Cisco HyperFlex Data Platform リリース 2.5 アドミニストレーション ガイド

初版：2017 年 4 月 10 日

最終更新：2017 年 9 月 8 日

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

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

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す。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す。

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す。

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。

シスコおよびシスコのロゴは、米国およびその他の国におけるシスコおよびその関連会社の商標を示します。To view a list of Cisco trademarks, go to this URL: http://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.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 新機能および変更情報 1

新機能および改訂された情報 1

第 2 章 HX ストレージ クラスタの概要 5

Cisco HX Data Platform の概要 5

ストレージ クラスタの物理コンポーネントの概要 6

HX Data Platform キャパシティの概要 7

キャパシティ削減の理解 9

ストレージ容量イベント メッセージ 10

HX Data Platform のハイ アベイラビリティの概要 11

ストレージ クラスタ ステータス 12

動作ステータスの値 12

復元力ステータスの値 13

HX Data Platform クラスタの耐障害性 13

データ レプリケーション係数の設定 15

クラスタ アクセス ポリシー 16

ストレージ クラスタ ノード障害に対する応答 16

HX Data Platform ReadyClone の概要 23

HX Data Platform ネイティブ スナップショットの概要 23

第 3 章 HX Data Platform インターフェイスへのログイン 25

HyperFlex クラスタ インターフェイスの概要 25

HX Data Platform ログイン クレデンシャルに関するガイドライン 26

HX Data Platform の名前、パスワード、および文字 27

HX Connect へのログイン 31
コントローラ VM（stcli）コマンド ラインへのログイン 32
ストレージ コントローラ パスワードの変更 34
Cisco HX Data Platform インストーラへのログイン 35
HX Data Platform REST API へのアクセス 36
Cisco HX Data Platform プラグインへのアクセス 37
Cisco TAC への連絡 38

第 4 章 HX ストレージ クラスタのモニタリング 41
HyperFlex クラスタのモニタリング 41
パフォーマンス チャートの表示 41
ストレージ クラスタのパフォーマンス チャート 42
ホスト パフォーマンスのチャート 42
データストア パフォーマンスのチャート 42
[パフォーマンス（Performance）] ポートレット 43
[データストアのトレンド（Datastore Trends）] ポートレット 44
パフォーマンス チャートのカスタマイズ 44
パフォーマンス期間の指定 44
カスタム範囲の指定 45
パフォーマンス チャートの選択 45
HX Data Platform プラグイン インターフェイスの使用法 47
Cisco HX Data Platform プラグインと vSphere Web クライアントの統合 47
Cisco HX Data Platform プラグインと vSphere インターフェイス間のリンク 47
Cisco HX Data Platform プラグイン タブの概要 47
HX Connect を使用した HyperFlex クラスタのモニタリング 48
ダッシュボード ページ 49
[アクティビティ（Activity）] ページ 51
[システム情報の概要（System Information Overview）] ページ 52
[ノード（Nodes）] ページ 55
[ディスク（Disks）] ページ 56

第 5 章 HX ストレージ クラスタ メンテナンスの準備 61

ストレージ クラスタのメンテナンス操作の概要 61

シリアル操作とパラレル操作 63

クラスタ ステータスの確認 64

ビーコンの設定 64

HX クラスタの vMotion の設定の確認 65

ストレージ クラスタ ノードのメンテナンス モード 66

Cisco HyperFlex のメンテナンス モードの開始 67

Cisco HyperFlex のメンテナンス モードの終了 69

バックアップ操作の作成 70

HX ストレージ クラスタのシャットダウンと電源オフ 75

HX ストレージ クラスタの電源オンと起動 78

vNIC または vHBA の変更後の PCI パススルーの設定 80

第 6 章 HX ストレージ クラスタの管理 83

クラスタ アクセス ポリシー レベルの変更 83

クラスタの再調整 83

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 84

スペース不足エラーの処理 85

クリーナー スケジュールの確認 86

ストレージ クラスタの vCenter 間の移動計画 86

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 87

vCenter クラスタからのストレージ クラスタの登録解除 88

新しい vCenter クラスタへのストレージ クラスタの登録 90

クラスタの名前の変更 91

第 7 章 暗号化の管理 93

自己暗号化ドライブの概要 93

HyperFlex クラスタが暗号化できることの確認 94

ローカル暗号化キーの構成 94

ローカル暗号化キーの変更 95
ローカルの暗号化キーの無効化 96
暗号化されたディスクを安全に消去する 96
リモート キー管理 97
リモート暗号化キーの構成 97
証明書署名要求の生成 98
CSR（証明書署名要求）を使用したキー管理サーバの構成 99
自己署名証明書の生成 101
SSC（自己署名証明書）を使用したキー管理サーバの構成 102
暗号化のやり直し 103

第 8 章 データストアの管理 105
データストアの管理 105
データストアの追加 106
データストアの編集 107
データストアのマウント 107
データストアのマウント解除 108
データストアの削除 109
部分的にマウント解除されたデータストアの回復 109

第 9 章 ディスクの管理 111
クラスタ内のディスクの管理 111
ディスクの要件 112
自己暗号化ドライブ（SED）の交換 115
SSD の交換 117
NVMe SSD の交換 119
ハウスキーピング SSD の交換 120
ハードディスク ドライブの交換または追加 122

第 10 章 ノードの管理 123
ノードの管理 123

ノード メンテナンス方法の特定 125
DNS アドレスまたはホスト名による検索 128
ESXi ホスト ルート パスワードの変更 129
ノード ソフトウェアの再インストール 129
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 130
ノード コンポーネントの交換 131
ノードの取り外し 133
ノード削除の準備 135
オンライン ストレージ クラスタからのノードの削除 136
オフライン ストレージ クラスタからのノードの削除 139
ノードの交換 141

第 11 章 HX コントローラ VM の管理 147
ストレージ コントローラ VM の管理 147
ストレージ コントローラ VM の電源のオン/オフ 147

第 12 章 ReadyClone の管理 149
HX Data Platform ReadyClone の概要 149
HX Data Platform ReadyClone の利点 149
サポート対象のベース VM 150
ReadyClone の要件 150
ReadyClone のベスト プラクティス 151
HX Data Platform ReadyClone の作成 151
HX Data Platform ReadyClone のカスタマイズの準備 153
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 154
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 154
カスタマイズ仕様を使用した ReadyClone の設定 155
仮想マシン ネットワーキングの管理 155

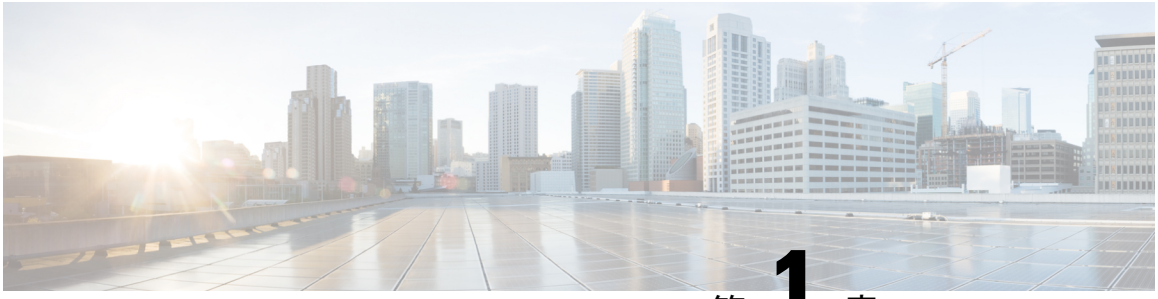
第 13 章 ネイティブ スナップショットの管理 157
HX Data Platform ネイティブ スナップショットの概要 157

HX Data Platform ネイティブ スナップショットの利点 158
ネイティブ スナップショットの考慮事項 159
ネイティブ スナップショットのベスト プラクティス 161
SENTINEL スナップショットについて 162
ネイティブ スナップショットのタイムゾーン 163
スナップショットの作成 164
スナップショットのスケジューリングの概要 165
スナップショットのスケジューリング 166
スケジュール済みスナップショットの頻度の設定 167
スナップショット スケジュールの削除 168
スナップショットへの復帰 168
スナップショットの削除 169

第 14 章 仮想マシンのディザスタ リカバリの管理 171
データ保護の概要 171
レプリケーションとリカバリの考慮事項 172
データ保護の用語 174
仮想マシンの保護の概要 175
データ保護のワークフロー 176
レプリケーション ネットワークの設定 177
レプリケーション ネットワークの編集 180
レプリケーション ペアの概要 181
レプリケーション ペアの作成 182
レプリケーション ペアの編集 183
レプリケーション ペアの削除 184
保護グループの作成 185
保護グループの編集 187
保護グループの削除 188
既存の保護グループでの仮想マシンの保護 189
新しい保護グループでの仮想マシンの保護 190
個別の仮想マシンの保護 192

仮想マシンの保護の解除 194
データ保護/リカバリ ワークフロー 195
仮想マシンのリカバリ 196
保護グループの仮想マシンのリカバリ 199
レプリケーション メンテナンスの概要 201
レプリケーションの一時停止 203
レプリケーションの再開 203
仮想マシンのリカバリのテスト 204
保護された仮想マシンの移行 206
保護グループの仮想マシンの移行 208

第 15 章 ユーザの管理 211
HyperFlex ユーザの管理の概要 211
ユーザ管理用語 213
AAA アカウンティングの監査ログ 213
HX データ プラットフォーム RBAC ユーザの作成 214
ユーザへの権限の割り当て 214



第 1 章

新機能および変更情報

• 新機能および改訂された情報 （1 ページ）

新機能および改訂された情報

次の表に、最新リリースの新機能とこのガイドの変更点の概要を示します。

表 *1 : HX* リリース *2.5* の新機能

機能	説明	追加日	参照先
暗号化	保管中のデータの暗号化専用のソフトウェア サポート。	2017 年 7 月 24 日	参照先 暗号化の管理 （93 ページ）
データ保護	保護された仮想マシンのデータのレプリケーションおよびリカバリ。	2017 年 7 月 24 日	参照先 暗号化の管理 （93 ページ）
RBAC	ロール ベースのユーザ アクセス。管理者と読み取り専用ユーザのアクセス権限ロール。	2017 年 7 月 24 日	参照先 ユーザの管理 （211 ページ）
HX Connect	新しい機能の暗号化とデータの保護のサポートを含む、新しい HTML5 ユーザ インターフェイス。	2017 年 7 月 24 日	参照先 HX Connect へのログイン （31 ページ）
NMVe ディスク	オールフラッシュ システムのキャッシュのための NMVe ディスクのサポート	2017 年 7 月 24 日	参照先 NVMe SSD の交換 （119 ページ）

表 *2 : HX* リリース *2.1* の新機能

機能	説明	追加日	参照先
SED	保管中のデータの暗号化専用のハードウェア サポート。	2017 年 4 月 20 日	ディスクの要件 （112 ページ）

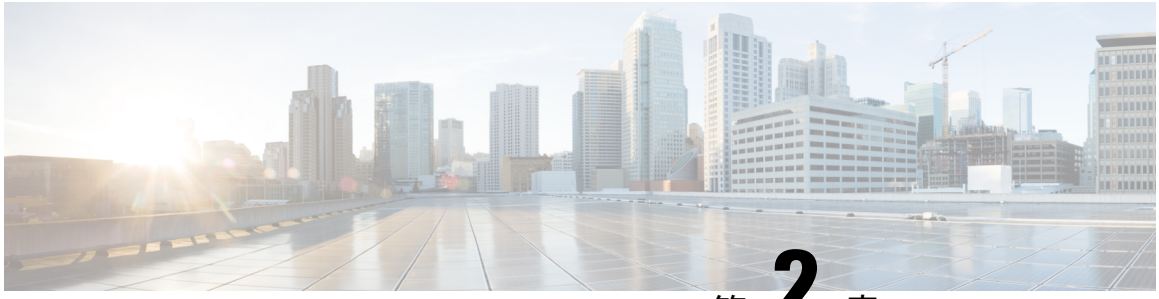
表 *3 : HX* リリース *2.0* の新機能

機能	説明	追加日	参照先
オール フラッシュ サーバ	永続ストレージとしてSSDを使用したサーバ。	2017 年 3 月 6 日	参照先 クラスタ内のディスクの管理 （111 ページ）
メンテナンス後のタスク	ネットワーキング VM に関する UCS Manager のマニュアルへの参照を提供するトピック。	2017 年 3 月 17 日	参照先 仮想マシン ネットワーキングの管理 （155 ページ）
章の再編成	ストレージクラスタのメンテナンスを管理対象コンポーネント（クラスタ、ホスト、コントローラ VM、データストア、ディスク）ごとの章に分割します。 クラスタの拡張を ReadyClone とスナップショットに関する章に分割します。	2017 年 3 月 6 日	コンテンツを参照してください。

表 *4 : HX* リリース *1.8* の新機能

機能	説明	追加日	参照先
容量イベント	容量イベント メッセージの説明を更新	2017 年 2 月 8 日	『Cisco HyperFlex Systems Troubleshooting Guide』を参照してください。
追加された新しいトピック	HX Data Platform ログイン クレデンシャルに関するガイドライン ストレージ コントローラ VM の電源のオン/オフ 部分的にマウント解除されたデータストアの回復	2016 年 11 月 21 日	次を参照データストアの管理 （105 ページ）
ガイドの新しい名前	1.7 アドミニストレーション ガイドは再編成され、名前が「管理ガイド」に変更されました。	2016 年 9 月 30 日	ガイド全体を参照。
ノードの削除および交換	ユーザは TAC によるサポートなしで、一部のクラスタ ノードを削除および交換できます。	2016 年 9 月 30 日	ノードの管理 （123 ページ）を参照してください。

機能	説明	追加日	参照先
ストレージ クラスタ ステータス	ステータスは復元力ステータスと動作ステータスに分類されます。	2016 年 9 月 30 日	参照先 ストレージ クラスタ ステータス （12 ページ）
ストレージ クラスタ イベント	一部のイベントは、解決イベントの発生時に自動的に承認されます。	2016/09/30	『Cisco HyperFlex Systems Troubleshooting Guide』を参照してください。
スナップショットおよび ReadyClone	ノード障害に対する耐障害性が強化されました。	2016 年 9 月 30 日	HX Data Platform ReadyClone の概要 （23 ページ）および次を参照してください。HX Data Platform ネイティブ スナップショットの概要 （23 ページ）
クラスタ メンテナンスの準備	ドキュメントが変更され、タスクの説明が改善されました。	2016 年 9 月 30 日	参照先 ストレージ クラスタのメンテナンス操作の概要 （61 ページ）
サポート バンドルの生成	ドキュメントが変更され、タスクの説明が追加されました。	2016 年 9 月 30 日	『Cisco HyperFlex Systems Troubleshooting Guide』を参照してください。



第 2 章

HX ストレージ クラスタの概要

- Cisco HX Data Platform の概要 （5 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 （6 ページ）
- HX Data Platform キャパシティの概要 （7 ページ）
- HX Data Platform のハイ アベイラビリティの概要 （11 ページ）
- ストレージ クラスタ ステータス （12 ページ）
- HX Data Platform クラスタの耐障害性 （13 ページ）
- ストレージ クラスタ ノード障害に対する応答 （16 ページ）
- HX Data Platform ReadyClone の概要 （23 ページ）
- HX Data Platform ネイティブ スナップショットの概要 （23 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 インターコネクト（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、ESX 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 プラグイン、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 クラスタ名を指定すると、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 HX Data Platform ストレージ クラスタには次のオブジェクトがあります。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。

  ストレージクラスタへのコンバージド 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。コンバージドノードを削除するには、コマンド ラインを使用します。

- **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、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、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。コンピューティング ノードでは、ストレージ クラスタにストレージ リソースが追加されません。

  ストレージ クラスタへのコンピューティング 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。コンピューティング ノードを削除するには、コマンド ラインを使用します。

- **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 クラスタ内のいずれかの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 プラグインが使用す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。

ストレージクラスタの観点からモニタリング可能であり、現場交換可能ユニット（FRU）として扱われる追加のオブジェクトには、次のものがあります。これらのオブジェクトの交換については、サーバ ハードウェア ガイドを参照してください。

- 電源装置（PSU）
- ネットワーク インターフェイス カード（NIC）

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。

- [クリーナー（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* コマンドライン インターフェイス リファレンス ガイド』を参照してください。
- [クラスタ キャパシティ（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。

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

- [データストア キャパシティ（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。

- [未使用キャパシティ、ストレージ クラスタ（Free Capacity, storage cluster）]：使用可能な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。

- [未使用キャパシティ、データストア（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、[未使用キャパシティ（Free capacity）] では、すべてのストレージ クラスタ データストアの可用性がより大きく示される場合があります。

- [複数ユーザ（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。

- [オーバープロビジョニング（Over-provisioning）]：すべてのデータストアに割り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。

- [プロビジョニング済み（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。

- [必要な容量（Space Needed）]：HX ストレージ クラスタ が空間イベント状態になると、[空き領域ステータス（Free Space Status）]フィールドが表示されます。[必要な容量（Space Needed）] は、リストされた [条件（Condition）] をクリアできるようにする必要がある、ストレージの量を示します。

- [使用済み（Used）]：リストされたストレージ クラスタまたはデータストアで使用されるストレージ 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 プラグインまたは HX Connect に [使用済み（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 [使用済み（Used）]は、どの程度のデータストア領域が、設定ファイルやログ ファイル、スナップショット、クローンなどの仮想マシン ファイルによって占有されているかを表します。仮想マシンの実行中、使用されたストレージ領域にはスワップ ファイルも含まれています。

- [利用可能容量（Usable Capacity）]：データの保存に使用できるストレージ クラスタのストレージの容量です。

キャパシティ削減の理解

[サマリー（Summary）] タブの [容量（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 6 TB 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 クローンを使用する場合、重複排除と圧縮による削減は特に有用です。

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

   ```
   = (1 - TUUS/TAS) * 100

   = (1 - 100GB / 200GB) *100

   = 50%
   ```

3. 圧縮による削減

   ```
   = (1 - TUB/TUUS) * 100

   = (1 - 25GB / 100GB) *100

   = 75%
   ```

4. 計算後の合計削減量

   ```
   = (1 - TUB/TAS) * 100

   = (1 - 25GB / 200GB) *100

   = 87.5%
   ```

ストレージ容量イベント メッセージ

クラスタ ストレージ容量には、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、および HX Data Platform プラグイン のアラーム ページとイベント 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ストレージクラスタの容量合計の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ストレージクラスタの容量合計の80%）を下回るまで削減し続けます。

- **SpaceCriticalEvent**：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ストレージクラスタの容量合計の 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 の HA 機能を使用する前に、vSphere Web クライアント上で DRS と 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 プラグイン、およびストレージ コントローラ VM stcli コマンドによって確認できます。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、2 種類のレポート ステータス要素により示されます。

- **動作ステータス**：クラスタの機能ストレージ管理とストレージクラスタ管理をストレージクラスタが実行できるかどうかを示します。ストレージクラスタが動作をどの程度適切に実行できるかを示します。
- **復元力ステータス**：ストレージ クラスタがストレージ クラスタ内でのノード障害を許容できるかどうかを示します。ストレージクラスタが中断をどの程度適切に処理できるかどうかを示します。

ストレージクラスタが特定の動作状態や復元力ステータスに移行するときに、連動する2つの設定が影響します。

- **データ レプリケーション係数**：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。

- [オンライン（Online）]：クラスタは I/O に対応する準備ができています。
- [オフライン（Offline）]：クラスタは I/O に対応する準備ができていません。
- [スペース不足（Out of space）]：クラスタ全体のスペースが不足しているか、または 1 つまたは複数のディスク領域が不足しています。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はできませんが、静的クラスタ情報を表示し続けることはできます。
- [読み取り専用（Readonly）]：クラスタは書き込みトランザクションを受け入れることはできませんが、静的クラスタ情報を表示し続けることはできます。

- [不明（Unknown）]：これは、クラスタがオンラインになる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。

復元力ステータスの値

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

復元力ステータスのオプションを次に示します。

- [正常（Healthy）]：データと可用性の点でクラスタは正常です。
- [警告（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。
- [不明（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

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。

- **クラスタ内のノードの数。**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 レプリケーション係数。**これは HX Data Platform のインストール時に設定され、その後は変更できません。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 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。

- **アクセス ポリシー。**これは、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	読み取り専用	Shutdown
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	読み取り専用	Shutdown
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にのみシャットダウンします。

（注） HXストレージクラスタは、シリアルディスク障害（同時ではないディスク障害）に耐えることができます。唯一の要件は、自己修復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にのみ適用されます。

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	読み取り専用	Shutdown
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が定義されます。オプションは、2 または 3 個のデータの冗長レプリカです。

- ハイブリッド サーバ（SSD 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。次の選択項目があります。

- 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 レプリケーション係数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。これがデフォルトです。

ストレージ クラスタ ノード障害に対する応答

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

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

オプションで、HX Connect および HX Data Platform プラグイン の関連付けられている [クラスタ ステータス/操作ステータス（Cluster Status/Operational Status）] または [復元力ステータス/復元力状況（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。	**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。	ノードが 2 時間以内に復元されない場合、ストレージクラスタは残りのノードのデータの再調整によって修復を開始します。 ノード障害を迅速に修復し、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。 **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。	2 台の SSD に障害が発生している場合、ストレージクラスタは自動的に修復されません。 ディスクが 1 分以内に復元されない場合、ストレージクラスタは残りのノードのデータの再調整によって修復を開始します。

クラスタ サイズ	同時障害発生数	障害の発生したエンティティ	実行するメンテナンス アクション
5+ ノード	2	最大 2 ノード。	ノードが 2 時間以内に復元されない場合、ストレージクラスタは残りのノードのデータの再調整によって修復を開始します。 ノード障害を迅速に修復し、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。 **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 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。
5+ ノード	2	2 つのノードのそれぞれで、2 つ以上のディスクに障害が発生する。	システムは、1 分後に自動的に再調整をトリガーし、ストレージクラスタの正常性を復元します。

