

Cisco UCS Central リリース 2.0 のリリースノート

初版：2017年5月15日

最終更新：2020年3月4日

はじめに

Cisco UCS Central 2.0 は、拡大する Cisco ユニファイド コンピューティング システム (Cisco UCS) 環境向けにスケーラブルな管理ソリューションを提供します。Cisco UCS Central は、標準化、グローバルポリシー、およびグローバルIDプールを通して、単一の管理ポイントからの複数の Cisco UCS ドメインの管理を簡略化します。代わりに Cisco UCS Central では、世界中に分散する多数の個別 Cisco UCS クラシックおよびミニ管理ドメインを対象とした、グローバルレベルでの UCS ドメインの管理と監視に重点を置いています。

このマニュアルでは、Cisco UCS Central ソフトウェア リリース 2.0 のシステム要件、新機能、解決済みの警告、既知の警告、および未解決の警告と回避策について説明します。また、技術文書の公開後に入手可能になった情報も含まれています。

Cisco.com で利用可能なその他のマニュアルを参照して、Cisco UCS Central の最新情報を取得してください。

マニュアルの変更履歴

リリース	日付	説明
2.0(1a)	2017年5月15日	Cisco UCS Central リリース 2.0 (1a) のリリース ノートを作成しました。
	2017年6月5日	Cisco HyperFlex システムのサポートを追加しました。
2.0 (1b)	2017年8月18日	Cisco UCS Central リリース 2.0(1b) のリリース ノートを作成しました。
	2017年10月24日	リリース 2.0(1b) でサポートされている M5 サーバの BIOS トークンのサポートを更新しました。

リリース	日付	説明
2.0 (1c)	2017年11月15日	Cisco UCS Central リリース 2.0(1c) 向けリリース ノートを作成しました。
	2017年11月17日	サービス プロファイルのグローバル化のためにサポートされている Cisco UCS Manager のバージョンを更新しました。
2.0 (1d)	2018年3月21日	Cisco UCS Central リリース 2.0(1d) のリリース ノートを作成しました。
2.0 (1e)	2018年5月18日	Cisco UCS Central リリース 2.0(1e) のリリース ノートを作成しました。
2.0 (1f)	2018年8月14日	Cisco UCS Central リリース 2.0(1f) のリリース ノートを作成しました。
2.0 (1g)	2019年1月2日	Cisco UCS Central リリース 2.0 (1g) のリリース ノートを作成しました。
2.0 (1h)	2019年3月18日	Cisco UCS Central リリース 2.0 (1h) のリリース ノートを作成しました。
2.0(1i)	2019年5月29日	Cisco UCS Central リリース 2.0(1i) のリリース ノートを作成しました。
2.0 (1j)	2019年9月23日	Cisco UCS Central リリース 2.0 (1j) のリリース ノートを作成しました。

リリース	日付	説明
2.0 (1k)	2020 年 3 月 4 日	<p>Cisco UCS Central リリース 2.0 (1k) のリリース ノートを作成しました。</p> <p>2.0(1d) または 2.0(1e) からのアップグレードパスを追加しました。</p> <p>リリース 2.0(1k) でサポートされている M5 サーバの BIOS トークンのサポートを更新しました。</p>

UCS Central からの Cisco UCS ドメイン管理の重要なガイドライン

Cisco UCS Central から Cisco UCS ドメインを管理する場合は、次のガイドラインに従うことを推奨します。

- Cisco UCS ドメインを登録する際は、常に Cisco UCS Central の完全修飾ドメイン名 (FQDN) を使用することを推奨します。ドメインが FQDN で登録されていれば、Cisco UCS Central の IP アドレスに変更があっても、その変更はドメインには透過的です。
 - Cisco UCS ドメインが Cisco UCS Central IP アドレスに登録されている場合、Cisco UCS Central の IP アドレスの変更が Cisco UCS Central ではサポートされません。詳細については、『[Cisco UCS Central インストールおよびアップグレードガイド](#)』の「[Cisco UCS Central IP アドレスの変更](#)」の項を参照してください。
- Cisco UCS Central をアップグレードする前に、完全な状態のバックアップを実行し、VM のスナップショットを取得することをお勧めします。
- データセンターの移行や障害復旧のケースをサポートするために、Cisco UCS Central インスタンスを移行することができます。Cisco UCS Central インスタンスの移行の詳細については、『[Cisco UCS Central インストールおよびアップグレードガイド](#)』の「[Cisco UCS Central インスタンス移行](#)」の項を参照してください。
- 実稼働システムに登録された Cisco UCS ドメインの登録を解除すると、重大な影響を与えます。Cisco UCS Central から永久的に管理しないことを再度選択した場合を除き、Cisco UCS ドメインの登録を解除しないでください。Cisco UCS Central からの Cisco UCS ドメインの登録と登録解除の詳細については、『[Cisco UCS Central インストールおよびアップグレードガイド](#)』の「[Cisco UCS ドメインおよび Cisco UCS Central](#)」の項を参照してください。

Cisco UCS Central から登録済みの Cisco UCS ドメインの登録を解除する場合は、次のようにします。

- Cisco UCS Central から Cisco UCS ドメインのサービスプロファイル、ポリシー、およびその他の設定を管理することはできなくなります。

- すべてのグローバル サービス プロファイルとポリシーがローカルになり、ローカル エンティティとして機能し続けます。ドメインを再登録しても、サービスプロファイルおよびポリシーはローカルのままです。

**重要**

- Cisco UCS Central は、新規インストールのハイアベイラビリティ (HA) をサポートしていません。Cisco では、単一の仮想マシンのスタンドアロンモードで Cisco UCS Central をインストールし、ハイパーバイザのハイアベイラビリティ機能を活用することを推奨しています。
- Cisco UCS Central リリース 2.0(1d) または 2.0(1e) から 2.0(1k) へのアップグレードは、CSCvt12270 が原因で失敗する可能性があります。Cisco では、最初に Cisco UCS Central 2.0(1j) にアップグレードしてから 2.0(1k) にアップグレードすることを推奨しています。この問題の詳細については、「[リリース 2.0\(1k\) で未解決の問題](#)」を参照してください。

**注意**

Cisco では、本稼働システムに登録された Cisco UCS ドメインの登録を解除する場合、Cisco テクニカル サポートにご連絡いただくことを推奨しています。

[関連資料 \(32 ページ\)](#) の最新情報については、Cisco.com の Cisco UCS Central を参照してください。

システム要件

対応ブラウザ

Cisco UCS Central GUI にアクセスするには、ご使用のコンピュータが次の最小システム要件を満たしている必要があります。

- Windows
 - Internet Explorer 11 以上
 - Firefox 45.0.2 以降
 - Chrome 49 以降
- Linux RHEL
 - Firefox 45.0.2 以降
 - Chrome 49 以降

- MacOS
 - Firefox 45.0.2 以降
 - Chrome 49 以降
 - Safari 9.0.3 以降

サポートされるオペレーティング システム

リリース済みの ISO は以下でサポートされます。

- VMWare ESXi 5.x、および ESXi 6.x
- Microsoft Hyper-V Server 2012 R2、Microsoft Hyper-V Server 2016
- Red Hat Enterprise Linux 6.5、6.8、7.2、7.3、7.4 上の KVM ハイパーバイザ

