Cisco UCS E シリーズ Integrated Management Controller リリース 3.2.2 GUI コンフィギュレーション ガイド

初版：2017 年 7 月 31 日

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

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

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 NONINFRINGEMENT 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.

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: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに xi

対象読者 xi

表記法 xi

関連 Cisco UCS 資料 xiii

第 1 章

概要 1

Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンの概要 1

サーバ ソフトウェア 2

Cisco Integrated Management Controller 3

Cisco IMC ユーザ インターフェイスの概要 5

Cisco IMC ホームページ 6

[ナビゲーション（Navigation）] ペインと [作業（Work）] ペイン 6

ツールバー 9

Cisco Integrated Management Controller オンライン ヘルプの概要 9

Cisco IMC へのログイン 9

Cisco IMC からのログアウト 10

第 2 章

サーバのオペレーティング システムまたはハイパーバイザのインストール 11

オペレーティング システムまたはハイパーバイザのインストール方法 11

KVM コンソール 12

PXE インストール サーバ 13

PXE インストール サーバを使用したオペレーティング システムまたはハイパーバイザのインストール 13

カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード 14

ホスト イメージ マッピング 15
ホスト イメージのマッピング 15
ホスト イメージのマッピング解除 17
ホスト イメージの削除 18

第 3 章 シャーシの管理 19
シャーシ要約 19
シャーシ サマリーの表示 19
サーバ アセット タグの作成 22
シャーシ インベントリ 22
電源のプロパティの表示 22
ストレージのプロパティの表示 23
ネットワーク アダプタのプロパティの表示 24
シャーシ センサーの表示 24
電源センサーの表示 24
温度センサーの表示 26
電圧センサーの表示 27
電流センサーの表示 27
ストレージ センサーの表示 28
障害サマリー 28
障害サマリーの表示 28
障害履歴 30
障害履歴の表示 30
Cisco IMC ログ 32
Cisco IMC ログの表示 32
システム イベント ログ 35
システム イベント ログの表示 35
ロギング制御 37
ロギング制御の表示 37
リモート サーバへの Cisco IMC ログの送信 38
Cisco IMC ログしきい値の設定 40

リモート サーバへのテスト Cisco IMC ログの送信 40

第 4 章 サーバの管理 43

BIOS の設定 43

BIOS セットアップの開始 43

主要な BIOS の設定 43

BIOS の詳細設定 44

サーバ管理 BIOS の設定 45

BIOS セットアップの開始 46

BIOS CMOS のクリア 47

BIOS の製造元カスタム設定の復元 47

サーバのブート順の管理 48

サーバのブート順 48

ブート デバイスの管理 48

UEFI セキュア ブートのイネーブル化 55

UEFI セキュア ブートのディセーブル化 55

サーバの実際のブート順の表示 56

ISRG2 でのモジュールの電力復元ポリシーの設定 57

ISR4K でのモジュールの電力復元ポリシーの設定 58

第 5 章 センサーの表示 59

シャーシ センサーの表示 59

電源センサーの表示 59

ファン センサーの表示 61

温度センサーの表示 61

電圧センサーの表示 62

電流センサーの表示 63

ストレージ センサーの表示 64

第 6 章 リモート プレゼンスの管理 65

Serial over LAN の設定 65

仮想メディアの設定 67
Cisco IMC マップされた vMedia ボリュームの作成 68
Cisco IMC マップされた vMedia ボリューム プロパティの表示 72
Cisco IMC マップされた vMedia ボリュームの削除 74
KVM コンソール 74
KVM コンソールの起動 74
仮想 KVM コンソール（HTML ベース） 75
Java ベース KVM と HTML5 ベース KVM の比較 78
仮想 KVM の設定 80
仮想 KVM のイネーブル化 81
仮想 KVM のディセーブル化 81
ホスト イメージ マッピング 82
ホスト イメージのマッピング 82
ホスト イメージのマッピング解除 84
ホスト イメージの削除 85

第 7 章 ユーザ アカウントの管理 87
ローカル ユーザの設定 87
パスワードの有効期限切れ 89
LDAP サーバ 90
LDAP サーバの設定 90
Cisco IMC での LDAP 設定およびグループ認証の設定 92
LDAP 証明書の概要 97
LDAP CA 証明書ステータスの表示 98
LDAP CA 証明書のエクスポート 98
LDAP CA 証明書のダウンロード 101
LDAP バインディングのテスト 103
LDAP CA 証明書の削除 104
ユーザ セッションの表示 104

第 8 章 シャーシ関連の設定 107

サーバの電源管理 107
Web UI からのホスト名/IP アドレスへの Ping 107
時間帯の選択 108

第 9 章 ネットワーク関連の設定 111
サーバ NIC の設定 111
サーバの NIC 111
サーバ NIC の設定 111
共通プロパティの設定 112
共通プロパティの設定の概要 112
共通プロパティの設定 113
ネットワーク セキュリティの設定 114
ネットワーク セキュリティ 114
ネットワーク セキュリティの設定 114
ネットワーク タイム プロトコルの設定 115
ネットワーク タイム プロトコル サービス設定 115
ネットワーク タイム プロトコル設定の設定 116

第 10 章 ストレージ アダプタの管理 117
ストレージ アダプタの管理 117
自己暗号化ドライブ（フル ディスク暗号化） 117
未使用の物理ドライブからの仮想ドライブの作成 118
既存のドライブ グループからの仮想ドライブの作成 121
仮想ドライブのトランスポート可能状態の設定 123
トランスポート可能としての仮想ドライブの設定 123
仮想ドライブのトランスポート可能状態の解除 124
外部設定のインポート 125
外部設定のクリア 126
ブート ドライブのクリア 126
JBOD モードのイネーブル化 127
JBOD のディセーブル化 127

コントローラのストレージ ファームウェア ログの取得 128
コントローラの設定のクリア 128
削除するドライブの準備 129
削除するドライブの準備の取り消し 129
専用ホット スペアの作成 130
グローバル ホット スペアの作成 130
ホット スペア プールからのドライブの削除 131
物理ドライブのステータスの切り替え 131
コントローラのブート ドライブとしての物理ドライブの設定 132
仮想ドライブの初期化 132
ブート ドライブとしての設定 133
仮想ドライブの編集 134
仮想ドライブの削除 136
仮想ドライブの非表示 136
バッテリ バックアップ ユニットの学習サイクルの開始 137
ストレージ コントローラのログの表示 137

第 11 章 コミュニケーション サービスの設定 139
HTTP の設定 139
SSH の設定 140
Redfish の設定 141
XML API の設定 142
Cisco IMC 用の XML API 142
XML API のイネーブル化 142
IPMI の設定 142
IPMI Over LAN 142
IPMI over LAN の設定 143
SNMP の設定 144
SNMP 144
SNMP プロパティの設定 144
SNMP トラップ設定の指定 146

テスト SNMP トラップ メッセージの送信 148
SNMP ユーザの管理 148
SNMP ユーザの設定 149

第 12 章 ファームウェアの管理 153
Cisco IMC ファームウェア 153
ファームウェア コンポーネントの表示 154
ファームウェアの更新 155
ファームウェアのアクティブ化 156

第 13 章 障害およびログの表示 159
障害サマリー 159
障害サマリーの表示 159
障害履歴 161
障害履歴の表示 161
Cisco IMC ログ 163
Cisco IMC ログの表示 163
システム イベント ログ 166
システム イベント ログの表示 166
ロギング制御 168
ロギング制御の表示 168
リモート サーバへの Cisco IMC ログの送信 169
Cisco IMC ログしきい値の設定 171
リモート サーバへのテスト Cisco IMC ログの送信 171

第 14 章 サーバ ユーティリティ 173
テクニカル サポート データのエクスポート 173
テクニカル サポート データのエクスポート 173
ローカル ファイルへのテクニカル サポート データのダウンロード 174
出荷時の初期状態へのリセット 175
Cisco IMC 設定のエクスポートとインポート 176

Cisco IMC 設定のエクスポートとインポート 176
Cisco IMC 設定のエクスポート 177
Cisco IMC 設定のインポート 179
ホストへのマスク不能割り込みの生成 181
Cisco IMC バナーの追加または更新 182
Cisco IMC の最後のリセット理由の表示 183
ローカル ファイルへのハードウェア インベントリのダウンロード 183
リモート サーバへのハードウェア インベントリ データのエクスポート 184

第 15 章 トラブルシューティング 187
最後の起動プロセスの記録 187
最後のクラッシュの記録 188
DVR Player のダウンロード 189

はじめに

この前書きは、次の項で構成されています。

- 対象読者 （xi ページ）
- 表記法 （xi ページ）
- 関連 Cisco UCS 資料 （xiii ページ）

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えた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

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールド ラベルなどの GUI 要素は、イタリック体（**italic**）で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルなどのメイン タイトルは、ボールド体（**bold**）で示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、`courier` フォントで示しています。

テキストのタイプ	説明
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、**this font**で示しています。 CLI コマンド内の変数は、イタリック体（*this font*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[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、角かっこで囲み、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。
< >	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。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

ワンポイント アドバイス 「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

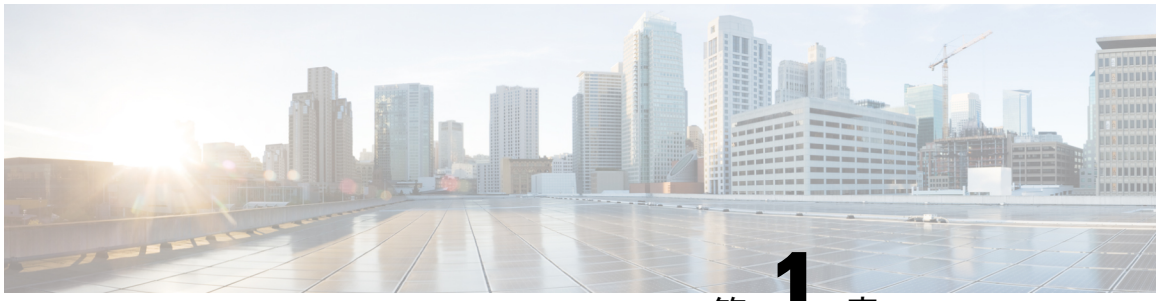
これらの注意事項を保存しておいてください

関連 Cisco UCS 資料

ドキュメント ロードマップ

すべての E シリーズ マニュアルの完全なリストについては、次の URL にある『Cisco UCS E-Series Servers Documentation Roadmap』を参照してください。
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/1-0/roadmap/e_series_road_map.html

関連 Cisco UCS 資料



第 1 章

概要

この章は、次の項で構成されています。

- Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンの概要 （1 ページ）
- サーバ ソフトウェア （2 ページ）
- Cisco Integrated Management Controller （3 ページ）
- Cisco IMC ユーザ インターフェイスの概要 （5 ページ）

Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンの概要

Cisco UCS E-Series Servers（E シリーズ サーバ）およびCisco UCS E シリーズ ネットワーク コンピュート エンジン（NCE）はサイズ、重量、電力の効率にすぐれたブレード サーバのファミリで、第 2 世代の Cisco サービス統合型ルータ（Cisco ISR G2）および Cisco ISR 4000 シリーズに搭載されています。 これらのサーバは、オペレーティング システム（Microsoft Windows や Linux など）上でベアメタルとして、あるいはハイパーバイザ（VMware vSphere Hypervisor、Microsoft Hyper-V、Citrix XenServer など）上で仮想マシンとして導入される、ブランチオフィス アプリケーション向けの汎用コンピューティング プラットフォームを提供します。

E シリーズ サーバは、汎用コンピューティングの強力な Intel Xeon プロセッサ用に特別に作られています。 また、シングル幅とダブル幅の 2 種類のフォーム ファクタがあります。 シングル幅のE シリーズ サーバは単一のサービス モジュール（SM）スロットに適しており、ダブル幅のE シリーズ サーバは 2 つの SM スロットに適しています。

NCEは価格と性能の点で最適化されたモジュールで、シスコのネットワーク アプリケーションおよび他の軽量な汎用アプリケーションをホストするようにビルドされています。これらは、SM、NIM、および EHWIC の 3 つのフォーム ファクタで提供されます。SM E シリーズ NCE は 1 つの SM スロットに、NIM E シリーズ NCE は 1 つの NIM スロットに、EHWIC E シリーズ NCE は 2 つの EHWIC スロットに収納できます。

（注）
- EHWIC E シリーズ NCE は Cisco ISR G2 のみに設置できます。
- NIM E シリーズ NCE は Cisco ISR 4000 シリーズにのみ設置できます。
- Cisco ISR 4331 には SM スロットが 1 つあります。Cisco ISR 4321 および Cisco ISR 4431 には SM スロットがありません。
- Citrix XenServer は E シリーズ サーバでのみサポートされます。
- Cisco UCS-E160S-M3/K9、UCS-E180D-M3/K9、および UCS-E1120D-M3/K9 サーバは、ISR 4000 シリーズでのみサポートされます。
- CIMC 3.2.x は EHWIC NCE ではサポートされていません。

（注） サポートされているEシリーズ サーバおよびNCEについて、また 1 つのルータあたりにインストール可能なサーバの最大数については、『*Hardware Installation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』の「Hardware Requirements」の項を参照してください。

サーバ ソフトウェア

E シリーズ サーバとNCEには、3 つの主要なソフトウェア システムが必要です。

- CIMC ファームウェア
- BIOS ファームウェア
- オペレーティング システムまたはハイパーバイザ

CIMC ファームウェア

Cisco Integrated Management Controller（CIMC）は、E シリーズ サーバまたはNCEのマザーボードに組み込まれている別の管理モジュールです。専用の ARM ベースのプロセッサが（メインサーバCPUから独立して）CIMCファームウェアを実行します。システムには、現行バージョンの CIMC ファームウェアが付属しています。CIMC ファームウェアは更新可能ですが、初期インストールは必要ありません。

CIMC はE シリーズ サーバおよびNCE用の管理サービスです。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。

BIOS ファームウェア

BIOS は、システム内のハードウェアを初期化し、ブート可能なデバイスを検出し、それらを指定された順序でブートします。オペレーティングシステムを起動したり、オペレーティング

システムが使用するハードウェアを設定したりします。使いやすい BIOS 管理機能により、ハードウェアを操作したり、使用したりできます。他にも BIOS では、システムを設定したり、ファームウェアを管理したり、BIOS エラー レポートを作成したりすることもできます。

システムには、現行バージョンの BIOS ファームウェアが付属しています。BIOS ファームウェアは更新可能ですが、初期インストールは必要ありません。

オペレーティング システムまたはハイパーバイザ

メイン サーバ CPU は Microsoft Windows や Linux などのオペレーティング システム上で、またはハイパーバイザ上で動作します。Microsoft Windows Server または VMware vSphere Hypervisor が事前にインストールされているE シリーズ サーバまたはNCEを購入することも、独自のプラットフォームをインストールすることもできます。

（注） E シリーズ サーバまたはNCEでテストされたプラットフォームについては、『『*Release Notes for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』』の「Software Requirements」の項を参照してください。

Cisco Integrated Management Controller

Cisco IMC は E シリーズ サーバ用の管理サービスです。Cisco IMC はサーバ内で実行されます。

（注） Cisco IMC 管理サービスは、サーバがスタンドアロン モードで動作している場合にだけ使用されます。E シリーズ サーバが UCS システムに統合されている場合は、UCS Manager を使用してそのサーバを管理する必要があります。UCS Manager の使用方法については、http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/1-0/roadmap/e_series_road_map.html の『*Cisco UCS E-Series Servers Documentation Roadmap*』に記載されている設定ガイドを参照してください。

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 または XML ベースの API 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。

- Cisco IMC CLI を呼び出すために Cisco IMC GUI を使用する
- Cisco IMC CLI で呼び出したコマンドを Cisco IMC GUI に表示する
- Cisco IMC GUI から Cisco IMC CLI 出力を生成する

Cisco IMC で実行可能なタスク

Cisco IMC を使用すると次のシャーシ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、SNMP 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
- Cisco IMC 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
- タイム ゾーンを設定しローカル タイムを表示する
- Cisco IMC ファームウェアをインストールしてアクティブにする
- BIOS ファームウェアをインストールしてアクティブにする
- CMC ファームウェアをインストールしてアクティブにする

Cisco IMC を使用すると次のサーバ管理タスクを実行できます。

- 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、SNMP 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
- Cisco IMC 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

- タイム ゾーンを設定しローカル タイムを表示する

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

Cisco IMC 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 Cisco IMC 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

Cisco IMC ユーザ インターフェイスの概要

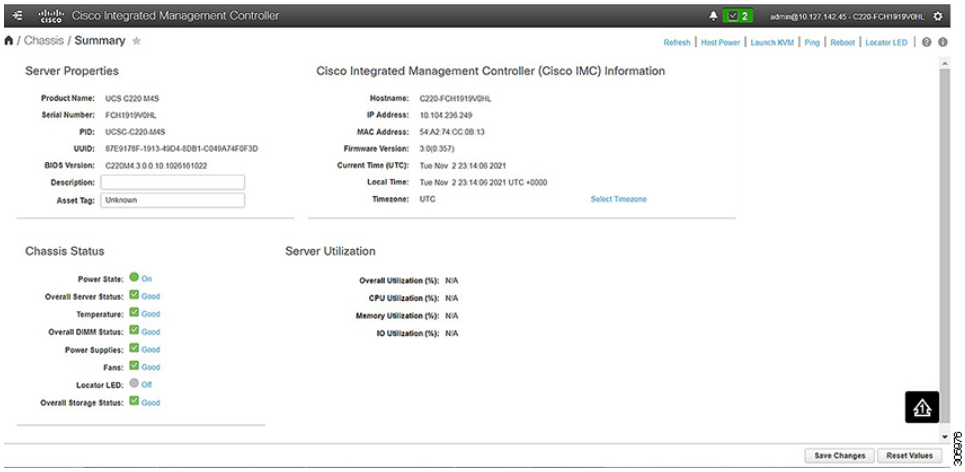
Cisco IMC ユーザ インターフェイスは、Cisco E シリーズ サーバの Web ベースの管理インターフェイスです。Web ユーザ インターフェイスは、eXtensible Widget Framework（XWT）フレームワークを使った HTML5 を使用して開発されます。ユーザ インターフェイスを起動して、次の最小要件を満たしている任意のリモート ホストからサーバを管理できます。

- Microsoft Internet Explorer 6.0 以降、Mozilla Firefox 3.0 以降
- Microsoft Windows 7、Microsoft Windows XP、Microsoft Windows Vista、Apple Mac OS X v10.6、Red Hat Enterprise Linux 5.0 以降のオペレーティング システム
- Transport Layer Security（TLS）バージョン 1.2

（注） Cisco IMC へのログインに使用するパスワードを失効した場合やパスワードを忘れた場合は、Cisco UCS E シリーズ サーバと Cisco UCS E シリーズ ネットワーク コンピュート エンジンのハードウェア インストレーション ガイドでパスワードの回復手順を参照してください。このガイドは http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/e/1-0/roadmap/e_series_road_map.html で入手できます。

Cisco IMC ホームページ

Cisco IMC GUI に初めてログインすると、次の図のようなユーザ インターフェイスが表示されます。



[ナビゲーション（Navigation）] ペインと [作業（Work）] ペイン

Cisco Integrated Management Controller GUI は、画面の左側にある [Navigation] ペインと、画面の右側にある [Work] ペインで構成されます。[Navigation] ペインの [Server]、[Chassis]、[Compute]、[Storage]、[Admin] メニューにあるリンクをクリックすると、右側の [Work] ペインに関連付けられたタブが表示されます。

[Navigation] ペインのヘッダーにはアクション ボタンが表示され、GUI 全体のナビゲーション マップを表示したり、インデックスを表示したり、お気に入りの作業ペインを選択して直接移動したりできます。[Pin] アイコンは、[Work] ペインが表示されたときに [Navigation] ペインがスライドしないようにします。

[Favorite] アイコンは星形のボタンで、アプリケーション内の特定の作業ペインをお気に入りにできます。これを行うには、選択した作業ウィンドウに移動して、[Favorite] アイコンをクリックします。アプリケーションの任意の場所からこの作業ウィンドウに直接アクセスするには、[Favorite] アイコンを再度クリックします。

GUI ヘッダーには、シャーシの全体的なステータスに関する情報およびユーザ ログイン情報が表示されます。

GUI ヘッダーには、障害の総数（緑色または赤色で示されます）も表示され、その横に [Bell] アイコンが付いています。ただし、このアイコンをクリックすると、さまざまなコンポーネントの致命的または重大な障害の概要のみが表示されます。すべての障害を表示するには、[すべて表示（View All）] ボタンをクリックして [障害サマリー（Fault Summary）] ペインを表示させます。

（注） ユーザ インターフェイスのオプションは、サーバによって異なります。

[ナビゲーション（Navigation）] ペインには次のメニューがあります。

- [Chassis] メニュー
- [Compute] メニュー
- [Storage] メニュー
- [Admin] メニュー

[Chassis] メニュー

[Chassis] メニューの各ノードは、[Work] ペインに表示される 1 つ以上のタブに続きます。これらのタブからは次の情報へアクセスできます。

[Chassis] メニューのノード名	[Work] ペインのタブで提供される情報
Inventory	サーバ、電源、Cisco VIC アダプタ、ダイナミック ストレージの管理情報。
Sensor	電源、ファン、温度、電圧、電流、LED の読み取り。
Faults and Logs	障害サマリー、障害履歴、システムイベント ログ、Cisco IMC ログおよびロギング制御。

[Compute] メニュー

[Compute] メニューにはサーバに関する情報が含まれており、次の情報が [Work] ペインに表示されます。

[Compute] メニューのノード名	[Work] ペインのタブで提供される情報
Inventory	インストール済みの CPU、メモリ カード、PCI アダプタ、Cisco VIC アダプタ、vNIC、ストレージ、信頼されたプラットフォーム モジュール（TPM）。
BIOS	インストール済みの BIOS ファームウェア バージョン、およびサーバのブート順。
Remote Management	LAN 設定上の KVM、仮想メディア、およびシリアル。
トラブルシューティング	ブートストラップ処理、クラッシュ レコーディング、最後に保存したブートストラップ プロセスを表示するプレーヤー。
Power Policies	電源復元ポリシーの設定。

[Compute] メニューのノード名	[Work] ペインのタブで提供される情報
ホスト イメージ マッピング	ホスト イメージのマッピング情報。

[Storage] メニュー

[Storage] メニューの各ノードは、Cisco UCS E シリーズ ラックマウント サーバにインストールされた LSI MegaRAID コントローラに対応します。各ノードは、[Work] ペインに表示される 1 つ以上のタブに続き、インストールされているコントローラに関する情報を提供します。

[Storage] メニューのノード名	[Work] ペインのタブで提供される情報
[コントローラ情報（Controller Info）]	選択した LSI MegaRAID コントローラに関する一般情報。
[物理ドライブ情報（Physical Drive Info）]	一般的なドライブ情報、識別情報、およびドライブのステータス。
Virtual Drive Info	一般的なドライブ情報、RAID 情報、物理ドライブ情報。
Battery Backup Unit	選択された MegaRAID コントローラのバックアップ バッテリ情報。
Storage Log	ストレージ メッセージ。

[Admin] メニュー

[Admin] メニューの各ノードは、[Work] ペインに表示される 1 つ以上のタブに続きます。これらのタブからは次の情報へアクセスできます。

[Admin] メニューのノード名	[Work] ペインのタブで提供される情報
User Management	ローカルで定義されたユーザ アカウント、Active Directory 設定、および現在のユーザ セッション情報。
Networking	NIC、IPv4、IPv6、VLAN、LOM プロパティとネットワーク セキュリティおよび NTP 設定。
通信サービス	HTTP、XML API、SSH、Redfish、IPMI over LAN、および SNMP 設定。
Certificate Management	セキュリティ証明書情報と管理。
イベント管理	プラットフォーム イベント管理。
Firmware Management	Cisco IMC および BIOS ファームウェア情報と管理。
ユーティリティ	テクニカル サポート データ収集、システム設定のインポートおよびエクスポート オプション、出荷時の初期状態の復元設定。

