Cisco UCS S3260 サーバと Cisco UCS Manager リリース 3.1 との統合

初版：2016 年 09 月 17 日

最終更新：2017 年 04 月 27 日

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

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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)

© 2016-2017 Cisco Systems, Inc. All rights reserved.

目 次

はじめに ix

対象読者 ix

表記法 ix

Cisco UCS の関連資料 xi

マニュアルに関するフィードバック xi

新機能および変更された機能に関する情報 1

このリリースの新規情報および変更情報 1

概要 3

Cisco UCS S3260 システムについて 3

このマニュアルの使用方法 5

Cisco UCS S3260 システム アーキテクチャの概要 6

展開オプション 8

Cisco UCS Manager を使用した管理 10

Server SIOC Connectivity 機能 12

UCSM 管理型 Cisco UCS S3260 への移行 15

UCSM 管理型 Cisco UCS S3260 への移行 15

スタンドアロン Cisco UCS C3160 サーバから Cisco UCS S3260 サーバへの移行 16

スタンドアロン 3260 から UCSM 管理型 3260 への移行 16

スタンドアロン Cisco UCS S3260 から UCSM 管理型 Cisco UCS S3260 への移行の前提条件 16

シャーシ HDD からのブート 17

スタンドアロン Cisco UCS S3260 から UCSM 管理型 Cisco UCS S3260 への移行 17

スタンドアロン Cisco UCS S3260 から UCSM 管理型 Cisco UCS S3260 [2.0(13) 以降のバージョン] への移行 19

システム IP アドレス 20

Cisco UCS Manager を使用したサーバ ポートの設定 21

UCSM 管理型 Cisco UCS S3260 からスタンドアロン Cisco UCS S3260 への移行 22
機器関連ポリシー 23
シャーシ ディスカバリ ポリシー 23
シャーシ/FEX ディスカバリ ポリシーの設定 25
シャーシ接続ポリシー 25
シャーシ接続ポリシーの設定 27
シャーシ プロファイル 29
Cisco UCS Manager のシャーシ プロファイル 29
シャーシ プロファイルに関するガイドラインおよび推奨事項 30
ウィザードを使用したシャーシ プロファイルの作成 30
シャーシ プロファイルの名前の変更 32
シャーシ プロファイルの複製 33
シャーシ プロファイルの削除 33
シャーシ プロファイルの関連付け 34
シャーシ プロファイルとシャーシの関連付け 34
シャーシ プロファイルとシャーシの関連付け解除 35
シャーシ プロファイル テンプレート 35
シャーシ プロファイル テンプレート 35
シャーシ プロファイル テンプレートの作成 36
シャーシ プロファイル テンプレートから 1 つ以上のシャーシ プロファイルの作成 37
シャーシ プロファイルからのシャーシ プロファイル テンプレートの作成 38
シャーシ テンプレート プロファイルの複製 38
シャーシ プロファイル テンプレートのメンテナンス ポリシーの変更 39
シャーシ プロファイル テンプレートへのシャーシ プロファイルのバインディング 39
シャーシ プロファイル テンプレートからのシャーシ プロファイルのバインド解除 40
シャーシ メンテナンス ポリシー 41
シャーシ メンテナンス ポリシーの作成 41
シャーシ プロファイルのメンテナンス ポリシーの変更 42
シャーシ メンテナンス ポリシーの削除 43

コンピューティング接続ポリシー 43
コンピューティング接続ポリシーの作成 44
コンピューティング接続ポリシーとシャーシ プロファイルの関連付け 45
Cisco UCS S3260 システム ストレージ管理 47
ストレージ サーバ機能およびコンポーネントの概要 47
Cisco UCS S3260 ストレージ管理操作 56
高可用性のためのディスクの共有 57
ディスク ゾーン分割ポリシー 57
ディスク ゾーン分割ポリシーの作成 58
ディスク スロットの作成と所有権の割り当て 60
シャーシ プロファイルへのディスク ゾーン分割ポリシーの関連付け 61
ディスクの移行 61
ストレージ エンクロージャ操作 63
シャーシ レベルのストレージ エンクロージャの削除 63
ファームウェア管理 65
Cisco UCS S3260 システムのファームウェア管理 65
シャーシ プロファイルのシャーシ ファームウェア パッケージによるファームウェアのアップグレード 67
シャーシ ファームウェア パッケージ 67
シャーシ プロファイルのシャーシ ファームウェア パッケージを使用したファームウェアのアップグレードのステージ 69
シャーシ プロファイルのファームウェア パッケージに対するアップデートの影響 69
シャーシ ファームウェア パッケージの作成 70
シャーシ ファームウェア パッケージのアップデート 71
既存のシャーシ プロファイルへのシャーシ ファームウェア パッケージの追加 73
Cisco UCS S3260 サーバを使用した UCS ドメインのアップグレード 73
S3260 シャーシ とサーバ エンドポイントの直接のファームウェア アップグレード 74
シャーシ エンドポイントのファームウェアの直接のアップグレード 75
S3260 シャーシ の CMC ファームウェアのアップデート 75
S3260 シャーシ の シャーシ アダプタファームウェアのアップデート 76
S3260 シャーシ の SAS エクスパンダのファームウェアのアップデート 77

S3260 シャーシ の SAS エクスパンダ ファームウェアのアクティブ化 78
S3260 シャーシ の CMC ファームウェアのアクティブ化 79
S3260 シャーシ の シャーシ アダプタ ファームウェアのアクティブ化 79
S3260 シャーシ のシャーシ ボード コントローラ ファームウェアのアクティブ化 80
サーバ エンドポイントのファームウェアの直接のアップグレード 80
Cisco UCS S3260 サーバ ノードの CIMC ファームウェアの更新 80
Cisco UCS S3260 サーバ ノードの CIMC ファームウェアのアクティブ化 81
Cisco UCS S3260 サーバ ノードの BIOS ファームウェアの更新 82
Cisco UCS S3260 サーバ ノードの BIOS ファームウェアのアクティブ化 83
Cisco UCS S3260 サーバ ノードのボード コントローラ ファームウェアのアクティブ化 84
Cisco UCS S3260 サーバ ノードのストレージ コントローラ ファームウェアのアクティブ化 85
シャーシ管理 87
Cisco UCS S3260 シャーシ 87
シャーシの確認 88
シャーシの稼働中止 89
シャーシの削除 89
シャーシのロケータ LED の電源投入 90
シャーシのロケータ LED の電源切断 90
インベントリからのゾーン分割ポリシーの作成 90
シャーシの POST 結果の表示 91
サーバ管理 93
Cisco UCS S3260 サーバ ノード管理 94
Cisco UCS S3260 サーバ ノードのブート 94
サービス プロファイルからの Cisco UCS S3260 サーバ ノードのブート 95
Cisco UCS S3260 サーバ ノードのブート順序の決定 95
Cisco UCS S3260 サーバ ノードのシャットダウン 96
サービス プロファイルからの Cisco UCS S3260 サーバ ノードのシャットダウン 97
Cisco UCS S3260 サーバ ノードのリセット 97
Cisco UCS S3260 サーバ ノードの出荷時の初期状態へのリセット 98

Cisco UCS S3260 サーバ ノードの再確認 99
シャーシからの Cisco UCS S3260 サーバ ノードの削除 100
Cisco UCS S3260 サーバ ノードからのインバンド設定の削除 101
Cisco UCS S3260 ノードの使用停止 101
Cisco UCS S3260 サーバ ノードの再稼働 102
S3260 シャーシ 内のサーバ スロットの再認識 102
設定データベースからの存在しない Cisco UCS S3260 サーバ ノードの削除 103
Cisco UCS S3260 サーバ ノードのロケータ LED のオン/オフ切り替え 104
Cisco UCS S3260 サーバ ノードのローカル ディスク ロケータ LED のオン/オフ切り替え 104
Cisco UCS S3260 サーバ ノードの CIMC のリセット 105
Cisco UCS S3260 サーバ ノードの CMOS のリセット 105
Cisco UCS S3260 サーバ ノードからの NMI の発行 106
Cisco UCS S3260 サーバ ノードの POST 結果の表示 107
Cisco UCS S3260 サーバ ノードのヘルス イベントの表示 107
ヘルス LED アラーム 109
ヘルス LED アラームの表示 109
SIOC 管理 111
Cisco UCS Manager での SIOC 管理 111
SIOC の削除または交換 111
SIOC の認識 112
CMC のリセット 113
CMC セキュア ブート 113
CMC セキュア ブートの注意事項と制約事項 113
CMC セキュア ブートの有効化 114

はじめに

- 対象読者，ix ページ
- 表記法，ix ページ
- Cisco UCS の関連資料，xi ページ
- マニュアルに関するフィードバック，xi 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	表示
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メインタイトル] のように示しています。
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。

テキストのタイプ	表示
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。
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（*italic*）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、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	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 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Cisco UCS の関連資料

ドキュメント ロードマップ

すべての B シリーズ マニュアルの完全なリストについては、『*Cisco UCS B-Series Servers Documentation Roadmap*』（URL：http://www.cisco.com/go/unifiedcomputing/b-series-doc）を参照してください。

すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、『Release Bundle Contents for Cisco UCS Software』を参照してください。

その他のマニュアル リソース

ドキュメントの更新通知を受け取るには、Twitter の Cisco UCS Docs をフォローしてください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、ucs-docfeedback@external.cisco.com までコメントをお送りください。ご協力をよろしくお願いいたします。

第 1 章

新機能および変更された機能に関する情報

- このリリースの新規情報および変更情報，1 ページ

このリリースの新規情報および変更情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

表 *1*：*Cisco UCS Manager*、*3.1(3a)* の新機能と動作変更

機能	説明	参照先
Server SIOC Connectivity 機能	シャーシに単一サーバとデュアル SIOC が装着されている場合、この機能を使用して、プライマリ SIOC および補助 SIOC の両方を経由するデータ パスを設定できます。	Server SIOC Connectivity 機能，（12 ページ）
2 番目の RAID コントローラとデュアル HBA コントローラのサポート	Cisco UCS S3260 システム では 2 番目の RAID コントローラとデュアル HBA コントローラがサポートされています。	Cisco UCS S3260 システムについて，（3 ページ）

機能	説明	参照先
Cisco UCS C3260/C3X60 の再ブランディング。	リリース 3.1(3) から、Cisco UCS S3260 システムでは Server SIOC Connectivity 機能がサポートされています。シャーシに単一サーバとデュアル SIOC が装着されている場合、この機能を使用して、プライマリ SIOC および補助 SIOC の両方を経由するデータパスを設定できます。	Cisco UCS S3260 システムについて，（3 ページ）

第 2 章

概要

- Cisco UCS S3260 システムについて，3 ページ
- このマニュアルの使用方法，5 ページ
- Cisco UCS S3260 システム アーキテクチャの概要，6 ページ
- 展開オプション，8 ページ
- Cisco UCS Manager を使用した管理，10 ページ
- Server SIOC Connectivity 機能，12 ページ

Cisco UCS S3260 システムについて

Cisco UCS S3260 は、サーバ ノードを 2 台搭載した高密度のストレージ ラック サーバで、ビッグ データ、クラウド、オブジェクト ストレージ、コンテンツ配信などの環境で使用される大容量な データ セットに最適化されています。これは、Cisco UCS S シリーズ ラックマウント サーバ製品 ファミリに属しています。

Cisco UCS Manager リリース 3.1(3) から、Cisco UCS C3260/C3X60 は Cisco UCS S3260 に名称変更されました。システムの一部のコンポーネントが引き続き C3260/C3X60 として表示されることがあります。このリリースでは、用語 S3260 および C3260/C3X60 は同義で使用されます。S3260 と C3260/C3X60 のいずれも同じハードウェア コンポーネントを指します。

Cisco UCS S3260 システムは、スタンドアロン環境でも、Cisco UCS Manager 統合での Cisco Unified Computing System の一部としても動作するように設計されています。従来の製品の Cisco UCS C3160 とほぼ同じ特性を引き継いでいますが、次の機能が追加されています。

- デュアル ポート 40Gbps をサポートする Cisco VIC 1300 シリーズの組み込みチップを含むシステム I/O コントローラ（SIOC）
- 最大 2 つのサーバ モジュールのサポート
- スタンドアロン モードでも、Cisco UCS Manager と共にでも動作する機能

- 個々のハード ディスク ドライブ（HDD）は専用モードまたは共有モードのサーバに割り当てることができます

さらに、Cisco UCS S3260 システムのサーバ スロットの 1 つは、3.5 インチ ドライブを 4 台追加するためのストレージ拡張モジュールで使用できます。また、サーバ モジュールには、そのモジュール専用の内部ストレージとしてソリッド ステート ドライブ（SSD）を 2 台格納できます。シャーシは、個々のサーバ モジュールに 3.5 インチ ドライブを割り当てるように設定できるシリアル接続 SCSI（SAS）エクスパンダをサポートしています。

リリース 3.1(3) から、Cisco UCS S3260 システムでは次の機能がサポートされています。

- Server SIOC Connectivity 機能
- オプションの I/O エクスパンダ モジュール内の 2 番目の RAID コントローラ
- デュアル HBA コントローラ

（注） Cisco UCS S3260 システムにデュアル HBA コントローラが搭載されている場合、Cisco UCS Manager を 3.1(3) より前のリリースにダウングレードすることはできません。

Cisco UCS S3260 システムで、両方のサーバにデュアル RAID コントローラまたはデュアル HBA コントローラが組み込まれていてはなりません。コントローラ タイプの併用はサポートされていません。

Cisco UCS S3260 システムでは Server SIOC Connectivity 機能がサポートされています。シャーシに単一サーバとデュアル SIOC が装着されている場合、この機能を使用して、プライマリ SIOC および補助 SIOC の両方を経由するデータ パスを設定できます。詳細については、Server SIOC Connectivity 機能, （12 ページ）を参照してください。

Cisco UCS S3260 システムでは、サーバ ノードの上部に接続するオプションの I/O エクスパンダ モジュールの 2 番目の RAID コントローラがサポートされています。コントローラにゾーン分割されているディスクの数によっては、Cisco UCS Manager、BMC、CMC、および BIOS を 3.1(3) より前のリリースにダウングレードすることはできません。

コントローラの設定	ダウングレードが可能かどうか
サーバの 2 台のコントローラ（そのうちの 1 つはオプション I/O エクスパンダ内のコントローラ）またはサーバの 1 台のコントローラ（オプション I/O エクスパンダ内のコントローラ）と、1 台以上のディスクが、オプション I/O エクスパンダ内のコントローラにゾーン分割されています。	いいえ

コントローラの設定	ダウングレードが可能かどうか
サーバの 2 台のコントローラ（そのうちの 1 つはオプション I/O エクスパンダ内のコントローラ）またはサーバの 1 台のコントローラ（オプション I/O エクスパンダ内のコントローラ）および 1 台以上のディスクが、オプション I/O エクスパンダ内のコントローラに事前プロビジョニングされています。	いいえ
サーバの 2 台のコントローラ（そのうち 1 つはオプションI/Oエクスパンダ内のコントローラ）またはサーバの 1 台のコントローラ（任意のスロット）およびディスクが、オプション I/O エクスパンダ内のコントローラにゾーン分割も事前プロビジョニングもされていません。	Yes