リリース済みの OVA は VMWare ESXi 5.x および ESXi 6.x でサポートされます。

トランスポート層のセキュリティのサポート

TLS 1.1 および 1.2 のサポート

Cisco UCS Central 2.0 は、TLS 1.1 および TLS 1.2 HTTPS 接続をサポートしています。

Cisco HyperFlex システムのサポート

Cisco UCS Central は、サポートされているバージョンの Cisco UCS Manager を実行している Cisco UCS ファブリック インターコネクタに接続されている Cisco HyperFlex サーバ ノードのインベントリとモニタリングのみをサポートします。Cisco HX Data Platform インストーラ OVA は現在、すべての必要なポリシーとサービス プロファイルを Cisco UCS Manager API を使用してローカルに作成および管理しており、グローバルポリシーとサービス プロファイルをサポートしていません。Cisco UCS Central 2.0 のグローバル化機能は、Cisco HyperFlex システムではサポートされていません。Cisco HX Data Platform の一部であるアップグレード機能と手順が Cisco UCS Central で手動で作成されたカスタム グローバル設定で動作しないため、Cisco では Cisco HyperFlex の Cisco UCS Central でグローバル サービス プロファイルとポリシーを手動で設定しないことを推奨しています。

Cisco UCS Central リリース 2.0 での変更

Cisco UCS Central リリース 2.0 の新機能

Cisco UCS Central 2.0 は、このトピックのセクションに記載されている新機能をサポートしています。これらの機能の一部は、Cisco UCS Manager リリース 3.1(3) 以降と互換性があるように Cisco UCS Central で構築されています。適切なサポートされている Cisco UCS Manager のリリースについての詳細は、[機能サポート マトリクス \(12 ページ\)](#) を参照してください。

機能	機能
IOE コントローラのサポート	Cisco UCS S3260 ストレージサーバ (UCS-C3K-M4RAID) の IO エクспанダで 2 番目の RAID コントローラをサポートしています。
HBA コントローラのサポート	Cisco UCS S3260 ストレージサーバ (UCS S3260-DHBA) 上のデュアル HBA コントローラをサポートしています。
BIOS アセット タグ	サービス プロファイルには、サーバを固有に識別するためのアセット タグが表示されるようになりました。
サービス プロファイルのグローバル化	Cisco UCS Manager から Cisco UCS Central に ローカルサービスプロファイルをグローバル化して、レガシー ソフトウェア環境で Cisco UCS Central を展開し、使用することができます。
統合化されたサーバ診断	サーバ上のハードウェア コンポーネントの健全性を確認し、サーバ上のハードウェア サブシステム (メモリや CPU など) に負荷をかけ、運用するためのさまざまなテストを提供します。
軽量アップグレード/ホットパッチ	サービス パックバンドルを介して、インフラストラクチャおよびサーバ コンポーネントの Cisco UCS Manager ファームウェア セキュリティ アップデートを提供します。
物理サーバでの KVM IP の設定	インバンドおよびアウトバンド管理のために、物理サーバ上で KVM IP を設定できます。
SED 管理、KMIP サポート	データ暗号化の管理のために、自己暗号化ドライブ (SEDs) 向けセキュリティ ポリシーが導入されました。メディア暗号キーの暗号化に必要なセキュリティ キーは、ローカルで設定することも、KMIPサーバを使用してリモートで設定することもできます。
Smart SSD	SSD 健全性のモニタリングをサポートし、さまざまな SSD プロパティに関する統計情報と、各プロパティのしきい値の制限を提供します。

機能	機能
ユーザー定義 FC ゾーン	ストレージレイ間の単一のデータ レプリケーションソリューションを示すように、VMに必要なすべてのゾーン分割をグループ化するための FC ゾーン プロファイルを作成できます。
ファームウェアの自動インストールによるファブリック エバキュエーション	FI のアップグレード中にファブリック 退避の自動設定をサポートし、自動インストール時に再起動します。また、適切なフェールオーバー設定がファームウェア アップグレード用に設定されていることを確認します。
HTML5 KVM クライアントの起動	Cisco UCS Central GUI から HTML5 ベースの KVM クライアントを直接起動します。
新しいポリシー	Cisco UCS Central 2.0 では、次の新しいポリシーが導入されています。 <ul style="list-style-type: none"> • IGMP スヌーピングを使用したマルチキャスト • 電源同期ポリシー • 統計情報しきい値ポリシー • グラフィックス カード ポリシー • QoS システム クラス • ハードウェア変更検出ポリシー • ポート自動検出ポリシー • KMIP 認定ポリシー
サーバ再起動ログ	リセットした最後の 5 つの理由と、電力遷移の時刻とソースに加えて、サーバの再起動ログを表示します。
Cisco UCS Manager DirectView タブ	CIMC セッション、システム イベント ログ、VIF パス、統計情報、温度、電源、およびインストールされているファームウェアの詳細を表示するために、2.0 から [Cisco UCS Manager サーバの統計情報 (Cisco UCS Manager Server Statistics)] タブの DirectView を起動します。

機能	機能
UI の機能拡張	<p>次の UI 拡張機能が導入されています。</p> <ul style="list-style-type: none"> • オブジェクトの名前別に包括的な検索を有効にするためのスポットライト検索バー。上位 10 件の結果と候補のエントリが表示されます。 • タブを復元して、開いているタブを保存し、Cisco UCS Central に再度ログインしたときに同じセッションへの直接アクセスを有効にします。 • ウィジェットメニューバーの [お気に入り (Favorites)] ウィジェットを使用すると、ポリシーを作成または編集するときに頻繁に使用するコンポーネント、タブ、ダイアログを保存できます。 • [ポリシーの複製 (Clone Policies)] アイコンでは、新しい名前、親組織またはドメイングループ、必要に応じた説明でポリシーの詳細な複製を有効にし、新しいポリシーを作成することなく細かい編集を行うことができます。

リリース 2.0(1k) の動作変更

- Cisco UCS Central 2.0(1k) は、次のハードウェアをサポートしています。

高密度第 4 世代ファブリック インターコネクト : Cisco UCS 64108 ファブリック インターコネクトは、Cisco Unified Computing System の中核を成す製品であり、システムのネットワーク接続と管理機能の両方を提供します。Cisco UCS 64108 ファブリック インターコネクトは、96 個の 10/25 Gbps ポート、16 個の 10/25 Gbps ユニファイド ポート、および 12 個の 40/100 Gbps アップリンク ポートをサポートします。
- Cisco UCS Central 2.0(1k) は、Cisco UCS Manager リリース 4.1(1a) でサポートされている追加の BIOS トークンをサポートしています。BIOS トークン、デフォルト、および値のサポートされている完全な最新リストについては、『[UCS サーバ BIOS トークン](#)』ガイドを参照してください。

