Cisco UCS C シリーズ サーバ統合型管理コントローラ コンフィギュレーション ガイド リリース 1.1(1)

Cisco UCS C-Series Servers Integrated Management Controller Configuration Guide, Release 1.1(1)

初版: 2010 年 03 月 31 日

Text Part Number: OL-22384-01-J

【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、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

この前書きの内容は次のとおりです。

対象読者

このガイドは、次の 1 つ以上に責任と専門知識を持つデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

マニュアルの構成

このマニュアルの構成は、次のとおりです。

タイトル	説明
概要	Cisco UCS C シリーズ ラックマウント サーバおよび CIMC GUI について説明します。

タイトル	説明
サーバの管理	CLI コマンドについて説明します。ブートデバイスの順序の設定、サーバへの電力の制御、およびサーバのリセット方法を説明します。
サーバのプロパティの表示	サーバの CPU、メモリ、電源、およびストレージのプロパティの表示方法を説明します。
サーバのセンサーの表示	電源、ファン、温度、電流、および電圧のセンサーの表示方法を説明します。
リモート プレゼンスの管理	仮想 KVM、仮想メディア、および Serial over LAN 接続の設定方法を説明します。
ユーザ アカウントの管理	ユーザを追加、削除、認証する方法、およびユーザ セッションの管理方法を説明します。
ネットワーク関連の設定	ネットワーク インターフェイス、ネットワーク設定、およびネットワーク セキュリティの設定方法を説明します。
コミュニケーション サービスの設定	HTTP、SSH、および IPMI によるサーバ管理コミュニケーションの設定方法を説明します。
証明書の管理	サーバ証明書を生成、アップロード、および管理する方法を説明します。
プラットフォーム イベント フィルタの設定	プラットフォーム イベント フィルタおよび SNMP 設定の設定および管理方法を説明します。
CIMC ファームウェア管理	ファームウェア イメージを取得、インストール、およびアクティブにする方法を説明します。
ログの表示	ログ メッセージを表示およびクリアする方法を説明します。
サーバ ユーティリティ	サポートデータをエクスポートする方法、サーバの設定を出荷時デフォルトにリセットする方法、および管理インターフェイスを再起動する方法を説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	意味
bold フォント	コマンド、キーワード、GUI 要素、およびユーザが入力したテキストは **bold** フォントで表示されます。
italic フォント	マニュアルのタイトル、新規用語または重要な用語、値を指定すべき引数は *italic* フォントで表示されます。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	必須の代替キーワードは、波カッコ内にグループ化され、垂直バーで区切られます。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	スイッチが表示する端末セッションおよび情報は、`courier` フォントで表示されます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。 この状況では、機器の損傷やデータの損失につながるような操作をする可能性があります。

ワンポイント アドバイス　ここで説明されている操作により時間を短縮できることを意味します。 この段落で説明する操作を実行すると、時間を節約することができます。

警告　読者に対する警告を意味します。 この状況では、身体に対する傷害につながるような操作をする可能性があります。

関連資料

Cisco UCS C シリーズ ラックマウント サーバに関するマニュアルは、次の URL から入手できます。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

概要

この章の構成は、次のとおりです。

Cisco UCS C シリーズ ラックマウント サーバの概要

Cisco UCS C シリーズ ラックマウント サーバを次に示します。

- Cisco UCS C200 M1 ラックマウント サーバ
- Cisco UCS C210 M1 ラックマウント サーバ
- Cisco UCS C250 M1 ラックマウント サーバ

UCS C200 M1 ラックマウント サーバ

Cisco UCS C200 M1 サーバは、高密度の 2 ソケット、1 RU ラックマウント サーバです。 このサーバは、実稼動レベルのネットワーク インフラストラクチャ、Web サービス、メインストリーム データセンター、およびブランチオフィスとリモートオフィス用のアプリケーションに対応できるように構築されています。

UCS C210 M1 ラックマウント サーバ

Cisco UCS C210 M1 サーバは、汎用の 2 ソケット、2 RU ラックマウント サーバです。 ストレージ集約型の負荷に対応するため、パフォーマンス、密度、効率をバランスよく実現するように設計

されています。このサーバは、ネットワーク ファイルおよびアプライアンス、ストレージ、データベース、コンテンツ配信など、さまざまな用途に対応できるように構築されています。

UCS C250 M1 ラックマウント サーバ

Cisco UCS C250 M1 サーバは、高性能かつメモリ集約的な 2 ソケット、2 RU ラックマウント サーバです。 パフォーマンスを向上させるように設計されており、要求の厳しいバーチャライゼーションや大量のデータセットの負荷に対応する容量を備えています。 また、C250 M1 サーバでは、メモリ フットプリントが小さいため、コストを削減することができます。

Cisco Integrated Management Controller

Cisco Integrated Management Controller（CIMC）は、C シリーズ サーバ用の管理サービスです。CIMC はサーバ内で動作します。

管理インターフェイス

Web ベースの GUI または SSH ベースの CLI を使用して、サーバにアクセスし、サーバを設定、管理、モニタできます。 ほとんどすべてのタスクは、これらのインターフェイスのいずれでも実行できます。また、一方のインターフェイスで実行されたタスクの結果は、もう一方のインターフェイスにも表示されます。 ただし、次の操作はできません。

- CIMC GUI を使用して CIMC CLI を呼び出す
- CIMC CLI で呼び出したコマンドを CIMC GUI に表示する
- CIMC GUI から CIMC CLI の出力を生成する

CIMC で実行可能なタスク

CIMC を使用すると次のサーバ管理タスクを実行できます。

- サーバの電源のオン、電源のオフ、電源再投入、リセット、およびシャットダウンを行う
- ロケータ LED を切り替える
- サーバのブート順を設定する
- サーバのプロパティとセンサーを表示する
- リモート プレゼンスを管理する
- ローカル ユーザ アカウントを作成して管理し、Active Directory によるリモート ユーザの認証をイネーブルにする
- NIC プロパティ、IPv4、VLAN、ネットワーク セキュリティなど、ネットワーク関連の設定を行う
- HTTP、SSH、IPMI Over LAN などのコミュニケーション サービスを設定する
- 証明書を管理する
- プラットフォーム イベント フィルタを設定する

- CIMC ファームウェアを更新する
- 障害、アラーム、およびサーバのステータスをモニタする

オペレーティング システムやアプリケーションのプロビジョニングや管理はできない

CIMC はサーバのプロビジョニングを行うため、サーバのオペレーティング システムの下に存在します。したがって、サーバでオペレーティング システムやアプリケーションのプロビジョニングや管理を行うためにこれを使用することはできません。 たとえば、次の操作を実行することはできません。

- Windows や Linux などの OS の展開
- OS やアプリケーションなどのソフトウェアに対するパッチの展開
- アンチウイルス ソフトウェア、モニタリング エージェント、バックアップ クライアントなどのベース ソフトウェア コンポーネントのインストール
- データベース、アプリケーション サーバ ソフトウェア、Web サーバなどのソフトウェア アプリケーションのインストール
- Oracle データベースの再起動、プリンタ キューの再起動、または CIMC 以外のユーザ アカウントの処理を含むオペレータ処理の実行
- SAN や NAS ストレージ上の外部ストレージの設定または管理

サーバ ソフトウェア

CIMC は、マザーボードに組み込まれている独立した管理モジュールです。 CIMC が備える専用の ARM ベース プロセッサが、CIMC ソフトウェアを実行します。 実行されているバージョンのファームウェアが付属しています。 ユーザは、[Firmware Update Management] ページで CIMC ファームウェアを更新できます。 初期 CIMC ファームウェアのインストールについて考える必要はありません。

Windows や Linux のような OS をサーバにインストールする必要はありません。 サーバは事前にインストールされた状態で出荷されます。 ただし、DVD ドライブまたはネットワークを使用して別の OS をサーバにインストールすることもできます。 CIMC を使用すると、KVM コンソールおよび vMedia を使用して新しい OS をインストールできます。

サーバでは次のオペレーティング システムがサポートされます。

- Windows Server 2003 R2（32 ビット、64 ビット）、Hyper-V 環境での Windows 7（64 ビット）、Hyper-V 環境での Windows Server 2008（Standard および Enterprise Edition、64 ビット）
- VMware ESX 3.5 U4、VMware vSphere 4、4 U1、4i、4i U1
- RedHat RHEL 5.3（64 ビット）、RHEL 5.4 KVM（64 ビット）、RHEL 6 KVM（64 ビット）、RedHat Rhat 4.8（64 ビット）、Fedora
- Novell SLES 10 SP3（64 ビット）、SLES 11（64 ビット）、SLES 11 SP1 XEN、aSLES 11 XEN（64 ビット）

- Solaris x86 10.x（64 ビット）
- Oracle OVM 2.1.2、2.2
- Oracle Enterprise Linux
- XenServer Citrix

（注） オペレーティング システムをインストールするときは、各製品のインストール マニュアルを参照してください。

サーバの NIC

CIMC への接続には、2 種類の NIC モードを使用できます。 一方のモードでは、プラットフォームに応じて、active-active または active-standby の冗長化モードを選択することもできます。

NIC モード

[NIC Properties] 領域の [NIC Mode] ドロップダウン リストでは、CIMC に到達できるポートを指定します。 プラットフォームに応じて、次のモード オプションを使用できます。

- Dedicated：CIMC への接続は、管理イーサネット ポートを経由して使用できます。
- Shared LOM：CIMC への接続は、LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを経由した場合だけ使用できます。

