Cisco HX Data Platform リリース 4.0 のリリース ノート

初版：2019 年 5 月 2 日

最終更新：2020 年 5 月 11 日

はじめに

Cisco HyperFlex™ システムは、ハイパーコンバージド システムのデザインが持つ力を最大限に活用できます。ソフトウェア デファインド インフラをベースとするこのシステムでは、Cisco Unified Computing System（Cisco UCS）サーバによるソフトウェア デファインドのコンピューティング、強力な Cisco HX Data Platform を利用したソフトウェア デファインド ストレージ、そして Cisco Application Centric Infrastructure（Cisco ACI）とも連携・統合可能な Cisco UCS ファブリックによるソフトウェアデファインドネットワーキングが一元化されています。こうしたテクノロジーにより接続とハードウェア管理を一元化することで、統合されたリソース プールをビジネス ニーズに合わせて提供できる、適応性の高い統合クラスタが実現します。

これらのリリース ノートは、Cisco HX Data Platform リリース 4.0 に関連しており、Cisco HX Data Platform の機能、制限事項、および問題について説明しています。

マニュアルの変更履歴

リリース	日付	説明
4.0(2b)	2020 年 5 月 11 日	4.0(2b) リリースの新機能で、ストレッチ クラスタ アップデートの OTV を追加しました。

リリース	日付	説明
4.0(2a)	2020 年 5 月 5 日	HX 4.0(2a) 新機能のセクションを、Cisco UCSM 4.1(1c) リリースからの、UCSM ハードウェアとソフトウェアの強化点と機能が含まれるようにアップデートしました。 M5 向けのホストアップグレードユーティリティ (HUU) を、HX 4.0(2a) に合わせて UCS 4.0(4k) にアップデートしました。
4.0(2b)	2020 年 4 月 22 日	Cisco HX Data Platform ソフトウェア リリース 4.0(2b) のリリース ノートを作成しました。
4.0(1b)	2020 年 3 月 30 日	M4 および M5 推奨 FI/サーバ ファームウェアを、HX 4.0(1b) に合わせて UCS 4.0(4h) にアップデートしました。
4.0(2a)	2020 年 3 月 24 日	M4 および M5 推奨 FI/サーバ ファームウェアを、HX 4.0(2a) に合わせて UCS 4.0(4h) にアップデートしました。
4.0(2a)	2020 年 2 月 11 日	Cisco HX Data Platform ソフトウェア リリース 4.0 (2a) のリリース ノートを作成しました。
3.5 (2c)	2020 年 1 月 15 日	延期されている Cisco HyperFlex リリース HX 3.5(2c) のリリース ノートの更新。
4.0(1b)	2019 年 12 月 23 日	HX 4.0(1b)、4.0(1a)、3.5(2f)、3.5(2e)、および 3.5(2d) の場合、M4 および M5 推奨 FI/サーバ ファームウェアを UCS 4.0(4e) に更新しました。
4.0(1b)	2019 年 12 月 13 日	HX 4.0(1b) および HX 4.0(1a) の解決済み警告のリストに CSCvs28167 を追加しました。

リリース	日付	説明
4.0(1b)	2019 年 11 月 25 日	未解決の問題リストに CSCvs02466 が追加されました。
4.0(1b)	2019 年 11 月 7 日	3.x 展開向け HyperFlex Edge およびファームウェア互換性マトリックスの更新 ストレージ クラスタ仕様の情報が更新されました。
4.0(1b)	2019 年 10 月 25 日	セキュリティ修正の一覧に CSCvj95606 および CSCvq24176 を追加しました。
4.0(1b)	2019 年 10 月 8 日	推奨される FI/サーバー ファームウェアのバージョンを更新しました。
4.0(1b)	2019 年 9 月 30 日	4.x 展開向け HyperFlex Edge およびファームウェア互換性マトリックスの HUU/CIMC 情報更新
4.0(1b)	2019 年 9 月 17 日	「関連する問題」の新しいセクションに CSCvq41985 が追加されました。
4.0(1b)	2019 年 9 月 16 日	4.x 展開向け HyperFlex Edge およびファームウェア互換性マトリックスの HUU/CIMC 情報更新
4.0(1b)	2019 年 9 月 10 日	3.x および 4.x 展開向け HyperFlex Edge およびファームウェア互換性マトリックスの HUU/CIMC 情報更新
4.0(1b)	2019 年 8 月 28 日	HyperFlex リリース 4.0(1b)、3.5 (2e) および 3.5 (2d) の HUU/CIMC 推奨ファームウェア バージョンが更新されました。

リリース	日付	説明
4.0(1b)	2019 年 8 月 23 日	HyperFlex リリース 3.5 (2e) および 3.5 (2d) の推奨 FI/サーバ ファームウェア バージョンが更新されました。
4.0(1b)	2019 年 8 月 21 日	4.x 展開向け HyperFlex Edge およびファームウェア互換性マトリックスに、Cisco IMC バージョン サポート情報が追加されました。
4.0(1b)	2019 年 8 月 19 日	Cisco HX Data Platform ソフトウェア リリース 4.0 (1b) のリリース ノートを作成しました。
4.0(1a)	2019 年 8 月 8 日	「アップグレード ガイドライン」セクションの「サポートされていない Cisco HX リリースの Cisco HyperFlex システム アップグレード ガイド」を説明する箇条書きを追加しました。
4.0(1a)	2019 年 8 月 5 日	HyperFlex が UCS server ファームウェア 4.0 (4a)、4.0 (4b)、および 4.0 (4c) をサポートしていないことを説明した重要な注意事項が追加されました。
4.0(1a)	2019 年 7 月 25 日	「4.x 展開のHyperFlex Edge およびファームウェア互換性マトリックス」のセクション」の HX220c M5/HXAF220c M5 クラスタから VIC 1457 へのコンポーネント情報が更新されました。

リリース	日付	説明
4.0(1a)	2019 年 7 月 22 日	• 「サポートされている VMware vSphere バージョンおよびエディション」の ESXi 6.7 U2 のリリース 3.5 (2e) サポートが追加され、ESXi 6.7 U2 の 3.5(2d)、3.5(2c)、3.5(2b) サポートが更新されました。 • リリース 3.5 (2e) の監視ノードバージョンが追加されました。
4.0(1a)	2019 年 7 月 5 日	リリース 4.0 (1a) の未解決の問題のリストに CSCvq39523 が追加されました。
4.0(1a)	2019 年 7 月 1 日	• 「サポートされているバージョンとシステム要件」セクションで、SED ベース HyperFlex システムの UCS Manager の重要なノートが更新されました。 • 「サポートされている VMware vSphere バージョンおよびエディション」の ESXi 6.7 U2 のリリース 3.5 (2b) サポートが更新されました。
4.0(1a)	2019 年 6 月 20 日	• リリース 4.0 (1a) の未解決の問題のリストに CSCvp64140 と CSCvp98910 が追加されました。 • HyperFlex Edge およびファームウェアの互換性の表を更新しました。

リリース	日付	説明
4.0(1a)	2019 年 6 月 17 日	更新されたブラウザの推奨事項
4.0(1a)	2019 年 5 月 31 日	4.0(1a) 機能が、Intersight 仮想アプライアンスおよび Intersight.com でサポートされていることを示す情報が追加されました。
4.0(1a)	2019 年 5 月 21 日	• 3.5 (2b) および 4.0 (1a) の M4/M5 推奨 FI/サーバ ファームウェアが更新されました。 • 「アップグレードのガイドライン」セクションで、Hypercheck Health Check Utility の推奨される使用方法を説明する箇条書きを追加しました。
4.0(1a)	2019 年 5 月 14 日	• DISA STIG の互換性に関する新機能の説明が追加されました。 • Hyper-V のストレージV クラスタ仕様が更新されました。 • 未解決の問題リストに CSCvp66277 が追加されました。
4.0(1a)	2019 年 5 月 8 日	• 4.0 (1a) の VMware vCenter バージョンが更新されました。 • サポートされる Microsoft ソフトウェア バージョンが更新されました。

リリース	日付	説明
4.0(1a)	2019 年 5 月 3 日	• 解決済みの問題リストに CSCvo36198 と CSCvk38003 が追加されました。 • 未解決の問題リストに CSCvp21417 が追加されました。
4.0(1a)	2019 年 4 月 29 日	Cisco HX Data Platform ソフトウェア リリース 4.0 (1a) のリリース ノートを作成しました。

新機能

Cisco HX Data Platform リリース 4.0 では、次の機能が提供されています。HyperFlex Edge クラスタの非表示のクラウド監視を含むこれらの機能は、Intersight 仮想アプライアンスと Intersight.com の両方でサポートされています。

リリース 4.0(2b) の新機能

- **7.6 TB SSD データドライブ**: HX Edge の設定でサポートされます。
- **すべての NVMe とすべてのフラッシュでの上限値が増加**: すべての NVMe (1TB、4TB、および 8TB) およびすべてのフラッシュ (7.6TB SSD) で上限値が増加しています。
- **クラスタのスケール上限値の増加**: クラスタでの最大スケールの上限値をサポート。Cisco HX Data Platform ストレージ クラスタの仕様 （20 ページ）を参照してください。
- **HW オフロード オプション**: ストレッチ クラスタ設定のハードウェア オフロード オプションをサポートします。
- **ストレッチ クラスタの Cisco Overlay Transport Virtualization**: ストレッチ クラスタのオーバーレイとして OTV をサポートします。

リリース 4.0(2a) の新機能

- **Cisco UCS Manager 4.1(1c)**—Cisco UCSM 4.1(1c) リリースからの、UCSM のハードウェアとソフトウェアの強化点と機能をサポートします。
- **ブースト モード**：このリリースでは、All NVMe、All Flash C240、All Flash C220、Hypervisor: ESX の設定に対してブースト モードが導入されています。ブースト モードを使用すると、Cisco HyperFlex クラスタでは、ストレージ コントローラ VM の CPU リソースを 4 vCPU で増やしより高い IOP を実現できます。設定情報については、『Cisco HyperFlex Data Platform 管理ガイド』を参照してください。

- **VMware vCenter 用の Cisco HyperFlex HTML プラグイン**：仮想化管理者は、vSphere クライアント UI から HyperFlex Connect をクロス起動し、HyperFlex Connect UI で管理アクションを実行することにより、Cisco HyperFlex 物理インフラストラクチャを管理およびモニタすることができます。
- **HX Edge の 25GE ネットワーキング**：HX Edge の 25GE ネットワーキングのサポート。
- **ストレッチ クラスタを備えた All NVMe**：ストレッチ クラスタ (ESX のみ) を備えた All NVMe をサポートします。
- **クラスタ アップグレードの資格テスト**：このリリースでは、アップグレード前にクラスタの準備状況をチェックするアップグレード前のテストを実行する機能が追加されています。チェックの例として、クラスタの状態の検証、再調整ステータス、コントローラ Vm の空き容量、ESXi のバージョンなどがあります。資格テストは、アップグレード プロセス中に発生する可能性のある予期しない問題を回避するために役立ちます。HyperFlex のアップグレードを実行する前にテストを実行することを強くお勧めします。
- **Smart Software Licensing の登録**：このリリースでは、ライセンスのステータスやソフトウェア使用率の傾向の追跡を容易にし、3 つのコア ライセンス機能である購入、管理、およびレポートをシンプルにするソフトウェアのサポートを追加します。
- **自己署名証明書の動的生成の拡張機能**：このリリースでは、以前のリリースで静的だったコントローラ VM で、自己署名 SSL 証明書のサポートが追加されています。静的証明書は、HXDP 4.0 (2a) へのアップグレード時に動的に生成された自己署名証明書に置き換えられるため、証明書はクラスタごとに固有になります。HXDP 4.0 (2a) とともにインストールされた新しいクラスタには、自己署名証明書が動的に生成されます。
- **アップグレード適性テスト**: このリリースでは、アップグレードのためのクラスタの準備状況と、インフラストラクチャの互換性をテストするためのサポートが追加されています。詳細については、『**Cisco HyperFlex Systems Upgrade guide for VMware ESXi, release 4.0**』または『Cisco HyperFlex Upgrade guide For Microsoft Hyper-V, release 4.0 』の「アップグレード適性テスト (Test Upgrade Eligibility)」の項を参照してください。

ディザスタ リカバリ

- **[リカバリ設定 (Recovery Settings Configuration)]**: このリリースでは、リカバリ設定をサポートして、リカバリ サイト間でのリソースのグローバル リカバリ パラメータとマッピングを定義できます。これらのパラメータは、リカバリ、リカバリのテスト、および移行操作の際に使用されます。
- **HyperFlex DR Powershell ランブック**：Powershell ランブック機能は、すべてのリカバリシナリオのために、ランブックのリカバリ設定をサポートするように拡張されています。New-HXrunbook ブックレットを使用して、複数の保護グループのランブックを生成できるようになりました。さらに、2 個の新しいコマンドレット、Wait-HXTask、および Get-HXTaskStatus が導入されました。
- **保護された仮想マシンのスケーラビリティ**：このリリースでは、双方向でクラスタごとに両方のクラスタおよび 750 VM 上の 1500 VM のサポートを追加し、1500 VM の制限を超

えることなく 2 個のクラスタ間で分割されます。詳細については、『Cisco HyperFlex Data Platform 管理ガイド』を参照してください。

- **システム管理 REST API の拡張**: RESY API を使用してデータ レプリケーション アクションを短時間で一時停止し、ユーザーに対してレプリケーションアクションの現在のステータスを明示的に通知します。

Hyper-V 用のデータプラットフォームを備えた Cisco HyperFlex

- **クラスタ対応更新 (CAU)**：これは、アップグレード プロセス中に可用性をほとんどまたはまったく失わずに、フェールオーバ クラスタ内の Windows サーバで更新を実行できる自動機能です。

新しいドライブのサポート：新しいドライブは 4.0 (2a) リリース用に認定されています。新しいドライブには、新しい容量ポイントと新しいキャッシュ ドライブ オプションが含まれています。新しいドライブの一部には、4.0(2a) で認定されている既存のドライブをすでに認定している代替ドライブがあります。これらのドライブは、既存のドライブと機能的に互換性があり、既存のドライブが使用できない場青には代替として使用できます。既存のクラスタの拡張、または異なるドライブの相互運用性に関する一般情報については、『 Cisco HyperFlex ドライブの互換性』を参照してください。

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

ドライブ機能	ドライブ PID	該当するプラットフォーム
代替ブート ドライブ	HX-M2-960GB	すべての既存の HX M5 サーバ
代替システム (またはハウスキーピング) ドライブ	HX-SD480G6I1X-EV	All NVMe を除くすべての既存の HX M5 サーバ
代替システム (またはハウスキーピング) ドライブ	HX-SD480GM1X-EV	All NVMe を除くすべての既存の HX M5 サーバ
All Flash の 800G 12G SAS キャッシュ ドライブ オプション	HX-SD800G123X-EP	次の HX M5 サーバ： HXAF220C-M5SX、 HXAF240C-M5SX、 HXAF-E-220M5SX
All NVMe 1TB 容量ドライブ	HX-NVME2H-I1000	All NVMe：HXAF220C-M5SN
All NVMe 4TB 容量ドライブ	HX-NVME2H-I4000	All NVMe：HXAF220C-M5SN
新しい高密度 All NVMe 8TB 容量ドライブ	HX-NVMEHW-I8000	All NVMe：HXAF220C-M5SN

ドライブ機能	ドライブ PID	該当するプラットフォーム
新しい高密度 All Flash 7.6 TB 容量ドライブ HX AF C240 のノードあたりの最大数は 12 台です。	HX-SD76T61X-EV	全フラッシュ構成: HXAF220C-M5SX、 HXAF240C-M5SX、 HXAF-E-220M5SX ESX のサポートのみ。
8TB LFF 容量の代替ドライブ	HX-HD8T7K4KAN	HX240C-M5L
新しい 3.8TB FIPS 準拠 SED SSD データ ドライブ	HX-SD38T2HTNK9	HXAF220C-M5SX、 HXAF240C-M5SX
新しい 960G FIPS 準拠 SED SSD データ ドライブ	HX-SD960G2HTNK9	HXAF220C-M5SX, HXAF240C-M5SX