リリース 2.0(1j) の動作変更

- Cisco UCS Central では、100 ロケールがサポートされています。

リリース 2.0(1i) の動作変更

- Cisco UCS Central グローバル サービス プロファイルまたはサービス プロファイル テンプレートの初期電源状態を変更することはできません。最初の電源状態は、サービス プロファイルの関連付けの一部として Cisco UCS Manager にプッシュされません。ただし、以前と同様にサーバで通常の電源操作を実行できます。この動作の変更は、不具合 CSCvp40200 の修正として導入されました。Cisco UCS Central 2.0 (1i) で解決済みの問題の詳細については、[リリース 2.0\(1i\) の解決済みの問題 \(24 ページ\)](#) を参照してください。
- Cisco UCS Central 2.0(1i) は、Cisco UCS Manager リリース 4.0(4a) でサポートされている追加の BIOS トークンをサポートしています。BIOS トークン、デフォルト、および値のサポートされている完全な最新リストについては、『[UCS サーバ BIOS トークン](#)』ガイドを参照してください。
- Cisco.com から <https://ucshclserver.cloudapps.cisco.com/fetch/current.tar> に保存されているハードウェア互換性カタログをダウンロードできません。Cisco では、次のコマンドを実行して HCL カタログをダウンロードし、UI から Cisco UCS Central にインポートすることを推奨しています。



注目 コマンドを実行する前に、インターネットに接続していることを確認してください。

```
curl -k -f --connect-timeout 30 --dump-header "hcl_download_header" -o current.tar.gz
  https://ucshclserver.cloudapps.cisco.com/fetch/current.tar.gz -u
  CCUsername:CCOPassword'
```

リリース 2.0(1g) の動作変更

- Cisco UCS Central 2.0 (1g) は、Cisco UCS C 480 ML M5 サーバをサポートしています。
- Cisco UCS Central では、新規インストールのハイ アベイラビリティはサポートされていません。

リリース 2.0(1f) の動作変更

Cisco UCS Central 2.0(1f) は、次のハードウェアをサポートしています。

- Cisco UCS 6454 ファブリック インターコネクタ
- Cisco UCS M5 サーバでの Cisco UCS VIC 1400 シリーズ アダプタ カード
- S3260 ストレージ サーバを搭載した新しい SIOC および Cisco UCS VIC 1400 アダプタ カード

Cisco UCS Central 2.0 (1f) は、Cisco UCS Manager リリース 4.0(1a) の BIOS トークンをサポートしています。BIOS トークン、デフォルト、および値のサポートされている完全な最新リストについては、『[Cisco UCS M5 サーバ BIOS トークン](#)』ガイドを参照してください。



(注) Cisco UCS Central は、Cisco UCS C-125 M5 サーバをサポートしていません。

リリース 2.0(1d) の動作変更

Cisco UCS Central 2.0(1d) は、Cisco UCS Manager リリース 3.2(3) でサポートされている Cisco UCS S3260M5 サーバの追加 BIOS トークンをサポートしています。BIOS トークン、デフォルト、および値のサポートされている完全な最新リストについては、『[Cisco UCS M5 サーバ BIOS トークン](#)』ガイドに記載されているリリース 3.2(2) の M5 サーバ BIOS トークンを参照してください。

次の表では、M5 サーバ モデルの BIOS トークンをサポートしている Cisco UCS Central および Cisco UCS Manager リリースを一覧にしています。

表 1: サポートされている M5 サーバ モデル

Cisco UCS Central リリース	Cisco UCS Manager リリース	サーバ モデル
2.0 (1d)	3.2(3)	S3260 M5 B200 M5 B480 M5 C220 M5 C240 M5 C480 M5

リリース 2.0(1c) の動作変更

Cisco UCS Central 2.0 (1c) は、Cisco UCS Manager リリース 3.2(2) でサポートされている Cisco UCS B480M5 および C480M5 サーバの追加 BIOS トークンをサポートしています。BIOS トークン、デフォルト、および値のサポートされている完全な最新リストについては、『[Cisco UCS M5 サーバ BIOS トークン](#)』ガイドに記載されているリリース 3.2(2) の M5 サーバ BIOS トークンを参照してください。

下の表では、M5 サーバ モデルの BIOS トークンをサポートしている Cisco UCS Central および Cisco UCS Manager リリースを一覧にしています。

表 2: サポートされている M5 サーバ モデル

Cisco UCS Central リリース	Cisco UCS Manager リリース	サーバ モデル
2.0 (1c)	3.2(2)	B200 M5 B480 M5 C220 M5 C240 M5 C480 M5

リリース 2.0(1b) の動作変更

Cisco UCS Central 2.0(1b) は、Cisco UCS Manager リリース 3.2(1) でサポートされている Cisco UCS B200M5、C220M5 および C240M5 サーバの新しい BIOS トークンのサポートを拡張します。BIOS トークン、デフォルト、および値のサポートされている完全な最新リストについては、『[Cisco UCS M5 サーバ BIOS トークン](#)』ガイドに記載されているリリース 3.2(2) の M5 サーバ BIOS トークンを参照してください。

BIOS ポリシーの **[BIOS 設定変更で再起動 (Reboot on BIOS Settings Change)]** プロパティは、Cisco UCS Central 2.0 (1b) へのアップグレード後、デフォルトで無効に設定されています。ベストプラクティスとして、このデフォルト設定を保持することを推奨します。

下の表では、M5 サーバモデルの BIOS トークンをサポートしている Cisco UCS Central および Cisco UCS Manager リリースを一覧にしています。

表 3: サポートされている M5 サーバ モデル

Cisco UCS Central リリース	Cisco UCS Manager リリース	サーバ モデル
2.0 (1b)	3.2(1)	B200 M5 C220 M5 C240 M5

リリース 2.0 の動作変更

廃止のお知らせ

- Cisco UCS Central Flex ベースの UI が含まれなくなりました。HTML5 UI は、使用可能な唯一のグラフィカル インターフェイスです。
- 統計情報管理機能は廃止され、Cisco UCS Central ではサポートされなくなりました。
- 2017 年 3 月 3 日以降、Cisco UCS Central バージョン 1.4 以前では更新されたファームウェア イメージリストを Cisco.com から取得できなくなります。Cisco UCS Central バージョン 1.4 以前を実行している場合は、手動で Cisco.com からファームウェア イメージを直接ダ

ウンロードして、Cisco UCS Central にインポートできます。引き続き、使用可能なイメージデータを Cisco UCS Central が Cisco.com から取得して、ファームウェア イメージを [イメージ ライブラリ (Image Library)] に配置するため、Cisco UCS Central リリース 1.5 以降にアップグレードすることをお勧めします。

