護の概要 \(174 ページ\)](#)
- [ディザスタリカバリの概要 \(190 ページ\)](#)
- [レプリケーションメンテナンスの概要 \(200 ページ\)](#)

データ保護の概要

HX Data Platform ディザスタリカバリ機能では、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、災害から仮想マシンを保護することができます。1つのクラスタで実行されている保護された仮想マシンをペアの他のクラスタにレプリケートします（その逆も同様です）。2つの対になったクラスタは通常、離れて配置され、各クラスタは他のクラスタで実行されている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 のレプリケーション 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ユーザにより使用され、リモートクラスタで VM が回復され実行されます。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仮想マシン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。

保護属性、その中でも重要なレプリケーション間隔（スケジュール）を割り当てることによって、各仮想マシン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、災害後に VM をリカバリする時に、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。レプリケーション間隔は 5 分から 24 時間までの範囲です。

保護グループと呼ばれる、新しいクラスタごとのグループ化構成は、保護された VM をグループ化し、同じ保護属性を割り当てます。VM は、属性がすでに定義されている保護グループに追加するだけで、保護することができます。

レプリケーションの設定には、HX Data Platform バージョン 2.5 またはそれ以降を実行している 2 つの既存のクラスタが必要です。どちらのクラスタも同じ HX Data Platform バージョンでなければなりません。この設定はオンラインで完了することができます。

まず、各クラスタがレプリケーションネットワーク用に設定されます。これには、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。プロセスの一環として、HX Connect は専用レプリケーションネットワーク用 VLAN を UCS マネージャから作成します。



- (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。

次に、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。

最後に、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状態をモニタすることができます。

災害後、クラスタ内のノード上で起動された `stcli` コマンドライン ツールを使用して、その VM のディザスタリカバリ サイトとして機能するクラスタで、保護された VM をリカバリして実行できます。

レプリケーションとリカバリの考慮事項

以下は、仮想マシンのレプリケーションの構成と仮想マシンのディザスタリカバリの実行時の考慮事項のリストです。

- **管理者**—モニタリングを除く、すべてのレプリケーションおよびリカバリタスクは、ローカルクラスタ上の管理者特権を持つユーザによってのみ実行できます。リモートクラスタに関連するタスクについては、指定したローカルおよびリモートの両方のユーザが管理者特権を持っている必要があります、それぞれのクラスタで vCenter SSO で構成されている必要があります。
- **記憶域**—リモートクラスタにレプリケーション スケジュールをサポートするのに十分な領域があることを確認します。保護された仮想マシンは、スケジュールされた間隔でリモートクラスタにレプリケート（コピー）されます。ストレージキャパシティの方法が適用されますが（重複排除、圧縮）、レプリケートされた各仮想マシンはストレージスペースを消費します。

リモートクラスタに十分なストレージ容量がないと、リモートクラスタの容量の使用率の最大値に到達する可能性があります。スペース不足エラーの場合は、[スペース不足エラーの処理 \(73 ページ\)](#) を参照してください。HX Cluster で利用できるスペースが適切に調整されるまでは、すべてのレプリケーションスケジュールは一時停止します。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。

- サポートされていないラスタレプリケーションの保護は2つのHX Cluster間で行われません。

- エッジクラスタ間、エッジクラスタへの、またはエッジクラスタからのレプリケーションはサポートされません。

- 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 Cluster内のノードを再起動しないでください。
- シンプロビジョニング—保護された仮想マシンは、元の保護され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。

保護グループの制限—

- 1つの保護グループに設定可能なVMの最大数は32です。
- ISOまたはフロッピーを使用するVMを保護グループに追加しないでください。

- HX以外データストア—非HXデータストア上のストレージを含むVMを保護している場合は、定期的にこのVMのレプリケートを試みますが失敗します。このVMの保護を解除するか、非HXストレージを取り外してください。

同様に、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。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の保護を解除して、保護を再適用します。

回復した仮想マシンの階層—

- 仮想マシンのレプリケーションの回復では、階層は保持されます。
- テストリカバリは、レプリケーション仮想マシンを統合し、レプリケーション階層を共通のクローニングされた基本ディスクに統合します。データは、すべてクローニングされた共通ディスクにあります。しかし、テストリカバリは新しいvm-uuidを持つクローンとしてのテストであるため、レプリケーション仮想マシンの階層構造は新たに開始されます。

- スナップショットメモリオプション—データ保護レプリケーションまたはリカバリのために仮想マシンを設定するときに、スナップショットメモリオプションを含まないようにしてください。

メモリスナップショットには、VMのメモリと電源状態が含まれています。このタイプのスナップショットは完了に時間がかかります。詳細については、VMware vSphere ベストプラクティスドキュメンテーションを参照してください。

- スナップショットのタイプ—HX Data Platform はさまざまな形式のスナップショット技術を使用します。各スナップショットは固有のユースケースを満たし、固有の特徴があります。これらに互換性はありません。

- ReadyClone は、標準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、ReadyCloneは別のゲストVMとなります。

- ネイティブ スナップショットは、動作している 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 をネイティブ スナップショットに戻すことができます。
- レプリケーションスナップショットは、VM レプリケーション保護の一部として作成されます。スケジュールされた時刻に、実行中の VM のレプリケーション スナップショットが作成されます。このスナップショットはリモートクラスタにレプリケート（コピー）されます。
- リカバリ テスト スナップショットは、リカバリ システムが動作していることを確認するために使用される一時的なスナップショットです。
- 回復された VM は、復元された VM で、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を復元することによって作成されます。