リリース 4.0 (1b) の新機能

- **第 2 世代 intel® Xeon® スケーラブル プロセッサ更新のサポート**: このリリースには、第 2 世代 Intel® Xeon® スケーラブル プロセッサ リフレッシュ (以前の Cascade Lake) のサポートが含まれています。

リリース 4.0 (1a) の新機能

リリース 4.0 (1a) には、次の新機能があります。

- **超軽量 HyperFlex Edge クラスタ**: このリリースでは、2 ノードの HyperFlex edge クラスタのサポートが導入され、小規模なフットプリントを必要とする環境で HyperFlex を実行できるようになりました。Cisco Intersight は、包括的なライフサイクル管理を提供します。リモート クラウドベースのインストール、集中型アップグレード、および非表示監視が含まれます。1GE と10GE ネットワーキングの両方のトポロジ オプションを使用できます。

- **拡張された HyperFlex Edge クラスタ**: このリリースでは、4 ノードの HyperFlex edge クラスタのサポートが追加され、リモート オフィスとブランチ オフィスのフルレンジ サイズのオプションが有効になります。2、3、または 4 ノードの HyperFlex Edge クラスタの現在のニーズに合わせて、ブランチ オフィス環境をサイジングします。Cisco Intersight は、フル イフサイクル管理と 1GE を提供し、10GE ネットワーキング オプションを使用できます。

- **Cisco Intersight 非表示クラウド監視**: 2 ノード クラスタでは、この機能により監視 VM、それらの vm を実行するインフラストラクチャ、および監視ソフトウェアの導入、拡張、パッチするための管理オーバーヘッドが不要になります。非表示クラウド監視は、障害が発生した場合にクラスタ HA を維持する役割を担います。この機能は追加コストなしで追加され、Cisco Intersight によって自動的に展開および管理されます。

- **クラウドによって提供される HyperFlex Edge のアップグレード**: Cisco Intersight によるこの機能では、HyperFlex Data Platform のマルチサイト オーケストレーション リモート アップグレードのサポートが追加されます。この機能は次の4.0パッチリリースで有効になり、

Interswitch を介して展開された HyperFlex Edge クラスタは、同時に 1 つまたは複数のサイト間でオーケストレーション アップグレードを実行できます。

- **オール NVMe HyperFlex**: このリリース以降、すべての NVMe ドライブから供給された新しいハイエンド パフォーマンス ノードを HyperFlex クラスタで使用できます。Intel と提携し、ホットプラグおよび突然の削除のために Intel VMD をサポートするように設計されています。この提供サービスは、エンタープライズ対応および完全に検証されたすべての NVMe HCI アプライアンスを業界で初めて公表しています。オール NVMe による機能は、220 フォーム ファクタ (1RU) で使用でき、最大パフォーマンスと最高の耐久性を実現するため、Intel Optane キャッシュ ドライブによって供給されています。

- **VMware Site Recovery Manager (SRM) 統合**: このリリースでは、SRM 向けに開発された Cisco のストレージ複製アダプタ (SRA) のサポートを提供します。SRA は、SRM の強力なオーケストレーションおよびランブック機能により、HyperFlex ネイティブ非同期複製を利用する機能を提供します。SRA には、テスト復元、計画された移行、および完全な障害復旧を実行する機能が含まれています。

  （注） HX SRA は VMware によって認定されており、VMWare SRM サイトからダウンロードすることができます。

- **HYPERFLEX DR Powershell のランブック**: HyperFlex のネイティブ障害復旧を使用する場合、自動ランブックの生成には新しい Powershell コマンドレットが含まれています。新しい-HXRunbook ブックレットは、テスト復元、計画された移行、および障害復旧の各ワークフローをサポートしています。これらのランブックは、サードパーティ製ソフトウェアの要件を必要とせず、DR ワークフローをオーケストレーションするために使用できます。

- **Hyper-V を搭載した Windows server 2019**: Hyper-V ベースの HyperFlex 展開の Windows Server 2019 オペレーティング システム用に、このリリースでサポートが追加されました。

- **KUBERNETES CSI プラグイン**: このリリースでは、Kubernetes Container Storage INTERFACE (CSI) 仕様に基づいて、HYPERFLEX CSI (HX) プラグインのサポートが追加されています。お客様は HX を使用して、Kubernetes バージョン1.13 以降で永続ボリュームをプロビジョニングおよび管理できます。注: Cisco Container Platform & Openshift Container Platform の Kubernetes 1.13 サポートは、それぞれの今後のリリースでサポートされています。

- **C480 Ml コンピューティング専用ノード**: このリリースでは、ディープラーニング/機械学習ワークロード用の新しいコンピューティング専用ノードとして、C480 ML のサポートが導入されています。Data scientists は、最大 8 個の NVidia SXM2 V100 GPU の電力を使用して、ディープ ラーニング ワークロードを高速化できるようになりました。ディープ ラーニング ワークロードを実行している VM では、GPU へのアクセスに PCIe パススルーを使用する必要があります。

- **高容量ドライブ**: SFF ハイブリッド HyperFlex クラスタ用の新しい 2.4 tb 10K RPM SAS HDD オプションと、LFF ハイブリッド用の 12tb 7.2 k RPM SAS HDD オプションが使用可能になりました。HyperFlex および HyperFlex Edge はどちらも、このフォームファクタで最大密度の 2.4 TB 容量ポイントをサポートします。HyperFlex Edge は LFF ドライブをサポー

トしていないことに注意してください。HyperFlex HyperV バージョンでは、新しい 12TB ドライブ オプションはまだサポートされていません。設定可能なオプションの完全なリストについては、HyperFlex 仕様シートを参照してください。

- **Hyper-v の新しいキャッシュとスケールの拡張**: NVMe & Optane SSD は、Hyper-V 導入のキャッシュ ドライブとしてサポートされるようになりました。さらに、スケール制限は、SFF (AF およびハイブリッド) & LFF (ハイブリッド) クラスタの両方に対して 16 + 16 (コンバージド + コンピューティング専用) に増加しました。
- **集中型監査ログのエクスポート**: このリリースでは、リモート syslog サーバによる監査ロギングのサポートが追加されています。この機能により、顧客は集中型リモート syslog サーバのすべての HyperFlex ノードからの監査ログを保持して、保持とコンプライアンスの要件を満たすことができます。
- **DISA の不適合**: このリリースでは、コントローラ VM、ESXi ホスト、および VCENTER の Disa stig の設定、削除、および確認のための新しい HX REST API が追加されています。これらの API を使用すると、顧客は STIF を一元的かつ安全に適用し、STG 設定の流用を検出し修正することで、DISA のセキュリティ要件を満たすことができます。

サポート対象バージョンおよびシステム要件

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

すべての要件については、以下を参照してください。

- VMware ESXi の Cisco HyperFlex システム インストール ガイド または
- Cisco HyperFlex Systems インストール ガイド（Microsoft Hyper-V 用）

ハードウェアおよびソフトウェアの相互運用性

ハードウェアとソフトウェアの相互依存関係の一覧については、それぞれの Cisco UCS Manager リリース バージョンの Cisco HyperFlex HX シリーズにおけるハードウェアおよびソフトウェアの相互運用性 [英語] を参照してください。

HyperFlex ソフトウェアのバージョン

Cisco HX Data Platform インストーラ、Cisco HX Data Platform、および Cisco UCS ファームウェアといった HX のコンポーネントは、さまざまなサーバにインストールされます。HX Storage Cluster とともに（またはその内部で）使用される各サーバの各コンポーネントに互換性があることを確認します。

- **HyperFlex は、UCS Manager および UCS Server Firmware バージョン 4.0(4a)、4.0(4b)、4.0(4c) をサポートしていません。**

重要 これらのファームウェア バージョンにアップグレードしないでください。

これらの UCS Manager のバージョンにアップグレードしないでください。

- 事前設定された HX サーバと、インストールされている Cisco UCS サーバ ファームウェアのバージョンが同じであることを確認します。Cisco UCS ファブリック インターコネクト（FI）のファームウェア バージョンが異なる場合、ファームウェア バージョンを揃える手順については『Cisco HyperFlex システム リリース 4.0 アップグレード ガイド (VMware ESXi 向け)』を参照してください。
  - **M4**:新しいハイブリッドまたはオール フラッシュ (Cisco HyperFlex HX240c M4 または HX220c M4)の導入の場合は、 Cisco UCS Manager 3.1(3k)、3.2(3i)、または 4.0(2b) 以降がインストールされていることを確認してください。詳細については、『推奨される Cisco HyperFlex HX Data Platform ソフトウェア リリース』を参照してください。
  - **M5**: 新しいハイブリッドまたはすべてのフラッシュ（Cisco HyperFlex HX240c M5 または HX220c M5）を展開する場合は、推奨される UCS ファームウェア バージョンがインストールされていることを確認してください。

重要 SED ベース HyperFlex システムについては、A（インフラストラクチャ）、B（ブレードサーバ）および C（ラック サーバ）バンドルが、すべての SED M4/M5 システムに対して Cisco UCS Manager バージョン 4.0(2b) 以降です。詳細については、CSCvh04307 を参照してください。SED ベース HyperFlex システムでは、すべてのクラスタが HyperFlex リリース 3.5(2b) 以降であることも確認します。詳細については、**Field Notice (70234)** および CSCvk17250 を参照してください。

  - HX サーバを再インストールするには、サポートされている互換性のあるソフトウェアのバージョンをダウンロードします。要件と手順については『 Cisco HyperFlex Systems Installation Guide for VMware ESXi 』を参照してください。

- **重要**： 4.0(1a) CIMC 以前のバージョンを実行している Intersight エッジ サーバについては、HUU にはファームウェアを更新するためのメカニズムが提案されます。

表 *1 : M4/M5* サーバの *HyperFlex* ソフトウェア バージョン

HyperFlex リリース	M4 推奨 FI/サーバ ファームウェア * (上記の重要な注意事項を必ず確認してください)	M5 推奨 FI/サーバ ファームウェア * (上記の重要な注意事項を必ず確認してください)
4.0(2b)	4.0 (4h)	4.0 (4h)
4.0(2a)	4.0 (4h)	4.0 (4h)
4.0(1b)	4.0 (4h)	4.0 (4h)
4.0(1a)	4.0 (4e)	4.0 (4e)

4.x 展開向けHyperFlex Edge およびファームウェア互換性マトリックス

Cisco HX データ プラットフォーム リリース 4.x に基づく導入

サーバのコンポーネント ファームウェアが、次の表に示されている最小バージョン以上であることを確認します。

重要 **HyperFlex Edge は、Cisco IMC バージョン 4.0 (4a)、4.0 (4b)、4.0 (4c)、4.0 (4d)、および 4.0 (4e) をサポートしていません。**

表 *2 : HX220c M4/HXAF220c M4* クラスタ

コンポーネント	ファームウェアの推奨バージョン - HXDP 4.x * (上記の重要な注意事項を必ず確認してください)
Cisco Integrated Management Controller（CIMC）	4.0 (下半期)
Host Upgrade Utility（HUU）ダウンロード リンク	4.0 (下半期) ソフトウェアのダウンロード

表 *3 : HX220c M5/HXAF220c M5* クラスタ

コンポーネント	ファームウェアの推奨バージョン - HXDP 4.x * (上記の重要な注意事項を必ず確認してください)
Cisco Integrated Management Controller（CIMC）	4.0(4k)
Host Upgrade Utility（HUU）ダウンロード リンク	4.0(4k) ソフトウェアのダウンロード

HyperFlex のライセンス

バージョン 2.6(1a) の時点で、HyperFlex は VMware PAC のライセンスをサポートしています。既存 VMware 組み込みライセンスは常にサポートされます。

バージョン 2.5(1a) の時点で、HyperFlex ではスマート ライセンス メカニズムを使用してライセンスを適用するようになっています。詳細および手順については、『*VMware ESXi* の *Cisco HyperFlex* システム インストール ガイド』を参照してください。

VMware vSphere ライセンスの要件

vSphere ライセンスを HyperFlex システムに適用する方法は、そのライセンスの購入方法に応じて変わります。

- **vSphereライセンスを HyperFlex** とともに購入した場合

  各 HyperFlex サーバはいずれも、出荷時に Enterprise または Enterprise Plus エディションがプレインストールされています。

  （注）
  - HX ノードには、プレインストール OEM ライセンスがあります。HX サーバを受け取った後、ブート ドライバのコンテンツを削除または上書きすると、プレインストールされたライセンスも削除されます。
  - OEM ライセンス キーは、新しい VMware vCenter 6.0 U1b 機能です。以前のバージョンは OEM ライセンスをサポートしていません。
  - プレインストールされた HX ノードはすべて同じ OEM ライセンス キーを共有します。vSphere OEM キーを使用すると、「`Usage`」の数が「`Capacity`」の値を超えることがあります。
  - [Assign license] セクションの [Add Host] ウィザードで vCenter に HX ホストを追加する場合は、[OEM license] を選択してください。

    実際の vSphere OEM ライセンス キーは難読化されています（例：0N085-XXXXX-XXXXX-XXXXX-10LHH）。
  - Standard、Essentials Plus、ROBO エディションは、HX サーバにプレインストールされていません。

- **vSphere ライセンスを HyperFlex** とともに購入していない場合

  HX ノードには、vSphere の基本ライセンスがプレインストールされています。初期設定後、ライセンスをサポートされている vSphere のバージョンに適用できます。

- **vSphere PAC ライセンスを** とともに購入した場合

VMwareからのPACライセンスレターの指示に従ってライセンスを MY VMware アカウントに追加し、次に指示に従って HX ホストを vCenter に追加して PAC ライセンスを割り当てます。

HyperFlex 補助ノードの HX データ プラットフォーム ソフトウェア バージョン

HyperFlex リリース	補助ノードのバージョン
4.0(2b)	1.0.8
4.0(2a)	1.0.8
4.0(1b)	1.0.4
4.0(1a)	1.0.4

VMware ESXi のソフトウェア要件

ソフトウェア要件には、互換性のある Cisco HyperFlex Systems（HX）、VMware vSphere および、VMware vCenter、および VMware ESXi コンポーネントのバージョンを使用していることを確認するための検証が含まれています。

- すべての HX サーバに、互換性のある vSphere のバージョンがプレインストールされていることを確認します。
- vCenter のバージョンが ESXi のバージョンと同じ、またはそれ以降であることを確認します。
- VMware Product Interoperability Matrix を参照して、vCenter と ESXi のバージョンに互換性があることを確認してください。次の表で ESXi と vCenter の両方がサポートされている限り、新しいバージョンの vCenter を古いバージョンの ESXi とともに使用することができます。
- ルートレベルの権限および関連パスワードが付与された vCenter 管理者アカウントがあることを確認します。

（注） VIC1457 では、ESXi 6.0 をサポートしていません。

次の表は、エンタープライズ、エンタープライズ プラス、スタンダード、エッセンシャルズ プラス、ROBO のVMware vSphereエディションすべてに適用されます。

HyperFlex のバージョン（Cisco Unified Communications Manager Version）	VMware ESXi のバージョン	VMware vCenter バージョン
4.0(2b)[1]	6.0 U3、6.5 U3、6.7 U3	6.0 U3、6.5 U3、6.7 U3

HyperFlex のバージョン（Cisco Unified Communications Manager Version）	VMware ESXi のバージョン	VMware vCenter バージョン
4.0(2a)[2]	6.0 U3、6.5 U3、6.7 U3	6.0 U3、6.5 U3、6.7 U3
4.0(1b)	6.0 U3、6.5 U3、6.7 U2[3]	6.0 U3, 6.5 U3, 6.7 U2
4.0(1a)	6.0 U3、6.5 U2、6.7 U2[4]	6.0 U3、6.5 の U2 6.7 U1