クラスタ サイズ	同時障害発生数	障害の発生したエンティティ	実行するメンテナンス アクション
5+ 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
			ディスクが **1 分**以内に復元されない場合、ストレージクラスタは残りのノードのデータの再調整によって修復を開始します。 ノードが **2 時間**以内に復元されない場合、ストレージクラスタは残りのノードのデータの再調整によって修復を開始します。 ストレージクラスタ内のノードで障害が発生し、別のノード上のディスクにも障害が発生している場合、ストレージクラスタは 1 分以内に障害発生ディスクの修復を開始します（障害発生ノードのデータは変更されません）。障害発生ノードが 2 時間経過後に稼動しない場合、ストレージクラスタが障害発生ノードの修復を開始します。 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。 **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。また、VM の複数コピーを作成できる拡張機能です。作成されたコピーはスタンドアロン VM として使用できます。

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。ReadClone 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。

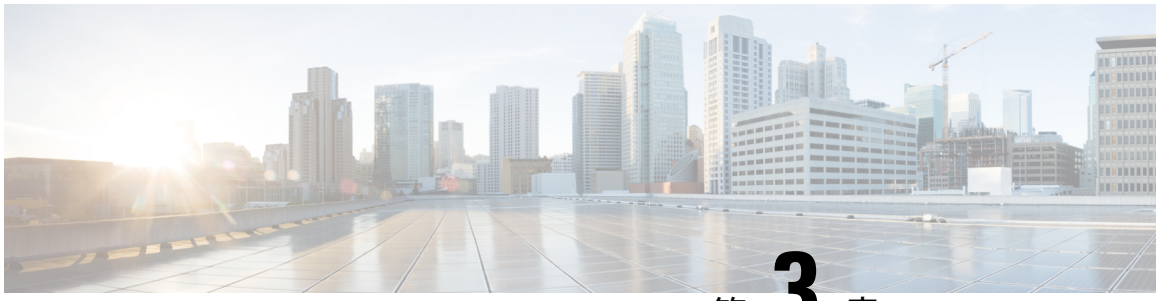
HX Data Platform ネイティブ スナップショットの概要

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 プラグインを使用して 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



第 3 章

HX Data Platform インターフェイスへのログイン

- HyperFlex クラスタ インターフェイスの概要 （25 ページ）
- HX Connect へのログイン （31 ページ）
- コントローラ VM（stcli）コマンド ラインへのログイン （32 ページ）
- Cisco HX Data Platform インストーラへのログイン （35 ページ）
- HX Data Platform REST API へのアクセス （36 ページ）
- Cisco HX Data Platform プラグインへのアクセス （37 ページ）
- Cisco TAC への連絡 （38 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 ストレージ クラスタ 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 ストレージクラスタ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、レプリケーション、データストア、ノード、ディスク、VM readyclones のタスク
- HX Data Platform プラグイン：モニタリング、パフォーマンス チャート、およびアップグレード、データストア、ノード、ディスク、VM ネイティブ スナップショット、VM readyclones 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 システム 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 システム の管理

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 ストレージ クラスタ の作成と拡張

- Cisco UCS Manager：HX ストレージ クラスタ のネットワーク、ストレージとストレージ アクセス、およびリソースの管理のタスク
- VMware vSphere Web クライアント および vSphere Client：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 ローラの VM パスワードは、HX Data Platform のインストール中に指定されます。インストール後は、stcli コマンド ラインを介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	ユーザ名	パスワード	注記
HX Data Platform OVA	root	root	Cisco123	
HX Data Platform インストーラ VM	root	root	Cisco123	
HX Connect	管理者または読み取り専用	vCenter を介して定義されているユーザ。	vCenter を介して定義されているユーザ。	
		定義済み `admin` または `root` ユーザ。	HX のインストール中に指定されます。	ログインには、先頭に `local/` が必要です。`local/admin` または `local/root`
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 を介して定義されているユーザ。 定義済み `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、stcli コマンドを使用します。

コンポーネント	権限レベル	ユーザ名	パスワード	注記
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ーは、HX Data Platform プラグイン へのアクセスを持っていません。
ESX 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 インストール後、パスワードを変更するときは、vCenter または esxcli コマンドを使用します。
UCS マネージャ	admin	設定に依存します。	設定に依存します。	
FI	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、および文字

印刷可能な ASCII 文字と拡張 ASCII 文字のほとんどは、名前とパスワードに使用できます。ただし一部の文字は、HX Data Platform のユーザ名、パスワード、仮想マシン名、ストレージ コントローラ VM 名、およびデータストア名に使用できません。フォルダとリソース プールには、使用できない文字がありません。

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は避けてください。

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、使用するシェルを考慮してください。シェルによって、注意が必要な文字は異なります。名前またはパスワードに特殊文字が含まれる場合は、'speci@lword!' のように単一引用符で囲みます。

HX ストレージ クラスタ名

HX クラスタ名は 50 文字を超えることができません。

仮想マシンおよびデータストア名

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は使用できます。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使用できます。

最大文字数：仮想マシン名は、最大 15 文字です。

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

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

ユーザ名の要件

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

UCS Manager ユーザ名の要件。

- 文字数：6 ～ 32 文字
- Cisco UCS Manager 内で一意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 パスワードの要件

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

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

コントローラ VM 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。ただし、Unix パスワード コマンドなど、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] [--password PASSWORD]

   変更は、HX クラスタのすべてのコントローラ VM に伝達されます。

UCS Manager および ESX のパスワード形式と文字の要件

以下は、UCS Manager および VMware ESXi のパスワードの形式と文字の要件の概要です。詳細については Cisco UCS Manager と VMware ESX 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・小文字の区別をします。（Unable to authenticate using the domain name, user name, and password that you specified. Please check the values that you entered and try again. Passwords are case sensitive.）」

- **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。

  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 のパスワードには、エスケープ（\）文字を使用できません。

  ESX パスワードには、これらの文字を使用できません。

  - ユーザ名やユーザ名を逆にしたものは使用できません。
  - ディ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。

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 ストレージ クラスタ 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提供します。

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。これもセッションをドロップするためです。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ーを閉じないでください。セッションはまだオープンなセッションとしてカウントされています。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 ストレージ クラスタ 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、ヘルプに説明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 で最大限の操作を実行するには、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 ストレージ クラスタ 管理 IP アドレスを検索します。

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 ストレージ クラスタ の管理 IP アドレスを入力します。

ステップ 3 HX ストレージ クラスタ のログイン クレデンシャルを入力します。

- **RBAC ユーザ**：Cisco HyperFlex Connect は、次のロールベースのアクセス制御（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 ストレージ クラスタ を変更できます
  - **読み取り専用**：読み取り専用ロールを持つユーザには、読み取り（表示）権限があります。HX ストレージ クラスタ 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 `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 とセッションを認識します。このため vCenter で発生するシステム メッセージは `local/root` ではなくセッションのユーザを示す可能性があります。たとえば、アラームで、`Acknowledged By might list com.springpath.sysmgmt.domain-c7` と表示されます。

目のアイコンをクリックしてパスワード フィールドのテキストを表示または非表示にします。このアイコンは、時々フィールドの他の要素によって分かりにくくなっています。目のアイコンの領域をクリックすると、切り替え機能の動作を継続します。

次のタスク

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

コントローラ VM（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 クラスタ情報を読み取るコマンドと HX クラスタを変更するコマンドに分かれています。

- 変更のコマンド：管理者レベルのアクセス許可が必要です。例：

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

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

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

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

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

ストレージ コントローラ VM で HX Data Platform コマンドライン インターフェイスにログインします。方法を選択します。

- 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]** > **[概要（Summary）]** > **[DNS 名（DNS Name）]** を選択します。
2. vSphere Web クライアントから、**[ホーム（Home）]** > **[VM とテンプレート（VMs and Templates）]** > **[vCenter サーバ（vCenter server）]** > ***[datacenter]*** > **[ESX エージェント（ESX Agents）]** > **[VM]** 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 クラスタの作成時に定義。