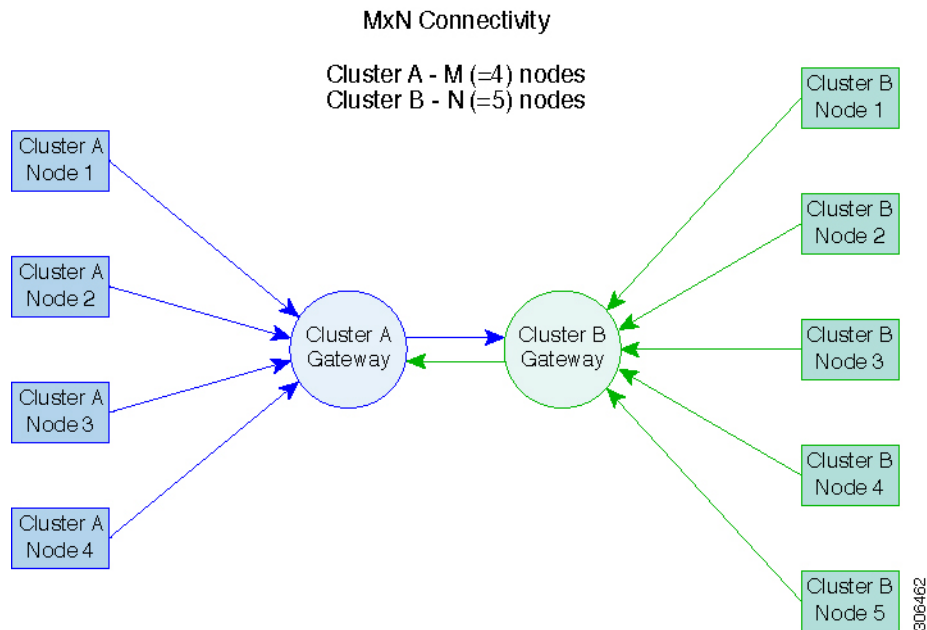
レプリケーション ネットワークとペアリングの考慮事項

データ保護のためにレプリケーションの使用を想定して、クラスタ間で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、このレプリケーションネットワークが作成されます。

以下は、レプリケーションネットワークとペアリングを設定するときに、考慮する事項のリストです。

- 効率的なレプリケーションをサポートするために、クラスタ間の $N \times M$ 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 ノードとの通信する必要があります。
- クラスタ間のレプリケーショントラフィックを有効にして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が可能になる必要があります。
- レプリケーショントラフィックは、クラスタとデータセンター内の他のトラフィックから隔離する必要があります。
- クラスタ間のトラフィックに対してこの隔離されたレプリケーションネットワークを作成するには、次の手順を実行します。
 - 各クラスタでレプリケーション ネットワークを作成します。
 - クラスタを関連付けるためにクラスタをペアリングし、クラスタ間の接続を $N \times M$ 属性を確立します。
- IP アドレス、サブネット、VLAN、およびゲートウェイは、各クラスタのレプリケーションネットワークに関連付けられます。両方のサイトで会社のファイアウォールとルータを設定し、クラスタとサイト間の通信を許可する必要があります。

クラスタ間 $M * N$ 接続性



データ保護の用語

フェールオーバー—ソース クラスタで障害が発生した場合の手動 VM リカバリ プロセスの一部。このコンテキストにおけるフェールオーバーは、ターゲットクラスタのレプリケーションスナップショットを稼働中の VM に変換することです。

レプリケーション間隔：レプリケーションスケジュールの設定の一部です。これは、保護された VM レプリケーションスナップショットが作成され、ターゲットクラスタにコピーされる頻度です。

ローカル クラスタ—VM クラスタ レプリケーションペアの 1 つ。現在 HX Connect を介して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します。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。保護されている VM:

- 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。
- レプリケーション スケジュールは個別または保護グループを通じて設定されます。

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したか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 クラスターVM レプリケーション クラスター ペアの1つ。リモート クラスターは、ローカル クラスターの保護された VM からレプリケーションの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 クラスター VM のレプリケーション スナップショットを格納するリモートのクラスター ロケーションを提供するためにまとめられた2つのクラスター。

レプリケーション ペアのクラスターは、リモートまたはローカル クラスター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ーは、レジデント VM を持つことが可能です。各クラスターは、そのレジデント VM に対してローカルです。各クラスターは、ペアリング済みのローカル クラスターに存在する VM に対してリモートです。

レプリケーション 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 のスナップショットの一種です。ローカル クラスターからリモート クラスターにコピーされます。

セカンダリ クラスターVM ディザスタ リカバリのターゲット クラスターの別の名前。

ソース クラスターVM リカバリ クラスター ペアの1つ。ソース クラスターは、保護された VM が存在する場所です。

ターゲット クラスターVM リカバリ クラスター ペアの1つ。ターゲット クラスターは、ソース クラスターの VM からレプリケーションのスナップショットを受信します。ターゲット クラスターは、ソース クラスターで障害が発生した場合、VM を回復するために使用されます。

仮想マシンの保護の概要

仮想マシンは、その保護属性を指定することによって保護できます。

- レプリケーションの間隔（レプリケーションの頻度と考えるもよい）
- 開始時刻（次の24時間以内で、仮想マシン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）
- 仮想マシンの停止でレプリケーション スナップショットを作成するかどうか。

保護グループを作成し、保護属性を割り当てることができます。仮想マシンを保護グループに追加することができます。そのグループを通じ、すべての仮想マシンに同じ保護属性が割り当てられます。

たとえば、3つの保護のクラス、金、銀、銅があるとします。各クラス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。

仮想マシンを保護するには、方法を選択します。



(注) 複数の仮想マシンを選択する場合、それらを保護グループに追加する必要があります。

- **個別**：1つの仮想マシンを選択して構成します。特定の仮想マシン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、個別に保護された仮想マシンにのみ影響を与えます。仮想マシンは、保護グループに含まれません。
- **既存の保護グループ**：1つ以上の仮想マシンを選択し、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。
- **新しい保護グループ**：2つ以上の仮想マシンを選択し、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。

データ保護のワークフロー

レプリケーションは、VMおよびそのデータを保護するためのプロセスです。次の手順を実行します。

- 2つのクラスタを設定します。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し、お互いがペアになるように設定します。
- ソースクラスタにレプリケーション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コピーする頻度（間隔）を設定するVMレプリケーションスケジュールを割り当てます。これは、個別のVMおよび保護グループのVMに設定されます。

レプリケーションワークフロー

1. HX Data Platform をインストールし2つのクラスタを作成します。
2. 各クラスタに少なくとも1つのデータストアを作成します。
3. HX Connect にログインします。
4. 複製ネットワークを作成する前に、IPアドレス、サブネットマスク、VLAN、および複製ネットワークに使用されるゲートウェイを確認します。複製ネットワークの作成後は、この新しい複製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. 複製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変更が完了したことを確認します。複製ペアを作成した後に、クラスタ間の接続を検証します。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。
6. クラスタレプリケーションネットワークを設定します。これを各クラスタで設定します。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。