（注） shared_lom モードでは、すべてのホスト ポートが同じサブネットに属している必要があります。

- Shipping（サポートされている場合）：CIMC への接続は、制限された出荷時デフォルト設定を使用して、管理イーサネット ポートを経由して使用できます。

（注） shipping モードは、CIMC への初期接続の目的だけに用意されています。 運用時には別のモードを設定します。

NIC 冗長化

[NIC Properties] 領域の [NIC Redundancy] ドロップダウン リストでは、NIC 冗長化の処理方法を指定します。

- None：冗長化は使用できません。
- Active-Active：すべてのイーサネット ポートが同時に動作します。 このモードは、CIMC への複数のパスを提供します。

- Active-Standby：1 つのポートから別のポートにフェールオーバーします。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。 使用できるモードについては、プラットフォームのインストレーションおよびサービス ガイドを参照してください。

サーバ ポート

次に示すのは、サーバ ポートとそのデフォルトのポート番号のリストです。

- HTTP：TCP ポート 80
- HTTPS：TCP ポート 443
- TFTP：UDP ポート 69
- SSH：TCP ポート 22
- IPMI：UDP ポート 623
- SoL：TCP ポート 22
- KVM：TCP ポート 2068

CIMC ユーザ インターフェイスの概要

CIMC ユーザ インターフェイスは、Cisco C シリーズ サーバの Web ベースの管理インターフェイスです。 CIMC ユーザ インターフェイスを起動して、次の最小要件を満たしているすべてのリモート ホストからサーバを管理できます。

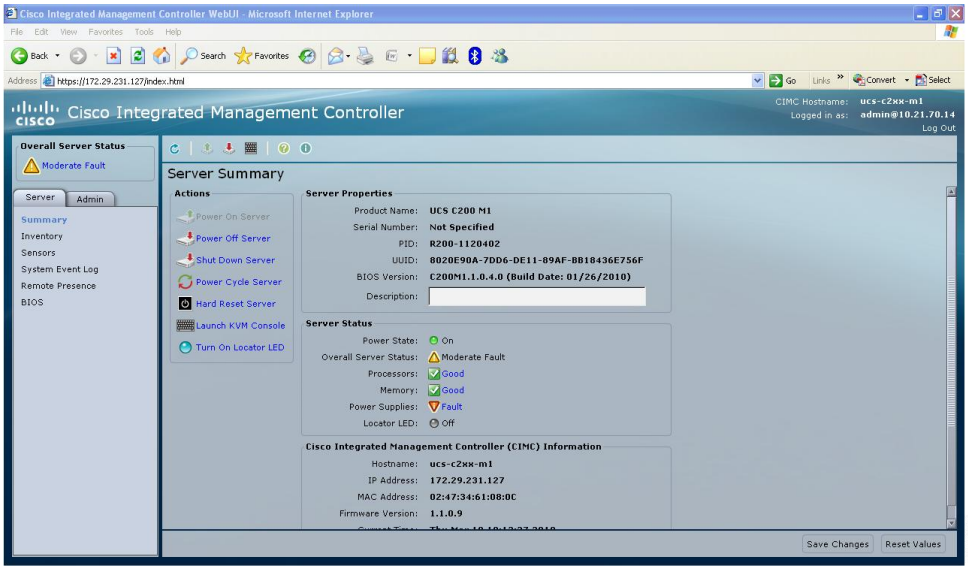
- Java 1.6 以降
- HTTP および HTTPS 対応
- Adobe Flash Player 10 以降

（注） CIMC へのログインに使用するパスワードを失効した場合や忘れた場合は、使用しているプラットフォームの Cisco UCS C シリーズ サーバ インストレーションおよびサービス ガイドでパスワードの回復手順を参照してください。

CIMC ホーム ページ

図 1 は CIMC のホーム ページです。

図 *1* : *CIMC* ホーム ページ



[Navigation] ペイン

[Navigation] ペインは、CIMC ユーザ インターフェイスの左側に表示されます。 [Navigation] ペインで [Server] タブまたは [Admin] タブのリンクをクリックすると、CIMC ユーザ インターフェイスの右側の [Work] ペインに選択したページが表示されます。

次の表では、[Navigation] ペインの要素について説明します。

要素名	説明
[Overall Server Status] 領域	[Overall Server Status] 領域は、[Server] タブおよび [Admin] タブの上にあります。 この領域をクリックすると、[Server Summary] ページがリフレッシュされます。
[Server] タブ	[Server] タブは、[Navigation] ペインにあります。 このタブには次のページへのリンクが含まれます。 • **[Summary]** • **[Inventory]** • **[Sensors]**

	• **[System Event Log]** • **[Remote Presence]** • [BIOS]
[Admin] タブ	[Admin] タブは、[Navigation] ペインにあります。このタブには次のページへのリンクが含まれます。 • **[Users Management]** • **[Network]** • **[Communication Services]** • **[Certificate Management]** • **[CIMC Log]** • **[Event Management]** • **[Firmware Management]** • **[Utilities]**

[Work] ペイン

[Work] ペインは、UI の右側に表示されます。 [Work] ペインには、[Server] タブまたは [Admin] タブでクリックしたリンクに応じて異なるページが表示されます。

次の表は、[Work] ペインの要素とページをまとめたものです。

ページまたは要素名	説明
[Summary]	このページには、サーバのプロパティ、サーバのステータス、および CIMC の情報が表示されます。 サーバ電源のオンやオフなどの操作も実行できます。
[Inventory]	このページには 4 つのタブがあります。 • [CPUs]：このタブには、CPU についての情報が表示されます。 • [Memory]：このタブには、メモリについての情報が表示されます。 • [Power Supplies]：このタブには、電源についての情報が表示されます。 • [Storage]：このタブには、ストレージについての情報が表示されます。

[Sensors]	このページには 4 つのタブがあります。 • [Power Supply Sensors]：このタブには、電源センサーが表示されます。 • [Fan Sensors]：このタブには、ファン センサーが表示されます。 • [Temperature Sensors]：このタブには、温度センサーが表示されます。 • [Voltage Sensors]：このタブには、電圧センサーが表示されます。
[System Event Log]	このページでは、システム イベント ログを表示できます。
[Remote Presence]	このページには 3 つのタブがあります。 • [Virtual KVM]：このタブでは、vKVM のプロパティを設定します。 • [Virtual Media]：このタブでは、仮想メディアのプロパティを設定します。 • [Serial over LAN]：このタブでは、Serial over LAN のプロパティを設定します。
[BIOS]	このページには 3 つの領域があります。 • [Actions]：この領域では、サーバのブート順の設定、壊れた BIOS のリカバリ、および BIOS CMOS のクリアを行います。 • [BIOS Properties]：この領域には BIOS の実行されているバージョンが表示されます。 • [Boot Order]：この領域には、設定されているブート順と実際のブート順が表示されます。
[User Management]	このページには 3 つのタブがあります。 • [Local Users]：このタブでは、ユーザを作成します。 • [Active Directory]：このタブでは、Active Directory のプロパティを設定します。 • [Sessions]：このタブには、現在のユーザ セッションが表示されます。
[Network]	このページには 2 つのタブがあります。

	• [Network Settings]：このタブでは、ネットワーク プロパティを設定します。 • [Network Security]：このタブでは、ネットワーク セキュリティを設定します。
[Communications Services]	このページには 3 つの領域があります。 • [HTTP Properties]：この領域では、HTTP のプロパティを設定します。 • [SSH Properties]：この領域では、SSH のプロパティを設定します。 • [IPMI over LAN Properties]：このタブでは、IPMI over LAN のプロパティを設定します。
[Certificate Management]	このページには 2 つの領域があります。 • [Actions]：この領域では、証明書を生成してアップロードします。 • [Current Certificate]：この領域には、サーバの現在の証明書が表示されます。
[CIMC Log]	このページには、CIMC のログが表示されます。
[Event Management]	このページには 2 つのタブがあります。 • [Platform Event Filters]：このタブでは、プラットフォーム イベント フィルタを設定します。 • [Trap Settings]：このタブでは、SNMP トラップを設定します。
[Firmware Management]	このページには 4 つの領域があります。 • [Actions]：この領域では、クライアント ブラウザまたは TFTP サーバから CIMC ファームウェアをインストールするか、またはインストールされている CIMC ファームウェアをアクティブにします。 • [CIMC Firmware]：この領域には、ファームウェアの実行、バックアップ、およびブートローダのバージョンのステータスが表示されます。 • [Last Firmware Install]：この領域には、ファームウェアの最後の更新に関する情報が表示されます。

[Utilities]	このページには 2 つの領域があります。 • [Actions]：この領域では、テクニカル サポート データをエクスポートし、CIMC を出荷時デフォルトにリセットし、CIMC を再起動します。 • [Last Technical Support Data Export]：この領域にはテクニカル サポート データの最後のエクスポートに関する情報が表示されます。

ツールバー

ツールバーは [Work] ペインの上に表示されます。

要素名	説明
[Refresh]	現在のページを更新します。
[Power On Server]	サーバの電源をオンにします。
[Power Off Server]	サーバの電源をオフにします。
[Launch KVM Console]	KVM コンソールを起動します。
[Help]	ヘルプを表示します。
[Info]	サーバ情報を表示します。

Cisco Integrated Management Controller オンライン ヘルプの概要

Cisco Integrated Management Controller は、左側の [Navigation] ペインと右側の [Work] ペインの 2 つの主要なセクションに分かれています。