ツールバー

ツールバーは [Work] ペインの上に表示されます。

ボタン名	説明
[更新（Refresh）]	現在のページを更新します。
Host Power	表示されるドロップダウン メニューから電源オプションを選択します。
Launch KVM	Java ベースまたは HTML ベースの KVM コンソールを起動するためのドロップダウン メニューが表示されます。
ping	[Ping Details] ポップアップ ウィンドウを起動します。
Reboot	Cisco IMC をリブートできます。

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

Cisco Integrated Management Controller（Cisco IMC）ソフトウェアの GUI は、左側にある [Navigation] ペインと右側にある [Work] ペインの 2 つの主要なセクションに分かれます。

このヘルプ システムは、各 Cisco IMC 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。

ページのヘルプにアクセスするには、次のいずれかを実行します。

- Cisco IMC GUI の特定のタブで、[Work] ペインの上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。

Cisco IMC へのログイン

始める前に

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、Cisco IMC への 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) （任意）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。

ヒント　未設定のシステムに対する初回ログイン時には、ユーザ名に **admin**、パスワードに **password** を使用します。

Web UI に初めてログインする際、次のようになります。

- Cisco IMC Web UI または CLI でデフォルトの管理者クレデンシャルを変更するまでは、操作を実行できません。
- パスワードの変更ポップアップ ウィンドウを閉じたりキャンセルしたりすることはできません。UI をタブで開くか、ブラウザ ページを更新すると、ポップアップ ウィンドウが引き続き表示されます。このポップアップ ウィンドウは、初期設定のリセット後にログインすると表示されます。
- 新しいパスワードとして単語「password」を選択することはできません。実行するスクリプトでこの制限が問題になる場合は、ユーザ管理オプションに再びログインしてパスワードを password に変更できますが、これに伴うリスクは完全に自分の責任となります。シスコでは推奨していません。

ステップ 4 [Log In] をクリックします。

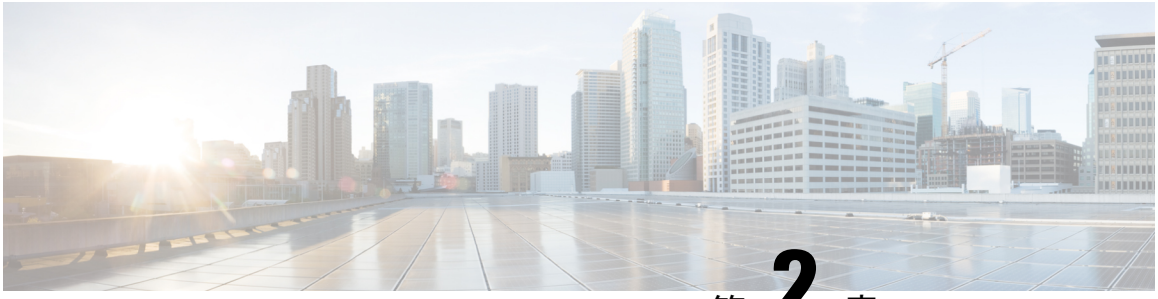
Cisco IMC からのログアウト

手順

ステップ 1 Cisco IMC の右上で、[**Log Out**] をクリックします。

ログアウトすると、Cisco IMC のログイン ページに戻ります。

ステップ 2 （任意） 再度ログインするか、Web ブラウザを閉じます。



第 2 章

サーバのオペレーティング システムまたはハイパーバイザのインストール

この章は、次の項で構成されています。

- オペレーティング システムまたはハイパーバイザのインストール方法 （11 ページ）
- KVM コンソール （12 ページ）
- PXE インストール サーバ （13 ページ）
- ホスト イメージ マッピング （15 ページ）

オペレーティングシステムまたはハイパーバイザのインストール方法

E シリーズ サーバおよびNCEは複数のオペレーティング システムとハイパーバイザをサポートします。インストールされるプラットフォームに関係なく、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
- ホスト イメージ マッピング

注意 仮想ドライブをマップするには 1 種類だけを使用する必要があります。たとえば、KVM コンソールまたは Host Image Mapping のいずれかを使用します。組み合わせて使用すると、サーバが未定義の状態になります。

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（ISO または IMG ファイル）
- コンピュータ上の USB フラッシュ ドライブ

KVM コンソールを使用して、サーバにオペレーティング システムまたはハイパーバイザをインストールし、次の作業を行うことができます。

- 起動中に F2 を押して、BIOS セットアップ メニューにアクセスします。
- 起動中に F8 を押して、CIMC 設定ユーティリティにアクセスします。

（注） CIMC Configuration Utility は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

- Cisco UCS M1 および M2 サーバの場合は、ブートアップ中に **Ctrl+H** を押し、WebBIOS にアクセスして RAID を設定します。

  Cisco UCS M3 サーバの場合は、ブートアップ中に **Ctrl+R** を押し、MegaRAID コントローラにアクセスして RAID を設定します。

（注） RAID は EHWIC E シリーズ NCE および NIM E シリーズ NCE ではサポートされていません。これらの SKU では、**Ctrl+H** および **Ctrl+R** は機能しません。

KVM コンソールを起動するための Java 要件

KVM コンソールを起動するためには、システムにリリース 1.6 以降の Java をインストールしておく必要があります。

証明書が Java で取り消しされたために KVM コンソールが起動しない場合は、Java の設定を変更する必要があります。次の手順を実行します。

1. Java コントロール パネルにアクセスします。

2. [Advanced] タブをクリックします。
3. [Perform certificate revocation on] で、[Do not check (not recommended)] ラジオ ボタンを選択します。詳細については、http://www.java.com/en/download/help/revocation_options.xmlを参照してください。

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オペレーティング システムまたはハイパーバイザ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、サーバにオペレーティング システムまたはハイパーバイザ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、オペレーティング システムまたはハイパーバイザ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、プラットフォーム、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、多数のサーバにプラットフォーム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オペレーティング システムまたはハイパーバイザのインストール

始める前に

VLAN 経由でサーバに到達できることを確認します。

手順

ステップ 1 ブート順を [PXE] に設定します。
ステップ 2 サーバをリブートします。

注意 共有 LOM インターフェイスを使用して CIMC にアクセスしている場合は、サーバのリブート プロセス中に CIMC GUI を使用しないでください。CIMC GUI を使用すると、イーサネット ポートに設定されていた IP アドレスがブート エージェントによってオーバーライドされるため、PXE のインストール中に GUI の接続が解除されます。

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オペレーティング システムまたはハイパーバイザのインストレーション ガイドを参照してください。

次のタスク

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。

カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード

手順

ステップ 1 https://my.vmware.com/web/vmware/login にアクセスします。

VMware ログイン ページが表示されます。

ステップ 2 自分の VMware クレデンシャルを入力し、[Log In] をクリックします。

VMware のアカウントがない場合は、[Register] をクリックして無料アカウントを作成します。

ステップ 3 [Downloads] をクリックし、ドロップダウン リストから [All Products] を選択します。

ステップ 4 必要に応じて、次のいずれかを実行します。

- VMware vSphere Hypervisor 5.1 イメージをダウンロードするには、[Search] フィールドで **ESXi-5.1.0-799733-custom-Cisco-2.1.0.3.iso** と入力し、[Search] アイコンをクリックします。[Search Results] から [VMware vSphere] > [Drivers & Tools] > [Cisco Custom Image for ESXi 5.1.0 GA Install CD] をクリックし、[Download] をクリックします。
- VMware vSphere Hypervisor 5.5 イメージをダウンロードするには、[Search] フィールドで **ESXi-5.5.0-1331820-custom-Cisco-5.5.0.1.iso** と入力し、[Search] アイコンをクリックします。[Search Results] から [VMware vSphere] > [Drivers & Tools] > [CISCO Custom Image for ESXi 5.5.0 GA Install CD] をクリックし、[Download] をクリックします。

次のタスク

VMware vSpere Hypervisor のイメージをインストールします。

ホスト イメージ マッピング

ホストイメージマッピング機能を使用すると、ホストイメージのダウンロード、マッピング、マッピング解除、または削除を行うことができます。Microsoft Windows、Linux、VMware などのホスト イメージを、リモート FTP または HTTP サーバから CIMC 内部リポジトリにダウンロードしてから、E シリーズ サーバまたはNCE内の USB コントローラの仮想ドライブにマップします。イメージをマップした後は、イメージをマウントした仮想ドライブが最初のブートデバイスになるようにブート順序を設定してから、サーバをリブートします。ホストイメージはファイル拡張子として .iso または .img がなければなりません。

また、ホスト イメージ マッピング機能により、診断イメージをダウンロードし、マウントできます。診断イメージのファイル拡張子は必ず .diag になります。

ホスト イメージのマッピング

始める前に

- admin 権限を持つユーザとして CIMC にログインします。
- 適切なサードパーティからホスト イメージ ファイルを取得します。

（注） VMware vSphere Hypervisor ではカスタマイズしたイメージが必要です。カスタマイズされたイメージをダウンロードするには、カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード （14 ページ）を参照してください。

（注） アップデートがすでに処理中であるときにイメージアップデートを開始すると、どちらのアップデートも失敗します。

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 3 [Host Image Mapping] ページで、[Add Image] をクリックします。

[Add New Mapping] ダイアログボックスが表示されます。次のフィールドに入力します。

名前	説明
[Server Type] ドロップダウン リスト	イメージが配置されているリモート サーバのタイプ。次のいずれかになります。 • **FTP** • **FTPS** • **HTTP** • **HTTPS** （注） 選択したリモート サーバによって、表示されるフィールドが変わります。
[Server IP Address] フィールド	リモート FTP または HTTP サーバの IP アドレス。
[File Path] フィールド	リモート FTP または HTTP サーバのパスおよびファイル名。 パスワードには、最大 80 文字を使用できます。 • ホスト イメージをインストールする場合、そのイメージのファイル拡張子は必ず .iso または .img になります。 • 診断イメージをインストールする場合、そのイメージのファイル拡張子は必ず .diag になります。
[Username] フィールド	リモート サーバのユーザ名。 ユーザ名は 1～20 文字の範囲で指定します。 （注） ユーザ名を設定しない場合は、ユーザ名として **anonymous** を入力し、パスワードとして任意の文字を入力します。
[Password] フィールド	ユーザ名のパスワード。 パスワードは 1～20 文字の範囲で指定します。 （注） ユーザ名を設定しない場合は、ユーザ名として **anonymous** を入力し、パスワードとして任意の文字を入力します。

ステップ 4 [Download] をクリックします。

[Host Image Mapping] ページが開きます。[Host Image Mapping Status] 領域で、イメージ ダウンロードのステータスを表示できます。イメージが正常にダウンロードされ、処理された後、ページがリフレッシュされます。ページがリフレッシュされた後、新しいイメージが [Image Information] 領域に表示されます。

ステップ 5 [Image Information] 領域で、マップするイメージを選択し、[Map Selected Image] をクリックします。

イメージがマップされ、USB コントローラの仮想ドライブにマウントされます。仮想ドライブには、次のいずれかを使用できます。

- 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
- CD/DVD：ブート可能 CD-ROM または DVD ドライブ

ステップ 6 イメージがマウントされている仮想ドライブが最初のブートデバイスになるように、ブート順を設定します。

ヒント イメージがどの仮想ドライブにマウントされているか確認するには、[Host Image Mapping] ページの [Host Image Update Status] 領域を参照してください。

ステップ 7 サーバをリブートします。

ステップ 8 イメージにアンサーファイルが含まれている場合、オペレーティング システムまたはハイパーバイザのインストールは自動化され、イメージがインストールされます。そうでない場合は、インストール ウィザードが表示されます。ウィザードの手順に従って、イメージをインストールします。

ステップ 9 オペレーティング システムまたはハイパーバイザをインストールした後にディスク ドライブが表示されない場合は、ドライバをインストールする必要があります。ドライバのインストール手順については、該当するオペレーティング システムまたはハイパーバイザのマニュアルを参照してください。

次のタスク

- 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。

ホスト イメージのマッピング解除

始める前に

admin 権限を持つユーザとして CIMC にログインします。

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 3 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 4 [Unmap Image] をクリックします。

USB コントローラの仮想ドライブから、マップされたイメージがアンマウントされます。

ホスト イメージの削除

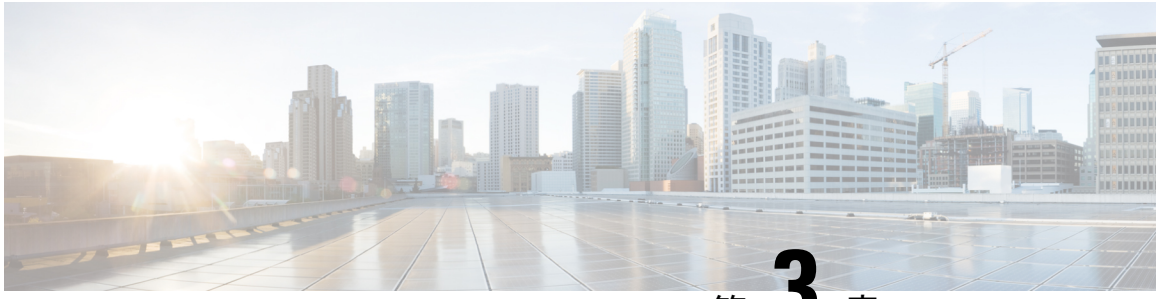
始める前に

admin 権限を持つユーザとして CIMC にログインします。

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。
ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。
ステップ 3 [Current Mappings Information] 領域で、削除するイメージを選択します。
ステップ 4 [Delete Selected Image] をクリックします。

イメージが SD カードから削除されます。



第 3 章

シャーシの管理

この章は、次の項で構成されています。

- シャーシ要約 （19 ページ）
- シャーシ インベントリ （22 ページ）
- シャーシ センサーの表示 （24 ページ）
- 障害サマリー （28 ページ）
- 障害履歴 （30 ページ）
- Cisco IMC ログ （32 ページ）
- システム イベント ログ （35 ページ）
- ロギング制御 （37 ページ）

シャーシ要約

シャーシ サマリーの表示

デフォルトでは、Cisco UCS E シリーズ ラックマウント サーバにログオンすると、シャーシの [Summary] ペインが Web UI に表示されます。次の手順を実行することで、別のタブまたは作業領域を開いている際に、シャーシのサマリーを表示することもできます。

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューの [Summary] をクリックします。

ステップ 3 [Chassis Summary] ペインの [Server Properties] 領域で、次の情報を確認します。

名前	説明
[Product Name] フィールド	シャーシのモデル名。
[Serial Number] フィールド	シャーシのシリアル番号。

名前	説明
[PID] フィールド	製品 ID。
UUID	サーバに割り当てられている UUID。
BIOS version	BIOS のバージョン名。
[Description] フィールド	サーバのユーザ定義の説明。
[アセット タグ（Asset Tag）] フィールド	サーバのユーザ定義のタグ。デフォルトでは、新しいサーバのアセット タグには [Unknown] と表示されます。

ステップ 4 [Chassis Summary] ペインの [Cisco IMC Information] 領域で、次の情報を確認します。

名前	説明
[Hostname] フィールド	Cisco IMC のユーザ定義のホスト名。デフォルトでは、ホスト名は EXXXX-YYYYYYYYYY 形式で表示されます（XXXX はサーバのモデル番号、YYYYYYYYYY はシリアル番号です）。
[IP Address] フィールド	Cisco IMC の IP アドレス
[MAC Address] フィールド	Cisco IMC に対するアクティブなネットワーク インターフェイスに割り当てられている MAC アドレス。
[Firmware Version] フィールド	現在の Cisco IMC ファームウェアのバージョン。
[Current Time] フィールド	Cisco IMC クロックが示している現在の日時。 （注） Cisco IMC NTP が無効になっている場合、サーバ BIOS から現在の日時を取得します。NTP を有効にすると、Cisco IMC は現在の時刻と日付を NTP サーバから取得します。この情報を変更するには、サーバをリブートし、BIOS 設定メニューへのアクセスに関するメッセージが表示されたら **F2** キーを押します。メインの BIOS 設定タブでオプションを使用して日付または時刻を変更します。
[Local Time] フィールド	選択したタイム ゾーンに準じた地域のローカル タイム。
[Timezone] フィールド	[Select Timezone] オプションをクリックして、タイム ゾーンを選択できます。[Select Timezone] ポップアップ画面で、マップの上にカーソルを移動してロケーションをクリックしてタイム ゾーンを選択するか、または [Timezone] ドロップダウン メニューからタイム ゾーンを選択します。

ステップ 5 [Chassis Summary] ペインの [Router Information] 領域で、次の情報を確認します。

名前	説明
[Router Model] フィールド	ルータのモデル名。
[Serial Number] フィールド	ルータのシリアル番号。

ステップ 6 [Chassis Summary] ペインの [Chassis Status] 領域で、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。次のいずれかになります。 • [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]**
[Overall DIMM Status] フィールド	メモリ モジュールの全体的なステータス。次のいずれかになります。 • **Good** • **[Fault]** • **[Severe Fault]** 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。
[全体のストレージ ステータス（Overall Storage Status）] フィールド	すべてのコントローラの全体的なステータス。次のいずれかになります。 • **Good** • **[Moderate Fault]** • **[Severe Fault]**

サーバ アセット タグの作成

始める前に

このタスクを実行するには、user または 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 [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューの [Summary] をクリックします。
ステップ 3 [Save Changes] をクリックします。

シャーシ インベントリ

電源のプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Inventory] をクリックします。
ステップ 3 [Inventory] 作業ウィンドウで、[Power Supplies] タブをクリックし、各電源の次の情報を確認します。

名前	説明
[Device ID] カラム	電源装置ユニットの ID。
[Status] カラム	電源装置のステータス。
[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。
[Product ID] カラム	ベンダーによって割り当てられた電源の製品識別子。

ストレージのプロパティの表示

始める前に

サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Inventory] をクリックします。

ステップ 3 [Inventory] 作業ウィンドウの [Storage] タブをクリックし、次の情報を確認します。

名前	説明
[コントローラ（Controller）] フィールド	コントローラ ドライブが存在する PCIe スロット。
[PCIスロット（PCI Slot）] フィールド	コントローラ ドライブが配置されている PCIe スロットの名前。
[製品名（Product Name）] フィールド	コントローラの名前。
[シリアル番号（Serial Number）] フィールド	ストレージ コントローラのシリアル番号。
[ファームウェアパッケージビルド（Firmware Package Build）] フィールド	アクティブなファームウェア パッケージのバージョン番号。
[製品ID（Product ID）] フィールド	コントローラの製品 ID。
[バッテリのステータス（Battery Status）] フィールド	バッテリのステータス。
[キャッシュメモリサイズ（Cache Memory Size）] フィールド	キャッシュ メモリのサイズ（MB 単位）。
[状況（Health）] フィールド	コントローラのヘルス状態。

ネットワーク アダプタのプロパティの表示

始める前に

サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Inventory] をクリックします。

ステップ 3 [Inventory] 作業ウィンドウの [Network Adapters] タブをクリックし、次の情報を確認します。

名前	説明
[Slot ID] カラム	アダプタが装着されているスロット。
[Product Name] カラム	アダプタの製品名。
[Number of Interfaces] カラム	アダプタのインターフェイスの数。
External Ethernet Interfaces	[ID]：外部イーサネット インターフェイスの ID。 [MAC Address]：外部イーサネット インターフェイスの MAC アドレス。

シャーシ センサーの表示

電源センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Power Supply] タブをクリックします。

ステップ 4 電源装置の次のセンサー プロパティを確認します。

[プロパティ（Properties）] 領域

名前	説明
[Redundancy Status] フィールド	電源装置の冗長性のステータス。

[Threshold Sensors] 領域

名前	説明
[Sensor Name] カラム	センサーの名前
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[Reading] カラム	現在の電力使用量（ワット単位）。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[Non-Recoverable Threshold Min] カラム	回復不可能な最小しきい値。
[Non-Recoverable Threshold Max] カラム	回復不可能な最大しきい値。

[Discrete Sensors] 領域

名前	説明
[Sensor Name] カラム	センサーの名前。
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**

名前	説明
[Reading] カラム	センサーの基本的な状態。

温度センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Temperature] タブをクリックします。

ステップ 4 次の温度センサーのプロパティを確認します。

名前	説明
[Sensor Name] カラム	センサーの名前
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[Temperature] カラム	現在の温度（摂氏単位）。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[Non-Recoverable Threshold Min] カラム	回復不可能な最小しきい値。

電圧センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Voltage] タブをクリックします。

ステップ 4 次の電圧センサーのプロパティを確認します。

名前	説明
[Sensor Name] カラム	センサーの名前
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[Voltage (V)] カラム	現在の電圧（ボルト単位）。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[Non-Recoverable Threshold Min] カラム	回復不可能な最小しきい値。
[Non-Recoverable Threshold Max] カラム	回復不可能な最大しきい値。

電流センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。
ステップ 3 [Sensors] 作業領域で、[Current] タブをクリックします。
ステップ 4 次の電流センサーのプロパティを確認します。

ストレージ センサーの表示

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。
ステップ 3 [Storage] タブの [Storage Sensors] 領域で、サーバの次のストレージに関する統計情報を表示します。

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に関する簡単な説明。

障害サマリー

障害サマリーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Faults Summary] タブで、次の情報を確認します。

表 *1 : [Actions]* 領域

名前	説明
[Total]	[Fault Entries] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。

名前	説明
[Show] ドロップダウン リスト	フィルタを使用して障害のエントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づき障害のエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *2 : [Fault Entries]* 領域

名前	説明
[Time]	障害が発生した時刻。

名前	説明
[Severity]	次のいずれかになります。 • [Cleared]：ある障害または状態が解消されました。 • **[Critical]** • **[Info]** • **[Major]** • **[Minor]** • 警告
[Code]	障害に割り当てられた固有識別情報。
[DN]	識別名（DN）は、サーバ上でのデバイスのエンドポイントおよびそのインスタンスの階層表現です。
[Probable Cause]	障害の原因となったイベントに関連付けられた固有識別情報。
[Description]	障害についての詳細情報。 提案される解決策も含まれます。

障害履歴

障害履歴の表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Faults History] タブで、次の情報を確認します。

表 *3 : [Actions]* 領域

名前	説明
[Total]	[Fault History] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。
[Show] ドロップダウン リスト	フィルタを使用して障害履歴エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づきエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *4 : [Faults History]* 領域

名前	説明
[Time]	障害が発生した時刻。
[Severity]	次のいずれかになります。 • **[Emergency]** • **[Alert]** • **[Critical]** • **[Error]** • **警告** • **[Notice]** • **[Informational]** • **[Debug]**
[Source]	イベントをログに記録したソフトウェア モジュール。
[Probable Cause]	障害の原因となったイベントに関連付けられた固有識別情報。
[Description]	障害についての詳細情報。 提案される解決策も含まれます。

次のタスク

Cisco IMC ログ

Cisco IMC ログの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Cisco IMC Log] タブで、次の情報を確認します。

表 *5 : [Actions]* 領域

名前	説明
[Clear Log] ボタン	すべてのログ ファイルを消去します。 （注） このオプションは、ユーザ ID に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。
[Total]	[Cisco IMC Log] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。

名前	説明
[Show] ドロップダウン リスト	フィルタを使用して Cisco IMC ログ エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づきログエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *6 : [Cisco IMC Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。

名前	説明
[Severity] カラム	イベントの重大度。次のいずれかになります。 • **[Emergency]** • **[Alert]** • **[Critical]** • **[Error]** • 警告 • **[Notice]** • **[Informational]** • **[Debug]**
[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。

システム イベント ログ

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 [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [System Event Log] タブで、次の情報を確認します。