機能サポート

設計に基づく動作の変更

- スポットライト検索バーは検索バーを置き換え、プロファイル、ポリシー、プール、VLAN/VSAN、テンプレート、ドメイン、組織、ドメイングループなどを名前、説明、およびラベルを検索できます。スポットライトでは、入力に応じて候補とともに検索ワールドが自動入力され、入力した用語と一致する上位 10 件の候補が表示されます。
- サイドバーのナビゲーションメニューのアイコンを使用すると、Cisco UCS Central のすべてのオブジェクトへの直接的かつ簡単なアクセスが可能になります。テーブルの参照、組織のナビゲーション、ドメイングループのナビゲーションがサイドバーのナビゲーションの一部になりました。
- 組織のツリービューから、その組織のプロファイル、テンプレート、プール、ポリシー、および許可された VLAN に直接移動することができます。選択した組織内の対応するタブが強調表示され、これらのオブジェクトをクリックすると開きます。
- Cisco UCS Central 2.0 では、Cisco UCS Central GUI およびコマンドラインから、サービスプロファイル、ドメイングループ、組織、サービスプロファイルテンプレートなどの重要なオブジェクトを削除することができません。Cisco UCS Central からこれらの項目を削除しようとする、潜在的な影響があるエラーメッセージが表示されます。
- サービスプロファイルを作成する前に、グローバルサービスプロファイルテンプレートを作成する必要があります。
- vNIC および vHBA の配置はインターフェイス配置と呼ばれるようになりました。
- 登録ポリシーはドメイングループ資格ポリシーと呼ばれるようになりました。
- ID 範囲資格ポリシーは ID 範囲アクセスコントロールポリシーと呼ばれるようになりました。
- ID 範囲アクセスコントロールポリシー用として認定された IP アドレスは存在しません。
- Cisco UCS Central では、設定のエクスポート (all-config) オプションとバックアップ (full-state) オプションのみが使用されます。論理設定やシステム設定などの他のバックアップタイプはサポートされません。

機能サポートマトリクス

次のテーブルに、Cisco UCS Central および Cisco UCS Manager の互換性のあるバージョンを示します。

Cisco UCS Central	サポートされる Cisco UCS Manager のバージョン
2.0 (1k)	2.1、2.2、3.0、3.1、3.2、4.0、4.1 最大 4.1 (1)
2.0 (1j)	2.1、2.2、3.0、3.1、3.2、および 4.0 最大 4.0 (4)
2.0 (1i)	2.1、2.2、3.0、3.1、3.2、および 4.0 最大 4.0 (4)
2.0 (1h)	2.1、2.2、3.0、3.1、3.2、および 4.0 最大 4.0 (2)
2.0 (1g)	2.1、2.2、3.0、3.1、3.2、および 4.0 最大 4.0 (2)
2.0 (1f)	2.1、2.2、3.0、3.1、3.2、および 4.0(1)
2.0 (1e)	2.1、2.2、3.0、3.1、および 3.2
2.0 (1d)	2.1、2.2、3.0、3.1、および 3.2
2.0 (1c)	2.1、2.2、3.0、3.1、および 3.2 最大 3.2(2)
2.0 (1b)	2.1、2.2、3.0、3.1、および 3.2(1)
2.0(1a)	2.1、2.2、3.0、および 3.1
1.5	2.1、2.2、3.0、3.1 および 3.1(2)
1.4	2.1、2.2、最大 2.2 (8)、3.0、3.1、最大 3.1
1.3	2.1、2.2、最大 2.2

次の表に、Cisco UCS Central の特定の機能と、それらの機能がサポートされる Cisco UCS Manager のリリースバージョンのリストを示します。



(注) 一部の機能は、今後の Cisco UCS Manager のリリースとの互換性を確保するために Cisco UCS Central で構築されています。

リリース 2.0 の機能サポート

Cisco UCS Central の機能	サポートされ る Cisco UCS Central のバー ジョン	サポートされる Cisco UCS Manager のバージョン			
		2.1	2.2	3.0	3.1/3.2/4.0
Cisco UCS S3260 ストレージサー バ (UCS-C3K-M4RAID) の IO エクスパン ダで 2 番目の RAID コントロー ラをサポートして います。	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
Cisco UCS S3260 ストレージサー バ (UCS S3260-DHBA) 上 のデュアル HBA コントローラをサ ポートしていま す。	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
デュアル SIOC の サポート	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
サービス プロ ファイルのグロー バル化	2.0(1a)	非対応	2.2 (8f)	No	3.1(2) 以降
BIOS Asset Tag	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
ホット パッチ/軽 量アップグレード	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
ユーザー定義ゾー ンプロファイル	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
統合化されたサー バ診断	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
SED セキュリティ ポリシー、Smart SSD、および KMIP のサポート	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降

Cisco UCS Central の機能	サポートされ る Cisco UCS Central のバー ジョン	サポートされる Cisco UCS Manager のバージョン			
		2.1	2.2	3.0	3.1/3.2/4.0
FI サーバポート の自動設定	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
物理サーバでの KVM IP の設定	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
ファームウェアの 自動インストール によるファブリック エバキュエー ション	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
ダイレクトファ ブリックイン ターコネクタのエ バキュエーション	2.0(1a)	No	2.2(4) 以降	No	3.1(1) 以降
Launch HTML5 KVM Client	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
マルチキャスト ポリシー	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
電源同期ポリシー	2.0(1a)	非対応	2.2(8)	No	3.1(2) 以降
統計情報しきい値 ポリシー	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
グラフィックス カードポリシー	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
QoS システムク ラス	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
ハードウェア変更 検出ポリシー	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
ポート自動検出ポ リシー	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
KMIP 認定ポリ シー	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降
サーバ再起動ログ	2.0(1a)	非対応	非対応	非対応	3.1 (3) 以降

Cisco UCS Central の機能	サポートされ る Cisco UCS Central のバー ジョン	サポートされる Cisco UCS Manager のバージョン			
		2.1	2.2	3.0	3.1/3.2/4.0
停止したラック サーバ、シャー シ、FEX の削除	2.0(1a)	あり	あり	非対応	3.1(1) 以降
VLAN Group	2.0 (1b)	非対応	非対応	非対応	3.1(2) 以降

リリース 1.5 の機能サポート

Cisco UCS Central の機能	サポートされ る Cisco UCS Central のバー ジョン	サポートされる Cisco UCS Manager のバージョン			
		2.1	2.2	3.0	3.1
Cisco UCS S3260 ストレージ サー バサポート	1.5(1a)	非対応	非対応	非対応	3.1(2) 以降
vNIC/vHBA ペア リング	1.5(1a)	非対応	2.2(7) 以降	No	3.1(2) 以降
トラフィック モ ニタリング	1.5(1a)	非対応	2.2(7) 以降	非対応	3.1(1) 以降
UUID 同期	1.5(1a)	非対応	2.2(7) 以降	No	3.1(2) 以降
PCI 用の管理ホス トポートの配置	1.5(1a)	非対応	非対応	非対応	3.1(1e) 以降
160 の LDAP グ ループ マッピン グのサポート	1.5(1a)	No	2.2(8) 以降	No	3.1(2) 以降

リリース 1.4 の機能サポート

Cisco UCS Central の機能	サポートさ れる Cisco UCS Central のバー ジョン	サポートされる Cisco UCS Manager のバージョン				
		2.1	2.2	2.5	3.0	3.1
ポート設定	1.4(1a)	No	2.2(7) 以降	非対応	非対応	3.1(1) 以降