ライセンス要件

S3260 システムが FI にアプライアンスとして接続されている場合（アプライアンス ポート）または Cisco UCS Manager 管理対象ノード（サーバ ポート）として接続されている場合は、ライセンス ETH_PORT_ACTIVATION_PKG（2G FI の場合）、40G_ETH_PORT_ACTIVATION_PKG（3G FI - 6332 の場合）、および 10G_PORT_ACTIVATION_PKG（3G FI ～ 6332-16UP の場合）を使用します。

ライセンス要件の詳細については、『*Cisco UCS Manager Server Management Guide*』の「*Server License Management*」の章を参照してください。

このマニュアルの使用方法

Cisco UCS Manager を使用して管理されている Cisco UCS S3260 システムは、Cisco UCS Manager を使用して管理されている他の S シリーズ ラック サーバによりサポートされている機能のほとんどをサポートしています。Cisco UCS S3260 システムでは、いくつかの新機能と管理機能も Cisco UCS Manager に導入されました。これらの特長と管理機能については、次の章で詳しく説明します。

- 概要：Cisco UCS Manager を使用して管理されるときの Cisco UCS S3260 システムとその接続のアーキテクチャに関する詳細情報を提供します。
- Cisco UCS Manager 管理型 Cisco UCS S3260 への移行：スタンドアロン Cisco UCS C3160 サーバまたはスタンドアロン Cisco UCS S3260 サーバから Cisco UCS Manager 管理型 Cisco UCS S3260 サーバへの移行に必要な手順について説明します。
- システム関連ポリシー：Cisco UCS S3260 システムに適用可能なシャーシ ディスカバリ ポリシーとシャーシ接続ポリシーについて説明します。

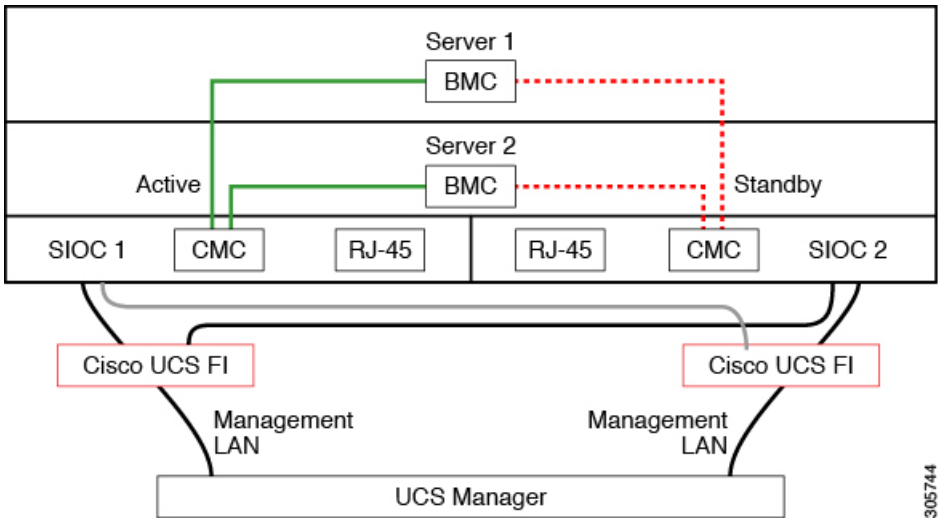
- シャーシ プロファイル：シャーシ プロファイルとシャーシ プロファイル テンプレートの詳細プロファイル情報情報を提供します。これを使用して Cisco UCS S3260 シャーシ のストレージ、ファームウェアとメンテナンスの特性を定義できるようになりました。
- ストレージ管理：Cisco UCS S3260 システムの新しいストレージ コンポーネントと、その管理方法について説明します。
- ファームウェア管理：ファームウェアを手動で更新できる Cisco UCS S3260 のシャーシ ファームウェア パッケージとエンドポイントについて詳しく説明します。
- シャーシ管理：Cisco UCS S3260 シャーシ の管理に関する詳細情報を提供します。
- サーバ管理：Cisco UCS S3260 サーバ ノードの管理に関する詳細情報を提供します。
- SIOC 管理：Cisco UCS S3260 シャーシ の一部であるシステム I/O コントローラ（SIOC）の管理に関する詳細情報を提供します。

Cisco UCS Manager リリース 3.1 以降のリリースでサポートされているすべての機能と設定タスクは、次の表に示す構成ガイドで説明されています。これらのガイドは、Cisco UCS S3260 システム用のこのクイック リファレンス ガイドとともに使用する必要があります。

Cisco UCS S3260 システム アーキテクチャの概要

アーキテクチャ概要

図 *1*：*Cisco UCS S3260* システム全体のアーキテクチャ図



このシステムは、シャーシ管理コントローラ（CMC）を使用してサーバ ノードを管理します。各システム I/O コントローラ（SIOC）モジュールには、内蔵型 CMC が組み込まれています。2 つの SIOC を使用する場合、2 つの CMC がアクティブ/スタンバイ構成で機能します。Cisco IMC イン

ターフェイスでログインしている SIOC 内の CMC がアクティブ CMC になります。アクティブ CMC を使用して、両方のサーバ ノードの BMC を管理できます。

すべてのユーザ インターフェイスは、アクティブ CMC でのみ動作します。構成の変更は、アクティブ CMC とスタンバイ CMC の間で自動的に同期されます。

システムの電源を再投入すると、デフォルトで SIOC 1 内の CMC がアクティブ CMC になります。次のいずれかの条件が発生すると、アクティブ CMC はスタンバイ CMC にフェールオーバーします。

- アクティブ CMC のリブートまたは障害が発生した場合。
- アクティブ CMC を持つ SIOC が取り外された場合。
- アクティブ CMC でネットワーク接続が失われた場合。

ビルディング ブロックと接続

Cisco UCS S3260 シャーシ は、次のモジュールで構成されるモジュラ アーキテクチャです。

ベース シャーシ

電源ユニット 4 つ、8 つのファンを搭載し、レール キットが付属しています。

サーバ ノード

1 台または 2 台のサーバ ノードごとに、2 つの CPU および、128 GB、256 GB、または 512 GB の DIMM メモリ、およびパススルー モードの RAID カードまたは 1 GB/4 GB のキャッシュを持つ RAID カードを選択、搭載可能です。

システム I/O コントローラ（SIOC）

1 つまたは 2 つのシステム I/O コントローラ（それぞれ 1300 シリーズ VIC を搭載）。Cisco UCS S3260 SIOC には Cisco UCS VIC 1300 シリーズの内蔵型チップが組み込まれているため、リムーバブル アダプタ カードはありません。

オプションのドライブ拡張ノード

4 つの 4TB ドライブ（合計容量：16TB）、4 つの 6TB ドライブ（合計容量：24TB）、または 4 個の 10TB ドライブ（合計容量：40TB）の選択。

ソリッドステート ブート ドライブ

1 つのサーバ ノードあたり最大 2 つの SSD

Cisco UCS ファブリック接続

Cisco UCS S3260 シャーシ は、次のいずれかの方法で接続できます。

- ファブリック インターコネクトへの直接接続。
- FEX による接続。

Cisco UCS ファブリック インターコネクトへの直接接続

1. Cisco UCS 6200 Series Fabric Interconnects：SIOC は 6248 FI ポートに直接接続できます。SIOC のアップリンクは、次の 2 つの方法のいずれかで FI ポートに接続できます。
   - QSA ケーブルを使用した、シングル FI ポートへの 10G 接続
   - ブレークアウト ケーブルを使用した、4 つの FI ポートへの 4*10G ポート チャネル接続
2. Cisco UCS 6300 Series Fabric Interconnects：SIOC のアップリンクは、シングル 40G 接続で 6300 シリーズ FI ポートに直接接続できます。

FEX による接続

N2348UPQ and 2232 FEX：SIOC は、QSA コネクタを使用して、シングル 10G 接続で FEX ポートに直接接続できます。

展開オプション

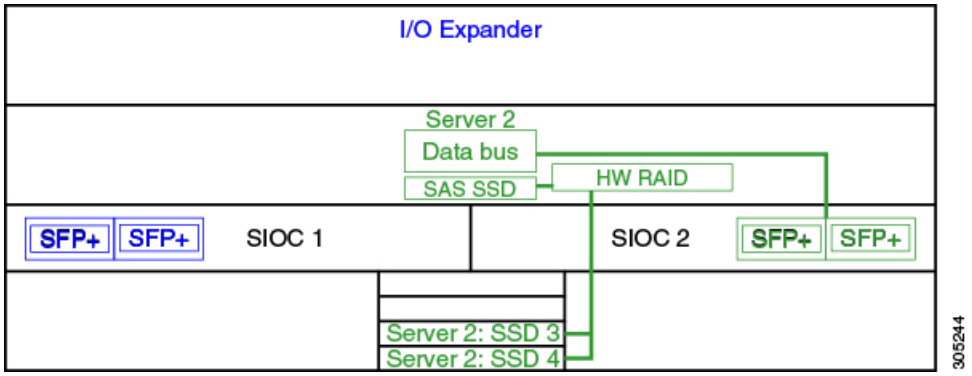
Cisco UCS S3260 システムの 3 つの主要な展開オプション（単一サーバ接続およびデュアル サーバ接続）について説明します。

単一サーバ接続

次の図は、単一サーバ システムの関連付けを示しています。

- サーバ ノード 2 のデータ バスは、SIOC 2 を介して接続します。
- サーバ 2 SSD 1 および 2 は、サーバ ノード 2 の RAID コントローラ カードによって制御できます。

図 *2*：*I/O* エクスパンダを備えた単一サーバ



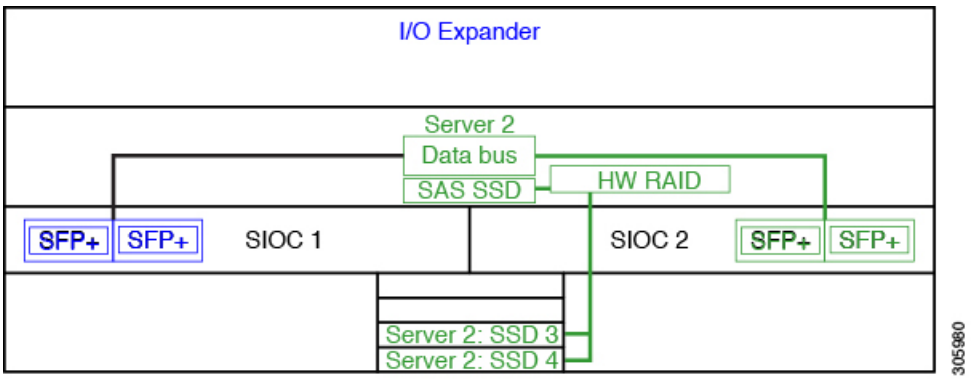
単一サーバ接続（Server SIOC Connectivity 機能を使用）

Cisco UCS S3260 システムに単一サーバとデュアル SIOC が含まれている場合、ユーザは Server SIOC Connectivity 機能を有効にできます。Server SIOC Connectivity 機能が有効な単一サーバ システムの関連性を次の図に示します。

- サーバ ノード 2 のデータ バスは、プライマリ SIOC および補助 SIOC 経由で接続しています。

（注） サーバ 1 のプライマリ SIOC は SIOC 1、サーバ 2 のプライマリ SIOC は SIOC 2 です。サーバ 1 の補助 SIOC は SIOC 2、サーバ 2 の補助 SIOC は SIOC 1 です。

図 *3* : ***Server SIOC Connectivity*** 機能を使用した単一サーバ単一 ***SIOC***



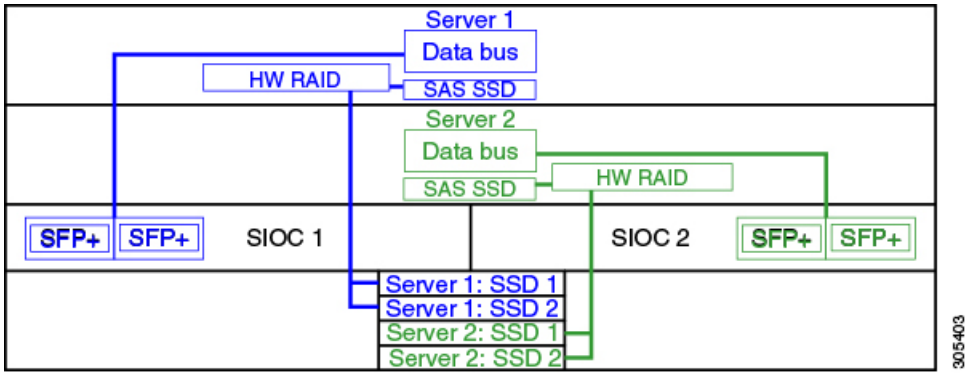
デュアル サーバ接続

このモードの導入では、各サーバ スロットに独立したサーバ ブレードが含まれています。SAS SSD などのさまざまなコンポーネントとともに冗長サーバ ノードは高可用性を提供します。

次の図は、デュアル サーバ システムを示しています。Cisco UCS C3X60 M3 サーバ ノードでは、サーバ 1 の PCH コントローラは SSD1 と SSD2 を制御し、サーバ 2 の PCH コントローラは SSD3

および SSD4 を制御します。Cisco UCS C3X60 M4 サーバ ノードでは、サーバ上の RAID コントローラ カードは、それぞれの SSD を制御します。

図 *4*：デュアル サーバ システム



重要 さまざまなサーバ ノードおよび関連するサービス ノートでサポートされているストレージ コントローラなどの Cisco UCS S3260 システムのストレージ コントローラに関する考慮事項の詳細については、『*Cisco UCS S3260 Storage Server Installation and Service Guide*』の「Storage Controllers」のセクションを参照してください。

Cisco UCS Manager を使用した管理

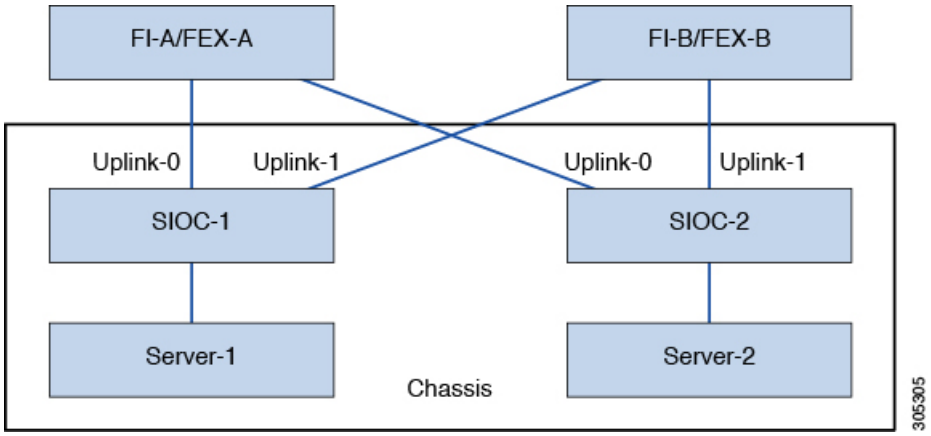
Cisco UCS S3260 システムはスタンドアロン モードで動作できますが、Cisco UCS Manager により管理することもできます。