[1] Cisco HyperFlex リリース 4.0(2) は、2020 年 3 月 12 日に VMware 一般サポートの終了に達したため、vSphere 6.0 (ESXi および vCenter) をサポートする最後の主要な HyperFlex リリースです。

[2] Cisco HyperFlex リリース 4.0(2) は、2020 年 3 月 12 日に VMware 一般サポートの終了に達したため、vSphere 6.0 (ESXi および vCenter) をサポートする最後の主要な HyperFlex リリースです。

[3] 6.7 U2 の使用は推奨されていません。詳細については、『CSCvq06952 および CSCvp88515 のソフトウェア アドバイザリ』を参照してください。

[4] 6.7 U2 の使用は推奨されていません。詳細については、『CSCvq06952 および CSCvp88515 のソフトウェア アドバイザリ』を参照してください。

Microsoft Hyper-V のソフトウェア要件

ソフトウェア要件には、互換性のある Cisco HyperFlex Systems（HX）コンポーネントおよび Microsoft Hyper-V (Hyper-V) コンポーネントのバージョンを使用していることを確認するための検証が含まれています。

HyperFlex ソフトウェアのバージョン

HX コンポーネント（Cisco HX Data Platform インストーラ、Cisco HX Data Platform、および Cisco UCS ファームウェア）は、別個のサーバにインストールされます。HX ストレージ クラスタ内で使用される各サーバの各コンポーネントに互換性があることを確認します。

- **Cisco HyperFlex M5 コンバージド ノード**: ハイブリッド (Cisco HyperFlex HX240c M5、HX220c M5) およびすべてのフラッシュ (Cisco HyperFlex HXAF240c M5、HXAF220c m5) について、Cisco UCS Manager 4.0 (2b) がインストールされていることを確認します。HX 4.0 (1a) は、すべての NVMe (HXAF220C M5SN) ノードで Hyper-v をサポートしていません。インストール要件および手順に関する詳細は、『*Microsoft Hyper-V の Cisco HyperFlex システム インストール ガイド*』を参照してください。

表 *4 :* サポートされている *Hyper-V* 上の *M5* サーバ *HyperFlex* ソフトウェアのバージョン

HyperFlex リリース	M5 推奨サーバ ファームウェア
4.0(2b)	4.0 (4h)
4.0(2a)	4.0 (4g)

HyperFlex リリース	M5 推奨サーバ ファームウェア
4.0(1b)	4.0 (4e)
4.0(1a)	4.0 (4e)

表 *5:* サポートされる *Microsoft* ソフトウェア バージョン

Microsoft コンポーネント	バージョン
Windows オペレーティング システム（Windows OS）	Windows Server 2016 Datacenter コアおよびデスクトップ エクスペリエンス。 （注） Windows Server 2016 Datacenter Core & Desktop Experience では、Windows 2016 ISO イメージは少なくとも Update Build Revision (UBR) 1884である必要があります。 Windows Server 2019 Datacenter-デスクトップの体験は、HXDP 4.0.1 (a) 以降からサポートされています。 （注） Windows Server 2019 Desktop Experience では、Windows 2019 ISO イメージは少なくとも Update Build Revision (UBR) 107 である必要があります。 Windows Server 2019 Datacenter-Core は現在サポートされて**いません**。 また、以下は現在サポートされていないことに注意してください。 ISO および Retail ISO をアクティベートした OEM は現在サポートされて**いません**。 Windows 2012r2 などの Windows サーバの以前のバージョンはサポートされて**いません**。 ISO の英語以外のバージョンはサポートされて**いません**。
Active Directory	Windows 2012 以降のドメインおよびフォレスト機能レベル

サポートされている Microsoft ライセンス エディション

1 個以上の HyperFlex ホストにインストールされている Microsoft Windows サーバのバージョンは、『Microsoft ライセンス取得』に記載されている Microsoft ライセンス要件に従ってライセンスが取得されている必要があります。

ブラウザの推奨事項

リストされている HyperFlex コンポーネントを実行するには、次のいずれかのブラウザを使用します。これらのブラウザはテストおよび承認済みです。他のブラウザでも動作する可能性はありますが、すべての機能をテストし、確認しているわけではありません。

表 *6* : 対応ブラウザ

ブラウザ	Cisco Intersight	Cisco UCS Manager	HX Data Platform インストーラ	HX Connect
Microsoft Internet Explorer	NA	11 以上	11 以上	11 以上
Google Chrome	62 以上	57 以上	70 以上	70 以上
Mozilla Firefox	57 以上	45 以上	60 以上	60 以上
Apple Safari	10 以上	9 以上	NA	NA
Opera	NA	35 以上	NA	NA

注

- **Cisco HyperFlex Connect**

  推奨される最小解像度は 1024 x 768 です。

- **Cisco HX Data Platform Plug-in**

  Cisco HX Data Platform Plug-inは、vSphere で実行されます。VMware Host Client システムのブラウザ要件については、https://www.vmware.com/support/pubs/ にある VMware のマニュアルを参照してください。

  HX Data Platform Plug-in は、vCenter HTML クライアントには表示されません。VCenter フラッシュ クライアントを使用する必要があります。

- **Cisco UCS Manager**

  ブラウザで次のものがサポートされている必要があります。

  - Java Runtime Environment 1.6 以降。
  - 一部の機能には、Adobe Flash Player 10 以降が必要です。

  Cisco UCS Manager に関するブラウザの最新情報については、最新の『Cisco UCS Manager スタートアップ ガイド』を参照してください。

Cisco HX Data Platform ストレージ クラスタの仕様

クラスタの制限

- Cisco HX Data Platform は、VMware の最大設定に従って、vCenter ごとに管理される最大 100 のクラスタをサポートします。
- Cisco HX Data Platform は、1 つの FI ドメインで任意の数のクラスタをサポートします。各 HX コンバージド ノードは、FEX を使用せずにファブリック A とファブリック B の専用 FI ポートに直接接続する必要があります。C シリーズのコンピューティング専用ノードも、両方の FI に直接接続する必要があります。B シリーズのコンピューティング専用ノードは、シャーシ I/O モジュールを介して両方のファブリックに接続されます。最終的に、FI 上の物理ポートの数により、UCS ドメインでサポートされる最大クラスタ サイズおよび個別のクラスタの最大数が決定します。

次の表では、Cisco HX Data Platform ストレージ クラスタの仕様を示しています。

ノード	VMware ESXi				Microsoft Hyper-V		ストレッチ クラスタ *(ESX でのみ使用可能)		
HX サーバ	HX220c M5 HX220c AF M5 HX240c M5 HX240c M5 HX220c M4 HX220c M4 HX240c M4 HX240c M4	HX240c M5L	HX220c M5 Edge HX220c M5 Edge HX220c M4 Edge HX220c M4 Edge	すべての ESXi 6.5 または 6.7 のみ。ESXi 6.0 または Hyper-V ではサポートされていません。	HX220c M5 HX220c AF M5 HX240c M5 HX240c M5	HX240c M5L	HX220c M5 HX220c AF M5 HX240c M5 HX240c M5	HX240c M5L	すべての

ノード	VMware ESXi				Microsoft Hyper-V		ストレッチ クラスタ * (ESX でのみ使用可能)		
コンピューティング専用 UCS B シリーズ/C シリーズ サーバ	B200 M5M4M3、B260 M4、B420 M4、B460 M4、B480 M5、C220 M5M4M3、C240 M5M4M3、C460 M4、C480 M5	B200 M5M4M3、B260 M4、B420 M4、B460 M4、B480 M5、C220 M5M4M3、C240 M5M4M3、C460 M4、C480 M5	—	B200 M5M4M3、B260 M4、B420 M4、B460 M4、B480 M5、C220 M5M4M3、C240 M5M4M3、C460 M4、C480 M5	C240 M5、C220 M5、B200 M4、B200 M5	C220 M5、C240 M5、B200 M4、B200 M5	B200 M5M4M3、B260 M4、B420 M4、B460 M4、B480 M5、C220 M5M4M3、C240 M5M4M3、C460 M4、C480 M5	B200 M5M4M3、B260 M4、B420 M4、B460 M4、B480 M5、C220 M5M4M3、C240 M5M4M3、C460 M4、C480 M5、	B200 M5M4M3、B260 M4、B420 M4、B460 M4、B480 M5、C220 M5M4M3、C240 M5M4M3、C460 M4、C480 M5、
サポートされるノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージド ノードのみ	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード	コンバージドおよびコンピューティング専用ノード

ノード	VMware ESXi				Microsoft Hyper-V		ストレッチ クラスタ * (ESX でのみ使用可能)		
HXDP-S ライセンスされたノードの制限 **コンピューティング専用喉に対して 1:1 比の HXDP-S** **MinMax**	コンバージド ノード : 3 ~ 32 (7.6 TB ドライブ構成の場合、AF 240 では最大 12 ドライブ/ノードに制限されます) コンピューティング専用ノード: 0 ～ 32	コンバージド ノード: 3 ~ 16 (12TB ドライブは最大 8 ノードに制限されます) コンバージド ノード: 0 ～ 16 (12TB ドライブは最大 8 ノードに制限されます)	M4 コンバージド ノード: 3 M5 コンバージド ノード: 2、3、または 4 HXDP-E ライセンスが必要	該当なし (Enterprise HXDP-P ライセンスが必要)	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード: 0 ～ 16	コンバージド ノード: 3 ～ 16 (12TB HDD オプションは HyperV ではサポートされていません) コンピューティング専用ノード: 0 ～ 16	該当なし (Enterprise HXDP-P ライセンスが必要)	該当なし (Enterprise HXDP-P ライセンスが必要)	該当なし (Enterprise HXDP-P ライセンスが必要)

ノード	VMware ESXi				Microsoft Hyper-V		ストレッチ クラスタ * (ESX でのみ使用可能)		
HXDP-P ライセンスされたノードの制限 **コンピューティング専用喉に対して 1:2 比の HXDP-P** **MinMax**	コンバージド ノード : 3 ~ 32 (7.6 TB ドライブ構成の場合、AF 240 では最大 12 ドライブ/ノードに制限されます) コンピューティング専用ノード: 0 ～ 32 (クラスタの最大サイズ)	コンバージド ノード: 3 ~ 16 (12TB ドライブは最大 8 ノードに制限されます) コンバージド ノード: 0 ～ 32 (12TB ドライブは最大 16 ノードに制限されます)	コンバージド ノード: 3 (HXDP-E ライセンスが必要)	コンバージド ノード: 3 ~ 32 コンピューティング専用ノード: 0 ～ 32 (クラスタの最大サイズ)	コンバージド ノード: 3 ~ 16 コンピューティング専用ノード: 0 ～ 16	コンバージド ノード: 3 ～ 16 (12TB HDD オプションは HyperV ではサポートされていません) コンピューティング専用ノード: 0 ～ 16	コンバージド ノード: サイトごとに 2 ～ 16 コンピューティング専用ノード: サイトごとに0 ～ 21 (クラスタの最大サイズ)	コンバージド ノード: サイトごとに 2 ～ 8 コンピューティング専用ノード: サイトごとに 0 ～ 16 (クラスタの最大サイズ)	コンバージド ノード: サイトごとに 2 ～ 16 コンピューティング専用ノード: サイトごとに0 ～ 21 (クラスタの最大サイズ)
クラスタの最大サイズ	64	48	3	64	32	32	サイトあたり 32/クラスタあたり 64	サイトあたり 24、クラスタあたり 48	サイトあたり 24、クラスタあたり 48

ノード	VMware ESXi				Microsoft Hyper-V		ストレッチ クラスタ *(ESX でのみ使用可能)		
コンピューティングからコンバージドへの最大比率	2:1 *	2:1 *	—	2:1 *	1:1	1:1	2:1 *	2:1 *	2:1 *
説明	✓	✓	非対応	✓	✓	✓	✓**	✓**	✓**

*エンタープライズ ライセンスが必要

**両方のサイトで同一の拡張を行う必要があります

注意事項と制約事項

- リリース 4.0(2a) 以降では、SCVM はコンピューティング ノードで不要になりました。
- **HX REST API アクセストークン管理**: HX REST API を利用するアプリケーションは、API コールを行うときにアクセス トークンを再使用する必要があります。AAA 取得アクセス トークン API を使用して取得すると、アクセス トークンは18日間 (1,555,200 秒) 有効です。さらに、AAA では、アクセス トークン取得 API リクエストに、レート制限が適用されます。15分のウィンドウでは、/auth を最大5回呼び出すことができます。各ユーザは、取り消されていないトークンを最大 8 つ作成することができます。次に /auth を呼び出すと、新しいトークンの余地を設けるため、最も古い発行済みトークンが自動的に取り消されます。システムには、最大で16の取り消されていないトークンが存在できます。ブルートフォース攻撃を防ぐために、認証試行が 10 回連続で失敗した場合、ユーザ アカウントは 120 秒間ロックされます。詳細については、『Cisco HyperFlex SYSTEMS REST API Reference』ガイドを参照してください。

  HxConnect は、ログインに AAA 認証 REST API を使用します。上記のレート制限は、HxConnect にも適用されます。

アップグレードのガイドライン

次のリストは、HyperFlex システムのアップグレードを実行する際の重要な基準を記載します。

- **サポートされていない HX Data Platform 1.7.x、1.8.x、2.0、2.1x、2.5x、2.6x クラスタ**—2.6(1a) 以前のバージョンからのユーザーは、4.0 またはそれ以降のリリースにアップグレードする前に、中間バージョンを通過する必要があります。サポートを終了した Cisco HyperFlex HX Data Platform ソフトウェア リリースから、Cisco ソフトウェア ダウンロード サイトの最新の提案されたリリースにアップグレードする必要がある場合、『サポートされていない Cisco HX リリースの Cisco HyperFlex システム アップグレード ガイド』を参照してください。詳細については、『Software Advisory for CSCvq66867 のソフトウェア アド

バイザリ: 警告: HXDP 1.8(1a)-1.8(1e) からアップグレードする場合は HXDP 2.6(1e) アップグレード パッケージのみ使用する』を参照してください。

- **Hypercheck ヘルス チェック ユーティリティ**: アップグレードする前に、Hypercheck クラスタでこの予防的ヘルス チェック ユーティリティを実行することを推奨します。これらのチェックにより、注意が必要なエリアがすぐに見やすくなり、シームレスなアップグレード エクスペリエンスを保証します。Hypercheck のインストールと実行方法の完全な手順の詳細については、『HyperFlex 健全性および事前アップグレード チェック ツール』を参照してください。

- **vSphere 6.7 ソフトウェア アドバイザリ**:ESXi 6.7U1 EP06 (build # 11675023) を実行している場合は、Cisco HX Data Platform リリース 4.0 (1a) にアップグレードしないでください。Cisco HX Data Platform リリース 4.0 (1a) を実行している場合は、6.7U1 EP06 (build # 11675023) にアップグレードしないでください。詳細については、ソフトウェア アドバイザリ CSCvo56350を参照してください。

  リリースに掲載されているソフトウェア ビルドバージョンは、他のすべてのローカルバージョンよりも優先されます。

- **必要な vCenter のアップグレード**：セキュリティを強化するために、Cisco HX Data Platform リリース 3.5(1a) 以降では TLS 1.2 を使用する必要があります。そのため、Cisco HX Data Platform リリース 3.5 にアップグレードする前に、vCenter を 6.0 U3f 以降にアップグレードする必要があります。さらに、HX Data Platform の互換性要件を満たすために、ESXi を必要に応じてアップグレードする必要があります。

- **アップグレード対象の最小 HXDP バージョン**：2.6(1f) 以降を実行中の HX Data Platform クラスタは、HX Connect UI を使用して 4.0 に直接アップグレードできます。