このヘルプ システムは、各 GUI ページと各ダイアログボックスのフィールドについて説明します。

ヘルプ ページにアクセスするには、次の操作を実行します。

- GUI の特定のタブで、[Work] ペイン上方のツールバーにある [Help] アイコンをクリックします。
- ダイアログボックスで、そのダイアログボックスの [Help] ボタンをクリックします。

（注） 使用可能なすべての C シリーズ マニュアルの一覧については、『*Cisco UCS C-Series Servers Documentation Roadmap*』（http://www.cisco.com/go/unifiedcomputing/c-series-doc）を参照してください。

CIMC へのログイン

操作を行う前に

Adobe Flash Player 10 以降がインストールされていない場合は、ローカル マシンにインストールします。

手順

ステップ 1 Web ブラウザで、CIMC の Web リンクを入力または選択します。

ステップ 2 セキュリティ ダイアログボックスが表示された場合は、次の操作を実行します。

a) （オプション） チェックボックスをオンにして、シスコからのすべてのコンテンツを受け入れます。

b) [Yes] をクリックして証明書を受け入れ、続行します。

ステップ 3 ログイン ウィンドウで、ユーザ名とパスワードを入力します。

ステップ 4 [Log In] をクリックします。

CIMC からのログアウト

手順

ステップ 1 CIMC の右上で、[Log Out] をクリックします。
ログアウトすると、CIMC のログイン ページに戻ります。

ステップ 2 （オプション） 再度ログインするか、Web ブラウザを閉じます。

第 2 章

サーバ OS のインストール

この章の構成は、次のとおりです。

OS のインストール方法

C シリーズ サーバは、複数のオペレーティング システムをサポートしています。インストールされている OS に関係なく、次のいずれかのツールを使用してサーバにインストールできます。

- KVM コンソール
- PXE インストール サーバ

KVM コンソール

KVM コンソールは CIMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。 KVM コンソールを使用すると、リモートの場所からサーバに接続できます。

サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、KVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージ ファイルです。 次のいずれでも仮想ドライブにマップできます。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージ ファイル
- ネットワーク上の CD/DVD またはフロッピー ドライブ

- ネットワーク上のディスク イメージ ファイル

KVM コンソールを使用してサーバに OS をインストールできます。

KVM コンソールを使用した OS のインストール

操作を行う前に

- OS インストール ディスクまたはディスク イメージ ファイルを見つけます。
- OS をインストールするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 OS インストール ディスクを CD/DVD ドライブにロードするか、ディスク イメージ ファイルをコンピュータにコピーします。

ステップ 2 CIMC が開いていない場合は、ログインします。

ステップ 3 [Navigation] ペインの [Server] タブをクリックします。

ステップ 4 [Server] タブの [Remote Presence] をクリックします。

ステップ 5 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。

ステップ 6 [Actions] 領域で、[Launch KVM Console] をクリックします。
[KVM Console] が別ウィンドウで開きます。

ステップ 7 KVM コンソールから、[Tools] ➤ [Launch Virtual Media] を選択し、[Virtual Media Session] ダイアログボックスを開きます。

ステップ 8 [Virtual Media Session] ダイアログボックスで、次のいずれかの方法を使用して仮想メディアをマップします。

- OS インストール ディスクが含まれている CD/DVD ドライブの [Mapped] チェックボックスをオンにします。
- [Add Image] をクリックし、OS インストール ディスク イメージに移動してこれを選択します。[Open] をクリックしてディスク イメージをマウントし、マウントされたディスク イメージの [Mapped] チェックボックスをオンにします。

（注） OS のインストール プロセスの間は、[Virtual Media Session] ダイアログボックスを開いたままにしておく必要があります。 ダイアログボックスを閉じると、すべての仮想メディアをマップできません。

ステップ 9 サーバを再起動します。
サーバを再起動すると、仮想 CD/DVD ドライブからインストール プロセスが開始します。 残りのインストール プロセスについては、インストールしている OS のインストレーション ガイドを参照してください。

次の手順

OS のインストールが完了したら、仮想メディアのブート順を元の設定にリセットします。

PXE インストール サーバ

Preboot Execution Environment（PXE）インストール サーバを使用すると、クライアントはリモートの場所から OS をブートおよびインストールできます。 この方法を使用するには、PXE 環境が設定されていて、VLAN（通常は専用のプロビジョニング VLAN）で使用できるようになっている必要があります。 さらに、サーバがネットワークからブートするように設定されている必要があります。 サーバは、ブートすると、PXE 要求をネットワーク経由で送信します。 PXE インストール サーバは、この要求に応答確認し、サーバに OS をインストールするイベントのシーケンスを開始します。

PXE サーバは、インストール ディスク、ディスク イメージ、またはスクリプトを使用して、OS をインストールできます。 また、独自のディスク イメージを使用して、OS、追加コンポーネント、またはアプリケーションをインストールすることもできます。

（注） PXEインストールは、多数のサーバにOSをインストールする場合に効率のよい方法です。 ただし、この方法を使用するには PXE 環境をセットアップする必要があることを考えると、他のインストール方法を使用する方が簡単な場合があります。

PXE インストール サーバを使用した OS のインストール

操作を行う前に

- VLAN 経由でサーバに到達できることを確認します。
- OSをインストールするには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 **PXE** のブート順を最初に設定します。

ステップ 2 サーバを再起動します。
VLAN で PXE インストール サーバを使用できる場合は、サーバが再起動するとインストール プロセスが開始します。 通常、PXEインストールは自動化されており、追加のユーザ入力を必要としません。 残りのインストール プロセスについては、インストールしている OS のインストレーション ガイドを参照してください。

次の手順

OS のインストールが完了したら、LAN のブート順を元の設定にリセットします。

第 3 章

サーバの管理

この章の構成は、次のとおりです。

全体のサーバ ステータスの表示

手順

ステップ 1 [Navigation] ペインの [Overall Server Status] 領域で、青色のヘルス レポート リンクをクリックして、[Server Summary] ペインを更新します。

ステップ 2 （オプション） [Server Summary] ペインで次の情報を確認します。

名前	説明
[Power State] フィールド	現在の電源状態。
[Overall Server Status] フィールド	サーバの全体的なステータス。 ここに指定できる値は次のとおりです。

名前	説明
	• [Memory Test In Progress]：サーバは搭載されているメモリのセルフテストを実行しています。 この状態は、通常、ブート プロセスの間に発生します。 • **Good** • **Moderate Fault** • **Severe Fault** • **Powered Off**
[Processors] フィールド	プロセッサの全体的なステータス。 ここに指定できる値は次のとおりです。 • **Good** • **Fault** • **Powered Off** このフィールドのリンクをクリックして、プロセッサに関する詳細情報を表示できます。
[Memory] フィールド	メモリ モジュールの全体的なステータス。 ここに指定できる値は次のとおりです。 • **Good** • **Fault** • **Powered Off** このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[Power Supplies] フィールド	電源装置の全体的なステータス。 ここに指定できる値は次のとおりです。 • **Good** • **Fault** • **Powered Off** このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[Fans] フィールド	電源装置の全体的なステータス。 ここに指定できる値は次のとおりです。 • **Good**

名前	説明
	• **Fault** • **Powered Off** このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。 （注） このフィールドが表示されるのは一部の C シリーズサーバだけです。
[HDD] フィールド	ハードドライブの全体的なステータス。 ここに指定できる値は次のとおりです。 • **Good** • **Fault** • **Powered Off** このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。 （注） このフィールドが表示されるのは一部の C シリーズサーバだけです。
[Locator LED] フィールド	ロケータ LED がオンかオフか。

ロケータ LED の切り替え

操作を行う前に

この操作を含むすべての電力制御操作には、ユーザ権限が必要になります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Turn On Locator LED] をクリックします。
ロケータ LED がオンになり、点滅します。

ステップ 4 [Actions] 領域で、[Turn Off Locator LED] をクリックします。
ロケータ LED がオフになります。

サーバのブート順の設定

操作を行う前に

サーバのブート順を設定するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [BIOS] をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [Actions] 領域で、[Configure Boot Order] をクリックします。
ブート順の説明が示されたダイアログボックスが表示されます。

ステップ 4 この説明を確認してから、[OK] をクリックします。
[Configure Boot Order] ダイアログボックスが表示されます。

ステップ 5 [Configure Boot Order] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[Device Types] テーブル	サーバのブート オプション。 次の 1 つ以上を選択できます。 • [HDD]：ハード ディスク ドライブ • [FDD]：フロッピー ディスク ドライブ • [CDROM]：ブート可能な CD-ROM • [PXE]：PXE ブート • [EFI]：Extensible Firmware Interface
[Add >]	選択したデバイス タイプを [Boot Order] テーブルに移動します。
[< Remove]	選択したデバイス タイプを [Boot Order] テーブルから削除します。
[Boot Order] テーブル	このサーバがブートできるデバイス タイプが、ブートが試行される順番に表示されます。
[Up]	選択したデバイス タイプを [Boot Order] テーブルで高いプライオリティに移動します。
[Down]	選択したデバイス タイプを [Boot Order] テーブルで低いプライオリティに移動します。