サブネット、ゲートウェイ、IPアドレスの範囲、レプリケーションネットワーク専用の帯域幅制限を指定します。HX Data Platform は、UCS Manager を通じて両方のクラスタに対し、UCS Manager を通じて VLAN を構成します。

7. 2つのクラスタを接続するレプリケーションペアを作成します。
これは、一方のクラスタから実行されます。
8. オプションで、保護グループを作成します。
 - スケジュールを設定します。各保護グループに、1つのスケジュールがあります。
 - 異なる仮想マシン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。仮想マシンは、1つの保護グループにのみ属することができます。
9. 次のいずれかとして、保護する仮想マシンを選択します。
個別の仮想マシン
保護グループに割り当てられている仮想マシン
10. 保護の設定
 1. 1つまたは複数の仮想マシンを選択します。[Protect] をクリックします。
 2. [Protect Virtual Machine] 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つの仮想マシンを保護します。
 - 1つの仮想マシン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仮想マシンを保護します。
 - 新しい保護グループを通じて複数の仮想マシンを保護します。
新しい保護グループを作成し、スケジュールを設定します。

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。レプリケーションネットワークと少なくとも1つのデータストアは、レプリケーションペアを作成する前に構成しなければなりません。

クラスタ2とクラスタ1をペアリングすることにより、レプリケーション用に明示的に設定されたクラスタ1上のすべてのVMはクラスタ2にレプリケートでき、レプリケーション用に明示的に設定されたクラスタ2上のすべてのVMはクラスタ2にレプリケートできることが指定されます。

クラスタ1のデータストアAとクラスタ2のデータストアBをペアリングすることにより、レプリケーション用に明示的に設定されたクラスタ1上のすべてのVMでは、データストアA

にファイルがある場合、それらのファイルはクラスタ2のデータストアBにレプリケートされることが指定されます。同様に、レプリケーション用に明示的に設定されたクラスタ2上のすべてのVMでは、データストアBにファイルがある場合、それらのファイルはクラスタ1のデータストア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。1つのクラスタを2つ以上の他のクラスタとペアリングすることはできません。ペアになっているクラスタ上の1つのデータストアは、他のクラスタ上の1つのデータストアとしかペアリングできません。

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 Storage Clusterはローカルクラスタで、ペアの片方です。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 Storage Clusterを識別します。ストレージコンポーネントを確保するため、レプリケーションペアを各HX Storage Clusterのデータストアにマップします。レプリケーションペアが設定されたら、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。

リモートクラスタでもこの手順を繰り返します。

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。
- レプリケーションネットワークを構成します。

ステップ1 HX Connectから、管理者権限を持つユーザ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ます。[レプリケーション>レプリケーションペア>レプリケーションのペアを作成する]を選択します。

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 Storage Cluster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。

ステップ3 [Remote Connection]のIDを入力し、[Pair]をクリックします。

UI 要素	基本情報
[Management IP or FQDN] フィールド	リモート HX Storage Cluster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。例: 10.10.10.10。
[User Name] と [Password] フィールド	リモート HX Storage Clusterの vCenter シングルサインオンまたはクラスタ固有のクレデンシャルを入力します。入力されたユーザは、管理者特権を持つユーザである必要があります。

HX Data Platform はリモート HX Storage Cluster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。

ステップ 4 両方のクラスタから [Datastore Mapping] を設定し、[Next] をクリックします。

(注) 保護する仮想マシンは選択したデータストア上に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。

UI 要素	基本情報
[Local Datastore] 列	このクラスタ、ローカル HX Storage Cluster 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。
[Remote Datastore] 列	HX Storage Cluster間でデータストアをペアリングします。 必要な [Local Datastore] 行で、[Remote Datastore] 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。

ステップ 5 [Summary] の情報を確認し、[Map Datastores] をクリックします。

UI 要素	基本情報
[Datastore] フィールド	このローカル HX Storage Cluster で選択したデータストア。
[Target Datastore] フィールド	レプリケーションスナップショットのコピー先となるリモート HX Storage Cluster のデータストア。

データストアのマッピングが失敗した場合、[データストアのマップ] をスキップし、次のようにペアリング後にクラスタ間の接続性の検証に進みます。

- ローカルクラスタノードのいずれかからピアクラスタのゲートウェイに ping を実行します。クラスタが A と B を応答したと想定し、クラスタ A から B にこのチェックを行い、逆も行います。

クラスタ A でコマンド `$ ping -I eth2 <replication-gateway-of-cluster-B>` を実行します。

たとえば、`$ ping -I eth2 10.45.0.1`。

- Ping の確認に失敗した場合（100% パケット損失が表示されます）、ファイアウォールとクラスタ A と B に関連付けられているルータを確認します。レプリケーションサブネットのトラフィックと VLAN を許可するように設定する必要があります。

サイト A でファイアウォールを許可する必要があります。

- A のレプリケーションサブネットからの発信トラフィック
- B のレプリケーションサブネットからの受信トラフィック

サイト B のファイアウォールを許可する必要があります。

- B のレプリケーションサブネットからの発信トラフィック

- A のレプリケーション サブネットからの受信トラフィック

ルータを許可する必要があります。

- A からの発信トラフィックは B にルーティングされるレプリケーションのサブネット
 - A のレプリケーション サブネットからの発信トラフィックは A にルートされます。
- **Ping** チェックが成功したがデータストアのマッピングが機能しない場合は、MTU の設定を確認します。コマンド `$ ping -I eth2 M` は `-s <bytes> <replication ip="" of="" b's="" node="">` を実行します。クラスタ A からクラスタ B にこのチェックを実行し、逆も行います。

Example:

```
$ ping -I eth2 -M do -s 1500 10.4.247.11
```

テストが失敗した場合、成功するまで MTU 数を減らして再試行します。デフォルトの 1500 の MTU が機能しない場合は、Cisco TAC にお問い合わせください。

次のタスク

データストアのマッピングに成功すると、レプリケーションネットワーク経由でクラスタ間の接続を確認できます。新しいレプリケーションペアを追加します。

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) レプリケーション ペアで使用されるデータストアを変更すると、ローカルクラスタとリモートクラスタの両方のすべての仮想マシンから保護が解除されます。