Cisco UCS Central の機能	サポートされる Cisco UCS Central のバージョン	サポートされる Cisco UCS Manager のバージョン				
		2.1	2.2	2.5	3.0	3.1
高度なローカルストレージ設定	1.4(1a)	No	2.2(7)以降	2.5(1)以降	No	3.1(1)以降
ブートポリシー内の複数の LUN	1.4(1a)	No	2.2(7)以降	2.5(1)以降	No	3.1(1)以降
一貫したデバイスの命名	1.4(1a)	No	2.2(4)以降	2.5(1)以降	3.0(1)以降	3.1(1)以降
ダイレクトアタッチドストレージ/FCゾーン分割	1.4(1a)	No	2.2(7)以降	非対応	非対応	3.1(1)以降
高度なホストファームウェアパック	1.4(1a)	No	2.2(6)以降	非対応	非対応	3.1(1)以降
usNIC 接続ポリシー	1.4(1a)	No	2.2(6)以降	非対応	非対応	3.1(1)以降
VMQ 接続ポリシー	1.4(1a)	No	2.2(6)以降	非対応	非対応	3.1(1)以降
装置ポリシー	1.4(1a)	No	2.2(7)以降	非対応	非対応	3.1(1)以降
次のリブート時のメンテナンスポリシー	1.4(1a)	非対応	非対応	非対応	非対応	3.1(1)以降

リリース 1.3 以前の機能サポート

Cisco UCS Central の機能	サポートされる Cisco UCS Central のバージョン	サポートされる Cisco UCS Manager のバージョン				
		2.1	2.2	2.5	3.0	3.1
マルチバージョン管理のサポートとサポートされる Cisco UCS Manager 機能の表示	1.1(2a)	No	2.2(1b) 以降	2.5(1a) 以降	3.0(1c) 以降	3.1(1a) 以降
ポリシー/ポリシー コンポーネントおよびリソースのインポート		No	2.2(1b) 以降	2.5(1a) 以降	3.0(1c) 以降	3.1(1a) 以降
バックアップイメージファイル用のリモートロケーションの指定		No	2.2(2b) 以降	2.5(1a) 以降	3.0(1c) 以降	3.1(1a) 以降
サードパーティ証明書		No	2.2(2c) 以降	2.5(1a) 以降	3.0(1c) 以降	3.1(1a) 以降
IPv6 インバンド管理サポート		No	2.2(2c) 以降	2.5(1a) 以降	3.0(1c) 以降	3.1(1a) 以降
再接続への予測影響		1.2(1a)	No	2.2(3a) 以降	2.5(1a) 以降	3.0(1c) 以降
高精度のブート順制御	No		2.2(1b) 以降	2.5(1a) 以降	3.0(1c) 以降	3.1(1a) 以降
スクリプト可能な vMedia	1.2(1e) 以降	No	2.2(2c) 以降	2.5(1a) 以降	3.0(2c) 以降	3.1(1a) 以降



- (注)
- ポリシー/ポリシー コンポーネントまたはリソースの検索は、Cisco UCS Manager のリリース 2.1(2x) と 2.1(3x) でサポートされます。ポリシーをインポートするには、Cisco UCS Manager のリリース 2.2(1b) 以降が必要です。
 - Precision Boot Order Control については、ブレードサーバが CIMC バージョン 2.2(1b) 以降でなければなりません。

アップグレードパス

Cisco UCS Central をリリース 2.0 にアップグレードするには、次のいずれかのリリースを使用します。

- 1.4 から 2.0 へ
- 1.5 から 2.0 へ
- Cisco UCS Central をリリース 2.0(1d) または 2.0(1e) から 2.0(1k) にアップグレードする場合は、最初にリリース 2.0(1j) にアップグレードし、次に 2.0(1k) にアップグレードする必要があります。



- (注) Cisco UCS Central の以前のリリースへのアップグレード方法についての詳細は、『[該当するリリースのインストールとアップグレードガイド](#)』を参照してください。

既知の制限事項と動作

特に記載されていない場合、次の既知の制限事項と動作があります。

不具合 ID	症状	回避策
CSCuy37428 CSCuv32055	<p>インストール直後に Cisco UCS ドメインを登録すると、次のいずれかの問題が表示されることがあります。</p> <ul style="list-style-type: none"> • RHEL 7.2 KVM に Cisco UCS Central をインストールした後、ドメインの登録が失敗します。 • ISO イメージを使用して VMware に Cisco UCS Central をインストールすると、Cisco UCS Manager と Cisco UCS Central 間の時間同期の問題が原因でドメイン登録が失敗することがあります。 	<p>この問題が発生した場合は、次のコマンドを使用して Cisco UCS Central の CLI から手動で証明書を再生成します。</p> <pre># connect policy-mgr # scope org # scope device-profile # scope security # scope keyring default # set regenerate yes # commit-buffer</pre>

不具合 ID	症状	回避策
<p>CSCux75985 CSCuy07572</p>	<p>ホスト ファームウェア パッケージ ポリシーからのコンポーネントの除外は、Cisco UCS Manager リリース2.2.7以降でサポートされています。コンポーネントを除外する場合、次の点に注意する必要があります。</p> <ul style="list-style-type: none"> • グローバルデフォルトホストファームウェアパッケージポリシーにはすべてのコンポーネントが含まれていますが、新しいカスタムホストファームウェアパッケージポリシーを作成すると、ローカルディスクコンポーネントが自動的に除外されます。 • バージョン 1.3 以前の Cisco UCS Central で作成されたホストファームウェアパッケージポリシーでは、コンポーネントの除外はサポートされません。これらのポリシーは、Cisco UCS Central リリース 1.5 にアップグレードしたときに変更されることはありません。 • 除外コンポーネント（デフォルトで除外されるローカルディスクコンポーネントを含む）を使用して独自のホストファームウェアパッケージポリシーを作成する場合、バージョン 2.2.7 より前の Cisco UCS Manager を実行しているサーバに関連付けられているサービスプロファイルに、そのホストファームウェアパッケージポリシーを含めることはできません。含めようとする、サービスプロファイルの関連付けの際に次のエラーメッセージが表示されます。 <p>UCSドメインに、このサービスプロファイルに適合するサーバ機能がありません。</p>	<p>除外されたコンポーネントを含むカスタムホストファームウェアパッケージポリシーで問題が発生した場合は、ホストファームウェアパッケージポリシーで除外されたすべてのコンポーネントを削除するか、Cisco UCS Manager のバージョンをリリース 2.2.7以降にアップグレードすることができます。</p>

セキュリティ修正

次のセキュリティ修正が解決されています。

リリース	不具合 ID	CVE ID	症状
2.0 (1k)	CSCvq70837	CVE-2017-1000486	Cisco UCS Central の Primefaces 脆弱性に対処し、修正しています。
2.0 (1j)	CSCvp38294	CVE-2015-0228、 CVE-2015-0253、 CVE-2015-3183、 CVE-2015-3185、 CVE-2016-0736、 CVE-2016-2161、 CVE-2016-5387、 CVE-2016-8740、 CVE-2016-8743、 CVE-2017-15710、 CVE-2017-15715、 CVE-2017-3167、 CVE-2017-3169、 CVE-2017-7659、 CVE-2017-7668、 CVE-2017-7679、 CVE-2018-0113、 CVE-2018-1283、 CVE-2018-1301、 CVE-2018-1302、 CVE-2018-1303、 CVE-2018-1312、 CVE-2018-1333	Cisco UCS Central の Apache 脆弱性に対処し、修正しています。
2.0 (1h)	CSCm91751	CVE-2016-2107	Cisco UCS Central の Open SSL Oracle パディングの脆弱性に対処し、修正しました。