表 *7 : [Actions]* 領域

名前	説明
[Clear Log] ボタン	ログ ファイルからすべてのイベントをクリアします。 （注） このオプションは、ユーザ ID に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。

名前	説明
[Total]	[System Event Log] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。
[Show] ドロップダウン リスト	フィルタを使用してイベントを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づきイベントを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *8 : [System Event Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。
[Severity] カラム	重大度フィールドには、テキストと色分けされたアイコンの両方が含まれます。アイコンについては、緑色は通常動作、黄色は情報を示し、警告、クリティカルおよび回復不能なエラーは赤色で表示されます。
[Description] カラム	イベントの説明。

ロギング制御

ロギング制御の表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Logging Controls] タブで、次の情報を確認します。

リモート ロギング

名前	説明
[Enabled] チェックボックス	オンにすると、Cisco IMC は [IP Address] フィールドで指定された Syslog サーバにログ メッセージを送信します。
[Host Name/IP Address] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[Port] フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

名前	説明
[Minimum Severity to Report] フィールド	リモート ログに含まれるメッセージの最低レベルを指定します。次のいずれかを選択できます。 • **[Emergency]** • **[Alert]** • **[Critical]** • **[Error]** • **警告** • **[Notice]** • **[Informational]** • **[Debug]**

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージはリモートでログに記録されません。たとえば、[Error] を選択した場合、Cisco IMC リモート ログには重大度が [Emergency]、[Alert]、[Critical]、[Error] のすべてのメッセージが含まれます。[Warning]、[Notice]、[Informational]、[Debug] のメッセージは表示されません。

Local Logging

この領域には、上記の表に示すように [Minimum Severity to Report] ドロップダウンリストのみが表示されます。ローカル ログに含めるメッセージの最低レベルを指定できます。

次のタスク

リモート サーバへの Cisco IMC ログの送信

Cisco IMC ログ エントリを受信するように 1 台または 2 台のリモート syslog サーバのプロファイルを設定できます。

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Remote Syslog Server] 領域のいずれかで、次のフィールドに値を入力します。

名前	説明
[Enabled] チェックボックス	オンにすると、Cisco IMC は [IP Address] フィールドで指定された Syslog サーバにログ メッセージを送信します。
[Host Name/IP Address] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[Port] フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

ステップ 4 （任意）[Minimum Severity to Report] ドロップダウン リストで、リモート ログに含まれるメッセージの最低レベルを指定します。

次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- **[Emergency]**
- **[Alert]**
- **[Critical]**
- **[Error]**
- 警告
- **[Notice]**
- **[Informational]**
- **[Debug]**

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージは、リモートでログに記録されません。たとえば、[**Error**] を選択した場合、Cisco IMC リモート ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

ステップ 5 [Save Changes] をクリックします。

Cisco IMC ログしきい値の設定

始める前に

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 必須: [**Local Logging**] 領域で、[**Minimum Severity to Report**] ドロップダウン リストを使用して、Cisco IMC ログに含まれるメッセージの最低レベルを指定します。

次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- **[Emergency]**
- **[Alert]**
- **[Critical]**
- **[Error]**
- 警告
- **[Notice]**
- **[Informational]**
- **[Debug]**

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージはログに記録されません。たとえば、[**Error**] を選択した場合、Cisco IMC ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

リモート サーバへのテスト Cisco IMC ログの送信

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

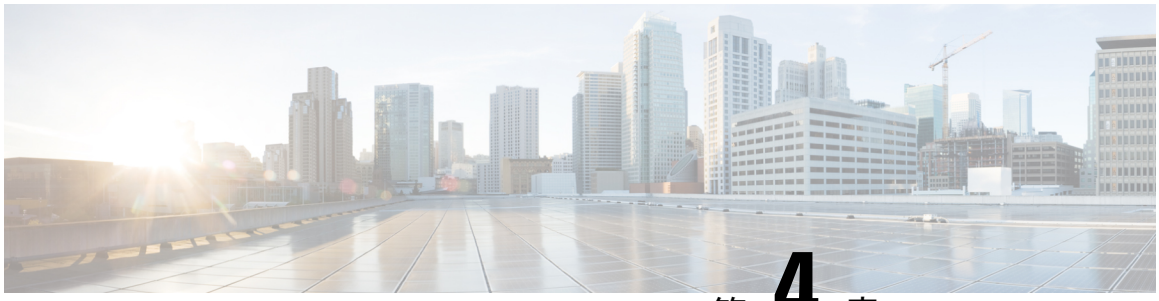
ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Faults and Logs] ペインの [Logging Controls] タブをクリックします。

ステップ 4 [**Action**] 領域の [**Send Test Syslog**] をクリックします。

設定されているリモート サーバにテスト Cisco IMC ログが送信されます。



第 4 章

サーバの管理

この章は、次の項で構成されています。

- BIOS の設定 （43 ページ）
- サーバのブート順の管理 （48 ページ）

BIOS の設定

BIOS セットアップの開始

BIOS セットアップを初めて入力するときは、管理者レベルとユーザレベルのパスワードを設定して、BIOS のセキュリティを確保してください。初めて BIOS メニューにアクセスするときに、管理者パスワードを設定する必要があります。（BIOS オプションの小さなサブセットへのアクセスのみを提供する）ユーザ パスワードは、BIOS セットアップ メニュー内で設定する必要があります。

管理者パスワードを設定するには、システムの起動時に F2 を押します。パスワードの設定を求めるメッセージが表示されます。

ユーザ パスワードを設定するには、ログイン後に [Security] タブに移動し、パスワードを設定します。

主要な BIOS の設定

始める前に

このタスクを実行するには、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 [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [Configure BIOS] タブで、[Main] タブをクリックします。

ステップ 4 変更を保存した後でサーバをリブートする必要があるかどうかを指定します。

[Save Changes] をクリックした後で変更内容を自動的に適用するには、**[Reboot Host Immediately]** チェックボックスをオンにします。Cisco IMCサーバをすぐに再起動して変更を適用します。

変更内容を後で適用するには、**[Reboot Host Immediately]** チェックボックスをオフにします。Cisco IMC変更を保存し、次回サーバを再起動する際に変更を適用します。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

ステップ 5 [Main] タブで、BIOS 設定のフィールドを更新します。

ステップ 6 [Main] タブの下部にあるボタンを使用して、パラメータのリセットまたはデフォルト値の復元を行うことができます。次のオプションを使用できます。

名前	説明
[**Save**] ボタン	BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 **[Reboot Host Immediately]** チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスが最初に開いたときに有効であった設定にリセットします。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。

BIOS の詳細設定

（注） 搭載されているハードウェアによっては、このトピックで説明されている一部の設定オプションが表示されない場合があります。

始める前に

このタスクを実行するには、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 [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [Configure BIOS] タブで、[Advanced] タブをクリックします。

ステップ 4 変更を保存した後でサーバをリブートする必要があるかどうかを指定します。

[Save Changes] をクリックした後で変更内容を自動的に適用するには、**[Reboot Host Immediately]** チェックボックスをオンにします。Cisco IMCサーバをすぐに再起動して変更を適用します。

変更内容を後で適用するには、**[Reboot Host Immediately]** チェックボックスをオフにします。Cisco IMC変更を保存し、次回サーバを再起動する際に変更を適用します。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

ステップ 5 [Advanced] タブで、関連フィールドを更新します。

ステップ 6 フィールドを更新したら、次の操作を実行します。

名前	説明
[**Save**] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。
[Reset] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。

サーバ管理 BIOS の設定

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [Configure BIOS] タブで、[Server Management] をクリックします。

ステップ 4 変更を保存した後でサーバをリブートする必要があるかどうかを指定します。

[Save Changes] をクリックした後で変更内容を自動的に適用するには、**[Reboot Host Immediately]** チェックボックスをオンにします。Cisco IMCサーバをすぐに再起動して変更を適用します。

変更内容を後で適用するには、**[Reboot Host Immediately]** チェックボックスをオフにします。Cisco IMC変更を保存し、次回サーバを再起動する際に変更を適用します。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

ステップ 5 [Server Management] タブで、関連フィールドを更新します。

ステップ 6 次のオプションを使用してアクションを完了します。

名前	説明
[**Save**] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。
[Reset] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。

BIOS セットアップの開始

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、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 [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [Actions] 領域で [Enter BIOS Setup] をクリックします。

ステップ 4 プロンプトで [OK] をクリックします。
BIOS セットアップの開始が有効になります。再起動すると、サーバは BIOS セットアップを開始します。

BIOS CMOS のクリア

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、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 [Compute] メニューをクリックします。
ステップ 2 作業ウィンドウの [BIOS] タブをクリックします。
ステップ 3 [Actions] 領域の [Clear BIOS CMOS] をクリックします。
ステップ 4 [OK] をクリックして確定します。
BIOS CMOS をクリアします。

BIOS の製造元カスタム設定の復元

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、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 [Compute] メニューをクリックします。
ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。
ステップ 3 作業ウィンドウの [BIOS] タブをクリックします。
ステップ 4 [Actions] 領域で、[Restore Manufacturing Custom Settings] をクリックします。
ステップ 5 [OK] をクリックして確定します。

サーバのブート順の管理

サーバのブート順

Cisco IMC を使用して、使用可能なブート デバイス タイプからサーバがブートを試行する順序を設定できます。レガシー ブート順の設定では、Cisco IMC によりデバイス タイプの並び替えが許可されますが、デバイス タイプ内のデバイスの並べ替えはできません。高精度ブート順の設定により、デバイスの線形順序付けができます。Web UI または CLI では、ブート順およびブート モードの変更、各デバイス タイプ下への複数のデバイスの追加、ブート順の並び替え、各デバイス タイプのパラメータの設定ができます。

ブート順の設定を変更すると、Cisco IMC は、サーバが次にリブートされるときに、設定されたブート順を BIOS に送信します。新しいブート順を実装するには、設定の変更後にサーバをリブートします。新しいブート順は以降のリブートで反映されます。設定されたブート順は、設定が Cisco IMC または BIOS 設定で再度変更されるまで保持されます。

（注） 次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。

- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
- ユーザが BIOS で直接、ブート順を変更した。
- BIOS が、ホストによって認識されているがユーザから設定されていないデバイスを追加した。

（注） ブート順の設定機能を使用して新しいポリシーを作成する場合、BIOS はこの新しいポリシーをシステムのデバイスにマッピングしようとします。実際にマッピングされたデバイス名とポリシー名が [**Actual Boot Order**] 領域に表示されます。BIOS が Cisco IMC の特定のポリシーにデバイスをマッピングできない場合は、実際のデバイス名が [**Actual Boot Order**] 領域に [**NonPolicyTarget**]として示されます。

ブート デバイスの管理

始める前に

デバイス タイプをサーバのブート順に追加するには、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 [Compute] メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域の [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 [Configure Boot Order] ダイアログボックスで、[Basic] タブをクリックし、[Device Types] テーブルからブート順に追加するデバイスを選択します。

ローカル HDD デバイスを追加するには、[Advanced] タブをクリックし、[Add Local HDD] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 （注） 一旦作成すると、デバイスの名前を変更することはできません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート設定で BIOS から認識できません。
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

PXE デバイスを追加するには、[**Add PXE**] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。

名前	説明
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。State には、次のいずれかを指定できます。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

SAN ブート デバイスを追加するには、[**Add SAN**] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。State には、次のいずれかを指定できます。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。

名前	説明
[**LUN**] フィールド	デバイスが装着されているスロットの論理ユニット。 0 ～ 255 の範囲内の数を入力してください。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

iSCSI ブート デバイスを追加するには、[**Add iSCSI**] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。State には、次のいずれかを指定できます。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。 （注） VIC カードの場合は、ポート番号ではなく vNIC インスタンスを使用します。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

SD カードを追加するには、[**Add SD Card**] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート設定で BIOS から認識できません。
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Lun] フィールド	デバイスが装着されているスロットの論理ユニット。 0 ～ 255 の範囲内の数を入力してください。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

USB デバイスを追加するには、[**Add USB**] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**Sub Type**] ドロップダウン リスト	特定のデバイスタイプの下位のサブデバイスタイプ。次のいずれかになります。 • **[CD]** • **[FDD]** • **[HDD]**
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。

名前	説明
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

仮想メディアを追加するには、[**Virtual Media**] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**Sub Type**] ドロップダウン リスト	特定のデバイス タイプの下位のサブデバイス タイプ。これは、次のいずれかになります。 • **[KVM Mapped DVD]** • **[Cisco IMC Mapped DVD]** • **[KVM Mapped HDD]** • **[Cisco IMC Mapped HDD]** • **[KVM Mapped FDD]**
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。State には、次のいずれかを指定できます。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[変更を保存（Save Changes）] ボタン	[Boot Order] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

PCH ストレージ デバイスを追加するには、[**PCH Storage**] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[**LUN**] フィールド	デバイスが装着されているスロットの論理ユニット。 • 0 ～ 255 の範囲の値を入力します。 • AHCI モードの SATA：1 ～ 10 の範囲の値を入力します • SWRAID モードの SATA：SATA の場合に 0、また 1 を入力します。 （注） SATA モードを使用できるのは一部の UCS E シリーズ サーバだけです。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

UEFI シェル デバイスを追加するには、[Add UEFI Shell] をクリックし、次のパラメータを更新します。

名前	説明
[Name] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。State には、次のいずれかを指定できます。 • [**Enabled**]：デバイスはブート順の設定で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。

名前	説明
[Order] フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Save Changes] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

UEFI セキュア ブートのイネーブル化

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [ブート順の設定（Configure Boot Order）] タブの [BIOS プロパティ（BIOS Properties）] 領域で、[UEFI セキュア ブート（UEFI Secure Boot）] チェックボックスをオンにします。

（注） オンにすると、ブート モードが UEFI セキュア ブートに設定されます。UEFI セキュア ブート オプションがディセーブルになるまで [**Configure Boot Mode**] は変更できません。

サポートされていない OS で UEFI セキュア ブートをイネーブルにすると、次の再起動時に、その特定の OS から起動することはできません。前の OS から起動しようとすると、Web UI のシステム ソフトウェア イベントの下にエラーが報告され記録されます。前の OS から起動するには、Cisco IMC を使用して UEFI セキュア ブート オプションをディセーブルにする必要があります。

ステップ 4 [Save Changes] をクリックします。

次のタスク

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

UEFI セキュア ブートのディセーブル化

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [BIOS プロパティ（BIOS Properties）] 領域で、[UEFI セキュア ブート（UEFI Secure Boot）] チェックボックスをオフにします。

ステップ 4 [Save Changes] をクリックします。

次のタスク

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

サーバの実際のブート順の表示

サーバの実際のブート順とは、サーバが最後にブートされたときに BIOS によって実際に使用されたブート順です。実際のブート順は、Cisco IMC で設定されたブート順とは異なる場合があります。

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域の [Configure Boot Order] をクリックします。

この領域には、Cisco IMC を介して設定されたブート順のデバイスと、サーバ BIOS によって使用される実際のブート順が表示されます。

[Configured Boot Devices] セクションには、Cisco IMC を介して設定されたブート順（[Basic] または [Advanced]）が表示されます。この設定が変更されると、次回そのサーバがブートしたときに、Cisco IMC がこのブート順を BIOS に送信します。基本設定では、デバイス タイプのみを指定できます。詳細設定では、スロット、ポート、LUN などの特定のパラメータを使用してデバイスを設定できます。

設定されたブート順を変更したり、以前に設定されたブート順を復元したりするには、管理者は [Configure Boot Order] ボタンをクリックできます。これらの変更をただちに有効にするには、サーバをリブートします。[BIOS] タブを更新することで、新しいブート順を確認できます。

（注） この情報は、次回のサーバのブート時に BIOS にのみ送信されます。Cisco IMC は、設定が変更されるまで、ブート順の情報を BIOS に再送信しません。

[Actual Boot Devices] セクションには、サーバが最後にブートされたときに BIOS によって実際に使用されたブート順が表示されます。次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。

- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
- ユーザが BIOS で直接、ブート順を変更した。手動による変更を上書きするには、Cisco IMC を介して設定されたブート順を変更し、サーバをリブートします。

（注） 設定されたブート順を使用して新しいポリシーを作成すると、BIOS はこの新しいポリシーをシステムに存在するデバイス（複数の場合あり）にマッピングしようとします。実際にマッピングされたデバイス名とポリシー名が [Actual Boot Order] 領域に表示されます。BIOS が Cisco IMC の特定のポリシーに検出されたデバイスをマッピングできない場合は、実際のデバイス名が [Actual Boot Order] 領域に [NonPolicyTarget] として示されます。

ISRG2 でのモジュールの電力復元ポリシーの設定

電力復元ポリシーによって、シャーシの電力供給が失われた後、サーバに電力を復元する方法が決定されます。

（注） GUI で変更された設定を確認できますが、設定を有効にするにはサーバをリブートする必要があります。

始める前に

このタスクを実行するには、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 [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [BIOS] をクリックしてから [Server Management] タブをクリックします。

ステップ 3 [Server Management] 領域で、次のフィールドを更新します。

名前	説明
[電力復元ポリシー（Power Restore Policy）] ドロップダウン リスト	予期しない電源損失後、シャーシ電源が復元されたときに実行されるアクション。次のいずれかになります。 Power On – サーバの電源がオンになり、停電を通知します。 Power Off– サーバは電源オフ状態のままです。 Restore Last State – サーバは停電前の状態に設定されます。

ステップ 4 **[Save（保存）]** をクリックします。

ISR4K でのモジュールの電力復元ポリシーの設定

電力復元ポリシーによって、シャーシの電力供給が失われた後、サーバに電力を復元する方法が決定されます。

始める前に

このタスクを実行するには、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

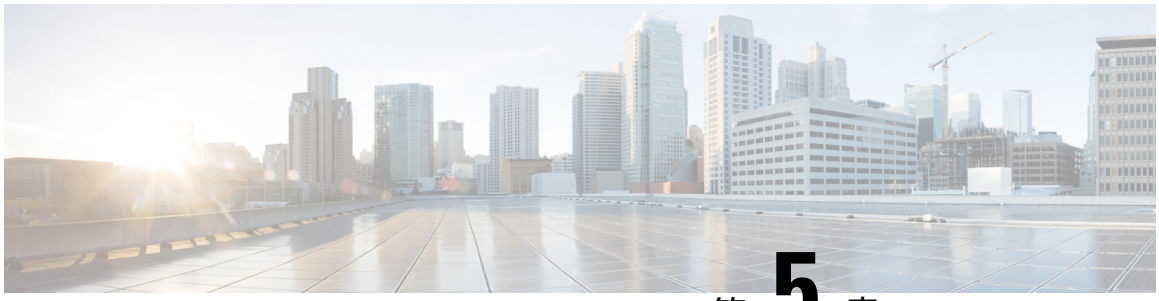
ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウで、[Power Policies] タブをクリックします。

ステップ 3 [Power Restore Policy] 領域で、次のフィールドを更新します。

名前	説明
[電力復元ポリシー（Power Restore Policy）] ドロップダウン リスト	予期しない電源損失後、シャーシ電源が復元されたときに実行されるアクション。次のいずれかになります。 Power On – サーバの電源がオンになり、停電を通知します。 Power Off– サーバは電源オフ状態のままです。 Restore Last State – サーバは停電前の状態に設定されます。

ステップ 4 **[保存（Save）]** をクリックします。



第 5 章

センサーの表示

この章は、次の項で構成されています。

• シャーシ センサーの表示 （59 ページ）

シャーシ センサーの表示

電源センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Power Supply] タブをクリックします。

ステップ 4 電源装置の次のセンサー プロパティを確認します。

[プロパティ（Properties）] 領域

名前	説明
[Redundancy Status] フィールド	電源装置の冗長性のステータス。

[Threshold Sensors] 領域

名前	説明
[Sensor Name] カラム	センサーの名前

名前	説明
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • 不明 • **[Informational]** • 標準 • 警告 • **[Critical]** • **Non-Recoverable**
[Reading] カラム	現在の電力使用量（ワット単位）。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[Non-Recoverable Threshold Min] カラム	回復不可能な最小しきい値。
[Non-Recoverable Threshold Max] カラム	回復不可能な最大しきい値。

[Discrete Sensors] 領域

名前	説明
[Sensor Name] カラム	センサーの名前。
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • 不明 • **[Informational]** • 標準 • 警告 • **[Critical]** • **Non-Recoverable**
[Reading] カラム	センサーの基本的な状態。

ファン センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Fan] タブをクリックします。

ステップ 4 次のファン センサーのプロパティを確認します。

名前	説明
[Sensor Name] カラム	センサーの名前
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[Speed (RPMS)] カラム	ファンの速度（RPM 単位）。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[Non-Recoverable Threshold Min] カラム	回復不可能な最小しきい値。
[Non-Recoverable Threshold Max] カラム	回復不可能な最大しきい値。

温度センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Temperature] タブをクリックします。

ステップ 4 次の温度センサーのプロパティを確認します。

名前	説明
[Sensor Name] カラム	センサーの名前
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • **不明** • **[Informational]** • **標準** • **警告** • **[Critical]** • **Non-Recoverable**
[Temperature] カラム	現在の温度（摂氏単位）。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[Non-Recoverable Threshold Min] カラム	回復不可能な最小しきい値。

電圧センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Voltage] タブをクリックします。

ステップ 4 次の電圧センサーのプロパティを確認します。

名前	説明
[Sensor Name] カラム	センサーの名前

名前	説明
[Sensor Status] カラム	センサーのステータス。次のいずれかになります。 • 不明 • **[Informational]** • 標準 • 警告 • **[Critical]** • **Non-Recoverable**
[Voltage (V)] カラム	現在の電圧（ボルト単位）。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[Non-Recoverable Threshold Min] カラム	回復不可能な最小しきい値。
[Non-Recoverable Threshold Max] カラム	回復不可能な最大しきい値。

電流センサーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。
ステップ 3 [Sensors] 作業領域で、[Current] タブをクリックします。
ステップ 4 次の電流センサーのプロパティを確認します。

ストレージ センサーの表示

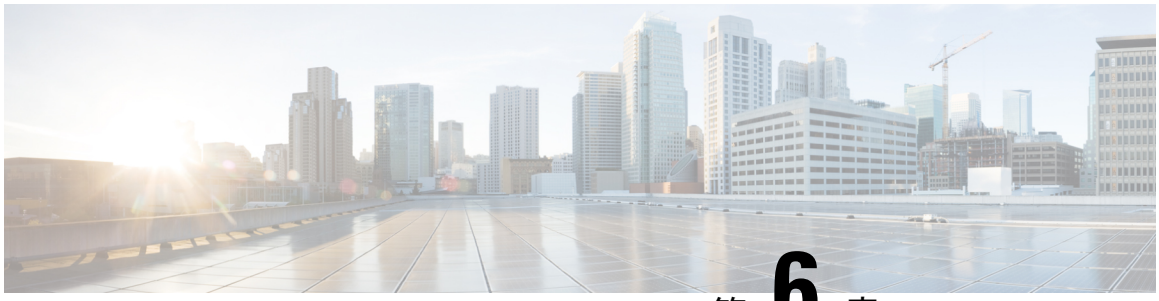
手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Sensors] をクリックします。

ステップ 3 [Storage] タブの [Storage Sensors] 領域で、サーバの次のストレージに関する統計情報を表示します。

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に関する簡単な説明。



第 6 章

リモート プレゼンスの管理

この章は、次の項で構成されています。

- Serial over LAN の設定 （65 ページ）
- 仮想メディアの設定 （67 ページ）
- KVM コンソール （74 ページ）
- KVM コンソールの起動 （74 ページ）
- 仮想 KVM コンソール（HTML ベース） （75 ページ）
- Java ベース KVM と HTML5 ベース KVM の比較 （78 ページ）
- 仮想 KVM の設定 （80 ページ）
- ホスト イメージ マッピング （82 ページ）

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 Cisco IMC 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。

始める前に

Serial over LAN を設定するには、管理者権限のあるユーザで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 [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [Remote Management] タブをクリックします。