ステップ 1 管理者として HX Connect にログインします。

ステップ 2 **[Replication] > [Replication Pairs] > [Edit]** を選択します。

ステップ 3 ローカルまたはリモートのデータストアを選択し、**[Finish]** をクリックします。

UI 要素	基本情報
[Local Datastore] 列	このクラスタ、ローカル HX Storage Cluster 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。

UI 要素	基本情報
[Remote Datastore] 列	<p>HX Storage Cluster間でデータストアをペアリングします。</p> <ol style="list-style-type: none"> 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。 <p>[Remote Datastore] 列のプルダウン メニューで、[Do not map this datastore] を選択します。</p> <ol style="list-style-type: none"> 必要な [Local Datastore] 行で、[Remote Datastore] 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。

レプリケーションペアの削除

ローカルおよびリモートのクラスタのレプリケーションペアを削除します。

[Replication] > [Replication Pairs] > [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。

当該のローカル HX Storage Clusterから次を実行します。リモート HX Storage Clusterにログインし、以下を実行します。

- すべての仮想マシンの保護を解除します。個別の保護を削除します。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。

ステップ 1 管理者として HX Connect 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。

- [Replication] > [Replication Pairs] > [Edit] を選択します。
- [Edit Replication Pair] ダイアログボックスの、[Remote Datastore] メニューから、[Do not map this datastore] を選択します。

UI 要素	基本情報
[Local Datastore] 列	<p>このクラスタ、ローカル HX Storage Clusterに構成されたデータストアの一覧です。</p> <p>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。</p>

UI 要素	基本情報
[Remote Datastore] 列	<p>HX Storage Cluster間でデータストアをペアリングします。</p> <ol style="list-style-type: none"> 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。 <p>[Remote Datastore] 列のプルダウンメニューで、[Do not map this datastore] を選択します。</p> <ol style="list-style-type: none"> 必要な [Local Datastore] 行で、[Remote Datastore] 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、[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 [Replication] > [Replication Pairs] > [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クレデンシャルを入力し、[Delete] をクリックします。

UI 要素	基本情報
[User Name] フィールド	リモート HX Storage Clusterの管理者ユーザ名を入力します。
[Password] フィールド	リモート HX Storage Cluster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方式の VM のグループです。

保護グループはローカルクラスタ上に作成します。保護グループは、それらが作成されたクラスタを介してのみ管理が可能で、それらが作成されたクラスタのみに保護を提供できます。保護グループがローカルの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 HX Connect にリストされます。ただし、保護グループは、そのローカルクラスタ、つまりそれが作成されたクラスタからのみ管理できます。

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 ペアを構成する必要があります。

ステップ 1 管理者として HX Connect にログインします。

ステップ 2 [Replication] > [Protection Groups] > [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	基本情報
[Protection Group Name] フィールド	<p>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。</p> <p>保護グループは、各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、リモートクラスタでは編集できません。クラスタには複数の保護グループを作成できます。</p>
[Protect virtual machines in this group every] フィールド	<p>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。デフォルトは1時間ごとです。プルダウンメニュー オプションは次のとおりです。</p> <p>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</p>
[Start protecting the virtual machines immediately] ラジオ ボタン	<p>この保護グループに最初に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場合、このラジオ ボタンを選択します。</p>
[Start protecting the virtual machines at] ラジオ ボタン	<p>最初のレプリケーション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。</p> <p>開始する前に複製について以下を確認します。</p> <ul style="list-style-type: none"> • 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。 <p>保護の開始時刻を指定するには、次のようにします。</p> <ol style="list-style-type: none"> 1. [Start protecting the virtual machines at] ラジオ ボタンをクリックします。 2. [time] フィールドをクリックし、時間と分を選択します。フィールドの外をクリックします。 <p>[Cluster time zone] と [Current time on cluster] は、適切なレプリケーションの開始時刻を選択するために参照されます。開始時刻は、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。</p> <p>クラスタの現在の時刻が 1:56:15 PM で、現在から 10 時間と 3 分後とは、11:59:00 PM 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。</p> <p>[hours, minutes from now] は、最初のレプリケーションはいつ発生するかを示します。これは、[time] フィールドの設定値を変更すると更新されます。</p>

UI 要素	基本情報
[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 Data Platform で仮想マシンを休止するには、このチェック ボックスをクリックします。 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 [Create Protection Group] をクリックします。

HX Data Platform で [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 [Replication] > [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します。

保護グループの編集

保護グループ内の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。

ステップ 1 管理者として HX Connect にログインします。

ステップ 2 [Replication] > [Protection Groups] > [Edit Schedule] 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内の情報を編集します。

UI 要素	基本情報
[Protect virtual machines in this group every] フィールド	プルダウンリストから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。次のオプションがあります。 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
[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 Data Platform で仮想マシンを休止するには、このチェックボックスをクリックします。 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 [Save Changes] をクリックします。

HX Data Platform は、保護グループの間隔および開始時間を更新します。新しい間隔の頻度を表示するには、[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。

ステップ 1 保護グループ内のすべての仮想マシンの保護を解除します。

- HX Connect で、**[Replication]** > **[Protected Virtual Machines]** を選択します。
- 保護グループ内のすべての仮想マシンを選択します。
- [Unprotect]** をクリックします。確認ポップアップで、**[Unprotect]** をクリックします。

ステップ 2 **[Replication]** > **[Protection Groups]** > **[*protection_group_name*]** を選択します。

ステップ 3 **[Delete]** をクリックします。確認ポップアップで、**[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 つ以上の仮想マシンを選択し、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。

ステップ 1 管理者特権で HX Connect にログインし、**[Virtual Machines]** を選択します。

これによりローカル 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 2 つ以上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 **[Protect]** をクリックします。

[Protect Virtual Machines] ウィザードの、**[Protection Group]** ページが表示されます。

ステップ 4 **[Add to an existing protection group]** ラジオ ボタンをクリックします

UI 要素	基本情報
[Set the protection parameters] テーブル	選択した仮想マシンの [Name] を確認します。 [Storage Provisioned] と [Storage Used] を使用して、リモート HX Storage Cluster に利用可能な十分なリソースがあることをチェックします。
[Add to an existing protection group] ラジオ 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、この仮想マシンに適用されます。
[Create a new protection group] ラジオ 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、リモートクラスタでは編集できません。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、[Next] をクリックします
選択した保護グループに、希望するスケジュール間隔があることを確認します。
[Protect Virtual Machines] ウィザードの、[Summary] ページが表示されます。