（注） UCS Mini 6324 では Cisco UCS Manager と Cisco UCS S3260 の統合はサポートされていません。

デュアル サーバ接続

次の図は、Cisco UCS Manager が管理するデュアル サーバ ノード搭載の Cisco UCS S3260 システムの接続を示しています。

図 *5*：*Cisco UCS S3260* システムと *Cisco UCS Manager* との統合

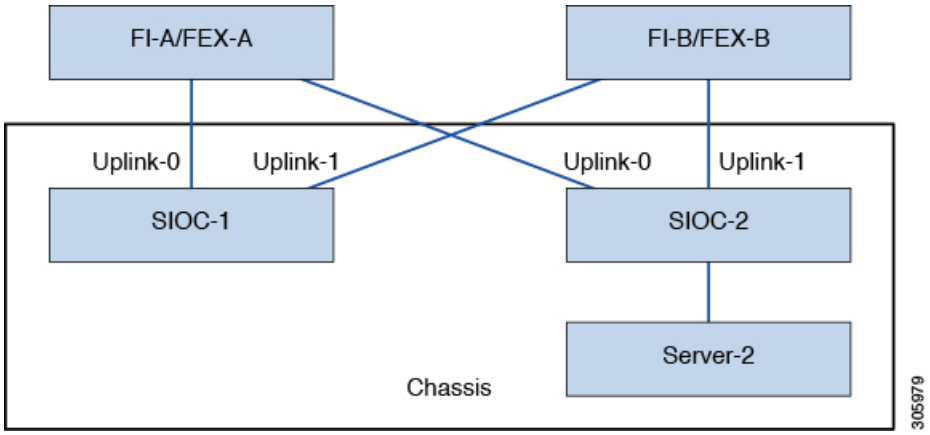


SIOC の 40G ポートは、ファブリック インターコネクトまたは FEX モジュールに接続できます。各 SIOC で、1 つのポートはプライマリ ファブリック インターコネクトおよび FEX に接続でき、もう 1 つのポートは下位のファブリック インターコネクトおよび FEX に接続できます。各 SIOC からのトラフィックは、ファブリック インターコネクトおよび FEX に到達できます。

単一サーバおよび単一 SIOC 接続

次の図は、Server SIOC Connectivity 機能を使用せずに Cisco UCS Manager により単一サーバおよび単一 SIOC が管理されている Cisco UCS S3260 システムの接続を示しています。

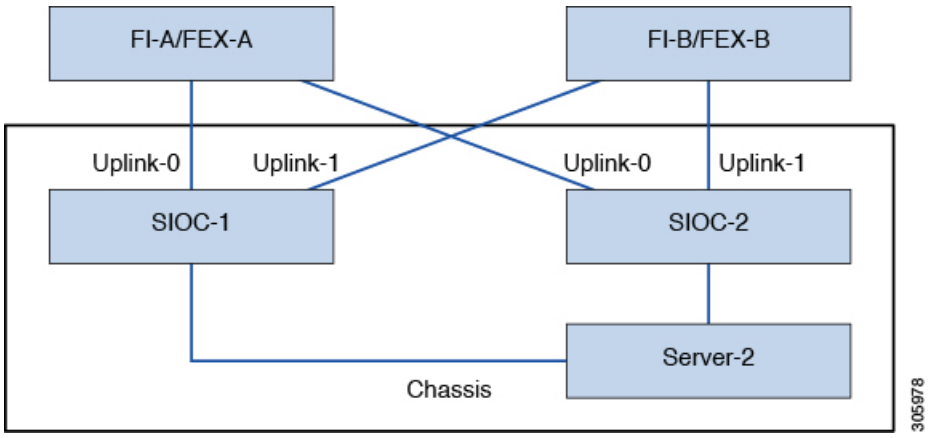
図 *6*：*Cisco UCS S3260* システムと *Cisco UCS Manager*（*Server SIOC Connectivity* 機能を使用しない単一サーバおよび単一 *SIOC*）



単一サーバおよびデュアル SIOC 接続（Server SIOC Connectivity 機能を使用）

次の図は、Server SIOC Connectivity 機能を使用して Cisco UCS Manager により単一サーバおよびデュアル SIOC が管理されている Cisco UCS S3260 システムの接続を示しています。

図 7：***Cisco UCS S3260*** システムと ***Cisco UCS Manager***（***Server SIOC Connectivity*** 機能を使用する単一サーバおよび単一 ***SIOC***）



Server SIOC Connectivity 機能

リリース 3.1(3) から、Cisco UCS S3260 システムでは Server SIOC Connectivity 機能がサポートされています。シャーシに単一サーバとデュアル SIOC が装着されている場合、この機能を使用して、プライマリ SIOC および補助 SIOC の両方を経由するデータ パスを設定できます。

（注）

サーバ 1 のプライマリ SIOC は SIOC 1、サーバ 2 のプライマリ SIOC は SIOC 2 です。サーバ 1 の補助 SIOC は SIOC 2、サーバ 2 の補助 SIOC は SIOC 1 です。

Server SIOC Connectivity 機能は、シャーシ プロファイルで [Compute Conn Policy] を使用して設定できます。このためには [single-server-dual-sioc] オプションを選択します。

Server SIOC Connectivity 機能の前提条件

この機能は次の条件を満たしている場合にのみ動作します。

- Cisco UCS S3260 システムでリリース 3.1(3) 以降が稼働している。
- 関連付けられている BIOS、BMC、および CMC ファームウェアで 3.1(3) 以降が動作している。
- シャーシに単一サーバとデュアル SIOC が装着されている。

ワークフロー：Cisco UCS Manager アップグレード

Cisco UCS Manager をリリース 3.1(3) 以降のリリースにアップグレードすると、シャーシディスカバリがトリガーされ、UCSM が サーバ SIOC 接続機能の動作状態を取得します。ユーザは シャーシ プロファイルの [Compute Conn Policy] で使用可能な [single-server-dual-sioc] オプションを使用してこの機能を有効にできます。

（注） コンピューティング接続ポリシーの設定を変更すると、保留イベントが発生します。この保留イベントを確認した後でのみ、シャーシ プロファイルの関連付けが自動的に開始します。

GUI で [Compute Conn Policy] プロパティを [single-server-dual-sioc] に設定すると、この操作によってサーバがリブートすることを警告するメッセージが Cisco UCS Manager により表示されます。メッセージの確認後に、シャーシの関連付けがトリガーされます。Server SIOC Connectivity 設定が正常に展開されると、サーバの詳細なディスカバリが Cisco UCS Manager により自動的にトリガーされます。

CLI で [Compute Conn Policy] プロパティを [single-server-dual-sioc] に設定したら、関連付けを開始するために **apply pending-changes immediate** コマンドを実行します。

[Compute Conn Policy] が [single-server-dual-sioc] に設定された場合は、Cisco UCS Manager を 3.1(3) より前のリリースにダウングレードすることはできません。Cisco UCS Manager では同様に、BMC、CMC、および BIOS を 3.1(3) より前のリリースにダウングレードすることはできません。

single-server-dual-sioc オプションが有効な場合にこの機能に影響する条件

- サーバの交換：サーバが交換されると、ブレードスロットの不一致が検出されます。スロットを確認するとサーバの詳細なディスカバリがトリガーされ、その後サービスプロファイルの関連付けが行われます。サービス プロファイルの関連付けがトリガーされると、次の 2 つの状況が発生する可能性があります。

  1. BIOS/BMC ファームウェアがホスト ファームウェアで指定されている場合：BIOS/BMC ファームウェアで単一サーバデュアル SIOC 接続がサポートされている場合は、サービス プロファイル関連付けプロセスが続行されます。BIOS/BMC ファームウェアで単一サーバデュアル SIOC 接続がサポートされていない場合は、この関連付けで設定の問題が発生します。
  2. ホスト ファームウェアで BIOS/BMC ファームウェアが指定されていない場合：Cisco UCS Manager は、実行中の BIOS/BMC バージョンで単一サーバ デュアル SIOC 接続がサポートされているかどうかを確認します。この機能がサポートされていない場合は、設定の問題は発生しません。

- SIOC の交換：交換した SIOC で 3.1(3) 以降が稼働している場合、1 つの SIOC が装着されるとユーザ確認メッセージが表示されます。SIOC アクションを確認すると、Cisco UCS Manager により FI と SIOC 間の接続が確立されます。さらに、Cisco UCS Manager はこの SIOC を経由するデータ パス接続があるサーバを再確認します。サーバに対して設定されている VNIC も再確認されます。詳細については、「SIOC の削除または交換, （111 ページ）」を参照してください。

交換した SIOC で古いバージョンのファームウェアが稼働している場合、Cisco UCS Manager では [Server SIOC Connectivity] 動作状態が [single-server-single-sioc] に自動的に変更されます。シャーシ プロファイルの関連付けを再度トリガーすることで、交換した SIOC のファームウェアを更新できます。

- SIOC の取り外し：SIOC を取り外すと、Cisco UCS Manager ではその SIOC と、サーバで作成された対応するアダプタ ユニットが欠落しているものとしてマークされます。
- シャーシへのサーバの追加：この機能が有効な状態で新しいサーバをシャーシに追加すると、サーバ ディスカバリが失敗します。
- シャーシ/サーバの関連付け解除：サーバまたはシャーシの関連付けが解除される場合、Server SIOC Connectivity 機能は無効になりません。

第 3 章

UCSM 管理型 Cisco UCS S3260 への移行

この章の内容は、次のとおりです。

- UCSM 管理型 Cisco UCS S3260 への移行，15 ページ
- スタンドアロン Cisco UCS C3160 サーバから Cisco UCS S3260 サーバへの移行，16 ページ
- スタンドアロン 3260 から UCSM 管理型 3260 への移行，16 ページ
- UCSM 管理型 Cisco UCS S3260 からスタンドアロン Cisco UCS S3260 への移行，22 ページ

UCSM 管理型 Cisco UCS S3260 への移行

（注） Cisco UCS C3160 の UCSM 管理型 Cisco UCS S3260 への直接移行はサポートされていません。まずスタンドアロン Cisco UCS C3160 をスタンドアロン Cisco UCS S3260 に移行してから、UCSM 管理型 Cisco UCS S3260 に移行します。

スタンドアロン Cisco UCS C3160 の UCSM 管理型 Cisco UCS S3260 への移行

スタンドアロン Cisco UCS C3160 を UCSM 管理型 Cisco UCS S3260 に移行するには、次を行います。

1. スタンドアロン Cisco UCS C3160 のスタンドアロン Cisco UCS Cisco UCS S3260 への移行
2. スタンドアロン Cisco UCS Cisco UCS S3260 の UCSM 管理型 Cisco UCS S3260 への移行
3. Cisco UCS Manager を使用したサーバ ポートの設定

スタンドアロン Cisco UCS Cisco UCS S3260 の UCSM 管理型 Cisco UCS S3260 への移行

スタンドアロン Cisco UCS Cisco UCS S3260 を UCSM 管理型 Cisco UCS S3260 に移行するには、次を行います。

1 スタンドアロン Cisco UCS Cisco UCS S3260 の UCSM 管理型 Cisco UCS S3260 への移行
2 Cisco UCS Manager を使用したサーバ ポートの設定

スタンドアロン Cisco UCS C3160 サーバから Cisco UCS S3260 サーバへの移行

Cisco UCS C3160 サーバを Cisco UCS S3260 サーバに移行するには、「Upgrading to Cisco UCS S3260 System With C3X60 M4 Server Nodes」を参照してください。

スタンドアロン 3260 から UCSM 管理型 3260 への移行

スタンドアロン Cisco UCS S3260 から UCSM 管理型 Cisco UCS S3260 への移行の前提条件

移行手順を開始する前に、次の条件を満足していることを確認します。

- システムが古いバージョンを実行している場合は、リリース 2.0(9) 以降の Cisco UCS S3260 Host Upgrade Utility（HUU）をダウンロードして実行してください。Host Upgrade Utility のダウンロード手順と使用方法については、リリース 2.0(9) 以降の Host Upgrade Utility ユーザ ガイドを使用します。使用しているリリースの HUU ガイドの手順を参照してください。
- DHCP サーバで設定されたか、スタティック IP アドレスとして手動で入力した、最大 5 個の IP アドレス。詳細については、「システム IP アドレス，（20 ページ）」を参照してください。
- UCSM 管理型 Cisco UCS S3260 へ移行する前に、既存のシステム設定のメモを作成することを推奨します。これらの設定には、次のようなものがあります。
  - サーバの UUID
  - ストレージ設定
  - ネットワーク コンフィギュレーション
  - ブート ポリシー
  - No. of vNICs
  - vNIC の配置
  - MAC アドレス
  - MTU

  移行後に Cisco UCS Manager を使用してこれらの構成を再度作成できます。

- シャーシ HDD からシステム ブート ボリュームが作成されたら、シャーシ HDD からのブート，（17 ページ）を実行します。

シャーシ HDD からのブート

はじめる前に

UCSM 管理型 Cisco UCS S3260 へ移行する前に、システム ブート ボリュームをシャーシ HDD から作成する場合にのみ、この手順を実行します。

手順

ステップ 1 [Disk Zoning Policy] が [Preserve Config] に設定されているシャーシ プロファイルとシャーシを関連付けます。
詳細については、「*Creating a Chassis Profile with the Wizard*」（GUI の手順）または「*Creating a Chassis Profile*」（CLI の手順）を参照してください。

ステップ 2 サーバのサービス プロファイル内では、[Prepare Claim Local LUN] オプションを使用して LUN とストレージ プロファイルを作成します。
LUN の名前を書き留めます。ストレージ プロファイルの詳細については、
[illegible]
を参照してください。

ステップ 3 サービス プロファイルを関連付けた後、サービス プロファイルのストレージ プロファイルに移動して、[Reclaim orphaned LUN] を選択し、再要求する LUN（シャーシ HDD 上の LUN）を選択します。

ステップ 4 ブート ポリシーでは、手順 2 で書き留めたものと同じ名前のローカル LUN を定義します。

次の作業

スタンドアロン Cisco UCS S3260 から UCSM 管理型 Cisco UCS S3260 への移行，（17 ページ）に進みます。

スタンドアロン Cisco UCS S3260 から UCSM 管理型 Cisco UCS S3260 への移行

重要 システムが 2.0(13) 以前のバージョンで実行している場合、スタンドアロン Cisco UCS S3260 を UCSM 管理型 Cisco UCS S3260 に移行するには、次の手順を実行します。