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-administator@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.
ECDSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
Are you sure you want to continue connecting (yes/no)?
```

c) プロンプト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 Web CLI ページから。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 パスワード コマンドを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 キーを押します。

Cisco HX Data Platform インストーラへのログイン

次に、HX データ プラットフォーム ソフトウェアをインストールします。

（注） Cisco HX データ プラットフォーム 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 ESX 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 ブラウザで、HX データ プラットフォーム インストーラがインストールされた VM の URL を入力します。

このアドレスは、前述の項「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 クレデンシャルを使用します。

ユーザ名：*root* パスワード：*Cisco123*

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

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

ステップ 3 HX Data Platform インストーラの [ワークフロー（Workflow）] ページが表示されます。このページには、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（Cluster Creation）]：UCS Manager、ESXi を設定して HX Data Platform ソフトウェアを導入する場合は、このボタンをクリックします。
- [クラスタの展開（Cluster Expansion）]：コンバージド ノードおよびコンピューティング ノードを既存のストレージ クラスタに追加する場合は、このボタンをクリックし、表示される [クラスタを展開する（Expand Cluster）] ページでデータを入力します。

新規クラスタを作成するために[クラスタの作成（Cluster Creation）]オプションを選択し、[次へ（Continue）] をクリックします。

ステップ 4 HX Data Platform インストーラの次の [ワークフロー（Workflow）] ページが表示され、以下のオプションが提供されます。

- [UCS Manager の構成を実行（Run UCS Manager Configuration）]：HX ノードに FI ポリシーとプロファイルを適用する場合は、このボタンをクリックします。
- [ESXi の構成を実行（Run ESXi Configuration）]：ESX サーバを設定する場合は、このボタンをクリックします。これによって表示されるページで、静的 IP アドレス、ホスト名、VLAN を設定します。

- [HX ソフトウェアを展開（Deploy HX Software）]：必要な設定データを入力して、ストレージ クラスタを手動で設定します。

HX Data Platform REST API へのアクセス

Cisco HyperFlex HX シリーズ システムは、完全内包型の仮想サーバ プラットフォームを通じて、コンピューティング、ストレージ、ネットワークの 3 つのレイヤと強力な Cisco HX Data Platform ソフトウェア ツールを結合し、シングル ポイント接続による簡素化された管理を実現します。Cisco HyperFlex 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、リソースの統合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、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、HTTP 呼び出しを実行するように構成することができます。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で Hyperflex の管理プレーンと直接インターフェイスすることができます。

これらのリソースは URI（Uniform Resource Identifier）を介してアクセスし、POST（作成）、GET（読み取り）、PUT（更新）、DELETE（削除）などの HTTP 動詞を使用して操作します。

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 リソースを消費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、DevNet アドレスにアクセスします。 https://developer.cisco.com/site/ucs-dev-center/docs/hyperflex/

developer.cisco.com で、**[Technologies]** > **[Data Center]** > **[UCS Dev Center]** > **[Cisco HyperFlex Systems REST API Reference]** を選択します。

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。

同じクレデンシャルを使用して、Swagger UI にログインします。

Cisco HX Data Platform プラグインへのアクセス

HX Data Platform プラグインへは vSphere Web クライアントからアクセスします。

（注） HX Data Platform プラグインは、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 プラグインは、vSphere シック クライアントとも呼ばれる vSphere Client for Windows 経由では入手できません。HX Data Platform プラグインのアクティビティに関して生成されたイベント メッセージが vSphere Client 表示に含まれています。HX Data Platform プラグライン タスクは、vSphere Client for Windows 経由では実行できません。

ステップ 1 vSphere Web クライアントから、vCenter パネル上部にある [ホーム（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 [ホーム（Home）] ページで [vCenter インベントリ リスト（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 プラグイン内で使用可能な 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。

[オブジェクト（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。[編集（edit）] アイコン（鉛筆）をクリックするか、[操作（Actions）] メニューから [クラスタの名前を変更（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。[概要（summary）]アイコン（緑色の紙）をクリックするか、[操作（Actions）] メニューから [概要（summary）] を選択します。

ステップ 5 [ナビゲータ（Navigator）] ペインのリストから、[*HX* ストレージ クラスタ（*HX storage cluster*）] 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表示されます。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 中央ペイン内のタブをクリックして、HX Data Platform プラグイン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。

タブ オプション	説明
要約	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。
モニタ（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。
管理	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 で受賞暦のあるテクニカル 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。

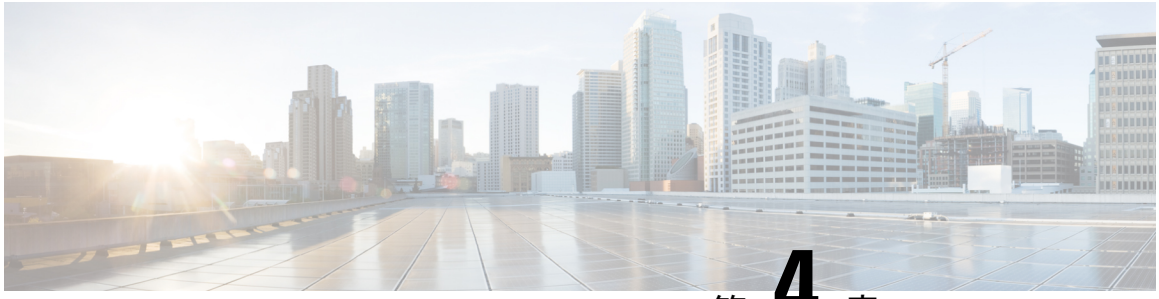
電話でサポート ケースを開く場合は、次のいずれかの電話番号をご利用ください。

- 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 5555

- 米国：1 800 553 2447

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 4 章

HX ストレージ クラスタのモニタリング

- HyperFlex クラスタのモニタリング （41 ページ）
- パフォーマンス チャートの表示 （41 ページ）
- HX Data Platform プラグイン インターフェイスの使用法 （47 ページ）
- HX Connect を使用した HyperFlex クラスタのモニタリング （48 ページ）

HyperFlex クラスタのモニタリング

この章では、HX ストレージクラスタ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 プラグイン
- 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

[パフォーマンスのモニタ（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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [クラスタ（cluster）] > [モニタ（Monitor）] > [パフォーマンス（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（[ストレージ クラスタ（Storage Cluster）]、[ホスト（Hosts）]、および [データストア（Datastores）]）。

ステップ 2 [ストレージ クラスタ（Storage Cluster）] をクリックして、[ストレージ クラスタのパフォーマンス（Storage Cluster Performance）] タブを表示します。

ステップ 3 [時（Hour）]、[日（Day）]、[週（Week）]、[月（Month）]、[最大（Max）]、[カスタム（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]、[スループット（Throughput）]、[遅延（Latency）]、[表示（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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [クラスタ（cluster）] > [モニタ（Monitor）] > [パフォーマンス（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（[ストレージ クラスタ（Storage Cluster）]、[ホスト（Hosts）]、および [データストア（Datastores）]）。

ステップ 2 [ホスト（Hosts）] をクリックして、[ホスト パフォーマンス（hosts performance）] タブを表示します。

ステップ 3 [時（Hour）]、[日（Day）]、[週（Week）]、[月（Month）]、[最大（Max）]、[カスタム（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]、[スループット（Throughput）]、[遅延（Latency）]、[表示（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、[ホスト（*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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [クラスタ（cluster）] > [モニタ（Monitor）] > [パフォーマンス（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（[ストレージ クラスタ（Storage Cluster）]、[ホスト（Hosts）]、および [データストア（Datastores）]）。

ステップ 2 [データストア（Datastores）] をクリックして、[データストア パフォーマンス（datastores performance）] タブを表示します。

ステップ 3 [時（Hour）]、[日（Day）]、[週（Week）]、[月（Month）]、[最大（Max）]、[カスタム（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]、[スループット（Throughput）]、[遅延（Latency）]、[表示（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。

[パフォーマンス（Performance）] ポートレット

[パフォーマンス（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。[パフォーマンス（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、[モニタ（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 インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > **/クラスタ（*cluster*）/** > **[概要（Summary）]** の順に選択します。

ステップ 2 [パフォーマンス（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（Throughput）	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。
現在（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。

[データストアのトレンド（Datastore Trends）] ポートレット

[データストアのトレンド（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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > /クラスタ（*cluster*）/ > [管理（Manage）]** の順に選択します。

ステップ 2 [テーブル（table）] リストから、[データストア（datastore）] を選択します。[概要（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、[トレンド（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
期間	[時（hour）]、[日（days）]、[週（week）]、[月（month）]、[すべて（all）]、または [カスタム（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]、[スループット（Throughput）]、[遅延（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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > /クラスタ（*cluster*）/ > [モニタ（Monitor）] > [パフォーマンス（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（Hour）	過去の時間のパフォーマンスを表示
日（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
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
カスタム（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 インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > **[クラスタ（cluster）]** > **[モニタ（Monitor）]** > **[パフォーマンス（Performance）]** の順に選択します

ステップ 2 [カスタム（Custom）] タブをクリックして、[カスタム範囲（Custom Range）] ダイアログボックスを表示します。

ステップ 3 [カスタム範囲（Custom Range）] ダイアログボックスのメソッドを選択します。

a) [最後（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。

b) 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。

c) [から（From）] をクリックし、[カレンダー（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。

d) [まで（To）] をクリックし、[カレンダー（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 [適用（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]、[スループット（Throughput）]、[遅延（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。

a) vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** > **[モニタ（Monitor）]** > **[パフォーマンス（Performance）]** の順に選択します。

b) [ストレージ クラスタ（Storage Cluster）]、[ホスト（Hosts）]、[データストア（Datastores）] のチャート設定のいずれかをクリックします。[ホスト（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]、[スループット（Throughput）]、[遅延（Latency）] の値を表示しません。

c) 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	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。オプションは次のとおりです。 • IOPS • スループット（Throughput） • 遅延
表示（Show）	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。
Read/Write	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。
Storage Cluster	チャート内のストレージ クラスタ名。
Hosts	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。
Datastores	チャート内のデータストア名。
IOPS Read/Write	1 秒当たりの入出力処理の最新のデータ ポイント。
Throughput Read/Write（Mbps）	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。

フィールド	説明
Latency Read/Write（msec）	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、[遅延（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。

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。

[サマリー（Summary）] タブには、[サマリー（Summary）]エリアと [ポートレット（Portlets）] エリアが表示されます。[サマリー（Summary）] タブのポートレットは、[キャパシティ（Capacity）]、[パフォーマンス（Performance）]、[ステータス（Status）] です。

[モニタ（Monitor）] タブには 2 つのサブタブがあります。

- [パフォーマンス（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 [遅延（Latency）]、[スループット（Throughput）]、および [IOPs] パフォーマンス チャートが表示されます。
- [イベント（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。

[管理（Manage）] タブには 2 つのサブタブがあります。

- [クラスタ（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（[ホスト（Hosts）]、[ディスク（Disks）]、[PSU]、[NIC]）が含まれます。
- [データストア（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、[サマリー（Summary）] タブと [ホスト（Hosts）] タブがあります。[サマリー（Summary）] タブには、[詳細（Details）]、[トレンド（Trends）]、[ディスク使用率の上位 VM（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。

- [ダッシュボード（Dashboard）]：HX ストレージ クラスタ ステータスの概要です。
- [アラーム、イベント、アクティビティ（Alarms, Events, Activity）]：詳細は、Cisco HyperFlex Systems Troubleshooting Guide を参照してください。
- [パフォーマンス（Performance）]：IOPS、スループット、遅延、およびレプリケーション ネットワーク帯域幅のグラフ。
- [システム情報（System Information）]：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（61 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 （64 ページ）を参照してください。

- [データストア（Datastores）]：データストアに関連するステータスおよびタスク。
- [仮想マシン（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。

- [暗号化（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。
- [レプリケーション（Replication）]：ディザスタ リカバリのための VM 保護タスク。

[アップグレード（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。

ダッシュボード ページ

重要 読み取り専用ユーザーには、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 でほとんどの操作を実行するには、管理者権限が必要です。

HX ストレージ クラスタのステータスの概要が表示されます。これは Cisco HyperFlex Connect にログイン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
[動作ステータス（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。 [情報（Information）] をクリックして（ⓘ）HX ストレージ クラスタ名とステータス データにアクセスします。
[復元力ヘルス（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。 [情報（Information）] をクリックして（ⓘ）復元力ステータスと、レプリケーションおよび障害データにアクセスします。
[容量（Capacity）]セクション	ストレージの合計の内訳と、ストレージの使用中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。

UI 要素	基本情報
[ノード（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。
[パフォーマンス（Performance）] セクション	設定可能な時間の HX ストレージ クラスタのパフォーマンス スナップショットを表示し、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、[パフォーマンス（Performance）] ページを参照してください。
[クラスタ タイム（Cluster Time）] フィールド	クラスタのシステムの日付と時間。

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
[更新（Refresh）] フィールドおよびアイコン	HX クラスタ 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。 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。
[フィルタ（Filter）] フィールド	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。 [フィルタ（Filter）] フィールドに選択テキストを入力します。 [フィルタ（Filter）] フィールドを空にするには、[x] をクリックします。 テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックして、フィルタを適用します。

UI 要素	基本情報
[エクスポート（Export）] メニュー	テーブル データの**現在の**ページのコピーを保存します。テーブルの内容は、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。 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。 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。

[アクティビティ（Activity）] ページ

ReadyClone と VM 電源の操作の進捗をモニタするために vSphere から収集された HX ストレージ クラスタ上の最近のアクティビティの一覧が表示されます。

UI 要素	基本情報
[すべて展開（Expand All）] と [すべて折りたたむ（Collapse All）] ボタン	[アクティビティ（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。 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。

UI 要素	基本情報
[アクティビティ（Activity）] リスト	次の詳細を含む最近のタスクの一覧が表示されます。 • ID • 説明 • VM 電源のオン/オフ/一時停止ステータス • タスク ステータス： • **進行中（In Progress）** • **Success** • **失敗しました（Failed）** VM 電源の操作に失敗した場合は、[既存の状態（Existing State）] フィールドと [必要な状態（Required State）] フィールドも含まれます。 • 日時スタンプ • 経過表示バー 展開された [アクティビティ（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。 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。

[システム情報の概要（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 ストレージ クラスタ 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 ストレージ クラスタ ステータス フィールド	• [オンライン（Online）]：クラスタの準備ができています。 • [オフライン（Offline）]：クラスタの準備ができていません。 • [読み取り専用（Read Only）]：クラスタでスペースが不足しています。 • [不明（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 クライアント にアクセスします。
[ハイパーバイザ（Hypervisor）] フィールド	この HX ストレージ クラスタにインストールされているハイパーバイザのバージョンです。
[HXDP バージョン（HXDP Version）] フィールド	この HX ストレージ クラスタにインストールされているインストーラ パッケージのバージョンです。
[データ レプリケーション係数（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。
[稼働時間（Uptime）] フィールド	この HX ストレージ クラスタがオンラインになっている時間の長さです。
[総容量（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。
[使用可能な容量（Available Capacity）] フィールド	このクラスタの空きストレージの容量です。
DNS サーバ（DNS Server(s)）	この HX ストレージ クラスタの DNS サーバの IP アドレスです。
NTP サーバ（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、[ノード（Nodes）] ページに移動します。

UI 要素	基本情報
[ノード（Node）] フィールド	このクラスタ上のノードの名前です。
[モデル（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。
[ディスク（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の数です。
[ノードのステータス（Node status）] フィールド	• **Online** • **オフライン** • **メンテナンス中** • **正常** • **警告**
[HXDP バージョン（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。
[タイプ（Type）] フィールド	• **ハイパーコンバージド** • **コンピューティング**
[ハイパーバイザ ステータス（Hypervisor Status）] フィールド	• **Online** • **オフライン** • **メンテナンス中** • **進行中（In Progress）**
[ハイパーバイザ アドレス（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は、次のポップアップデータに含まれます。

表 *5:* ディスクのキャッシュ

UI 要素	基本情報
[スロット番号（Slot Number）] フィールド	ドライブの場所です。
[シリアル番号（Serial Number）] フィールド	このディスクの物理シリアル番号です。

UI 要素	基本情報
[ディスクの状態（Disk State）] フィールド	• 待受開始（Ready）
[容量（Capacity）] フィールド	ディスク サイズの合計です。
[ロケータ LED（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 *6 :* 永続ディスク

UI 要素	基本情報
[スロット番号（Slot Number）] フィールド	ドライブの場所です。
[シリアル番号（Serial Number）] フィールド	このディスクの物理シリアル番号です。
[ディスクの状態（Disk State）] フィールド	• 待受開始（Ready） • ブラックリスト • 削除対象
[使用済み容量 / 総容量（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。
[ストレージ使用率（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（Locator 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。

[ノード（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
[HX メンテナンス モードを開始（Enter HX Maintenance Mode）] ボタン	このボタンにアクセスするノードを選択します。 [HX メンテナンス モードを確認（Confirm HX Maintenance Mode）] ダイアログ ボックスを開きます。

UI 要素	基本情報
[HX メンテナンス モードを終了（Exit HX Maintenance Mode）] ボタン	このボタンにアクセスするノードを選択します。 すべての保守タスクを完了した後、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。
[ノード（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。
[ハイパーバイザ アドレス（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。
[ハイパーバイザの状態（Hypervisor Status）] カラム	• **Online** • **オフライン** • **メンテナンス中** • **進行中（In Progress）**
[コントローラ アドレス（Controller Address）] カラム	HX ストレージ コントローラ VM の IP アドレス。
[コントローラの状態（Controller Status）] カラム	• **Online** • **オフライン** • **メンテナンス中**
[モデル（Model）] カラム	このノードの物理ハードウェアのモデル番号です。
[バージョン（Version）] カラム	このノードにインストールされている HyperFlex Data Platform インストーラ パッケージのバージョンです。
[ディスク（Disks）] カラム	ノード内のディスクの数です。 選択したノード名でフィルター処理した [ディスク（Disks）] ページを開くには数をクリックします。

[ディスク（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。

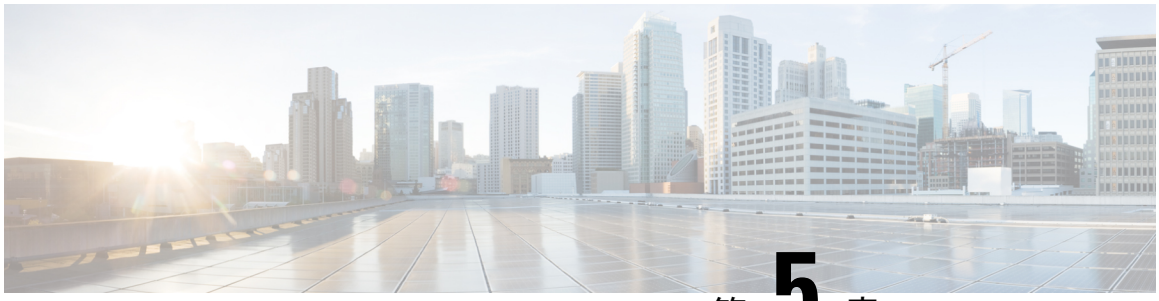
UI 要素	基本情報
[ノード（Node）] カラム	ディスクが存在するノードの名前です。
[スロット（Slot）] カラム	SED ドライブの場所です。これは保守作業のためのドライブを識別します。

UI 要素	基本情報
[容量（Capacity）] カラム	ディスク サイズの合計です。

UI 要素	基本情報	
[ステータス（Status）] カラム		次の状態は無視できます。 • **無効（Invalid）** • **標準** • [削除済み（Removed）] : [安全に消去する（Secure Erase）] オプションを使用した後に SED ディスクを削除するときの状態です。 • **時間切れ（Time out）** • **不明**

UI 要素	基本情報	
	• [利用可能（Available）]：新しく追加された、保管中データ対応のディスクの初期の状態です。 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。 • [ブラックリスト（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、[修復（Repairing）] の状態に移行する前に、クラスタがディスクを修復しようとする移行状態である可能性があります。 • [要求（Claimed）]：ディスクが認識され、使用中の状態です。 • [無視（Ignored）]：ディスクがクラスタによって使用されていない状態です。たとえば、HX コントローラ VM システム ディスク、他のデータ（有効なファイル システム パーティション）を含むディスク、または I/O の障害が発生しているディスクです。 • [削除 OK（Ok To Remove）]：SEDディスクが [安全に消去する（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、[削除 OK（Ok To Remove）] の状態になったディスクは、クラスタから使用されません。	

UI 要素	基本情報
	• [修復（Repairing）]：ブラックリスト登録済みディスクが現在修復されている状態です。 • [削除対象（To Be Removed）]：ディスクがRMAにスケジュールされているときの状態です。
[暗号化（Encrypted）] 列	• [有功（Enabled）]：この保管中データ対応ディスクの暗号化が設定されています。 • [無効（Disabled）]：この保管中データ対応ディスクの暗号化は設定されていません。 これは、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。 • **ロック（Locked）** • **不明**
[タイプ（Type）] カラム	• **不明** • [回転（Rotational）]：ハイブリッド ドライブ • [ソリッド ステート（Solid State）]：SSD ドライブ
[使用率（Usage）] カラム	• **不明** • **キャッシュ** • **永久的（Persistent）**
[ロケータ LED をオンにする（Turn On Locator LED）] と [ロケータ LED をオフにする（Turn Off Locator LED）] ラジオ ボタン	ラジオ ボタンにアクセスするディスクを選択します。 ディスクを探すために役立つホスト上の物理光またはビーコンを、アクティブ化または非アクティブ化します。
（省略可能）[安全に消去する（Secure Erase）] ボタン	このボタンは、HXストレージクラスタがローカル キー暗号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。 ボタンにアクセスするディスクを選択します。 クラスタで使用中の暗号化キーを入力し、[安全に消去する（Secure Erase）] をクリックしてから [はい、このディスクを消去します（Yes, erase this disk）] をクリックし、ローカルの暗号化キーを安全に消去します。



第 5 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 （61 ページ）
- シリアル操作とパラレル操作 （63 ページ）
- クラスタ ステータスの確認 （64 ページ）
- ビーコンの設定 （64 ページ）
- HX クラスタの vMotion の設定の確認 （65 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 （66 ページ）
- Cisco HyperFlex のメンテナンス モードの開始 （67 ページ）
- Cisco HyperFlex のメンテナンス モードの終了 （69 ページ）
- バックアップ操作の作成 （70 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 （75 ページ）
- HX ストレージ クラスタの電源オンと起動 （78 ページ）
- vNIC または vHBA の変更後の PCI パススルーの設定 （80 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 モードで実行するとき、これは Cisco HX Data Platform がオフラインで、ストレージ コントローラ VM は稼働中で、Cisco HX Data Platform 管理は、stcli コマンド ライン、HX Connect、および HX Data Platform プラグイン を介して表示可能であることを意味します。vSphere Web クライアントは、ストレージ I/O 層について報告できます。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 プラグイン のビーコン 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 120 GB SSD には使用できません。サーバでハウスキーピング SSD の物理的な位置を確認します。

- 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。

メンテナンス後のタスク

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動している。
- 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）とディスクの検索および特定を支援するために LED をオンにするメソッドです。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 LED ビーコンがあります。

Cisco UCS Manager でノード ビーコンを設定します。HX Data Platform プラグイン または HX Connect のユーザ インターフェイスを介してディスク ビーコンを設定します。

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

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

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

c) サーバが見つかったら、ロケータ LED をオフにします。

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

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

a) vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** > **[管理（Manage）]** の順に選択します。
b) [管理（Manage）] タブで、**[クラスタ（Cluster）]** > ***[クラスタ（cluster）]*** > ***[ホスト（host）]*** > **[ディスク（Disks）]** > ***[ディスク（disk）]*** を選択します。
c) オブジェクトの物理的な場所を探して、ビーコンをオンにします。

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

d) ディスクが見つかったら、ビーコンをオフにします。

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

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

a) HX Connect にログインします。
b) **[システム情報（System Information）]** > **[ディスク（Disks）]** の順に選択します。
c) ノードを選択し、[ロケータ LED をオンにする（Turn On Locator LED）] または [ロケータ LED をオフにする（Turn Off Locator LED）] をクリックします。

ハウスキーピング SSD と キャッシュ NVMe SSD を除いて、選択されているノード上のすべてのディスクのビーコン LED を切り替えます。ハウスキーピング SSD またはキャッシュ NVMe SSD には、LED ビーコンの機能はありません。

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. vMotion ポート グループが 9000 MTU に設定されており、VLAN ID が 0 に設定されていることを設定で確認します。

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 10.104.0.20` と入力します

7. vmotion vNICS に関連付けられた CDP 情報を表示して、適切な VLAN がファブリック インターコネクトから割り当てられていることを確認してください。

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 **/ホスト（*host*）/** を選択してから、メニューを右クリックして [メンテナンス モード（maintenance mode）] を選択します。
- ESX コマンド ラインで 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） レプリケーション構成がある場合は、アップグレードや拡張、またはクラスタの保守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。このローカルの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、一時停止および再開を行います。

HX ストレージ クラスタ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ます。

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

（注） すべての保守タスクを完了した後、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 Web クライアントにログインします。
2. [ホーム（Home）] > [ホストおよびクラスタ（Hosts and Clusters）] に移動します。
3. [HX クラスタ（HX Cluster）] が含まれている [データセンター（Datacenter）] を展開します。
4. [HX クラスタ（HX Cluster）] を展開し、ノードを選択します。
5. ノードを右クリックし、[Cisco HX メンテナンス モード（Cisco HX Maintenance Mode）] > [HX メンテナンス モードの開始（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 **[モニタ（Monitor）]** > **[タスク（Tasks）]** タブで [メンテナンス モードの開始（Enter Maintenance Mode）] タスクの進行状況をモニタできます。

操作が失敗すると、エラー メッセージが表示されます。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） レプリケーション構成がある場合は、アップグレードや拡張、またはクラスタの保守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、またはクラスタの保守が完了した後、レプリケーションを再開します。このローカルの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、一時停止および再開を行います。

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ます。

1. HX Connect へのログイン：*https://<cluster management ip>*。
2. メニューで [システム情報（System Information）] をクリックします。
3. [ノード（Nodes）] をクリックし、メンテナンス モードから削除するノードの行をクリックします。
4. [HX メンテナンス モードの終了（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. [ホーム（Home）] > [ホストおよびクラスタ（Hosts and Clusters）] に移動します。
3. [HX クラスタ（HX Cluster）] が含まれている [データセンター（Datacenter）] を展開します。
4. [HX クラスタ（HX Cluster）] を展開し、ノードを選択します。
5. ノードを右クリックして、[Cisco HX メンテナンス モード（Cisco HX Maintenance Mode）] > [HX メンテナンス モードの終了（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 **[モニタ（Monitor）]** > **[タスク（Tasks）]** タブで [メンテナンス モードの終了（Exit Maintenance Mode）] タスクの進行状況をモニタできます。

操作が失敗すると、エラー メッセージが表示されます。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 [ナビゲーション（Navigation）] ペインで [管理（Admin）] をクリックします。

ステップ 2 [すべて（All）] ノードをクリックします。

ステップ 3 [ワーク（Work）] ウィンドウで、[一般（General）] タブをクリックします。

ステップ 4 [アクション（Actions）] 領域の [バックアップ設定（Backup Configuration）] をクリックします。

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

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

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

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

[名前（Name）]	説明
[アイデンティティの保存（Preserve Identities）] チェックボックス	このチェックボックスは、バックアップ操作の [すべての設定（All configuration）] および [システム設定（System Configuration）] タイプで選択されたままになり、次の機能が提供されます。 • [すべての設定（All configuration）]：vHBA、WWPN、WWNN、vNIC、MAC、UUID などのプールから取得したすべての ID がバックアップ ファイルに保持されます。また、シャーシ、FEX、ラック サーバの ID と、シャーシ、FEX、ラック サーバ、IOM、ブレード サーバのユーザ ラベルも保持されます。 （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。 • [システム設定（System Configuration）]：シャーシ、FEX、ラック サーバの ID と、シャーシ、FEX、ラック サーバ、IOM、ブレードサーバのユーザ ラベルがバックアップ ファイルに保持されます。 （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。 このチェックボックスがバックアップ操作の [論理設定（Logical Configuration）] で選択されている場合は、vHBA、WWPN、WWNN、vNIC、MAC、UUID などのプールから取得したすべての ID がバックアップ ファイルに保持されます。 （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。
[バックアップ ファイルの場所（Location of the Backup File）] フィールド	バックアップ ファイルの保存場所。次のいずれかになります。 • [リモート ファイル システム（Remote File System）]：バックアップ XML ファイルはリモート サーバに保存されます。Cisco UCS Manager GUI によって次に示すフィールドが表示され、リモート システムのプロトコル、ホスト、ファイル名、ユーザ名、パスワードを指定できます。 • [ローカル ファイル システム（Local File System）]：バックアップ XML ファイルはローカルに保存されます。 HTML ベースの Cisco UCS Manager GUIには、[ファイル名（Filename）] フィールドが表示されます。バックアップ ファイルの名前を ***<filename>*.xml** 形式で入力します。ファイルがダウンロードされ、ブラウザの設定に応じた場所に保存されます。

[名前（Name）]	説明
[プロトコル（Protocol）] フィールド	リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。 • **FTP** • **TFTP** • **SCP** • **SFTP** • [USB A]：ファブリック インターコネクト A に挿入された USB ドライブ。 このオプションは特定のシステム設定でしか使用できません。 • [USB B]：ファブリック インターコネクト B に挿入された USB ドライブ。 このオプションは特定のシステム設定でしか使用できません。
[ホスト名（Hostname）] フィールド	バックアップ ファイルが格納されている場所のホスト名または IP アドレス（IPv4 または IPv6）。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。 （注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が **[グローバル（global）]** に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[リモート ファイル（Remote File）] フィールド	バックアップ設定ファイルのフル パス。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
[ユーザ（User）] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。

[名前（Name）]	説明
[パスワード（Password）] フィールド	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。 Cisco UCS Manager ではこのパスワードは保存されません。そのため、バックアップ操作をすぐに有効にして、実行する予定がない限り、このパスワードを入力する必要はありません。

ステップ 7 **[OK]** をクリックします。

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

[管理状態（Administrative 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。[バックアップ設定（Backup Configuration）] ダイアログボックスの [バックアップ操作（Backup Operations）] テーブルに、バックアップ操作が表示されます。

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

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

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

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

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

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

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 （70 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、「次にやるべきこと：」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（`stCtlVM`）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、**[電源（Power）] > [電源オフ（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、**[電源（Power）] > [電源オフ（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、**[メンテナンス モード（Maintenance Mode）] > [メンテナンスモードの開始（Enter Maintenance Mode）]** 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、**[電源（Power）] > [シャットダウン（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 インターコネクト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 インターコネクトには電源ボタンが付いていません。

Cisco UCS ファブリック インターコネクト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。
   - アップグレードのタスクについては、*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 （78 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 （75 ページ）の手順を実行します。

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 インターコネクト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 インターコネクトにログインします。
2. 次のコマンドを発行します。

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

ステップ 2 すべての ESX ホストを FI に接続します。

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

   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。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（`stCtlVM`）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、**[電源（Power）] > [電源オン（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。

ESXi 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) stCtlVM 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 設定（DirectPath I/O Configuration）] ページを選択します。

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

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

ステップ 5 パススルー用の LSI カードを選択します。

a) [DirectPath I/O 設定（DirectPath I/O Configuration）] ページから、[パススルーの設定（Configure Passthrough）] を選択します。

b) [パススルー用のデバイスをマーク（Mark devices for passthrough）] リストから、パススルー用の LSI カードを選択します。

c) **[OK]** をクリックします。

ステップ 6 ESX ホストをリブートします。

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

a) 不明な PCI デバイスを見つけて削除します。

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

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

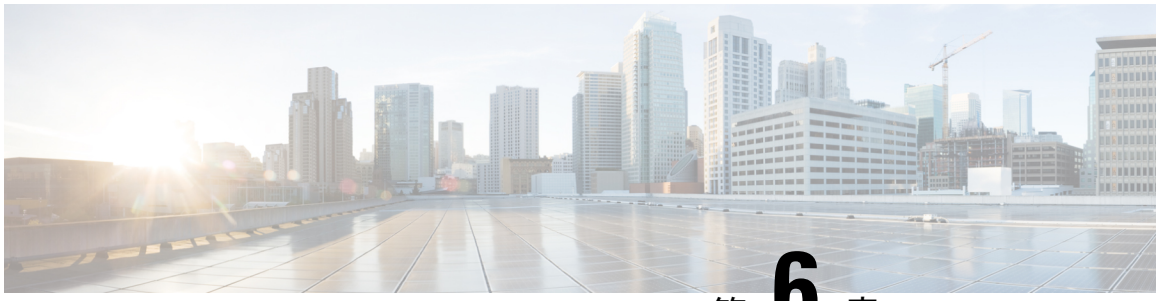
b) LSI ロジック PCI デバイスを見つけて追加し直します。

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

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

ステップ 8 HX メンテナンス モードから ESX ホストを削除します。

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 6 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 （83 ページ）
- クラスタの再調整 （83 ページ）
- スペース不足エラーの処理 （85 ページ）
- ストレージ クラスタの vCenter 間の移動計画 （86 ページ）
- クラスタの名前の変更 （91 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 インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > ***[クラスタ（cluster）]*** > **[概要（Summary）]** の順に選択します。

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

[自己修復の状態（Self healing status）] フィールドには、再調整アクティビティまたは N/A（再調整が現在アクティブではない場合）が示されます。

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

a) `ssh` を使用してコントローラ VM にログインします。

b) コントローラ VM 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 [最近のタスク（Recent Tasks）] タブに、ステータス メッセージが表示されます。

スペース不足エラーの処理

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

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

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

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

ステップ 2 未使用の VM を削除するには、次の手順を実行します。

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

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

c) 削除する VM をダブルクリックします。

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

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

f) VM の電源をオフにします。

g) VM を削除します。

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

a) **[vCenter]** > **[仮想マシン（Virtual Machines）]** に移動して、インベントリ内の VM を表示します。
b) 使用する VM をダブルクリックします。
c) **[概要（Summary）]** > **[質問に回答（Answer Questions）]** をクリックしてダイアログボックスを表示します。
d) [再試行（Retry）] オプション ボタンをクリックして、[OK] をクリックします。

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。

`cleaner` 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

ストレージ クラスタの vCenter 間の移動計画

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

ストレージ クラスタを 1 つの vCenter クラスタから移動するには、リストされている手順が必要です。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 （87 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 （87 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 （88 ページ）
4. stcli cluster reregister コマンドを使用して HX ストレージ クラスタ 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 （90 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 クラスタ が 1.8(1c) より古い HX Data Platform のバージョンを実行している場合は、新しい vCenter の再登録を試行する前にアップグレードします。
- このタスクは、メンテナンス ウィンドウが表示されている間に実行します
- クラスタが正常でありアップグレードの状態が [OK] で正常であること確認します。コントローラ VM のコマンド ラインから stcli コマンドを使用して状態を表示できます。

  # **stcli cluster info**

  次の応答を確認します。

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

- VCenter が起動し実行中であることを確認します。
- vCenterクラスタ間でストレージ クラスタを移動する場合、スナップショット スケジュールはストレージ クラスタと共に移動しません。

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 クラスタが作成されたときに指定された vCenter クラスタです。

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

ステップ 3 新しく作成されたクラスタ内の新しい 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 （88 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

このステップは省略可能であり、必要ありません。そのまま古い vCenter の HX Data Platform プラグイン の登録だけにすることをお勧めします。

始める前に

ある vCenter サーバと別の vCenter との間でストレージ 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 （87 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 クラスタが異なる vCenter に完全移行されるまでこの手順を試みないでください。この手順を実行すると、vCenter に登録されている既存の HX クラスタには障害になります。

ステップ 1 古い vCenter サーバ MOB 拡張マネージャにログインします。

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&doPath=extensionList
```