- **クラスタの対応状況**：アップグレードを進める前に、クラスタが適切にブートストラップされて、更新済みプラグインがロードされていることを確認します。3.5 より前のリリースからのアップグレードには、手動のクラスタ ブート ストラップが必要です。

- **クラスタの対応状況**：アップグレードを進める前に、クラスタが適切にブートストラップされて、更新済みプラグインがロードされていることを確認します。3.5(1a) よりも前の HX リリースでは、手動クラスタブートストラップが必要です。詳細については、「手動ブートストラップによるアップグレード プロセス」(『VMware ESXi の Cisco HyperFlex システム リリース 4.0 アップグレード ガイド』)を参照してください。HX リリース 3.5(1a) までのすべてのバージョンでは、アップグレードで必要なため、このクラスタブートストラップの手順はスキップしないでください。自動ブートストラップは、HX リリース 3.5(1a) 以降でサポートされています。詳細については、「自動ブートストラップによるアップグレード プロセス」(『VMware ESXi の Cisco HyperFlex システム リリース 4.0 アップグレード ガイド』)を参照してください。

  手動ブートストラップは、Intersight クラスタではサポートされていません。

- **アップグレードの開始**: 2.5(1a) 以降のリリースからアップグレードする場合は、HX Connect UI または CLI の `stcli` コマンドを使用してください。2.5(1a) より前のリリースからアップグレードする場合は、CLI `stcli` コマンドまたはvSphere Web ClientのHX Data Platform Plug-inを使用します。vCenter プラグインは、2.5(1a) リリース以降のアップグレードには

使用しないでください。vCenter プラグインは、2.5(1a) リリース以降のアップグレードには使用しないでください。

現在のクラスタのバージョンが 3.5 (1a) 以降である場合は、`stcli`コマンドを使用する必要はありません。4.0 への直接アップグレードが可能です。

- **アップグレードの完了—**アップグレード ウィンドウでは、一時的に自己修復 (または再調整) が無効になっています。アップグレードが失敗する場合、できるだけ早くアップグレードを完了する必要があります。

- **ESXi および HXDP の互換性**: クラスタが HX Data Platform バージョンの実行に基づいて ESXi の互換性のあるバージョンを実行していることを確認します (「VMware ESXi のソフトウェア要件」の項を参照してください)。ESXi の互換性は、ESXi のメジャー バージョンおよび更新リリースによって決定されます。通常、アップグレード操作を一度の最適化されたリブートと組み合わせる場合、HXDP と ESXi を一緒にアップグレードすることをお勧めします。分割アップグレードを実行する場合は、最初に HX Data Platform をアップグレードしてから、ESXi のアップグレードに進みます。

- **vSphere 6.5 にアップグレードする場合**：

  （注）
  - 特定のクラスタ機能（ネイティブ/スケジュール スナップショット、ReadyClones、HX メンテナンス モードの開始/終了など）は、アップグレードの開始時から 2.5 以降への HX Data Platform のアップグレードが完了するまで動作しません。
  - オフライン zip バンドルを使用して ESXi をアップグレードした後、ESX の [Exit Maintenance Mode] オプションを使用します。HX Data Platform のアップグレードが完了するまでは、vSphere Web クライアント内で ESX の [メンテナンス モードの終了（Exit Maintenance Mode）] オプションは動作しません。

- vSphere 6.0 のアップグレード：vSphere 6.0 を 6.5 に移行する場合は、次の順序でコンポーネントをアップグレードします。

  1. HX Data Platform と UCS ファームウェアをアップグレードします。
  2. HX Data Platform と ESXi をアップグレード。
  3. HX Data Platform のみを最初にアップグレードし、次に ESXi および/または UCS ファームウェアをアップグレードするか、両方アップグレードします。

- **M4 サーバ ファームウェア アップグレード**:円滑な動作を確実にして、既知の問題を修正するには、サーバファームウェアをアップグレードします。特に、長期間にわたる安定性を確保するために、このリリースで使用可能になった新しい SAS HBA ファームウェアを推奨します。

- 可能な場合は常に、3.1(3c) 以降の C バンドルにアップグレードするようにしてください。
- 3.1(2f) より前のバージョンの C バンドルを使用している場合は、UCS サーバ ファームウェア（C バンドル）のコンバインド アップグレードを行って、サーバ ファームウェアを 3.1(3c) 以降に、HX Data Platform を 2.5 にアップグレードする必要があります。これらのアップグレードを 2 つの別々の操作に分割しないでください。
- クラスタがすでに 3.1(2f) 以降の C バンドルで稼働している場合、必要に応じて HX Data Platform のみのアップグレードまたはコンバインドアップグレードを実行できます。

- **M5サーバ ファームウェアのアップグレード**：M5 世代のサーバでは、ファームウェア バージョン 3.2(2d) 以降を実行する必要があります。
- **ファームウェア ダウングレード** — HX-installer から UCSM のダウングレードはサポートされていません。
- M4/M5 の混在ドメイン：既存の M4 クラスタが含まれる UCS ドメインに新しい別個の M5 クラスタをインストールすると、同じドメインに M4 と M5 が混在することになります。このような場合、オーケストレーションされた UCS サーバ ファームウェアのアップグレードは、M4 クラスタに Cisco HX Data Platform リリース 2.6 以降がインストールされるまで動作しません。したがって、最初に UCS サーバ ファームウェアを最新の 3.1(3) または 3.2(2) パッチ リリースにアップグレードしてから、既存の USC ドメインに新しい M5 クラスタを追加することがベスト プラクティスです。さらに、新しい M5 クラスタを 1.7 HX Data Platform クラスタと同じドメインに追加する場合は常に、1.7 HX Data Platform クラスタを最初にアップグレードする必要があります。
- メンテナンス時間枠：HX Data Platform と UCS ファームウェアの両方をアップグレードする場合、メンテナンス時間枠の大きさに応じて、vSphere HX Data Platform Plug-inを介したコンバインドアップグレードまたは分割アップグレードのいずれかを選択できます。Cisco UCS Manager インフラストラクチャ アップグレードでは、AutoInstall の使用のみをサポートしており、直接のサーバ ファームウェア アップグレードは、HX Data Platform Plug-in から提供されているアップグレード オーケストレーション フレームワークでのみ実行する必要があります。
- **サポートされていない自己暗号化ドライブ (SEDs)**: 新しいバージョンの HX Data Platform で最近認定された自己暗号化ドライブ (SEDs) を追加または交換する場合は、HX Data Platform にアップグレードした後にのみ、新しいドライブを互換性のあるバージョンに挿入してくださいすべてのドライブは SED ドライブである必要があり、SED と非 SED の混在はサポートされていません。
-
- **外部ホスト アクセスの有効化**: Cisco HX Data Platform リリース 4.0 (1a) を使用すると、管理ネットワーク上のポート 445 はセキュリティ強化のためにブロックされます。4.0 より前のポートでは、外部ホストアクセスを有効にするポート 445 ポートが開いていることに注意してください。以前のリリースから 4.0 (1a) にアップグレードしていて、外部ホストアクセスを続行する場合は、ユーティリティを使用して [select hosts (ホストの選択)] を開

くことができます。外部ホスト アクセスの有効化の詳細については、『Microsoft hyper-v のインストール ガイド』の「SCVMM への HyperFlex 共有の設定」の項を参照してください。

混合クラスタ展開のガイドライン

- M5 コンバージド ノードを持つ既存の M4 クラスタの展開がサポートされています。
- M4 コンバージド ノードを持つ既存の M5 クラスタの展開がサポートされています。
- M4 または M5 コンバージド ノードを持つ既存の混合 M4/M5 クラスタの展開がサポートされています。
- サポートされているコンピューティング専用ノードを追加することは、HX Data Platform 2.6 またはそれ以降のインストーラを使用した M4、M5、混合 M4/M5 クラスタすべてで許可されています。いくつかの例となる組み合わせがここにリストされています。その他多くの組み合わせが可能です。

```
Example combinations:
Expand mixed M4/M5 cluster with compute-only B200, C220, C240 M4/M5
Expand M4 cluster with compute-only B200 M5, C220 M5, C240M5
```

- 混合クラスタを作成するには、展開ワークフローのみがサポートされています。混合 M4/M5 サーバを持つ最初のクラスタ作成はサポートされていません。
- すべての M5 サーバは、既存の M4 サーバのフォーム ファクタ（220/240）、タイプ（Hybrid/AF）、セキュリティ機能（非 SED のみ）およびディスク設定（数量、容量、非 SED）と一致する必要があります。ドライブの互換性の詳細については、『Cisco HyperFlex Drive Compatibility』ドキュメントを参照してください。
  - HX220-M4 と組み合わせるとき、HX220-M5 は最大 6 の容量ディスク（2 ディスク スロットは空のまま）を使用します。
- HX Edge、SED、LFF、Hyper-v、およびストレッチ クラスタは、混合 M4 および M5 クラスタをサポートしていません。

リリース 3.5 向け混合クラスタ拡張のガイドライン

混合クラスタは、同じストレージ クラスタ内の M4 および M5 HX コンバージド ノードの両方を持つことで定義されます。混合クラスタを設定するとき、以下のガイドラインが適用されます。

- M5 コンバージド ノードを持つ既存の M4 クラスタの展開がサポートされています。
- M4 コンバージド ノードを持つ既存の M5 クラスタの展開がサポートされています。
- M4 または M5 コンバージド ノードを持つ既存の混合 M4/M5 クラスタの展開がサポートされています。
- サポートされているコンピューティング専用ノードを追加することは、HX Data Platform 2.6 またはそれ以降のインストーラを使用した M4、M5、混合 M4/M5 クラスタすべてで許

可されています。いくつかの例となる組み合わせがここにリストされています。その他多くの組み合わせが可能です。

```
Example combinations:
Expand mixed M4/M5 cluster with compute-only B200, C220, C240 M4/M5
Expand M4 cluster with compute-only B200 M5, C220 M5, C240M5
```

- 混合クラスタを作成するには、展開ワークフローのみがサポートされています。混合 M4/M5 サーバを持つ最初のクラスタ作成はサポートされていません。
- すべての M5 サーバは、既存の M4 サーバのフォーム ファクタ（220/240）、タイプ（Hybrid/AF）、セキュリティ機能（非 SED のみ）およびディスク設定（数量、容量、非 SED）と一致する必要があります。
  - HX220-M4 と組み合わせるとき、HX220-M5 は最大 6 の容量ディスク（2 ディスク スロットは空のまま）を使用します。
- HyperFlex Edge は混合クラスタをサポートしません。
- SED SKU は混合クラスタをサポートしません。