手順

ステップ 1 2.0(13) 用の Cisco UCS S3260 HUU を使用して、システム全体を Cisco IMC リリース 2.0(13) にアップグレードします。Cisco UCS S3260 システム内のすべてのサーバ ノードに対して HUU を実行します。

ステップ 2 シャット ダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。

ステップ 3 システムにキーボードとモニタを接続します。

1. システムの背面にあるサーバ ノードの外部 KVM コネクタに KVM ケーブル（Cisco PID N20-BKVM）を接続します。
2. VGA モニタと USB キーボードを KVM ケーブルのコネクタに接続します。

ステップ 4 電源コードを接続し、システムの電源をオンにします。F8 の押下を求めるプロンプトが表示されるのを待ちます。

ステップ 5 プロンプトが表示されたら、F8 を押して、Cisco IMC 設定ユーティリティを起動します。

ステップ 6 目的の IP アドレス、NIC モード、NIC 冗長化に応じてネットワーク プロパティを設定します。

1. 5 つの IP アドレスを設定するという、Cisco UCS S3260 システムの要件に注意します。詳細については、「システム IP アドレス，（20 ページ）」を参照してください。手順のこの時点では、システムは次の 3 つのアドレスを必要とします。
   - 1 つの管理 IP アドレス
   - 各 SIOC 用に 1 つの CMC アドレス
   - 各サーバ ノード用に 1 つの BMC アドレス

   （注） DHCP サーバを使用している場合、アドレスは DHCP サーバによって定義されます。DHCP をディセーブルにした場合は、ユーザ固有のスタティック管理 IP アドレスとネットワーク設定を指定する必要があります。
2. ネットワーク設定は、ブート時に F8 を押すと開かれる Cisco IMC 設定ユーティリティを使用して行います。http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/s/hw/S3260/install/S3260.html の「*Setting Up the System Using the Cisco IMC Configuration Utility*」を参照してください。
3. CMC および BMC コントローラのスタティック IP アドレスを設定する場合は、Cisco IMC 管理インターフェイスを使用することが求められています。http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/s/hw/S3260/install/S3260.html の「*Setting Static CMC and BMC Internal IP Addresses*」を参照してください。

ステップ 7 Cisco UCS Host Upgrade Utility を使用して、残りのシステム コンポーネントを Cisco IMC リリース 2.0(13) 以降にアップグレードします。
ユーティティのダウンロード手順と使用方法については、リリース 2.0(13) 以降の Host Upgrade Utility ユーザ ガイド（『HUU Guides』）を使用してください

アップグレードが完了したら、Cisco UCS S3260 システムの UCSM 統合への準備が完了します。

ステップ 8 F8 を押すことを求めるプロンプトが表示されたら、F8 を押して Cisco IMC 設定ユーティリティを起動します。

ステップ 9 サーバを工場出荷時のデフォルトに設定するか、またはユーティリティを使用する次の手順を実行してサーバ コントローラを工場出荷時のデフォルトに設定するには、『Resetting Cisco IMC to Factory Defaults』を参照してください。

1. F1 を押して、ユーティリティの 2 番目の画面に移動します。
2. [Factory Default] の下の [Chassis Controller Configuration] オプションを選択します。[Server Controller Configuration] は選択**しない**でください。
3. F10 キーを押して変更を保存し、BMC をリブートします。
4. リブートが完了するまで待ちます（約 5 分）。

ステップ 10 SIOC の 40G ポートを、ファブリック インターコネクトまたは FEX モジュールに接続できます。各 SIOC で、1 つのポートが FI-A/FEX-A に接続され、他のポートが FI-B/FEX-B に接続されます。各 SIOC からのトラフィックは、どちらの FI/FEX にも到達できます。「Cisco UCS S3260 システム アーキテクチャの概要, （6 ページ）」を参照してください。

次の作業

サーバ ポートを設定します。「Cisco UCS Manager を使用したサーバ ポートの設定, （21 ページ）」を参照してください。

スタンドアロン Cisco UCS S3260 から UCSM 管理型 Cisco UCS S3260 [2.0(13) 以降のバージョン] への移行

重要 システムがすでに 2.0(13) 以降のバージョンで実行している場合、スタンドアロン Cisco UCS S3260 を UCSM 管理型 Cisco UCS S3260 に移行するには、次の手順を実行します。

手順

ステップ 1 シャット ダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。

ステップ 2 システムにキーボードとモニタを接続します。

1. システムの背面にあるサーバ ノードの外部 KVM コネクタに KVM ケーブル（Cisco PID N20-BKVM）を接続します。
2. VGA モニタと USB キーボードを KVM ケーブルのコネクタに接続します。

ステップ 3 電源コードを接続し、システムの電源をオンにします。F8 の押下を求めるプロンプトが表示されるのを待ちます。

ステップ 4 プロンプトが表示されたら、F8 を押して、Cisco IMC 設定ユーティリティを起動します。

ステップ 5 サーバを工場出荷時のデフォルトに設定するか、またはユーティリティを使用する次の手順を実行してサーバ コントローラを工場出荷時のデフォルトに設定するには、『Resetting Cisco IMC to Factory Defaults』を参照してください。

1. F1 を押して、ユーティリティの 2 番目の画面に移動します。
2. [Factory Default] の下の [Chassis Controller Configuration] オプションを選択します。[Server Controller Configuration] は選択**しない**でください。
3. F10 キーを押して変更を保存し、BMC をリブートします。
4. リブートが完了するまで待ちます（約 5 分）。

ステップ 6 SIOC の 40G ポートを、ファブリック インターコネクトまたは FEX モジュールに接続できます。各 SIOC で、1 つのポートが FI-A/FEX-A に接続され、他のポートが FI-B/FEX-B に接続されます。各 SIOC からのトラフィックは、どちらの FI/FEX にも到達できます。「Cisco UCS S3260 システム アーキテクチャの概要, （6 ページ）」を参照してください。

次の作業

サーバ ポートを設定します。「Cisco UCS Manager を使用したサーバ ポートの設定, （21 ページ）」を参照してください。

システム IP アドレス

Cisco UCS S3260 システム システムは、最大 5 つの IP アドレスを設定できます。

（注） システム内に存在するすべてのコントローラは、相互に通信するために、割り当てられた IP アドレスが必要です。すべての IP アドレスは DHCP サーバで割り当てることができます。ユーザが固定 IP アドレスを割り当てることもできます。

- 管理 IP：これは、システム全体の仮想 IP アドレスです。このアドレスには、システムの Cisco IMC インターフェイスに、SIOC 1 または SIOC 2 のアクティブ シャーシ管理コントローラへの LAN 接続経由でアクセスするときにログインします。
- SIOC 1 CMC IP：これは SIOC 1 のシャーシ管理コントローラ（CMC）の内部アドレスです。このアドレスは DHCP サーバによって割り当てることができます。または、Cisco IMC インターフェイスを使用してスタティック アドレスを設定することもできます。
- SIOC 2 CMC IP：これは SIOC 2 の CMC の内部アドレスです（インストールされている場合）。このアドレスは DHCP サーバによって割り当てることができます。または、Cisco IMC インターフェイスを使用してスタティック アドレスを設定することもできます。

- サーバ 1 BMC IP：これはサーバ ノード 1 のボード管理コントローラ（BMC）の内部アドレスです。このアドレスは DHCP サーバによって割り当てることができます。または、Cisco IMC インターフェイスを使用してスタティック アドレスを設定することもできます。
- サーバ 2 BMC IP：これはサーバ ノード 2 の BMC の内部アドレスです（インストールされている場合）。このアドレスは DHCP サーバによって割り当てることができます。または、Cisco IMC インターフェイスを使用してスタティック アドレスを設定することもできます。

Cisco UCS Manager を使用したサーバ ポートの設定

サーバポートとしてイーサネットポートを設定するには、次の手順を実行します。ポートをサーバ ポートとして設定すると、移行プロセスは完了です。

（注） スタンドアロン Cisco UCS S3260 に接続されたイーサネット ポートがアプライアンス ポートとしてすでに設定されていれば、サーバ ポートとして再設定します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] > [Fixed Module] > [Ethernet Ports] の順に展開します。

ステップ 3 [Ethernet Ports] ノードの下のポートをクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

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

ステップ 6 ドロップダウン リストから [Configure as Server Port] を選択します。

次の作業

これで移行プロセスは完了です。Cisco UCS S3260 は S3260 シャーシ を自動的に検出します。シャーシ ディスカバリ ポリシー，（23 ページ） シャーシ ディスカバリに関する詳細情報を提供します。サーバ管理，（93 ページ） Cisco UCS Manager を使用してサーバを管理する方法の詳細を提供します。

Cisco UCS Manager を使用して、スタンドアロン Cisco UCS S3260 に存在する設定を再作成できます。「このマニュアルの使用方法，（5 ページ）」に示されている Cisco UCS Manager 設定ガイドには詳細な情報が記載されています。

UCSM 管理型 Cisco UCS S3260 からスタンドアロン Cisco UCS S3260 への移行

手順

ステップ 1 シャーシの稼働を中止します。「シャーシ管理」の章の「シャーシの稼働中止」の手順を参照してください。

ステップ 2 SIOC ケーブルを取り外します。

次の作業

これで移行プロセスは完了です。シャーシをスタンドアロン モードで使用できるようになりました。詳しい設定については、Cisco UCS S3260 システム の構成ガイドでサーバの管理について参照してください。Cisco UCS S3260 システム の構成ガイドは http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html にあります。

第 4 章

機器関連ポリシー

- シャーシ ディスカバリ ポリシー，23 ページ
- シャーシ接続ポリシー，25 ページ

シャーシ ディスカバリ ポリシー

シャーシ ディスカバリ ポリシーは、新しい Cisco UCS S3260 シャーシ または既存のスタンドアロン Cisco UCS S3260 シャーシ を Cisco UCS システムに追加した際のシステムによる対応方法を規定します。 Cisco UCS S3260 システム アーキテクチャの概要，（6 ページ） では、Cisco UCS Managerが管理するCisco UCS S3260 システムの接続を説明します。Cisco UCS Managerは、システム I/O コントローラ（SIOC）からファブリック ポート チャネルのファブリック インターコネクトへのリンクをグループ化するかどうかの決定にシャーシディスカバリ ポリシーの設定を使用します。

以前のスタンドアロン Cisco UCS S3260 シャーシ を Cisco UCS システムに追加するには、最初に工場出荷時のデフォルトに設定する必要があります。これにより、シャーシの両 SIOC を両方のファブリック インターコネクトに接続できます。シャーシの SIOC をファブリック インターコネクトに接続し、ポートをサーバポートとしてマークすると、シャーシディスカバリが開始されます。

サーバ ディスカバリ

Cisco UCS S3260 シャーシ が検出されると、Cisco UCS Manager は Cisco UCS S3260 サーバ ノードを自動的に検出します。

（注） サーバ ディスカバリはサーバに対応する SIOC が存在しない場合、失敗します。

リンクのグループ化

Cisco UCS S3260 シャーシ を FEX 経由で Cisco UCS 6200 シリーズ ファブリック インターコネクトに接続、または Cisco UCS 6300 シリーズ ファブリック インターコネクトに直接接続する場合、Cisco UCS Manager は [Port Channel] のプリファレンスを無視し、SIOC は、非ポート チャネル モードで動作します。

Cisco UCS S3260 シャーシ を Cisco UCS 6200 シリーズ ファブリック インターコネクトに直接接続すると、リンクのグループ化を使用して、シャーシの検出時に SIOC からファブリック インターコネクトへのすべてのリンクがファブリック ポート チャネルにグループ化されているかどうかを判断できます。リンクのグループ化を [Port Channel] に優先設定している場合、SIOC からファブリック インターコネクトへのリンクがすべてファブリック ポート チャネルにグループ化されます。[None] に設定すると、SIOC からのリンクはファブリック インターコネクトにピン接続されます。

Cisco UCS S3260 シャーシ が 4x10G ブレークアウト ケーブルを介して Cisco UCS 6200 シリーズ ファブリック インターコネクトに接続されている場合、リンクのグループ化プリファレンスを [Port Channel] に設定します。これを行わないと、シャーシ ディスカバリは完了しません。

Cisco UCS S3260 シャーシ がシングル 10G ケーブルを介してファブリック インターコネクトに接続されている場合、リンクのグループ化プリファレンスを [None] に設定します。

Cisco UCS Manager GUI の [Link Group Preference] 値を変更した後、変更を有効にするには、Cisco UCS S3260 シャーシ の稼働を中止してから再稼働させます。

Cisco UCS ドメイン では、他のシャーシが [Port Channel] モードで稼働している場合、次を実行します。

1. [Link Group Preference] が [Port Channel] に設定された Cisco UCS システムのシャーシを検出します
2. Cisco UCS S3260 シャーシ のリンク集約のプリファレンスをシャーシ接続ポリシーを通じて変更します
3. シャーシの稼働を中止します
4. シャーシを再稼働します

シャーシ/FEX ディスカバリ ポリシーの設定

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] ノードをクリックします。

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

ステップ 4 [Global Policies] サブタブをクリックします。

ステップ 5 [Chassis/FEX Discovery Policy] 領域で、アクションとリンクのグループ化のプリファレンスを指定します。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

次の作業

特性のシャーシのファブリック ポート チャネルの接続をカスタマイズするには、シャーシ接続ポリシーを設定します。

シャーシ接続ポリシー

シャーシ接続ポリシーは、特定のシャーシがシャーシディスカバリ後にファブリック ポート チャネルに含められるかどうかを決定します。このポリシーは、グローバル シャーシ ディスカバリ ポリシーで指定したのとは異なる方法で 1 つ以上のシャーシを設定する場合に役立ちます。

デフォルトでは、シャーシ接続ポリシーはグローバルに設定されます。これはつまり、接続制御はシャーシが新しく検出されたときに、シャーシディスカバリ ポリシーに設定された内容を使用して設定されることを意味しています。シャーシが検出されると、接続制御が「なし」と「ポート チャネル」のどちらに設定されるかを、シャーシ接続ポリシーが制御します。

（注） シャーシ接続ポリシーは、Cisco UCS Manager によって、ハードウェア設定がファブリック ポート チャネルをサポートする場合にだけ作成されます。