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

b) 管理者用のログイン クレデンシャルを入力します。

ステップ 2 リストをスクロールして、HX Data Platform の拡張機能を探します。

```
com.springpath.sysmgmt and com.springpath.sysmgmt.uuid.
```

（注） HyperFlex クラスタが複数ある場合は、登録を解除する正しいクラスタ ID を選択することを確認します。クラスタ ID を表示するには、コントローラ VM にログインしてコマンドを実行します。

```
# show cluster info
```

ステップ 3 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 各拡張文字列の登録を解除します。

a) ページを下にスクロールして、[UnregisterExtension] をクリックします。

b) 1 つの拡張文字列をフィールドに貼り付け、[メソッドの呼び出し（Invoke Method）] をクリックします。

c) 他の文字列についても同じ手順を繰り返します。

ステップ 5 vSphere クライアント サービスを再起動します。

vSphere クライアント サービスが再起動されると、HX Data Platform の拡張機能が削除されます。vSphere クライアント サービスを再起動すると、ブラウザを介した vCenter へのアクセスが一時的に無効になります。

追加情報については、VMware のナレッジ ベース『Stopping, starting, or restarting VMware vCenter Server Appliance 6.0 services（2109887）』を参照してください。

ステップ 6 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 を使用している Linux vCenter サーバにログインします。
b) HX Data Platform プラグイン フォルダを含む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 プラグイン 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) 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 プラグイン フォルダを含む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 プラグイン フォルダとファイルを削除します。

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

d) [サービス（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
```

ステップ 7 HX クラスタがもう古い vCenter 上ではないことを確認します。

a) 古い vCenter からログアウトします。
b) 古い vCenter に再びログインし、HX Data Platform プラグイン が削除されていることを確認します。

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 （90 ページ）に進みます。

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 （88 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-sso-url NEWVCENTERSSOURL] --vcenter-user NEWVCENTERUSER [--vcenter-password NEWVCENTERPASSWORD]

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-url NEWVCENTERURL	必須作業です。	新しい vCenter の URL、<*vcentername*>。<*vcentername*> には、FQDN または IP アドレスを指定できます。
--vcenter-user NEWVCENTERUSER	必須作業です。	新しい vCenter 管理者のユーザ名。
--vcenter-cluster NEWVCENTERCLUSTER	必須作業です。	新しい vCenter クラスタの名前。
--vcenter-datacenter NEWDATACENTER	必須作業です。	新しい vCenter データセンターの名前。
--vcenter-password NEWVCENTERPASSWORD	これはオプションです。	新しい vCenter 管理者のパスワード。
--vcenter-sso-url NEWVCENTERSSOURL	これはオプションです。	新しい vCenter SSO サーバの URL。これを指定しない場合は、`--vcenter-url` から推論されます。

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。

クラスタの名前の変更

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、vCenter クラスタではなく、HX クラスタ の名前の変更に適用されます。

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

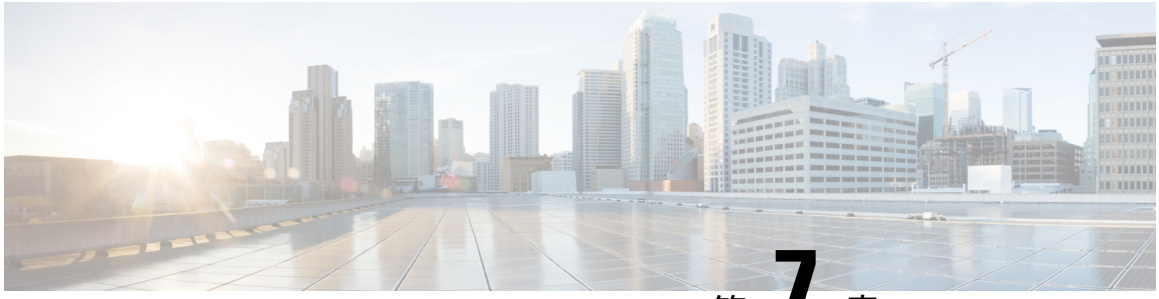
ステップ 2 [クラスタの名前変更（Rename Cluster）] ダイアログボックスを開きます。ストレージ クラスタを右クリックするか、またはタブ上部にある [操作（Actions）] ドロップダウンリストをクリックします。

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

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

HX クラスタ名は 50 文字を超えることができません。

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 7 章

暗号化の管理

- 自己暗号化ドライブの概要 （93 ページ）
- HyperFlex クラスタが暗号化できることの確認 （94 ページ）
- ローカル暗号化キーの構成 （94 ページ）
- ローカル暗号化キーの変更 （95 ページ）
- ローカルの暗号化キーの無効化 （96 ページ）
- 暗号化されたディスクを安全に消去する （96 ページ）
- リモート キー管理 （97 ページ）
- リモート暗号化キーの構成 （97 ページ）
- 証明書署名要求の生成 （98 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 （99 ページ）
- 自己署名証明書の生成 （101 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 （102 ページ）
- 暗号化のやり直し （103 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、発信データを復号化する特別なハードウェアが含まれています。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。メディアの暗号化キーは、データ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 キーを構成するときは、キーを忘れないでください。キーを忘れた場合、回復できず、ドライブの電源が再投入されるとデータは失われます。キーは、キー管理サーバ（KMIP サーバとも呼ばれます）を使用してリモートで構成できます。この方法は、ローカル管理のキーの保管および回復に関連する問題に対処します。

SED の復号化と暗号化はハードウェアを介して行われます。したがって、システム全体のパフォーマンスに影響しません。SED は、瞬時暗号化消去によりディスクのリタイアメントと再デプロイメントコストを削減します。暗号化消去はメディア暗号化キーを変更することによって行われます。ディスクのメディア暗号化キーを変更すると、ディスク上のデータは復号化できず、すぐに使用できなくなります。

HyperFlex クラスタが暗号化できることの確認

HX Data Platform プラグイン を使用して確認します

1. HX Data Platform プラグイン から vSphere Web クライアント にログインします。
2. **[Cisco HX Data Platform]** > **[hx_cluster]** > **[概要（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、[概要（Summary）] タブの上部に [保管中のデータの暗号化可能（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いることを確認します

1. HX Connect UI から、[暗号化（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、[暗号化（Encryption）] ページに [保管中のデータの暗号化対応可（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、[暗号化（Encryption）] を選択します。

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

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

UI 要素	基本情報
[UCS Manager のホスト名（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*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[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、[ローカルキー（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 [暗号化を有効にする（Enable Encryption）] をクリックします。

ローカル暗号化キーの変更

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

ステップ 2 [暗号化（Encryption）] ページで、[再キー（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 のホスト名（UCS Manager host name）] フィールド	例：*10.193.211.120*。
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名。
[パスワード（Password）] フィールド	<*root*> パスワード。

[Next] をクリックします。

ステップ 4 クラスタの [既存の暗号化キー（Existing Encryption Key）] と [新しい暗号化キー（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 [再キー（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、[暗号化（Encryption）] を選択します。

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

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

UI 要素	基本情報
[UCS Manager のホスト名（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*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

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

ステップ 6 クラスタで暗号化キーを無効にすることを確認するために [暗号化を無効にしますか？（Disable encryption?）] ダイアログ ボックスで、[はい（Yes）] 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、[システム情報（System Information）] を選択します。

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

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

ステップ 4 クラスタ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 [安全に消去する（Secure erase）] をクリックします。

ステップ 6 [このディスクを消去しますか?（Erase this disk?）] ダイアログ ボックスで、[はい、このディスクを消去します（Yes, erase this disk）] をクリックし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、設定でローカルの証明機関を指定し、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は、『HyperFlex Encryption and SafeNet Key Management TechNote』と『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。

リモート暗号化キーの構成

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

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

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

UI 要素	基本情報
[UCS Manager のホスト名（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*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[Next] をクリックします。

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

次の証明書の 1 つを使用するためにクラスタ内の自己暗号化ドライブを持つサーバを構成できます。

- [証明機関署名付きの証明書を使用する（Use certificate authority signed certificates）]：外部証明機関によって署名された証明書署名要求（CSR）を生成します。
- [自己署名の証明書を使用する（Use self-signed certificates）]：自己署名の証明書を生成します。

[Next] をクリックします。

ステップ 5

次のタスク

証明書署名要求または自己署名の証明書を生成できます。

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、[暗号化（Encryption）] を選択します。

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

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

UI 要素	基本情報
[UCS Manager のホスト名（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*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[Next] をクリックします。

ステップ 4 [キー管理サーバ（Key Management Server）] > [証明機関署名の証明書を使用する（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）サーバを構成するリモート暗号化キーを生成するには、次の詳細を完了します。

UI 要素	基本情報
[電子メール アドレス（Email address）] フィールド	<*admin*> 電子メール アドレス
[組織名（Organization name）] フィールド	証明書を要求している組織。 32 文字以内で入力します。
[組織ユニット名（Organization unit name）] フィールド	組織ユニット。 64 文字以内で入力します。
[地域（Locality）] フィールド	証明書を要求している会社の本社が存在する市または町。 32 文字以内で入力します。
[状態（State）] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以内で入力します。
[国（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。
[有効な日数（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、[証明書の生成（Generate certificates）] をクリックします。

ステップ 7 証明書をダウンロードして、証明機関によって署名された証明書を取得します。[閉じる（Close）] をクリックします。

次のタスク

1. 署名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。

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、それが証明機関によって署名され、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、[暗号化（Encryption）] を選択します。

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

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

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

UI 要素	基本情報
[UCS Manager のホスト名（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*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[Next] をクリックします。

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

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

ステップ 7 [構成の続行（Continue configuration）] ドロップダウン リストから [キー管理サーバ の構成（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 キー管理サーバ（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
[プライマリ キー管理サーバ（Primary key management server）] フィールド	プライマリ キー管理サーバの IP アドレスを入力します。
（省略可能）[セカンダリ キー管理サーバ（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。
[ポート番号（Port Number）] フィールド	キー管理サーバに使用するポート番号を入力します。
[公開キー（Public key）] フィールド	KMIP サーバ構成中に生成された証明書機関の公開ルート証明書を入力します。

ステップ 9 [保存（Save）] をクリックし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、[暗号化（Encryption）] を選択します。

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

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

UI 要素	基本情報
[UCS Manager のホスト名（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*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[Next] をクリックします。

ステップ 4 [キー管理サーバ（Key Management Server）] > [自己署名の証明書を使用する（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）サーバを構成するリモート暗号化キーを生成するには、次の詳細を完了します。

UI 要素	基本情報
[電子メール アドレス（Email address）] フィールド	<*admin*> 電子メール アドレス
[組織名（Organization name）] フィールド	証明書を要求している組織。 32 文字以内で入力します。
[組織ユニット名（Organization unit name）] フィールド	組織ユニット。 64 文字以内で入力します。
[地域（Locality）] フィールド	証明書を要求している会社の本社が存在する市または町。 32 文字以内で入力します。

UI 要素	基本情報
[状態（State）] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 32 文字以内で入力します。
[国（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。
[有効な日数（Valid for (days)）] フィールド	証明書の有効期間。

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

ステップ 7 証明書をダウンロードして、証明機関によって署名された証明書を取得します。[閉じる（Close）] をクリックします。

次のタスク

1. 署名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、[暗号化（Encryption）] を選択します。

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

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

ステップ 4 次の Cisco UCS Manager 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
[UCS Manager のホスト名（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*>
[ユーザ名（User name）] フィールド	<*admin*> ユーザ名
[パスワード（Password）] フィールド	<*root*> パスワード

[Next] をクリックします。

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

UI 要素	基本情報
[プライマリ キー管理サーバ（Primary key management server）] フィールド	プライマリ キー管理サーバの IP アドレスを入力します。
（省略可能）[セカンダリ キー管理サーバ（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。
[ポート番号（Port Number）] フィールド	キー管理サーバに使用するポート番号を入力します。
[公開キー（Public key）] フィールド	KMIP サーバ構成中に生成された証明書機関の公開ルート証明書を入力します。

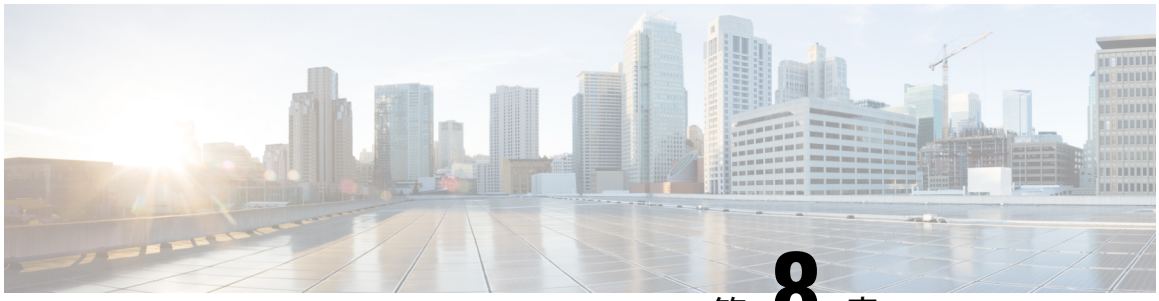
ステップ 6 [保存（Save）] をクリックしてクラスタをリモート管理キーで暗号化します。

暗号化のやり直し

Cisco UCS Manager のクレデンシャルを入力して、HyperFlex クラスタを安全に暗号化するための、キー管理サーバまたは ローカル キーの構成を再起動します。

UI 要素	基本情報
[UCS Manager のホスト名（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*>

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



第 8 章

データストアの管理

- データストアの管理 （105 ページ）
- データストアの追加 （106 ページ）
- データストアの編集 （107 ページ）
- データストアのマウント （107 ページ）
- データストアのマウント解除 （108 ページ）
- データストアの削除 （109 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 （109 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が使用す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 プラグイン 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 インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > **/クラスタ（*cluster*）/** > **[管理（Manage）]** > **[データストア（Datastores）]** の順に選択します。
- HX Connect から、[データストア（Datastores）] を選択します。

ステップ 2 新規作成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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > /クラスタ（*cluster*）/ > [管理（Manage）] > [データストア（Datastores）]** の順に選択します。
- HX Connect から、[データストア（Datastores）] を選択します。

ステップ 2 [データストアの作成（create datastore）] を選択します。

ステップ 3 データストアの名前を入力します。vSphere Web クライアントでは、データストア名に 42 文字の制限があります。各データストアに固有の名前を割り当てます。

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 プラグイン 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 4 k です。

ステップ 6 [OK] をクリックして変更を確定するか、[キャンセル（Cancel）] をクリックして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。新しいデータストアを表示するために必要な場合は、[更新（Refresh）] アイコンをクリックします。

HX Data Platform プラグイン から、**[管理（Manage）] > [データストア（Datastores）] > [ホスト（Hosts）]** タブをクリックして、新しいデータストアのマウント状態を確認します。

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、[ホスト（Hosts）] > [構成（Configuration）] > [データストア（Datastores）] で、[ドライブの種類（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 Data Platform プラグイン データストアでは、名前の変更ができ、編集（ペンシル）オプションを使用して、ストレージの割り当てを変更できます。

（注） コントローラ VM を使用してデータストアの名前を変更しないでください。

ステップ 1 インターフェイスを選択します。

- vSphere Web クライアント ナビゲータから、**[vCenter インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > **/クラスタ（*cluster*）/** > **[管理（Manage）]** > **[データストア（Datastores）]** の順に選択します。
- HX Connect から、[データストア（Datastores）] を選択します。

ステップ 2 [データストア（*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がありません。このステップをスキップします。

ステップ 4 [編集（Edit）] データストアをクリックします。

ステップ 5 データストアの名前を変更して、必要に応じて他の編集を適用します。**[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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > /クラスタ（*cluster*）/ > [管理（Manage）] > [データストア（Datastores）]** の順に選択します。
- HX Connect から、[データストア（Datastores）] を選択します。

ステップ 2 [データストア（*datastore*）] を選択します。

ステップ 3 [マウント（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 インベントリ リスト（vCenter Inventory Lists）] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > /クラスタ（*cluster*）/ > [管理（Manage）] > [データストア（Datastores）]** の順に選択します。
- HX Connect から、[データストア（Datastores）] を選択します。

ステップ 2 [データストア（*datastore*）] を選択します。

ステップ 3 [マウント解除（Unmount）] をクリックします。

ステップ 4 データストアのマウント解除を確認し、[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 のいずれかまたは CLI を介して、マウント解除するか削除します。

b) UI または CLI を使用してデータストアを再マウントします。

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 インベントリ リスト（vCenter Inventory Lists）]** > **[Cisco HyperFlex Systems]** > **[Cisco HX Data Platform]** > **/クラスタ（*cluster*）/** > **[管理（Manage）]** > **[データストア（Datastores）]** の順に選択します。
- HX Connect から、[データストア（Datastores）] を選択します。

ステップ 2 [データストア（*datastore*）] を選択します。

ステップ 3 [削除（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 プラグイン の UI または CLI を介して、データストアのマウント、マウント解除、または削除を試みます。

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
```