名前	説明
[Apply] ボタン	設定されているブート順に対する変更を保存するか、または以前に設定したブート順を再適用します。 CIMC は、サーバが次に再起動されるときに、設定されているブート順を BIOS に送信します。
[Cancel] ボタン	変更を保存しないで、または既存の設定を再適用しないで、ダイアログボックスを閉じます。 このオプションを選択すると、サーバが次に再起動されるときに、実際のブート順は変更されません。

ステップ 6 [Apply] をクリックします。
サーバに接続しているデバイスによっては、実際のブート順に追加のデバイス タイプが付加される場合があります。

次の手順

サーバを再起動して、新しいブート順でブートします。

サーバの電源投入

（注） サーバの電源がCIMC経由以外の何らかの方法でオフにされた場合、サーバは電源をオンにしてもすぐにはアクティブになりません。 サーバは、CIMCが初期化を完了するまでスタンバイモードで動作します。

操作を行う前に

サーバの電源をオンにするには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Power On Server] をクリックします。
[Power on the server?] というメッセージが示されたダイアログボックス が表示されます。

ステップ 4 [OK] をクリックします。

サーバの電源オフ

操作を行う前に

サーバの電源をオフにするには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Power Off Server] をクリックします。
[Power Off the Server?] というメッセージが示されたダイアログボックス が表示されます。

ステップ 4 [OK] をクリックします。

サーバ電源の再投入

操作を行う前に

サーバの電源を再投入するには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Power Cycle Server] をクリックします。
[Power Cycle the Server?] というメッセージが示されたダイアログボックス が表示されます。

ステップ 4 [OK] をクリックします。

サーバのリセット

操作を行う前に

サーバをリセットするには、使用権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Hard Reset Server] をクリックします。
[Hard Reset the Server?] というメッセージが示されたダイアログボックス が表示されます。

ステップ 4 [OK] をクリックします。

サーバのシャットダウン

操作を行う前に

サーバをシャットダウンするには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Shut Down Server] をクリックします。
[Shut Down the Server?] というメッセージが示されたダイアログボックス が表示されます。

ステップ 4 [OK] をクリックします。

第 4 章

サーバのプロパティの表示

この章の構成は、次のとおりです。

CPU のプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

ステップ 3 [Inventory] ペインの [CPUs] タブをクリックします。

ステップ 4 各 CPU で次の情報を確認します。

名前	説明
[Socket Name] フィールド	CPU が装着されているソケット
[Serial Number] フィールド	CPU のシリアル番号
[Vendor] フィールド	CPU のベンダー
[Version] フィールド	CPU のバージョン
[Number of Cores] フィールド	CPU のコアの数

名前	説明
[Signature] フィールド	CPU のシグニチャ
[Max Speed] フィールド	ソケットでサポートされている最大 CPU 速度
[Number of Threads] フィールド	CPU が同時に処理できる最大スレッド数

メモリのプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

ステップ 3 [Inventory] ペインの [Memory] タブをクリックします。

ステップ 4 メモリに関する次の情報を確認します。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Name] カラム	メモリ モジュールが装着されている DIMM スロットの名前
[Capacity] カラム	DIMM のサイズ（MB 単位）
[Speed] カラム	メモリ モジュールのクロック速度（メガヘルツ単位）
[Type] カラム	メモリのタイプ

電源のプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

ステップ 3 [Inventory] ペインの [Power Supplies] タブをクリックします。

ステップ 4 各電源で次の情報を確認します。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Device ID] カラム	電源装置ユニットの ID。
[Input] カラム	電源装置への入力（ワット単位）。
[Max Output] カラム	電源装置からの最大出力（ワット単位）。
[FW Version] カラム	電源装置のファームウェア バージョン。

ストレージのプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

ステップ 3 [Inventory] ペインの [Storage] タブをクリックします。

ステップ 4 ストレージに関する次の情報を確認します。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Name] カラム	ストレージ デバイスの名前。
[Status] カラム	ストレージデバイスのステータス。ここに指定できる値は次のとおりです。

名前	説明
	• **absent** • **present**

第 5 章

サーバのセンサーの表示

この章の構成は、次のとおりです。

電流センサーの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [Current] タブをクリックします。

ステップ 4 [Current] タブで、電流関連の統計情報を表示します。

LED センサーの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [Sensors] をクリックします。
ステップ 3 [Sensors] ペインの [LEDs] タブをクリックします。
ステップ 4 [LEDs] タブに LED に関する統計情報が表示されます。

ファン センサーの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [Sensors] をクリックします。
ステップ 3 [Sensors] ペインの [Fan] タブをクリックします。
ステップ 4 サーバのファンに関する次の統計情報が表示されます。
ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Sensor Name] カラム	センサーの名前。
[Status] カラム	センサーのステータス。 ここに表示される値は次のとおりです。 • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
[Speed] カラム	ファンの速度（RPM 単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。

名前	説明
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

電源センサーの表示

ヒント　カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

手順

ステップ 1　[Navigation] ペインの [Server] タブをクリックします。

ステップ 2　[Server] タブの [Sensors] をクリックします。

ステップ 3　[Sensors] ペインの [Power Supply] タブをクリックします。

ステップ 4　[Properties] 領域で、[Redundancy Status] フィールドにサーバの電源装置の冗長性のステータスが表示されます。

ステップ 5　[Threshold Sensors] 領域で、次に示すサーバの統計情報を表示できます。

名前	説明
[Sensor Name] カラム	センサーの名前。
[Status] カラム	センサーのステータス。 ここに表示される値は次のとおりです。 • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
[Reading] カラム	現在の電力使用量（ワット単位）。

名前	説明
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

ステップ 6 [Discrete Sensors] 領域で、次に示すサーバの統計情報を表示できます。

名前	説明
[Sensor Name] カラム	センサーの名前。
[Status] カラム	センサーのステータス。 ここに表示される値は次のとおりです。 • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
[Reading] カラム	ここに指定できる値は次のとおりです。 • **absent** • **present**

温度センサーの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [Temperature] タブをクリックします。

ステップ 4 サーバの温度に関する次の統計情報が表示されます。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Sensor Name] カラム	センサーの名前。
[Status] カラム	センサーのステータス。 ここに表示される値は次のとおりです。 • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
[Temperature] カラム	現在の温度（摂氏単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

電圧センサーの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [Voltage] タブをクリックします。

ステップ 4 サーバの電圧に関する次の統計情報が表示されます。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Sensor Name] カラム	センサーの名前。
[Status] カラム	センサーのステータス。 ここに表示される値は次のとおりです。 • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**
[Voltage] カラム	現在の電圧（ボルト単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

第 6 章

リモート プレゼンスの管理

この章の構成は、次のとおりです。

Serial over LAN の設定

Serial over LAN を使用すると、管理対象システムのシリアル ポートの入出力を IP 経由でリダイレクトできます。 ホスト コンソールへ CIMC を使用して到達する場合は、サーバで Serial over LAN を設定して使用します。

操作を行う前に

Serial over LAN を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Remote Presence] をクリックします。

ステップ 3 [Remote Presence] ペインの [Serial over LAN] タブをクリックします。

ステップ 4 [Serial over LAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	オンにすると、このサーバで Serial over LAN がイネーブルになります。
[Baud Rate] フィールド	システムが Serial over LAN 通信に使用するボー レート。

ステップ 5 [Save Changes] をクリックします。

仮想メディアの設定

操作を行う前に

仮想メディアを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Remote Presence] をクリックします。

ステップ 3 [Remote Presence] ペインの [Virtual Media] タブをクリックします。

ステップ 4 [Virtual Media Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	オンにすると、仮想メディアがイネーブルになります。 （注） このチェックボックスをオフにすると、すべての仮想メディア デバイスはホストから自動的に切断されます。
[Active Sessions] フィールド	現在実行されている仮想メディア セッションの数。
[Enable Virtual Media Encryption] チェックボックス	オンにすると、すべての仮想メディア通信は暗号化されます。

ステップ 5 [Save Changes] をクリックします。

KVM コンソール

KVM コンソールは CIMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。 KVM コンソールを使用すると、リモートの場所からサーバに接続できます。

サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、KVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージ ファイルです。 次のいずれでも仮想ドライブにマップできます。

- コンピュータ上の CD/DVD またはフロッピー ドライブ

- コンピュータ上のディスク イメージ ファイル
- ネットワーク上の CD/DVD またはフロッピー ドライブ
- ネットワーク上のディスク イメージ ファイル

KVM コンソールを使用してサーバに OS をインストールできます。

仮想 KVM の設定

操作を行う前に

仮想 KVM を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Remote Presence] をクリックします。

ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。

ステップ 4 [Virtual KVM] タブ で、次のフィールドに入力します。

名前	説明
[Enabled] チェックボックス	オンにすると、仮想 KVM がイネーブルになります。 （注） 仮想メディア ビューアにはKVMを使用してアクセスします。 KVM コンソールをディセーブルにすると、CIMC はホストに接続されているすべての仮想メディア デバイスへのアクセスもディセーブルにします。
[Max Sessions] フィールド	許可されている KVM の同時セッションの最大数。 1 ～ 4 の範囲の整数を入力します。
[Active Sessions] フィールド	サーバで実行されている KVM セッションの数。
[Remote Port] フィールド	KVM 通信に使用するポート。
[Enable Video Encryption] チェックボックス	オンにすると、サーバは KVM で送信されるすべてのビデオ情報を暗号化します。
[Enable Local Server Video] チェックボックス	オンにすると、KVM セッションはサーバに接続されているすべてのモニタにも表示されます。