セキュリティ修正

次のセキュリティ上の問題が解決されます。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvq63138	CVE-2019-13132、CVE-2019-9924	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンド挿入を実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq71240	CVE-2019-11719、 CVE-2019-11727、 CVE-2019-11729	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンド挿入を実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvr06339	CVE-2019-1125	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンド挿入を実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvs06094	CVE-2015-9383、 CVE-2018-14498、 CVE-2018-20406、 CVE-2018-20852、 CVE-2019-10160、 CVE-2019-13117、 CVE-2019-13118、 CVE-2019-14287、 CVE-2019-14973、 CVE-2019-15903、 CVE-2019-17546、 CVE-2019-18197、 CVE-2019-18218、 CVE-2019-5010、 CVE-2019-5094CVE-2019-5481、 CVE-2019-5482、 CVE-2019-9636、 CVE-2019-9740、 CVE-2019-9947、CVE-2019-9948	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンド挿入を実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvp65019	CVE-2017-13168、 CVE-2017-18174、 CVE-2017-18216、 CVE-2018-10876、 CVE-2018-10877、 CVE-2018-10878、 CVE-2018-10879、 CVE-2018-10880、 CVE-2018-10881、 CVE-2018-10882、 CVE-2018-10902、 CVE-2018-10938、 CVE-2018-12233、 CVE-2018-12896、 CVE-2018-13053CVE-2018-13094、 CVE-2018-13096、 CVE-2018-13405、 CVE-2018-13406、 CVE-2018-14609、 CVE-2018-14617、 CVE-2018-14633、 CVE-2018-14734、 CVE-2018-15572、 CVE-2018-15594、 CVE-2018-16276、 CVE-2018-16658、 CVE-2018-17182、 CVE-2018-17972、 CVE-2018-18021CVE-2018-18690、 CVE-2018-18710、 CVE-2018-6554、 CVE-2018-6555、CVE-2018-9363	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンド挿入を実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvo98516	NA	この脆弱性は、HTML iframe 保護が不十分であることに起因します。攻撃者は、悪意のある HTML iframe を含む攻撃者制御の web ページにユーザを誘導することで、この脆弱性をエクスプロイトする可能性があります。不正利用が成功すると、攻撃者はクリックジャックやその他クライアント側のブラウザ攻撃を行うことができます。
4.0(2a)	CSCvj95584	NA	この脆弱性は、統計情報収集サービスの認証が不十分であることに起因します。攻撃者は、影響を受けるデバイスの統計情報収集サービスに適切にフォーマット化されたデータ値を送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は Web インターフェイス統計情報で、ユーザーに無効なデータを提示する可能性があります。
4.0(2a)	CSCvp24343	CVE-2018-15380	脆弱性は、影響を受けるデバイスで Web UI の CSRF 保護が不十分なことが原因です。攻撃者は、ユーザーが悪意のあるリンクをクリックしたり、悪意のある PDF ファイルを開いたりするように仕向けることにより、この脆弱性を不正利用する可能性があります。不正利用が成功すると、攻撃者はユーザーの権限で任意のコードを実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvq19949	CVE-2019-11834、CVE-2019-11835	CVE-2019-11834 および CVE-2019-11835 によって特定された cJSON バージョンを使用した脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvr54398	CVE-2018-12207、CVE-2019-11135	CVE-2018-12207 および CVE-20190-11135 によって特定された VMware ESXi を使用した MCEPSC および TAA の脆弱性に対する HX ESXi イメージパッチ。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq19546	CVE-2019-11477、CVE-2019-11478、CVE-2019-11479	CVE-2019-11477、CVE-2019-11478、CVE-2019-11479 によって特定された Linux カーネルに影響する CP ネットワーキングの脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvr54399	CVE-2018-12207、CVE-2019-11135	CVE-2018-12207、CVE-2019-11135 によって特定された Microsoft Hyper-V ハイパーバイザを使用した際の脆弱性に対する Microsoft セキュリティ パッチの認定。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp76463	CVE-2016-10708、CVE-2018-15473、CVE-2018-20685、CVE-2019-6109、CVE-2019-6111	CVE-2019-6111 によって特定された OpenSSH の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvp66679	CVE-2016-2105、 CVE-2016-2106、 CVE-2016-2107、 CVE-2016-2109、 CVE-2016-2176、 CVE-2016-2177、 CVE-2016-2178、 CVE-2016-2179、 CVE-2016-2180、 CVE-2016-2181、 CVE-2016-2182、 CVE-2016-2183、 CVE-2016-6302、 CVE-2016-6303、 CVE-2016-6304、 CVE-2016-6305、CVE-、 CVE-CVE-2016-6306、 CVE-2016-6307、 CVE-2016-6308、 CVE-2016-7055、 CVE-2016-8610、 CVE-2017-3731、 CVE-2017-3732、 CVE-2017-3735、 CVE-2017-3736、 CVE-2017-3737、 CVE-2017-3738、 CVE-2018-0495、 CVE-2018-0732、 CVE-2018-0734、 CVE-2018-0735、 CVE-2018-0737、CVE-、 CVE-CVE-2018-0739、 CVE-2018-12384、 CVE-2018-12404、 CVE-2018-5407、CVE-2019-1559	OpenSSL と LibNSS に関連付けられている複数の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp66555	CVE-2016-10087	CVE-2016-10087 によって特定された libpng の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvp34586	CVE-2014-9092、 CVE-2016-3616、 CVE-2017-15232、 CVE-2018-11212、 CVE-2018-11213、 CVE-2018-11214、 CVE-2018-1152、CVE-2018-13785	Libjpg と libpng に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp31207	CVE-2018-16428、 CVE-2018-16429	CVE-2018-16428 および CVE-2018-16429 によって特定された Glib に関連する脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvr36903	CVE-2019-15133、 CVE-2019-15903、 CVE-2019-5010、 CVE-2019-5481、 CVE-2019-5482、 CVE-2019-9636、 CVE-2019-9740、 CVE-2019-9947、CVE-2019-9948	Curl、expat、python 2.7、python 3.5、3.6、3.7、freetype、giflib に関連付けられている複数の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq92032	CVE-2019-14379、 CVE-2019-12384、 CVE-2019-14439	複数のサードパーティ製ソフトウェアの脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq43250	CVE-2018-16062、 CVE-2018-16402、 CVE-2018-16403、 CVE-2018-18310、 CVE-2018-18520、 CVE-2018-18521、 CVE-2019-7149、 CVE-2019-7150、CVE-2019-7665	Elfutils に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvq43230	CVE-2017-5953、CVE-2019-12735	Vim に関連する脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq43213	CVE-2016-6153、 CVE-2017-10989、 CVE-2017-13685、 CVE-2017-2518、 CVE-2017-2519、 CVE-2017-2520、 CVE-2018-20346、 CVE-2018-20505、 CVE-2018-20506、 CVE-2019-8457、 CVE-2019-9936、CVE-2019-9937	Sqlite3 に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq43209	CVE-2018-20843	Glib 2.0 に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq43205	CVE-2018-20843	Expat に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq43194	CVE-2016-3189、CVE-2019-12900	Bzip2 に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvq10694	CVE-2018-12115、 CVE-2018-0734、 CVE-2018-5407、 CVE-2018-12120、 CVE-2018-12121、 CVE-2018-12122、 CVE-2018-12123、 CVE-2018-12116、 CVE-2019-5737、CVE-2019-5739	NodeJS に関連付けられている複数の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq10388	CVE-2019-10906、 CVE-2016-10745	Pallets Jinja str.format_map に関連付けられ、CVE-2019-10906 および CVE-2016-10745 によって特定される脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq09178	CVE-2014-8501、 CVE-2014-9939、 CVE-2015-9262、 CVE-2016-10087、 CVE-2016-2226、 CVE-2016-4487、 CVE-2016-4488、 CVE-2016-4489、 CVE-2016-4490、 CVE-2016-4491、 CVE-2016-4492、 CVE-2016-4493、 CVE-2016-6131、 CVE-2018-10963、 CVE-2018-13785CVE-2018-17100、 CVE-2018-17101、 CVE-2018-18557、 CVE-2018-18661、 CVE-2018-7456、CVE-2018-8905	複数のセキュリティの脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvq07568	CVE-2019-9893	Libseccomp に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvq06755	CVE-2017-12447	Pixbuf に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp93817	CVE-2018-6594	Python 暗号に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp86721	CVE-2018-20483、CVE-2019-5953	Wget に関連付けられている脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp66748	CVE-2018-6594	Python Crypto に関連付けられた複数の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp66734	CVE-2017-17512	実用的なユーティリティに関連する脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp66689	CVE-2018-1000030	Python に関連付けられている複数の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvp66672	CVE-2016-10713、 CVE-2018-1000156、 CVE-2018-6951	CVE-2016-10713 によって特定された複数のパッチの脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp66664	CVE-2016-10165、 CVE-2018-16435	CVE-2016-10165 によって識別されるほとんどの CMS に関連する脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp64746	CVE-2011-5325、 CVE-2016-7076、 CVE-2017-1000368、 CVE-2019-11068	CVE-2011-5325/CVE-2019-11068/CVE-2016-7076、CVE-2017-1000368 で特定される Tenable スキャンに関連する脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp34792	CVE-2016-9318、 CVE-2017-16932、 CVE-2017-18258、 CVE-2018-14404、 CVE-2018-14567	XMLSec 1.2.23 以前およびその他の製品で使用され、CVE-2016-9318 によって識別される、libxml2 2.9.4 以前に関連する脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvp29266	CVE-2018-10916	LFTP リモート ファイル名の不正アクセスの脆弱性に関連付けられ、CVE-2018-10916 によって特定される脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(2a)	CSCvo34097	CVE-2018-7750	CryptographyDeprecationWarning に関連付けられている脆弱性：署名者および確認者は廃止されました。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0(2a)	CSCvr39793	CVE-2019-16056	Python python 2.7、3.5 の複数の脆弱性。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。
4.0 (1b)、3.5 (2g)	CSCvq24176	CVE-2018-15380	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンドを実行する可能性があります。 この脆弱性は、入力に対する不十分な検証に起因します。攻撃者はクラスタ サービスマネージャに接続し、バインドされたプロセスにコマンドを挿入することにより、この脆弱性を悪用する可能性があります。悪用が成功すると、攻撃者は影響を受けるホスト上でルート ユーザーとしてコマンドを実行する可能性があります。 この脆弱性に対処するソフトウェア アップデートは、すでに Cisco からリリースされています。脆弱性に対処する回避策があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0 (1b)、3.5 (2g)	CSCvj95606	CVE-2018-15380	Cisco HyperFlex のクラスタ サービス マネージャの脆弱性により、認証されていない隣接する攻撃者がルート ユーザーとしてコマンド挿入を実行する可能性があります。 この脆弱性は、保護されていないリスニング インターフェイスが原因で発生します。攻撃者は、リッスンしているインターフェイスに接続し、バインドされたプロセスにコマンドを挿入することにより、この脆弱性を悪用する可能性があります。悪用により、攻撃者は影響を受けるホスト上でルート ユーザーとしてコマンドを実行する可能性があります。 詳細については、関連する『Cisco セキュリティ アドバイザリ』を参照してください。

リリース	不具合 ID	CVE	説明
4.0(1b)	CSCvo88997		VC アラーム中に検出された JVM 1.8 U121 メモリ リークに関連する脆弱性。 (REST API を使用した同時 40 コール)。

リリース	不具合 ID	CVE	説明
		CVE-2017-10053、 CVE-2017-10067、 CVE-2017-10074、 CVE-2017-10078、 CVE-2017-10081、 CVE-2017-10087、 CVE-2017-10089、 CVE-2017-10090、 CVE-2017-10096、 CVE-2017-10101、 CVE-2017-10102、 CVE-2017-10107、 CVE-2017-10108、 CVE-2017-10109、 CVE-2017-10110CVE-2017-10111、 CVE-2017-10115、 CVE-2017-10116、 CVE-2017-10118、 CVE-2017-10135、 CVE-2017-10176、 CVE-2017-10193、 CVE-2017-10198、 CVE-2017-10243、 CVE-2017-10274、 CVE-2017-10281、 CVE-2017-10285、 CVE-2017-10295、 CVE-2017-10345、 CVE-2017-10346CVE-2017-10347、 CVE-2017-10348、 CVE-2017-10349、 CVE-2017-10350、 CVE-2017-10355、 CVE-2017-10356、 CVE-2017-10357、 CVE-2017-10388、 CVE-2017-3509、 CVE-2017-3511、 CVE-2017-3526、 CVE-2017-3533、 CVE-2017-3539、 CVE-2017-3544、	

リリース	不具合 ID	CVE	説明
		CVE-2018-2579CVE-2018-2582、 CVE-2018-2588、 CVE-2018-2599、 CVE-2018-2602、 CVE-2018-2603、 CVE-2018-2618、 CVE-2018-2629、 CVE-2018-2633、 CVE-2018-2634、 CVE-2018-2637、 CVE-2018-2641、 CVE-2018-2663、 CVE-2018-2677、 CVE-2018-2678、 CVE-2018-2783、 CVE-2018-2790、CVE-、 CVE-CVE-2018-2794、 CVE-2018-2795、 CVE-2018-2796、 CVE-2018-2797、 CVE-2018-2798、 CVE-2018-2799、 CVE-2018-2800、 CVE-2018-2814、 CVE-2018-2815、 CVE-2018-2952、 CVE-2018-3136、 CVE-2018-3139、 CVE-2018-3149、 CVE-2018-3150、 CVE-2018-3169、 CVE-2018-3180、CVE-、 CVE-CVE-2018-3183、 CVE-2018-3214、CVE-2019-2422	
4.0(1b)	CSCvm58031	NA	TomcatおよびNginx ログは、リリース 3.5 の HX Connect を介して生成されたサポート バンドルでは収集されません。

リリース	不具合 ID	CVE	説明
4.0(1a)	CSCvn35119	CVE-2018-18584 CVE-2018-18585	Cisco HX Data Platform に含まれている **libmspack** ソフトウェアパッケージのバージョンに関連付けられている脆弱性。
4.0(1a)	CSCvn82282	CVE-2018-14719 CVE-2018-14720 CVE-2018-1000873 CVE-2018-14721 CVE-2018-19360 CVE-2018-19362 CVE-2018-19361 CVE-2018-14718	FasterXML Jackson-Databind Time Value Field Denial of Service に関連付けられた脆弱性。
4.0(1a)	CSCvo05054	CVE-2013-3587	Cisco HX Data Platform に含まれている **OpenSSL Protocol** ソフトウェアパッケージのバージョンに関連付けられている脆弱性。
4.0(1a)	CSCvo27818	CVE-2018-16487 CVE-2018-19361	サードパーティ製ソフトウェアのサービス妨害に関連する脆弱性。
3.5(2a)	CSCvm53149	CVE-2018-1092 CVE-2018-7492 CVE-2018-8087 CVE-2018-1068 CVE-2018-8781	**Linux kernel for Ubuntu 17.10** に関連付けられている脆弱性。

リリース 4.0(2b) の解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs70967	**stcli services dns remove**は、インターフェイスファイルから DNS サーバ情報を削除します。	2.5(1d)	4.0(2b)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvt10522	HX 4.0 (1b)、Intersight の実稼働クラウドから新しく展開されます。 CSI (Kubernetes 統合) を有効にしている場合、ユーザは次のエラーを受信します。 **Volume_access_enable 中に障害が発生し、「ゼロ以外の終了コード 1」というエラーが出ました。**	4.0(1b)	4.0(2b)
CSCvt13947	HX Connect で次のアラート/イベントを受信します。HX コントローラ VM {HOSTNAME} 複数の設定済み DNS サーバが応答していません。	4.0(2a)	4.0(2b)
CSCvt14914	4.0.2 a へのアップグレード後に、API、UI、CLI は、空のドライブ スロットがいくつかあると表示します。 これらのドライブは、sysmtool、lsscsi、および stcli コマンドの出力では表示されます。 クラスタは正常であり、エラーはありません。	4.0(2a)	4.0(2b)
CSCvs69154	HX コントローラで DNS サーバが正常に変更された後も、展開中に追加された元の DNS エントリを確認できます。	3.5 (2d)	4.0(2b)
CSCvs30080	HyperFlex Connect および vCenter は、HX および非 HX データストアで APD アラームを表示します。これは、HyperFlex で、本来存在しないはずの問題が発生していることを意味します。	3.5(2e)	4.0(2b)
CSCvs74286	ノードの再起動後、ノード内のすべてのディスクがロックされる問題がありました。 **sed-client.sh -U** コマンドを使用すれば、正常にロック解除することができますが、もう一度再起動すると、ドライブは再びロックされます。	4.0(2a)	4.0(2b)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvt13929	HyperFlex で「stcli license...」コマンドを実行すると、次のようなエラーが表示されます。 root@SpringpathController:/tmp# stcli license show all Show smart licensing failed (スマート ライセンスの表示に失敗しました:): Smart Agent is not ready, please wait a minute and try again (Smart Agent の準備ができていません。しばらく待ってから、もう一度やり直してください)	4.0(2a)	4.0(2b)
CSCvt20144	HX 4.0 (2a) にアップグレードした後、最初に再起動される Robo/Edge ノードは、永続ドライブ PID: HX-HD24TB10K4KN を無視します。 クラスタは縮小状態になり、キャパシティは減少します。	4.0(2a)	4.0(2b)
CSCvs21562	Exhibitor の実行中は、Zookeeper が起動できません。ただし、「echo srvr」は何も返しません。	3.5 (2b)	4.0(2b)
CSCvs91787	HyperFlex のアップグレードを実行すると、Enterprise Plus または Enterprise ハイパーバイザのライセンスがないホストが原因で、検証の警告が発生することがあります。 Upgrade Validation Warning: (アップグレード検証の警告) ESXi host esx1.lab.test should be configured with VMware Enterprise license for upgrade to continue. (ESXi host esx1.lab.test のアップグレードを続行するには、VMware Enterprise のライセンスを使用して設定する必要があります。)	4.0(2a)	4.0(2b)
CSCvs69317	ストレージ コントローラ (SCVM) の root と admin のパスワードが異なる場合、インストーラの設定の段階でクラスタの拡張が失敗します。	3.5 (2g)	4.0(2b)
CSCvt06983	ESXi のアップグレード中にパニックが発生します。	3.5 (2g)	4.0(2b)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs54285	動作中のクラスタ ノードは、Linux カーネルでハングする可能性があります。これは、意図した動作からの逸脱として分類されます。	4.0(2a)	4.0(2b)
CSCvs69007	10+10 ノード HX 3.5 (2g) ストレッチ クラスタで再調整が失敗します。	3.5 (2g)	4.0(2b)
CSCvr54687	クラスタが IOVisor からアクセスできなくなります。	3.5 (2d)	4.0(2b)
CSCvt61297	ストレージ コントローラでパニックが発生します。	4.0(2a)	4.0(2b)
CSCvt63306	サポートバンドルのサイズは、storfs-support コマンドを使用して収集すると非常に大きくなります。	4.0(2a)	4.0(2b)
CSCvt72807	/var/stv の使用率が 80% を超えると、**FileSystemUsageWarningEvent** または **FileSystemUsageAlertEvent** に関連付けられている storfs がクラッシュします。	4.0(2a)	4.0(2b)