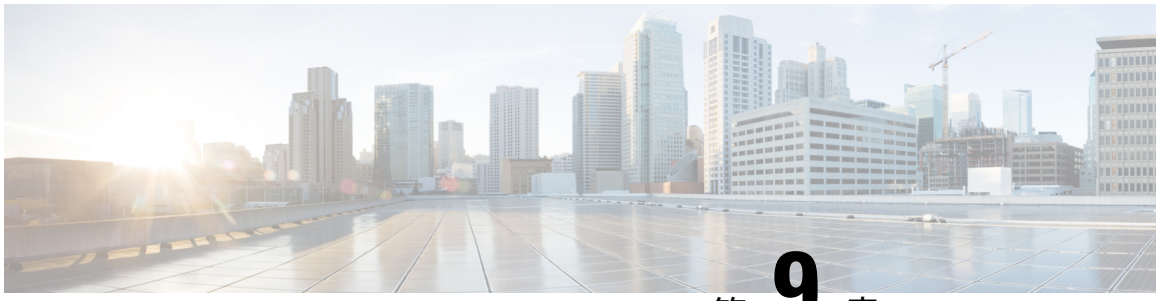
d) `storagerm` サービスを停止します。

```
# /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 9 章

ディスクの管理

- クラスタ内のディスクの管理 （111 ページ）
- ディスクの要件 （112 ページ）
- 自己暗号化ドライブ（SED）の交換 （115 ページ）
- SSD の交換 （117 ページ）
- NVMe SSD の交換 （119 ページ）
- ハウスキーピング SSD の交換 （120 ページ）
- ハードディスク ドライブの交換または追加 （122 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ド 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クラスタ概要情報に表示され続ける場合があります。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。CPUのサイズを大きくするには、コンピューティング専用ノードを追加できます。ソリッドステート ディスク（SSD）のみが搭載されたサーバーは、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り、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 SAS ディスクは、すべてパススルー 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。

- 発注ツールにおいて利用可能なディスクのみがサポートされます。
- オールフラッシュの場合、HXAF240 ノードでは最大 23 台のドライブが Cisco HyperFlex でサポートされます。

コンバージド ノード

次の表に示すディスクに加えて、すべてのコンバージド ノードには、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。

（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 ディスクまたは永続ディスクを交換する際は、元のディスクと同じタイプとサイズを常に使用します。
- 異なるタイプのストレージ ドライブを混在させないでください。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 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。
- キャッシュ NVMe と非 NVMe ドライブ タイプをサーバで混在させないでください。キャッシュ用にすべて NVMe SSD、またはすべて非 NVMe SSD を使用します。

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。SSD を混在させないでください。

HX240 サーバ

サーバ タイプ（Server Type）	ハウスキーピング	キャッシュ（前面）	永続（前面）
HXAF240C M4 SED オールフラッシュ 保管中のデータの暗号化可能	1 X 120 GB SATA SSD（前面） または 1 X 240 GB SATA SSD（前面）	1 X 800 GB SAS SSD	6 ～ 10 X 800 GB SAS SSD
HXAF240C M4SX オールフラッシュ	1 X 120 GB SATA SSD（背面） または 1 X 240 GB SATA SSD（背面）	1 X 400 GB SAS SSD	6 ～ 10 X 3.8 TB SATA SSD または 6 ～ 10 X 960 GB SATA SSD
HX240C M4 SED ハイブリッド 保管中のデータの暗号化可能	1 X 120 GB SATA SSD（前面） または 1 X 240 GB SATA SSD（前面）	1 X 1.6 TB SAS SSD	6 ～ 22 X 1.2 TB SAS HDD

サーバ タイプ（**Server Type**）	ハウスキーピング	キャッシュ（前面）	永続（前面）
HX240C M4 ハイブリッド	1 X 120 GB SATA SSD（背面） または 1 X 240 GB SATA SSD（背面）	1 X 1.6 TB SATA SSD	6 ～ 23 X 1.2 TB SAS HDD

HX 220 サーバ

サーバとタイプ	ハウスキーピング（前面）	キャッシュ（前面）	永続（前面）
HXAF220C M4 SED オールフラッシュ 保管中のデータの暗号化可能	1 X 120 GB SATA SSD または 1 X 240 GB SATA SSD	1 X 800 GB SAS SSD	6 X 800 GB SAS SSD
HXAF220C M4S オールフラッシュ	1 X 120 GB SATA SSD または 1 X 240 GB SATA SSD	1 X 400 GB SAS SSD	6 X 3.8 TB SATA SSD または 6 X 960 GB SATA SSD
HX220C M4 SED ハイブリッド 保管中のデータの暗号化可能	1 X 120 GB SATA SSD または 1 X 240 GB SATA SSD	1 X 800 GB SAS SSD	6 X 1.2 TB SAS HDD
HX220C M4 ハイブリッド	1 X 120 GB SATA SSD または 1 X 240 GB SATA SSD	1 X 480 GB SATA SSD	6 X 1.2 TB SAS HDD
HX220C M4 ハイブリッド ROBO	1 X 120 GB SATA SSD または 1 X 240 GB SATA SSD	1 X 480 GB SATA SSD	3 ～ 6 X 1.2 TB SAS HDD

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。

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
• Cisco B200 M3/M4 • B260 M4 • B420 M4 • B460 M4 • C240 M3/M4 • C220 M3/M4 • C460 M4	方法を選択します。 • ESX インストールでのミラー設定での SD カード。 • ローカル ドライブの HDD または SSD。 • SAN ブート。

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 クラスタ 内のすべてのサーバは、保管中のデータ対応である必要があります。
- 暗号化は、クラスタの作成後に、HX Connect を使用して、HX クラスタ 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 クラスタ に暗号化を適用するかどうかを決定します。

- **暗号化が構成されていない**：SED を削除または交換するには暗号化に関連した前提条件の手順が必要です。SSD の交換（117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 （122 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。入力するよう求められます。
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、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、以下の手順を完了します。

ステップ 1 HX クラスタ 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 **[システム情報（System Information）]** > **[ディスク（Disks）]** ページを選択します。

ステップ 4 削除するディスクを識別し、確認します。

1. [ロケータ LED をオンにする（Turn On Locator LED）] ボタンを使用します。
2. 物理的にサーバ上のディスクを表示します。
3. [ロケータ LED をオフにする（Turn Off Locator LED）] ボタンを使用します。

ステップ 5 削除するディスクに対応する [スロット（Slot）] 行を選択します。

ステップ 6 [安全に消去する（Secure erase）] をクリックします。このボタンは、ディスクを選択した後にのみ利用可能です。

ステップ 7 ローカルの暗号化キーを使用する場合は、フィールドに [暗号化キー（Encryption Key）] を入力して [安全に消去する（Secure erase）] をクリックします。

リモートの暗号化サーバを使用する場合、操作は必要ありません。

ステップ 8 このディスク上のデータを削除することを確認し、[はい、このディスクを消去 します（Yes, erase this disk）] をクリックします。

警告　　これは、ディスクからすべてのデータを削除します。

ステップ 9 選択した [ディスク スロット（Disk Slot）] の [ステータス（Status）] が [削除できます（Ok To Remove）] に変わるまで待ち、指示に従ってディスクを物理的に削除します。

次のタスク

（注） この中、またはいずれかのHXクラスタ内の別のサーバから削除したドライブを再利用しないでください。削除したドライブを再利用する必要がある場合は、TAC にお問い合わせください。

1. SED 上のデータを安全に消去した後、ディスク タイプ（SSD またはハイブリッド）に適したディスクの交換タスクに進みます。

   ディスク タイプの [タイプ（Type）] 列を確認します。

   - **ソリッド ステート**（SSD）：SSD の交換 （117 ページ）とサーバのハードウェア ガイドを参照してください。
   - **回転**（ハイブリッド ドライブ）：ハードディスク ドライブの交換または追加 （122 ページ）とサーバのハードウェア ガイドを参照してください。

2. 削除および交換された SED のステータスを確認します。

   SED を削除した場合。

   - [ステータス（Status）]：[削除できます（Ok To Remove）] のままです。
   - [暗号化（Encryption）]：[有功（Enabled）] から [不明（Unknown）] に変わります。

   SED を交換する場合、新しい SED は HX クラスタ によって自動的に消費されます。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。暗号化を適用すると、セキュリティ キーが新しいディスクに適用されます。

   - [ステータス（Status）]：**[無視（Ignored）]** > **[請求（Claimed）]** > **[利用可（Available）]** に遷移します。
   - [暗号化（Encryption）]：暗号化キーが適用された後に、**[無効（Disabled）]** > **[有効（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。
- キャッシュディスクまたは永続ディスクを交換する際は、元のディスクと同じタイプとサイズを常に使用します。

ステップ 1 障害が発生した SSD を特定します。

- キャッシュまたは永続 SSD の場合、ディスク ビーコン チェックを実行します。ビーコンの設定 （64 ページ）を参照してください。

  キャッシュと永続 SSD のみビーコン要求に応答します。NVMe キャッシュ SSD とハウスキーピング SSD は、ビーコン要求には応答しません。
- キャッシュ NVMe SSD の場合、物理的チェックを実行します。これらのドライブは、HX サーバのドライブ ベイ 1 にあります。
- HXAF240c または HX240c サーバのハウスキーピング SSD の場合、サーバ背面の物理的チェックを実行します。
- HXAF220c または HX220c のサーバのハウスキーピング SSD の場合、サーバのドライブ ベイ 2 の物理的チェックを実行します。

ステップ 2 **障害が発生した SSD がハウスキーピング SSD の場合**、サーバのタイプに基づいて続行します。

- HXAF220c または HX220c サーバの場合、ステップ 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 （119 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 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ドライブの交換後、HX Data Platform は、SDD を識別してストレージ クラスタを更新します。

ノードにディスクを追加すると、ディスクはすぐに HX で使用できるようになります。

ステップ 4 Cisco UCS Manager が新しいディスクを [UCS Manager サーバのインベントリ ストレージ（UCS Manager Server Inventory Storage）] タブに含めることができるようにするには、サーバ ノードを再認識します。これは、キャッシュ ディスクと永続ディスクに適用されます。

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 クラスタ 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 と HX220 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 サーバー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、ビーコン要求には応答しません。

故障した SSD が NVMe SSD でない場合は、SSD の交換 （117 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) **[システム情報（System Information）] > [ノード（Nodes）] > *[node]* > [HX メンテナンス モードの開始（Enter HX Maintenance Mode）]** を選択します。

ステップ 3 サーバ 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ドライブの交換後、HX Data Platform は、SDD を識別してストレージ クラスタを更新します。

ノードにディスクを追加すると、ディスクはすぐに HX で使用できるようになります。

ステップ 4 ESXi ホスト をリブートします。これにより、ESXi で NVMe の SSD が検出されます。

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 が新しいディスクを [UCS Manager サーバのインベントリ ストレージ（UCS Manager Server Inventory Storage）] タブに含めることができるようにするには、サーバ ノードを再認識します。これは、キャッシュ ディスクと永続ディスクに適用されます。

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。
- キャッシュディスクまたは永続ディスクを交換する際は、元のディスクと同じタイプとサイズを常に使用します。

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。

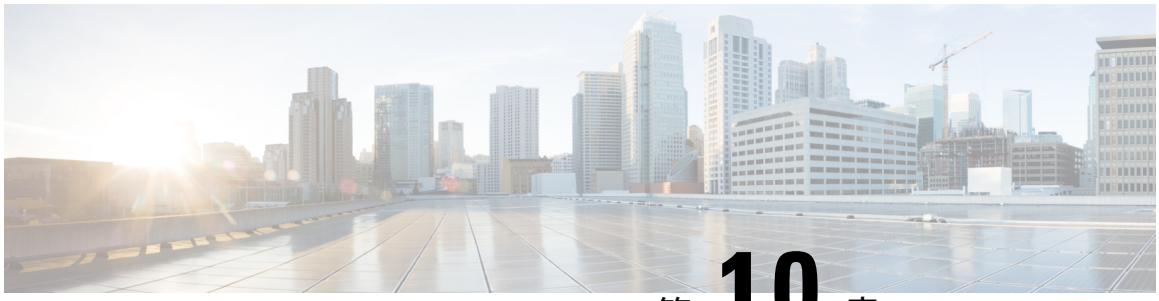
ステップ 2 ストレージ クラスタ内の各ノードに、同じサイズの HDD を追加します。

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 イベント（vCenter Event）] ログには、ノードへの変更を反映したメッセージが表示されます。

（注） ディスクをノードに追加すると、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 [インベントリ ストレージ（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 10 章

ノードの管理

- ノードの管理 （123 ページ）
- ノード メンテナンス方法の特定 （125 ページ）
- DNS アドレスまたはホスト名による検索 （128 ページ）
- ESXi ホスト ルート パスワードの変更 （129 ページ）
- ノード ソフトウェアの再インストール （129 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 （130 ページ）
- ノード コンポーネントの交換 （131 ページ）
- ノードの取り外し （133 ページ）
- ノードの交換 （141 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 プラグイン、vCenter UI、およびさまざまなログに動作ステータス（オンライン、オフライン）値と復元力ステータス値（正常、警告）として報告されます。

（注） 機能状態の区別は、HX Connect と HX Data Platform プラグインのビューに表示されるストレージ クラスタの動作ステータスと復元力ステータスに影響しますが、それらのステータスとは別個のものです。データ レプリケーション係数（2 または 3）、クラスタ アクセス ポリシー（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 プラグイン、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 または HX Data Platform プラグイン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のものがあります。

- **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	方法	注記（Notes）
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	方法	注記（Notes）
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	方法	注記（Notes）
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	方法	注記（Notes）
3 つ以上	1 つ以上	TAC によるサポートのみ。	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。 （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。

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

a) HX Data Platform インストーラ仮想マシンにログインします。ssh または vSphere コンソール インターフェイスを使用します。

b) resolv.conf.d ファイルを編集します。

```
# vi /etc/resolvconf/resolv.conf.d/base
```

c) 変更を確認します。

```
# resolvconf -u
# cat /etc/resolv.conf
```

d) DNS サーバが IP アドレスまたはホスト名から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。

a) HX Data Platform インストーラ仮想マシンにログインします。ssh または vSphere コンソール インターフェイスを使用します。

b) hosts ファイルを編集用に開きます。

```
# vi /etc/hosts
```

c) 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 プラグインを介して、またはストレージ コントローラ VM 上で stcli cluster 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、**[構成（Configuration）]** > **[DNS サーバ（DNS Servers）]** を選択します。

ステップ 6 データセンター名とクラスタ名を探してメモします。

vCenter クライアントまたは Web クライアントから、データセンター名とクラスタ名が表示されるまでスクロールします。それらを書き留めます。この名前は、後のステップで使用します。

ステップ 7 vCenter からクラスタを削除します。

vCenter から、**[データセンター（datacenter）]** > **[クラスタ（cluster）]** を選択します。[クラスタ（cluster）] を右クリックして、[削除（Delete）] を選択します。

（注） [データセンター（datacenter）] は削除しないでください。

ステップ 8 vCenter で [クラスタ（cluster）] を再作成します。

a) vCenter から、[データセンター（datacenter）] を右クリックします。[新規クラスタ（New Cluster）] を選択します。
b) 削除したクラスタとまったく同じ名前を [クラスタ名（Cluster Name）] に入力します。これは、ステップ 6 で書き留めた名前です。

ステップ 9 FQDN 名を使用して、[クラスタ（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、**[データセンター（datacenter）]** > **[クラスタ（cluster）]** を右クリックします。[ホストの追加（Add Host）] を選択します。
b) FQDN を使用して ESXi ホストを選択します。
c) クラスタ内の各 ESXi ホストに対して繰り返します。

ステップ 10 クラスタを vCenter に再登録します。

```
#  stcli cluster reregister
--vcenter-datacenter <datacenter_name>
--vcenter-cluster <hx_cluster_name>
--vcenter-url <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 （90 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

    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。支援が必要な場合は、TAC に連絡してください。
  - 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。

表 7: 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（Workflow）
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（Workflow）
4 ノード クラスタ	1	**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。
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	**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 ノード クラスタ	2	**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。 両方のノードを指定します。 **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。
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、**[ホーム（Home）] > [ホストとクラスタ（Hosts and Clusters）] > [ホスト（Hosts）] > [ホスト（*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 メンテナンス モード（Cisco HX Maintenance Mode）] > [HX メンテナンス モードの開始（Enter HX Maintenance Mode）]** の順に選択します。

[vSphere メンテナンス モード（vSphere Maintenance Mode）] オプションは、ホストの右クリック メニューの上部にあります。リストの下部までスクロールし、[Cisco HX メンテナンス モード（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) 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 [ノードの管理（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 クラスタ内のノードを取り外す場合は、TAC と一緒に作業することを強くお勧めします。

クラスタ内のノードの数	方法
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。

クラスタ内のノードの数	方法
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 （139 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 （139 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。次の機能が含まれています。

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	いずれか 1 つが必須。	ストレージ クラスタ ノードの一意の ID 番号。ID は、stcli cluster info コマンドでリストされます。

オプション	必須またはオプション	説明
--ip-1 NAME1	いずれか 1 つが必須。	ストレージクラスタ ノードの IP アドレス。IP は、stcli cluster info コマンドで `stNode` フィールド `NAME` の下にリストされます。
--id-2 ID2	これはオプションです。	ストレージ クラスタ ノードの一意の ID 番号。ID は、`stcli cluster info` コマンドでリストされます。
--ip-2 NAME2	これはオプションです。	ストレージクラスタ ノードの IP アドレス。IP は、stcli cluster info コマンドで `stNode` フィールド `NAME` の下にリストされます。 `--ip` オプションは、現在サポートされていません。
-f, --force	これはオプションです。	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
```

応答

```
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 [正常（Healthy）] になるまで、ストレージ クラスタの再調整が行われます。この期間中に障害テストを実行しないでください。ストレージ クラスタは引き続き正常です。

ストレージ クラスタ内にノードがないため、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 クラスタ内のノードを取り外す場合は、TAC と一緒に作業することを強くお勧めします。

クラスタ内のノードの数	方法
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。
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 （136 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。次の機能が含まれています。

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) すべてのストレージ クラスタ ノードを HX メンテナンス モードにします。
d) 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。

応答

```
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 [正常（Healthy）] になるまで、ストレージ クラスタの再調整が行われます。この期間中に障害テストを実行しないでください。ストレージ クラスタの正常性は引き続き [普通（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、クラスタは当初3または4ノードとなります。

  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

クラスタ サイズ	交換するノード	ワークフロー（Workflow）
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	交換するノード	ワークフロー（**Workflow**）
4 ノード クラスタ	1	**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 インストーラ（HX Installer）] > [クラスタ拡張（Expand Cluster）]** を使用して、交換用ノードを追加します。 （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。
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（**Workflow**）
5 ノード クラスタ	1	**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 インストーラ（HX Installer）] > [クラスタ拡張（Expand Cluster）]** を使用して、交換用ノードを追加します。 （**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。

クラスタ サイズ	交換するノード	ワークフロー（Workflow）
5 ノード クラスタ	2	**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。 両方のノードを指定します。 **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 インストーラ（HX Installer）] > [クラスタ拡張（Expand Cluster）]** を使用して、交換用ノードを追加します （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。
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

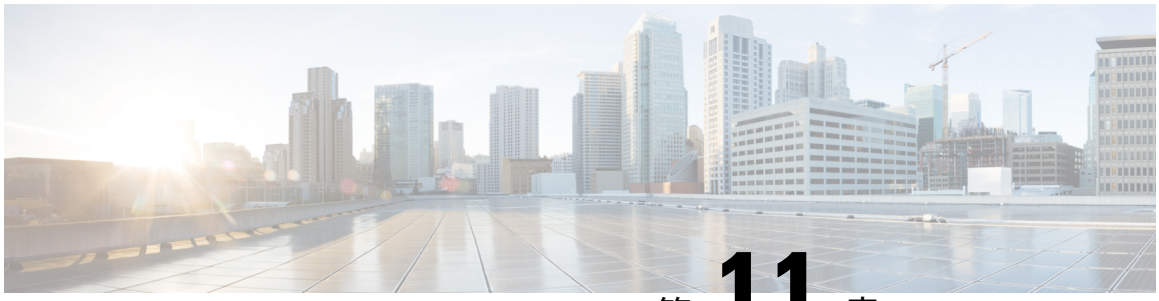
  この方法は、HX クラスタが最初から 5 ノード以上で構成され、現在も 5 ノード以上である場合にのみ使用します。

- 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 11 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 （147 ページ）
- ストレージ コントローラ VM の電源のオン/オフ （147 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。

a) vSphere Web クライアントにログインします。

b) VM を探します。

ナビゲータから、**[vCenter インベントリ リスト（vCenter Inventory Lists）] > [仮想マシン（Virtual Machines）] > *[vm]*** の順に選択します。

ストレージ コントローラ VM の名前には、`stCtlVM` というプレフィックスが付きます。

c) 右クリック メニューまたは [操作（Actions）] メニューから、**[電源（Power）] > [電源オン（Power On）]** または **[電源（Power）] > [電源オフ（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。

a) VM の ESX ホストのコマンド ラインにログインします。

b) VM vmid を探します。

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
```

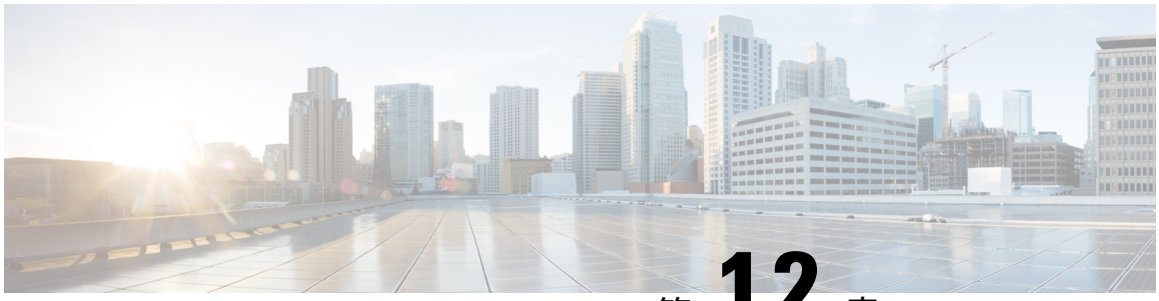
ストレージ コントローラ VM の名前には、stCtlVM というプレフィックスが付きます。

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 12 章

ReadyClone の管理

- HX Data Platform ReadyClone の概要 （149 ページ）
- HX Data Platform ReadyClone の利点 （149 ページ）
- サポート対象のベース VM （150 ページ）
- ReadyClone の要件 （150 ページ）
- ReadyClone のベスト プラクティス （151 ページ）
- HX Data Platform ReadyClone の作成 （151 ページ）
- HX Data Platform ReadyClone のカスタマイズの準備 （153 ページ）
- カスタマイズ仕様を使用した ReadyClone の設定 （155 ページ）
- 仮想マシン ネットワーキングの管理 （155 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。また、VM の複数コピーを作成できる拡張機能です。作成されたコピーはスタンドアロン VM として使用できます。

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。ReadClone 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 Data Platform 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 インベントリ リスト（vCenter Inventory Lists）]** > **[仮想マシン（Virtual Machines）]** の順に選択します。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、[操作（Actions）] メニューを開きます。[VM 情報（VM information）] ポートレット内で、VM を右クリックするか [操作（Actions）] メニューをクリックします。

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。
Customization Specification	ドロップダウンリストをクリックして、リストからクローン向けの [カスタマイズ仕様（Customization Specification）] を選択します（このリストには vCenter で使用可能なカスタマイズ仕様が含まれます）。 システムは、選択したホスト VM のカスタマイズ仕様をフィルタリングします。たとえば、選択したホスト VM がゲスト VM 向けに Windows OS を使用する場合、ドロップダウンリストには Windows OS のカスタマイズ仕様が表示されます。
VM 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'	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。 システムには、ダイアログ ボックス内の [ゲスト名（Guest Name）] 列にある、ゲスト VM の名前が表示されます。 [カスタマイズ仕様（Customization Specification）] 自体にも、同様のオプションがあります。この HX Data Platform ReadyClone のバッチのカスタマイゼーション プロセスでは、[カスタマイズ仕様（Customization Specification）] オプションで指定したオプションがオーバーライドされます。 • [カスタマイズ仕様（Customization Specification）] に静的ゲートウェイ、静的サブネット、または静的 IP アドレスに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 クラスタ名またはホスト名を設定します。

Control	説明
	• [カスタマイズ仕様（Customization Specification）] に、DHCP を使用して IP アドレスを取得する NIC もしくはネットワーク アダプタが含まれる場合、システムはストレージクラスタ名またはホスト名のみを指定されたゲスト名に設定します。
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 の最近のタスク（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、ReadyClones の作成中にのみ、一時的に VM の特別な電源オフとして表示されます。

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 サマリー（VM Summary）] タブに移動し、ゲスト ツールが動作していることを確認します。

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

[vSphere Web クライアント ゲストのカスタマイズ（vSphere Web Client Guest Customization）] ウィザードを使用して、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、[カスタマイズ仕様マネージャ（Customization Specification Manager）] 内にリストされます。これを使用して、仮想マシンのゲスト オペレーティング システムをカスタマイズすることができます。

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

[vSphere Web クライアント ゲストのカスタマイズ（vSphere Web Client Guest Customization）] ウィザードを使用して、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 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、[カスタマイズ仕様マネージャ（Customization Specification Manager）] 内にリストされます。これを使用して、仮想マシンのゲスト オペレーティング システムをカスタマイズすることができます。

カスタマイズ仕様を使用した 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キング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 ネットワーキング情報については、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。

で、『*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 13 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 （157 ページ）
- HX Data Platform ネイティブ スナップショットの利点 （158 ページ）
- ネイティブ スナップショットの考慮事項 （159 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 （161 ページ）
- SENTINEL スナップショットについて （162 ページ）
- ネイティブ スナップショットのタイムゾーン （163 ページ）
- スナップショットの作成 （164 ページ）
- スナップショットのスケジューリングの概要 （165 ページ）
- スナップショットのスケジューリング （166 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 （167 ページ）
- スナップショット スケジュールの削除 （168 ページ）
- スナップショットへの復帰 （168 ページ）
- スナップショットの削除 （169 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 プラグインを使用して 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

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 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（HX 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 managerTM 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