リリース	不具合 ID	CVE ID	症状
2.0 (1f)	CSCvh74209	CVE-2015-5600、 CVE-2015-6563、 CVE-2015-6564、 CVE-2016-10009、 CVE-2016-10010、 CVE-2016-10011、 CVE-2016-10012、 CVE-2016-8858、 CVE-2016-3115、 CVE-2007-6750	Cisco UCS Central の Open SSH および Apache HTTP サーバ脆弱性に対処し、修正しました。
2.0 (1d)	CSCvg47507	CVE-2017-1000100、 CVE-2017-1000254、 CVE-2017-1000257、 CVE-2017-7407	複数の curl 脆弱性に対処しました。
	CSCvf85637	脆弱な SSH 暗号 Cisco UCS Central	Cisco UCS Central は、すべてのバージョンの脆弱な SSH 暗号を無効にしました。
	CSCvh62085	Spectre および Meltdown の脆弱性	Spectre と Meltdown に関連する脆弱性に対処し、修正しました。
2.0 (1c)	CSCvf71978	Cisco UCS Central クロスサイトスクリプティングの脆弱性	Cisco UCS Central のクロスサイトスクリプティングの脆弱性に対処しました。
	CSCvf71986	Cisco UCS Central セッション修正の脆弱性	Cisco UCS Central のセッション修正の脆弱性に対処しました。
	CSCvf85660	Cisco UCS Central Apache の弱い暗号の脆弱性	Cisco UCS Central は、デフォルトの署名付き証明書の SHA2 をサポートします。

リリース	不具合 ID	CVE ID	症状
2.0(1a)	CSCvb48578	CVE-2016-6304 CVE-2016-6305 CVE-2016-2183 CVE-2016-6303 CVE-2016-6302 CVE-2016-2182 CVE-2016-2180 CVE-2016-2177 CVE-2016-2178 CVE-2016-2179 CVE-2016-2181 CVE-2016-6306 CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052	OpenSSL および TLS プロトコルの脆弱性に対処しました。
	CSCvc90364	CVE-2016-0736、 CVE-2016-2161、 CVE-2016-5387、 CVE-2016-8740、 CVE-2016-8743	リモート web サーバの脆弱性に対処しました。
	CSCvb85545	CVE-2016-5195	DIRTY CoW の脆弱性に対処しました。
	CSCvc23477 CSCvd72180	NTP 2016 年 11 月および 2017 年 3 月の Cisco UCS Central	NTP サーバの脆弱性に対処しました。

リリース 2.0(1k) の解決済みの問題

次の警告は Cisco UCS Central リリース 3.0(1jk) で解決されました。

リリース	説明
CSCvr02845	Cisco UCS Central Cisco UCS 6454 および 64108 ファブリック インターコネクタのファームウェアバンドルを正常にダウンロードできるようになりました。
CSCvr09400	Cisco UCS 6454 ポート 49-54 は、Cisco UCS Central からネットワーク アップリンクまたは FCoE アップリンク ポートとして設定できるようになりました。
CSCvr56397	ディスク グループ ポリシーは、Cisco UCS Central から UCS HWRAID の RAID1 を設定するために、ディスク スロット ID で 253 および 254 の値をサポートしています。

リリース 2.0(1j) で解決済みの問題

次の警告は Cisco UCS Central リリース 2.0(1j) で解決されました。

リリース	説明
CSCvp76562	Cisco UCS Central で 4GFI のインフラストラクチャ ファームウェア アップグレードプロファイルを作成できるようになりました。インフラストラクチャのアップグレードは正常に完了することができます。
CSCvp47201	ダウンロードしたインフラストラクチャ ファームウェア パッケージは、プラットフォームバンドル間の名前の競合を避けるために固有の名前が付けられています。Cisco UCS Central のインフラストラクチャ ファームウェア アップグレードプロセスによって、適切なプラットフォームに基づいてイメージが選択されるようになりました。
CSCvq94753	Cisco UCS Central で SCP/SFTP を使用した復元は固定されています。

リリース 2.0(1i) の解決済みの問題

次の警告は Cisco UCS Central リリース 2.0(1i) で解決されました。

リリース	説明
CSCvo21755	Cisco UCS Central SNMP ポーリングを使用したプロセス間でのメモリ使用率が高くなりません。
CSCvp13960	Cisco UCS Central 2.0 (x) では、サーバプールと vmedia ポリシーをグローバル サービス プロファイルに同時に適用できます。
CSCvp21297	Cisco UCS Central 2.0 (1d) および 2.0 (1h) の VLAN グループに追加された VLAN は、Cisco UCS Manager にプッシュされたときに削除されなくなります。
CSCvp40200	Cisco UCS Central 2.0 に関連付けられているサーバは、 hard-reset によって予期せずトリガされることはありません。

リリース 2.0(1h) の解決済みの問題

次の警告は Cisco UCS Central リリース 2.0(1h) で解決されました。

リリース	説明
CSCvm81056	VLAN グループは、新しい VLAN が既存の VLAN グループに追加された場合、または Cisco UCS Central 2.0(1d) を使用して vNIC テンプレートに同じ VLAN が追加された場合に、アップリンク ポート チャネルから削除されなくなりました。

リリース	説明
CSCvo45661	FCOE ID 4011 および 4012 を持つ VSAN を、次の Cisco UCS Central 2.0 (1g) から作成できるようになりました。 <ul style="list-style-type: none"> • Cisco UCS Manager 4.0(2b) を実行している Cisco UCS 6332 ファブリック インターコネクト • Cisco UCS Manager 3.2(3i) を実行している Cisco UCS 6248 ファブリック インターコネクト
CSCvo62782	Cisco UCS Central GUI を使用した Cisco.com クレデンシャルの設定に失敗することはなくなります。これで、クレデンシャルを保存できるようになります。

リリース 2.0(1g) の解決済みの問題

次の警告は Cisco UCS Central リリース 2.0(1g) で解決されました。

リリース	説明
CSCvm81311	動的および静的 vNICs の Cisco UCS Central によってパスされた Adminvcon 値が一致しないため、Cisco UCS Manager DATA Management Engine (DME) はクラッシュしません。
CSCvd51108	Cisco UCS Central 永続ポーリング時の SNMP メモリの使用量が増加しているため、仮想マシンが応答しなくなりました。