リリース 4.0(2a) の解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
ESXi、インストール、アップグレード、展開、管理			
CSCvo39912	通常のシナリオでは、サービス プロファイルの更新後にHX のアップグレードが保留中の ACK を取得します。この場合、サービス プロファイルの更新に HX アップグレードが保留中の ACK を取得しておらず、常に待機状態であったため、UCS のみのアップグレードが停止しました。	3.5 (2d)	4.0(2a)
CSCvq39471	MotherBoardReplace-1.2 を使用して古い stNode/pNodes から ZK をクリーンアップすると、データストアがマウント解除され、HyperFlex データストア 0 のサイズが変更され、クラスタ内のすべての VM がオフラインになります。	3.5(1a)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvm77294	クラスタのアップグレードとエラーの取得： アップグレードの検証に失敗しました。 vCenter の設定を確認しています。理由:アップグレードの検証に失敗しました。DRS 障害：設定されたフェールオーバを満たすリソースが不足しています	2.6(1e)	4.0(2a)
CSCvo70650	DR 複製が設定されているノードでは、クラスタの展開が失敗します。 DR 複製が設定されている HX クラスタが展開されている場合は、管理 VLAN 情報ではなく、複製 VLAN 情報でインストーラ UI がプルされます。その情報を正しい管理 VLAN id と名前に変更しても、ESXi の複製 VLAN の VLAN でノードが設定されているため、機能しないように見えます。これにより、ホスト到達不能エラーによるノード追加の障害が発生します。	3.5(2a)	4.0(2a)
CSCvo91624	お客様によりサーバがファームウェアのアップグレードを 1 個ずつ自動的に完了しなかったことを報告しました。 ユーザーはホストをメンテナンス モードにし、手動で保留中の要求を確認して、UCS ファームウェアのアップグレードを完了する必要があります。 メンテナンス ポリシーは、設計に従ってデフォルト (ユーザー ack) に設定されます。	3.5(1a)	4.0(2a)
CSCvo93017	クラスタが「失敗」状態になっている状態で、stcli ノードの削除が試行された場合、クラスタからノードを削除できなかった場合でも、出力は正常に表示されます。	3.5 (1i)	4.0(2a)
CSCvp31021	HyperFlex クラスタのアップグレードは、検証中に「DRS 検証が失敗しました」というエラーで失敗する場合があります。	3.5(1a)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp58318	HX クラスタの展開が失敗し、次のエラー メッセージが表示されます。 MAC アドレス プール設定障害 150 [ErrorDescription]：不正なアドレス ブロック範囲定義コリジョン。	3.5 (2b)	4.0(2a)
CSCvq34873	カーボン キャッシュによるメモリ使用量。	3.5 (2b)	4.0(2a)
CSCvr03240	ESXi クラスタのアップグレードは、「ノードのメンテナンス モードが失敗しました」というエラーで失敗します。	3.5 (2g)	4.0(2a)
CSCvr88978	storfs プロセスは、HX メンテナンス モードの終了またはストレージ コントローラを再起動するその他のタスクでは自動的に開始されません。	3.5(2e)	4.0(2a)
CSCvp10707	インストール後のスクリプトは次のメッセージで失敗します。 HX ノードでの ipmitool の実行に失敗しました。	3.5(2a)	4.0(2a)
CSCvp46539	HyperFlex 拡張ワークフローでは、VLAN 名が正しくプルされません。	4.0(1a)	4.0(2a)
CSCvq45087	HXクラスタの展開中: クラスタ作成の検証フェーズ-HX インストーラがエラーで失敗する可能性があります。 `*** from \var\log\springpath\stDeploy.log ***`	3.5(2a)	4.0(2a)
CSCvq91380	HXインストーラが、ESXホストを設定するために SOL にログインできません。	3.5 (2b)	4.0(2a)
CSCvr44222	その他の設定パラメータを使用して DRS が有効になっている場合、手動または部分的に自動化された設定パラメータは、クラスタの展開時に完全に自動化されるように変更されます。	3.5 (2d)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp82175	検証タスク名の 1 つに入力ミスがあります。タスク名は「SED と非 SED ディスクが混在しているノードを検証中」です。 これは「SED と非 SED ディスクが混在しているノードを検証中」である必要があります。	3.5(1a)	4.0(2a)
CSCvo12359	小さい NVMe ドライブを使用したこの組み合わせは、拡張操作ではサポートされていません。たとえば、ドライブが 375GB のみで、より大きなキャッシング SSD を持つ既存のクラスタに追加できない場合などです。	3.0(1i)	4.0(2a)
CSCvp66679	Hyperflex に、次の Common Vulnerabilities および Exposures によって識別される脆弱性の影響を受けるバージョンの OpenSSL が含まれています。 CVE-2018-0495	3.5(1a)	4.0(2a)
CSCvo00511	GPU pci パススルーが接続されている VM でネイティブ スナップショットを取得すると、SDK 呼び出し例外が発生します。	3.0(1e)	4.0(2a)
CSCvo62867	EAM エラーが原因でノード交換スクリプトが失敗します。	3.0(1i)	4.0(2a)
CSCvo79760	クラスタ (HX リリース >= 3.5) とクラスタ (HX リリース<3.5) のペアリング中に、クラスタでリモート複製ネットワークテストが失敗します(HX リリース < 3.5)。	3.5(1a)	4.0(2a)
CSCvo87061	最新のサポート ワークフロー バンドルの問題を修正しました。これ以上にはヒットしません。	3.0(1b)	4.0(2a)
CSCvo87080	3 ノードクラスタでは、スクリプトが「健全な」クラスタ ステータスを検索するため、MBreplace スクリプトは失敗します。	3.5(2a)	4.0(2a)
CSCvp12359	3.5.2 b または 4.0 で実行している場合、MbReplace スクリプト (tar) はハングします。	3.5(2a)	4.0(2a)
CSCvp63958	HX 複製のクリーンアップが次のエラーで失敗しました:「NA 3.5(2a)：情報：DR の状態がクリーンではありません」。	3.5(2a)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp66277	Check_stig_parameters API は ASA に準拠していないため、クラスタのコンプライアンス状態を誤って表示します。	4.0(1a)	4.0(2a)
CSCvq06952	CBT が有効になっている VM でのスナップショットの作成が失敗し、「vmreparent vmkfstools clone1 でエラーが発生しました」というエラーが表示されます。	3.5 (2c)	4.0(2a)
CSCvo60587	リモート DR レプリケーション パートナー/ピアを設定するときに、HyperFlex GUI はリモート レプリケーション パートナーの TCP ポートの到達可能性テスト結果を表示します。 これにより、迅速な初期接続結果を得ることが可能で、頻繁に顧客が手動で確認します。 到達可能性テストに失敗した場合、情報ウィンドウと HX アラートがトリガーされ、到達不可能な宛先ピア IP と特定のポートがリストに一覧表示されます。	3.5(2a)	4.0(2a)
CSCvr67130	レプリケーション ネットワーク用に複数の IP プールが設定されていて、ローカル レプリケーション ネットワーク テストが失敗している場合は、この問題が発生している可能性があります。	3.5 (2b)	4.0(2a)
CSCvp05204	MBreplace およびソフトウェア再展開スクリプトのタスク オプションをスキップします。スクリプトには、json ファイルを変更することなく、ユーザー入力としてタスクをスキップするオプションがあります。	3.5(2a)	4.0(2a)
CSCvq34357	HyperV の SCVM コンソールの「print_req_error: I/O error, dev fd0, sector 0」でエラーが発生しました。 SSH セッションでは起動しません。	4.0(1a)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvk36222	VM ネットワーク スイッチは、インストール プロセスの一部としてすでに作成されています。 理想としては、初期インストール プロセス中に ip アドレスの割り当ても実行する必要があります。インストール後の手順は必須ではありません。代わりに、インストール後のスクリプトの一部として実行できます。	3.0(1d)	4.0(2a)
CSCvg53223	2.1(1) から 2.5(1c) への HX アップグレード中に影響を受ける storfs サービス アップグレードされていない storfs サービスを停止した HX ノードは停止を引き起こしました。	2.5(1c)	4.0(2a)
CSCvp37536	HX ストレッチ クラスタ監視 VM は、リブート時に DHCP に戻ります。	3.5 (1b)	4.0(2a)
CSCvp46578	HyperFlex ストレッチ クラスタ監視は、NTP サーバではプログラミングされていません。	3.5 (2b)	4.0(2a)
CSCvr18528	HyperFlex クラスタは、ノード/サーバのメンテナンス後に修復されません。	3.5 (2b)	4.0(2a)
CSCvr97089	Eth1 データインターフェイス 9K MTU でのパケット損失率が高くなります。	4.0(2a)	4.0(2a)
CSCvr16760	HyperFlex クラスタの修復状態が 87% に留まっており、進行できません。	3.5(2f)	4.0(2a)
CSCvq22898	場合によっては、同じ VM に対して 2 つのレプリケーションが発生することがあります。 GUI から、この VM のレプリケーション ステータスは「進行中」状態であることが示されていますが、レプリケーション層ではジョブがスタックされていません。それ以降のレプリケーションは成功するはずです。	4.0(2a)	4.0(2a)
CSCvp13990	予期しない停電が発生すると、hyperflex クラスタが正常に起動できなくなります。 すべてのプロセスが実行中で、時刻が同期され、必要に応じてすべてのノードが相互に vmkping を実行できます。	3.5(2a)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp33657	ノード ID の代わりに IP アドレスを指定すると、**stcli node maintenanceMode** コマンドは失敗します。	4.0(1a)	4.0(2a)
CSCvr31573	2 ノードエッジ クラスタ (Intersight/arbitrator 接続の問題が発生している場合) では、クラスタがダウンするため、HX メンテナンス モードを開始できません。	4.0(1a)	4.0(2a)
CSCvr89066	/Var/support/ZKTxnlog の古いファイルは、日次 zklog-cleanup cron job ジョブでは消去されません。	3.5 (2c)	4.0(2a)
CSCvo86431	ノードがメンテナンス モードの場合、ノードがメンテナンスモードから復帰した後にのみ、ディスクの削除または交換が UI に反映されます。これは、メンテナンス中に storfs がノード上で実行されておらず、メンテナンス モードから復帰するまでディスク アクティビティを検出できないためです。	3.5(2a)	4.0(2a)

CSCvr01645	クラスタがオフラインになり、IO 要求の処理を停止する可能性があります。
	`root@cvm:~# stcli cluster storage-summary --detail`
	`Get cluster storage summary failed: java.net.ConnectException: Connection refused: /192.168.142.100:10207`
		3.5 (2c)	4.0(2a)

CSCvq80340	ストレッチ クラスタの展開が HyperFlex インストーラの「フォーマット ノード ノード使用中」というメッセージで失敗し、crmZoneType 値が storfs または /opt/springpath/config/stretch.tunes で 1 と表示されます。	3.5 (2d)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvq63888	アップグレード中に、Cisco.com からダウンロードしたアップグレード パッケージをアップロードします。アップグレード パッケージは、ファイル タイプ .tgz hxconnect で、storfs-packages-4.0.1a-33028.tar ファイルを受け入れます。異なるタイプの圧縮を使用し、ESXi でブートストラップおよび scvmclient のアップグレードのためにファイルを展開できない場合は、アップグレードを開始すると失敗する可能性があります。	3.0(1c)	4.0(2a)
CSCvr52098	Intersight を使用して hyperflex をインストールしようとすると、次のエラーが表示されます。 タスクが失敗しました。「vCenter クラスタへホストを追加する際にエラーが発生しました。vCenter にホストを手動で追加して再試行してください。アドレスを取得できませんでした：名前ごとにホスト化できませんでした：lookup Hostname.company.com on 0.0.0.0:53: read udp 127.0.0.1:45430->127.0.0.1:53: read: 接続が拒否されました	4.0(2a)	4.0(2a)
CSCvo92952	クラスタの作成の検証を実行中に、CoreAPI コールがクラスタ管理 API に対してタイムアウトする場合があります。	3.5(2a)	4.0(2a)
CSCvq95460	ESXi バージョンが異なる場合は、拡張 vMotion 互換性の非互換性により、「混合モード拡張チェック」で検証が失敗します。	3.5 (2d)	4.0(2a)
CSCvr66309	「ストレージ コントローラ VM でソフトウェア パッケージをインストール中」にカスタム ワークフローが「ハイパーバイザ設定」 +「展開」(clean disk partition = no) が使用されている場合、この障害がインストーラで表示されます。	3.0(1i)	4.0(2a)
CSCvq93831	HX インストーラは、設定を JSON ファイルにエクスポートする際に、VLAN ID の範囲でカンマをセミコロンで置き換えているように見えます。	3.5 (2d)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp22693	サポートされていないブラウザを使用している場合、HX Connect ユーザーはログインできません。これらのユーザーには、不正なユーザーを示すエラーが表示されます。	4.0(1a)	4.0(2a)
CSCvp24343	Cisco HyperFlex ソフトウェアの Web ベースの管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者が、該当システムに対してクロスサイト要求偽造 (CSRF) 攻撃を実施する可能性があります。 脆弱性は、影響を受けるデバイスで Web UI の CSRF 保護が不十分なことが原因です。攻撃者は、ユーザーが悪意のあるリンクをクリックしたり、悪意のある PDF ファイルを開いたりするように仕向けることにより、この脆弱性を不正利用する可能性があります。不正利用が成功すると、攻撃者はユーザーの権限で任意のコードを実行する可能性があります。 この脆弱性に対処するソフトウェア アップデートは、すでに Cisco からリリースされています。脆弱性に対処する回避策はありません。 このアドバイザリは、次のリンク先で確認できます。 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-hyperflex-csrf	4.0(1a)	4.0(2a)
CSCvq22844	保留中のアクティビティを確認せず、UCSM でサーバが再起動し、HX Connect 進捗フローにメッセージを追加します。 HX Connect は、制御されたローリング サーバのアップグレードをバックグラウンドで実行しています。	3.5 (2d)	4.0(2a)
CSCvr43786	クラスタ名が正しくないため、コンピューティング ノードの展開操作が失敗します。	4.0(1b)	4.0(2a)
CSCvp41241	データの再同期中の RF 2 クラスタのシャットダウン。ノード障害後 (非 storfs)。その後、複数のディスク読み取り障害が発生します。ハードブラックリストに登録されています。	2.6(1e)	4.0(2a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvo13143	HyperFlex Edge ノードは、導入時に ESXi ホスト名を適切に設定しません。	4.0(1a)	4.0(2a)

リリース 4.0(1) の解決済みの問題 (1b)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
ESXi、インストール、アップグレード、展開、管理			

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs28167		2.6(1e)	4.0(1b)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客はHXインストーラOVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチ クラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラー メッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。
	条件：
	顧客は HX 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a) または 4.0(1b) を展開している場合、Cisco は OVA ファイルに再署名して再投稿しており、パッチが適用された OVA ファイルを使用している場合この問題は発生しません。OVA ファイルが修正されたことを示す OVA ファイル名の「p1」サフィックスを探します。
	ファイル名の例：
	VMware ESXi 用 Cisco HyperFlex Data Platform インストーラ用の HX 4.0(1b) パッチ OVA ファイル:
	`Cisco-hx-data-platform-installer-v1.7.1-14786.ova 4.0.1 b-33133p1-esx`
	Cisco HyperFlex Data Platform ストレッチ クラスタ Witness：
	`HyperFlex-Witness-1.0.4 p1 ova`
	他の HX リリースで OVA ファイルを使用しているお客様は、次の回避策を参照してください。
	回避策		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
	影響を受ける OVA ファイルでの展開が失敗した後、続行するには 2 つのオプションがあります（インストーラおよびOVA ファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェストファイルを検出可能なため、vCenter は証明書の有効性を確認します。 **1.** OVA ファイルをローカル ディレクトリにダウンロードして展開します。 **2.** .mf ファイルを削除します **3.** 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 **4.** vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftool はダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。
	`root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX host>/`
	2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
	3. VM とコンソールの電源をオンにします
	4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
	5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
	6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
	`address <desired ip address of installer>`
	`netmask X.X.X.X`
	`gateway X.X.X.X`
	`<esc> :wq`
	7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
	8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
	9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvp64140	Windows Server Hyper-V で HyperFlex インストーラを実行しているときに、クラスタ作成プロセスが失敗し、「クラスタ作成プロセス中にエラーが発生しました。このコンテンツをダウンストリームに送信できません」というエラーが発生します。この現象は、Cisco VIC 1457 MLOM (PID: HX-MLOM-UCSC-MLOM-C25Q-04-04) と Windows Server Datacenter または Core with Hyper-V バージョン 2016 または 2019 で設定/発注された Hyperflex ノードを使用した Hyperflex クラスタの展開中に発生します。	4.0(1a)	4.0(1b)
CSCvo69067	クラスタにミクロン 5200 ドライブを追加すると、クラスタ容量が増加することはありません。	3.5 (2b)	4.0(1b)