スナップショットのパラメータ

- **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 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 バッキング タイプをサポートします。最も一般的なタイプは FlatVer2 形式です。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 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、次のリンクの 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

[すぐにスナップショット作成（Snapshot Now）] または [スケジュール済みスナップショット（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係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 のスケジュールされたタスク（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 のスケジュールされたタスク（vSphere Scheduled

Task）] タブでは [HX Data Platform スケジュール スナップショット（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 タスク（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で完了したというステータスを表示することがあります。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 インベントリ リスト（vCenter Inventory Lists）]** > **[仮想マシン（Virtual Machines）]** の順に選択し、vCenter 内での VM のリストを表示します。

ステップ 2 ストレージ クラスタ VM を選択し、[操作（Actions）] メニューを開きます。[VM 情報（VM information）] ポートレット内で、VM を右クリックするか [操作（Actions）] メニューをクリックします。

（注） ストレージ クラスタのリソース プール上に HX Data Platform に属していないデータストアがないことを確認します。そうでない場合、スナップショットは失敗します。

ステップ 3 **[Cisco HX Data Platform]** > **[今すぐスナップショット（Snapshot Now）]** の順に選択して、[スナップショット（Snapshot）] ダイアログボックスを表示します。

ステップ 4 [スナップショット（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。

[最近のタスク（Recent Tasks）] タブでは、次のステータス メッセージが表示されます。

```
Create virtual machine native snapshot.

The first snapshot
```

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 フォルダ、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
午後 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、VM フォルダ、またはリソース プール リストを選択します。

たとえば、**[vCenter インベントリ リスト（vCenter Inventory Lists）] > [仮想マシン（Virtual Machines）]** の順に選択し、vCenter 内での VM のリストを表示します。

ステップ 2 ストレージ クラスタ VM、VM フォルダ、またはリソース プールを選択し、[操作（Actions）] メニューを開きます。

オブジェクトを右クリックするか、または [操作（Actions）] メニューをクリックします。

ステップ 3 [操作（Actions）] メニューから **[Cisco HX Data Platform] > [スケジュール スナップショット（Schedule Snapshot）]** の順に選択し、[スケジュール スナップショット（Schedule Snapshot）] ダイアログ ボックスを表示します。

ステップ 4 スナップショットの頻度を選択します。

時間単位、日単位、週単位の頻度を示すボックスをクリックし、開始日、開始時刻、および期間を設定します。

ステップ 5 保持するスナップショットの数を設定します。

最大数に達すると、新しいスナップショットの作成に伴って古いスナップショットが削除されます。

ステップ 6 必要に応じて、既存のスケジュール済み項目を選択解除します。

以前のスケジュールが存在している場合は、項目を選択解除すると、今後のスケジュールからこれらの項目が削除されます。

ステップ 7 [OK] をクリックしてスケジュールを受け入れ、ダイアログを閉じます。

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、VM フォルダ、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 [スケジュール スナップショット（Schedule Snapshot）] ダイアログボックスで、[時間単位のスナップショットを有効にする（Enable Hourly Snapshot）]、[日単位のスナップショットを有効にする（Enable Daily Snapshot）]、または [週単位のスナップショットを有効にする（Enable Weekly Snapshot）] のチェックボックスをオンにします。

ステップ 2 ドロップダウン リストの [開始（Start）] をクリックし、開始時間を選択します。時間、15 分単位の分、午前または午後を選択します。

ステップ 3 スナップショット スケジュールを時間単位で設定するには、[終了日時（Until）] ドロップダウン リストをクリックして、終了時間を選択します。時間、15 分単位の分、午前または午後を選択します。時間で、[開始（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（[日（Days）]）を指定します。

ステップ 5 [保持（Retention）] で、数値を入力するか矢印ボタンを使用して、スケジュールごとに保持するコピーの最大数を指定します。

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、VM フォルダ、またはリソース プール リストを選択します。

たとえば、**[vCenter インベントリ リスト（vCenter Inventory Lists）] > [仮想マシン（Virtual Machines）]** の順に選択し、vCenter 内での VM のリストを表示します。

ステップ 2 ストレージ クラスタ VM、VM フォルダ、またはリソース プールを選択し、[操作（Actions）] メニューを開きます。

オブジェクトを右クリックするか、または [操作（Actions）] メニューをクリックします。

ステップ 3 [操作（Actions）] メニューから **[Cisco HX Data Platform] > [スケジュール スナップショット（Schedule Snapshot）]** の順に選択し、[スケジュール スナップショット（Schedule Snapshot）] ダイアログ ボックスを表示します。

ステップ 4 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、VM フォルダ、またはリソース プールを選択します。vCenter のタブ、**[管理（Manage）] > [スケジュールされたタスク（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。

スナップショットへの復帰

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 インベントリ リスト（vCenter Inventory Lists）] > [仮想マシン（Virtual Machines）] の順に選択し、vCenter 内の VM のリストを表示します。

ステップ 2 ストレージ クラスタ VM を選択し、[操作（Actions）] メニューを開きます。[VM 情報（VM information）] ポートレット内で、VM を右クリックするか [操作（Actions）] メニューをクリックします。

ステップ 3 **[スナップショット（Snapshots）] > [スナップショットの管理（Manage Snapshots）]** を選択し、vSphere Snapshot Manager を開きます。

ステップ 4 選択した VM のスナップショット階層から、復元するスナップショットを選択します。

ステップ 5 **[復元（Revert to）] > [はい（Yes）] > [閉じる（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、**[VM とテンプレート（VMs and Templates）] > [*vcenter_server*] > [スナップショット（Snapshots）] > [データセンター（*datacenter*）] > [*vm*]** の順序で選択します。

ステップ 2 ***[vm]*** を右クリックして、**[スナップショット（Snapshots）] > [スナップショットの管理（Manage Snapshots）]** を選択します。

ステップ 3 スナップショットを選択し、[削除（Delete）] をクリックします。

（注） [すべて削除（Delete All）] オプションのみを使用して、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 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 （171 ページ）
- 仮想マシンの保護の概要 （175 ページ）
- データ保護/リカバリ ワークフロー （195 ページ）
- レプリケーション メンテナンスの概要 （201 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 15 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。この設定はオンラインで完了することができます。

2 つのクラスタ間のレプリケーションでは、両方のクラスタがオールフラッシュ、またはハイブリッドである必要があります。混在構成はサポートされません。オールフラッシュとハイブリッド クラスタ間ではレプリケーションはできません。

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。

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、他のクラスタの管理者資格情報が必要です。

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。

- 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権限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対し、指定したローカルおよびリモートの両方のユーザは管理者権限を持っている必要があり、それぞれのクラスタで vCenter SSO で構成される必要があります。
- レプリケーション スケジュールをサポートするリモート クラスタ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 （85 ページ）を参照してください。HX クラスタ 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。
- レプリケーション保護は 2 つの HX クラスタ の間で行われます。
  - 両方のクラスタを同じタイプ（どちらも all flash か、どちらも hybrid）にする必要があります。

- 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。

- 復元、レプリケーション、またはリカバリ操作中に、HX クラスタ 内の任意のノードを再起動しないでください。
- 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。
- 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ます。

  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、新しい vm-uuid を持つクローンとしてテストされてからは、テストリカバリは新しいレプリケーション仮想マシンの階層構造を開始します。

- HX Data Platform は、スナップショット テクノロジーのいくつかのフォームを使用します。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した。

データ保護の用語

フェールオーバー：ソース クラスタで災害時に、動作している VM の場所をシフトするプロセスです。つまり、プライマリ クラスタに障害が発生し、セカンダリ クラスタが動作している VM を引継ぎます。

ローカル クラスタ：ローカル クラスタは、リモート クラスタとのレプリケーション ペアに対して構成タスクが実行されるクラスタです。通常、レプリケーションのコンテキストで使用されます。

移行：災害ではなく、定期的なシステム メンテナンスと管理のために、いつでも使用されます。移行では、リカバリと同様に、VM の最新のレプリケーション スナップショット コピーが動作中の VM になります。ソースとターゲットのクラスタ間のペアはそのままです。

プライマリ クラスタ：プライマリが単に動作中の VM が現在存在する場所であることを除き、ソース対ターゲットに類似した別の用語セットです。セカンダリに VM を移行すると、セカンダリはプライマリになります。通常、フェールオーバーのコンテキストで使用されます。

保護された仮想マシン：個別にまたは保護グループを通じてレプリケーションが構成された VM です。

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 テスト：リカバリ プロセスを災害時に成功させるメンテナンス タスクです。

リモート クラスタ：リモート クラスタは、ローカル クラスタとのレプリケーション ペアのもう片方の半分です。通常、レプリケーションのコンテキストで使用されます。

レプリケーション ペア：ローカル 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場所を提供する 2 つのクラスタです。

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種類です。ソース クラスタからターゲット クラスタにコピーされます。

セカンダリ クラスタ：プライマリが単に動作中の VM が現在存在する場所であることを除き、ソース対ターゲットに類似した別の用語セットです。セカンダリに VM を移行すると、セカンダリはプライマリになります。通常、フェールオーバーのコンテキストで使用されます。

ソース クラスタ：ソース クラスタは、VM が存在する場所です。通常、リカバリのコンテキストで使用されます。

ターゲット クラスタ：ターゲット クラスタは VM レプリケーション スナップショットのコピーが存在する場所です。通常、リカバリのコンテキストで使用されます。

- レプリケーション ペアのソース 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の VM または保護グループのいずれかとして構成されます。

保護グループ：VM のグループにレプリケーションのスケジュールを割り当てるためのメカニズム

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。

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も考えられる）
- 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みる時刻の指定）
- 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でき、そのグループを通じて、すべてに同じ保護属性が割り当てられます。

たとえば、保護の3つのクラス、金、銀、銅があるとします。レプリケーション間隔を、金には 15 分、銀には 4 時間、銅には 24 時間などと、各クラスの保護グループを設定します。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入れます。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. 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。
5. 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、1 つのクラスタから実行されます。
6. 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。
7. 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
8. 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。[保護（Protect）] をクリックします。
   2. 仮想マシンの保護ウィザードでのオプションは次のとおりです。
      - 既存の保護グループを通じて 1 つの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 ネットワークの設定

レプリケーション ペアを設定する前に、レプリケーション ネットワークが、ローカルおよびリモートの両方のクラスタで設定されていることが必要です。ローカル クラスタで設定を完了してから、リモート クラスタにログインして、そこで設定を完了します。

始める前に

- 2 つの HX ストレージ クラスタ です。

  両方のクラスタが、すべてフラッシュまたはハイブリッドの同じタイプである必要があります。異なるタイプのクラスタを混在させることはできません。

ステップ 1 このクラスタの管理ネットワークの管理者として HX Connect にログインします。

ステップ 2 **[レプリケーション（Replication）] > [設定（Configure）]** を選択します。

レプリケーション ネットワークは一度のみ構成できます。構成後は、使用可能な IP アドレスとネットワークの帯域幅を編集できます。

ステップ 3 ネットワーク情報を入力します。

UI 要素	基本情報
[VLAN 名（VLAN Name）] フィールド	チェックボックスを選択した場合、このフィールドにはデフォルトの VLAN 名が入力されます。 レプリケーション ネットワークで使用するため、Cisco UCS Manager を通じて VLAN を手動で設定した場合、その VLAN 名を入力します。

UI 要素	基本情報
[VLAN ID] フィールド	必須作業です。上または下向きの矢印をクリックして VLAN ID の番号を選択します。 レプリケーション ネットワークで使用するため、Cisco UCS Manager を通じて構成した VLAN ID を入力します。これは、HX Data Platform 管理トラフィック ネットワーク と データ トラフィック ネットワーク とは別です。形式の例：1 レプリケーションは、2 つの HX ストレージ クラスタ の間にあります。各 HX ストレージ クラスタ は、レプリケーション ネットワークに専用の VLAN を必要とします。 値を追加すると、追加の識別子を含むようにデフォルトの VLAN 名が更新されます。VLAN ID の値は、手動で入力した VLAN 名には影響しません。 レプリケーションペアの各 HX ストレージクラスタには異なる VLAN ID 番号を使用してください。
ファブリックインターコネクトでこのレプリケーションの VLAN ID を構成します。[（推奨（Recommended））]チェックボックス	この設定は、デフォルトでオンになっています。 レプリケーション ネットワークへの VLAN の適用を有効にするにはこのチェック ボックスをクリックします。
[UCS Manager のホスト IP または FQDN（UCS Manager host IP or FQDN）]	必須作業です。VLAN ID で Cisco UCS Manager を更新するには、Cisco UCS Manager のホストとログイン クレデンシャルが必要です。 Cisco UCS Manager の [ユーザ名（User name）] および [パスワード（Password）] を入力します。 [パスワード（Password）] テキストの表示を切り替えるには、目のアイコンをクリックします。
[ユーザ名（User Name）] と [パスワード（Password）]	必須作業です。Cisco UCS Manager アクセス用の管理者レベルのユーザ名とパスワード。
[サブネット（Subnet）] フィールド	必須作業です。レプリケーション ネットワークで使用するサブネットをネットワーク プレフィックス表記で入力します。これは、HX Data Platform 管理トラフィック ネットワーク と データ トラフィック ネットワーク とは別です。形式の例：p.q.r.s/<number of bits>, 1.1.1.1/20
[ゲートウェイ（Gateway）] フィールド	必須作業です。レプリケーション ネットワーク用のゲートウェイを入力します。これは、HX Data Platform 管理トラフィック ネットワーク と データ トラフィック ネットワーク とは別です。形式の例：1.2.3.4

UI 要素	基本情報
[IP 範囲（IP Range）] フィールド	必須作業です。レプリケーション ネットワークで使用する IP アドレスの範囲を入力します。[から（from）] および [まで（to）] の値を入力します。[から（from）] の値には、[まで（to）] の値より小さい値を指定する必要があります。コンテンツの例：from 10.10.10.20 to 10.10.10.30 必要な IP アドレスの最小数は、HX ストレージ クラスタ のノード数プラス 1 です。たとえば、4 ノードがある HX ストレージ クラスタ の場合、少なくとも 5 つの IP アドレスの範囲を入力してください。クラスタにノードを追加する計画がある場合は、追加ノードをカバーするのに十分な数の IP アドレスを含めます。ただし IP アドレスはいつでも追加できます。
[IP 範囲の追加（Add IP Range）] フィールド	必須作業です。クリックして、[IP 範囲（IP Range）] の [から（From）] および [まで（To）] フィールドに入力した IP アドレスの範囲を追加します。
[IP 範囲（ip ranges）] リスト	レプリケーション ネットワークで使用できる IP アドレスの一覧が表示されます。これらは編集できません。 割り当てされていない IP アドレスの数を表示するには、[クラスタ レプリケーション ネットワーク（Cluster Replication Network）] フィールドの [未使用 IP（Unused IPs）] を参照してください。
[アウトバウンド レプリケーション帯域幅の上限の設定（Set outbound replication bandwidth limit）] チェックボックス	必須作業です。デフォルトは [無制限（unlimited）] です。ネットワークの最大帯域幅をネットワークで使用可能な合計に設定します。 **1.** チェックボックスをクリックします。 **2.** レプリケーション ネットワークが発信トラフィックに使用できる最大のネットワーク帯域幅を入力します。許容値は 10 ～ 100000 です。 これは、このローカル HX ストレージ クラスタ から、ペアになっているリモート HX ストレージ クラスタ にレプリケーション スナップショットをコピーするのに使用されます。

ステップ 4 [構成] をクリックします。

HX Data Platform はリモート ネットワークを確認してログインし、UCS Manager から VLAN を取得して、ローカル クラスタ内の各ノードに IP アドレスを割り当てます。

次のタスク

レプリケーション ペアの両方の HX ストレージ クラスタ にレプリケーション ネットワークを構成してください。

レプリケーション ネットワークの編集

構成済みのレプリケーションがある HX クラスタ を展開するときは、レプリケーション ネットワークに使用できる十分な IP アドレスがあることを確認します。レプリケーション ネットワークでは、クラスタ内の各ノード 1 台に 1 つに加えてもう 1 つ専用の IP アドレスが必要です。このため、3 ノードのクラスタでは 4 つの IP アドレスが必要です。ノードをもう 1 つクラスタに追加する場合は、少なくとも 5 つの IP アドレスが必要です。 IP アドレスを追加するには、レプリケーション ネットワークを編集します。

ノードを削除すると、割り当てられた IP アドレスが解放されます。

ステップ 1 このクラスタの管理ネットワークの管理者として HX Connect にログインします。

ステップ 2 **[レプリケーション（Replication）]** > **[編集（Edit）]** ボタンを選択します。

レプリケーション ネットワークを作成した後は、使用する IP の範囲を編集し、レプリケーション トラフィックの発信帯域幅の値を設定できます。レプリケーション ネットワーク サブネット、ゲートウェイ、および VLAN ID は参照用にのみ表示され、編集できません。

ステップ 3 フィールドを必要に応じて更新し、[変更の保存（Save Changes）] をクリックします。

UI 要素	基本情報
[VLAN ID] フィールド	このレプリケーション ネットワーク用に構成された VLAN ID です。この値は変更できません。
[サブネット（Subnet）] フィールド	レプリケーション ネットワーク用に構成されたネットワーク プレフィックス表記のサブネット。この値は変更できません。
[ゲートウェイ（Gateway）]フィールド	レプリケーションネットワーク用に構成されたゲートウェイ。この値は変更できません。
[IP 範囲（IP Range）] フィールド	レプリケーション ネットワークで使用する IP アドレスの範囲を入力します。[から（from）]および[まで（to）]の値を入力します。[から（from）]の値には、[まで（to）]の値より小さい値を指定する必要があります。コンテンツの例：from 10.10.10.20 to 10.10.10.30 必要な IP アドレスの最小数は、HX ストレージ クラスタ のノード数プラス 1 です。たとえば、4 ノードがある HX ストレージ クラスタ の場合、少なくとも 5 つの IP アドレスの範囲を入力してください。クラスタにノードを追加する計画がある場合は、追加ノードをカバーするのに十分な数の IP アドレスを含めます。ただし IP アドレスはいつでも追加できます。
[IP 範囲の追加（Add IP Range）] フィールド	クリックして、[IP 範囲（IP Range）] の [から（From）] および [まで（To）] フィールドに入力した IP アドレスの範囲を追加します。

UI 要素	基本情報
[IP 範囲（ip ranges）] リスト	レプリケーション ネットワークで使用できる IP アドレスの一覧が表示されます。これらは編集できません。 割り当てされていない IP アドレスの数を表示するには、[クラスタ レプリケーション ネットワーク（Cluster Replication Network）] フィールドの [未使用 IP（Unused IPs）] を参照してください。
[アウトバウンド レプリケーション帯域幅の上限の設定（Set outbound replication bandwidth limit）] チェックボックス	これはオプションです。デフォルトは [無制限（unlimited）] です。ネットワークの最大帯域幅をネットワークで使用可能な合計に設定します。 1. チェックボックスをクリックします。 2. レプリケーション ネットワークが発信トラフィックに使用できる最大のネットワーク帯域幅を入力します。許容値は 10 ～ 100000 です。 これは、このローカル HX ストレージ クラスタ から、ペアになっているリモート HX ストレージ クラスタ にレプリケーション スナップショットをコピーするのに使用されます。

レプリケーション ペアの概要

レプリケーション クラスタ ペアの作成は、レプリケーション用 VM の設定の前提条件です。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って、レプリケーション用に明示的に設定されたクラスタ 1 上のすべての VM はクラスタ 2 にレプリケートでき、レプリケーション用に明示的に設定されたクラスタ 2 上のすべての VM はクラスタ 2 にレプリケートできることを指定しています。

クラスタ 1 のデータストア A とクラスタ 2 のデータストア B をペアリングすることによって、レプリケーション用に明示的に設定されるたクラスタ 1 上のすべての VM では、データストア A にファイルがある場合、それらのファイルはクラスタ 2 のデータストア B にレプリケートされることを指定しています。同様に、レプリケーション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。クラスタは、他の 1 つ以上のクラスタとペアリングすることができます。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することはできません。

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 ストレージ クラスタ はローカル クラスタで、ペアの最初の半分です。このダイアログによって、ペアの 2 つ目の半分で、リモート クラスタである、別の HX ストレージ クラスタ 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ストレージ クラスタ のデータストアにマップします。

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

- 各クラスタにレプリケーション ネットワークを構成します。
- 各クラスタに 1 つ以上のデータストアを作成します。
- ローカルとリモートの両方の HX ストレージ クラスタ がシングル サインオン（SSO）を使用していることを確認します。
- 管理者特権を持つユーザを指定します。
- 管理者権限を持つユーザとして HX Connect にログインします。

ステップ 1 HX Connect から、**[レプリケーション（Replication）] > [レプリケーション ペアの作成（Create Replication Pair）]** を選択します。

ステップ 2 レプリケーション ペアの [名前（Name）] を入力し、[次へ（Next）] をクリックします。

2 つの HX ストレージ クラスタ の間のレプリケーション ペアの名前を入力します。この名前は、ローカルおよびリモートの両方のクラスタに設定されます。この名前は変更できません。

ステップ 3 [リモート接続（Remote Connection）] の ID を入力し、[ペア（Pair）] をクリックします。

UI 要素	基本情報
[管理 IP または FQDN（Management IP or FQDN）] フィールド	リモート HX ストレージ クラスタ 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。10.10.10.10 などです
[ユーザ名（User Name）] と [パスワード（Password）] フィールド	リモート HX ストレージ クラスタ の 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。入力したユーザには管理者権限が必要です。