リリース 2.0(1f) の解決済みの問題

次の問題は Cisco UCS Central リリース 2.0(1f) で解決されました。

リリース	説明
CSCvk12385	svc_server_DME ログでは、Cisco UCS Manager の障害によるメモリ リークは検出されなくなりました。
CSCvi75816	関連付けられていないグローバル サービス プロファイル (GSP) で、Cisco UCS ドメインが新しいドメイングループに移動するのを防ぐことができなくなりました。
CSCvi85023	障害 F1000035 (fltStorageItemCapacityWarning : 90% を超える/boot パーティションのディスク使用率) が、以前のバージョンから Cisco UCS Central 2.0 (1d) へのアップグレード中に表示されなくなりました。
CSCvi86491	Cisco UCS Central でサービス プロファイルの名前を変更すると、設定が元のテンプレート設定に戻ります。

リリース	説明
CSCvj12410	M.2 コントローラの UEFI ブートパラメータは、Cisco UCS Central で使用できるようになりました。
CSCvk06781	非ルート ドメイン グループの VLAN ポート数の最適化を無効にするオプションが、Cisco UCS Central で使用できるようになりました。
CSCvk38338	QOS システム クラス ポリシーが適用されている場合、障害 F14533382 は発生しなくなります。
CSCvd39239	Cisco UCS Central ドメイン登録に関連する古い/孤立した障害を消去できるようになりました。

リリース 2.0(1e) の解決済みの問題

次の問題は Cisco UCS Central リリース 2.0(1e) で解決されました。

リリース	説明
CSCvj44960	Cisco UCS Central インバンド プロファイルが UCS ドメイン用に設定され、ドメイン FI が再起動すると、サーバが再起動することはなくなりました。

リリース 2.0(1d) の解決済みの問題

次の警告は Cisco UCS Central リリース 2.0(1d) で解決されました。

不具合 ID	症状
CSCvg81832	Cisco UCS Central Cisco UCS C シリーズ ラック サーバの HTML5 KVM を起動します。
CSCvh05008	Cisco UCS Central GUI から ドメイン グループの下に IP プールを作成できるようになりました。
CSCvh11135	Cisco UCS Central がハングしなくなり、大規模な展開で正常に機能します。
CSCvg91479	Cisco UCS Central でのスポットライト検索は、複数のロケールを持つユーザーに対して機能するようになりました。
CSCvh88028	CLI を使用する LDAP ユーザーは、ログイン中にパスワードの有効期限エラーを取得しません。
CSCvi32682	UCS ドメインで Cisco UCS Central サブスクリプションをアクティブ化した場合の影響の予測は、タイムアウトになりません。

不具合 ID	症状
CSCvi05444	Cisco UCS Central のスポットライトの検索では、サービスプロファイルの適切な所有権が表示されます。

リリース 2.0(1c) の解決済みの問題

次の問題は Cisco UCS Central リリース 2.0(1c) で解決されました。

不具合 ID	症状
CSCvf37185	Cisco UCS Central SNMP Managed Information Base (MIB) ライブラリは、Cisco UCS Central 2.0 でロードされ、Cisco UCS Central 固有 MIB の snmpwalk が失敗しません。
CSCve51309	[ドメイン設定 (Domain Settings)] で [設定を再適用 (Reapply Configuration)] を選択すると、サーバのアウトバンド IP が割り当てられるようになりました。
CSCve88234	Cisco UCS Central スポットライト検索で、ローカルサービスプロファイルの結果が表示されるようになりました。
CSCvg48615	Cisco UCS Central では、Cisco UCS Manager リリース 3.2(2b) でサポートされる BIOS トークンをさらにサポートしています。
CSCvf64818	Call home モニタリングの一部である Call Home アラートは、Cisco UCS Central リリース 1.5 または 2.0 を介して無効にした後、有効ステータスにとどまることがありません。
CSCvf83421	VLAN の変更後、Cisco UCS Central HTML GUI の[影響予測 0] で、[サーバの再起動が必要 (Server needs reboot)] ステータスが表示されません。
CSCvf84627	Cisco UCS Central ドメインプロファイルでインバンド KVM IP を使用しているときに、障害 F11000491 と F10017451 が表示されなくなります。
CSCvf57811	Cisco UCS Central 1.5 (1b) のグローバル サービス プロファイルが、ブレードサーバまたはラックサーバからの関連付けが解除された後に、[非グループ化 (Ungrouped)] 状態に移行しません。
CSCvg11782	サーバプールにラックサーバが存在する場合、Cisco UCS Central 2.0 (1a) でサービスプロファイルのグローバル化が失敗します。
CSCve31096	サービスプロファイルのグローバル化は、VLAN の権限の問題により、Cisco UCS Central 2.0 (1a) で失敗しました。

リリース 2.0(1b) の解決済みの問題

Cisco UCS Central リリース 2.0(1b) では、次の問題が解決済みです。

不具合 ID	症状
CSCvf22068	[ユーザー ラベル (User Label)] オプションは、Cisco UCS CENTRAL HTML5 GUI で、テンプレートの更新から取得したグローバル サービス プロファイルで使用できるようになりました。
CSCvf16476	グローバル サービス プロファイルから KVM コンソールを起動すると、仮想メディアをアクティブ化できるようになりました。
CSCve25720	VLAN グループを使用すると、Cisco UCS Manager で VLAN メンバシップが更新されるようになりました。
CSCve39559	グローバル シャーシファームウェア パックでストレージ コントローラが除外コンポーネントとして選択されている場合、グローバル シャーシ プロファイルの関連付けは失敗しません。
CSCve70783	Cisco UCS Central 内の任意のファイルに、認証されたローカル ユーザーがアクセスできません。

リリース 2.0 で解決済みの問題

Cisco UCS Central リリース 2.0(1a) では、次の問題が解決済みです。

不具合 ID	症状
CSCva84992	無効なクッキーが原因で発生した Httpd コアが、Cisco UCS Central (1a) で断続的に発生しなくなりました。
CSCvb02359	SNMPD は、Cisco UCS Central 1.3 またはそれ以前のバージョンからバージョン 1.4 以降へのアップグレード後に定期的にクラッシュすることはありません。この問題は、アップグレード後にログファイルがいっぱいになったために発生しました。
CSCvb05938	UCS Central の証明書要求によって、組織 (O) および組織単位 (OU) 名フィールドが正しく処理されるようになりました。
CSCvb26696	ポリシー参照関連の障害は、Cisco UCS Central Resource Manager でクリーンアップされるようになりました。
CSCvb38828	すべての Call Home 設定が Cisco UCS Central のルートからプッシュされるようになりました。ドメイングループで変更した後、ルート設定に戻ることができます。
CSCvb41775	VLAN を削除しても、Cisco UCS Central リリース 1.4 (a) からの古い VLAN エントリは存在しなくなりました。