ステップ 6 [Summary] ページの情報を確認し、[Add to Protection Group] をクリックします。
HX Data Platform により、仮想マシンがレプリケーション保護に追加されます。[Replication] または [Virtual Machines] ページを表示して確認します。[Replication] ページに保護グループが表示されることに注意してください。

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を使用する : 2 つ以上の仮想マシンを選択し、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。

ステップ 1 管理者特権で HX Connect にログインし、[Virtual Machines] を選択します。
これによりローカル 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 2 つ以上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 [Protect] をクリックします。

[Protect Virtual Machines] ウィザードの、[Protection Group] ページが表示されます。

ステップ 4 [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、[Next] をクリックします。

[Protection Schedule Wizard Page] 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、[Next] をクリックします。

UI 要素	基本情報
[Protect virtual machines in this group every] フィールド	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。デフォルトは 1 時間ごとです。プルダウン メニュー オプションは次のとおりです。
[Start protecting the virtual machines immediately] ラジオ ボタン	この保護グループに最初に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場合、このラジオ ボタンを選択します。

UI 要素	基本情報
[Start protecting the virtual machines at] ラジオ ボタン	<p>最初のレプリケーション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には、次のことが必要です。</p> <ul style="list-style-type: none"> • 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。 <p>保護の開始時刻を指定するには、次のようにします。</p> <ol style="list-style-type: none"> 1. [Start protecting the virtual machines at] ラジオ ボタンをクリックします。 2. [time] フィールドをクリックし、時間と分を選択します。フィールドの外をクリックします。 <p>[hours, minutes from now] は、最初のレプリケーションはいつ発生するかを示します。これは、[time] フィールドの設定値を変更すると更新されます。</p> <p>[Cluster time zone] と [Current time on cluster] は、適切なレプリケーションの開始時刻を選択するために参照されます。開始時刻は、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。</p> <p>クラスタの現在の時刻が 1:56:15 PM で、現在から 10 時間と 3 分後とは、11:59:00 PM 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。</p>
[Use VMware Tools to quiesce the virtual machine] チェックボックス	<p>レプリケーション スナップショットを取る前に HX Data Platform で仮想マシンを休止するには、このチェックボックスをクリックします。</p> <p>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。</p>

[Protect Virtual Machines] ウィザードの、[Summary] ページが表示されます。

ステップ 6 [Summary] ページの情報を確認し、[Add to Protection Group] をクリックします。

概要の内容を確認し、選択した仮想マシンに適用する設定を確認します。

- 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

HX Data Platform により、仮想マシンがレプリケーション保護に追加されます。[Replication] または [Virtual Machines] ページを表示して確認します。[Replication] ページに保護グループが表示されることに注意してください。

個別の仮想マシンの保護

このタスクでは、仮想マシンを保護する方法について説明します。

- **個別**：1つの仮想マシンを選択して構成します。特定の仮想マシン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、個別に保護された仮想マシンにのみ影響を与えます。仮想マシンは、保護グループに含まれません。
- **既存の保護グループ**：1つ以上の仮想マシンを選択し、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。

ステップ 1 管理者特権で HX Connect にログインし、[Virtual Machines] を選択します。

これによりローカル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 [Protect] をクリックします。

[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	基本情報
[Add to an existing protection group] ラジオ ボタン	<p>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。</p> <p>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。</p> <p>追加の構成は必要ありません。[Protect Virtual Machine] をクリックします。</p>
[Protect this virtual machine independently] ラジオ ボタン	<p>この仮想マシン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。</p>
[Protect this virtual machine every] フィールド	<p>プルダウンリストから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。次のオプションがあります。</p> <p>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</p>
[Start protecting the virtual machines immediately] ラジオ ボタン	<p>この保護グループに最初に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場合、このラジオ ボタンを選択します。</p>
[Start protecting the virtual machines at] ラジオ ボタン	<p>最初のレプリケーション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には、次のことが必要です。</p> <ul style="list-style-type: none"> • 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。 <p>保護の開始時刻を指定するには、次のようにします。</p> <ol style="list-style-type: none"> 1. [Start protecting the virtual machines at] ラジオ ボタンをクリックします。 2. [time] フィールドをクリックし、時間と分を選択します。フィールドの外をクリックします。 <p>[hours, minutes from now] は、最初のレプリケーションはいつ発生するかを示します。これは、[time] フィールドの設定値を変更すると更新されます。</p> <p>[Cluster time zone] と [Current time on cluster] は、適切なレプリケーションの開始時刻を選択するために参照されます。開始時刻は、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。</p> <p>クラスタの現在の時刻が 1:56:15 PM で、現在から 10 時間と 3 分後とは、11:59:00 PM 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。</p>

UI 要素	基本情報
[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 Data Platform で仮想マシンを休止するには、このチェックボックスをクリックします。 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 5 [Protect Virtual Machine] をクリックします。

仮想マシンの状態は、[Virtual Machine] ページと [Replication] ページに更新されます。[Replication] ページに保護グループが表示されないことに注意してください。

これで、この仮想マシンで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

保護グループを削除する場合は、その保護グループ内の仮想マシンの保護を解除する必要があります。



(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、仮想マシン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 \(200ページ\)](#) を参照してください。

ステップ 1 管理者として HX Connect にログインします。

ステップ 2 [Virtual Machines] を選択します。

これによりローカル クラスタ上の仮想マシンが一覧表示されます。

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。

一度に 1 つの仮想マシンの保護を解除できます。

ステップ 4 [Unprotect] をクリックし、確認のクリックをします。

仮想マシンの状態が、[protected] から [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。

VM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—仮想マシンのリカバリは、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 スナップショットを復元します。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。

計画済み移行ワークフロー—計画済みの移行を実行すると、レプリケーション スケジュールを停止し、最新のコピーを複製して、ターゲット上で回復し、ソースからターゲットに所有権ををスイッチし、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—計画されていない移行を実行すると、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。リカバリの実行後は、このタスクを完了して、新しいクラスタに対して復元されたVMを保護します。