HX Data Platform はリモート HX ストレージ クラスタ を確認し、レプリケーション ペア名を割り当てます。

（注） 保護される仮想マシンは、レプリケーション ペアのデータストアの 1 つになければなりません。

ステップ 4 両方のクラスタから [データストアのマッピング（Datastore Mapping）] を設定し、[次へ（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する必要があります。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
[ローカル データストア（Local Datastore）] 列	このクラスタ、ローカル HX ストレージ クラスタ に構成されたデータストアの一覧です。 ローカル ストアをリモート ストアにマップします。
[リモート データストア（Remote Datastore）] 列	HX ストレージ クラスタ 間のデータストアをペアリングします。 必要な [ローカル データストア（Local Datastore）] 行で、[リモート データストア（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は、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を選択します。

ステップ 5 概要情報を確認し、[データストアをマップする（Map Datastores）] をクリックします。

UI 要素	基本情報
[データストア（Datastores）] フィールド	このローカル HX ストレージ クラスタ で選択したデータストア。
[ターゲット 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 ストレージ クラスタ のデータストア。

レプリケーション ペアの編集

レプリケーションペアを編集すると、レプリケーションペアのデータストアが変更されます。

（注） 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 **[レプリケーション（Replication）] > [レプリケーション ペア（Replication Pairs）] > [編集（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、[完了（Finish）] をクリックします。

UI 要素	基本情報
[ローカル データストア（Local Datastore）] 列	このクラスタ、ローカル HX ストレージ クラスタ に構成されたデータストアの一覧です。 ローカル ストアをリモート ストアにマップします。
[リモート データストア（Remote Datastore）] 列	HX ストレージ クラスタ 間のデータストアをペアリングします。 1. ローカル データストアの選択を変更するには、現在のローカル データストアへのマッピングを削除します。 [リモート データストア（Remote Datastore）] 列のプルダウン メニューで、[このデータストアをマップしない（Do not map this datastore）] を選択します。 2. 必要な [ローカル データストア（Local Datastore）] 行で、[リモート データストア（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。これは、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を選択します。

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。

[レプリケーション（Replication）] > [レプリケーション ペア（Replication Pairs）] > [削除（Delete）] を選択します。

始める前に

ローカルおよびリモートの両方のクラスタで、レプリケーション ペアから依存関係を削除します。

このローカル HX ストレージ クラスタ から次を実行します。リモート HX ストレージ クラスタ 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。個々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。

a) **[レプリケーション（Replication）] > [レプリケーション ペア（Replication Pairs）] > [編集（Edit）]** を選択します。

b) [レプリケーション ペアの編集（Edit Replication Pair）] ダイアログ ボックスの、[リモート データストア（Remote Datastore）] メニューから、[このデータストアをマップしない（Do not map this datastore）] を選択します。

UI 要素	基本情報
[ローカル データストア（Local Datastore）] 列	このクラスタ、ローカルHXストレージクラスタに構成されたデータストアの一覧です。 ローカル ストアをリモート ストアにマップします。
[リモートデータストア（Remote Datastore）] 列	HX ストレージ クラスタ 間のデータストアをペアリングします。 1. ローカルデータストアの選択を変更するには、現在のローカルデータストアへのマッピングを削除します。 [リモート データストア（Remote Datastore）] 列のプルダウン メニューで、[このデータストアをマップしない（Do not map this datastore）] を選択します。 2. 必要な [ローカル データストア（Local Datastore）] 行で、[リモートデータストア（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。これは、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を選択します。

c) すべての可能なリモート データストアが、[このデータストアをマップしないでください（Do not map this datastore）] に設定されていることを確認します。

d) [終了（Finish）] をクリックします。

ステップ 3 **[レプリケーション（Replication）] > [レプリケーション ペア（Replication Pairs）] > [削除（Delete）]** を選択します。

ステップ 4 リモート クラスタの管理者のクレデンシャルを入力し、[削除（Delete）] をクリックします。

UI 要素	基本情報
[ユーザ名（User Name）] フィールド	リモート HX ストレージ クラスタ の管理者ユーザ名を入力します。
[パスワード（Password）] フィールド	リモートHXストレージクラスタの管理者パスワードを入力します。

保護グループの作成

ローカルクラスタ上の保護グループを作成します。保護グループは、それらが作成されるクラスタによってのみ管理され、また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、それが作成されるクラスタである、そのローカル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 **[レプリケーション（Replication）] > [保護グループ（Protection Groups）] > [保護グループの作成（Create Protection Group）]** を選択します。

ステップ 3 ダイアログ フィールドに情報を入力します。

UI 要素	基本情報
[保護グループ名（Protection Group Name）] フィールド	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。名前はリモートの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。クラスタに複数の保護グループを作成できます。
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	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。 15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間
[仮想マシンの保護をすぐに開始（Start protecting the virtual machines immediately）] 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
[仮想マシンの保護の開始時刻（Start protecting the virtual machines at）] ラジオ ボタン	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。 • 少なくとも 1 つの仮想マシンが保護グループに追加されている。 • スケジュールされた開始時刻に達している。 保護の開始時刻を指定するには、次のようにします。 1. [仮想マシンの保護の開始時刻（Start protecting the virtual machines at）] ラジオ ボタンをクリックします。 2. [時刻（time）]フィールドをクリックし、時間と分を選択します。フィールドの外をクリックします。 [クラスタのタイムゾーン（Cluster time zone）] と [クラスタの現在の時刻（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。開始時間は、ローカル クラスタの時計に基づいています。次に例を示します。 クラスタの現在の時刻が 13:56:15 で、現在から 10 時間と 3 分後とは、23:59 に最初のレプリケーションが発生することを意味します。 [現在からの時間と分（hours, minutes from now）] は最初のレプリケーションが発生する時を示します。これは、[時刻（time）] フィールドの設定値を変更すると更新されます。
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェック ボックス	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 [保護グループの作成（Create Protection Group）] をクリックします。

HX Data Platform で [保護グループ（Protection Group）] タブに新しいグループが追加されます。この保護グループは、このクラスタ上の仮想マシンを保護するために利用可能です。

ステップ 5 **[レプリケーション（Replication）] > [保護グループ（Protection Groups）]** の順にクリックして新しい保護グループを表示または編集します。

VM の数はゼロ（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 **[レプリケーション（Replication）]** > **[保護グループ（Protection Groups）]** > **[スケジュールの編集（Edit Schedule）]** を選択します。

ステップ 3 ダイアログ フィールドの情報を編集します。

UI 要素	基本情報
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	プルダウン リスト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。 15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェック ボックス	レプリケーション スナップショットを取る前に HX 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 [変更の保存（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、[保護グループ（Protection Groups）] タブを参照してください。

保護グループの削除

始める前に

保護グループからすべての仮想マシンを削除します。

ステップ 1 保護グループ内のすべての仮想マシンを保護解除します。

a) HX Connect で、**[レプリケーション（Replication）]** > **[保護された仮想マシン（Protected Virtual Machines）]** を選択します。
b) 保護グループ内のすべての仮想マシンを選択します。
c) [保護の解除（Unprotect）] をクリックします。確認ポップアップで、[保護の解除（Unprotect）] をクリックします。

ステップ 2 **[レプリケーション（Replication）]** > **[保護グループ（Protection Groups）]** > ***[protection_group_name]*** を選択します。

ステップ 3 [削除（Delete）] をクリックします。確認ポップアップで、[削除（Delete）] をクリックします。

既存の保護グループでの仮想マシンの保護

このタスクでは、既存の保護グループを使用して複数の仮想マシンを保護する方法について説明します。

既存の保護グループを使用する：1 つまたは複数の仮想マシンと既存の保護グループに対する仮想マシンを選択します。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

構成されたレプリケーション ネットワークおよびレプリケーション ペアです。

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 管理者権限で HX Connect にログインし、[仮想マシン（Virtual Machines）] を選択します。

これによりローカル 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 [保護（Protect）] をクリックします。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、[保護グループ（Protection Group）] ページが表示されます。

ステップ 4 [既存の保護グループに追加（Add to an existing protection grou）] ラジオ ボタンをクリックします

UI 要素	基本情報
[保護パラメータの設定（Set the protection parameters）] テーブル	選択した仮想マシンの [名前（Name）] を確認します。 [プロビジョニング済みストレージ（Storage Provisioned）] と [使用済みのストレージ（Storage Used）] を使用して、リモート HX ストレージ クラスタ 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。
[既存の保護グループに追加（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。
[新しい保護グループの作成（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。名前はリモートの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。クラスタに複数の保護グループを作成できます。

ステップ 5 プルダウンリストから保護グループを選択し、[次へ（Next）] をクリックします

選択した保護グループに、希望するスケジュール間隔があることを確認します。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、[概要（Summary）] ページが表示されます。

ステップ 6 [概要（Summary）] ページの情報を確認し、[保護グループに追加（Add to Protection Group）] をクリックします。

HX Data Platform は、仮想マシンをレプリケーション保護に追加します。[レプリケーション（Replication）] または [仮想マシン（Virtual Machines）] ページを表示して確認します。[レプリケーション（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。

新規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

構成されたレプリケーション ネットワークおよびレプリケーション ペアです。

ステップ 1 管理者権限で HX Connect にログインし、[仮想マシン（Virtual Machines）] を選択します。

これによりローカル 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 [保護（Protect）] をクリックします。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、[保護グループ（Protection Group）] ページが表示されます。

ステップ 4 [新しい保護グループを作成（Create a new protection group）] ラジオ ボタンをクリックして、保護グループの名前を追加し、[次へ（Next）] をクリックします。

[保護スケジュール ウィザード ページ（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、[次へ（Next）] をクリックします。

UI 要素	基本情報
[このグループの仮想マシンを次の間隔で保護（Protect virtual machines in this group every）] フィールド	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。
[仮想マシンの保護をすぐに開始（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。
[仮想マシンの保護の開始時刻（Start protecting the virtual machines at）] ラジオ ボタン	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。 • 少なくとも 1 つの仮想マシンが保護グループに追加されている。 • スケジュールされた開始時刻に達している。 保護の開始時刻を指定するには、次のようにします。 1. [仮想マシンの保護の開始時刻（Start protecting the virtual machines at）] ラジオ ボタンをクリックします。 2. [時刻（time）] フィールドをクリックし、時間と分を選択します。フィールドの外をクリックします。 [現在からの時間と分（hours, minutes from now）] は最初のレプリケーションが発生する時を示します。これは、[時刻（time）] フィールドの設定値を変更すると更新されます。 [クラスタのタイムゾーン（Cluster time zone）] と [クラスタの現在の時刻（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。開始時間は、ローカル クラスタの時計に基づいています。次に例を示します。 クラスタの現在の時刻が 13:56:15 で、現在から 10 時間と 3 分後とは、23:59 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。

UI 要素	基本情報
[VMware ツールを使用して仮想マシンを休止する（Use VMware Tools to quiesce the virtual machine）] チェック ボックス	レプリケーション スナップショットを取る前に HX 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。

[仮想マシンの保護（Protect Virtual Machines）] ウィザードの、[概要（Summary）] ページが表示されます。

ステップ 6 [概要（Summary）] ページの情報を確認し、[保護グループに追加（Add to Protection Group）] をクリックします。

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 は、仮想マシンをレプリケーション保護に追加します。[レプリケーション（Replication）] または [仮想マシン（Virtual Machines）] ページを表示して確認します。[レプリケーション（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入れます。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

構成されたレプリケーション ネットワークおよびレプリケーション ペアです。

ステップ 1 管理者権限で HX Connect にログインし、[仮想マシン（Virtual Machines）] を選択します。

これによりローカル 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 [保護（Protect）] をクリックします。

[仮想マシンの保護（Protect Virtual Machine）] ダイアログボックスが表示されます。

ステップ 4 必要に応じてフィールドに入力します。

UI 要素	基本情報
[既存の保護グループに追加（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。 追加の構成は必要ありません。[仮想マシンの保護（Protect Virtual Machine）] をクリックします。
[この仮想マシンを個別に保護（Protect this virtual machine independently）] ラジオ ボタン	間隔、スケジュールオプション、および仮想マシンの保護を定義するための VMware ツール オプションを有効にします。
[この仮想マシンを次の間隔で保護（Protect this virtual machine every）] フィールド	プルダウン リストから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。 15 分、30 分、1 時間、90 分、2 時間、4 時間、8 時間、12 時間、24 時間
[仮想マシンの保護をすぐに開始（Start protecting the virtual machines immediately）] 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
[仮想マシンの保護の開始時刻（Start protecting the virtual machines at）] ラジオ ボタン	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。 • 少なくとも 1 つの仮想マシンが保護グループに追加されている。 • スケジュールされた開始時刻に達している。 保護の開始時刻を指定するには、次のようにします。 1. [仮想マシンの保護の開始時刻（Start protecting the virtual machines at）] ラジオ ボタンをクリックします。 2. [時刻（time）] フィールドをクリックし、時間と分を選択します。フィールドの外をクリックします。 [現在からの時間と分（hours, minutes from now）] は最初のレプリケーションが発生する時を示します。これは、[時刻（time）] フィールドの設定値を変更すると更新されます。 [クラスタのタイムゾーン（Cluster time zone）] と [クラスタの現在の時刻（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。開始時間は、ローカルクラスタの時計に基づいています。次に例を示します。 クラスタの現在の時刻が 13:56:15 で、現在から 10 時間と 3 分後とは、23:59 に最初のレプリケーションが発生することを意味します。
[VMware ツールで仮想マシンを休止する（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 [仮想マシンの保護（Protect Virtual Machine）] をクリックします。

仮想マシンの状態は、[仮想マシン（Virtual Machine）] ページと [レプリケーション（Replication）] ページに更新されます。[レプリケーション（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 （203 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 [仮想マシン（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 [保護を解除（Unprotect）] をクリックし、クリックして確認ます。

仮想マシンの状態が、[保護（protected）] から [非保護（unprotected）] に変わります。

データ保護/リカバリ ワークフロー

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ときに実行されます。そこで、フェールオーバーは、ソースからターゲット クラスタに VM のプライマリ クラスタの関連付けをシフトします。VM と保護されたグループが回復すると、新しいクラスタで再度保護できます。

仮想マシンのリカバリでは、stcli dp vm コマンドを使用して、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。

移行プロセスと区別するために、リカバリ プロセスでは、ソースとターゲット クラスタ間のペアリングが削除（切断）されるので、新しいソース（旧ターゲット）クラスタは新しいクラスタとレプリケーション ペアを形作ることができます。

リカバリ

災害後に使用されます。リカバリでは、移行と同様に、VMの最新のレプリケーションスナップショット コピーが動作中の VM になります。元のソースとターゲット クラスタの間のペアリングは削除（切断）されます。新しいソース（旧ターゲット）クラスタは別のクラスタとペアになることができます。次の手順を実行します。

1. 保護された VM と保護グループの一覧を生成します。

```
# stcli dp vm list --brief
```

2. すべてのレプリケーション アクティビティを停止します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm halt
```

これにより新しいレプリケーションのスナップショットを作成するのに、部分的または破損した VM は使用されません。

3. VM を使用するレプリケーション VM から動作中の VM に、VM のフェールオーバーを回復します。

```
# stcli dp vm recover failover --vmid VMID
```

これはターゲット クラスタのレプリケーション スナップショット コピーを動作中 VM に変更するプロセスを実行します

4. リカバリ テストのステータスをモニタします。

```
# stcli dp vm recover status --id JOB-ID
```

5. 回復された VM コンテンツを確認します。

6. 必要に応じて手順 3 ～ 5 を繰り返して、すべての VM を回復します。

- すべての個別に保護された VM は並列して回復できます。
- それぞれ別の保護グループからの 1 つの VM は、並列して回復できます。
- 保護グループ内では VM を順次に回復する必要があります。並列で実行することはできません。

7. レプリケーション クラスタ ペア間の接続を削除（破棄）します。

```
# stcli dp peer forget
```

これにより、新しいソース（旧ターゲット）クラスタは別の正常なクラスタとペアになることができます。

8. VM の保護を解除し、保護グループを削除します。

```
# stcli dp vm delete --vmid VMID
```

9. 新しいソース（旧ターゲット）クラスタを新しいクラスタとペアにし、個別に、または保護グループで再度 VM を保護します。

仮想マシンのリカバリ

仮想マシンのリカバリでは、stcli dp vm コマンドを使用して、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。

移行プロセスと区別するために、リカバリ プロセスにはソース クラスタとターゲット クラスタ間のペアリングの削除が含まれます。

（注） 個別に保護された、または、別の保護グループに属している仮想マシンでリカバリを実行する場合の同時リカバリ操作の最大数は 20 です。

始める前に

- 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 ターゲット（リカバリ）クラスタ内のノードのコントローラ VM にログインします。

リカバリ クラスタは、レプリケーション スナップショットをコピーしたターゲット 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たクラスタでした。

ステップ 2 リカバリする仮想マシンを特定します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm list --brief
```

このコマンドでは、VM の一意の識別子、BIOS UUID を一覧表示します。

ステップ 3 ソース クラスタからターゲット クラスタへのすべての潜在的なレプリケーションを停止します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm halt
```

stcli dp vm halt [-h] --vmid VMID [--force]

構文の説明

オプション	必須またはオプション	説明
--vmid VMID	必須作業です。	指定した BIOS UUID に一致する仮想マシンでコマンドを実行します。
--force	これはオプションです。	引数の検証とリカバリを行わないでください

ステップ 4 リカバリを実行します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm recover failover --vmid VMID
```

- `folder`、`resourcepool`、`newname`、`poweron`、`test-network` または `network-mapping` などの、任意の省略可能なパラメータを指定してテスト リカバリをカスタマイズします。
- このコマンドは、`job-id` を返します。`job-id` を使ってリカバリの状態をモニタします。

stcli dp vm recover failover [-h] --vmid VMID [--resourcepool-id RESOURCEPOOL-ID | --resourcepool-name RESOURCEPOOL-NAME] [--folder-id FOLDER-ID | --folder-name FOLDER-NAME] [--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]] [--poweron] [--force]

構文の説明

オプション	必須またはオプション	説明
--vmid VMID	必須作業です。	指定した BIOS UUID に一致する仮想マシンでコマンドを実行します。
--resourcepool-id RESOURCEPOOL-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のリソースプールに配置します。
--resourcepool-name RESOURCEPOOL-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のリソースプールに配置します。
--folder-id FOLDER-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のフォルダに配置します。
--folder-name FOLDER-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のフォルダに配置します。
--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]	これはオプションです。	送信元ネットワークを宛先ネットワークにマップします。形式は `source_network:destination_network` です。次に例を示します。 `--network-mapping "source_network1:destination_network1","source_network2:destination_network2"`
--poweron	これはオプションです。	リカバリ後に VM の電源をオンにします
--force	これはオプションです。	引数の検証とリカバリを行わないでください

ステップ 5 前のコマンドからの `job-id` を参照して、ジョブの状態をモニタします。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm recover status --id <job-id> --list
```

```
summary_step_state: SUCCEEDED
Description: Successfully completed Failover recovery for VMID 564d3432-d4fd-5cdc-b742-b3cfad73144c
time_submitted: 08/31/17_23:07
time_elapsed_millis: 588097052
Jobid: ebf813ff-a91a-40b2-a6dd-51564c8092c0
state: COMPLETED
Message: Performing Failover recovery for VMID 564d3432-d4fd-5cdc-b742-b3cfad73144c
time_started: 08/31/17_23:07
```

ステップ 6 ターゲット クラスタの回復された VM のコンテンツを確認します。

`--poweron` オプションが使用され、仮想マシンの電源が自動的にオンにならない場合は、vCenter を介して仮想マシンの電源をオンにします。

ステップ 7 元のソース クラスタとターゲット クラスタ間のレプリケーション ペアの構成を削除します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp peer forget
```

ステップ 8 仮想マシンの保護を解除します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm delete --vmid VMID
```

または、HX Connect を使用して仮想マシンの保護を解除します。

ステップ 9 新しいクラスタとターゲット クラスタをペアリングします。その後で、仮想マシンを保護します。

保護グループの仮想マシンのリカバリ

仮想マシンのリカバリでは、stcli dp group コマンドを使用して、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。

移行プロセスと区別するために、リカバリ プロセスにはソース クラスタとターゲット クラスタ間のペアリングの削除も行われます。

（注） 同じ保護グループ内の仮想マシンでリカバリを実行する場合は、並列にではなく、一度に1つの仮想マシンでリカバリ コマンドを実行します。これはシリアルに行う操作です。同じ保護グループ内の仮想マシンでの並列リカバリはサポートされません。

始める前に

- 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ます。

ターゲット クラスタで、ソース クラスタからターゲット クラスタに仮想マシンを移行するために次を実行します。

ステップ 1 ターゲット（リカバリ）クラスタ内のノードのコントローラ VM にログインします。

リカバリ クラスタは、レプリケーション スナップショットをコピーしたターゲットクラスタです。ソース クラスタは、仮想マシンが存在していたクラスタでした。

ステップ 2 移行する仮想マシンを特定します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp group list --brief
```

このコマンドでは、VM の一意の識別子、BIOS UUID を一覧表示します。

ステップ 3 ソース クラスタからターゲット クラスタへのすべての潜在的なレプリケーションを停止します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp group halt
```

stcli dp group halt [-h] --groupid GROUPID [--force]

構文の説明

オプション	必須またはオプション	説明
--groupid GROUPID	必須作業です。	リストされた groupid に一致する保護グループの仮想マシンのレプリケーションを停止します。
--force	これはオプションです。	引数を検証せずにレプリケーションを停止します。

ステップ 4 リカバリを実行します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm recover failover
```

- `folder`、`resourcepool`、`newname`、`poweron`、`test-network` または `network-mapping` などの、任意の省略可能なパラメータを指定してテスト リカバリをカスタマイズします。
- このコマンドは、`job-id` を返します。`job-id` を使ってリカバリの状態をモニタします。

stcli dp vm recover failover [-h] --vmid VMID [--resourcepool-id RESOURCEPOOL-ID | --resourcepool-name RESOURCEPOOL-NAME] [--folder-id FOLDER-ID | --folder-name FOLDER-NAME] [--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]] [--poweron] [--force]