リリース 4.0(1a) の解決済みの問題

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
ESXi、インストール、アップグレード、展開、管理			

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvs28167		2.6(1e)	4.0(1a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	Cisco HyperFlex でノード置換をインストールまたは完了するため、顧客はHXインストーラOVA（オープン仮想アプライアンス）ファイルをダウンロードする必要があります。ストレッチ クラスタを展開するには、顧客はさらに Witness OVA をダウンロードする必要があります。リリース HX 3.5(2g) の登校前に CCO で投稿されたすべてのコードは、2019 年 11 月 26 日に期限切れになっている証明書を検出しました。Cisco は更新された証明書で、HX リリース 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a)、4.0(1b) に関連付けられている OVA ファイルを再署名および再投稿しました。その他のリリースについては、期限切れの OVA を持つ OVF テンプレートを展開しようとすると、次のエラー メッセージ「OVA パッケージは無効な証明書で署名されています」で失敗します。
	条件：
	顧客は HX 3.5(2e)、3.5.2(f)、3.5.2(g)、4.0(1a) または 4.0(1b) を展開している場合、Cisco は OVA ファイルに再署名して再投稿しており、パッチが適用された OVA ファイルを使用している場合この問題は発生しません。OVA ファイルが修正されたことを示す OVA ファイル名の「p1」サフィックスを探します。
	ファイル名の例：
	VMware ESXi 用 Cisco HyperFlex Data Platform インストーラ用の HX 4.0(1a) パッチ OVA ファイル:
	`Cisco-hx-data-platform-installer-v1.7.1-14786.ova 4.0.1 a-33028p1-esx`
	Cisco HyperFlex Data Platform ストレッチ クラスタ Witness：
	`HyperFlex-Witness-1.0.4 p1 ova`
	他の HX リリースで OVA ファイルを使用しているお客様は、次の回避策を参照してください。
	回避策
	影響を受ける OVA ファイルでの展開が失敗した		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
	後、続行するには 2 つのオプションがあります（インストーラおよびOVA ファイルに適用）。 オプション A：ローカル マニフェスト ファイルを削除します。 マニフェストファイルを検出可能なため、vCenter は証明書の有効性を確認します。 **1.** OVA ファイルをローカル ディレクトリにダウンロードして展開します。 **2.** .mf ファイルを削除します **3.** 残りのファイルを新しいアーカイブに追加して、「.tar」から「.ova」にファイルの拡張子を変更します。 **4.** vCenter で「OVF テンプレートで展開」を使用して新しく OVA ファイルを作成する展開を続行します。vCenter は証明書を所持していないためファイルを表示します。これは予想された動作で、展開は問題なく続行します。 オプション B - ローカル マニフェスト ファイルを削除します。 ovftool で手動展開：VMware の ovftool を使用して、証明書確認をバイパス中に OVA を展開します。ovftoolはダウンロードして顧客のコンピュータで実行可能です。ovftool も HX コントローラ VM で事前インストールされます。これはノード交換とクラスタ拡張にも役立ちます。		

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み

	1. skipManifestcheck スイッチを発生させている間、ovftool を使用して OVA ファイルをデータストアに展開します。次に例を示します。
	`root@SpringpathControllerABCDEFGH:~# ovftool --skipManifestCheck -ds=datastore http://<path to ova>/Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova vi://root@<IP of management ESX host>/`
	2. OVA を展開し、以前指定した ESXi ホストの vCenter に存在している必要があります。
	3. VM とコンソールの電源をオンにします
	4. root / Cisco123 のユーザー名/パスワードのデフォルトの組み合わせで VM にログインします
	5. **vi /etc/network/eth0.interface** を発行して VM の IP を静的に設定します
	6. 「iface eth0 inet dhcp」を「iface eth0 inet static」に変更します。次のいずれかが独自のラインと指定したタブで必要になります
	`address <desired ip address of installer>`
	`netmask X.X.X.X`
	`gateway X.X.X.X`
	`<esc> :wq`
	7. ファイルを確認および保存後、VM が再起動します。VM は現在希望している IP アドレスでブートされる必要があります
	8. WebGUI 経由での最初のログイン（引き続きデフォルトのユーザー名/パスワードの組み合わせ）は、ユーザーがパスワードを変更します。
	9. パスワードの変更後、ユーザーは希望のインストール/拡大/ノードの交換アクティビティを開始できます。		

CSCvk17250	異なるセクター サイズのディスクが HX ノードに配置されると、クラスタが不安定になります。	3.0(1d)	4.0(1a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvo36198	ログインすると、仮想センター アカウントの代わりにローカル HX ユーザー アカウントを使用して、VC が到達可能になると、「仮想センター到達不能」または「リソース情報を更新できません」というエラー メッセージが断続的に表示されます。	3.5(1a)	4.0(1a) 3.5 (2c)
CSCvk38003	HXDP は EMC RecoverPoint では動作しません。VMware API (FSS-Readdir) のサポートが必要です。	3.0(1d)	4.0(1a) 3.5 (2b)
CSCvm90352	HyperFlex ストレージ コントローラ VM での Zookeeper (Exhibitor) プロセスは、`/var/zookeeper` で空き領域が不足している場合、要求に応答できない場合があります。	2.5(1c) 2.5(1d)	4.0(1a) 3.5(2a) 3.0(1i)
CSCvn02151	HX スナップショットには非同期統合を使用します。	2.6(1c)	4.0(1a)
CSCvo90713	バックアップ ベンダーの HX Quiesced スナップショット。	3.5 (2b)	4.0(1a)
CSCvn17787	クラスタの作成/クラスタの拡張ワークフローは、検証手順で次のエラー メッセージが表示され停止します。 FIRMWARE-Check UCSC-SAS-M5HD FIRMWARE-Check UCSC-SAS-M5HD : Required: 00.00.00.29,00.00.00.32,00.00.00.35,00.00.00.50, Found: 00.00.00.58; 必要なアクション: 必須バージョンにコントローラ ファームウェアを更新する	3.5(2a)	4.0(1a)
CSCvn73127	ローカル データストアが ESXi で検索されると、Kernel の移行に失敗します。	3.0(1d)	3.5 (2b)
CSCvk46364	容量ディスクが最初に挿入され、キャッシング ディスクが次に挿入される場合、2 個のディスクが交換されると (キャッシング ディスクおよび別の容量ディスク)、ノードがシャットダウンします。	2.6(1b)	3.5(2a)
Hyper-V			
CSCvn28721	クラスタの拡張はエラー コード `500` 操作のタイムアウトで失敗する可能性があります。	3.5(2a)	4.0(1a)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvn54300	アップグレード時に、ユーザーの vSwitch に作成されたチームで VLAN を削除します。新規インストール時には、複数の Vlan が入力されていても、1つの VLAN タグだけが vSwitch とチームに設定されます。	3.5(2a)	3.5 (2b)
CSCvn60486	Hyper-V クラスタをアップグレードするとき、**stUpgradeService** および Zookeeper サーバ間でレアな競合状態のアカウント上では、アップグレード オーケストレーションはアップグレード検証エラーをスローし、アップグレード プロセスが中断します。	3.5(2a)	3.5 (2b)

リリース 4.0(2b) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害
CSCvt55712	EAM サービスが実行されていない場合、vCenter の登録が失敗します。	vCenter で EAM サービスを開始/再開します。	4.0(2a)
CSCvt45344	HyperFlex ストレッチ クラスタで、書き込み遅延が原因でアプリケーションのパフォーマンスが低下し、クラスタに問題が残り、再調整が停止します。 この不具合は、現在調査中です。	同様の状況が発生していると思われる場合は、Cisco TAC にお問い合わせください。	3.5(2a)
CSCvt36374	コントローラ VM の/var/stv フォルダがいっぱいになることがあります。	ログファイルがローテーションされない場合は、/var/log/springpath フォルダからログファイルを削除してください。関連するサービスを停止し、/var/log/springpath フォルダから大きなログファイルを削除して、サービスを再起動します。	3.5 (2g)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvt89709	DR ネットワークを使用して設定されたクラスタでは、IPTable ルールを有効にしている間、StMgr が初期化されず、デッドロックでスタックします (stMgr .log から確認できます)。	StMgr を再起動すると、再度初期化されます。	4.0(2b)

リリース 4.0(2a) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs75553	ユーザーがグループ内で保護されている VM をグループ内の他の VM とともに復元する場合は、スタンドアロンモードで「復元」状態に移行します。選択した VM は「復元済み」状態に移行します。	スタンドアロンモードで、選択した VM の [復元 (recover)] をもう一度クリックします。これにより、VM が復元した状態に移行します。	4.0(2a)
CSCvq38279	Hyper-V: 複製した DC が使用されたとき、インストール時に Windows フェールオーバークラスタが正常に作成されませんでした。	クラスタをクリーンアップして、フェールオーバークラスタを再作成します。HX ストレージクラスタに触れる必要はありません。	3.5(2e)
CSCvr20922	HyperFlex クラスタのストレージ使用率が 92 %の使用可能容量を超えています。	クラスタの使用率をできるだけ低くしてください。読み取り専用状態を回避するには、92% 未満にしてください。	3.5 (2d)、4.0 (1a)
CSCvs74286	ノードの再起動後、ノード内のすべてのディスクがロックされました。 「Sed-client.sh-U」コマンドを使用してロックが正常に解除されましたが、別途再起動でテストする必要があり、ドライブが再度ロックされました。	NA	4.0(1b)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs93245	暗号化を有効にすると、HX connect の暗号化ステータスに注意が表示されますが、すべてのディスクで暗号化が成功します。 -「自己暗号化ドライブ サービス」は、すべてのノードで実行されています。 -暗号化のエラー メッセージはありません。 -USB0 インターフェイスが起動しています。 -「サポート済み」と表示されているすべての SED ディスク：1、「有効」: 1、「ロック済み」：0、	VM を回復するには、データ ディスクをコピーして新しい VM に接続します。	3.5 (2g)
CSCvs54285	HX リリース 4.0(1b) を実行しているクラスタ ノードは、Linux カーネルでハングする可能性があります。これは、意図した動作からの逸脱として分類されます。	永続的な設定として kernel.panic_on_oops を有効にします。これにより、ノードがパニック状態になり、すぐに再起動します。	4.0(1b)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs41324	HX クラスタでの K8/iscsi スタックの有効化。		4.0(2a)

不具合 ID	症状	回避策	リリースで検出された障害
		HX クラスタで K8 を有効にする手順。 すべてのコントローラ VM で次の手順を実行します。 **1.** 「/etc/init/scvmclient.conf」を更新して「iscsiEnable」を「true」に調整します。 **# sed -ie "s/iscsiEnable=false/iscsiEnable=true/" /etc/init/scvmclient.conf** **2.** 設定をリロードするには、次の initctl cisco-amp コマンドを実行します。 **# initctl reload-configuration** **3.** Scvmclient プロセスを再起動します。 **# stop scvmclient; start scvmclient** **4.** システム DS をマウントするには、次の initctl cisco-amp コマンドを実行します。 **# initctl emit --no-wait system-datastore-created** **5.** 次のコマンドを使用して、「iscsiEnable」の調整が「true」に設定されていることを確認します。 **# ps-eaf |grep scvmclient |grep-v grep** **root 6241 1 1 Dec06 ? 01:40:07 /opt/springpath/storfs-core/scvmclient -T logEnabled=false -T logSyslogEnabled=true -T logEchoToScreen=false -T statLoggingToFile=false -T**	

不具合 ID	症状	回避策	リリースで検出された障害
		statLoggingToSyslog=true -T logDir=/var/log/springpath -T nfsBackendServerList=10.107.48.100 -T iscsiEnable=true -T iscsiUseAsync=true -T iscsiConfigFilePath=/fs/SYSTEM/iscsi.conf# ps -eaf | grep scvmclient | grep -v grep	
CSCvr83056	HyperFlex データストアの NFS キューの深さは256として表示されます。これは、パフォーマンス (遅延を含む) の問題を引き起こす可能性があります。	次の手順を使用して、NFS キューの深さを確認し、必要に応じて増やすことができます。 **root@HXESXI1] vsish -e get /vmkModules/nfsclient/mnt/[DATASTORE]/properties | grep -i maxqdepth maxQDepth:256 <- Low value [root@HXESXI1] vsish -e set /vmkModules/nfsclient/mnt/[DATASTORE]/properties maxQDepth 1024 [root@HXESXI1] vsish -e get /vmkModules/nfsclient/mnt/[DATASTORE]/properties | grep -i maxqdepth maxQDepth:1024 <- Optimal value** これを有効にするには、ESXi ホストを再起動する必要があります。 ノードを HyperFlex メンテナンスモードにして、変更を適用するためにノードをグレースフル リブートしてください。	3.5(2e)
CSCvs47735	クラスタ内の1個のノードがオフラインになっている場合、「stcli cluster storage-summary」には root@SCVM 使用できない2個のノードが表示されます。~# stcli cluster storage-summary。	これは表面的なものです。クラスタが正常なステータスに戻ると、エラーが解消されます。	4.0(1b)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvs69317	ストレージコントローラ (SCVM) の root と admin のパスワードが異なる場合、インストーラの設定の段階でクラスタの拡張が失敗します。	SCVMs のルートと管理者パスワードの両方を同じに変更します。 **stcli security password set -u admin**	3.5 (2g)
CSCvs69154	HX コントローラで DNS サーバが正常に変更された後も、展開中に追加された元の DNS エントリを確認できます。	NA	3.5(2d)
CSCvs53555	アップグレードが失敗した場合、またはノードを HX メンテナンスモードに移行しようとするなどのタスクが発生した場合、次のエラー メッセージが表示されることがあります。	この問題を特定して修正するために、TAC と連携させることを強くお勧めします。 **1.** すべてのノードの /opt/springpath/sysmgmt/stMgr-10.conf で、「getcluster」を 2m から 8m に変更します。 **2.** すべてのノードで stMgr を再起動します	3.5(2e)
CSCvt13947	HX Connect で次のアラート/イベントを受信します。HX コントローラ VM {HOSTNAME} 複数の設定済み DNS サーバが応答していません。	ルートとして各ストレージコントローラ VM で次のコマンドを実行します。 **grep -i 'monitor_dns_servers": true' /opt/springpath/watchdog/watchdog.conf.json && sed -ie '/"monitor_dns_servers": true/"monitor_dns_servers": false/' /opt/springpath/watchdog/watchdog.conf.json && grep -i 'monitor_dns_servers": true' /opt/springpath/watchdog/watchdog.conf.json && restart watchdog**	4.0(2a)
CSCvs21562	Exhibitor の実行中は、Zookeeper が起動できません。ただし、「echo srvr」は何も返しません。	/var/log/zookeeper/version-2 または/var/log/zookeeper/standalone/version-2 以下に空の (サイズ 0) ログファイルがあれば、削除します。	3.5 (2b)

リリース 4.0(1b) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害
インストール、アップグレード、展開			
CSCvs02466	サーバー ファームウェア 4.0(4e) へのアップグレード後、M.2 ブートディスクがサーバーインベントリに表示されません。その結果、サーバはM.2ディスクにインストールされている OS で起動できません。この問題は、サーバーの再認識およびコミッション解除と再受信確認後も発生します。	1. サーバーをコミッション解除する 2. サーバーの電源ドレイン - サーバー背面にある両方の電源コードを10秒間取り外してから、電源コードを再挿入します。 3. サーバーを再コミッションします。	4.0 (4e)
CSCvq32721	多くのディスクが障害または手動でオフラインになったため、クラスタに ENOSPC が生じます。	フラッシャを手動で再起動します。	3.5(2e)
CSCvq38279	[Hyper-V]複製した DC が使用されたとき、インストール時に Windows フェールオーバー クラスタが正常に作成されませんでした。	クラスタをクリーンアップして、フェールオーバー クラスタを再作成します。HX ストレージ クラスタに触れる必要はありません。	3.5(2e)
CSCvq54992	リリース 3.5 (2a) から 3.5 (2x)、4.x へのアップグレードで、 scvmclient がアップグレードされません。リカバリ ポイントが機能しない可能性があります。	Scvmclient VIB を手動でインストール/アップグレードし、それが現在の HXDP バージョンと一致していることを確認します。	3.5 (2b)
管理			
CSCvj22992	[HyperV]VM が複数のノードに表示されます。	VM を回復するには、データディスクをコピーして新しい VM に接続します。	3.0(1b)
CSCvm99150	1 個の ESX ノードで MTU を 9000 から 1500 に変更すると、すべてのノードで storfs プロセスが再起動します。	1. 実行中のクラスタでは、ESX レベルで MTU を変更しないでください。 2. 元の値に戻します。	3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp23718	8TB または 12TB のディスク ドライブを搭載したクラスタでは、クラスタ内で別のノードに障害が発生してから数分の間、I/O が停止する可能性があります。		4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
		インストール後 (新規展開の場合)、または 4.0 1a へのアップグレード後 (既存の展開の場合)は、すべてのコントローラ VM に次の手順を実行します。 1. (すべてのコントローラ VM 上の) 次の調整ファイルを編集します。 /opt/springpath/config/1ff.tunes /opt/springpath/config/vsi_1.6bb.tunes 2. セット cleanerEnableSegSummaryCleaning 「false」になります。 3. 上記のファイルを編集した後、次の手順を実行します。 a. すべてのコントローラ VM に SSH でログインします。 b.「Storfstool---Z」を実行します。 c. 次のコマンドを実行して、値を確認します。調整値は「true」にする必要があります **# cat /opt/springpath/config/tunables/cleanerEnableSegSummaryCleaning** **cleanerEnableSegSummaryCleaning = true** d. 次のコマンドを入力し、調整の変更を動的に適用します。 **# echo false > /opt/springpath/config/tunables/cleanerEnableSegSummaryCleaning** e. 調整値が変更されていることを確認します。次のコマンドを実行します。値は「false」にする必要がありま	