次の表に、FC/FCoE のさまざまな接続とメディア タイプのサポートを示します。

表 *2*：*FC/FCoE* の接続とメディア タイプのサポート

FI	接続	サポート	ポート チャネル	FC/FCoE
63xx	直接接続 40 GB	対応	非対応	対応

FI	接続	サポート	ポート チャネル	FC/FCoE
63xx	直接接続 10 GB – QSA	対応 ブレークアウトを使用しない	非対応	対応
63xx	直接接続 4x10 GB – ブレイクアウト	非対応	該当なし	該当なし
63xx	2348UPQ FEX - 10 GB – QSA	対応	非対応	対応
63xx	2348UPQ FEX - 4x10 GB - ブレークアウト	非対応	該当なし	該当なし
62xx	直接接続 – 4x10 GB - ブレークアウト ケーブル	対応	ポリシー駆動ですが、非ポートチャネルはサポートされる構成ではありません	非対応
62xx	直接接続 – 10 GB – QSA	対応	ポリシー駆動	対応。非ポートチャネル シャーシ ディスカバリ ポリシーの場合
62xx	2232 FEX - 10 GB - QSA	対応	非対応	対応
62xx	2232xx - 4x10 GB - ブレークアウト ケーブル	非対応	該当なし	該当なし
6324	直接接続 - 40 GB	非対応	該当なし	該当なし
6324	直接接続 - 10 GB – QSA	非対応	該当なし	該当なし

シャーシ接続ポリシーの設定

⚠

注意 シャーシの接続モードを変更すると、シャーシの稼働が停止し、再稼働することになります。その間トラフィックが中断されます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。

ステップ 3 SIOC とファブリック インターコネクト間の接続を設定するシャーシをクリックします。

ステップ 4 [Work] ペインで、[Connectivity Policy] タブをクリックします。

ステップ 5 シャーシの各 SIOC について、シャーシとファブリック接続用に [Admin State] フィールド で次のいずれかの値を選択します。

- [None]：リンクをポート チャネルにグループ化しません
- [Port Channel]：IOM からファブリック インターコネクトへのすべてのリンクがポート チャネルにグループ化されます。
- [Global]：シャーシはこの設定をシャーシ ディスカバリ ポリシーから継承します。これはデフォルト値です。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

第 5 章

シャーシ プロファイル

- Cisco UCS Manager のシャーシ プロファイル，29 ページ
- シャーシ プロファイルに関するガイドラインおよび推奨事項，30 ページ
- ウィザードを使用したシャーシ プロファイルの作成，30 ページ
- シャーシ プロファイルの名前の変更，32 ページ
- シャーシ プロファイルの複製，33 ページ
- シャーシ プロファイルの削除，33 ページ
- シャーシ プロファイルの関連付け，34 ページ
- シャーシ プロファイル テンプレート，35 ページ
- シャーシ メンテナンス ポリシー，41 ページ
- コンピューティング接続ポリシー，43 ページ

Cisco UCS Manager のシャーシ プロファイル

シャーシ プロファイルはシャーシのストレージ、ファームウェアとメンテナンスの特性を定義します。Cisco UCS S3260 シャーシ のシャーシ プロファイルを作成できます。シャーシ プロファイルがシャーシに関連付けられると、Cisco UCS Manager は自動的にシャーシ プロファイルで指定された設定に一致するようにシャーシを設定します。

重要 各 S3260 シャーシ は、いつの時点においても 1 つのシャーシ プロファイルだけに関連付けることができます。同様に、各シャーシ プロファイルは 1 度に 1 つの S3260 シャーシ だけに関連付けることができます。

シャーシ プロファイルには、次の情報が含まれます。

- Chassis definition：プロファイルを割り当てる特定のシャーシを定義します。

- Maintenance policy：プロファイルに適用されるメンテナンス ポリシーが含まれます。
- Firmware specifications：このプロファイルによるシャーシに適用できるシャーシ ファームウェア パッケージを定義します。
- Disk zoning policy：ストレージ ディスクに適用されるゾーン分割ポリシーが含まれます。
- Compute Connection policy：プライマリ SIOC、補助 SIOC、およびサーバ間のデータパスを定義します。

シャーシプロファイルに関するガイドラインおよび推奨事項

シャーシ プロファイルまたはシャーシ プロファイル テンプレートに含まれるポリシー（ディスク ゾーン分割ポリシーなど）に固有のガイドラインと推奨事項に加え、シャーシプロファイルとシャーシを関連付ける機能に影響する以下のガイドラインと推奨事項も順守してください。

- 各 S3260 シャーシ は 1 つのシャーシ プロファイルだけに関連付けることができます。同様に、各シャーシ プロファイルは 1 度に 1 つの S3260 シャーシ だけに関連付けることができます。
- シャーシプロファイルは、Cisco UCS S3260 シャーシ 上でのみサポートされます。Cisco UCS 5108 ブレード サーバ シャーシは、シャーシ プロファイルをサポートしておらず、シャーシ プロファイルに関連付けることはできません。
- Cisco UCS S3260 シャーシ では、S シリーズ サーバ ソフトウェアの Cisco UCS Manager リリース 3.1(2) より前のバンドルはサポートされません。

ウィザードを使用したシャーシ プロファイルの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 シャーシ プロファイルを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 組織を右クリックし、[Create Chassis Profile] を選択します。

ステップ 5 [Identify Chassis Profile] パネルで、シャーシ プロファイルの [Name] を指定して、[Next] をクリックします。

この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

このシャーシ プロファイルの説明（任意）を入力できます。

（注） シャーシ プロファイルを素早く作成するには、名前を指定した後で、[Finish] をクリックします。Cisco UCS Manager は、指定された名前とすべてのシステム デフォルト値を使用して新しいシャーシ プロファイルを作成します。

ステップ 6 （任意）[Maintenance Policy] パネルで、メンテナンス ポリシーを指定して [Next] をクリックします。
このパネルから新しいメンテナンス ポリシーを作成できます。シャーシ メンテナンス ポリシーの作成, （41 ページ） シャーシ メンテナンス ポリシーの作成に関する詳細な情報が表示されます。

ステップ 7 （任意）[Chassis Assignment] パネルで、次を指定して [Next] をクリックします。

a) ドロップダウン リストから [Chassis Assignment] を指定します。
[Chassis Assignment] に次のいずれかを指定できます。

- Assign Later：シャーシ プロファイルを作成して設定した後で、シャーシを割り当てることができます。
- Select existing Chassis：シャーシ プロファイルに割り当てられるシャーシを選択するのに使用できる、使用可能で関連付けられていないシャーシの表が表示されます。

  シャーシに関連付けられた後にシャーシプロファイルの移行を制限する場合は、[Restrict Migration] チェックボックスをオンにします。

  移行を制限しない場合、既存のシャーシプロファイルを移行する前に、Cisco UCS Manager による新規シャーシに対する互換性チェックは実行されません。シャーシ タイプが類似していない場合、関連付けが失敗することがあります。

b) [Chassis Firmware Package] をこのシャーシに関連付けるには、[Chassis Firmware Package] 領域を展開して、シャーシ ファームウェア パッケージを指定します。
このパネルからシャーシ ファームウェア パッケージを作成できます。シャーシ ファームウェア パッケージの作成, （70 ページ） シャーシ ファームウェア パッケージの作成に関する詳細な情報が表示されます。

c) コンピューティング接続ポリシーをこのシャーシ プロファイルに関連付けるには、[Compute Connection Policy] 領域を展開してコンピューティング接続ポリシーを指定します。コンピューティング接続ポリシーおよび Server SIOC Connectivity 機能の詳細については、Server SIOC Connectivity 機能, （12 ページ）を参照してください。
このパネルからコンピューティング接続ポリシーを作成できます。コンピューティング接続ポリシーの作成, （44 ページ） コンピューティング接続ポリシーの作成に関する詳細な情報が表示されます。

ステップ 8 （任意）[Disk Zoning Policy] パネルで、ディスク ゾーン分割ポリシーを指定して [Next] をクリックします。

このパネルからディスク ゾーン分割ポリシーを作成できます。 ディスク ゾーン分割ポリシーの作成, （58 ページ） ディスク ゾーン分割ポリシーの作成に関する詳細な情報が表示されます。

（注） ディスク ゾーン分割ポリシーを選択しないと、デフォルトのディスク ゾーン分割ポリシーが使用されます。デフォルトのディスク ゾーン分割ポリシーでは [Preserve Config] が選択されています。

ステップ 9 [Finish] をクリックします。

シャーシ プロファイルの名前の変更

シャーシ プロファイルの名前を変更すると、次のことが起こります。

- シャーシ プロファイルの以前の名前を参照するイベント ログと監査ログは、その名前のまま保持されます。
- 名前変更の操作を記録する、新しい監査データが作成されます。
- シャーシ プロファイルの以前の名前で生じたすべての障害データは、新しいシャーシ プロファイル名に転送されます。

（注） 保留中の変更があるシャーシ プロファイルの名前は変更できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 名前を変更するシャーシ プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 名前を変更するシャーシ プロファイルをクリックします。

ステップ 5 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 6 [Actions] 領域で、[Rename Chassis Profile] をクリックします。

ステップ 7 [Rename Chassis Profile] ダイアログボックスで、[New Name] フィールドにシャーシ プロファイルの新しい名前を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

ステップ 8 [OK] をクリックします。

シャーシ プロファイルの複製

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 複製するシャーシ プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 複製するシャーシ プロファイルを右クリックし、[Create a Clone] を選択します。

ステップ 5 [Create Clone From Service Profile] ダイアログボックスで次の作業を行います。

a) 新しいプロファイルに使用する名前を [Clone Name] フィールドに入力します。
この名前には、1～16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

この名前は、シャーシプロファイルを作成する組織またはサブ組織内で一意である必要があります。

b) （任意） シャーシ プロファイルを作成する組織またはサブ組織を選択します。

c) [OK] をクリックします。

ステップ 6 作成したシャーシ プロファイルに移動し、すべてのオプションが正しいことを確認します。

シャーシ プロファイルの削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 削除するシャーシ プロファイルを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

ステップ 5 [OK] をクリックします。

シャーシ プロファイルの関連付け

シャーシ プロファイルとシャーシの関連付け

作成時にシャーシプロファイルをシャーシに関連付けなかった場合、またはシャーシプロファイルを関連付けるシャーシを変更する場合には、次の手順を実行します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 新しいシャーシに関連付けるシャーシ プロファイルが含まれる組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 シャーシに関連付けるシャーシ プロファイルを右クリックし、[Change Chassis Profile Association] を選択します。

ステップ 5 [Associate Chassis Profile] ダイアログ ボックスで、ドロップダウン リストから [Select existing Chassis] オプションを選択します。
シャーシ プロファイルに割り当てられるシャーシを選択するのに使用できる、使用可能で関連付けられていないシャーシの表が表示されます。

ステップ 6 使用可能なシャーシの表の [Select] 列で、このシャーシ プロファイルに関連付けるシャーシのラジオ ボタンをクリックします。

ステップ 7 （任意） シャーシに関連付けられた後にシャーシプロファイルの移行を制限する場合は、[Restrict Migration] チェックボックスをオンにします。
移行を制限しない場合、既存のシャーシ プロファイルを移行する前に、Cisco UCS Manager による新規シャーシに対する互換性チェックは実行されません。両方のシャーシのハードウェアが類似していない場合、関連付けが失敗することがあります。

ステップ 8 [OK] をクリックします。

シャーシ プロファイルとシャーシの関連付け解除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 シャーシとの関連付けを解除するシャーシ プロファイルが含まれる組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 シャーシとの関連付けを解除するシャーシ プロファイルを右クリックし、[Disassociate Chassis Profile] を選択します。

ステップ 5 [Disassociate Chassis Profile] ダイアログ ボックスで、[Yes] をクリックして確認します。

ステップ 6 （任意） シャーシのステータスおよび FSM をモニタして、関連付けの解除が完了したことを確認します。

シャーシ プロファイル テンプレート

シャーシ プロファイル テンプレート

シャーシ プロファイル テンプレートを使用して、メンテナンス ポリシーやディスク ゾーン分割ポリシーなどの基本的なパラメータを共通させることで、複数のシャーシ プロファイルを迅速に作成できます。

ヒント 既存のシャーシ プロファイルに類似した値を持つ 1 つのシャーシ プロファイルだけが必要な場合は、Cisco UCS Manager GUI でシャーシ プロファイルを複製できます。

たとえば、類似した値を持つ数個のシャーシ プロファイルが必要である場合、手動、または既存のシャーシ プロファイルから、シャーシ プロファイル テンプレートを作成できます。その後、このテンプレートを使用して、シャーシ プロファイルを作成できます。

Cisco UCS は、次のタイプのシャーシ プロファイル テンプレートをサポートしています。

初期テンプレート

初期テンプレートから作成されたシャーシ プロファイルはテンプレートのプロパティをすべて継承します。初期シャーシ プロファイル テンプレートから作成されたシャーシ プロファイルはテンプレートにバインドされます。ただし、初期テンプレートに対して行われた変更は、バインドされたシャーシ プロファイルに自動的に伝播されません。バインドされたシャーシ プロファイルに変更を伝播したい場合は、そのシャーシ プロファイルをアンバインドしてから、再び初期テンプレートにバインドします。

アップデート テンプレート

テンプレートのアップデートから作成されたシャーシ プロファイルはテンプレートのプロパティをすべて継承し、そのテンプレートへの接続をそのまま保持します。テンプレートを変更すると、このテンプレートから作成されたシャーシプロファイルが自動的にアップデートされます。

シャーシ プロファイル テンプレートの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル テンプレート（Chassis Profile Templates）] の順に展開します。

ステップ 3 シャーシ プロファイル テンプレートを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 組織を右クリックし、[Create Chassis Profile Template] を選択します。

ステップ 5 [Identify Chassis Profile Template] パネルで、シャーシ プロファイルの [Name]、[Type] を指定し、[Next] をクリックします。
このシャーシ プロファイル テンプレートの説明（任意）を入力できます。

（注） シャーシ プロファイル テンプレートを素早く作成するには、名前を指定した後で、[Finish] をクリックします。Cisco UCS Manager は、指定された名前とすべてのシステム デフォルト値を使用して新しいシャーシ プロファイル テンプレートを作成します。

ステップ 6 （任意）[Chassis Maintenance Policy] パネルで、シャーシ メンテナンス ポリシーを指定して [Next] をクリックします。
このパネルから新しいシャーシ メンテナンス ポリシーを作成できます。

ステップ 7 （任意）[Policies] パネルで、次を指定して [Next] をクリックします。

a) シャーシ ファームウェア パッケージを関連付けるには、[Chassis Firmware Package] 領域を展開して、シャーシ ファームウェア パッケージを指定します。

このパネルからシャーシ ファームウェア パッケージを作成できます。 シャーシ ファームウェア パッケージの作成, （70 ページ） シャーシ ファームウェア パッケージの作成に関する詳細な情報が表示されます。

b) コンピューティング接続ポリシーを関連付けるには、[Compute Connection Policy] 領域を展開してコンピューティング接続ポリシーを指定します。コンピューティング接続ポリシーおよび Server SIOC Connectivity 機能の詳細については、Server SIOC Connectivity 機能, （12 ページ）を参照してください。
このパネルからコンピューティング接続ポリシーを作成できます。 コンピューティング接続ポリシーの作成, （44 ページ） コンピューティング接続ポリシーの作成に関する詳細な情報が表示されます。