ステップ 3 [Remote Management] 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、サーバで Serial over LAN（SoL）が有効になります。
[Baud Rate] ドロップダウン リスト	システムが SoL 通信に使用するボー レート。次のいずれかになります。 • **[9600 bps]** • **[19.2 kbps]** • **[38.4 kbps]** • **[57.6 kbps]** • **[115.2 kbps]**
[Com Port] ドロップダウン リスト	システムが SoL 通信をルーティングするシリアル ポート。 （注） このフィールドを使用できるのは一部の E シリーズ サーバだけです。使用できない場合、サーバは、SoL 通信に COM ポート 0 を使用します。 次のいずれかを選択できます。 • [com0]：SoL 通信は、外部デバイスへの物理 RJ45 接続またはネットワーク デバイスへの仮想 SoL 接続をサポートする、外部からアクセス可能なシリアル ポートである COM ポート 0 を介してルーティングされます。 このオプションを選択すると、システムは、SoL をイネーブルにし、RJ45 接続をディセーブルにします。これは、サーバが外部シリアル デバイスをサポートできなくなることを意味します。 • [com1]：SoL 通信は、SoL だけを介してアクセス可能な内部ポートである、COM ポート 1 経由でルーティングされます。 このオプションを選択した場合、COM ポート 1 上の SoL および COM ポート 0 上の物理 RJ45 接続を使用できます。 （注） Com Port 設定を変更すると、既存のすべての SoL セッションは切断されます。

名前	説明
[SSH Port] フィールド	Serial over LAN に直接アクセスできるポート。このポートを使用すると、SoL へのダイレクト アクセスを提供する Cisco IMC シェルを迂回できます。 有効な範囲は 1024 ～ 65535 です。デフォルト値は 2400 です。 （注） SSH Port 設定を変更すると、既存のすべての SSH セッションは切断されます。

ステップ 5 [Save Changes] をクリックします。

仮想メディアの設定

始める前に

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 [Compute] メニューをクリックします。
ステップ 2 作業ウィンドウの [Remote Management] タブをクリックします。
ステップ 3 [Remote Management] ペインで、[Virtual Media] タブをクリックします。
ステップ 4 [仮想メディア プロパティ（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。

Cisco IMC マップされた vMedia ボリュームの作成

始める前に

このタスクを実行するには、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 [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [Remote Management] タブをクリックします。

ステップ 3 [Remote Management] タブで、[Virtual Media] タブをクリックします。

ステップ 4 [Current Mappings] 領域で、[Add New Mapping] をクリックします。

ステップ 5 [Add New Mapping] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Volume] フィールド	マッピング用にマウントされるイメージの ID。
[Mount Type] ドロップダウン リスト	マッピングのタイプ。次のいずれかになります。 （注） 選択したマウント タイプの通信ポートがスイッチでイネーブルになっていることを確認します。たとえば、マウント タイプとして CIFS を使用している場合は、ポート 445（これはその通信ポートです）がスイッチでイネーブルになっていることを確認します。同様に、HTTP の場合はポート 80、HTTPS の場合は 443、NFS の場合は 2049 をそれぞれイネーブルにします。 • [NFS]：ネットワーク ファイル システム。 • [CIFS]：Common Internet File System。 • [WWW(HTTP/HTTPS)]：HTTP ベースまたは HTTPS ベースのシステム。 （注） 仮想メディアをマウントする前に、Cisco IMC はサーバに ping を実行することによって、エンド サーバへの到達可能性の確認を試みます。

名前	説明
[リモート共有（Remote Share）] フィールド	マップするイメージの URL。形式は選択された [Mount Type] によって異なります。 • [NFS]：**serverip:/share** を使用します。 • [CIFS]：**serverip://share** を使用します。 • [WWW(HTTP/HTTPS)]： **http[s]://serverip/share** を使用します。
[Remote File] フィールド	リモート共有の .iso または .img ファイルの名前と場所。

名前	説明
[Mount Options] フィールド	

名前	説明
	カンマ区切りリストで入力される業界標準のマウント オプション。オプションは選択された [Mount Type] によって異なります。 [NFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • **ro** • **rw** • **nolock** • **noexec** • **soft** • **port=VALUE** • **timeo=VALUE** • **retry=VALUE** [CIFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • **soft** • **nounix** • **noserverino** • **guest** • [username=VALUE]：**guest** が入力された場合は無視されます。 • [password=VALUE]：**guest** が入力された場合は無視されます。 • **sec=VALUE** リモートサーバとの通信時に認証に使用するプロトコル。CIFS 共有の設定に応じて、[VALUES] の値は次のいずれかになります。 • [なし（None）]：認証は使用されません。 • [Ntlm]：NT LAN Manager（NTLM）セキュリティ プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [Ntlmi]：NTLMi のセキュリティプロトコル。このオプションは、CIFS Windows サーバでデジタル署名が

名前	説明
	有効な場合のみ使用します。 • [Ntlmssp]：NT LAN Managerのセキュリティ サポート プロバイダー（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [Ntlmsspi]：NTLMSSPi プロトコル。このオプションは、CIFS Windows サーバでデジタル署名が有効な場合のみ使用します。 • [Ntlmv2]：NTLMv2 セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 • [Ntlmv2i]：NTLMv2i のセキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 [WWW(HTTP/HTTPS)] を使用している場合は、このフィールドを空白のままにするか、次のように入力します。 • **noauto** （注） 仮想メディアをマウントする前に、Cisco IMC はサーバに ping を実行することによって、エンド サーバへの到達可能性の確認を試みます。 • **username=VALUE** • **password=VALUE**
[User Name] フィールド	選択された [Mount Type] のユーザ名（必要な場合）。
[Password] フィールド	選択されたユーザ名のパスワード（必要な場合）。

ステップ 6 **[保存（Save）]** をクリックします。

Cisco IMC マップされた vMedia ボリューム プロパティの表示

始める前に

このタスクを実行するには、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 [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 作業ウィンドウの [Remote Management] タブをクリックします。

ステップ 4 [Remote Management] タブで、[Virtual Media] タブをクリックします。

ステップ 5 [Current Mappings] テーブルから行を選択します。

ステップ 6 [Properties] をクリックし、次の情報を確認します。

名前	説明
[Add New Mapping] ボタン	新しいイメージを追加できるダイアログボックスが開きます。
[Properties] ボタン	選択したイメージのプロパティを表示または変更できるダイアログボックスが開きます。
[Unmap] ボタン	マウントされた vMedia のマップを解除します。
Last Mapping Status	最後に試行されたマッピングのステータス。
[Volume] カラム	イメージの ID。
[Mount Type] ドロップダウンリスト	マッピングのタイプ。
[Remote Share] フィールド	イメージの URL。
[Remote File] フィールド	イメージの厳密なファイル位置。
[Status] フィールド	マップの現在のステータス。次のいずれかになります。 • [OK]：マッピングは正常です。 • [In Progress]：マッピングが進行中です。 • [Stale]：Cisco IMC にマッピングが古いという理由を示すテキスト文字列が表示されます。 • [**Error**]：Cisco IMC にエラーの理由を示すテキスト文字列が表示されます。

Cisco IMC マップされた vMedia ボリュームの削除

始める前に

このタスクを実行するには、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 [Compute] メニューをクリックします。
ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。
ステップ 3 作業ウィンドウの [Remote Management] タブをクリックします。
ステップ 4 [Remote Management] タブで、[Virtual Media] タブをクリックします。
ステップ 5 [Current Mappings] テーブルから行を選択します。
ステップ 6 [Unmap] をクリックします。

KVM コンソール

KVM コンソールは Cisco IMC 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（ISO または IMG ファイル）
- コンピュータ上の USB フラッシュ ドライブ
- 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（ISO または IMG ファイル）
- ネットワーク上の USB フラッシュ ドライブ

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 コンソールの起動

KVM コンソールは、ホームページまたは [Remote Management] 領域から起動できます。

手順

ステップ 1 ホームページからコンソールを起動するには、[Navigation] ペインで、[Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューの [Summary] をクリックします。

ステップ 3 ツールバーから、[Launch KVM] をクリックし、[Java based KVM] または [HTML based KVM] を選択します。

ステップ 4 または、[Navigation] ペインの [Compute] メニューをクリックします。

ステップ 5 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 6 作業ウィンドウの [Remote Management] タブをクリックします。

ステップ 7 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。

ステップ 8 [Virtual KVM] タブで、[Launch Java based KVM console] または [Launch HTML based KVM console] をクリックします。

ステップ 9 必須: ポップアップ ウィンドウに表示されている URL リンク（HTML ベースの KVM コンソールのみ）をクリックして、クライアント アプリケーションをロードします。KVM コンソールを起動するたびにリンクをクリックする必要があります。

仮想 KVM コンソール（HTML ベース）

KVM コンソールは Cisco IMC 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。遠隔地のサーバから接続して制御し、この KVM セッション中にアクセスできる仮想ドライブに物理ロケーションをマッピングすることができます。

[ファイル（File）] メニュー

メニュー項目	説明
[ファイルにキャプチャ（Capture to File）] ボタン	JPG イメージとして現在の画面を保存できる [保存（Save）] ダイアログボックスが開きます。
[終了（Exit）] ボタン	KVM コンソールを閉じます。

[View] メニュー

メニュー項目	説明
Keyboard	ユーザがデータの入力に使用できる KVM コンソールの仮想キーボードを表示します。
[更新（Refresh）]	サーバの現在のビデオ出力を使用してコンソール表示を更新します。

メニュー項目	説明
Full Screen	画面全体になるように KVM コンソールを拡大します。

[Macros] メニュー

リモート システムで実行するキーボード ショートカットを選択します。

メニュー項目	説明
[サーバマクロ（Server Macros）] メニュー	Cisco IMC からダウンロードされたサーバ サイド マクロがある場合、表示します。サーバサイドマクロがダウンロードされていない場合、このメニュー項目は無効になります。
[静的マクロ（Static Macros）] メニュー	マクロの定義済みのセットを表示します。
[ユーザ定義マクロ（User Defined Macros）] メニュー	作成済みのユーザ定義マクロを表示します。
[Manage] ボタン	マクロの作成および管理ができる [Configure User Defined Macros] ダイアログ ボックスを開きます。 システム定義されたマクロは削除できません。

[Tools] メニュー

メニュー項目	説明

[Session Options]	以下の項目が指定できる [セッション オプション（Session Options）] ダイアログを開きます。
	• [Scaling]：画面の縦横率を維持するかどうかを指定します。 [Maintain Aspect Ratio] チェックボックスをオンまたはオフにします（デフォルトはオン）。
	• ターゲット システムで使用するマウス アクセラレーション。デフォルトは、[Absolute positioning (Windows, Newer Linux & MAC OS X)] です。その他のオプションを次に示します。
	  • **Relative Positioning, no acceleration**
	  • **Relative Positioning (RHEL, Older Linux)**

[セッション ユーザ リスト（Session User List）]	アクティブ KVM セッションを持つすべてのユーザ ID を表示する [セッション ユーザ リスト（Session User List）] ダイアログ ボックスを開きます。
[Chat]	他のユーザと通信するための [Chat] ボックスを開きます。

[Power] メニュー

メニュー項目	説明
[Power On System] ボタン	システムの電源を入れます。 このオプションは、システムの電源がオンになっている場合は無効で、システムの電源がオフになっている場合に有効です。
[Power Off System] ボタン	仮想コンソール セッションからシステムの電源をオフにします。 このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。
[Reset System (warm boot)] ボタン	電源をオフにすることなくシステムを再起動します。 このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。
[Power Cycle System (cold boot)] ボタン	システムの電源をオフにしてから、再度オンにします。 このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。

[Virtual Media] メニュー

名前	説明
Activate Virtual Devices	vMedia セッションをアクティブにし、ユーザがローカル コンピュータまたはネットワークから、ドライブまたはイメージ ファイルをアタッチできるようにします。
[Map CD/DVD]	ローカル マシンから CD または DVD イメージをマップし、イメージにドライブをマップできます。 （注） このオプションは、[Activate Virtual Devices] をクリックした場合に使用できます。

名前	説明
[Map Removable Disk]	ローカル マシンから削除可能なディスク イメージをマップし、イメージにドライブをマップできます。 （注） このオプションは、[Activate Virtual Devices] をクリックした場合に使用できます。
[Map Floppy Disk]	ローカル マシンからフロッピー ディスク イメージをマップし、イメージにドライブをマップできます。 （注） このオプションは、[Activate Virtual Devices] をクリックした場合に使用できます。

[Help] メニュー

名前	説明
[Help Topics]	このオプションをクリックすると、このウィンドウに戻ります。
[About KVM Viewer]	KVM ビューアのバージョン番号を表示します。

Settings

[Settings] アイコンは、HTML KVM ビューア ウィンドウの右上隅にあります。

名前	説明
[Logged in as:]	ユーザ ロール ID を表示します。
[Host Name]	ホスト名を表示します。
[Log Out]	KVM ビューアからログアウトできます。

Java ベース KVM と HTML5 ベース KVM の比較

次の表に、Java ベース KVM と HTML5 ベース KVM の間の相違点を示します。

メニュー オプション	アクション	Java ベース KVM で使用可能	HTML5 ベース KVM で使用可能
ファイル	Open	Yes	該当なし
	Capture to file	対応	対応
	Paste Text from Clipboard	○	なし
	Paste Text from File	○	なし
	Exit	対応	対応
ビュー	Refresh	対応	対応
	Fit	○	なし
	Video-Scaling	○	なし
	Full-Screen	対応	対応
	Mini-Mod	○	なし
	Keyboard	NA	Yes
マクロ	Server Macros	対応	対応
	Static Macros	対応	対応
	User Defined Macros	対応	対応
	Manage	対応	対応
ツール	Session Option	対応	対応
	Single Cursor	○	なし
	Stats	○	なし
	Session User List	対応	対応
	チャット	対応	対応
	Recorder/Playback Controls	○	なし
	Export Video	○	なし
電源	Power On	対応	対応
	Power OFF	対応	対応
	Reset System	対応	対応

メニュー オプション	アクション	Java ベース KVM で使用可能	HTML5 ベース KVM で使用可能
	Power Cycle system	対応	対応
仮想メディア	Create Image	○	なし
	Activate Virtual Devices	対応	対応
	Physical Device Mapping	○	なし

仮想 KVM の設定

始める前に

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 [Compute] メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。

ステップ 3 作業ウィンドウの [Remote Management] タブをクリックします。

ステップ 4 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。

ステップ 5 [Virtual KVM] タブで、次のフィールドに値を入力します。

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、Cisco IMC 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] ドロップダウン リスト	許可されている KVM の同時セッションの最大数。選択できる数値は 1 ～ 4 です。
[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。

名前	説明
[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 6 [Save Changes] をクリックします。

仮想 KVM のイネーブル化

始める前に

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 [Compute] メニューをクリックします。
ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。
ステップ 3 作業ウィンドウの [Remote Management] タブをクリックします。
ステップ 4 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。
ステップ 5 [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 6 [Save Changes] をクリックします。

仮想 KVM のディセーブル化

始める前に

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 [Compute] メニューをクリックします。
ステップ 2 [コンピューティング（Compute）] メニューでサーバを選択します。
ステップ 3 作業ウィンドウの [Remote Management] タブをクリックします。
ステップ 4 [Remote Management] ペインで、[Virtual KVM] タブをクリックします。
ステップ 5 [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 6 [Save Changes] をクリックします。

ホスト イメージ マッピング

ホストイメージマッピング機能を使用すると、ホストイメージのダウンロード、マッピング、マッピング解除、または削除を行うことができます。Microsoft Windows、Linux、VMware などのホスト イメージを、リモート FTP または HTTP サーバから CIMC 内部リポジトリにダウンロードしてから、E シリーズ サーバまたはNCE内の USB コントローラの仮想ドライブにマップします。イメージをマップした後は、イメージをマウントした仮想ドライブが最初のブートデバイスになるようにブート順序を設定してから、サーバをリブートします。ホストイメージはファイル拡張子として .iso または .img がなければなりません。

また、ホスト イメージ マッピング機能により、診断イメージをダウンロードし、マウントできます。診断イメージのファイル拡張子は必ず .diag になります。

ホスト イメージのマッピング

始める前に

- admin 権限を持つユーザとして CIMC にログインします。
- 適切なサードパーティからホスト イメージ ファイルを取得します。

（注） VMware vSphere Hypervisor ではカスタマイズしたイメージが必要です。カスタマイズされたイメージをダウンロードするには、カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード （14 ページ）を参照してください。

（注） アップデートがすでに処理中であるときにイメージアップデートを開始すると、どちらのアップデートも失敗します。

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 3 [Host Image Mapping] ページで、[Add Image] をクリックします。

[Add New Mapping] ダイアログボックスが表示されます。次のフィールドに入力します。

名前	説明
[Server Type] ドロップダウン リスト	イメージが配置されているリモート サーバのタイプ。次のいずれかになります。 • **FTP** • **FTPS** • **HTTP** • **HTTPS** （注） 選択したリモート サーバによって、表示されるフィールドが変わります。
[Server IP Address] フィールド	リモート FTP または HTTP サーバの IP アドレス。
[File Path] フィールド	リモート FTP または HTTP サーバのパスおよびファイル名。 パスワードには、最大 80 文字を使用できます。 • ホスト イメージをインストールする場合、そのイメージのファイル拡張子は必ず .iso または .img になります。 • 診断イメージをインストールする場合、そのイメージのファイル拡張子は必ず .diag になります。
[Username] フィールド	リモート サーバのユーザ名。 ユーザ名は 1～20 文字の範囲で指定します。 （注） ユーザ名を設定しない場合は、ユーザ名として **anonymous** を入力し、パスワードとして任意の文字を入力します。
[Password] フィールド	ユーザ名のパスワード。 パスワードは 1～20 文字の範囲で指定します。 （注） ユーザ名を設定しない場合は、ユーザ名として **anonymous** を入力し、パスワードとして任意の文字を入力します。

ステップ 4 [Download] をクリックします。

[Host Image Mapping] ページが開きます。[Host Image Mapping Status] 領域で、イメージ ダウンロードのステータスを表示できます。イメージが正常にダウンロードされ、処理された後、ページがリフレッシュされます。ページがリフレッシュされた後、新しいイメージが [Image Information] 領域に表示されます。

ステップ 5 [Image Information] 領域で、マップするイメージを選択し、[Map Selected Image] をクリックします。

イメージがマップされ、USB コントローラの仮想ドライブにマウントされます。仮想ドライブには、次のいずれかを使用できます。

- 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
- CD/DVD：ブート可能 CD-ROM または DVD ドライブ

ステップ 6 イメージがマウントされている仮想ドライブが最初のブートデバイスになるように、ブート順を設定します。

ヒント イメージがどの仮想ドライブにマウントされているか確認するには、[Host Image Mapping] ページの [Host Image Update Status] 領域を参照してください。

ステップ 7 サーバをリブートします。

ステップ 8 イメージにアンサーファイルが含まれている場合、オペレーティング システムまたはハイパーバイザのインストールは自動化され、イメージがインストールされます。そうでない場合は、インストール ウィザードが表示されます。ウィザードの手順に従って、イメージをインストールします。

ステップ 9 オペレーティング システムまたはハイパーバイザをインストールした後にディスク ドライブが表示されない場合は、ドライバをインストールする必要があります。ドライバのインストール手順については、該当するオペレーティング システムまたはハイパーバイザのマニュアルを参照してください。

次のタスク

- 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。

ホスト イメージのマッピング解除

始める前に

admin 権限を持つユーザとして CIMC にログインします。

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 3 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 4 [Unmap Image] をクリックします。

USB コントローラの仮想ドライブから、マップされたイメージがアンマウントされます。

ホスト イメージの削除

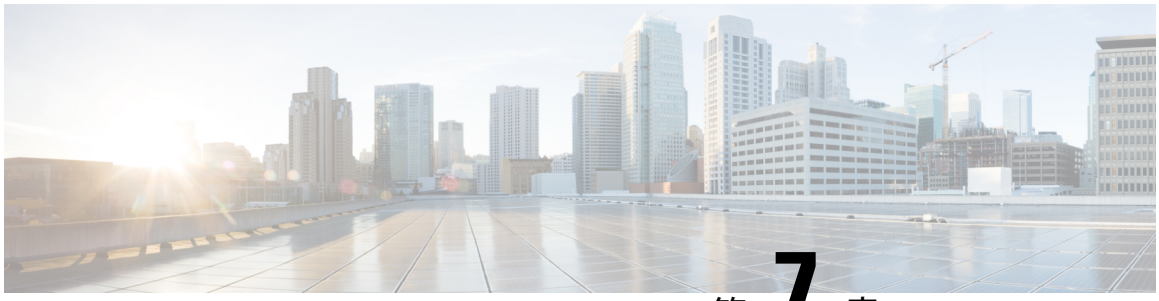
始める前に

admin 権限を持つユーザとして CIMC にログインします。

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。
ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。
ステップ 3 [Current Mappings Information] 領域で、削除するイメージを選択します。
ステップ 4 [Delete Selected Image] をクリックします。

イメージが SD カードから削除されます。



第 7 章

ユーザ アカウントの管理

この章は、次の項で構成されています。

- ローカル ユーザの設定 （87 ページ）
- パスワードの有効期限切れ （89 ページ）
- LDAP サーバ （90 ページ）
- ユーザ セッションの表示 （104 ページ）

ローカル ユーザの設定

Cisco IMC では、強力なパスワード ポリシーが実装されるようになったため、サーバに最初にログインした際に、ガイドラインに従って強力なパスワードを設定するよう要求されます。[Local User] タブには [Disable Strong Password] ボタンが表示され、そのボタンを使用することで、強力なパスワードポリシーを無効にし、ガイドラインを無視して希望するパスワードを設定することができます。強力なパスワードを無効にすると、[Enable Strong Password] ボタンが表示されます。デフォルトでは、強力なパスワード ポリシーが有効になっています。

始める前に

ローカルユーザアカウントを設定または変更するには、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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[User Management] をクリックします。

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

ステップ 4 ローカル ユーザ アカウントを設定または変更するには、[Local User Management] ペインの行をクリックして、[Modify User] をクリックします。

ステップ 5 [ユーザの詳細の変更（Modify 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] フィールド	ユーザの固有識別情報。
[Username] フィールド	ユーザのユーザ名。 1 ～ 16 文字の範囲で入力します。
[Role Played] フィールド	ユーザに割り当てられているロール。次のいずれかになります。 • [read-only]：このロール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]：このロールのユーザは、次のタスクを実行できます。 • 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 • タイム ゾーンを設定する • ping • [admin]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。
[Enabled] チェックボックス	オンにすると、ユーザは Cisco IMC でイネーブルになります。
[Change Password] チェックボックス	オンにすると、変更を保存した場合、このユーザのパスワードが変更されます。新しいユーザ名の場合は、このチェックボックスをオンにする必要があります。

名前	説明
[New Password] フィールド	このユーザ名のパスワード。フィールドの横の [Help] アイコンの上にカーソルを重ねると、パスワードを設定する際の以下のガイドラインが表示されます。 • パスワードは 8 ～ 20 文字とすること。 • パスワードにユーザ名を含めないこと。 • パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。 • 大文字の英字（A ～ Z）。 • 小文字の英字（a ～ z）。 • 10 進数の数字（0 ～ 9）。 • アルファベット以外の文字（!、@、#、$、%、^、&、*、-、_、=、'）。 これらのルールは、セキュリティ上の理由からユーザに強力なパスワードを定義するように意図されています。ただし、これらのガイドラインを無視して希望するパスワードを設定する場合は、[ローカル ユーザ（Local Users）] タブで [強力なパスワードの無効化（Disable Strong Password）] ボタンをクリックします。強力なパスワード オプションが無効にされている場合は、1 ～ 20 文字のパスワードを設定できます。
[Confirm New Password] フィールド	確認のためのパスワードの再入力。