ステップ 5 [Save Changes] をクリックします。

仮想 KVM のディセーブル化

操作を行う前に

仮想KVMをディセーブルにするには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [Remote Presence] をクリックします。
ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。
ステップ 4 [Virtual KVM] タブで、[Enabled] チェックボックスをオフにします。
ステップ 5 [Save Changes] をクリックします。

仮想 KVM のイネーブル化

操作を行う前に

仮想 KVM をイネーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [Remote Presence] をクリックします。
ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。
ステップ 4 [Virtual KVM] タブで、[Enabled] チェックボックスをオンにします。
ステップ 5 [Save Changes] をクリックします。

第 7 章

ユーザ アカウントの管理

この章の構成は、次のとおりです。

Active Directory

Active Directory はさまざまなネットワーク サービスを提供するテクノロジーであり、LDAP と同様のディレクトリ サービス、Kerberos ベースの認証、DNS ベースの名前付けなどが含まれます。CIMC は、Active Directory の Kerberos ベースの認証サービスを利用します。

CIMC で Active Directory をイネーブルにすると、すべてのユーザ認証とロール許可は Active Directory によって実行され、CIMC はローカル データベースを無視します。 CIMC が Active Directory に接続できない場合、CIMC はローカル データベースに戻ります。

[Active Directory Properties] 領域の [Enable Encryption] チェックボックスをオンにすることで、サーバに Active Directory への送信データを暗号化するよう要求できます。

CIMC での Active Directory の設定

操作を行う前に

Active Directory を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [User Management] ペインの [Active Directory] タブをクリックします。

ステップ 4 [Active Directory Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	オンにすると、すべてのユーザ認証とロール許可は Active Directory によって実行され、CIMC はローカル ユーザ データベースを無視します。 （注） CIMC が Active Directory への接続を確立できない場合、CIMC は自動的にローカル ユーザ データベースの使用に戻ります。
[Server IP Address] フィールド	Active Directory サーバの IP アドレス。
[Timeout] フィールド	CIMC が Active Directory への接続を確立できないと判断するまで待機する秒数。
[Enable Encryption] チェックボックス	オンにすると、サーバは Active Directory に送信するすべての情報を暗号化します。
[Domain] フィールド	すべてのユーザが属する必要のあるドメイン。
[Attributes] フィールド	ユーザのロールとロケール情報を保持する LDAP アトリビュート。 このプロパティは、常に、名前と値のペアで指定されます。 システムは、ユーザ レコードで、このアトリビュート名と一致する値を検索します。 LDAP アトリビュートは、次のアトリビュート ID である必要があります。 1.3.6.1.4.1.9.287247.1 （注） このプロパティを指定しない場合、ユーザ アクセスは read-only に制限されます。

ステップ 5 [Save Changes] をクリックします。

Active Directory サーバの設定

CIMC を設定して、Active Directory をユーザの認証と認可に使用できます。 Active Directory を使用するには、CIMC のユーザ ロールとロケールを保持するアトリビュートを使用してユーザを設定します。 CIMC のユーザ ロールとロケールにマップされた既存の LDAP アトリビュートを使用できます。または、Active Directory スキーマを変更して、アトリビュート ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair アトリビュートのような新規のカスタム アトリビュートを追加できます。 Active Directory スキーマの変更の詳細については、 http://technet.microsoft.com/en-us/library/bb727064.aspx にある記事を参照してください。

Active Directory サーバで次の手順が実行します。

（注） この例では CiscoAVPair という名前のカスタム アトリビュートを作成しますが、CIMC のユーザ ロールとロケールにマップされた既存の LDAP アトリビュートを使用することもできます。

手順

ステップ 1 Active Directory スキーマ スナップインがインストールされていることを確認します。

ステップ 2 Active Directory スキーマ スナップインを使用して、次のプロパティを持つ新しいアトリビュートを追加します。

プロパティ	値
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
Description	CiscoAVPair
Syntax	Case Sensitive String

ステップ 3 Active Directory スナップインを使用して、ユーザ クラスに CiscoAVPair アトリビュートを追加します。

a) 左ペインで [Classes] ノードを展開し、U を入力してユーザ クラスを選択します。
b) [Attributes] タブをクリックして、[Add] をクリックします。
c) C を入力して CiscoAVPair アトリビュートを選択します。
d) [OK] をクリックします。

ステップ 4 CIMC にアクセスできるようにするユーザに対し、次のユーザ ロール値を CiscoAVPair アトリビュートに追加します。

ロール	CiscoAVPair アトリビュート値
admin	shell:roles="admin"
user	shell:roles="user"
read-only	shell:roles="read-only"

（注） アトリビュートに値を追加する方法の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx にある記事を参照してください。

次の手順

CIMC を使用して Active Directory を設定します。

ローカル ユーザの設定

操作を行う前に

ローカル ユーザを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [User Management] ペインの [Local User] タブをクリックします。

ステップ 4 ローカル ユーザを設定するには、行をクリックします。

ステップ 5 [User Details] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[ID] カラム	ユーザの固有識別情報。
[Enabled] チェックボックス	オンにすると、ユーザは CIMC でイネーブルになります。
[User Name] カラム	ユーザのユーザ名。
[Role] カラム	ユーザに割り当てられているロール。 ここに指定できる値は次のとおりです。 • [read-only]：このユーザは情報を表示できますが、変更することはできません。 • [user]：このユーザは次のことが可能です。

名前	説明
	◦すべての情報を表示する ◦電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する ◦KVM コンソールと仮想メディアを起動する ◦すべてのログをクリアする ◦ロケータ LED を切り替える • [admin]：このユーザは、GUI、CLI、IPMI で可能なすべての処理を実行できます。

ステップ 6 パスワード情報を入力します。

ステップ 7 [Save Changes] をクリックします。

ユーザ セッションの表示

手順

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

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [User Management] ペインの [Sessions] タブをクリックします。

ステップ 4 現在のユーザ セッションに関する次の情報が表示されます。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Session ID] カラム	セッションの固有識別情報。
[Username] カラム	ユーザのユーザ名。
[IP Address] カラム	ユーザがサーバにアクセスした IP アドレス。
[Type] カラム	ユーザがサーバにアクセスした方法。
[Action] カラム	ユーザ アカウントに admin 権限があり、関連付けられているユーザ セッションを強制的に終了できる場合は、このカラムに

名前	説明
	[Terminate] と表示されます。 それ以外の場合は、[N/A] と表示されます。 （注） このタブから現在のセッションを終了することはできません。

第 8 章

ネットワーク関連の設定

この章の構成は、次のとおりです。

Server NIC Configuration

サーバの NIC

CIMC への接続には、2 種類の NIC モードを使用できます。 一方のモードでは、プラットフォームに応じて、active-active または active-standby の冗長化モードを選択することもできます。

NIC モード

[NIC Properties] 領域の [NIC Mode] ドロップダウン リストでは、CIMC に到達できるポートを指定します。 プラットフォームに応じて、次のモード オプションを使用できます。

- Dedicated：CIMC への接続は、管理イーサネット ポートを経由して使用できます。
- Shared LOM：CIMC への接続は、LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを経由した場合だけ使用できます。

（注） shared_lom モードでは、すべてのホスト ポートが同じサブネットに属している必要があります。

- Shipping（サポートされている場合）：CIMC への接続は、制限された出荷時デフォルト設定を使用して、管理イーサネット ポートを経由して使用できます。

（注） shipping モードは、CIMC への初期接続の目的だけに用意されています。 運用時には別のモードを設定します。

NIC 冗長化

[NIC Properties] 領域の [NIC Redundancy] ドロップダウン リストでは、NIC 冗長化の処理方法を指定します。

- None：冗長化は使用できません。
- Active-Active：すべてのイーサネット ポートが同時に動作します。 このモードは、CIMC への複数のパスを提供します。
- Active-Standby：1 つのポートから別のポートにフェールオーバーします。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。 使用できるモードについては、プラットフォームのインストレーションおよびサービス ガイドを参照してください。

サーバ NIC の設定

NIC モードと NIC 冗長化を設定する場合は、サーバの NIC を設定します。

操作を行う前に

NIC を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Network] をクリックします。

ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。

ステップ 4 [NIC Properties] 領域で、次のプロパティを更新します。

名前	説明
[NIC Mode] ドロップダウン リスト	NIC モード。 ここに指定できる値は次のとおりです。 • [Dedicated]：CIMC へのアクセスに管理ポートを使用します。 • [Shared LOM]：CIMC へのアクセスに LAN On Motherboard（LOM; マザーボードのオンボード LAN）ポートを使用します。

名前	説明
	• [Shipping]：すべてのオプションにアウトオブザボックスのデフォルトを使用します。 （注） このオプションを使用できるのは一部のCシリーズ サーバだけです。
[NIC Redundancy] ドロップダウン リスト	NIC 冗長化オプションは、[NIC Mode] ドロップダウン リストで選択されているモードに依存します。 あるオプションが表示されない場合、そのオプションは選択されているモードでは使用できません。 次のオプションを使用できます。 • [None]：設定されている NIC モードに関連付けられた各ポートは個別に動作します。 問題が発生した場合、ポートはフェールオーバーしません。 • [active-active]：サポートされている場合、設定されている NIC モードに関連付けられたすべてのポートは同時に動作します。 これにより、スループットが増加し、CIMC への複数のパスが提供されます。 • [active-standby]：設定されている NIC モードに関連付けられたポートで障害が発生した場合、トラフィックは、その NIC モードに関連付けられている他のポートの 1 つにフェールオーバーします。 （注） このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じサブネットに接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。
[MAC Address] フィールド	[NIC Mode] フィールドで選択されている CIMC ネットワーク インターフェイスの MAC アドレス。