フェールバック—フェールバックは、元のソースに仮想マシンを移行するために使用するプロセスです。

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。



(注) リカバリのテストはクラスタ実行中に中断することはありません。意図としては、実際の障害の際にVMが回復可能なことを確認するためです。

始める前に

仮想マシン 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。
- 保護された仮想マシンは、ターゲット クラスタへのレプリケーションを最近完了しました。これらのレプリケートされた仮想マシンは、ターゲット クラスタで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。回復した VM に別のテストが必要な場合、以前に作成された VM を削除してください。

ステップ 1 管理者として、ターゲット クラスタの HX 接続にログインします。

ステップ 2 [レプリケーション > リモート VM] タブ > *protected_vm* に進みます。

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] 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	基本情報
[Resource Pool] 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] 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： <ul style="list-style-type: none"> • 検出された仮想マシン • HX テスト リカバリ
[電源オン/オフ] 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 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。
ネットワークのテスト 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 Storage Cluster 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。 <ul style="list-style-type: none"> • ストレージコントローラ データ ネットワーク • ストレージコントローラ管理ネットワーク • 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] ラジオ ボタン	ソースとターゲット クラスタ ネットワーク間のマップを作成することを選択します。 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。

ステップ 4 [VM を回復する] 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

仮想マシンのリカバリでは、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

- 仮想マシン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、リカバリ側のすべての 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、復旧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しない場合は、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に対してリカバリを実行する場合、同時リカバリ操作の最大数は 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。
- 保護された仮想マシンは、ターゲット クラスタへのレプリケーションを最近完了しました。これらのレプリケートされた仮想マシンは、ターゲット クラスタでスナップショットとして保存されています。

ターゲット クラスタのディザスタ リカバリを行うには、次を実行します。

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 複製 (Replication) > > リモート VM タブ (Remote VMs tab) > > *protected_vm* を選択し、[リカバ (Recover)] をクリックします。

ステップ 3 VM を復旧し、ローカルクラスタ上に新しい VM を構築するには、[VM のリカバリ (Recover VM)] ボタンをクリックします。

(注) ここに記載されているフィールドはすべてオプションです。

UI 要素	基本情報
[Resource Pool] 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)] ドロップダウンメニュー	新しい VM を格納する場所を選択します。
[電源オフ (Power Off)] オプション ボタン	リカバリした 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	<p>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は選択します。</p> <ul style="list-style-type: none"> • 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。 <p>ネットワーク オプションの事例:</p> <ul style="list-style-type: none"> • ストレージ コントローラ データ ネットワーク • ストレージ コントローラ 管理 ネットワーク • ストレージ コントローラ 複製 ネットワーク • VM ネットワーク

ステップ 4 [VM のリカバリ (Recover VM)] をクリックします。

ステップ 5 リカバリ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。

保護グループの仮想マシンのリカバリ

ステップ 1 [保護された VM] をクリックし、[リカバリの準備] をクリックします。

これは、保護グループからすべての VM を移動し、[回復中] 状態にすると、[スタンドアロン保護済み VM] サブ ウィンドウに表示されます。

ステップ 2 保護グループの一部であった個々の仮想マシンを回復します。詳細については、[仮想マシンのリカバリ \(193 ページ\)](#) を参照してください。

ステップ 3 保護グループ内のすべての VM に手順 2 (仮想マシンを回復する) を実行します。

計画された移行ワークフロー

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。

ソースからターゲットへ保護された VM を移行するためには、次の手順を使用します。移行プロセスの最後で同じスケジュールが使用され、ターゲットからソースへ保護の方向が反転しません。



注目 このプロセスは戻すことができません。

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 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、仮想マシンが存在しているクラスタです。

ステップ 2 WebCLI 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>
```

結果 : タスク ID が返されます。

ソース VM の電源オフし、最終的な違いがレプリケートされます。保護ステータスを [回復済み] に変更します。

ステップ 3 WebCLI を使用して、prepareFailover タスクのステータスをモニタします。

```
stcli dp vm hxtask -vmid <VMID> -id <task id>
```

前のステップからタスク ID を使用します。

ステップ 4 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 5 [レプリケーション] > > [リモート VM] タブ > > *protected_vm* を選択し、[回復] をクリックします。

ステップ 6 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] ボタンをクリックします。

[このクラスタの VM を回復する] ダイアログ ボックスの次のフィールドの値を入力します、。

UI 要素	基本情報
[Resource Pool] 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	基本情報
[フォルダ (Folders)] ドロップ ダウン メニュー	新しい VM を格納する場所を選択します。
[電源オフ (Power Off)] オプ ション ボタン	リカバリした 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。 <ul style="list-style-type: none"> • 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。 <p>ネットワーク オプションの事例:</p> <ul style="list-style-type: none"> • ストレージコントローラ データ ネットワーク • ストレージコントローラ管理ネットワーク • ストレージコントローラ複製ネットワーク • VM ネットワーク

ステップ 7 [VM を回復する] をクリックします。

ステップ 8 ソース クラスタの以下のコマンドを実行して、ソース VM 登録を解除し、VM の所有権を転送します。

```
stcli dp vm prepareReverseProtect -vmid <VMID>
```

結果：タスク ID が返されます。

VM の保護ステータスとして [保護中] と表示されます。

ステップ 9 WebCLI を使用して、PrepareReverseProtect タスクのステータスをモニタします。

```
stcli dp vm hxtask -vmid<VMID> -id <task id>
```

前のステップからタスク ID を使用します。

ステップ 10 ターゲット クラスタで次のコマンドを実行します。

```
stcli dp vm reverseProtect -vmid <VMID>
```

結果：タスク ID が返されます

VM の保護ステータスとして [保護済み] と表示されます。

ステップ 11 WebCLI を使用して、reverseProtect タスクのステータスをモニタします。