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。

パスワードの有効期限切れ

パスワードの有効期限を設定することができ、その期限を過ぎるとパスワードは期限切れになります。管理者として、この時間を日数で設定できます。この設定は、すべてのユーザに共通です。パスワードの期限が切れると、ユーザはログイン時に通知され、パスワードをリセットしない限りログインできなくなります。

（注） 古いデータベースにダウングレードした場合、既存のユーザが削除されます。データベースはデフォルト設定に戻ります。以前に設定されたユーザは消去され、データベースは空になります。つまり、データベースのユーザ名はデフォルトの「admin」、パスワードは「password」となります。サーバにはデフォルトのユーザデータベースが残っているため、デフォルトのクレデンシャルの変更機能が有効になっています。これは、ダウングレード後に「admin」ユーザがデータベースに初めてログインする際に、そのユーザはデフォルトのクレデンシャルを強制的に変更する必要があることを意味します。

パスワード設定時刻

「パスワード設定時刻」は、すべての既存ユーザに対し、移行またはアップグレードが発生した時刻に設定されています。新規ユーザ（アップグレード後に作成されたユーザ）の場合、パスワード設定時刻は、ユーザが作成され、パスワードが設定された時刻に設定されます。一般ユーザ（新規および既存）の場合、パスワード設定時刻は、パスワードが変更されるたびに更新されます。

LDAP サーバ

Cisco IMC は、ディレクトリ内の情報を整理し、この情報へのアクセスを管理するディレクトリ サービスをサポートしています。Cisco IMC は、Lightweight Directory Access Protocol（LDAP）をサポートしています。これは、ネットワークでのディレクトリ情報を保存し維持するものです。さらに、Cisco IMC は Microsoft Active Directory（AD）もサポートします。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。Cisco IMC は LDAP での Kerberos ベースの認証サービスを利用します。

Cisco IMC で LDAP が有効になっている場合、ローカル ユーザ データベース内に見つからないユーザ アカウントに関するユーザ認証とロール許可は、LDAP サーバによって実行されます。LDAP ユーザ認証の形式は username@domain.com です。

LDAP サーバへの送信データを暗号化するようサーバに要求できます。

LDAP サーバの設定

ユーザ認証および権限付与のために LDAP を使用するよう、Cisco IMC を設定できます。LDAP を使用するには、Cisco IMC に関するユーザ ロール情報とロケール情報を保持する属性を使ってユーザを設定します。Cisco IMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用できます。または、LDAP スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair 属性などの新しいカスタム属性を追加できます。

重要 スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

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

LDAP サーバに対して次の手順を実行する必要があります。

手順

ステップ 1 LDAP 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 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属性を追加します。

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 スナップインを使用して、ユーザ クラスに CiscoAVPair 属性を追加します。

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 属性を選択します。

d) [OK] をクリックします。

ステップ 4 Cisco IMC 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 属性に追加します。

ロール	CiscoAVPair 属性値
admin	**shell:roles="admin"**
user	**shell:roles="user"**
read-only	**shell:roles="read-only"**

（注） 属性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 の記事を参照してください。

次のタスク

Cisco IMC を使用して LDAP サーバを設定します。

Cisco IMC での LDAP 設定およびグループ認証の設定

始める前に

このタスクを実行するには、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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[User Management] をクリックします。

ステップ 3 [User Management] ペインで、[LDAP] をクリックします。

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

名前	説明
[Enable LDAP] チェックボックス	これを選択した場合、まずLDAPサーバによってユーザ認証とロール許可が実行された後、ローカル ユーザ データベースに存在しないユーザ アカウントによって実行されます。
[Base DN] フィールド	ベース識別名。このフィールドは、ユーザおよびグループのロード元を示します。 Active Directory サーバでは、これは **dc=domain,dc=com** という形式でなければなりません。
[Domain] フィールド	すべてのユーザが属する必要のある IPv4 ドメイン。 グローバル カタログ サーバのアドレスを少なくとも 1 つ指定していない限り、このフィールドは必須です。
[Enable Encryption] チェックボックス	これを選択した場合、サーバは LDAP サーバに送るすべての情報を暗号化します。
[Enable Binding CA Certificate] チェックボックス	オンにすると、LDAP CA 証明書をバインドできます。

名前	説明
[Timeout (0 - 180) seconds]	LDAP 検索操作がタイムアウトするまで Cisco IMC が待機する秒数。 検索操作がタイムアウトになった場合、Cisco IMC はこのタブで次にリストされているサーバ（存在する場合）に接続しようと試行します。 （注） このフィールドに指定する値は、全体的な時間に影響を及ぼす可能性があります。
[User Search Precedence]	ローカル ユーザ データベースと LDAP ユーザ データベースの間の検索の順序を指定できます。次のいずれかになります。 • [Local User Database]（デフォルト設定） • **[LDAP User Database]**

（注） [暗号化を有効にする（Enable Encryption）] チェックボックスと [CA 証明書のバインディングの有効化（Enable Binding CA Certificate）] チェックボックスをオンにした場合は、[LDAP サーバ（LDAP Server）] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

ステップ 5 [LDAP サーバの設定（Configure LDAP Servers）] 領域で、次のプロパティを更新します。

名前	説明
[Pre-Configure LDAP Servers] オプション ボタン	これを選択すると、Active Directory は事前構成された LDAP サーバを使用します。
[LDAP Servers] フィールド	
[サーバ（Server）]	6 つの LDAP サーバの IP アドレス。 LDAP に Active Directory を使用している場合、サーバ1、2、3はドメイン コントローラ、サーバ4、5、6はグローバル カタログです。LDAP 用に Active Directory を使用していない場合は、最大で 6 つの LDAP サーバを構成できます。 （注） また、ホスト名の IP アドレスも提供できます。

名前	説明
Port	サーバのポート番号。 LDAP に Active Directory を使用している場合、サーバ 1、2、3（ドメイン コントローラ）のデフォルト ポート番号は 389 です。サーバ 4、5、6（グローバル カタログ）のデフォルト ポート番号は 3268 です。 LDAPS 通信は TCP 636 ポートで発生します。グローバル カタログ サーバへの LDAPS 通信は TCP 3269 ポートで発生します。
[Use DNS to Configure LDAP Servers] オプション ボタン	これを選択した場合、DNS を使って LDAP サーバへのアクセスを設定できます。
[DNS パラメータ（DNS Parameters）] フィールド	
[Source]	DNS SRV 要求に使われるドメイン名を取得する方法を指定します。次のいずれかを指定できます。 • [Extracted]： ログイン ID からのドメイン名抽出ドメインを使用するよう指定します。 • [Configured]：設定された検索ドメインの使用を指定します。 • [設定済み - 抽出済み（Configured-Extracted）]：設定された検索ドメインよりも、ログイン ID から抽出されるドメイン名を使用することを指定します。
[Domain to Search]	DNS クエリーのソースとして機能する設定済みドメイン名。 ソースが [抽出済み（Extracted）] と指定される場合、このフィールドは無効になります。
[Forest to Search]	DNS クエリーのソースとして機能する設定済みフォレスト名。 ソースが [Extracted] と指定される場合、このフィールドは無効になります。

ステップ 6 [Binding Parameters] 領域で、次のプロパティを更新します。

名前	説明
[Method]	次のいずれかを指定できます。 • [Anonymous]： ユーザ名とパスワードを NULL にする必要があります。このオプションが選択され、 LDAP サーバで匿名ログインが設定されている場合は、ユーザがアクセスすることができます。 • [Configured Credentials]： 初期バインド プロセスで既知のクレデンシャル セットを指定する必要があります。初期バインド プロセスが成功した場合、ユーザ名の Distinguished Name（DN）が照会され、再バインディング プロセス用に再利用されます。再バインディング プロセスが失敗すると、ユーザはアクセスを拒否されます。 • [Login Credentials]： ユーザ クレデンシャルが必要です。バインド プロセスが失敗すると、ユーザはアクセスを拒否されます。 デフォルトでは、[ログイン クレデンシャル（Login Credentials）] オプションが選択されます。
[Binding DN]	ユーザの識別名（DN）。このフィールドは、バインディング方式として [設定済みクレデンシャル（Configured Credentials）] オプションを選択した場合にのみ編集可能になります。
Password	ユーザのパスワード。このフィールドは、バインディング方式として [Configured Credentials] オプションを選択した場合にのみ編集可能になります。

ステップ 7 [Search Parameters] 領域で、次のフィールドを更新します。

名前	説明
[Filter Attribute]	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドには [sAMAccountName] と表示されます。

名前	説明
[Group Attribute]	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドには [memberOf] と表示されます。
[Attribute]	ユーザのロールとロケール情報を保持する LDAP 属性。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、この属性名と一致する値を検索します。 LDAP 属性では、Cisco IMC ユーザ ロールおよびロケールにマップされる既存の LDAP 属性を使用することも、スキーマを変更して新しい LDAP 属性を作成することもできます。（たとえば CiscoAvPair など）。 （注） このプロパティを指定しない場合、ユーザはログインできません。オブジェクトは LDAP サーバ上に存在していますが、このフィールドで指定される属性と正確に一致する必要があります。
Nested Group Search Depth (1-128)	LDAP グループ マップで別の定義済みグループ内にネストされた LDAP グループを検索するパラメータ。このパラメータでは、ネストされたグループ検索の深さを定義します。

ステップ 8 （任意） [Group Authorization] 領域で、次のプロパティを更新します。

名前	説明
[LDAP Group Authorization] チェックボックス	これを選択した場合、ローカル ユーザ データベースにない LDAP ユーザに関しても、グループ レベルでユーザ認証が実行されます。 このチェックボックスをオンにすると、Cisco IMC は [**Configure Group**] ボタンをイネーブルにします。
[Group Name] カラム	サーバへのアクセスが許可されているグループの名前を LDAP データベースに指定します。
[Group Domain] カラム	LDAP サーバのドメインがグループに存在する必要があります。

名前	説明
[Role] カラム	すべてのユーザに割り当てられているこの LDAP サーバ グループのロール。次のいずれかになります。 • [read-only]：このロール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]：このロールのユーザは、次のタスクを実行できます。 • 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 • タイム ゾーンを設定する • ping • [admin]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。
[Configure] ボタン	Active Directory グループを設定します。
[Delete] ボタン	既存の LDAP グループを削除します。

ステップ 9 [Save Changes] をクリックします。

LDAP 証明書の概要

Cisco E シリーズ サーバでは、LDAP バインディング ステップ時に、LDAP クライアントがインストール済み CA 証明書またはチェーン CA 証明書に対してディレクトリ サーバ証明書を検証できるようになっています。リモート ユーザ認証のために信頼されたポイントまたはチェーン証明書を Cisco IMC に入力できないことにより、誰でもユーザ認証用のディレクトリ サーバを複製してセキュリティ違反が発生する恐れがある場合は、この機能を導入します。

暗号化された TLS/SSL 通信中にディレクトリ サーバ証明書を検証するには、LDAP クライアントに新しい設定オプションが必要です。

LDAP CA 証明書ステータスの表示

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] メニューで、[User Management] をクリックします。

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

ステップ 4 [Certificate Status] 領域で、次のフィールドの値を確認します。

名前	説明
[Download Status]	このフィールドには、LDAP CA 証明書のダウンロード ステータスが表示されます。
[Eport Status]	このフィールドには、LDAP CA 証明書のエクスポート ステータスが表示されます。

LDAP CA 証明書のエクスポート

始める前に

このアクションを実行するには、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。

署名付き LDAP CA 証明書をエクスポートするには、あらかじめ証明書がダウンロードされ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] メニューで、[User Management] をクリックします。

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

ステップ 4 [Export LDAP CA Certificate] リンクをクリックします。

[Export LDAP CA Certificate] ダイアログボックスが表示されます。

名前	説明
[Export to Remote Location]	

名前	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用さ

名前	説明
	れません。 • [パスワード（Password）]フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Export to Local Desktop]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

ステップ 5 [Export Certificate] をクリックします。

LDAP CA 証明書のダウンロード

始める前に

- このアクションを実行するには、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。
- このアクションは、バインディング CA 証明書が有効にされていないと実行できません。

（注） Cisco IMC では CA 証明書またはチェーン CA 証明書のみを使用する必要があります。デフォルトの CA 証明書の形式は .cer です。チェーン CA 証明書を使用する場合は、Cisco IMC にダウンロードする前に .cer 形式に変換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] メニューで、[User Management] をクリックします。
ステップ 3 [User Management] ペインの **[LDAP]** タブをクリックします。
ステップ 4 [Download LDAP CA Certificate] リンクをクリックします。

[Download LDAP CA Certificate] ダイアログボックスが表示されます。

名前	説明
[Download from remote location] オプション ボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルを保管するサーバの IP アドレスまたはホスト名。[Download Certificate from] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [Path and Filename] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC に使用する必要があるパスおよびファイル名。 • [Username] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名前	説明
[Download through browser client] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）]ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[Paste Certificate content] オプション ボタン	このオプションを選択することで、署名付き証明書の内容をコピーして [Paste certificate content] テキスト フィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。
[Download Certificate] ボタン	証明書をサーバにダウンロードするために使用します。

LDAP バインディングのテスト

始める前に

このアクションを実行するには、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。

（注） [Enable Encryption] チェックボックスと [Enable Binding CA Certificate] チェックボックスをオンにする場合は、[LDAP Server] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

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] メニューで、[User Management] をクリックします。

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

ステップ 4 [Test LDAP Binding] リンクをクリックします。

[Test LDAP CA Certificate Binding] ダイアログボックスが表示されます。

名前	説明
[Username] フィールド	ユーザ名を入力します。

名前	説明
[Password] フィールド	対応するパスワードを入力します。

ステップ 5 [Test] をクリックします。

LDAP CA 証明書の削除

始める前に

このアクションを実行するには、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] メニューで、[User Management] をクリックします。
ステップ 3 [User Management] ペインの **[LDAP]** タブをクリックします。
ステップ 4 [Delete LDAP CA Certificate] リンクをクリックし、[OK] をクリックして確定します。

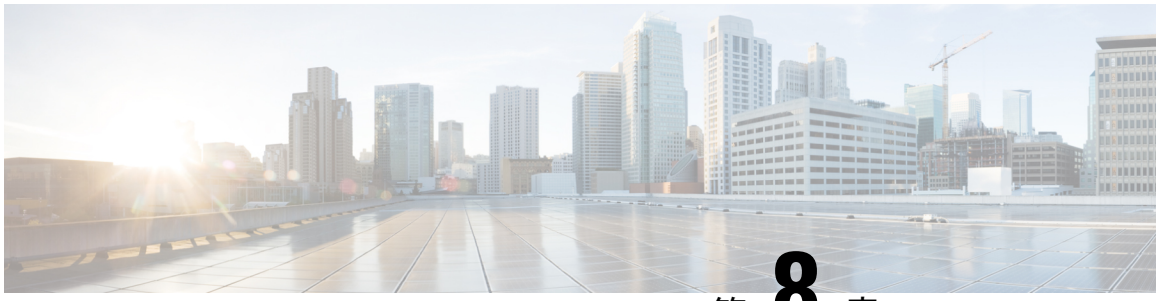
ユーザ セッションの表示

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。
ステップ 2 [Admin] メニューで、[User Management] をクリックします。
ステップ 3 [User Management] ペインで、[Session Management] をクリックします。
ステップ 4 [Sessions] ペインで、現在のユーザ セッションに関する次の情報を表示します。

名前	説明
[Session ID] カラム	セッションの固有識別情報。
[User name] 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。シリアル接続の場合は、[N/A] と表示されます。

名前	説明
[Type] カラム	ユーザがサーバにアクセスするために選択したセッション タイプ。次のいずれかになります。 • [webgui]：ユーザが Web UI を使用してサーバに接続されていることを示します。 • [CLI]：ユーザが CLI を使用してサーバに接続されていることを示します。 • [serial]：ユーザがシリアル ポートを使用してサーバに接続されていることを示します。



第 8 章

シャーシ関連の設定

この章は、次の項で構成されています。

- サーバの電源管理 （107 ページ）
- Web UI からのホスト名/IP アドレスへの Ping （107 ページ）
- 時間帯の選択 （108 ページ）

サーバの電源管理

始める前に

このタスクを実行するには、user または 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 [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューの [Summary] をクリックします。

ステップ 3 作業ウィンドウ上部のツールバーで、[Host Power] リンクをクリックします。

Web UI からのホスト名/IP アドレスへの Ping

始める前に

このタスクを実行するには、user または 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 作業ウィンドウ上部のツールバーで、[Ping] アイコンをクリックします。

ステップ 2 [**Ping Details**] ダイアログボックスで、次のフィールドを更新します。

Actions	説明
[*Hostname/IP Address] フィールド	到達するホスト名または IP アドレス。
[*Number of Retries] フィールド	IP アドレスに ping を送ることが許可された再試行の最大数。デフォルト値は 3 です。有効な範囲は 1 ～ 10 です。
[*Timeout] フィールド	ping の最大応答時間。デフォルト値は 10 秒です。有効な範囲は 1 ～ 20 秒です。
[Ping Status] フィールド	ping の結果を表示します。
[Details] ボタン	ping アクティビティの詳細を表示します。
[Ping] ボタン	IP アドレスを ping します。
[Cancel] ボタン	ping を実行せずにダイアログボックスを閉じます。

ステップ 3 [Ping] をクリックします。

時間帯の選択

始める前に

このタスクを実行するには、user または 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 [Chassis] メニューをクリックします。

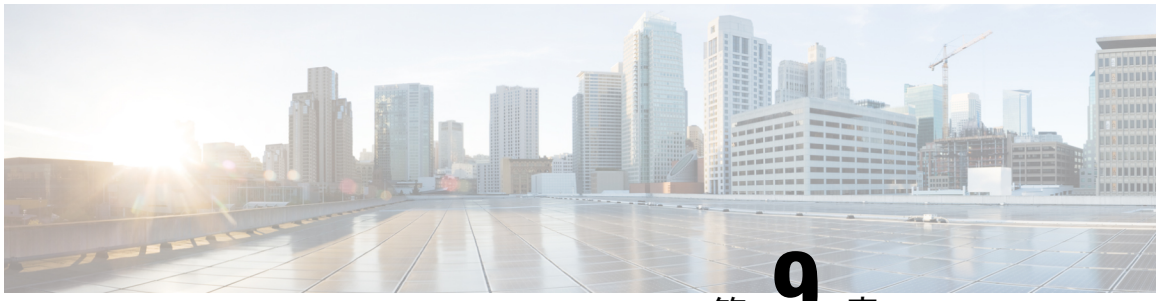
ステップ 2 [Chassis] メニューの [Summary] をクリックします。

ステップ 3 [Cisco Integrated Management Controller (Cisco IMC) Information] 領域で、[Select Timezone] をクリックします。

[Select Timezone] 画面が表示されます。

ステップ 4 [Select Timezone] ポップアップ画面で、マップの上にカーソルを移動してロケーションをクリックしてタイム ゾーンを選択するか、または [Timezone] ドロップダウン メニューからタイム ゾーンを選択します。

ステップ 5 **[保存（Save）]** をクリックします。



第 9 章

ネットワーク関連の設定

この章は、次の項で構成されています。

- サーバ NIC の設定 （111 ページ）
- 共通プロパティの設定 （112 ページ）
- ネットワーク セキュリティの設定 （114 ページ）
- ネットワーク タイム プロトコルの設定 （115 ページ）

サーバ NIC の設定

サーバの NIC

NIC モード

NIC モード設定は、Cisco IMC に到達できるポートを決定します。プラットフォームに応じて、次のネットワーク モード オプションを使用できます。

- [Dedicated]：Cisco IMC へのアクセスに使用される管理ポート。

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。

始める前に

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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Networking] をクリックします。

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

名前	説明Cisco IMC
[NIC Mode] ドロップダウン リスト	Cisco IMC へのアクセスに使用可能なポート。次のいずれかになります。 • [専用（Dedicated）]：Cisco IMC へのアクセスに使用される管理ポート。 • [Shared LOM]：CIMC へのアクセスにマザーボードのオンボード LAN（LOM）ポートを使用します。
[NIC Interface] フィールド	[NIC Mode] フィールドで選択されているネットワーク インターフェイス。

ステップ 4 [Save Changes] をクリックします。

共通プロパティの設定

共通プロパティの設定の概要

ホスト名

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）拡張機能は、ホスト名を DHCP パケットに追加することによって利用でき、DHCP サーバ側でこれを解釈または表示できます。ホスト名は DHCP パケットのオプション フィールドに追加され、最初に DHCP サーバに送信される DHCP DISCOVER パケットで送信されます。

サーバのデフォルトのホスト名は EXXXX-YYYYYYYYYYY です（XXXX はサーバのモデル番号で、YYYYYYYYYYY はシリアル番号です）。この一意のストリングはクライアント ID として機能し、DHCP サーバから Cisco IMC にリースされる IP アドレスを追跡してマッピングするのに役立ちます。サーバのステッカーまたはラベルとしてデフォルト シリアル番号が製造者から提供され、サーバを識別するのに役立ちます。

ダイナミック DNS

ダイナミック DNS（DDNS）は、Cisco IMC から DNS サーバのリソース レコードを追加または更新するために使用されます。Web UI または CLI を使用してダイナミック DNS をイネーブルにできます。[DDNS] オプションを有効にすると、DDNS サービスは現在のホスト名、ドメイン名、および管理 IP アドレスを記録し、Cisco IMC から DNS サーバのリソース レコードを更新します。

（注） DDNS サーバは、次の DNS 設定のいずれかが変更された場合に、DNS サーバの以前のリソース レコード（もしあれば）を削除し、新しいリソース レコードを追加します。

- ホスト名
- LDAP 設定のドメイン名
- DDNS と DHCP がイネーブルの場合に、ネットワークまたはサブネットの変更による新しい IP アドレスまたは DNS IP またはドメイン名を DHCP が取得する場合。
- DHCP がディセーブルの場合に、CLI または Web UI を使用してスタティック IP アドレスを設定する場合。
- **dns-use-dhcp** コマンドを入力する場合。

[**Dynamic DNS Update Domain**]：ドメインを指定できます。ドメインは、メイン ドメインまたはサブ ドメインのどちらでも可です。このドメイン名は、DDNS 更新のため Cisco IMC のホスト名に付加されます。

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。

始める前に

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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Networking] をクリックします。

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

a) [Management Hostname] フィールドに、ホストの名前を入力します。

デフォルトでは、ホスト名は EXXXX-YYYYYYYYYYY 形式で表示されます（XXXX はサーバのモデル番号、YYYYYYYYYYY はシリアル番号です）。

（注） また、DHCP が有効である場合、発信される DHCP DISCOVER パケットにも Cisco IMC ホスト名が含まれます。

b) [Dynamic DNS] チェックボックスをオンにします。

c) [**Dynamic DNS Update Domain**] フィールドに、ドメイン名を入力します。

ステップ 4 [Save Changes] をクリックします。

ネットワーク セキュリティの設定

ネットワーク セキュリティ

Cisco IMC 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、サービス拒否（DoS）攻撃から保護するために使用されます。Cisco IMC 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。

始める前に

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] メニューをクリックします。

ステップ 2 [Networking] ペインで、[Network Security] をクリックします。

ステップ 3 [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。

名前	説明
[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 4 [IP Filtering] 領域で、次のプロパティを更新します。

名前	説明
[Enable IP Filtering] チェックボックス	IP フィルタリングをイネーブルにするには、このボックスをオンにします。
[IP フィルタ（IP Filter）] フィールド	サーバへのセキュアなアクセスを提供するために、選択した IP のセットのみにアクセスを許可するフィルタを設定できるようになりました。このオプションでは、IP アドレスを保存するための 4 つのスロット（IP フィルタ 1、2、3、および 4）が提供されます。IP フィルタの設定時に、単一の IP アドレスまたは IP アドレスの範囲を割り当てることができます。IP フィルタを設定すると、他の IP アドレスを使用してサーバにアクセスできなくなります。