ステップ 5 [Save Changes] をクリックします。

共通プロパティの設定

サーバを説明するには、共通プロパティを使用します。

操作を行う前に

共通プロパティを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Network] をクリックします。
ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
ステップ 4 [Hostname] フィールドに、ホストの名前を入力します。
ステップ 5 [Save Changes] をクリックします。

IPv4 の設定

操作を行う前に

IPv4 を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Network] をクリックします。
ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
ステップ 4 [IPv4 Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable IPv4] チェックボックス	オンにすると、IPv4 がイネーブルになります。
[Use DHCP] チェックボックス	オンにすると、CIMC は DHCP を使用します。
[IP Address] フィールド	CIMC の IP アドレス。
[Subnet Mask] フィールド	IP アドレスのサブネット マスク。
[Gateway] フィールド	IP アドレスのゲートウェイ。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、CIMC は DNS サーバ アドレスを DHCP から取得します。
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。

名前	説明
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。

ステップ 5 [Save Changes] をクリックします。

VLAN への接続

操作を行う前に

VLAN に接続するには、admin としてログインしている必要があります。

手順

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

ステップ 2 [Admin] タブの [Network] をクリックします。

ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。

ステップ 4 [VLAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable VLAN] チェックボックス	オンにすると、CIMC は仮想 LAN に接続されます。
[VLAN ID] フィールド	VLAN ID。
[Priority] フィールド	VLAN でのこのシステムのプライオリティ。

ステップ 5 [Save Changes] をクリックします。

Network Security Configuration

ネットワーク セキュリティ

CIMC は、IP ブロッキングをネットワーク セキュリティとして使用します。IP ブロッキングは、サーバまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接続を防ぎます。

IP ブロッキングは、これらのコンピュータから Web サイト、メール サーバ、またはその他のインターネット サーバへの不要な接続を効果的に禁止します。

禁止 IP の設定は、一般的に、Denial of Service（DoS; サービス拒絶）攻撃から保護するために使用されます。 CIMC は、IP ブロッキングの失敗回数を設定して、IP アドレスを禁止します。

ネットワーク セキュリティの設定

IP ブロッキングの失敗回数を設定する場合は、ネットワーク セキュリティを設定します。

操作を行う前に

ネットワーク セキュリティを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Network] をクリックします。

ステップ 3 [Network] ペインの [Network Security] タブをクリックします。

ステップ 4 [IP Blocking Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable IP Blocking] チェックボックス	このチェックボックスをオンにすると、IP ブロッキングがイネーブルになります。
[IP Blocking Fail Count] フィールド	指定された時間ユーザがロックアウトされる前に、ユーザが試行できるログインの失敗回数。 この回数のログイン試行失敗は、[IP Blocking Fail Window] フィールドで指定されている期間内に発生する必要があります。 3 ～ 10 の範囲の整数を入力します。
[IP Blocking Fail Window] フィールド	ユーザをロックアウトするためにログイン試行の失敗が発生する必要のある期間（秒数）。 60 ～ 120 の範囲の整数を入力します。
[IP Blocking Penalty Time] フィールド	ユーザが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザがロックアウトされている秒数。 300 ～ 900 の範囲の整数を入力します。

ステップ 5 [Save Changes] をクリックします。

第 9 章

コミュニケーション サービスの設定

この章の構成は、次のとおりです。

HTTP の設定

操作を行う前に

HTTP を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Communication Services] をクリックします。

ステップ 3 [HTTP Properties] 領域で、次のプロパティを更新します。

名前	説明
[HTTP/S Enabled] チェックボックス	HTTP および HTTPS が CIMC でイネーブルかディセーブルか。
[HTTP Port] フィールド	HTTP 通信に使用するポート。 デフォルトは 80 です。
[HTTPS Port] フィールド	HTTPS 通信に使用するポート。 デフォルトは 443 です。

名前	説明
[Session Timeout] フィールド	HTTP 要求の間、CIMC がタイム アウトしてセッションを終了するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 1,800 秒です。
[Max Sessions] フィールド	CIMC で許可されている HTTP および HTTPS の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている HTTP および HTTPS セッションの数。

ステップ 4 [Save Changes] をクリックします。

SSH の設定

操作を行う前に

SSH を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Communication Services] をクリックします。

ステップ 3 [SSH Properties] 領域で、次のプロパティを更新します。

名前	説明
[SSH Enabled] チェックボックス	SSH が CIMC でイネーブルかディセーブルか。
[SSH Port] フィールド	セキュア シェル アクセスに使用するポート。 デフォルトは 22 です。
[SSH Timeout] フィールド	SSH要求がタイムアウトしたものとシステムが判断するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 1,800 秒です。

名前	説明
[Max Sessions] フィールド	CIMC で許可されている SSH の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている SSH セッションの数。

ステップ 4 [Save Changes] をクリックします。

IPMI Over LAN

IPMI では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。 このサービス プロセッサは Baseboard Management Controller（BMC; ベースボード管理コントローラ）と呼ばれ、サーバのマザーボードに存在します。 BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。

通常動作の間、IPMI は、サーバのオペレーティング システムがシステム ヘルスについての情報を取得し、システムのハードウェアを制御できるようにします。 たとえば、IPMI を使用すると、温度、ファンの速度、および電圧などのセンサーをモニタして、問題を事前に検出できます。 サーバの温度が指定されているレベルより高くなった場合、サーバのオペレーティング システムは BMC に対して、ファンの速度を上げたり、プロセッサの速度を下げたりして問題に対処するよう指示できます。

IPMI over LAN の設定

IPMI over LAN は、CIMC を IPMI メッセージで管理する場合に設定します。

操作を行う前に

IPMI over LAN を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Communication Services] をクリックします。

ステップ 3 [IPMI over LAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	このサーバで IMPI アクセスが許可されているか、許可されていないか。

名前	説明
[Privilege Level Limit] ドロップダウン リスト	IPMI を使用してシステムにアクセスするユーザに割り当てる必要のあるユーザ ロール。 ここに指定できる値は次のとおりです。 • [read-only]：このユーザは情報を表示できますが、変更することはできません。 • [user]：このユーザは次のことが可能です。 ◦すべての情報を表示する ◦電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する ◦KVM コンソールと仮想メディアを起動する ◦すべてのログをクリアする ◦ロケータ LED を切り替える • [admin]：このユーザは、GUI、CLI、IPMI で可能なすべての処理を実行できます。 （注） このフィールドの値は、ログインを試みるユーザに割り当てられているロールと正確に一致する必要があります。 たとえば、このフィールドを [read-only] に設定し、admin ロールを持つユーザが IPMI を使用してログインを試みると、ログインできません。
[Encryption Key] フィールド	IMPI 通信に使用する IMPI 暗号キー。

ステップ 4 [Save Changes] をクリックします。

第 10 章

証明書の管理

この章の構成は、次のとおりです。

サーバ証明書の管理

Certificate Signing Request（CSR; 証明書署名要求）を生成して新しい証明書を取得し、新しい証明書を CIMC にアップロードして現在のサーバ証明書と交換することができます。 サーバ証明書は、Verisign のようなパブリック Certificate Authority（CA; 認証局）、または独自に使用している認証局のいずれかによって署名されます。

手順

	コマンドまたはアクション	目的
ステップ 1	CIMC から CSR を生成します。	
ステップ 2	証明書の発行と署名を行う認証局に CSR ファイルを送信します。 組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。	

	コマンドまたはアクション	目的
ステップ 3	新しい証明書を CIMC にアップロードします。	（注） アップロードされた証明書は、CIMC によって生成された CSR から作成される必要があります。 この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

操作を行う前に

証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

ステップ 3 [Actions] 領域で、[Generate New Certificate Signing Request] リンクをクリックします。
[Generate New Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 4 [Generate New Certificate Signing Request] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[Common Name] フィールド	CIMC の完全修飾ホスト名
[Organization Name] フィールド	証明書を要求している組織
[Organization Unit] フィールド	組織ユニット
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町
[State Name] フィールド	証明書を要求している会社の本社が存在する州または行政区分
[Country Code] ドロップダウンリスト	会社が存在している国
[Email] フィールド	会社の電子メールの連絡先。

ステップ 5 [Generate CSR] をクリックします。

[Opening csr.txt] ダイアログボックスが表示されます。

ステップ 6 CSR ファイル csr.txt を管理するには、次のいずれかの手順を実行します。

a) [Open With] をクリックして csr.txt を表示します。

b) [Save File] をクリックしてから [OK] をクリックし、ローカル マシンに csr.txt を保存します。

次の手順

証明書の発行と署名を行う認証局にCSRファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

自己署名証明書の作成

パブリック Certificate Authority（CA; 認証局）を使用してサーバ証明書の生成と署名を行う代わりに、独自のCAを運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。 OpenSSL の詳細については、 http://www.openssl.org を参照してください。

（注） これらのコマンドは、CIMC CLI ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

操作を行う前に

組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* **例:** `# openssl genrsa -out ca.key 1024`	このコマンドは、CA で使用される RSA 秘密鍵を生成します。 （注） ユーザ入力なしで CA が鍵にアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA 鍵が含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename*	このコマンドは、指定された鍵を使用して、CA の自己署名証明書を新規に作成します。 証明書は指定された期間有効になります。 このコマンドは、