ステップ 8 （任意）[Disk Zoning Policy] パネルで、ディスク ゾーン分割ポリシーを指定して [Next] をクリックします
このパネルからディスク ゾーン分割ポリシーを作成できます。

ステップ 9 [Finish] をクリックします。

シャーシ プロファイル テンプレートから 1 つ以上のシャーシ プロファイルの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル テンプレート（Chassis Profile Templates）] の順に展開します。

ステップ 3 シャーシ プロファイルのベースとして使用するシャーシ プロファイル テンプレートを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 プロファイルの作成元となるシャーシプロファイルテンプレートを右クリックし、[Create Chassis Profiles From Template] を選択します。

ステップ 5 [Create Chassis Profiles From Template] ダイアログボックスで、必要なフィールドに値を入力します。

ステップ 6 [OK] をクリックします。

シャーシ プロファイルからのシャーシ プロファイル テンプレートの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 テンプレートのベースとして使用するシャーシ プロファイルが含まれる組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 テンプレートの作成元となるシャーシ プロファイルを右クリックし、[Create a Chassis Profile Template] を選択します。

ステップ 5 [Create Template From Chassis Profile] ダイアログボックスで、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

シャーシ テンプレート プロファイルの複製

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル テンプレート（Chassis Profile Templates）] の順に展開します。

ステップ 3 複製するシャーシ テンプレート プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 複製するシャーシ テンプレート プロファイルを右クリックし、[Create a Clone] を選択します。

ステップ 5 [Create Clone From Chassis Template Profile] ダイアログボックスで次の作業を行います。

a) 新しいプロファイルに使用する名前を [Clone Name] フィールドに入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

この名前は、シャーシ テンプレート プロファイルを作成する組織またはサブ組織内で一意である必要があります。

b) （任意） シャーシ テンプレート プロファイルを作成する組織またはサブ組織を選択します。
c) [OK] をクリックします。

ステップ 6 作成したシャーシテンプレートプロファイルに移動し、すべてのオプションが正しいことを確認します。

シャーシ プロファイル テンプレートのメンテナンス ポリシーの変更

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル テンプレート（Chassis Profile Templates）] の順に展開します。

ステップ 3 変更するシャーシ メンテナンス ポリシーを含むシャーシ プロファイル テンプレートが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 変更するシャーシ プロファイル テンプレートをクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Change Chassis Maintenance Policy] をクリックします

ステップ 7 [Change Chassis Maintenance Policy] ダイアログボックスで、[Chassis Maintenance Policy] ドロップダウン リストからシャーシのメンテナンス ポリシーを指定して、[OK] をクリックします。
このパネルから新しいメンテナンス ポリシーを作成できます。

シャーシ プロファイル テンプレートへのシャーシ プロファイルのバインディング

シャーシ プロファイルをシャーシ プロファイル テンプレートにバインドすることができます。シャーシ プロファイルをテンプレートにバインドした場合、Cisco UCS Manager により、シャーシプロファイルテンプレートに定義された値を使って、シャーシプロファイルが設定されます。既存のシャーシプロファイル設定がテンプレートに一致しない場合、Cisco UCS Manager により、シャーシプロファイルが再設定されます。バインドされたシャーシプロファイルの設定は、関連付けられたテンプレートを使用してのみ変更できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 バインドするシャーシ プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 バインドするシャーシ プロファイルをクリックします。

ステップ 5 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 6 [Actions] 領域で、[Bind to a Template] をクリックします。

ステップ 7 [ind to a Chassis Profile Template] ダイアログボックスで、次の手順を実行します。

a) [Chassis Profile Template] ドロップダウン リストから、シャーシ プロファイルにバインドするテンプレートを選択します。

b) [OK] をクリックします。

シャーシ プロファイル テンプレートからのシャーシ プロファイルのバインド解除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 バインド解除するシャーシ プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 バインド解除するシャーシ プロファイルをクリックします。

ステップ 5 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 6 [Actions] 領域で [Unbind from the Template] をクリックします。

ステップ 7 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

シャーシ メンテナンス ポリシー

シャーシ メンテナンス ポリシーの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [ポリシー（Policies）] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 [Chassis Maintenance Policies] を右クリックし、[Create Maintenance Policy] を選択します。

ステップ 5 [Create Chassis Maintenance Policy] 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
[Name] フィールド	ポリシーの名前。 この名前には、1～16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーを使用する場所とタイミングに関する情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

名前	説明
[Reboot Policy] フィールド	シャーシプロファイルがシャーシに関連付けられたとき、またはシャーシにすでに関連付けられているシャーシプロファイルに変更を加えたときは、プロセスを完了するためにシャーシをリブートする必要があります。[Reboot Policy] フィールドは、このシャーシ メンテナンス ポリシーを含むシャーシプロファイルのいずれかに関連付けられたシャーシで電源の再投入がいつ発生するかを決定します。シャーシプロファイルとシャーシ プロファイル テンプレートがサポートするのは1つのリブート ポリシーだけです。 [User Ack]：シャーシ プロファイルの関連付けが完了したり、変更が行われたりした後で、ユーザはシャーシの電源を手動で再投入する必要があります。

ステップ 6 [OK] をクリックします。

次の作業

ポリシーをシャーシ プロファイルまたはシャーシ プロファイル テンプレートに含めます。

シャーシ プロファイルのメンテナンス ポリシーの変更

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 変更するメンテナンス ポリシーを含むシャーシプロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 変更するシャーシ プロファイルを右クリックし、[Change Chassis Maintenance Policy] を選択します。

ステップ 5 [Change Chassis Maintenance Policy] ダイアログボックスで、[Chassis Maintenance Policy] ドロップダウン リストからシャーシのメンテナンス ポリシーを指定して、[OK] をクリックします。

このパネルから新しいシャーシ メンテナンス ポリシーを作成できます。

（注） シャーシ プロファイルは、混乱が生じる変更が適用されると即座にリブートします。

シャーシ メンテナンス ポリシーの削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。
ステップ 2 [シャーシ（Chassis）] > [ポリシー（Policies）] > *[Organization_Name]* の順に展開します。
ステップ 3 [Chassis Maintenance Policies] を展開します。
ステップ 4 削除するシャーシ メンテナンス ポリシーを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

コンピューティング接続ポリシー

コンピューティング接続ポリシーは、サーバ SIOC 接続のユーザ設定を保存するために使用されます。これらの設定は、[Server SIOC Connectivity] プロパティを使用して行われます。このプロパティは次のいずれかに設定できます。

- [single-server-single-sioc]（デフォルト）：シャーシに単一サーバと単一 SIOC またはデュアル サーバとデュアル SIOC が装着されている場合に、1 つの SIOC を経由するデータ パスを設定します。
- [single-server-dual-sioc]：有効な場合は、シャーシに単一サーバとデュアル SIOC が装着されていると、プライマリ SIOC および補助 SIOC の両方を経由するデータ パスを設定できます。詳細については、Server SIOC Connectivity 機能, （12 ページ）を参照してください。

コンピューティング接続ポリシーの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [ポリシー（Policies）] > *[Organization_Name]* の順に展開します。

ステップ 3 [Compute Connection Policies] を右クリックして、[Create Compute Connection Policy] を選択します。

ステップ 4 [Create Compute Connection Policy] ペインで次の情報を入力します。

- [Name]：ポリシーの名前を入力します。
- [Description]：ポリシーの簡単な説明。
- [Server SIOC Connectivity]：次のいずれかを選択します。
  - [single-server-single-sioc]（デフォルト）：シャーシに単一サーバと単一 SIOCまたはデュアル サーバとデュアル SIOC が装着されている場合に、1 つの SIOC を経由するデータ パスを設定します。
  - [single-server-dual-sioc]：有効な場合は、シャーシに単一サーバとデュアル SIOC が装着されていると、プライマリ SIOC および補助 SIOC の両方を経由するデータ パスを設定できます。詳細については、Server SIOC Connectivity 機能, （12 ページ）を参照してください。

ステップ 5 [OK] をクリックします。

（注） GUI で [Compute Conn Policy] プロパティを [single-server-dual-sioc] に設定すると、この操作によってサーバがリブートすることを警告するメッセージが Cisco UCS Manager により表示されます。メッセージの確認後に、シャーシの関連付けがトリガーされます。Server SIOC Connectivity 設定が正常に展開されると、サーバの詳細なディスカバリが Cisco UCS Manager により自動的にトリガーされます。

コンピューティング接続ポリシーとシャーシプロファイルの関連付け

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] > *[Chassis_Profile_Name]* の順に展開します。

ステップ 3 [Policies] タブを選択します。

ステップ 4 [Compute Connection Policies] 領域を展開します。

ステップ 5 [Compute Connection Policies] ドロップダウンリストからポリシーを選択します。

ステップ 6 [Save Changes] をクリックします。

第 6 章

Cisco UCS S3260 システム ストレージ管理

- ストレージ サーバ機能およびコンポーネントの概要，47 ページ
- Cisco UCS S3260 ストレージ管理操作，56 ページ
- 高可用性のためのディスクの共有，57 ページ
- ストレージ エンクロージャ操作，63 ページ

ストレージ サーバ機能およびコンポーネントの概要

ストレージ サーバ機能

次の表に、Cisco UCS S3260 システムの機能の概要を示します。

表 *3*：*Cisco UCS S3260* システムの機能

機能	説明
シャーシ	4 ラック ユニット（4RU）シャーシ
プロセッサ	• Cisco UCS S3260 M3 サーバ ノード：各サーバ ノード内の 2 つの Intel Xeon E5-2600 v2 シリーズ プロセッサ。 • Cisco UCS S3260 M4 サーバ ノード：各サーバ ノード内の 2 つの Intel Xeon E5-2600 v4 シリーズ プロセッサ。
メモリ	各サーバ ノード内で最大 16 個の DIMM。
マルチビット エラー保護	このシステムは、マルチビット エラー保護をサポートします。

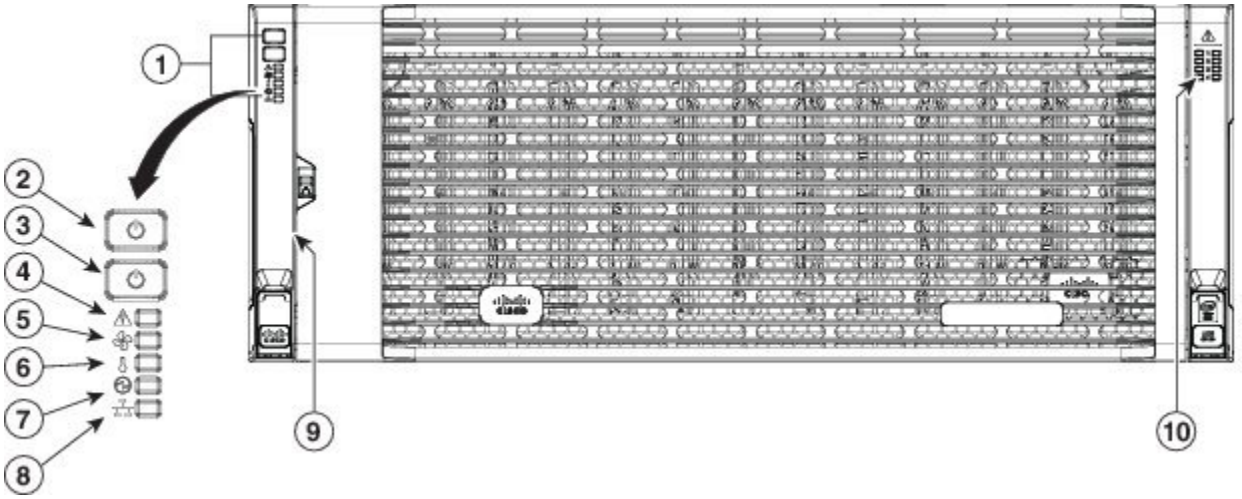
機能	説明
ストレージ	システムには次のストレージオプションがあります。 • 最大 56 台のトップ ローディング 3.5 インチ ドライブ • オプションのドライブ エクスパンダ モジュール内に最大 4 台の 3.5 インチ、リア ローディング ドライブ • 最大 4 台の 2.5 インチ、リア ローディング SAS ソリッド ステート ドライブ（SSD） • サーバ ノード内部の 1 台の 2.5 インチ NVMe ドライブ （注） これが適用されるのは、CX360 M4 サーバのみです。
ディスク管理	このシステムは、最大 2 台のストレージ コントローラをサポートしています。 • 各サーバ ノード内に Cisco ストレージ コントローラ カード用の専用メザニン形式ソケット 1 基
RAID バックアップ	supercap 電源モジュール（SCPM）は、RAID コントローラ カードにマウントされます。
PCIe I/O	オプションの I/O エクスパンダは、8x Gen 3 PCIe 拡張スロットを 2 つ提供します。
ネットワークおよび管理 I/O	システムには、システム I/O コントローラ（SIOC）を 1 つまたは 2 つ搭載できます。それにより、背面パネル管理とデータ接続が可能になります。 • SIOC ごとに 2 つの SFP+ 40 Gb ポート • SIOC ごとに 1 つの 10/100/1000 イーサネット専用管理ポート サーバ ノードごとに、KVM ケーブルで 2 つの USB を接続できる 1 つの背面パネル KVM コネクタ、1 つの VGA DB-15 コネクタ、1 つのシリアル DB-9 コネクタがあります。

機能	説明
電源	2 台または 4 台の電源装置、各 1050 W（ホットスワップ可能で 2+2 冗長）。
冷却	前面から背面に冷却を引き出す 4 つの内蔵ファンモジュール、ホットスワップ可能。各ファンモジュールには 2 つのファンが内蔵されています。 さらに、各電源にはファンが 1 個あります。

前面パネルの機能

次の図に、Cisco UCS S3260 システムの前面パネルの機能を示します。

図 *8*：前面パネルの機能



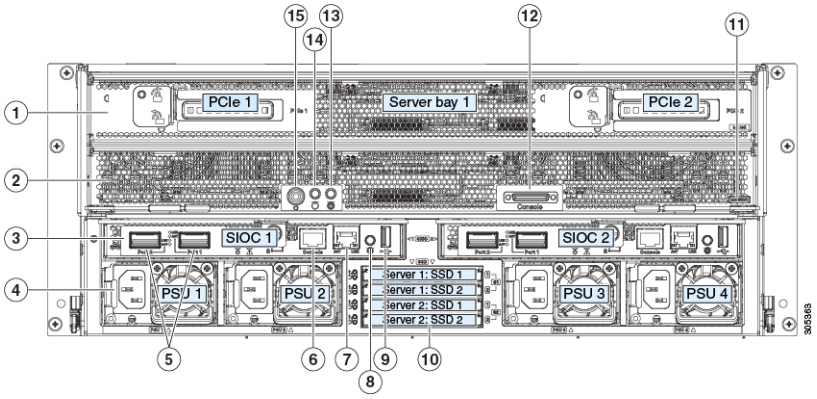
1	操作パネル	6	温度ステータス LED
2	システム電源ボタン/LED	7	電源装置ステータス LED
3	システムユニット識別ボタン/LED	8	ネットワーク リンク アクティビティ LED
4	システム ステータス LED	9	引き出し型の資産タグ（前面ベゼルの下に表示されない）