不具合 ID	症状
CSCvb46833	中断された Cisco UCS ドメインは、Cisco UCS Central バージョン 1.3 (1a) から 1.5 (1a) へのアップグレード後に再認識され、その状態から移行できるようになりました。Cisco UCS Central では、なく、Call Home ポリシーが cisco ucs ドメインにプッシュダウンされ、「プロファイル用に設定された電子メールがありません」と表示されません。
CSCvb66577	ドメイングループから別のドメインにドメインを移動すると、Cisco UCS Central に警告メッセージが表示されるようになりました。
CSCvb76019	未解決の VLAN 名は、Cisco UCS Central リリース 1.4 のサービス プロファイル テンプレートに存在しなくなりました。
CSCvb81404	ドメイングループの syslog ファイルサイズの問題が、Cisco UCS Central 1.4.c に存在しません。
CSCvb88419	Cisco UCS Central リリース 1.4b からリリース 1.5(1a) へのアップグレード後、VLAN はポートチャネル設定から失われることはなくなりました。
CSCvc03633	サービス レジストリのクラッシュ後に生成された重複エントリが、 <i>chassisversionholder.txt</i> ファイルに存在しません。
CSCvc07417	すべてのドメイングループの動作設定がルートからプッシュされるようになりました。
CSCvc34656	グローバル サービス プロファイル定義の LUN でのリモート操作は、Cisco UCS Central では失敗します。
CSCvc42518	Cisco UCS Central のポリシー名が、Cisco UCS Manager のポリシー名と一致するようになりました。
CSCvc44482	Cisco UCS Central UI に、サービス プロファイル上の iSCSI vNICs の誤ったファブリック ID が表示されなくなりました。
CSCvc46131	アウトオブバンド機能を備えていない HDD は、サポート対象外として動作していません。これで N/A が表示されます。
CSCvc64224	重複する範囲の IP プールを使用している場合、プライベート範囲の IP アドレスが使用可能として表示されなくなりました。
CSCvc74991	Cisco UCS Central で、vNIC/vHBA 冗長ペアとグローバル サーバプールを使用した場合の重大な障害が発生しなくなりました。
CSCvc92353	Cisco UCS Central は PowerTools を使用して、ローカル デスクトップにバックアップ ファイルをダウンロードできません。

不具合 ID	症状
CSCvd01775	Cisco UCS Manager は、イメージが使用できない場合に Cisco UCS Central からアップグレードが実行されたとき、偽りのアップグレードを実行しません。
CSCvd13002	IPv4 アドレスの欠落メッセージを Cisco UCS Central からクリアできるようになりました。
CSCvd19031	Cisco UCS Central SFTP バックアップ オンデマンドまたはスケジュールが失敗しました。
CSCvd60762	サービスプロファイルで電源ポリシーへの変更後に、サーバの停止が発生しなくなりました。
CSCvd72684	Cisco UCS Central での LDAP 設定は、Cisco UCS Central から下位レベルの Cisco UCS ドメインに完全にプッシュされるようになりました。
CSCvd91971	冗長性ペアのプライマリ vNIC は、最初に VMQ 接続ポリシーを Cisco UCS Manager にプッシュします。

リリース 2.0(1k) で未解決の問題

Cisco UCS Central リリース 2.0 (1k) では、次の問題がオープンになっています。

不具合 ID	症状	回避策
CSCvt12270	Cisco UCS Central リリース 2.0(1d) または 2.0(1e) からリリース 2.0 (1k) へのアップグレードは、ブートパーティションがいっぱいになり失敗する可能性があります。	最初に Cisco UCS Central 2.0(1j) にアップグレードし、次に 2.0(1k) にアップグレードする必要があります。

リリース 2.0(1g) で未解決の問題

Cisco UCS Central リリース 2.0(1g) では、次の問題がオープンになっています。

不具合 ID	症状	回避策
CSCvm81056	VLAN グループは、新しい VLAN が既存の VLAN グループに追加された場合、または Cisco UCS Central 2.0(1d) を使用して vNIC テンプレートに同じ VLAN を追加した場合に、アップリンクポートチャネルから削除されます。	VLAN グループをアップリンクポートチャネルに再度追加します。

リリース 2.0 で未解決の問題

Cisco UCS Central リリース 2.0 では、次の問題が表示されています。

不具合 ID	症状	回避策
CSCvk21902	Cisco UCS Central 2.x からその他の上位バージョンへのアップグレードは、 不明な例外エラー により失敗します。	コンソールから、 [ゲスト (Guest)] > [Send Control + Alt + Delete] を選択して VM を再起動します。再起動が完了すると、アップグレード要求は再度開始され、完了します。
CSCvm81311	Cisco UCS Manager Data Management Engine (DME) は、動的および静的 vNICs の Cisco UCS Central によってパスされた Adminvcon 値が一致しないためにクラッシュします。	なし
CSCvi33069	Cisco Connection Online (CCO) アカウントのユーザー名に大文字の文字が使用されている場合、Cisco UCS Central はイメージライブラリにファームウェアをダウンロードできません。	CCO アカウントのユーザー名には小文字を使用します。
CSCve19522	リリース 3.1(3a) の Cisco UCS ドメインは、[可視性ステータスの消失 (Lost Visibility)] に移行し、正しい登録状態への復元に失敗します。	Cisco UCS Manager CLI から Cisco UCS ドメインの pmon を再起動します。 local mgmt# pmon start local mgmt# pmon start この不具合は、Cisco UCS Manager リリース 3.2(1a) で解決されています。
CSCve15708	3.1(3a) ファームウェアを持つ Cisco UCS ドメインでは、IPv6 アドレスを使用して Cisco UCS Manager を UCS Central に登録すると、次の FSM エラーメッセージが表示されます。 UCS Central のホスト名を解決できません。DNS エントリを確認してください。	Cisco UCS Manager リリース 3.1(2) にダウングレードします。 この不具合は、Cisco UCS Manager リリース 3.2(1a) で解決されています。

不具合 ID	症状	回避策
CSCvd47047	異なるバージョンのブレードサーバとラックサーバからホストファームウェアパッケージポリシーを作成すると、Cisco UCS Central では成功しますが、Cisco UCS Manager では失敗します。これは、Cisco UCS Manager バージョン 3.1 (1) 以前のブレードサーバとラックサーバの混合バージョンに対する Cisco UCS Central のサポートによるものです。	Cisco UCS Manager バージョン 3.1(2) 以降を実行している Cisco UCS ドメインに適用されている場合は、ホストファームウェアパッケージポリシーで同じバージョンの B および C バンドルを設定します。
CSCuz65590	WWXN プールを、関連付けられたグローバルサービスプロファイルの静的 ID に変更すると、Cisco UCS Manager は、Cisco UCS Central の ID とは異なる ID を vHBA に割り当てます。	Cisco UCS Central の vHBA に新しい ID を割り当てます。
CSCve02287	Cisco UCS Central は、iso イメージを使用して新規インストールを実行するときに、不十分なシステムリソースに関する警告なしでインストールを完了します。	インストールプロセスを開始する前に、 システム要件 を確認してください。

関連資料

これらのリリース ノートに加え、Cisco.com の次の場所で、Cisco UCS Central に関する資料を参照できます。

- [Cisco UCS Documentation Roadmap](#)
- 『[Cisco UCS Central Install and Upgrade Guides](#)』
- [Cisco UCS Central Configuration Guides](#)
- [Cisco UCS Central ビデオ](#)
- [Cisco UCS Central CLI 参照マニュアル](#)
- [Cisco UCS Central ベスト プラクティスと運用](#)

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2017–2020 Cisco Systems, Inc. All rights reserved.