```
stcli dp vm hxtask -vmid <VMID> -id <task id>
```

前のステップからタスク ID を使用します。

未計画の移行ワークフロー

計画されていない移行を実行すると、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。

障害が発生したとき、保護の方向を逆にするとき、通常は未計画の移行が実行されます。



注目 このプロセスは戻すことができません。

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 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、仮想マシンが存在しているクラスタです。

ステップ 2 リモート VM リストから、VM を選択します。このクラスタのワークフローで 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。VM のデータは保持します。

ステップ 3 [レプリケーション > > リモート VM] タブ > > *protected_vm* を選択し、[回復] 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] ボタンをクリックします。

[このクラスタの VM を回復する] ダイアログ ボックスの次のフィールドの値を入力します、。

UI 要素	基本情報
[Resource Pool] 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 メニュー	新しい VM を格納する場所を選択します。
[電源オフ (Power Off)] オプション ボタン	リカバリした 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。

UI 要素	基本情報
ネットワークのマッピング	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>ネットワーク オプションの事例:</p> <ul style="list-style-type: none"> • ストレージコントローラ データ ネットワーク • ストレージコントローラ管理ネットワーク • ストレージコントローラ複製ネットワーク • VM ネットワーク

ステップ 5 [VM を回復する] をクリックします。

ステップ 6 ソース クラスタの以下のコマンドを実行して、ソース VM 登録を解除し、VM の所有権を転送します。

```
stcli dp vm prepareReverseProtect -vmid <VMID>
```

結果 : タスク ID が返されます。

VM の保護ステータスとして [保護中] と表示されます。

ステップ 7 WebCLI を使用して、PrepareReverseProtect タスクのステータスをモニタします。

```
stcli dp vm hxtask -vmid<VMID> -id <task id>
```

前のステップからタスク ID を使用します。

ステップ 8 ターゲット クラスタで次のコマンドを実行します。

```
stcli dp vm reverseProtect -vmid <VMID>
```

結果 : タスク ID が返されます

VM の保護ステータスとして [保護済み] と表示されます。

ステップ 9 WebCLI を使用して、reverseProtect タスクのステータスをモニタします。

```
stcli dp vm hxtask -vmid <VMID> -id <task id>
```

前のステップからタスク ID を使用します。

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。

-
- 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 VM を回復する）を実行します。詳細については、[仮想マシンのリカバリ（193 ページ）](#)を参照してください。
- ステップ 2** ペアリングを忘れ、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、クラスタは元のソースにペアリングされなくされます。
- 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（190 ページ）](#)を参照してください。
- ステップ 4** 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（177 ページ）](#)を参照してください。
- ステップ 5** 仮想マシンを保護します。
- 

## 仮想マシンのフェールバック

フェールバックは、仮想マシンを元のソースに戻すために使用されるプロセスです。

フェールバックは、次のシナリオで実行できます。

### シナリオ1-メンテナンス期間中

1. ソースからターゲットへの計画的な移行を実行します。
2. 新しいソースから新しいターゲットへの計画的な移行を実行します。

詳細については、[計画された移行ワークフロー（195 ページ）](#)を参照してください。

### シナリオ2-災害インシデント発生後

1. ソースからターゲットへの計画外の移行を実行します。詳細については、[未計画の移行ワークフロー（197 ページ）](#)を参照してください。
2. 新しいソースから新しいターゲットへの計画的な移行を実行します。詳細については、[計画された移行ワークフロー（195 ページ）](#)を参照してください。

## 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ごとにバックグラウンドで実行されます。レプリケーションメンテナンスタスクには次のものがあります。

- **リカバリのテスト**：リカバリメソッドが動作しているかどうかをテストします。詳細については、[仮想マシンのリカバリのテスト（191 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**：HX Storage Clusterでメンテナンスを行う準備をしていて、レプリケーションを設定済みの場合、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。

HX Storage Clusterのメンテナンスアクティビティには、ノードの追加または再起動、あるいは HX Storage Clusterのアップグレードが含まれます。通常、HX Clusterでノードを HX メンテナンスモードにする必要がある場合は、レプリケーションを一時停止して再開します。

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**：HX Storage Cluster 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。

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ターゲットクラスタに VM をシフトするオプション。ターゲットクラスタは移行した VM の新しいソースクラスタになります。詳細については、[計画された移行ワークフロー（195 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

HX Storage Clusterのメンテナンスを行うための準備をする際にレプリケーションの構成が適用済みになっている場合は、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。

HX Storage Clusterのメンテナンスアクティビティには、ノードの追加または再起動、あるいは HX Storage Clusterのアップグレードが含まれます。通常、HX Clusterでノードを HX メンテナンスモードにする必要がある場合は、レプリケーションを一時停止して再開します。

- 
- ステップ 1** ストレージコントローラ VM にログインします。
  - ステップ 2** 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** メンテナンスまたはアップグレードのタスクを実行します。
-

### 次のタスク

メンテナンスまたはアップグレードのタスクを続行して完了します。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

HX Storage Clusterのメンテナンスを行うための準備をする際にレプリケーションの構成が適用済みになっている場合は、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。

HX Storage Clusterのメンテナンスアクティビティには、ノードの追加または再起動、あるいはHX Storage Clusterのアップグレードが含まれます。通常、HX ClusterでノードをHX メンテナンス モードにする必要がある場合は、レプリケーションを一時停止して再開します。

アクティビティの完了後、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 Storage Clusterが一時停止されており、メンテナンスまたはアップグレードのタスクが完了していることを確認します。

---

**ステップ 1** ストレージ コントローラ VM にログインします。

**ステップ 2** コマンドラインから `stcli dp schedule resume` コマンドを実行します。

---

すべての保護された仮想マシンの構成済みレプリケーション スケジュールが開始されます。





## 第 15 章

# ユーザの管理

- [HyperFlex ユーザの管理の概要 \(203 ページ\)](#)
- [HX データ プラットフォーム RBAC ユーザの作成 \(206 ページ\)](#)
- [ユーザへの権限の割り当て \(206 ページ\)](#)

## HyperFlex ユーザの管理の概要

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のタイプには次のものがあります。

- **admin** : HX Data Platform に含まれている定義済みユーザ。パスワードは、HX Clusterの作成時に設定されます。同じパスワードが root に適用されます。このユーザは読み取りおよび変更のアクセス許可を持ちます。
- **root** : HX Data Platform に含まれている定義済みユーザ。パスワードは、HX Clusterの作成時に設定されます。同じパスワードが admin に適用されます。このユーザは読み取りおよび変更のアクセス許可を持ちます。
- **administrator** : 作成された HX Data Platform ユーザ。このユーザは vCenter を介して作成され、RBAC ロールの administrator が割り当てられます。このユーザは読み取りおよび変更のアクセス許可を持ちます。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 HX Data Platform ユーザ。このユーザは vCenter を介して作成され、RBAC ロールの read-only が割り当てられます。このユーザは読み取りアクセス許可のみを持ちます。パスワードは、ユーザの作成時に設定されます。

| HX インターフェイス             | admin | root | hx_admin | hx_readonly |
|-------------------------|-------|------|----------|-------------|
| HX Data Platform インストーラ | 必須    | 任意   | 無効       | 無効          |

| HX インターフェイス                           | admin                                                                   | root                                                                   | hx_admin                                                             | hx_readonly                                                                                                            |
|---------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| HX Connect                            | ほとんどのHXタスクを実行できます。<br><br>ログインには Local/ の拡張子が必要です。例：<br><br>local/admin | ほとんどのHXタスクを実行できます。<br><br>ログインには Local/ の拡張子が必要です。例：<br><br>local/root | ほとんどのHXタスクを実行できます。<br><br>優先ユーザ。                                     | モニタリング情報の参照のみが可能です。<br><br>HX タスクを実行できません。<br><br>優先ユーザ。                                                               |
| stcli コマンドラインを持つストレージコントローラ VM        | 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。                                                     | ほとんどのHXタスクを実行できます。<br><br>ログインには vc- の拡張子が必要です。例：<br><br>vc hx_admin | ステータスを表示するには、非インタラクティブ stcli コマンドのみ実行できます。<br><br>HX タスクを実行できません。<br><br>ログインには vc- の拡張子が必要です。例：<br><br>vc hx_readonly |
| vCenter を介した HX Data Platform Plug-in | 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。                                                     | ほとんどのHXタスクを実行できます。<br><br>vCenter SSO ユーザ。                           | vCenter 情報のみ表示可能です。<br><br>HX Data Platform Plug-in を表示できません。<br><br>vCenter SSO ユーザ。                                  |
| HX REST API                           | ほとんどのHXタスクを実行できます。<br><br>ログインには Local/ の拡張子が必要です。例：<br><br>local/admin | ほとんどのHXタスクを実行できます。<br><br>ログインには Local/ の拡張子が必要です。例：<br><br>local/root | ほとんどのHXタスクを実行できます。<br><br>ログインには vc- の拡張子が必要です。例：<br><br>vc hx_admin | ステータス レベル REST API のみ実行できます。<br><br>HX タスクを実行できません。<br><br>ログインには vc- の拡張子が必要です。例：<br><br>vc hx_readonly               |

## ユーザ管理用語

- **認証**：ログインクレデンシャルに関する用語。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、指名ユーザのユーザクレデンシャルを確認します。認証は、一般的にユーザクレデンシャルを確認して、セッションを認証されたユーザと関連付けます。
- **承認**：アクセス許可に関する用語。これらのプロセスは、ユーザ/クライアントアプリケーションが何らかのアクション（管理対象エンティティの作成、読み取り、更新、または削除、あるいはプログラムの実行など）を実行することをユーザの ID に基づいて許可します。承認により、認証済みユーザがサーバ上で実行できることが定義されます。
- **アカウントティング**：ユーザ操作の追跡に関する用語。これらのプロセスは、レコードをキープし、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の操作を追跡します。情報はログに保存されます。これらのログは、HX Connect または他の HX Data Platform 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**：個人には ID が付与されます。これは割り当てられたロールであり、付与された権限が伴っています。
- **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、リソースおよびリソースによって公開されている機能の間のリンクです。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ていますが、読み取り専用ロールは、そのデータストアが存在することを表示するだけです。
- **特権**：ID 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、など。
- **リソース**：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、いずれも、REST API を使用してクライアントアプリケーションに公開されているリソースです。
- **ロール**：権限範囲レベルを定義します。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など。ロールは、特定の ID に割り当てられます。

## AAA アカ운ティングの監査ログ

AAA アカ운ティングをサポートするため、HX Data Platform 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。

HX Connect を含む HX Data Platform 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 Systems Troubleshooting Guideを参照してください。

- **stMgrAudit.log**：stcli アクティビティの監査レコードが含まれます。

以下は、サンプル エントリです。キーワード Audit に注目してください。