5	ファン ステータス LED	10	内蔵ドライブのステータス LED

背面パネルの機能

次の図に、Cisco UCS S3260 システムの背面パネルの機能を示します。

図 *9*：前面パネルの機能



1	サーバ ベイ 1 • （オプション）I/O エクスパンダ（図を参照）（Cisco UCS S3260 M4 サーバ ノードのみに搭載） • （オプション）サーバ ノード • （オプション）ドライブ拡張モジュール	8	現時点ではサポートされていません。

2	サーバ ベイ 2 • （オプション）サーバ ノード（図の Cisco UCS S3260 M4） （オプション）ドライブ拡張モジュール	9	現時点ではサポートされていません。
3	システム I/O コントローラ（SIOC） • サーバ ベイ 1 にサーバ ノードがある場合は SIOC 1 が必要 • サーバ ベイ 2 にサーバ ノードがある場合は SIOC 2 が必要です	10	ソリッド ステート ドライブ ベイ（最大で 4 つの 2.5 インチ SAS SSD） • ベイ 1 および 2 の SSD には、サーバ ベイ 1 のサーバ ノードが必要です • ベイ 3 および 4 の SSD には、サーバ ベイ 2 のサーバ ノードが必要です
4	電源装置（4、2+2 として冗長）	11	Cisco UCS S3260 M4 サーバ ノードのラベル（M4 SVRN） （注） このラベルは、Cisco UCS S3260 M4 サーバ ノードを識別します。Cisco UCS S3260 M3 サーバ ノードにはラベルがありません。

5	40 Gb SFP+ ポート（SIOC ごとに 2 つ）	12	KVM コンソール コネクタ（サーバ ノードごとに 1 つ） USB 2 個、VGA 1 個、シリアル コネクタ 1 個を装備した KVM ケーブルで使用
6	Chassis Management Controller（CMS）のデバッグ ファームウェア ユーティリティ ポート（SIOC ごとに 1 つ）	13	サーバ ノードのユニット識別ボタン/LED
7	10/100/1000 専用管理ポート、RJ-45 コネクタ（SIOC ごとに 1 つ）	14	サーバ ノードの電源ボタン
		15	サーバ ノードのリセット ボタン（サーバ ノードのチップセットをリセット）

ストレージ サーバ コンポーネント

サーバ ノード

Cisco UCS S3260 システムは、1 つまたは 2 つのサーバ ノードで構成され、それぞれのノードには 2 つの CPU、128 GB、256 GB、または 512 GB の DIMM メモリ、最大 4 GB キャッシュの RAID カードまたはパススルー コントローラが搭載されています。サーバ ノードは次のいずれかです。

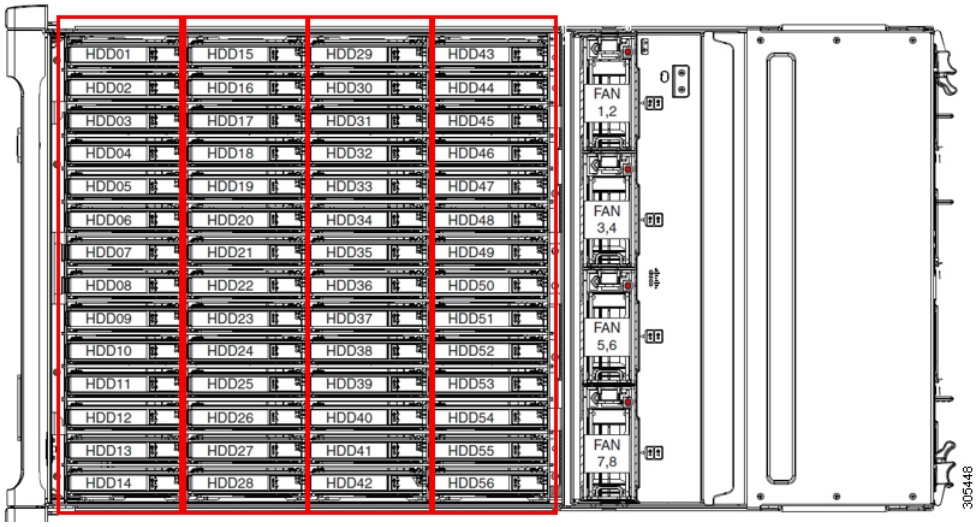
- Cisco UCS S3260 M3 サーバ ノード
- Cisco UCS S3260 M4 サーバ ノード：このノードに、サーバ ノードの上部に接続するオプションの I/O エクスパンダが含まれる場合があります。

ディスク スロット

Cisco UCS S3260 シャーシ の HDD マザーボードに 14 ディスク スロットが 4 行と、HDD 拡張トレイに追加の 4 ディスク スロットがあります。次の図は、上面からアクセス可能でホットスワップ可能な 56 台の 3.5 インチの 6 TB または 4 TB 7200 rpm NL-SAS HDD ドライブのディスクの配置を

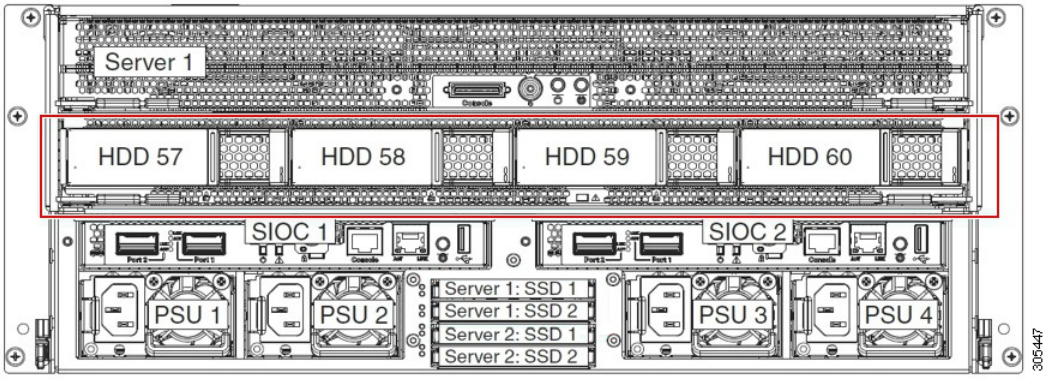
示しています。ディスク スロットに 2 つの SAS ポートがあり、それぞれがシャーシの SAS エクスパンダに接続されます。

図 *10*：*Cisco UCS S3260* 上面図



次の図は、HDD 拡張トレイに 4 つの追加ディスク スロットを備えた Cisco UCS S3260 シャーシを示しています。

図 *11*：*HDD* 拡張トレイを搭載した *Cisco UCS 3260*（背面図）



2 つのサーバ ノードと 2 つの SIOC がある場合、次の機能を使用できます。

1. 上のサーバ ノードは左の SIOC（サーバ スロット 1、SIOC1）を使用します。
2. 下のサーバは右の SIOC（サーバ スロット 2、SIOC2）を使用します。

2 つの SIOC を搭載した 1 つのサーバ ノードがある場合、Server SIOC Connectivity 機能を有効にできます。リリース 3.1(3) から、Cisco UCS S3260 システムでは Server SIOC Connectivity 機能がサ

ポートされています。シャーシに単一サーバとデュアル SIOC が装着されている場合、この機能を使用して、プライマリ SIOC および補助 SIOC の両方を経由するデータ パスを設定できます。

SAS エクスパンダ

Cisco UCS S3260 システムには、冗長モードで動作し、サーバ上のストレージ コントローラにシャーシ レベルでディスクを接続する 2 つの SAS エクスパンダがあります。SAS エクスパンダは、ストレージ コントローラの間に 2 つのパスを提供するため、可用性が向上します。それらには、次の利点があります。

- ハード ドライブのプールを管理します。
- サーバのストレージ コントローラへのハード ドライブのディスクのゾーン設定。

次の表に、各 SAS エクスパンダのポートの、導入の種類に基づくディスクへの接続方法について示します。

ポート範囲	接続
1 ～ 56	上面からアクセス可能なディスク
57 ～ 60	HDD 拡張トレイのディスク。

（注） ストレージ コントローラと SAS エクスパンダ間の SAS のアップリンクの数は、サーバに搭載されているコントローラのタイプによって異なることがあります。

ストレージ エンクロージャ

Cisco UCS S3260 システムのストレージ エンクロージャには次のタイプがあります。

シャーシ レベルのストレージ エンクロージャ

- HDD motherboard enclosure：シャーシの 56 のデュアル ポート ディスク スロットは、HDD マザーボード エンクロージャで構成されています。
- HDD 拡張トレイ：Cisco UCS S3260 システムの追加された 4 つのデュアル ディスク スロットは HDD 拡張トレイで構成されています。

（注） HDD 拡張トレイは現場交換可能ユニット（FRU）です。ディスクは挿入時は未割り当てのままであり、ストレージ コントローラに割り当てることができます。ディスク ゾーン分割の実行方法の詳細については、次を参照してください。 ディスク ゾーン分割ポリシー，（57 ページ）

サーバ レベルのストレージ エンクロージャ

サーバ レベルのストレージ エンクロージャは、サーバに事前に割り当てられた専用のエンクロージャです。次のいずれかになります。

- 背面ブート SSD エンクロージャ：このエンクロージャには、Cisco UCS S3260 システムの背面パネル上の 2 つの 2.5 インチ ディスク スロットが搭載されています。各サーバは 2 つの専用ディスク スロットを備えています。これらのディスク スロットは SATA SSD をサポートします。
- Server board NVMe enclosure：このエンクロージャには 1 つの PCIe NVMe コントローラが搭載されています。

（注） Cisco UCS S3260 システムでは、ディスクを上記の 2 種類のエンクロージャに物理的に配置できますが、ホスト OS からは、ディスクはすべて 1 つの SCSI エンクロージャの一部と見なされます。これらは単一 SES エンクロージャとして動作するように設定された SAS エクスパンダに接続されます。

ストレージ コントローラ

メザニン ストレージ コントローラ

次の表に、さまざまなストレージ コントローラのタイプ、ファームウェアのタイプ、モード、共有および OOB サポートを示します。

表 *4*：

ストレージ コントローラのタイプ	ファームウェアのタイプ	モード	共有	OOB サポート
UCSC-S3X60-R1GB	メガ RAID	HW RAID、JBOD	非対応	対応
UCS-C3K-M4RAID	メガ RAID	HW RAID、JBOD	非対応	対応
UCSC-S3X60-HBA	イニシエータ ターゲット	パススルー	対応	対応

その他のストレージ コントローラ

SW RAID コントローラ：Cisco UCS S3260 システムのサーバは、SW RAID コントローラに接続する PCIe ライザ に埋め込まれている 2 つの専用内部 SSD をサポートしています。このコントローラは、Cisco C3000 M3 サーバでサポートされます。

NVMe コントローラ：このコントローラは、Cisco UCS S3260 システムのサーバによって NVMe ディスクのインベントリとファームウェアのアップデート用に使用されます。

さまざまなサーバ ノードでサポートされているストレージ コントローラに関する詳細は、関連するサービス ノートを参照してください。

- Cisco UCS S3260 ストレージ サーバ サービス ノート用 Cisco UCS C3X60 M3 サーバ ノード
- Cisco UCS S3260 ストレージ サーバ サービス ノート用 Cisco UCS C3X60 M4 サーバ ノード

Cisco UCS S3260 ストレージ管理操作

次の表に、Cisco UCS Manager 統合 Cisco UCS S3260 システムで、実行できるさまざまなストレージ管理操作を示します。

動作	説明	次を参照してください。
高可用性のためのディスクの共有	Cisco UCS S3260 システムの SAS エクスパンダはシャーシ レベルでドライブ プールを管理できます。高可用性のためにディスクを共有するには、次の手順を実行してください。 1 ディスク ゾーン分割ポリシーを作成します。 2 ディスクのスロットを作成し、所有権を割り当てます。 3 シャーシ プロファイルにディスクを関連付けます。	このガイドの「ディスク ゾーン分割ポリシー」セクション。

動作	説明	次を参照してください。
ストレージ プロファイル、ディスク グループおよびディスク グループ設定ポリシー	Cisco UCS S3260 システムのストレージ ディスクの定義、ディスクの割り当ておよび管理のために、Cisco UCS Manager のストレージ プロファイルとディスク グループ ポリシーを利用できます。	『』『』の「Storage Profiles」セクション
ストレージ エンクロージャ操作	サーバで、HDD 拡張トレイを交換するか、以前に挿入したトレイを取り外します。	このガイドの「シャーシ レベルのストレージエンクロージャの削除」セクション。

高可用性のためのディスクの共有

ディスク ゾーン分割ポリシー

ディスク ゾーン分割を使用してサーバ ノードにドライブを割り当てることができます。ディスク ゾーン分割は、同一サーバのコントローラまたは異なるサーバのコントローラで実行することができます。ディスクの所有権は次のいずれかになります。

未割り当て

未割り当てのディスクとは、サーバ ノードに表示されていないものを指します。

専用

専用ディスクとは、コントローラのみに割り当てられるものを指します。

（注） ディスクは割り当てられたコントローラにのみ表示されます。

Shared

共有ディスクとは、複数のコントローラに割り当てられるものを指します。これらは、サーバがクラスタ構成で動作し、各サーバに HBA モードのストレージ コントローラがある場合に絞って使用されます。

重要 ディスクの移行と孤立した LUN の要求：サーバ（サーバ 1）へゾーン分割されたディスクを別のサーバ（サーバ 2）に移行するには、仮想ドライブ（LUN）を転送準備完了としてマークするか、仮想ドライブを非表示にする処理を実行します。次に、そのディスクに割り当てるディスク ゾーン分割ポリシーを変更できます。仮想ドライブ管理の詳細については、『Cisco UCS Manager Storage Management Guide』の「*Disk Groups and Disk Configuration Policies*」のセクションを参照してください。

ディスク ゾーン分割ポリシーの作成

手順

ステップ 1 [Navigation] ペインで [Chassis] をクリックします。

ステップ 2 [Policies] > [root] の順に展開します。

ステップ 3 [Disk Zoning Policies] を右クリックし、[Create Disk Zoning Policy] を選択します。

ステップ 4 [Create Disk Zoning Policy] ダイアログボックスで、次を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明（Description）] フィールド	ポリシーの説明。シスコでは、ポリシーを使用する場所と時期に関する情報を含めることを推奨しています。 256 文字以内で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Preserve Config] 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、スロット番号、所有権、割り当てられたサーバ、割り当てられたコントローラとコントローラのタイプなどのディスクに関するすべての設定関連情報を維持します。 （注） デフォルトでは、[Preserve Config] チェックボックスはオフになっています。