	コマンドまたはアクション	目的
	例: `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例: `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL コンフィギュレーション ファイルに追加します。 この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL コンフィギュレーション ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** 例: `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。 サーバ証明書は、出力ファイルに含まれています。

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。 これらのコマンドは、OpenSSL を実行している Linux サーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 1024 Generating RSA private key, 1024 bit long
modulus .............++++++ .....++++++ e is 65537 (0x10001) # /usr/bin/openssl
 req -new -x509 -days 365 -key ca.key -out ca.crt You are about to be asked to enter
information that will be incorporated into your certificate request. What
 you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank For some fields
 there will be a default value, If you enter '.', the field will be left
 blank. ----- Country Name (2 letter code) [GB]:US State or Province Name
 (full name) [Berkshire]:California Locality Name (eg, city) [Newbury]:San
Jose Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A Common Name (eg, your name
 or your server's hostname) []:example.com Email Address []:admin@example.com
 # echo "nsCertType = server" > openssl.conf # /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt
 -set_serial 01 -CAkey ca.key -out server.crt -extfile openssl.conf Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com Getting CA Private Key #
```

次の手順

新しい証明書を CIMC にアップロードします。

サーバ証明書のアップロード

操作を行う前に

証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。

アップロードする証明書ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。

（注） [CIMC Certificate Management] メニューを使用して最初に CSR を生成してから、その CSR を使用してアップロードする証明書を取得する必要があります。 この方法で取得されていない証明書はアップロードしないでください。

手順

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

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

ステップ 3 [Actions] 領域で、[Upload Server Certificate] をクリックします。
[Upload Certificate] ダイアログボックスが表示されます。

ステップ 4 [Upload Certificate] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[File] フィールド	アップロードする証明書ファイル。
[Browse] ボタン	適切な証明書ファイルに移動できるダイアログボックスが表示されます。

ステップ 5 [Upload Certificate] をクリックします。

第 11 章

プラットフォームイベントフィルタの設定

この章の構成は、次のとおりです。

プラットフォーム イベント フィルタ

Platform Event Filter（PEF; プラットフォーム イベント フィルタ）は、アクションをトリガしたり、ハードウェア関連の重要なイベントが発生したときはアラートを生成したりできます。 PEF ごとに、プラットフォーム イベントが発生したときに実行するアクション（またはアクションを実行しないこと）を選択できます。また、プラットフォームイベントが発生したときにアラートを生成して送信することもできます。アラートは SNMP トラップとして送信されるので、アラートを送信するには、先に SNMP トラップの宛先を設定する必要があります。

プラットフォームイベントアラートの生成はグローバルにイネーブルまたはディセーブルにできます。 ディセーブルにすると、PEF がアラートを送信するように設定されていても、アラートは送信されません。

プラットフォーム イベント アラートのイネーブル化

操作を行う前に

プラットフォーム イベント アラートをイネーブルするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Event Management] をクリックします。
ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。
ステップ 4 [Platform Event Alerts] 領域で、[Enable Platform Event Alerts] チェックボックスをオンにします。
ステップ 5 [Save Changes] をクリックします。

プラットフォーム イベント アラートのディセーブル化

操作を行う前に

プラットフォーム イベント アラートをディセーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Event Management] をクリックします。
ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。
ステップ 4 [Platform Event Alerts] 領域で、[Enable Platform Event Alerts] チェックボックスをオフにします。
ステップ 5 [Save Changes] をクリックします。

プラットフォーム イベント フィルタの設定

操作を行う前に

プラットフォーム イベント フィルタを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Event Management] をクリックします。
ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。
ステップ 4 [Platform Event Filters] 領域で、各イベントの次のフィールドに入力します。

名前	説明
[ID] カラム	一意のフィルタ ID。
[Event] カラム	イベント フィルタの名前。
[Action] カラム	フィルタごとに、目的の処理をスクロール リスト ボックスから選択します。 ここに指定できる値は次のとおりです。 • [None]：アラートは送信されますが、他の処理は実行されません • [Reboot]：アラートが送信され、サーバを再起動します • [Power Cycle]：アラートが送信され、サーバの電源を再投入します • [Power Off]：アラートが送信され、サーバの電源をオフにします
[Send Alert] カラム	アラートを送信するフィルタごとに、このカラムの対応するチェックボックスを選択します。 （注） アラートを送信するには、フィルタ トラップの設定を正しく設定し、[Enable Platform Event Alerts] チェックボックスもオンにする必要があります。

ステップ 5 [Save Changes] をクリックします。

次の手順

PEF を設定してアラートを送信する場合は、次のタスクを完了させます。

- プラットフォーム イベント アラートのイネーブル化, 61 ページ
- SNMP トラップ設定の指定, 63 ページ

SNMP トラップ設定の指定

操作を行う前に

NIC を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Event Management] をクリックします。

ステップ 3 [Event Management] ペインの [Trap Settings] タブをクリックします。

ステップ 4 [SNMP Community] 領域で、トラップ情報の送信先となる SNMP コミュニティの名前を入力します。

ステップ 5 [Trap Destinations] 領域で、次のフィールドに入力します。

名前	説明
[ID] カラム	トラップの宛先 ID。 この値は変更できません。
[Enabled] カラム	使用する SNMP トラップの宛先ごとに、このカラムの対応するチェックボックスをオンにします。
[Trap Destination IP Address] カラム	SNMP トラップ情報の送信先の IP アドレス。

ステップ 6 [Save Changes] をクリックします。

第 12 章

CIMC ファームウェア管理

この章の構成は、次のとおりです。

ファームウェアの概要

C シリーズ サーバは、cisco.com からダウンロードされたファームウェアを使用します。このファームウェアでは、C シリーズ サーバのファームウェアをアップグレードすることがシスコによって認可されています。

ダウンロードするファームウェアは、.zip ファイルにパッケージ化されています。 シスコからファームウェアの .zip ファイルをダウンロードした後、これを使用してサーバのファームウェアを更新することができます。また、シスコでは各イメージのリリース ノートも提供しており、イメージを取得したのと同じ Web サイトから入手できます。

警告 .zip ファイルを使用してサーバの再イメージ化を行わないでください。

再イメージ化には .bin ファイルを使用します。 この .zip ファイルから適切な .bin アップグレード ファイルを展開する必要があります。 この .bin ファイルは、TFTP サーバまたはローカル マシンに展開できます。 ブラウザ経由の CIMC ファームウェアのインストール，68 ページまたはTFTP サーバからの CIMC ファームウェアのインストール，67 ページで参照したように、再イメージ化は TFTP サーバまたはローカル マシンのブラウザを使用して行うことができます。

（注） ファームウェアを更新するときは、古いバージョンのファームウェアを新しいバージョンのファームウェアにアップグレードすることも、新しいバージョンのファームウェアを古いバージョンのファームウェアにダウングレードすることもできます。

CIMC は、サーバの実行中にアップタイムに影響を与えることなくファームウェアをコンポーネントにインストールできるように、ファームウェアの更新プロセスを段階的に分けています。 アクティブにするまでサーバを再起動する必要がないため、夜間やその他のメンテナンス期間にこのタスクを実行することができます。 ファームウェアの更新は、次の段階で行われます。

インストール

この段階では、CIMC は選択されたファームウェア バージョンをサーバに転送します。 インストールプロセスでは、サーバ上の非アクティブ スロット内のファームウェアが常に上書きされます。 ファームウェアは次のいずれかの方法でインストールできます。

- ブラウザ クライアント経由：コンピュータ上でファームウェア イメージを参照し、サーバにインストールすることができます。
- TFTP サーバから：TFTP サーバにあるファームウェア イメージをインストールできます。

アクティブ化

この段階では、CIMC は非アクティブのファームウェア バージョンをアクティブとして設定し、サーバを再起動します。 サーバを再起動すると、非アクティブ スロットはアクティブ スロットになり、アクティブ スロットは非アクティブ スロットになります。 新規のアクティブ スロット内のファームウェアが、実行中のバージョンとなります。

シスコからの CIMC ファームウェアの取得

手順

ステップ 1 cisco.com に移動します。

ステップ 2 最上部のツールバーで、[Support] をクリックし、ドロップダウン メニューから [Software Download] を選択します。

ステップ 3 左下隅にある [Unified Computing] リンクをクリックしてからログインします。

ステップ 4 [Cisco C-Series Rack-Mount Servers] ノードを展開します。
次のリンクが表示されます。

- Cisco UCS C250 M1 Extended-Memory Rack-Mount Server
- Cisco UCS C210 M1 General-Purpose Rack-Mount Server
- Cisco UCS C200 M1 High-Density Rack-Mount Server

ステップ 5 適切なリンクをクリックします。

ステップ 6 [Unified Computing System (UCS) Integrated Management Controller Firmware] リンクをクリックしてから、適切なリリース バージョンのリンクをクリックします。

ステップ 7 [Download Now] をクリックします。
[Download Cart] ダイアログボックスが表示されます。