ステップ 5 [Save Changes] をクリックします。

ネットワーク タイム プロトコルの設定

ネットワーク タイム プロトコル サービス設定

デフォルトでは、Cisco IMC がリセットされると、ホストと時刻が同期されます。NTP サービスを導入すると、Cisco IMC を設定して NTP サーバで時刻を同期することができます。デフォルトでは、NTP サーバは Cisco IMC で動作しません。少なくとも 1 台、最大 4 台の、NTP サーバまたは時刻源サーバとして動作するサーバの IP/DNS アドレスを指定し、NTP サービスをイネーブルにして設定する必要があります。NTP サービスをイネーブルにすると、Cisco IMC は設定された NTP サーバと時刻を同期します。NTP サービスは Cisco IMC でのみ変更できます。

（注） NTP サービスをイネーブルにするには、DNS アドレスよりも、サーバの IP アドレスを指定することを推奨します。

ネットワーク タイム プロトコル設定の設定

NTP を設定すると、IPMI の **Set SEL time** コマンドはディセーブルになります。

始める前に

このタスクを実行するには、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] メニューをクリックします。

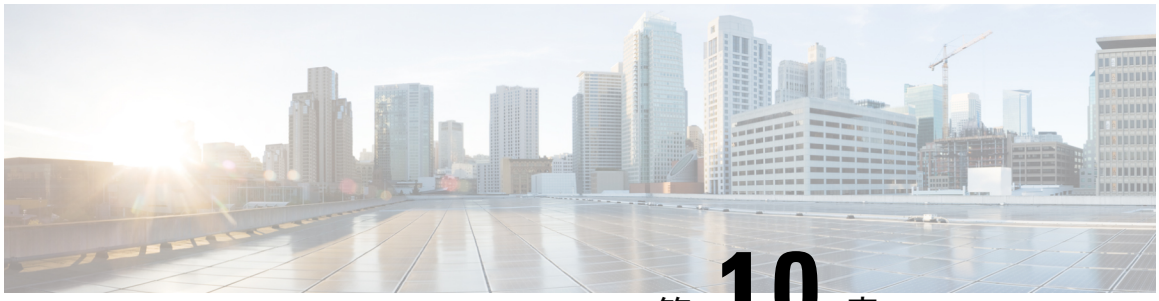
ステップ 2 [Admin] メニューで、[Networking] をクリックします。

ステップ 3 [Networking] ペインで、[NTP Setting] をクリックします。

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

名前	説明
[Enable NTP]	NTP サービスをイネーブルにするには、このボックスをオンにします。
[Server 1]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Server 2]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Server 3]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Server 4]	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[Status] メッセージ	サーバがリモートの NTP サーバと時刻を同期できるかどうかを示します。次のいずれかになります。 • [synchronized to NTP server (RefID) at stratum 7]：NTP サービスが有効で、複数または個々の IPv4 または IPv6 ベースの NTP サーバが追加される場合。 • [unsynchronized]：NTP サービスが有効で、不明または到達不能なサーバが追加される場合。 • [NTP service disabled]：NTP サービスが無効な場合。

ステップ 5 [Save Changes] をクリックします。



第 10 章

ストレージ アダプタの管理

この章は、次の項で構成されています。

- ストレージ アダプタの管理 （117 ページ）

ストレージ アダプタの管理

自己暗号化ドライブ（フル ディスク暗号化）

Cisco IMC は、自己暗号化ドライブ（SED）をサポートしています。ドライブ内の特別なハードウェアがリアルタイムで入力データを暗号化し、出力データを復号します。この機能は、フル ディスク暗号化（FDE）とも呼ばれます。

ドライブ上のデータは、ドライブに入力される際に暗号化され、出力される際に復号されます。ただし、ドライブをロックしている場合は、データを取得するためにセキュリティ キーは必要ありません。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。データをこのように保存すると、データを非暗号化してドライブから取得するためにセキュリティ キーが必要になります。ドライブのロックを解除すると、その暗号化キーが削除され、保存されたデータは使用できなくなります。これは、Secure Erase と呼ばれます。FDE は、キー ID とセキュリティ キーで構成されます。

FDE 機能は次の操作をサポートしています。

- コントローラでのセキュリティの有効化および無効化
- セキュアな仮想ドライブの作成
- 非セキュアなドライブ グループの保護
- 外部の設定ドライブのロック解除
- 物理ドライブ（JBOD）でのセキュリティの有効化
- セキュアな SED ドライブのクリア

- セキュアな外部設定のクリア

デュアル SIOC 環境でのコントローラ セキュリティの設定時に考慮するシナリオ

（注） デュアル SIOC 接続は、一部のサーバでのみ使用できます。

コントローラのセキュリティは、個別に有効、無効、または変更できます。ただし、ローカル キー管理とリモート キー管理は、サーバ上のすべてのコントローラに適用されます。したがって、キー管理モードの切り替えを伴うセキュリティ アクションは慎重に行う必要があります。両方のコントローラが安全で、コントローラの 1 つを別のモードに移動する場合は、もう一方のコントローラでも同じ操作を実行する必要があります。

次の 2 つのシナリオを考えてみましょう。

- シナリオ 1：キー管理はリモートに設定されています。両方のコントローラは安全で、リモート キー管理を使用します。ローカル キー管理に切り替える場合は、各コントローラのキー管理を切り替えて、リモート キー管理を無効にします。
- シナリオ2：キー管理はローカルに設定されています。両方のコントローラは安全で、ローカル キー管理を使用します。リモート キー管理に切り替える場合は、リモート キー管理を有効にして、各コントローラのキー管理を切り替えます。

いずれかのコントローラでコントローラ セキュリティ方式を変更しないと、セキュアなキー管理がサポートされていない設定状態になります。

未使用の物理ドライブからの仮想ドライブの作成

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [Actions] 領域で、[Create Virtual Drive from Unused Physical Drives] をクリックします。

[Create Virtual Drive from Unused Physical Drives] ダイアログボックスが表示されます。

ステップ 4 [Create Virtual Drive from Unused Physical Drives] ダイアログボックスで、新しい仮想ドライブの RAID レベルを選択します。

次のいずれかになります。

- [Raid 0]：単純なストライピング。

- [Raid 1]：単純なミラーリング。
- [Raid 5]：パリティ付きストライピング。
- [Raid 6]：2 つのパリティ ドライブによるストライピング。
- [Raid 10]：スパンされたミラーリング。
- [Raid 50]：パリティ付きのスパンされたストライピング。
- [Raid 60]：2 つのパリティ ドライブによるスパンされたストライピング。

ステップ 5 [Create Drive Groups] 領域で、グループに含める 1 つ以上の物理ドライブを選択します。

[Drive Groups] テーブルにドライブを追加するには、[>>] ボタンを使用します。ドライブ グループから物理ドライブを削除するには、[<<] ボタンを使用します。

（注） ドライブ グループで最も小さな物理ドライブのサイズによって、すべての物理ドライブに使用される最大サイズが定義されます。すべての物理ドライブの領域の最大使用を保証するには、ドライブ グループ内のすべてのドライブのサイズをほぼ同じにすることを推奨します。

（注） Cisco IMC は、RAID コントローラのみを管理し、サーバに接続された HBA は管理しません。

ステップ 6 [Virtual Drive Properties] 領域で、次のプロパティを更新します。

名前	説明
[Virtual Drive Name] フィールド	作成する新しい仮想ドライブの名前。
[Read Policy] ドロップダウン リスト	先行読み出しキャッシュ モード。
[キャッシュ ポリシー（Cache Policy）] ドロップダウン リスト	バッファリング読み取りに使用されるキャッシュ ポリシー。
[Strip Size] ドロップダウン リスト	各ストライプのサイズ（KB 単位）。

名前	説明
[書き込みポリシー（Write Policy）] ドロップダウン リスト	次のいずれかになります • [Write Through]：データがキャッシュによって、物理ドライブに書き込まれます。以降の該当データのキャッシュからの読み取りが充足されるため、パフォーマンスが改善されます。 • [Write Back]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。このポリシーを必要とする仮想ドライブは、電源障害の発生時にBBUでキャッシュの安全性を確保できない場合、[Write Through] キャッシングにフォールバックします。 • [書き込みバック不良BBU（Write Back Bad BBU）]：このポリシーでは、バッテリバックアップユニットに欠陥があったり、放電していたりする場合でも、書き込みキャッシングは [書き込みバック（Write Back）] のままです。
[Disk Cache Policy] ドロップダウン リスト	次のいずれかになります • [Unchanged]：ディスク キャッシュ ポリシーは変更されません。 • [Enabled]：ディスクで IO キャッシングを許可します。 • [Disabled]：ディスク キャッシングを許可しません。
[Access Policy] ドロップダウン リスト	次のいずれかになります • [Read Write]：ホストが VD で読み取り/書き込みを実行できます。 • [Read Only]：ホストは VD から読み取りのみ行うことができます。 • [Blocked]：ホストは VD の読み取りおよび書き込みができません。
[Size] フィールド	作成する仮想ドライブのサイズ。値を入力し、次のいずれかの単位を選択します。 • MB • GB • TB

ステップ 7 [Generate XML API Request] ボタンをクリックして、API 要求を生成します。

ステップ 8 [Close] をクリックします。

ステップ 9 [Create Virtual Drive] をクリックします。

既存のドライブ グループからの仮想ドライブの作成

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [Actions] 領域で、[Create Virtual Drive from an Existing Virtual Drive Group] をクリックします。

[Create Virtual Drive from an Existing Virtual Drive Group] ダイアログボックスが表示されます。

ステップ 4 [Create Virtual Drive from an Existing Virtual Drive Group] ダイアログボックスで、新しい仮想ドライブの作成に使用するドライブ グループの仮想ドライブを選択します。

ステップ 5 [Virtual Drive Properties] 領域で、次のプロパティを更新します。

名前	説明
[Virtual Drive Name] フィールド	作成する新しい仮想ドライブの名前。
[Read Policy] ドロップダウン リスト	先行読み出しキャッシュ モード。
[キャッシュ ポリシー（Cache Policy）] ドロップダウン リスト	バッファリング読み取りに使用されるキャッシュ ポリシー。
[Strip Size] ドロップダウン リスト	各ストライプのサイズ（KB 単位）。

名前	説明
[書き込みポリシー（Write Policy）] ドロップダウン リスト	次のいずれかになります • [Write Through]：データがキャッシュによって、物理ドライブに書き込まれます。以降の該当データのキャッシュからの読み取りが充足されるため、パフォーマンスが改善されます。 • [Write Back]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。このポリシーを必要とする仮想ドライブは、電源障害の発生時にBBUでキャッシュの安全性を確保できない場合、[Write Through] キャッシングにフォールバックします。 • [書き込みバック不良BBU（Write Back Bad BBU）]：このポリシーでは、バッテリバックアップユニットに欠陥があったり、放電していたりする場合でも、書き込みキャッシングは [書き込みバック（Write Back）] のままです。
[Disk Cache Policy] ドロップダウン リスト	次のいずれかになります • [Unchanged]：ディスク キャッシュ ポリシーは変更されません。 • [Enabled]：ディスクで IO キャッシングを許可します。 • [Disabled]：ディスク キャッシングを許可しません。
[Access Policy] ドロップダウン リスト	次のいずれかになります • [Read Write]：ホストが VD で読み取り/書き込みを実行できます。 • [Read Only]：ホストは VD から読み取りのみ行うことができます。 • [Blocked]：ホストは VD の読み取りおよび書き込みができません。
[Size] フィールド	作成する仮想ドライブのサイズ。値を入力し、次のいずれかの単位を選択します。 • MB • GB • TB

ステップ 6 [Generate XML API Request] ボタンをクリックして、API 要求を生成します。

ステップ 7 [Close] をクリックします。

ステップ 8 [Create Virtual Drive] をクリックします。

仮想ドライブのトランスポート可能状態の設定

仮想ドライブを MegaRAID コントローラ間で移動するには、[Set Transport Ready] 機能を使用します。この機能を使用すると、仮想ドライブの保留中 IO アクティビティがすべて完了されてから仮想ドライブがオペレーティング システムから隠され、キャッシュがフラッシュされ、すべてのバックグラウンド操作が一時停止された後、現在の進行状況がディスク データ フォーマットに保存されます。これにより、ドライブを移動することが可能になります。仮想ドライブを移動すると、その仮想ドライブと同じドライブ グループに属する他のすべてのドライブが移動されたドライブと同じ変更を継承します。

グループに設定された最後の物理ドイブが現在のコントローラから除去されると、そのドライブ グループは外部ドライブ グループとなり、外部構成ルールのすべてが適用されます。ただし、トランスポート準備機能によって外部構成の動作が変更されることはありません。

仮想ドライブをトランスポート可能状態から解除することもできます。これにより、仮想ドライブがオペレーティング システムで使用可能になります。

トランスポート可能状態の仮想ドライブには、次の制限が適用されます。

- 現在、最大で 16 個のトランスポート可能状態のドライブ グループがサポートされています。
- この機能は、ハイ アベイラビリティ構成ではサポートされません。
- 次の場合は、仮想ドライブをトランスポート可能状態に設定することはできません。
  - ドライブ グループの仮想ドライブが再構成中の場合
  - ドライブ グループの仮想ドライブに固定キャッシュが含まれている場合
  - ドライブ グループの仮想ドライブがキャッシュ可能としてマークされているか、CacheCade 仮想ドライブに関連付けられている場合
  - 仮想ドライブが CacheCade 仮想ドライブの場合
  - 仮想ドライブがオフラインの場合
  - 仮想ドライブがブート可能な仮想ドライブの場合

トランスポート可能としての仮想ドライブの設定

始める前に

- このタスクを実行するには、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。

- 仮想ドライブをトランスポート可能にするには、仮想ドライブが最適な状態になっていなければなりません。

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [Work] ペインで [Virtual Drive Info] タブをクリックします。

ステップ 4 [Virtual Drives] 領域で、トランスポート可能として設定するドライブを選択します。

ステップ 5 [Actions] 領域で、[Set Transport Ready] をクリックします。

[Set Transport Ready] ダイアログボックスが表示されます。

ステップ 6 この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
[Initialize Type] ドロップダウンリスト	選択した仮想ドライブをトランスポート可能として設定するために使用する初期化タイプを選択できます。次のいずれかになります。 • [Exlude All]：専用ホットスペア ドライブをすべて除外します。 • [Include All]：排他的に使用可能な専用ホットスペア ドライブまたは共有される専用ホットスペア ドライブをすべて含めます。 • [Include Dedicated Hot Spare Drive]：排他的に使用可能な専用ホットスペア ドライブを含めます。
[Set Transport Ready] ボタン	選択した仮想ドライブをトランスポート可能として設定します。
[Cancel] ボタン	操作をキャンセルします。

（注） 仮想ドライブをトランスポート可能として設定すると、その仮想ドライブに関連付けられているすべての物理ドライブが [Ready to Remove] として表示されます。

仮想ドライブのトランスポート可能状態の解除

始める前に

- このタスクを実行するには、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。

- 仮想ドライブがトランスポート可能状態になっている必要があります。

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [Work] ペインで [Virtual Drive Info] タブをクリックします。

ステップ 4 [Virtual Drives] 領域でトランスポート可能として設定されているドライブを選択します。

ステップ 5 [Actions] 領域で、[Clear Transport Ready] をクリックします。

これにより、選択したトランスポート可能な仮想ドライブが元の最適な状態に戻されます。

外部設定のインポート

別のコントローラで以前に設定されている 1 つ以上の物理ドライブがサーバにインストールされると、それらは外部設定として識別されます。コントローラにこれらの外部設定をインポートできます。

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [RAID controller] 領域に、[Controller Info] タブがデフォルトで表示されます。

ステップ 3 [**Actions**] 領域で、[**Import Foreign Config**] をクリックします。

（注） KMIP が有効になっていない場合は、[Secure Key Verification] ダイアログボックスが表示され、外部設定のインポート プロセスを開始するためのセキュリティ キーを入力するように指示されます。

KMIP が有効な場合は、[セキュアキー検証（Secure Key Verification）] ダイアログボックスに次のようなメッセージが表示されます。「ドライブのセキュリティがリモートキー管理により有効になっている場合、セキュリティ キーの指定は任意です（*If drive security has been enabled via remote key management, specifying Security key is optional.*）」。*Click on verify to start foreign configuration import.*」

これにより、セキュリティ キーを入力せずに [Verify] をクリックし、インポートを開始することができます。

ステップ 4 [OK] をクリックして確定します。

外部設定のクリア

重要 このタスクでは、コントローラのすべての外部設定をクリアします。また、外部設定をホスティングしているすべての物理ドライブからすべての設定情報が削除されます。このアクションは元に戻せません。

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
[RAID Controller] 領域に、[Controller Info] タブがデフォルトで表示されます。

ステップ 3 [Actions] 領域で、[Clear Foreign Config] をクリックします。

ステップ 4 [OK] をクリックして確定します。

ブート ドライブのクリア

重要 このタスクでは、コントローラのブート ドライブ設定がクリアされます。このアクションは元に戻せません。

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
[RAID Controller] 領域に、[Controller Info] タブがデフォルトで表示されます。

ステップ 3 [**Actions**] 領域で、[**Clear Boot Drive**] をクリックします。

ステップ 4 [OK] をクリックして確定します。

JBOD モードのイネーブル化

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、未設定の適切なドライブを選択します。
ステップ 5 [アクション（Actions）] 領域で [JBOD の有効化（Enable JBOD）] をクリックします。
ステップ 6 [**OK**] をクリックして確定します。

JBOD のディセーブル化

（注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

始める前に

JBOD オプションは、選択したコントローラに対してイネーブルにする必要があります。

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、JBOD ドライブを選択します。
ステップ 5 [アクション（Actions）] 領域で [JBOD の無効化（Disable JBOD）] をクリックします。
ステップ 6 [**OK**] をクリックして確定します。

コントローラのストレージ ファームウェア ログの取得

このタスクは、コントローラのストレージ ファームウェア ログを取得し、それを /var/log の場所に配置します。これにより、テクニカル サポート データが要求された場合にこのログ データを確実に使用できるようになります。

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 作業領域に、[Controller Info] タブがデフォルトで表示されます。

ステップ 3 [Actions] 領域で、[Get Storage Firmware Log] をクリックします。

ステップ 4 [OK] をクリックして確定します。

重要 コントローラのストレージ ファームウェア ログを取得するには 2 ～ 4 分かかる場合があります。このプロセスが完了するまで、テクニカル サポート データのエクスポートを開始しないでください。

コントローラの設定のクリア

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [Controller Info] 領域で、[Clear All Configuration] をクリックします。

ステップ 4 [OK] をクリックして確定します。

これにより、既存のコントローラ設定がクリアされます。

削除するドライブの準備

（注） [Unconfigured Good] ステータスを表示する物理ドライブのみでこのタスクを実行できます。

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、削除するドライブを選択します。
ステップ 5 [Actions] 領域で、[Prepare for Removal] をクリックします。
ステップ 6 [OK] をクリックして確定します。

削除するドライブの準備の取り消し

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、[Ready to Remove] 状態のドライブを選択します。
ステップ 5 [Actions] 領域で、[Undo Prepare for Removal] をクリックします。
ステップ 6 [OK] をクリックして確定します。

専用ホット スペアの作成

始める前に

このタスクを実行するには、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 **[Storage]** タブをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、専用ホット スペアを作成する未設定の適切なドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[専用ホット スペアの作成（Make Dedicated Hot Spare）] をクリックします。

[Make Dedicated Hot Spare] ダイアログボックスが表示されます。

ステップ 6 [Virtual Drive Details] 領域で、次のプロパティを更新します。

名前	説明
[Virtual Drive Number] ドロップダウン リスト	ホット スペアとして物理ドライブを専用する仮想ドライブを選択します。
[Virtual Drive Name] フィールド	選択された仮想ドライブの名前。
[専用ホット スペアの作成（Make Dedicated Hot Spare）] ボタン	専用のホット スペアを作成します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

ステップ 7 [Make Dedicated Hot Spare] をクリックして確定します。

グローバル ホット スペアの作成

始める前に

このタスクを実行するには、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 **[Storage]** タブをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、グローバル ホット スペアを作成する未設定の適切なドライブを選択します。
ステップ 5 [Actions] 領域で、[Make Global Hot Spare] をクリックします。

ホット スペア プールからのドライブの削除

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。
ステップ 2 [ストレージ（Storage）] タブで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [Work] ペインで [Physical Drive Info] タブをクリックします。
ステップ 4 [Physical Drives] 領域で、ホット スペア プールから削除するグローバル ホット スペアまたは専用ホット スペアを選択します。
ステップ 5 [Actions] 領域で、[Remove From Hot Spare Pools] をクリックします。

物理ドライブのステータスの切り替え

始める前に

- このタスクを実行するには、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。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルにする必要があります。

手順

ステップ 1 [Navigation] ペインの **[Storage]** タブをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、unconfigured good として設定するドライブを選択します。

ステップ 5 [**Actions**] 領域で、[**Set State as Unconfigured Good**] をクリックします。

ステップ 6 [**OK**] をクリックして、JBOD モードがディセーブルになっていることを確認します。

[**Set State as JBOD**] オプションがイネーブルになります。

ステップ 7 物理ドライブの JBOD モードをイネーブルにするには、[**Set State as JBOD**] をクリックします。

ステップ 8 [OK] をクリックして確定します。

[**Set State as Unconfigured Good**] オプションがイネーブルになります。

コントローラのブート ドライブとしての物理ドライブの設定

始める前に

- このタスクを実行するには、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。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルにする必要があります。

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Physical Drive Info] タブをクリックします。

ステップ 4 [Physical Drives] 領域で、コントローラのブート ドライブとして設定するドライブを選択します。

ステップ 5 [Actions] 領域で、[Set as Boot Drive] をクリックします。

ステップ 6 [OK] をクリックして確定します。

仮想ドライブの初期化

ドライブを初期化すると、仮想ドライブ上のすべてのデータが失われます。初期化を実行する前に、保存する仮想ドライブのデータをバックアップします。

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。

ステップ 4 [Virtual Drives] 領域で、初期化するドライブを選択します。

ステップ 5 [Actions] 領域で、[Initialize] をクリックします。

[Initialize Virtual Drive] ダイアログボックスが表示されます。

ステップ 6 仮想ドライブに使用する初期化のタイプを選択します。

次のいずれかになります。

- [Fast Initialize]：このオプションは、仮想ドライブへのデータの書き込みをすぐに開始できます。
- [Full Initialize]：新しい設定で完全な初期化が実行されます。初期化が完了するまで、新しい仮想ドライブにデータを書き込むことができません。

ステップ 7 [Initialize VD] をクリックしてドライブを初期化するか、[Cancel] をクリックして、変更を行わずにダイアログボックスを閉じます。

ステップ 8 ドライブで実行しているタスクのステータスを表示するには、[Operations] 領域で [Refresh] をクリックします。

次の詳細情報が表示されます。

名前	説明
[Operation]	ドライブで実行中の操作の名前。
[Progress in %]	操作の進行状況（完了した割合）。
[Elapsed Time in secs]	操作開始から経過した時間（秒数）。

ブート ドライブとしての設定

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。

ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、コントローラが起動する必要のあるドライブを選択します。
ステップ 5 [Actions] 領域で、[Set as Boot Drive] をクリックします。
ステップ 6 [OK] をクリックして確定します。

仮想ドライブの編集

手順

ステップ 1 [Navigation] ペインの [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、[Edit Virtual Drive] をクリックします。
ステップ 5 この説明を確認してから、[OK] をクリックします。
[Edit Virtual Drive] ダイアログボックスが表示され、データをバックアップするよう指示されます。
ステップ 6 [移行する RAID レベルを選択（Select RAID Level to migrate）] ドロップダウン リストから、RAID レベルを選択します。