```
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、他の情報も含まれています。監査イベントを抽出するには、スクリプトを使用して単語 `Audit` を抽出します。

- **audit.log** : REST API アクティビティの監査レコードが含まれます。

以下は、サンプル エントリです。ユーザ名 `administrator@vsphere.local` に注目してください

```
2017-03-29-01:47:28.779 - 127.0.0.1 -> 127.0.0.1 - GET /rest/clusters 200;
administrator@vsphere.local 454ms
```

## HX データ プラットフォーム RBAC ユーザの作成

HX Data Platform は、管理者および読み取り専用の 2 種類のユーザをサポートしています。HX Data Platform の新しいユーザは、VMware vCenter インターフェイスを介して作成されます。

### 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。

**ステップ 1** vCenter 管理者として vSphere Web Client にログインします。

**ステップ 2** [Navigator Home] から、[Administration] > [Users and Groups] > [Users] に進みます。

**ステップ 3** [Add] (+) アイコンをクリックして、ユーザを追加します。[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。ユーザ名およびパスワードの要件については [HX Data Platform の名前、パスワード、文字 \(24 ページ\)](#) 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 \(206 ページ\)](#) を参照してください。

## ユーザへの権限の割り当て

権限は、vCenter の RBAC ロールを通じてユーザに割り当てられます。権限を割り当てるには、管理者または読み取り専用グループにユーザを追加します。



### 始める前に

ユーザを作成します。

---

**ステップ 1** vSphere Web Clientで、**[Navigator Home] > [Administration] > [Global Permissions] > [Manage]** の順に選択します。

**ステップ 2** **[Add] (+)** アイコンをクリックして権限を割り当てます。

**ステップ 3** **[Assigned Role]** を選択します。

**[Global Permission Root - Add Permission]** ダイアログボックスで、**[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**
- **Read only**

**ステップ 4** **[Users and Groups]** 領域で、**[Add]** をクリックします。

**ステップ 5** **[Select Users/Groups]** ダイアログボックスで、*user\_name* を選択して **[Add]** をクリックします。

**ステップ 6** **[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。

---