ステップ 8 [Download Cart] ダイアログボックスの情報を確認してから、[Proceed with Download] をクリックします。
[Software Download Rules] ページが表示されます。

ステップ 9 ダウンロード ルールを確認してから、[Agree] をクリックします。
ダウンロード内容を示すダイアログボックスが表示されます。 [Select Location] ダイアログボックスも表示されます。 このダイアログボックスにフォーカスが置かれます。

ステップ 10 [Select Location] ダイアログボックスで場所を選択し、[Open] をクリックします。
ダウンロードが開始します。

ステップ 11 ダウンロードが終了したら、[Close] をクリックします。
ダウンロードしたファイルは、.zip ファイルです。

警告 .zip ファイルを使用してサーバの再イメージ化を行わないでください。

再イメージ化には .bin ファイルを使用します。 この .zip ファイルから適切な .bin アップグレード ファイルを展開する必要があります。 この .bin ファイルは、TFTP サーバまたはローカル マシンに展開できます。 ブラウザ経由の CIMC ファームウェアのインストール, 68 ページまたはTFTP サーバからの CIMC ファームウェアのインストール, 67 ページで参照したように、再イメージ化は TFTP サーバまたはローカル マシンのブラウザを使用して行うことができます。

展開した適切な .bin ファイルの名前は、再イメージ化しているモデル サーバによって異なります。 1.0.2 ファームウェアの更新ファイルの例を次のとおりです。

- C200 および C210：upd-pkg-c200-m1-cimc.full.1.0.2.bin
- C250：upd-pkg-c250-m1-cimc.full.1.0.2.bin

次の手順

CIMC ファームウェアをサーバにインストールします。

TFTP サーバからの CIMC ファームウェアのインストール

操作を行う前に

- ブラウザ経由で CIMC ファームウェアをインストールするには、admin 権限を持つユーザとしてログインする必要があります。
- シスコから CIMC の .zip ファームウェア ファイルを取得します。

- TFTP サーバで、適切な .bin アップグレード ファイルを解凍します。

手順

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

ステップ 2 [Admin] タブの [Firmware Management] をクリックします。

ステップ 3 [Actions] 領域で、[Install CIMC Firmware from TFTP Server] をクリックします。

ステップ 4 [Install Firmware] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[TFTP Server IP Address] フィールド	ファームウェア イメージが存在する TFTP サーバの IP アドレス。
[Image Path and Filename] フィールド	サーバ上のファームウェア イメージ ファイルの名前。 この名前を入力するときは、イメージ ファイルの相対パスを、TFTP ツリーの最上位からファイルの場所まで含めてください。

ステップ 5 [Install Firmware] をクリックします。

次の手順

CIMC ファームウェアをアクティブにします。

ブラウザ経由の CIMC ファームウェアのインストール

操作を行う前に

- ブラウザ経由で CIMC ファームウェアをインストールするには、admin 権限を持つユーザとしてログインする必要があります。
- シスコから CIMC の .zip ファームウェア ファイルを取得します。
- ローカル マシンで、適切な .bin アップグレード ファイルを解凍します。

手順

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

ステップ 2 [Admin] タブの [Firmware Management] をクリックします。

ステップ 3 [Actions] 領域で、[Install CIMC Firmware through Browser Client] をクリックします。

ステップ 4 [Install Firmware] ダイアログボックスで、次のいずれかの操作を実行します。

- [Browse] をクリックし、[Choose File] ダイアログボックスを使用してインストールする .bin ファイルを選択します。
- インストールするファームウェア イメージのフル パスとファイル名を入力します。

ステップ 5 [Install Firmware] をクリックします。

次の手順

CIMC ファームウェアをアクティブにします。

インストールされているファームウェアのアクティブ化

操作を行う前に

- ファームウェアをアクティブにするには、admin 権限を持つユーザとしてログインする必要があります。
- CIMC ファームウェアをサーバにインストールします。

手順

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

ステップ 2 [Admin] タブの [Firmware Management] をクリックします。

ステップ 3 [Actions] 領域で、[Activate CIMC Firmware] をクリックします。
[Activate Firmware] ダイアログボックスが表示されます。

ステップ 4 [Activate Firmware] ダイアログボックスで、アクティブにするファームウェア イメージを選択します。

ステップ 5 [Activate Firmware] をクリックします。

第 13 章

ログの表示

この章の構成は、次のとおりです。

CIMC Log

CIMC ログの表示

手順

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

ステップ 2 [Admin] タブの [CIMC Log] をクリックします。

ステップ 3 ログの CIMC イベントごとに次の情報を確認します。

名前	説明
[Timestamp] カラム	イベントが発生した日時。
[Source] カラム	イベントをログに記録したソフトウェア モジュール。
[Description] カラム	イベントの説明。

ステップ 4 [Entries Per Page] ドロップダウン リストから、各ページに表示する CIMC イベントの数を選択します。

ステップ 5 CIMC イベントのページを前方および後方に移動するには [<Newer] および [Older>] をクリックし、リストの先頭に移動するには [<<Newest] をクリックします。
デフォルトでは、最新の CIMC イベントがリストの先頭に表示されます。

CIMC ログのクリア

操作を行う前に

CIMC ログをクリアするには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [CIMC Log] をクリックします。
ステップ 3 [CIMC Log] ペインで、[Clear Log] をクリックします。
ステップ 4 表示されるダイアログボックスで [OK] をクリックします。

System Event Log

システム イベント ログの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [System Event Log] をクリックします。
ステップ 3 ログのシステム イベントごとに次の情報を確認します。

名前	説明
[Timestamp] カラム	イベントが発生した日時。
[Severity] カラム	イベントの重大度。 ここに指定できる値は次のとおりです。 • **Unknown** • **Informational** • **Normal** • **Warning** • **Critical** • **Non-Recoverable**

名前	説明
[Description] カラム	イベントの説明。

ステップ 4 （オプション） [Entries Per Page] ドロップダウン リストから、各ページに表示するシステム イベントの数を選択します。

ステップ 5 （オプション） システム イベントのページを前方および後方に移動するには [<Newer] および [Older>] をクリックし、リストの先頭に移動するには [<<Newest] をクリックします。
デフォルトでは、最新のシステム イベントがリストの先頭に表示されます。

システム イベント ログのクリア

操作を行う前に

システムイベントログをクリアするには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [System Event Log] をクリックします。

ステップ 3 [System Event Log] ペインで、[Clear Log] をクリックします。

ステップ 4 表示されるダイアログボックスで [OK] をクリックします。

第 14 章

サーバ ユーティリティ

この章の構成は、次のとおりです。

テクニカル サポート データのエクスポート

このタスクは、Cisco Technical Assistance Center（TAC）から要求された場合に実行します。 このユーティリティは、TAC が技術上の問題をトラブルシューティングおよび解決する際に役立つ設定情報、ログ、および診断データが含まれる要約レポートを作成します。

手順

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

ステップ 2 [Admin] タブの [Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export Technical Support Data] をクリックします。

ステップ 4 [Export Technical Support Data] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[TFTP Server IP Address] フィールド	サポート データ ファイルを保存する必要のある TFTP サーバの IP アドレス。
[Path and Filename] フィールド	サーバでサポート データを保存する必要のあるファイルの名前。 この名前を入力するときは、ファイルの相対パスを、TFTP ツリーの最上位から目的の場所まで含めてください。

ステップ 5 [Export] をクリックします。

次の手順

生成されたレポート ファイルを Cisco TAC に提供します。

CIMC の再起動

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMC の再起動が必要になることがあります。 この手順は、通常のサーバ メンテナンスには含まれません。 CIMC を再起動した後にログオフすると、CIMC は数分間使用できません。

（注） サーバが Power-On Self Test（POST; 電源投入時自己診断テスト）を実行しているとき、または Extensible Firmware Interface（EFI）シェルを操作しているときに CIMC を再起動すると、サーバの電源は、CIMC の再起動が完了するまでオフになります。

操作を行う前に

CIMC を再起動するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Utilities] をクリックします。
ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reboot CIMC] をクリックします。
ステップ 4 [OK] をクリックします。

破損した BIOS のリカバリ

操作を行う前に

- 破損した BIOS を回復するには、admin としてログインしている必要があります。
- BIOS リカバリ ISO イメージを準備します。 BIOS リカバリ ISO イメージは、ファームウェア配布パッケージの [Recovery] フォルダ内にあります。
- リカバリ手順の最後にサーバの電源が再投入されるため、サーバのダウンタイムをスケジュール設定します。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [BIOS] をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [Actions] 領域で、[Recover Corrupt BIOS] をクリックします。
[Recover Corrupt BIOS] ウィザードが表示されます。

ステップ 4 [Recover Corrupt BIOS] ウィザードを使用して、破損した BIOS を回復します。

CIMC の出荷時デフォルトへのリセット

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMC の出荷時デフォルトへのリセットが必要になることがあります。 これを行うと、ユーザが設定可能なすべての設定がリセットされます。

この手順は、通常のサーバ メンテナンスには含まれません。 CIMC をリセットした後は、ログオフしてから再びログインする必要があります。 また、接続が失われ、ネットワーク設定を再び指定する必要がある場合もあります。

操作を行う前に

CIMC を出荷時デフォルトにリセットするには、admin 権限を持つユーザとしてログインする必要があります。

手順

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

ステップ 2 [Admin] タブの [Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reset CIMC to Factory Default Configuration] をクリックします。

ステップ 4 [OK] をクリックします。
ホストが BIOS POST（電源投入時自己診断テスト）を実行しているとき、または EFI シェル内にあるときに CIMC を再起動すると、ホストの電源が短時間オフになります。 準備ができると、CIMC の電源はオンになります。

索 引

V

W

あ

い

お

か

き

こ

さ

し

す

せ

つ

て

ね

ふ

め

ゆ

り

ろ