RAID のマイグレーション基準については次の表を参照してください。

名前	説明
[**Select RAID Level to migrate**] ドロップダウン リスト	移行する RAID レベルを選択します。移行は次の RAID レベルで許可されています。 • **[RAID 0]** から **[RAID 1]** へ • **[RAID 0]** から **[RAID 5]** へ • **[RAID 0]** から **[RAID 6]** へ • **[RAID 1]** から **[RAID 0]** へ • **[RAID 1]** から **[RAID 5]** へ • **[RAID 1]** から **[RAID 6]** へ • **[RAID 5]** から **[RAID 0]** へ • [RAID 5] から [RAID 1] へ • [RAID 5] から [RAID 6] へ ある raid レベルから別のレベルに移行する場合、新しいRAIDレベルのデータ アームは、既存のもの以上である必要があります。 RAID 6 の場合、RAID 6 には二重分散パリティがあるため、データ アームはドライブ数から 2 を引いた数になります。たとえば、8 台のドライブで RAID 6 を作成する場合、データ アームの数は 8 – 2 = 6 となります。この場合、RAID 6 から RAID 0 に移行する場合は、RAID 0 には最低 6 台のドライブが必要です。それより少ないドライブ数を選択すると、[**Edit**] または [**Save**] ボタンが無効になります。 追加する場合は、ドライブを削除しないままでRAID 0に移行できます。 （注） RAID レベルの移行は、次の場合にはサポートされません。 • RAID グループに複数の仮想ドライブがある場合。 • SSD/HDD RAID グループの組み合わせがある場合。

ステップ 7 [Virtual Drive Properties] 領域の [**Write Policy**] ドロップダウン リストから、次のいずれかを選択します。

- [Write Through]：データがキャッシュによって、物理ドライブに書き込まれます。以降の該当データのキャッシュからの読み取りが充足されるため、パフォーマンスが改善されます。

- [Write Back]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。このポリシーを必要とする仮想ドライブは、電源障害の発生時に BBU でキャッシュの安全性を確保できない場合、[Write Through] キャッシングにフォールバックします。
- [書き込みバック不良 BBU（Write Back Bad BBU）]：このポリシーでは、バッテリ バックアップユニットに欠陥があったり、放電していたりする場合でも、書き込みキャッシングは [書き込みバック（Write Back）] のままです。

ステップ 8 [Save Changes] をクリックします。

仮想ドライブの削除

重要 このタスクでは、ブートされたオペレーティング システムを実行するドライブを含む仮想ドライブを削除します。そのため、仮想ドライブを削除する前に、保持するデータをバック アップします。

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、削除する仮想ドライブを選択します。
ステップ 5 [Actions] 領域で、[Delete Virtual Drive] をクリックします。
ステップ 6 [OK] をクリックして確定します。

仮想ドライブの非表示

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Virtual Drive Info] タブをクリックします。
ステップ 4 [Virtual Drives] 領域で、非表示にする仮想ドライブを選択します。
ステップ 5 [Actions] 領域で、[Hide Drive] をクリックします。
ステップ 6 [OK] をクリックして確定します。

バッテリ バックアップ ユニットの学習サイクルの開始

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Battery Backup Unit] タブをクリックします。
ステップ 4 [Actions] ペインで [Start Learn Cycle] をクリックします。
ダイアログでタスクを確認するためのプロンプトが表示されます。
ステップ 5 [OK] をクリックします。

ストレージ コントローラのログの表示

始める前に

このタスクを実行するには、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 [Storage] メニューをクリックします。
ステップ 2 [Storage] メニューで、適切な LSI MegaRAID コントローラをクリックします。
ステップ 3 [RAID Controller] 領域で、[Storage Log] タブをクリックし、次の情報を確認します。

名前	説明
[Time] 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。次のいずれかになります。 • [Emergency] • [Alert] • [Critical] • [Error] • Warning • [Notice] • [Informational] • デバッグ（Debug）
[Description] カラム	イベントの説明。

第 11 章

コミュニケーション サービスの設定

この章は、次の項で構成されています。

- HTTP の設定 （139 ページ）
- SSH の設定 （140 ページ）
- Redfish の設定 （141 ページ）
- XML API の設定 （142 ページ）
- IPMI の設定 （142 ページ）
- SNMP の設定 （144 ページ）

HTTP の設定

始める前に

このタスクを実行するには、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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[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 Cisco IMC でイネーブルかどうか。
[Redirect HTTP to HTTPS Enabled] チェックボックス	イネーブルの場合、HTTP 経由で試行される通信はすべて同等の HTTPS アドレスにリダイレクトされます。 HTTP をイネーブルにしている場合は、このオプションをイネーブルにすることを強く推奨します。

名前	説明
[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。
[Session Timeout] フィールド	HTTP 要求の間、Cisco IMC 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	Cisco IMC 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	Cisco IMC 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

始める前に

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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[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 Cisco IMC でイネーブルかどうか。
[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。

名前	説明
[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。
[Max Sessions] フィールド	Cisco IMC 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	現在 Cisco IMC で実行されている SSH セッションの数。

ステップ 4 [Save Changes] をクリックします。

Redfish の設定

始める前に

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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。

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

名前	説明
[Redfish Enabled] チェックボックス	Redfish が Cisco IMC でイネーブルかどうか。
[Max Sessions] フィールド	最大セッション数。
[Active Sessions] フィールド	アクティブなセッションの数。

ステップ 4 [Save Changes] をクリックします。

XML API の設定

Cisco IMC 用の XML API

Cisco Cisco IMC XML アプリケーション プログラミング インターフェイス（API）は、E シリーズ ラックマウント サーバ用の Cisco IMC に対するプログラマチック インターフェイスです。この API は、HTTP または HTTPS 経由で XML ドキュメントを受け取ります。

XML API のイネーブル化

始める前に

このタスクを実行するには、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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。

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

名前	説明
[XML API Enabled] チェックボックス	このサーバで API アクセスが許可されているかどうか。
[Max Sessions] フィールド	Cisco IMC で許可されている API 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	現在 Cisco IMC で実行されている API セッションの数。

ステップ 4 [Save Changes] をクリックします。

IPMI の設定

IPMI Over LAN

インテリジェント プラットフォーム管理インターフェイス（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 プロセッサはベースボード管理コントローラ（BMC）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、Cisco IMC を IPMI メッセージで管理する場合に設定します。

始める前に

このタスクを実行するには、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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。

ステップ 3 [IPMI over LAN Properties] 領域で、BMC 1、BMC 2、CMC 1、CMC 2 の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 IPMI アクセスが許可されているかどうか。

名前	説明
[Privilege Level Limit] ドロップダウン リスト	このサーバで IPMI セッションに割り当て可能な最高特権レベル。次のいずれかになります。 • [read-only]：IPMI 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。このオプションを選択した場合、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • [user]：IPMI ユーザはいくつかの機能を実行できますが、管理タスクは実行できません。このオプションを選択した場合、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ セッションと読み取り専用セッションだけです。 • [admin]：IPMI ユーザは使用可能なすべてのアクションを実行できます。このオプションを選択した場合、「Administrator」ユーザ ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
[Encryption Key] フィールド	IPMI 通信に使用する IPMI 暗号キー。
[Randomize] ボタン	IPMI 暗号化キーをランダムな値に変更できます。

ステップ 4 [Save Changes] をクリックします。

SNMP の設定

SNMP

Cisco UCS E シリーズ ラックマウント サーバは、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートの情報を送信したりするために、簡易ネットワーク管理プロトコル（SNMP）をサポートしています。

SNMP プロパティの設定

始める前に

このタスクを実行するには、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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

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

名前	説明
[SNMP Enabled] チェックボックス	このサーバが指定のホストに SNMP トラップを送信するかどうか。 （注） このチェックボックスをオンにしたら、SNMP ユーザまたはトラップを設定する前に、[Save Changes] をクリックする必要があります。
[SNMP Port] フィールド	Cisco IMC SNMP エージェントが動作するポート。 1 ～ 65535 の範囲内の SNMP ポート番号を入力します。デフォルト ポート番号は、161 です。 （注） システム コールに予約済みのポート番号（たとえば 22、23、80、123、443、623、389、636、3268、3269、2068 など）は、SNMP ポートとして使用できません。
[Access Community String] フィールド	Cisco IMC が任意の SNMP に含めるデフォルトの SNMP v1 または v2c コミュニティ名により、動作が実行されます。 最大 18 文字の文字列を入力します。
[SNMP Community Access] ドロップダウン リスト	次のいずれかになります。 • [Disabled]：このオプションは、インベントリ テーブルの情報へのアクセスをブロックします。 • [Limited]：このオプションは、インベントリ テーブルの情報の読み取りアクセスが部分的に提供します。 • [フル（Full）]：このオプションは、インベントリ テーブルの情報の読み取りフル アクセスを提供します。 （注） SNMP コミュニティ アクセスは、SNMP v1 および v2c ユーザのみに適用されます。

名前	説明
[Trap Community String] フィールド	他のデバイスに SNMP トラップを送信するために使用される SNMP コミュニティ グループの名前。 最大 18 文字の文字列を入力します。 （注） このフィールドは、SNMP v1 および v2c ユーザのみに表示されます。SNMP v3 ユーザは、SNMP v3 クレデンシャルを使用する必要があります。
[System Contact] フィールド	SNMP の実装を担当するシステムの連絡先。 電子メール アドレスまたは名前と電話番号など、最大 64 文字の文字列を入力します。
[System Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 64 文字の文字列を入力します。
[SNMP Input Engine ID] フィールド	ユーザ定義の一意の静的エンジン ID。
[SNMP Engine ID] フィールド	管理用デバイスを識別する一意の文字列。[SNMP Input Engine ID] が定義されている場合は、その値から文字列が生成されます。そうでない場合は、BMC シリアル番号から派生します。

ステップ 5 [Save Changes] をクリックします。

次のタスク

SNMP トラップを設定します。

SNMP トラップ設定の指定

始める前に

このタスクを実行するには、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] メニューをクリックします。
ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。
ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。
ステップ 4 [Trap Destinations] タブをクリックします。

ステップ 5 [トラップ宛先（Trap Destinations）] 領域で、次のいずれかを実行できます。

- テーブルから既存のユーザを選択し、[Modify Trap] をクリックします。
- 新しいユーザを作成するには、[Add Trap] をクリックします。

（注） フィールドが強調表示されていない場合は、[有効（Enabled）] を選択します。

ステップ 6 [Trap Details] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ID] フィールド	トラップの宛先 ID。この値は変更できません。
[Enabled]	オンにすると、このトラップがサーバでアクティブになります。
[バージョン（Version）] ドロップダウン リスト	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **[V2]** • **[V3]**
[Type]	送信するトラップのタイプ。次のいずれかになります。 • [Trap]：このオプションを選択すると、トラップが宛先に送信されますが、通知は受信しません。 • [Inform]：V2 ユーザに対してのみこのオプションを選択できます。これを選択すると、宛先でトラップが受信されたときに通知を受け取ります。
[User] ドロップダウン リスト	ドロップダウン リストに使用可能なすべてのユーザが表示されます。そのリストからユーザを選択します。
[Destination Address] フィールド	SNMP トラップ情報の送信先のアドレス。トラップの宛先として IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
Port	サーバがトラップの宛先との通信に使用するポート。 1 ～ 65535 の範囲内のトラップの宛先のポート番号を入力します。

ステップ 7 [Save Changes] をクリックします。

ステップ 8 トラップの宛先を削除する場合は、行を選択し、[Delete] をクリックします。

削除の確認プロンプトで、[OK] をクリックします。

テスト SNMP トラップ メッセージの送信

始める前に

このタスクを実行するには、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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] をクリックします。

ステップ 4 [Trap Destinations] 領域で、目的の SNMP トラップ宛先の行を選択します。

ステップ 5 [Send SNMP Test Trap] をクリックします。

SNMP テスト トラップ メッセージがトラップ宛先に送信されます。

（注） テストメッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

SNMP ユーザの管理

始める前に

- このタスクを実行するには、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。
- SNMP がイネーブルである必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

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

名前	説明
[Add User] ボタン	テーブル内で使用できる行をクリックし、このボタンをクリックして新規の SNMP ユーザを追加します。
[Modify User] ボタン	テーブル内で変更するユーザを選択し、このボタンをクリックして、選択した SNMP ユーザを変更します。

名前	説明
[Delete User] ボタン	テーブル内で削除するユーザを選択し、このボタンをクリックして、選択した SNMP ユーザを削除します。
[ID] カラム	SNMP ユーザに対してシステムが割り当てる識別子。
[Name] カラム	SNMP ユーザ名。
[Auth Type] カラム	ユーザ認証タイプ。
[Privacy Type] カラム	ユーザ プライバシー タイプ。

ステップ 5 [Save Changes] をクリックします。

SNMP ユーザの設定

始める前に

- このタスクを実行するには、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。
- SNMP がイネーブルである必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。
ステップ 2 [Admin] メニューで、[Communication Services] をクリックします。
ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。
ステップ 4 [User Settings] 領域で、次のいずれかの操作を実行します。

- テーブルから既存のユーザを選択し、[Modify User] をクリックします。
- [Users] 領域で行を選択し、[Add User] をクリックして新しいユーザを作成します。

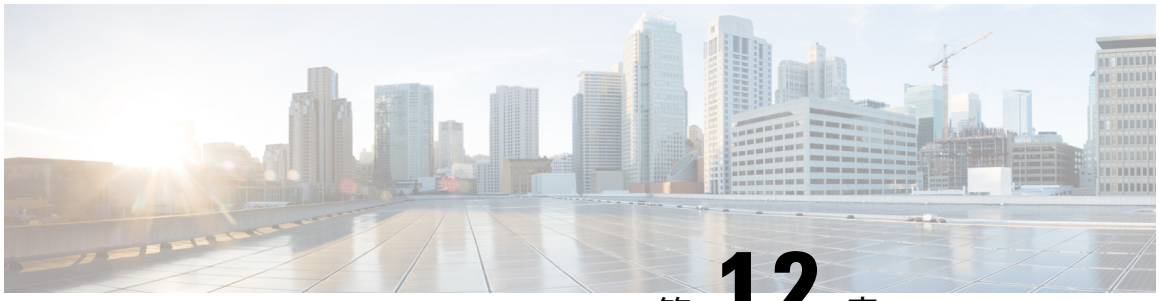
ステップ 5 [SNMP User Details] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[ID] フィールド	ユーザの固有識別情報。このフィールドは変更できません。
[Name] フィールド	SNMP ユーザ名。 1 ～ 31 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。

名前	説明
[Security Level] ドロップダウン リスト	このユーザのセキュリティ レベル。次のいずれかになります。 • [no auth, no priv]：このユーザには、許可パスワードもプライバシー パスワードも不要です。 • [auth, no priv]：このユーザには、許可パスワードが必要ですが、プライバシーパスワードは不要です。このオプションを選択すると、Cisco IMC は後述の Auth フィールドをイネーブルにします。 • [auth, priv]：このユーザには、許可パスワードとプライバシー パスワードの両方が必要です。このオプションを選択すると、Cisco IMC は Auth フィールドおよび Privacy フィールドをイネーブルにします。
[Auth Type] ドロップダウン	許可タイプ。次のいずれかになります。 • **[MD5]** • **[SHA]**
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。
[Privacy Type] ドロップダウン	プライバシー タイプ。次のいずれかになります。 • **[DES]** • **[AES]**
[Privacy Password] フィールド	この SNMP ユーザのプライバシー パスワード。 8～64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

ステップ 6 [Save Changes] をクリックします。

ステップ 7 ユーザを削除する場合は、ユーザを選択し、[Delete User] をクリックします。
削除の確認プロンプトで、[OK] をクリックします。



第 12 章

ファームウェアの管理

この章は、次の項で構成されています。

- Cisco IMC ファームウェア （153 ページ）
- ファームウェア コンポーネントの表示 （154 ページ）
- ファームウェアの更新 （155 ページ）
- ファームウェアのアクティブ化 （156 ページ）

Cisco IMC ファームウェア

Web UI の単一ページから次のファームウェア コンポーネントを管理できます。

- アダプタ ファームウェア：アクティブなイメージとバックアップ イメージで構成されている主要なオペレーティング ファームウェアで、次のような異なるインターフェイスからインストールできます。
  - ホスト アップグレード ユーティリティ（HUU）
  - Web UI：ローカルおよびリモートのプロトコル
  - XML API：リモート プロトコル

  ファームウェア イメージをローカル ファイル システムまたは TFTP サーバからアップロードできます。
- ブートローダ ファームウェア：ブートローダ ファームウェアは、Cisco IMC からインストールできません。このファームウェアは、Host Upgrade Utility を使用してインストールできます。

次の個々のコンポーネントのファームウェアを更新できます。

- BMC
- BIOS
- CMC

ハードディスク ドライブ（HDD）のファームウェアは、上述のアダプタ ファームウェアと同じインターフェイスからインストールすることもできます。

ファームウェア コンポーネントの表示

手順

ステップ 1 [Admin] メニューで、[Firmware Management] をクリックします。

ステップ 2 [General] タブの [Firmware Management] 領域で、次の情報を確認します。

名前	説明
[Update] ボタン	ダイアログボックスが開き、ローカル マシンまたはリモート サーバで利用可能なファームウェア イメージ ファイルをインストールできます。
[Activate] ボタン	ダイアログボックスが開き、サーバでアクティブにする使用可能なファームウェア バージョンを選択できます。 **重要** ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで新しいファームウェアをアクティブ化しないでください。
[component] 列	ファームウェアを更新できるコンポーネントのリスト。
[Running Version] カラム	現在有効なコンポーネントのファームウェア バージョン。

名前	説明
[Backup Version] カラム	サーバにインストールされている別のファームウェア バージョン（存在する場合）。バックアップバージョンは現在動作していません。これをアクティブにするには、[Activate] をクリックします。 （注） 新しいファームウェアをインストールすると、既存のバックアップバージョンはすべて削除され、新しいファームウェアがバックアップバージョンになります。サーバで新しいバージョンを実行するには、新しいファームウェアを手動でアクティブにする必要があります。
[Bootloader Version] カラム	コンポーネントのブートローダ ソフトウェアに関連付けられているブートローダ バージョン。
[Status] カラム	このサーバのファームウェアのアクティブ化のステータス。
[Progress in %] カラム	操作の進行状況のパーセンテージ。

ファームウェアの更新

[Firmware Management] 領域から選択したコンポーネントに応じて、ローカル ディスクまたはリモート サーバからファームウェア パッケージをインストールできます。インストールを確認した後、BMC によってコンポーネントのバックアップ メモリ スロット内のファームウェアバージョンが選択したバージョンに置き換えられます。

手順

ステップ 1 [Admin] メニューで、[Firmware Management] をクリックします。

ステップ 2 [Firmware Management] 領域で、[Component] カラムからコンポーネントを選択し、[Update] をクリックします。

[Update Firmware] ダイアログボックスが表示されます。

ステップ 3 ダイアログボックスで次の情報を確認します。

名前	説明
[Install Firmware through Browser Client] オプション ボタン	ファームウェア パッケージがローカル マシンに存在する場合は、このオプション ボタンをクリックします。
[リモートサーバによるファームウェアのインストール（Install Firmware through Remote Server）] オプション ボタン	ファームウェア パッケージがリモート サーバに存在する場合は、このオプション ボタンをクリックします。

ステップ 4 ブラウザのクライアントを介してファームウェアをインストールするには、[Browse] をクリックしてインストールするファームウェア ファイルに移動します。

ステップ 5 ファイルを選択してから、[Install Firmware] をクリックします。

ステップ 6 リモート サーバを使用してファームウェアを更新するには、[Install Firmware from] ドロップダウンリストからリモート サーバのタイプを選択します。次のいずれかを選択できます。

- **TFTP**
- **[FTP]**
- **SFTP**
- **SCP**
- **[HTTP]**

ステップ 7 選択したリモート サーバのタイプに応じて、サーバの [IP/Hostname] および [Image Path and Filename] フィールドに詳細を入力します。

ファームウェアをインストールすると、新しいイメージが非アクティブなイメージと置き換わります。インストール後にイメージをアクティブにすることができます。

重要 FTP、SFTP、SCP サーバ タイプの場合は、ユーザ クレデンシャルを提供する必要があります。

ステップ 8 [Install Firmware] をクリックして、ダウンロードとインストールを開始します。

ファームウェアのアクティブ化

手順

ステップ 1 [Admin] メニューで、[Firmware Management] をクリックします。

ステップ 2 [Firmware Management] 領域で、[Component] カラムからコンポーネントを選択し、[Activate] 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。

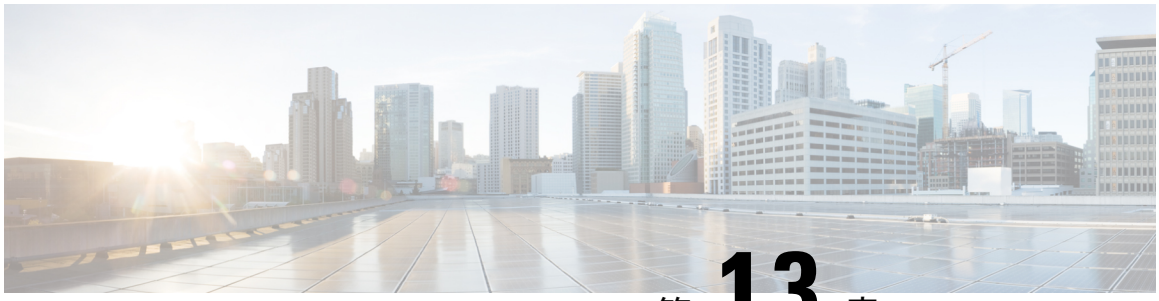
ステップ 3 [Activate Firmware] ダイアログボックスで、アクティブにするファームウェア イメージ（オプション ボタン）を選択します。このイメージは実行中のバージョンになります。

ステップ 4 [Activate Firmware] をクリックします。

選択したファームウェア イメージに応じて、アクティブ化のプロセスが開始されます。

重要 アクティブ化の進行中は、次のことを行わないでください。

- サーバのリセット、電源オフ、またはシャットダウン
- BMC のリブートまたはリセット
- 他のファームウェアのアクティブ化
- テクニカル サポートまたは設定データのエクスポート



第 13 章

障害およびログの表示

この章は、次の項で構成されています。

- 障害サマリー （159 ページ）
- 障害履歴 （161 ページ）
- Cisco IMC ログ （163 ページ）
- システム イベント ログ （166 ページ）
- ロギング制御 （168 ページ）

障害サマリー

障害サマリーの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Faults Summary] タブで、次の情報を確認します。

表 *9 : [Actions]* 領域

名前	説明
[Total]	[Fault Entries] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。

名前	説明
[Show] ドロップダウン リスト	フィルタを使用して障害のエントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づき障害のエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *10 : [Fault Entries]* 領域

名前	説明
[Time]	障害が発生した時刻。

名前	説明
[Severity]	次のいずれかになります。 • [Cleared]：ある障害または状態が解消されました。 • **[Critical]** • **[Info]** • **[Major]** • **[Minor]** • 警告
[Code]	障害に割り当てられた固有識別情報。
[DN]	識別名（DN）は、サーバ上でのデバイスのエンドポイントおよびそのインスタンスの階層表現です。
[Probable Cause]	障害の原因となったイベントに関連付けられた固有識別情報。
[Description]	障害についての詳細情報。 提案される解決策も含まれます。

障害履歴

障害履歴の表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Faults History] タブで、次の情報を確認します。

表 *11 : [Actions]* 領域

名前	説明
[Total]	[Fault History] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。
[Show] ドロップダウン リスト	フィルタを使用して障害履歴エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づきエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *12 : [Faults History]* 領域

名前	説明
[Time]	障害が発生した時刻。
[Severity]	次のいずれかになります。 • **[Emergency]** • **[Alert]** • **[Critical]** • **[Error]** • **警告** • **[Notice]** • **[Informational]** • **[Debug]**
[Source]	イベントをログに記録したソフトウェア モジュール。
[Probable Cause]	障害の原因となったイベントに関連付けられた固有識別情報。
[Description]	障害についての詳細情報。 提案される解決策も含まれます。