不具合 ID	症状	回避策	リリースで検出された障害
		す。 # **cat /tmp/procfs/sys/vmware/logging/cleanerEnableSegSummaryCleaning** **cleanerEnableSegSummaryCleaning = false** **f. umount /tmp/stprocfs**	
CSCvp26319	HX 3.5(2b) FlexVol から HX 4.0 CSI へのアップグレードは機能しません。FlexVol は引き続き動作します。	1. 設定ファイルを手動で更新して、リンクローカルアドレスを * に変更します。 2. コントローラと ESX で scvmclient を再起動します。	4.0(1a)
CSCvp62512	7ノードクラスタの修復は、再調整の変更 AMS の要件が修復プロセスをブロックしているため、非常に遅くなります。	ノードが修復されるまで再調整を無効にし、再調整を再度有効にします。	3.5(2a)
CSCvq49412	クラスタ内のストレージ容量を使用している場合は、[site failover cluster (サイトフェールオーバークラスタ)] の下にあります。クラスタでは、すべてのパス (APD) のダウン状態が発生する可能性があります。	NA	3.5(2a)
CSCvp36364	この製品には、次の Common Vulnerabilities および Exposures によって識別される脆弱性の影響を受けるサードパーティソフトウェアが含まれています。 CVE-2016-0762、CVE-2016-6797、CVE-2016-6816、CVE-2016-8735、CVE-2017-5647、CVE-2017-12615、CVE-2017-12616、CVE-2017-12617、CVE-2017-7674、CVE-2018-1304、CVE-2018-8014、CVE-2018-1336、CVE-2018-8034、CVE-2018-11784、CVE-2019-0232	NA	4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvq11456	stcli cluster info コマンドは、UCSM VIP アドレスを提供する必要があります。現在、ucsm-host.com が表示されています	NA	3.5(2d)
CSCvq32530	HyperFlex アップグレードの検証が失敗しました。これは、クラスタが内部データベースに無関係な stNodes を持っているためです。	現在、回避策はありません。古いエントリは、HyperFlex の日々の操作には影響しません。	3.5(2a)
CSCvq42378	メンテナンスモードでない場合、すべてのドライブが HX Connect に表示され、予想どおりに更新されます。 メンテナンスモードでは、追加のドライブが HX Connect にスロット番号なしで表示されます。	NA	3.5(2a)
CSCvq61825	クラスタの再作成後に HX Connect で複製されたノード。	重複するノードをクリーンアップするには、TAC にお問い合わせください。	3.5 (2b)
CSCvq66245	Hyper-V での HyperFlex のインストールには、「stcli security whitelist」コマンドセットが含まれていません。	NA	4.0(1a)

リリース 4.0(1a) で未解決の問題

不具合 ID	症状	回避策	リリースで検出された障害
インストール、アップグレード、展開			

不具合 ID	症状	回避策	リリースで検出された障害
CSCvq39523	[Hyper-V] VIC 14xx の着信ノードでは、統合されたノードの展開が失敗します。		4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害

		1. 着信ノードの Windows/ハイパーバイザでジャンボ フレームを設定します。
		Get-NetAdapter storage-data-a | Get-NetAdapterAdvancedProperty -RegistryKeyword *JumboPacket | Set-NetAdapterAdvancedProperty -RegistryValue 9014
		Get-NetAdapter storage-data-b | Get-NetAdapterAdvancedProperty -RegistryKeyword *JumboPacket | Set-NetAdapterAdvancedProperty -RegistryValue 9014
		2. ジャンボ フレームをサポートするために、すべてのインターフェイスが正しく設定されていることを確認します。
		Get-NetAdapter *storage* | Get-NetAdapterAdvancedProperty | ? RegistryKeyword -match "jumbo" | ft -auto
		次のメッセージが表示される必要があります。
		`Name DisplayName DisplayValue RegistryKeyword RegistryValue`
		`---- ----------- ------------ ---------------- -------------`
		`vswitch-hx-storage-data Jumbo Packet 9014 Bytes *JumboPacket {9014}`
		`storage-data-b Jumbo Packet Bytes 9014 *JumboPacket {9014}`
		`storage-data-a Jumbo Packet Bytes 9014 *JumboPacket`	

不具合 ID	症状	回避策	リリースで検出された障害
		{9014} 3. 着信ノードまたは展開されているノードのみを再起動します。 4. インストーラで (以前にエラーがあった時点から) クラスタの展開を再試行します。	
CSCvp12241	2 個のノードの HyperFlex Edge クラスタが正常にフェールバックされず、正常に復帰しない可能性があります。Intersight への接続がまったく機能しない場合に、発生する場合があります (例: トランザクションの遅延が 100 ミリ秒を超える場合など)。	両方のノードがアップ状態で実行中であり、回避策を試行する前に回復する時間を与えていることを確認します (数時間)。回復を与えておらずフェールバックしている場合、両方のコントローラ VM (両方のノードで同時に実行することを推奨) で次のコマンドを実行して再起動します。**restart hxRoboController**.	4.0(1a)
CSCvp20102	ESXi HX クラスタ (通常またはストレッチまたは 2N robo) で VC が使用できない場合、データストアの作成/削除は失敗します。	DS 操作を実行する前に、VC が使用可能であることを確認します。	4.0(1a)
CSCvk23212	HX メンテナンス モードからホストを終了し、他のノードで storfs パニックが発生すると、緊急クラスタが HX 3.0 (1b) でシャットダウンします。	「Good」として見なされるドライブの取り外しと再挿入は避けてください。取り外され再装着した「Good」ドライブでテストを実行した場合は、詳細な手順について Cisco TAC にお問い合わせください。	3.0(1b) 3.5(1a)
CSCvm55176	Hyper-V のインストール中に後で制約付き委任を実行することを選択した場合、HX Connect UI での反映に長時間がかかることがあります。	AD ポリシーが有効になるまで、少なくとも 30 分間待機します。問題が解決しない場合は、メンテナンス モードを使用して 1 個ずつホストを再起動します。	3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvo88857	ユーザーが ISCSI インターフェイスをセットアップするオプションを選択すると、インストーラプロセスが失敗します。	インストール後に ISCSI インターフェイスを手動で追加します。	3.5(2a)
CSCvp20230	クラスタの無効状態が原因で、ストレッチクラスタのアップグレードがランダムに失敗します。	1. 次のコマンドを実行します。**stcli cluster upgrade --components hxdp --clean** 2. HX アップグレードを再度実行します。 3. 必要に応じて手順 1 および 2 を繰り返します。	3.5 (2b) 3.5(1a)
CSCvm53679	HX Hyper-V インストールが失敗し、`HXBootstrap.log` には次のメッセージが含まれています。 「`Active Directory Web` サービスが実行されているデフォルトサーバを見つけることができません。」	このエラーは、Windows がドメインコントローラを検出できなかったことを示します。HXInstaller の詳細入力にドメインコントローラの特定の IP を追加してください。	3.5(1a) 3.0(1e)
管理			

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp98910	2 ノードネットワーク パーティションの修復後、分離ノードのデータストアは 15 分間使用できません。	次の 2 つのオプションがあります。 A) ARP エントリがタイムアウトするまで 15 ～ 20 分間待機してから、データストアが再びマウントされるようになります。 B) ARP エントリを手動でリセットするには、次の手順を実行します。 1. 現在の eth1: 0 を確認します。HyperFlex コントローラ VM とノードの両方から IP/Mac への MAC アドレス。 コントローラ VM のシェルから「**ifconfig eth1:0**」を実行します。 2. データストアが使用できないノードで、次のコマンドを使用して、ESXi ARP キャッシュ内の上記の IP アドレスの MAC アドレス エントリを確認します。 「**esxcli network ip neighbor list**」 3. IP アドレスが誤った MAC アドレスに割り当てられている場合は、次に示すように ARP テーブルからエントリを消去します。 `esxcli network ip neighbor remove -a <IP_address> -v 4`	4.0(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvp21417	EMC RecoverPoint の導入は次のエラーで失敗します。「vRPA ビューでのリポジトリ デバイスの検出に失敗しました。」	3.5 (2b) または 4.0 I (1a) にアップグレードする場合は、RecoverPoint 機能を有効にすると、クラスタ内のノードHX メンテナンス モードで、ローリング ノードの実行が必要になる場合があります。クラスタが正常であり、1 個のノード障害 (3 ノードまたは 4 ノード クラスタの場合) と 2 個のノード障害 (5 以上のノード クラスタの場合) が許容されることを確認します。	3.5 (2b)
CSCvo89507	サポートされていないミクロン5200 ドライブを HX クラスタに追加した後、それらをサポートするリリースに HX をアップグレードすると、クラスタでリモートセキュリティが有効になっている場合 (コントローラ VM の連続リブートなどの特定のケースで)、ドライブがロックされる可能性があります。	システムからミクロン 5200 ドライブを取り外します。リリース 3.5 (2b) にアップグレードし、次にディスクの拡張ワークフローを追加します。	4.0(1a) 3.5 (2b)
CSCvn76916	HX データストアの使用率は、データストア上で VM の組み合わせを使用する場合よりも高くなります。	NA	3.5(1a)
CSCvo83276	VM のバックアップは、バックアップ VM のスナップショット中にオフになります。	スナップショットを再度取得します。	3.5(1a)

不具合 ID	症状	回避策	リリースで検出された障害
CSCvn11045	ノードを再起動すると、HX ノードはクラッシュし続けます。	1. インターフェイスがアップしているかどうか、およびループバックインターフェイスに ping を実行できるかどうかを確認します。 **ifconfig-aping 127.0.0.1** 2. ループバック インターフェイスを起動します: **ip link set lo up** 3. サービスが実行されていることを確認します。**status scvmclientstatus storfs** 4. 次のサービスを開始します。**scvmclientstart storfs**	3.5(1a) 3.0(1e)
CSCvp09978	クラスタ情報は、Smart call home が無効になっているにも関わらず、有効になっていることを示しています。	代わりに、 **stcli services sch show**コマンドを使用します。	3.5 (2b)

関連する問題

不具合 ID	症状	リリースで検出された障害	リリースで解決済み
CSCvq41985	組み込みのキックスタート ファイルを使用して CIMC にマウントされた ISO から ESXi 6.5 または6.7をインストールしようとすると、組み込み KS.CFG ファイルを読み取るときにインストールが失敗することがあります。ESXi インストーラでは、ポップアップ エラーが次の状態になります。 <path>/KS.CFG □□□□□□□□□□□□□□□□□□□□□	Cisco IMC 4.0 (1a)	オープン（Open）

関連資料

マニュアル	説明
設置前チェックリスト	設置作業を開始する前に**必要な**構成情報を収集するための、編集可能なファイルです。チェックリストに記入し、シスコアカウント チームにご提出ください。
VMware ESXi インストレーション ガイド	HyperFlex Systems の初期構成、および関連するポスト クラスタ設定タスクに関する詳細情報です。複数の HX クラスタの設定方法、HX クラスタの展開方法、混在した HX クラスタのセットアップ方法や、外部ストレージの接続方法についても説明しています。
ストレッチ クラスタ ガイド	HyperFlex ストレッチ クラスタのインストールと設定手順を提供し、ミッションクリティカルなワークロードにアクティブ-アクティブなディザスタ回避ソリューションを展開できるようになります。
Microsoft Hyper-V インストレーション ガイド	Microsoft Hyper-V に Cisco HyperFlex システムをインストールし、設定する方法について、インストールおよび設定手順を説明します。
エッジ導入ガイド	リモート、ブランチ オフィス（ROBO）、およびエッジ環境にハイパーコンバージェンスをもたらすように設計された、HyperFlex Edge の導入手順を説明します。
アドミニストレーション ガイド	クラスタ、暗号化、データの保護（複製とリカバリ）、ReadyClone、ネイティブ スナップショット、およびユーザ管理を管理および監視する方法について説明します。インターフェイスには、HX Connect、HX Data Platform プラグイン、および`stcli`コマンドが含まれます。
Hyper-V 管理のためのガイド	Hyper-V クラスタ、暗号化、データの保護（複製とリカバリ）、ReadyClone、Hyper-V チェックポイント、およびユーザ管理を管理および監視する方法について説明します。インターフェイスには、Cisco HyperFlex Systems、および `hxcli` コマンドが含まれます。
Kubernetes 管理ガイド	Kubernates の HyperFlex ストレージ インテグレーションに関する情報、HyperFlex Connect の Kubernates サポートに関する情報、Cisco のコンテナ プラットフォームおよび RedHat OpenShift コンテナ プラットフォームの両方に対して、HyperFlex FlexVolume ストレージ インテグレーションを設定する方法に関する手順を示します。

マニュアル	説明
Citrix ワークスペース アプライアンスの管理ガイド	Citrix ワークスペース、およびCitrix 仮想アプリとデスクトップサービスなどの関連する Citrix クラウド サブスクリプションを接続するための、HyperFlex システムのインストール、設定、および展開の手順を示します。Citrix 対応 HCI ワークスペース アプライアンス プログラムは、Citrix クラウドに接続する Microsoft Hyper-V で展開された Cisco HyperFlex システムを有効にします。
HyperFlex Intersight インストレーションガイド	クラウドから安全なインフラストラクチャ管理を提供するように設計された HyperFlex Intersight のインストール、設定、および導入手順を提供します。
アップグレード ガイド	Cisco HX Data Platform の既存のインストールのアップグレード方法、アップグレード ガイドライン、およびさまざまなアップグレード タスクに関する情報を提供します。
ネットワーク/外部ストレージ管理ガイド	HyperFlex Systems 固有のネットワークおよび外部ストレージ管理タスクに関する情報を提供します。
コマンド ライン インターフェイス（CLI）ガイド	HX Data Platform の `stcli` コマンドについての CLI リファレンス情報を提供します。
障害復旧の Cisco HyperFlex PowerShell Cmdlets	データ保護のために Cisco PowerShell Cisco HXPowerCLI cmdlets を使用する方法に関する情報を提供します。
REST API 入門ガイド REST API リファレンス	外部アプリケーションが Cisco HyperFlex の管理プレーンと直接対話できるようにする、REST API に関連する情報を提供します。
トラブルシューティング ガイド	設置、構成、 から への構成、および から への構成に関するトラブルシューティング ガイドです。さらにこのガイドでは、システム イベント、エラー、Smart Call Home、およびシスコ サポートに関する情報を提供します。
技術メモ	独立したナレッジ ベースからの記事を記載しています。
UCS Manager リリース 4.0 リリース ノート	推奨される FI/サーバ ファームウェアに関する情報を提供します。