構文の説明

オプション	必須またはオプション	説明
--vmid VMID	必須作業です。	指定した BIOS UUID に一致する仮想マシンでコマンドを実行します。
--resourcepool-id RESOURCEPOOL-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のリソースプールに配置します。
--resourcepool-name RESOURCEPOOL-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のリソースプールに配置します。
--folder-id FOLDER-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のフォルダに配置します。
--folder-name FOLDER-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のフォルダに配置します。
--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]	これはオプションです。	送信元ネットワークを宛先ネットワークにマップします。形式は `source_network:destination_network` です。次に例を示します。 `--network-mapping "source_network1:destination_network1","source_network2:destination_network2"`

オプション	必須またはオプション	説明
--poweron	これはオプションです。	リカバリ後に VM の電源をオンにします
--force	これはオプションです。	引数の検証とリカバリを行わないでください

ステップ 5 前のコマンドからの `job-id` を参照して、ジョブの状態をモニタします。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm recover status --id <job-id> --list
```

```
summary_step_state: SUCCEEDED
Description: Successfully completed Failover recovery for VMID 564d3432-d4fd-5cdc-b742-b3cfad73144c
time_submitted: 08/31/17_23:07
time_elapsed_millis: 588097052
Jobid: ebf813ff-a91a-40b2-a6dd-51564c8092c0
state: COMPLETED
Message: Performing Failover recovery for VMID 564d3432-d4fd-5cdc-b742-b3cfad73144c
time_started: 08/31/17_23:07
```

ステップ 6 保護グループ内のすべての VM で、ステップ 4 とステップ 5 を繰り返します。

ステップ 7 ターゲット クラスタの回復された VM のコンテンツを確認します。

`--poweron` オプションが使用され、仮想マシンの電源が自動的にオンにならない場合は、vCenter を介して仮想マシンの電源をオンにします。

ステップ 8 仮想マシンの保護を解除します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm delete --vmid VMID
```

または、HX Connect を使用して仮想マシンの保護を解除します。

ステップ 9 元のソース クラスタとターゲット クラスタ間のレプリケーション ペアの構成を削除します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp peer forget
```

ステップ 10 保護グループを削除します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm delete --groupid GROUPID
```

または、HX Connect を使用して保護グループを削除します。

ステップ 11 新しいクラスタとターゲット クラスタをペアリングします。その後で、仮想マシンを保護します。

レプリケーション メンテナンスの概要

レプリケーションは、設定されている場合、定義されているスケジュールごとにバック 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。

  stcli dp vm recover test コマンドを使用します。

- **レプリケーションの一時停止**：HXストレージクラスタ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 ストレージ クラスタ 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ストレージクラスタ のアップグレードが含まれます。通常、HX クラスタ でノードが HX メンテナンス モードに入る必要がある場合、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 ストレージ クラスタ のメンテナンス アクティビティが完了したら、レプリケーション スケジュールを再開します。

  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。

  stcli dp vm recover failover コマンドを使用します。

移行

災害ではなく、定期的なシステム メンテナンスと管理のために、いつでも使用されます。移行では、リカバリと同様に、VM の最新のレプリケーション スナップショット コピーが動作中のVMになります。ソースとターゲットのクラスタ間のペアはそのままです。次の手順を実行します。

1. 保護された VM のリストを生成します。

   ```
   # stcli dp vm list --brief
   ```

2. ソース クラスタでのレプリケーション アクティビティを停止します。

   ```
   # stcli dp vm halt
   ```

   これにより新しいレプリケーションのスナップショットを作成するのに、部分的または破損した VM は使用されません。

3. VM を使用するレプリケーション VM から動作中の VM に、VM のフェールオーバーを回復します。

   ```
   # stcli dp vm recover failover --vmid VMID
   ```

   これはターゲット クラスタのレプリケーション スナップショット コピーを動作中 VM に変更するプロセスを実行します

   クラスタ レプリケーション ペアはそのままです。切断されたピアは使用されません。

4. リカバリ テストのステータスをモニタリングします。

   ```
   # stcli dp vm recover status --id JOB-ID
   ```

5. 回復された VM の内容を検証します。

リカバリ テスト

リカバリ プロセスを保証するメンテナンス タスクは、災害発生時に正常に行われます。次の手順を実行します。

1. 保護された VM のリストを生成します。

```
# stcli dp vm list --brief
```

2. 保護された各 VM でリカバリ テストを行います。

```
# stcli dp vm recover test
```

3. リカバリ テストのステータスをモニタリングします。

```
# stcli dp vm recover status --id JOB-ID
```

4. 回復された VM の内容を検証します。

レプリケーションの一時停止

HX ストレージ クラスタ のメンテナンスを行うための準備をする際に構成済みのレプリケーションがある場合は、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 ストレージ クラスタ 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ストレージクラスタ のアップグレードが含まれます。通常、HXクラスタ でノードがHXメンテナンスモードに入る必要がある場合、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 ストレージ クラスタ のメンテナンスを行うための準備をする際に構成済みのレプリケーションがある場合は、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 ストレージ クラスタ 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ストレージクラスタ のアップグレードが含まれます。通常、HXクラスタ でノー

ドがHXメンテナンスモードに入る必要がある場合、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ストレージクラスタの一時停止と、保守またはアップグレードのタスクの完了を確認します。

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。

仮想マシンのリカバリのテスト

仮想マシンとデータのリカバリは、stcli dp vm コマンドによって行います。リカバリ メソッドが機能しているかどうかをテストするのには、次を実行します。

始める前に

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ます。

ステップ1 リカバリ クラスタ内のノードのコントローラ VM にログインします。

リカバリ クラスタは、レプリケーション スナップショットをコピーしたターゲット 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たクラスタでした。

ステップ2 リカバリする仮想マシンを特定します。コマンドを実行します。

```
# stcli dp vm list --brief
```

このコマンドでは、VM の一意の識別子、BIOS UUID を一覧表示します。

ステップ3 リカバリ テストを実行します。コマンドを実行します。

```
# stcli dp vm recover test
```

- `folder`、`resourcepool`、`newname`、`poweron`、`test-network` または `network-mapping` などの、任意の省略可能なパラメータを指定してテスト リカバリをカスタマイズします。
- このコマンドは、`job-id` を返します。
- デフォルトでは、テスト リカバリは `HxTestRecovery` フォルダ内にある同じ名前の VM を回復します。

stcli dp vm recover test [-h] --vmid VMID [--resourcepool-id RESOURCEPOOL-ID | --resourcepool-name RESOURCEPOOL-NAME] [--folder-id FOLDER-ID | --folder-name FOLDER-NAME] [--test-network TESTNETWORK] [--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]] [--poweron] [--force] [--newname NEWNAME]

構文の説明

オプション	必須またはオプション	説明
--vmid VMID	必須作業です。	指定した BIOS UUID に一致する仮想マシンをリストします。
--resourcepool-id RESOURCEPOOL-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のリソースプールに配置します。
--resourcepool-name RESOURCEPOOL-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のリソースプールに配置します。
--folder-id FOLDER-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のフォルダに配置します。
--folder-name FOLDER-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のフォルダに配置します。
--test-network TESTNETWORK	これはオプションです。	テストリカバリに使用するネットワークをテストします。リカバリ後、すべての送信元ネットワークがこのネットワークに割り当てられます。
--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]	これはオプションです。	送信元ネットワークを宛先ネットワークにマップします。形式は `source_network:destination_network` です。次に例を示します。 `--network-mapping "source_network1:destination_network1","source_network2:destination_network2"`
--poweron	これはオプションです。	リカバリ後に VM の電源をオンにします。
--force	これはオプションです。	引数を検証せずにリカバリを実行します。
--newname NEWNAME	これはオプションです。	テストで回復した VM の新しい名前。

ステップ 4 前のコマンドからの `job-id` を参照して、ジョブの状態をモニタします。コマンドを実行します。

```
# stcli dp vm recover status --id <job-id>
```

stcli dp vm recover status [-h] [--id JOBID [JOBID ...] | --list]

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。

保護された仮想マシンの移行

移行は、災害ではない定期的なシステム メンテナンスと管理のためにいつでも使用できるフェールオーバーの形式です。移行では、リカバリと同様に、VMの最新のレプリケーション スナップショット コピーが動作中の VM になります。ソースとターゲットのクラスタ間のペアはそのままです。

始める前に

- 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ます。

ターゲット クラスタで、ソース クラスタからターゲット クラスタに仮想マシンを移行するために次を実行します。

ステップ 1 ターゲット クラスタ内のノードのコントローラ VM にログインします。

レプリケーション スナップショットをコピーしたターゲット 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たクラスタでした。

ステップ 2 移行する仮想マシンを特定します。コマンドを実行します。

```
# stcli dp vm list --brief
```

このコマンドでは、VM の一意の識別子、BIOS UUID を一覧表示します。

ステップ 3 ソース クラスタからターゲット クラスタへのすべての潜在的なレプリケーションを停止します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp vm halt
```

stcli dp vm halt [-h] --vmid VMID [--force]

構文の説明

オプション	必須またはオプション	説明
--vmid VMID	必須作業です。	指定した BIOS UUID に一致する仮想マシンでコマンドを実行します。
--force	これはオプションです。	引数の検証とリカバリを行わないでください

ステップ 4 移行を実行します。コマンドを実行します。

```
# stcli dp vm recover failover
```

- folder、resourcepool、newname、poweron、test-network または network-mapping などの、任意の省略可能なパラメータを指定してテスト リカバリをカスタマイズします。
- このコマンドは、job-id を返します。job-id を使ってリカバリの状態をモニタします。

stcli dp vm recover failover [-h] --vmid VMID [--resourcepool-id RESOURCEPOOL-ID | --resourcepool-name RESOURCEPOOL-NAME] [--folder-id FOLDER-ID | --folder-name FOLDER-NAME] [--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]] [--poweron] [--force]

構文の説明

オプション	必須またはオプション	説明
--vmid VMID	必須作業です。	指定した BIOS UUID に一致する仮想マシンでコマンドを実行します。
--resourcepool-id RESOURCEPOOL-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のリソース プールに配置します。
--resourcepool-name RESOURCEPOOL-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のリソース プールに配置します。
--folder-id FOLDER-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のフォルダに配置します。
--folder-name FOLDER-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のフォルダに配置します。
--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]	これはオプションです。	送信元ネットワークを宛先ネットワークにマップします。形式は source_network:destination_network です。次に例を示します。 --network-mapping "source_network1:destination_network1","source_network2:destination_network2"
--poweron	これはオプションです。	リカバリ後に VM の電源をオンにします
--force	これはオプションです。	引数の検証とリカバリを行わないでください

ステップ 5 前のコマンドからの job-id を参照して、ジョブの状態をモニタします。コマンドを実行します。

```
# stcli dp vm recover status --id <job-id>
```

ステップ 6 ターゲット クラスタの回復された VM のコンテンツを確認します。

ステップ 7 元のソース クラスタから保護構成を削除します。

a) ソース クラスタにログインします。

b) すべての仮想マシンの保護を解除します。コマンドを実行します。

```
# stcli dp vm delete --vmid VMID
```

または、HX Connect を使用して仮想マシンの保護を解除します。

c) 電源をオフにして、元の VM を削除します。

ステップ 8 HX Connect を介してターゲット クラスタにログインし、仮想マシンの保護を再構成します。

保護グループの仮想マシンの移行

移行は、災害ではない定期的なシステム メンテナンスと管理のためにいつでも使用できるフェールオーバーの形式です。移行では、リカバリと同様に、VMの最新のレプリケーション スナップショット コピーが動作中の VM になります。ソースとターゲットのクラスタ間のペアはそのままです。

始める前に

- 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ます。

ターゲット クラスタで、ソース クラスタからターゲット クラスタに仮想マシンを移行するために次を実行します。

ステップ 1 ターゲット クラスタ内のノードのコントローラ VM にログインします。

レプリケーション スナップショットをコピーしたターゲット 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たクラスタでした。

ステップ 2 移行する仮想マシンを特定します。コマンドを実行します。

```
# stcli dp group list --brief
```

このコマンドでは、VM の一意の識別子、BIOS UUID を一覧表示します。

ステップ 3 ソースクラスタからターゲットクラスタへのすべての潜在的なレプリケーションを停止します。ターゲット クラスタでコマンドを実行します。

```
# stcli dp group halt
```

stcli dp group halt [-h] --groupid GROUPID [--force]

構文の説明	オプション	必須またはオプション	説明
	--groupid GROUPID	必須作業です。	リストされた groupid に一致する保護グループの仮想マシンのレプリケーションを停止します。

オプション	必須またはオプション	説明
--force	これはオプションです。	引数を検証せずにレプリケーションを停止します。

ステップ 4 移行を実行します。コマンドを実行します。

```
# stcli dp vm recover failover
```

- `folder`、`resourcepool`、`newname`、`poweron`、`test-network` または `network-mapping` などの、任意の省略可能なパラメータを指定してテスト リカバリをカスタマイズします。
- このコマンドは、`job-id` を返します。`job-id` を使ってリカバリの状態をモニタします。

stcli dp vm recover failover [-h] --vmid VMID [--resourcepool-id RESOURCEPOOL-ID | --resourcepool-name RESOURCEPOOL-NAME] [--folder-id FOLDER-ID | --folder-name FOLDER-NAME] [--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]] [--poweron] [--force]

構文の説明

オプション	必須またはオプション	説明
--vmid VMID	必須作業です。	指定した BIOS UUID に一致する仮想マシンでコマンドを実行します。
--resourcepool-id RESOURCEPOOL-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のリソースプールに配置します。
--resourcepool-name RESOURCEPOOL-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のリソースプールに配置します。
--folder-id FOLDER-ID	省略可能なペアの 1 つ。	回復した VM を指定された ID のフォルダに配置します。
--folder-name FOLDER-NAME	省略可能なペアの 1 つ。	回復した VM を指定された名前のフォルダに配置します。
--network-mapping NETWORKMAPPING [NETWORKMAPPING ...]	これはオプションです。	送信元ネットワークを宛先ネットワークにマップします。形式は `source_network:destination_network` です。次に例を示します。 `--network-mapping "source_network1:destination_network1","source_network2:destination_network2"`
--poweron	これはオプションです。	リカバリ後に VM の電源をオンにします
--force	これはオプションです。	引数の検証とリカバリを行わないでください

ステップ 5 前のコマンドからの `job-id` を参照して、ジョブの状態をモニタします。コマンドを実行します。

```
# stcli dp vm recover status --id <job-id>
```

ステップ 6 保護グループ内のすべての VM で、ステップ 4 とステップ 5 を繰り返します。

（注） 保護グループ内の VM に対して、一度に 1 つの仮想マシンで stcli dp vm recover failover コマンドを実行します。これはシリアルに行う操作です。同じ保護グループ内の VM でのパラレル リカバリはサポートされていません。

ステップ 7 ターゲット クラスタの回復された VM のコンテンツを確認します。

ステップ 8 元のソース クラスタから保護構成を削除します。

a) ソース クラスタにログインします。

b) すべての仮想マシンの保護を解除します。コマンドを実行します。

```
# stcli dp vm delete --vmid VMID
```

または、HX Connect を使用して仮想マシンの保護を解除します。

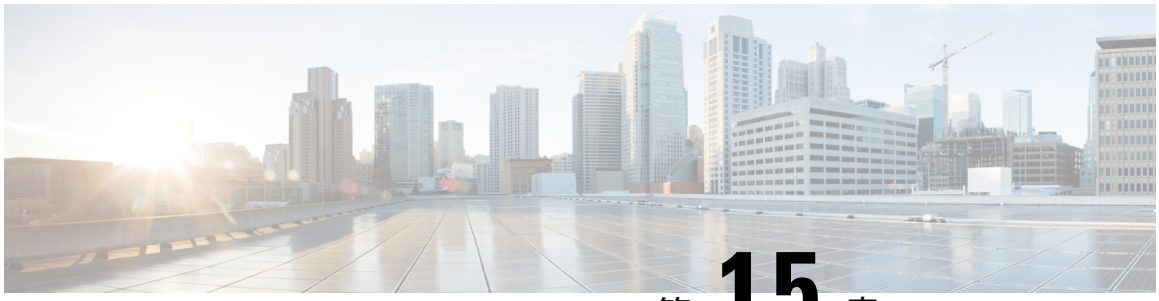
c) 電源をオフにして、元の VM を削除します。

d) 保護グループを削除します。

```
# stcli dp vm delete --groupid GROUPID
```

または、HX Connect を使用して保護グループを削除します。

ステップ 9 HX Connect を介してターゲット クラスタにログインし、仮想マシンの保護を再構成します。



第 15 章

ユーザの管理

- HyperFlex ユーザの管理の概要 （211 ページ）
- HX データ プラットフォーム RBAC ユーザの作成 （214 ページ）
- ユーザへの権限の割り当て （214 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 クラスタ 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 クラスタ 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 の役割、`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 の役割、`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。

ユーザ（User）	HX Data Platform インストーラ	HX Connect	HX Data Platformstcli コマンド ラインを使用したストレージコントローラ VM	vCenter を介した HX Data Platform プラグイン	HX REST API
admin	必須（Required）	`local/` プレフィックスが必要です。例：`local/admin`	管理者権限 ほとんどの HX タスクを実行できます。	管理者権限 すべての HX タスクを実行できます。	`local/` プレフィックスが必要です。例：`local/admin`
root	オプション	`local/` プレフィックスが必要です。例：`local/admin`	root 権限 すべての HX タスクを実行できます。	root 権限 すべての HX タスクを実行できます。	`local/` プレフィックスが必要です。例：`local/admin`
hx-admin-user	無効	管理者権限 ほとんどの HX タスクを実行できます。 優先ユーザ。	`vc-` プレフィックスが必要です。例：`vc-hxadmin` 管理者権限 ほとんどの HX タスクを実行できます。	vCenter SSO ユーザ。 管理者権限 ほとんどの HX タスクを実行できます。	`vc-` プレフィックスが必要です。例：`vc-hxadmin` 管理者権限 ほとんどの HX タスクを実行できます。
hx-readonly-user	無効	読み取り専用権限 モニタリング情報を参照するのみができます。ほとんどの HX タスクは実行できません。 優先ユーザ。	`vc-` プレフィックスが必要です。例：`vc-hxreadonly` 読み取り専用権限 モニタリング情報を参照するのみができます。ほとんどの HX タスクは実行できません。	vCenter SSO ユーザ。 読み取り専用権限 モニタリング情報を参照するのみができます。ほとんどの HX タスクは実行できません。	`vc-` プレフィックスが必要です。例：`vc-hxreadonly` 読み取り専用権限 モニタリング情報を参照するのみができます。ほとんどの HX タスクは実行できません。

ユーザ管理用語

- **認証**：ログイン クレデンシャル用。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**：アクセス許可用。これらのプロセスは、ユーザの ID に基づいて、ユーザ/クライアントアプリケーションが、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を実行などの、いくつかのアクションを実行することを許可します。承認は、認証済みユーザがサーバ上での実行を許可されることを定義します。
- **アカウンティング**：ユーザ操作の追跡用。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、付与された権限を持つロールを割り当てられている ID がプロビジョニングされます。
- **権限**：リソースを使用するためにロールに与えられる設定。これは、ロール、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、ロールの変更はデータストアをマウントするために付与された権限ですが、読み取り専用ロールは、データストアが存在することを表示できるだけです。
- **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**：GET、POST、DELETE、HEAD、およびその他の HTTP 動詞を使用して HTTP 経由でその機能と管理制御が公開されている、HX プラットフォーム全体です。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、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すべてのリソースです。
- **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 アカウンティングの監査ログ

AAA アカウンティングをサポートするため、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。

  サンプル エントリです。キーワード `Audit` をメモします。

```
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、同様に他の情報が含まれています。監査イベントのフィルタ処理は、スクリプトを使用して単語 `Audit` をフィルタします。

- **audit.log**：REST API アクティビティの監査レコードが含まれます。

  サンプル エントリです。ユーザ名 `administrator@vsphere.local` をメモします

  ```
  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。VMware vCenter インターフェイスを介して HX Data Platform の新しいユーザが作成されます。

始める前に

ユーザを作成するには、管理者特権が必要です。

ステップ 1 vCenter 管理者として vSphere Web クライアント にログインします。

ステップ 2 [ナビゲーター ホーム（Navigator Home）] から、**[管理（Administration）] > [ユーザとグループ（Users and Groups）] > [ユーザ（Users）]** に進みます。

ステップ 3 [追加（Add）]（+）アイコンをクリックして、ユーザを追加します。 [ユーザの新規作成（New User）] の情報を入力し、[OK] をクリックします。

新しいユーザの [ユーザ名（User Name）] および [パスワード（Password）] 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唯一の特殊文字は、アンダースコア（_）、ダッシュ（-）、ドット（.）です。ユーザ名とパスワード要件についてはHX Data Platform の名前、パスワード、および文字 （27 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 （214 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 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 クライアントで、**[ナビゲータ ホーム（Navigator Home）] > [管理者（Administration）] > [グローバル権限（Global Permissions）] > [管理（Manage）]** の順に選択します。

ステップ 2 [追加（Add）]（+）アイコンをクリックして権限を割り当てます。

ステップ 3 [割り当て済みの権限（Assigned Role）] を選択します。

[グローバル権限ルート - 権限の追加（Global Permission Root - Add Permission）] ダイアログボックスで、[割り当て済みの権限（Assigned Role）] ドロップダウン メニューから選択します。次のいずれかを実行します。

- **管理者（Administrator）**
- **読み取り専用（Read only）**

ステップ 4 [ユーザとグループ（Users and Groups）] 領域で、[追加（Add）] をクリックします。

ステップ 5 [ユーザ/グループの選択（Select Users/Groups）] ダイアログボックスで、*user_name* を選択して [追加（Add）] をクリックします。

ステップ 6 [名前確認（Check names）] ボタンをクリックしてユーザ名を確認します。

ステップ 7 [OK] をクリックして各ダイアログボックスを閉じます。