次のタスク

Cisco IMC ログ

Cisco IMC ログの表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。
ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Cisco IMC Log] タブで、次の情報を確認します。

表 *13 : [Actions]* 領域

名前	説明
[Clear Log] ボタン	すべてのログ ファイルを消去します。 （注） このオプションは、ユーザ ID に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。
[Total]	[Cisco IMC Log] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。

名前	説明
[Show] ドロップダウン リスト	フィルタを使用して Cisco IMC ログ エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づきログ エントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *14 : [Cisco IMC Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。

名前	説明
[Severity] カラム	イベントの重大度。次のいずれかになります。 • **[Emergency]** • **[Alert]** • **[Critical]** • **[Error]** • 警告 • **[Notice]** • **[Informational]** • **[Debug]**
[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。

システム イベント ログ

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 [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [System Event Log] タブで、次の情報を確認します。

表 *15 : [Actions]* 領域

名前	説明
[Clear Log] ボタン	ログ ファイルからすべてのイベントをクリアします。 （注） このオプションは、ユーザ ID に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。

名前	説明
[Total]	[System Event Log] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。
[Show] ドロップダウン リスト	フィルタを使用してイベントを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づきイベントを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [Filter] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[Go] をクリックします。 設定したフィルタ条件を保存するには、[Save] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリを表示します。 • [Manage Preset Filters]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [List of pre-defined filters]：システム定義のフィルタを表示します。 （注） [Filter] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *16 : [System Event Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。
[Severity] カラム	重大度フィールドには、テキストと色分けされたアイコンの両方が含まれます。アイコンについては、緑色は通常動作、黄色は情報を示し、警告、クリティカルおよび回復不能なエラーは赤色で表示されます。
[Description] カラム	イベントの説明。

ロギング制御

ロギング制御の表示

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Logging Controls] タブで、次の情報を確認します。

リモート ロギング

名前	説明
[Enabled] チェックボックス	オンにすると、Cisco IMC は [IP Address] フィールドで指定された Syslog サーバにログ メッセージを送信します。
[Host Name/IP Address] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[Port] フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

名前	説明
[Minimum Severity to Report] フィールド	リモート ログに含まれるメッセージの最低レベルを指定します。次のいずれかを選択できます。 • **[Emergency]** • **[Alert]** • **[Critical]** • **[Error]** • 警告 • **[Notice]** • **[Informational]** • **[Debug]**

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージはリモートでログに記録されません。たとえば、[Error] を選択した場合、Cisco IMC リモート ログには重大度が [Emergency]、[Alert]、[Critical]、[Error] のすべてのメッセージが含まれます。[Warning]、[Notice]、[Informational]、[Debug] のメッセージは表示されません。

Local Logging

この領域には、上記の表に示すように [Minimum Severity to Report] ドロップダウンリストのみが表示されます。ローカル ログに含めるメッセージの最低レベルを指定できます。

次のタスク

リモート サーバへの Cisco IMC ログの送信

Cisco IMC ログ エントリを受信するように 1 台または 2 台のリモート syslog サーバのプロファイルを設定できます。

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Remote Syslog Server] 領域のいずれかで、次のフィールドに値を入力します。

名前	説明
[Enabled] チェックボックス	オンにすると、Cisco IMC は [IP Address] フィールドで指定された Syslog サーバにログ メッセージを送信します。
[Host Name/IP Address] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[Port] フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

ステップ 4 （任意） [Minimum Severity to Report] ドロップダウン リストで、リモート ログに含まれるメッセージの最低レベルを指定します。

次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- **[Emergency]**
- **[Alert]**
- **[Critical]**
- **[Error]**
- 警告
- **[Notice]**
- **[Informational]**
- **[Debug]**

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージは、リモートでログに記録されません。たとえば、[**Error**] を選択した場合、Cisco IMC リモート ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

ステップ 5 [Save Changes] をクリックします。

Cisco IMC ログしきい値の設定

始める前に

手順

ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 必須: [**Local Logging**] 領域で、[**Minimum Severity to Report**] ドロップダウン リストを使用して、Cisco IMC ログに含まれるメッセージの最低レベルを指定します。

次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- **[Emergency]**
- **[Alert]**
- **[Critical]**
- **[Error]**
- 警告
- **[Notice]**
- **[Informational]**
- **[Debug]**

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージはログに記録されません。たとえば、[**Error**] を選択した場合、Cisco IMC ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

リモート サーバへのテスト Cisco IMC ログの送信

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

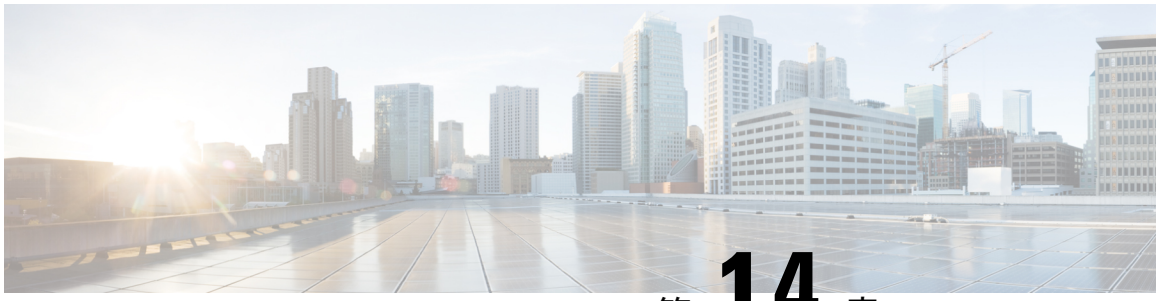
ステップ 1 [Navigation] ペインの [Chassis] メニューをクリックします。

ステップ 2 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Faults and Logs] ペインの [Logging Controls] タブをクリックします。

ステップ 4 [**Action**] 領域の [**Send Test Syslog**] をクリックします。

設定されているリモート サーバにテスト Cisco IMC ログが送信されます。



第 14 章

サーバ ユーティリティ

この章は、次の項で構成されています。

- テクニカル サポート データのエクスポート （173 ページ）
- 出荷時の初期状態へのリセット （175 ページ）
- Cisco IMC 設定のエクスポートとインポート （176 ページ）
- ホストへのマスク不能割り込みの生成 （181 ページ）
- Cisco IMC バナーの追加または更新 （182 ページ）
- Cisco IMC の最後のリセット理由の表示 （183 ページ）
- ローカル ファイルへのハードウェア インベントリのダウンロード （183 ページ）
- リモート サーバへのハードウェア インベントリ データのエクスポート （184 ページ）

テクニカル サポート データのエクスポート

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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[テクニカルサポート データのエクスポート（Export Technical Support Data）] をクリックします。

ステップ 4 [Export] をクリックします。

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

ローカル ファイルへのテクニカル サポート データのダウンロード

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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

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

ステップ 4 [Download Technical Support Data to Local File] 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
[Generate Technical Support Data] オプション ボタン	ダウンロードするテクニカル サポート データ ファイルがない場合、Cisco IMC によってこのオプション ボタンが無効化されます。 [Generate] をクリックして、データ ファイルを作成します。データ収集が完了したら、[Actions] 領域の [Download Technical Support Data to Local File] をクリックして、ファイルをダウンロードします。
[Download to local file] オプション ボタン	テクニカル サポート データ ファイルがダウンロード可能な場合、Cisco IMC によってこのオプション ボタンがイネーブルになります。 既存のファイルをダウンロードするには、このオプションを選択し、[Download] をクリックします。 （注） サーバにサポート対象ネットワーク アダプタ カードのいずれかがある場合、データ ファイルにはアダプタ カードからのテクニカル サポート データも含まれています。
[Generate] ボタン	テクニカル サポート データ ファイルを作成できます。
[Download] ボタン	テクニカル サポート データ ファイルを作成後にダウンロードできます。

ステップ 5 [Generate] をクリックして、データ ファイルを作成します。データ収集が完了したら、[Actions] 領域の [Download Technical Support Data to Local File] をクリックして、ファイルをダウンロードします。

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

出荷時の初期状態へのリセット

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やサーバのトラブルシューティング時など、稀なケースで、サーバ コンポーネント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。サーバ コンポーネント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。この移行中、一部のインベントリ情報が使用できない場合があります。

BMC を工場出荷時の設定にリセットすると、シリアル番号が Cisco IMCXXXXXX 形式で表示されます。XXXXXX はサーバのシリアル番号です。

始める前に

サーバ コンポーネント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] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

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

ステップ 4 [Reset to Factory Default] ダイアログボックスで、次の情報を確認します。

ステップ 5 [Reset] をクリックして、選択したコンポーネントを工場出荷時の設定にリセットします。

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 Cisco IMC 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、Cisco IMC の電源はオンになります。再起動時に、ネットワーク設定モードはデフォルトで [Cisco Card] モードに設定されます。

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 設定のバックアップを実行するには、システム設定のスナップショットを作成し、生成された Cisco IMC 設定ファイルをネットワーク上の場所にエクスポートします。エクスポート操作で保存されるのは、管理プレーンからの情報だけです。サーバ上のデータはバックアップされません。ユーザアカウントやサーバ証明書など、機密情報の設定はエクスポートされません。

エクスポートされた Cisco IMC 設定ファイルは、同じシステムで復元したり、別の Cisco IMC システムにインポートしたりできます。ただし、インポートするシステムのソフトウェアのバージョンとエクスポートするシステムのソフトウェアのバージョンが同じであるか、両者の設定に互換性があることが前提となります。設定ファイルを設定テンプレートとして他のシステムにインポートする場合は、IP アドレスやホスト名などシステム固有の設定を変更する必要があります。インポート操作によって情報が変更されるのは、管理プレーンだけです。

Cisco IMC 設定ファイルは XML テキスト ファイルで、その構造と要素は Cisco IMC コマンドモードに対応しています。

エクスポートまたはインポート操作を実行する場合は、次のガイドラインを考慮してください。

- エクスポートまたはインポートは、システムがアップ状態で、稼働しているときに実行できます。エクスポート操作によるサーバまたはネットワーク トラフィックへの影響はありませんが、インポート操作によって IP アドレスなどが変更されると、トラフィックが中断されたりサーバがリブートされたりすることがあります。
- エクスポートとインポートを同時に実行することはできません。

次の機能でインポートまたはエクスポート操作を実行できます。

- Cisco IMC バージョン

  （注） この情報のみをエクスポートできます。

- ネットワーク設定
- テクニカルサポート
- ローカル ログおよびリモート ログのロギング制御
- 電力ポリシー
- BIOS - BIOS パラメータ

（注） 高精度ブートはサポートされません。

- 通信サービス
- リモート プレゼンス
- ユーザ管理 - LDAP
- SNMP

Cisco IMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作でユーザアカウントやサーバ証明書をエクスポートしないでください。

始める前に

バックアップ リモート サーバの IP アドレスを取得します。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。
ステップ 2 [Admin] メニューで、[Utilities] をクリックします。
ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export Configuration] をクリックします。
ステップ 4 [Export Configuration] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export To] ドロップダウン リスト	XML 設定ファイルを保存する場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルを保存するには、このオプションを選択して [エクスポート（Export）] をクリックします。 このオプションを選択すると、Cisco IMC GUI に [ファイルのダウンロード（File Download）] ダイアログボックスが表示され、設定ファイルを保存する場所に移動できます。 • [Remote Server]：XML 設定ファイルをリモート サーバからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバのフィールドが表示されます。
[Export To] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルのエクスポート先となるサーバの IPv4 または IPv6 アドレス、またはホスト名。[Export to] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールド名は異なる場合があります。
[Path and Filename] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。

名前	説明
Username	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
Password	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Passphrase]	エクスポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードの暗号化に AES256 アルゴリズムを使用するパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください：! # $ & < > ? ; ' | ` ~ \ % ^ ( )"

ステップ 5 [Export] をクリックします。

Cisco IMC 設定のインポート

始める前に

コンフィギュレーション ファイルのインポート時に SNMP 設定情報を復元する場合は、インポートを行う前にこのサーバで SNMP がディセーブルになっていることを確認します。インポートを実行するときに SNMP がイネーブルになっている場合、Cisco IMC では設定ファイルに保存されている値によって現在の値は上書きされません。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 4 [Import Configuration] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Import From] ドロップダウン リスト	XML コンフィギュレーション ファイルの場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルをインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示され、インポートするファイルに移動できます。 • [Remote Server]：XML 設定ファイルをリモート サーバからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバのフィールドが表示されます。
[Import From] ドロップダウン リスト	（注） これらのオプションは、[Remote] を選択した場合にのみ使用できます。 リモート サーバのタイプ。次のいずれかになります。 • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルを保存するサーバの IPv4 または IPv6 アドレス、またはホスト名。[Import From] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールド名は異なる場合があります。
[Path and Filename] フィールド	リモート サーバ上の設定ファイルのパスおよびファイル名。

名前	説明
Username	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
Password	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[Passphrase]	インポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードの暗号化に AES256 アルゴリズムを使用するパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください：! # $ & < > ? ; ' | ` ~ \ % ^ ( )" （注） 設定ファイルの暗号化されたセクションを編集しそれをインポートしようとすると、編集内容は無視され、インポート操作画面には部分的な成功メッセージが表示されます。

ステップ 5 [Import] をクリックします。

ホストへのマスク不能割り込みの生成

状況によっては、サーバがハングして、従来のデバッグ メカニズムに応答しない場合があります。ホストへのマスク不能割り込み（NMI）を生成することにより、サーバのクラッシュ ダンプ ファイルを作成および送信して、サーバのデバッグに使用することができます。

サーバに関連付けられたオペレーティング システムの種類によっては、このタスクで OS が再起動される場合があります。

始める前に

- 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。
- サーバの電源が投入されている。

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。
ステップ 2 [Admin] メニューで、[Utilities] をクリックします。
ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate NMI to Host] をクリックします。
ステップ 4 [Generate NMI to Host] ダイアログボックスで、次の情報を確認します。

Actions	説明
[Generate NMI to] ドロップダウン リスト	マスク不能割り込み（NMI）を生成するサーバを選択できます。次のいずれかになります。 • **[Server 1]** • **[Server 2]**

ステップ 5 [Send] をクリックします。

このアクションは、OS を再起動する可能性のあるホストに NMI 信号を送信します。

Cisco IMC バナーの追加または更新

著作権表記やカスタマイズされたメッセージなどの重要な情報を入力して、Cisco IMC バナーを追加または更新できます。次の手順を実行します。

始める前に

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Add/Update Cisco IMC Banner] をクリックします。

ステップ 4 [Add/Update Cisco IMC Banner] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Banner (80 Chars per line. Max 2K Chars.)] フィールド	Web UI またはコマンドライン インターフェイスにログインする前に、ログイン画面に表示する著作権情報またはメッセージを入力します。
[Restart SSH] チェックボックス	オンにすると、[Save Banner] ボタンをクリックした後にアクティブな SSH セッションが終了します。

ステップ 5 [Save Banner] をクリックします。

次のタスク

Cisco IMC の最後のリセット理由の表示

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Last Reset Reason] 領域の下にある次の情報を確認します。

名前	説明
[コンポーネント（Component）] フィールド	最後にリセットされたコンポーネント。
[Status] フィールド	コンポーネントが最後にリセットされた理由。次のいずれかになります。 • [watchdog-reset]：Cisco IMC のメモリが容量一杯に到達した時点でウォッチドッグ タイマーがリセットします。 • [ac-cycle]：PSU 電源ケーブルが取り外されています（電源入力なし）。 • [graceful-reboot]：Cisco IMC のリブートが実行されます。

ローカルファイルへのハードウェアインベントリのダウンロード

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

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

ステップ 4 [Generate Inventory Data] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Generate Inventory Data] オプション ボタン	ダウンロードするハードウェア インベントリ データ ファイルがない場合、Cisco IMC によってこのオプション ボタンが表示されます。
[Download to local file] オプション ボタン	インベントリ データ ファイルがダウンロード可能な場合、Cisco IMC によってこのオプション ボタンがイネーブルになります。 既存のファイルをダウンロードするには、このオプションを選択し、[Download] をクリックします。

ステップ 5 [Generate] をクリックして、データ ファイルを作成します。データ収集が完了したら、[Download Inventory Data to Local File] オプション ボタンを選択して [Download] をクリックし、ファイルをローカルにダウンロードします。

リモート サーバへのハードウェア インベントリ データのエクスポート

手順

ステップ 1 [Navigation] ペインの [Admin] メニューをクリックします。

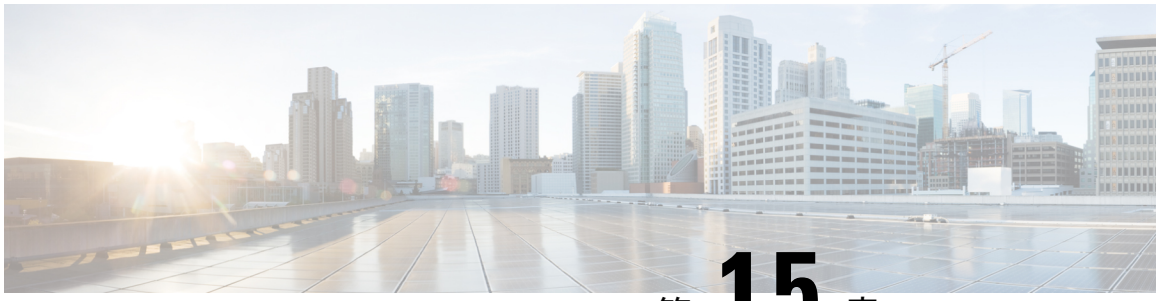
ステップ 2 [Admin] メニューで、[Utilities] をクリックします。

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

ステップ 4 [Export Hardware Inventory Data] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export Hardware Inventory Data to] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • **[TFTP Server]** • **[FTP Server]** • **[SFTP Server]** • **[SCP Server]** • **[HTTP Server]** （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	データ ファイルを保存する必要のあるサーバのIPアドレスまたはホスト名。[Export Hardware Inventory Data to] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。
[Path and Filename] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。
Username	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
Password	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

ステップ 5 [Export] をクリックします。



第 15 章

トラブルシューティング

この章は、次の項で構成されています。

- 最後の起動プロセスの記録 （187 ページ）
- 最後のクラッシュの記録 （188 ページ）
- DVR Player のダウンロード （189 ページ）

最後の起動プロセスの記録

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [TroubleShooting] タブをクリックします。

ステップ 3 [**Troubleshooting**] タブの [**Bootstrap Process Recording**] 領域で、[**Enable Recording**] チェックボックスをオンにします。

デフォルトで、このオプションは有効になっています。

注意 このタスクはトラブルシューティング目的のもので、常に有効にしていると Cisco IMC パフォーマンスに影響する場合があります。

ステップ 4 （任意） BIOS POST するまで起動プロセスを記録する場合は、[**Stop On BIOS POST**] 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。

ステップ 6 [Work] ペイン上部のツールバーで、[**Power On Server**] をクリックします。

ステップ 7 [**Bootstrap Process Recording**] ペインの [**Actions**] 領域で、[**Play Recording**] をクリックします。

サポートされている Java バージョンに関する手順を示した確認ダイアログ ボックスが表示されます。

ステップ 8 手順を確認し、[**OK**] をクリックします。

[DVR Player Controls] ダイアログボックスが開きます。このダイアログボックスは、最後の起動プロセスの記録を再生します。[**Stop On BIOS POST**] オプションをイネーブルにしている場合は、システムは BIOS POST まで記録プロセスを再生します。

この記録を確認して、システムがリブートした要因を分析できます。

ステップ 9 [**Bootstrap Process Recording**] 領域の [**Actions**] 領域で、[**Download Recording**] をクリックします。

ダウンロードするには、手順に従ってください。

（注） ファイルがローカルドライブに .dvc 形式で保存されます。KVM プレーヤーまたはオフライン プレーヤーを使用してこの記録を表示できます。[**Download Recording**] オプションを選択するたびに、最後の起動プロセスが記録され、ファイル名が自動生成され、事前に指定されたパスに保存されます。

ステップ 10 ダウンロードが完了すると、記録のビデオを再生するファイルを選択できるので、選択して [**Open**] をクリックします。
[DVR Player Controls] ウィンドウが開き、選択したファイルのビデオが再生されます。

最後のクラッシュの記録

手順

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [TroubleShooting] タブをクリックします。

ステップ 3 [Troubleshooting] タブの [Crash Recording] 領域で、[Enable Recording] チェックボックスをオンにします。

注意 このタスクはトラブルシューティング目的のもので、常に有効にしていると Cisco IMC パフォーマンスに影響する場合があります。

ステップ 4 [Save Changes] をクリックします。
[**Actions**] 領域の [**Capture Recording**] ボタンがイネーブルになります。

ステップ 5 （任意） [**Actions**] 領域で、[**Capture Recording**] をクリックし、自動的にクラッシュしたシステムの記録をキャプチャします。

（注） このオプションを選択すると、既存のクラッシュ レコード ファイルが上書きされます。[OK] をクリックして作業を続行します。

ステップ 6 サーバ上で実行された操作の記録を表示するには、[アクション（Actions）] 領域の [メッセージを再生する（Play Recording）] をクリックします。

サポートされている Java バージョンに関する手順を示した確認ダイアログ ボックスが表示されます。

ステップ 7 手順を確認し、[**OK**] をクリックします。

[DVR Player Controls] ダイアログボックスが表示されます。このダイアログボックスは、最後の数分にサーバ上で実行された操作の記録を再生します。この記録を確認して、システムがクラッシュした要因を分析できます。

ステップ 8 [**Crash Recording**] 領域の [**Actions**] 領域で、[**Download Recording**] をクリックします。

ダウンロードするには、手順に従ってください。

（注） ファイルがローカル ドライブに `.dvc` 形式で保存されます。KVM プレーヤーまたはオフライン プレーヤーを使用してこの記録を表示できます。[**Download Recording**] オプションを選択するたびに、最後のクラッシュ プロセスが記録され、ファイル名が自動生成され、事前に指定されたパスに保存されます。

ステップ 9 ダウンロードが完了すると、記録のビデオを再生するファイルを選択できるので、選択して [**Open**] をクリックします。
[DVR Player Controls] ウィンドウが開き、選択したファイルのビデオが再生されます。

DVR Player のダウンロード

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 [サーバ（Server）] タブの [トラブルシューティング（Troubleshooting）] をクリックします。

ステップ 3 [**Troubleshooting**] タブの [**Player**] 領域で、[**Download Player**] をクリックします。

ステップ 4 ダウンロードするには、手順に従ってください。これらのファイルは、ローカル ドライブに .tgz ファイル形式で zip 化されたファイルとして保存されます。

オフライン プレーヤーは、Windows、Linux、および MAC で保存されます。

ステップ 5 zip ファイルを解凍します。zip ファイルは通常、ブートストラップ ファイル下に保存され、名前は形式

`offline.tgz` に従います。

ステップ 6 ビデオ録画を確認したいスクリプト ファイルを開きます。

（注） Windows で録画を再生する場合は、システムで起動している Java バージョンとスクリプト ファイル内のバージョンが同じであることを確認します。Windows のスクリプト ファイルが録画を再生しない場合は、次の手順に従います。

a) Windows のスクリプト ファイルをデスクトップに抽出します。

b) メモ帳を使用してファイルを開きます。
c) jre を検索し、システムで起動しているバージョンと一致するよう Java バージョンを置き換えます。デフォルトでは、Java のバージョンは jre7 に設定されています。
d) ファイルを保存します。

Java のバージョンを更新したら、抽出したファイルをデスクトップから削除できます。

（注） Java のバージョンの検証は Windows OS にのみ必要です。Linux および MAC の場合は、Java のバージョンが自動的に選択されます。

ステップ 7 スクリプトファイルがダウンロードされるフォルダに移動し、ビデオ録画を再生するスクリプトファイルを開きます。

DVR プレーヤーが開始され、サーバ上で実行された操作のビデオが再生されます。