[Disk Zoning Information] 領域で、次を入力します。

名前	フィールド
[Name] カラム	ディスク スロットの名前。
[Slot Number] カラム	ディスクのスロット番号。
[Ownership] カラム	スロットの所有権の値。次のいずれかになります。 • 未割り当て • Dedicated • Shared （注） デュアル HBA コントローラを使用する場合は、特定の条件下では共有モードを使用できません。デュアル HBA コントローラの共有モードの条件を確認するには、表 5：デュアル HBA コントローラの共有モードの制約事項，（59 ページ）を参照してください。 • シャーシのグローバル ホット スペア
[Assigned to Server] 列	ディスクが割り当てられているサーバの ID。
[Assigned to Controller] 列	ディスクが割り当てられているコントローラの ID。
[Controller Type] 列	コントローラのタイプ。ディスクが専用または共有のいずれでも、コントローラ タイプは常に SAS です。

表 *5*：デュアル *HBA* コントローラの共有モードの制約事項

サーバ	HDD トレイ	コントローラ	共有モードのサポート
Cisco UCS S3260	いいえ	デュアル HBA	未サポート
Cisco UCS S3260	HDD トレイ	デュアル HBA	未サポート
事前プロビジョニング	HDD トレイ	デュアル HBA	未サポート

ディスク スロットの作成と所有権の割り当て

ディスク ゾーン分割ポリシーの作成後、ディスク スロットを作成し、所有権を割り当てる必要があります。

手順

ステップ 1 [Navigation] ペインで [Chassis] をクリックします。

ステップ 2 [Policies] > [root] > [Disk Zoning Policies] の順に展開して、ディスク スロットを追加するディスク ゾーン分割ポリシーを選択します。

ステップ 3 [Work] ペインで、[Actions] の下の [Add Slots to Policy] をクリックします。

ステップ 4 [Add Slots to Policy] ダイアログボックスで、次のように入力します。

名前	説明
[Ownership] チェックボックス	ディスク スロットの所有権。次のいずれかになります。 • Unassigned：このオプションは、デフォルトで選択されます。 [Slot Range] フィールドにスロット番号を設定できます。 • Dedicated：このオプションを選択すると、[Server]、[Controller]、およびディスク スロットの [Slot Range] の値を設定する必要があります。 • Shared：このオプションを選択すると、ディスク スロットに対する、[Slot Range] と、割り当てられているサーバ、割り当てられているコントローラ、コントローラのタイプなどのコントローラ情報の値を設定する必要があります。 （注） デュアル HBA コントローラを使用する場合は、特定の条件下では共有モードを使用できません。デュアル HBA コントローラの共有モードの条件を確認するには、表 5：デュアル HBA コントローラの共有モードの制約事項, （59 ページ）を参照してください。 • Chassis Global Hot Spare ：このオプションを選択すると、ディスク スロットに対する [Slot Range] の値を設定する必要があります。

ステップ 5 [OK] をクリックします。

シャーシ プロファイルへのディスク ゾーン分割ポリシーの関連付け

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 シャーシ プロファイルを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 組織を右クリックし、[Create Chassis Profile] を選択します。

ステップ 5 [Identify Chassis Profile] ページで、シャーシ プロファイルの名前を指定し、[Next] をクリックします。

ステップ 6 （任意）[Maintenance Policy] ページで、メンテナンス ポリシーの名前を指定して [Next] をクリックします。

ステップ 7 [Chassis Assignment] ページで、[Chassis Assignment] の下の [Select existing Chassis] を選択し、このシャーシプロファイルに関連付けるシャーシを選択します。[Next] をクリックします。

ステップ 8 [Disk Zoning] ページで、このシャーシ プロファイルに関連付けるディスクのゾーン分割に関するポリシーを指定します。

ステップ 9 [Finish] をクリックします。

ディスクの移行

1 つのサーバから別のサーバへゾーン分割されているディスクを移行する前に、転送準備完了として仮想ドライブ（LUN）をマークするか、または仮想ドライブの非表示操作を実行する必要があります。これにより、サービス プロファイルからのすべての参照がディスクの移行前に削除されたことを確認します。仮想ドライブの詳細については、『』『』の「virtual drives」セクションを参照してください

手順

ステップ 1 [Navigation] ペインで、[Equipment] > [Chassis] > [Servers] の順にクリックします。

ステップ 2 ディスクの移行を実行するサーバを選択します。

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

ステップ 4 [Storage] サブタブをクリックします。

ステップ 5 [LUNs] サブタブをクリックします。

ステップ 6 別のサーバに移行するための仮想ドライブを準備するストレージ コントローラを選択します。

ステップ 7 移行するディスクを選択します。

ステップ 8 [Actions] 領域で、次のいずれかを選択します。

名前	説明
Rename	ディスクの名前を変更するには、このリンクをクリックします。
Delete	ディスクを削除するには、このリンクをクリックします。
Set Transportation Ready	1 つのサーバから別のサーバへ仮想ドライブを安全に移行するには、このリンクをクリックします。 （注） ディスク グループのすべての仮想ドライブは、移行またはサーバノードから割り当て解除される前に、非表示としてマークされている必要があります。
ClearTransportation Ready	仮想ドライブの状態の転送準備完了をクリアするには、このリンクをクリックします。

名前	説明
Hide Virtual Drive	1 つのサーバから別のサーバへ仮想ドライブを安全に移行するには、このオプションをクリックします。 （注） ディスク グループのすべての仮想ドライブは、移行またはサーバ ノードから割り当て解除される前に、非表示としてマークされている必要があります。
Unhide Virtual Drive	仮想ドライブを表示して入出力処理を有効にするには、このリンクをクリックします。

ストレージ エンクロージャ操作

シャーシ レベルのストレージ エンクロージャの削除

物理的に取り外した後で、Cisco UCS Manager の HDD 拡張トレイに対応するストレージ エンクロージャを削除できます。サーバ レベルまたは他のシャーシ レベルのストレージエンクロージャは削除できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [Chassis] > [Servers] > [Storage Enclosures] の順に展開します。
ステップ 3 削除するストレージ エンクロージャを選択します。
ステップ 4 [Actions] 領域で [Remove Enclosure] をクリックします。

第 7 章

ファームウェア管理

- Cisco UCS S3260 システムのファームウェア管理，65 ページ
- シャーシ プロファイルのシャーシ ファームウェア パッケージによるファームウェアのアップグレード，67 ページ
- S3260 シャーシ とサーバ エンドポイントの直接のファームウェア アップグレード，74 ページ

Cisco UCS S3260 システムのファームウェア管理

Cisco UCS では、シスコから取得し、シスコによって認定されたファームウェアを使用して、Cisco UCS ドメインのエンドポイントをサポートします。各エンドポイントは、機能するためにファームウェアが必要な Cisco UCS ドメインのコンポーネントです。

『』『』には、完全なファームウェア管理プロセスの詳細情報が記載されています。さらに、Cisco UCS Manager リリース 3.1(2) 以降では、シャーシのファームウェア ポリシーを定義し、Cisco UCS S3260 シャーシ に関連付けられたシャーシ プロファイルに格納することで、Cisco UCS S3260 シャーシ コンポーネントのファームウェアをアップグレードできます。

Cisco UCS Manager を通じて S3260 シャーシ とサーバを含む Cisco UCS ドメインを次のようにアップグレードできます。

- 自動インストール によるインフラストラクチャ コンポーネントのアップグレード：自動インストール を使用することで 1 つの手順で Cisco UCS Manager ソフトウェアおよびファブリック インターコネクトなどのインフラストラクチャ コンポーネントをアップグレードできます。『』『』には、自動インストール プロセスの詳細情報が記載されています。
- シャーシ プロファイルのシャーシ ファームウェア パッケージを介したシャーシのアップグレード：このオプションにより、1 つの手順ですべてのシャーシ エンドポイントをアップグレードできます。シャーシ ファームウェア パッケージを介してアップグレード可能なシャーシ エンドポイントは次のとおりです。
  - シャーシ アダプタ

- シャーシ管理コントローラ
- シャーシ ボード コントローラ
- ローカル ディスク

（注） シャーシ ファームウェア パッケージを介してシャーシのローカル ディスクをアップグレードできます。ホスト ファームウェア パッケージを介してサーバのローカル ディスクをアップグレードします。

- SAS エクスパンダ

ホスト ファームウェア パッケージを介してのみストレージ コントローラをアップグレードすることができます。

シャーシ ファームウェア パッケージを介したシャーシ コンポーネントのアップグレードは Cisco UCS S3260 シャーシ に固有です。

- サービス プロファイルのファームウェア パッケージを使用してサーバをアップグレード：このオプションを使用すると 1 回のステップですべてのサーバのエンドポイントをアップグレードできるため、サーバのリブートによる中断時間を短くすることができます。サービス プロファイルの更新の延期導入とこのオプションを組み合わせて、スケジュールされたメンテナンス時間中にサーバのリブートが行われるようにすることができます。ホスト ファームウェア パッケージを介してアップグレード可能なサーバ エンドポイントは次のとおりです。
  - CIMC
  - BIOS
  - ボード コントローラ
  - ストレージ コントローラ
  - ローカル ディスク

  『』『』には、ホストのファームウェア パッケージを使用したサーバ エンドポイントのアップグレードに関する詳細情報が記載されています。

また、各インフラストラクチャ、シャーシとサーバ エンドポイントでファームウェアを直接アップグレードすることもできます。このオプションにより、ファブリック インターコネクト、SAS エクスパンダ、CMC、シャーシ アダプタ、ストレージ コントローラ、ボード コントローラを含む、多くのインフラストラクチャ、シャーシ、サーバ エンドポイントを直接アップグレードできます。ただし、直接アップグレードは、ストレージ コントローラ、HBA ファームウェア、HBA オプション ROM、ローカル ディスクなど、すべてのエンドポイントで利用できるわけではありません。

この章では、Cisco UCS S3260 システム向けに新しく導入された次のファームウェア管理機能について説明します。

- シャーシプロファイルのシャーシファームウェア パッケージを介したファームウェアのアップグレード
- Cisco UCS S3260 シャーシ とサーバ エンドポイントでのファームウェアの直接のアップグレード

シャーシ プロファイルのシャーシ ファームウェア パッケージによるファームウェアのアップグレード

Cisco UCS Manager リリース 3.1(2) では Cisco UCS S3260 シャーシ のシャーシ プロファイルとシャーシ ファームウェア パッケージのサポートが追加されています。シャーシ ファームウェア パッケージを定義し、シャーシに関連付けられたシャーシプロファイルに格納することで、Cisco UCS S3260 シャーシ エンドポイントのファームウェアをアップグレードできます。シャーシ プロファイルに関連付けられたシャーシのファームウェアを手動でアップグレードすることはできません。

（注） いずれかのシャーシ コンポーネントが障害状態になると、シャーシ プロファイルの関連付けは失敗します。シャーシ プロファイルの関連付けを進める前に、シャーシ コンポーネントをバックアップすることをお勧めします。シャーシ コンポーネントをバックアップせずに関連付けを続行するには、関連付けの前にコンポーネントを除外します。

シャーシ プロファイルでサーバのファームウェアをアップグレードすることはできません。サービス プロファイルでサーバのファームウェアをアップグレードします。

シャーシのサーバは、シャーシのアップグレード プロセスが開始する前に、自動的に電源が切断されます。

シャーシ ファームウェア パッケージ

このポリシーでは、シャーシ ファームウェア パッケージ（シャーシ ファームウェア パック）を構成するファームウェアバージョンのセットを指定することができます。シャーシファームウェア パッケージには、次のサシャーシ エンドポイントのファームウェアが含まれています。

- シャーシ アダプタ
- シャーシ管理コントローラ
- シャーシ ボード コントローラ
- ローカル ディスク

（注） [Local Disk] は、デフォルトでシャーシ ファームウェア パッケージから除外されます。

- SAS エクスパンダ

ヒント 同じシャーシ ファームウェア パッケージに複数のタイプのファームウェアを含めることができます。たとえば、1 つのシャーシ ファームウェア パッケージに、異なる 2 つのアダプタのモデル用のボード コントローラ ファームウェアとシャーシ アダプタ ファームウェアの両方を含めることができます。ただし、同じ種類、ベンダー、モデル番号に対しては1つのファームウェア バージョンしか使用できません。システムはエンドポイントで必要なファームウェア バージョンを認識し、それ以外のファームウェア バージョンは無視します。

また、新しいシャーシファームウェアパッケージを作成するとき、または既存のシャーシファームウェアパッケージを変更するときに、シャーシファームウェアパッケージから特定のコンポーネントのファームウェアを除外できます。たとえば、シャーシファームウェアパッケージによってボードコントローラ ファームウェアをアップグレードしない場合は、ファームウェアパッケージ コンポーネントのリストからボード コントローラ ファームウェアを除外できます。

重要 各シャーシ ファームウェア パッケージは除外コンポーネントの 1 つのリストと関連付けられます。

シャーシ ファームウェア パッケージは、このポリシーが含まれるシャーシ プロファイルに関連付けられたすべてのシャーシにプッシュされます。

このポリシーにより、同じポリシーを使用しているシャーシ プロファイルに関連付けられているすべてのシャーシでシャーシファームウェアが同一となります。したがって、シャーシプロファイルをあるシャーシから別のシャーシに移動した場合でも、ファームウェア バージョンはそのまま変わりません。さらに、シャーシファームウェアパッケージのエンドポイントのファームウェアバージョンを変更した場合、その影響を受けるシャーシプロファイルすべてに新しいバージョンが即座に適用されます。

影響を受けるシャーシ ファームウェア パッケージに対し、このポリシーをシャーシ プロファイルに含め、そのシャーシのプロファイルにシャーシを関連付けます。

このポリシーは他のどのポリシーにも依存していません。ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認します。Cisco UCS Manager によりシャーシとシャーシプロファイルの関連付けが実行される際にファームウェアイメージが使用できない場合、Cisco UCS Manager はファームウェアのアップグレードを無視し、関連付けを完了します。

シャーシ プロファイルのシャーシ ファームウェア パッケージを使用したファームウェアのアップグレードのステージ

シャーシ プロファイルのシャーシ ファームウェア パッケージ ポリシーを使用して、シャーシ ファームウェアをアップグレードすることができます。

注意 エンドポイントを追加するか、既存のエンドポイントのファームウェア バージョンを変更することにより、シャーシ ファームウェア パッケージを修正すると、Cisco UCS Manager は [Pending Activities] をクリックして変更を確認した後で、エンドポイントをアップグレードします。このプロセスにより、シャーシ間のデータ トラフィックが中断されます。

新しいシャーシ プロファイル

新しいシャーシ プロファイルの場合、このアップグレードは次のステージで行われます。

シャーシ ファームウェア パッケージ ポリシーの作成

このステージでは、シャーシ ファームウェア パッケージを作成します。

シャーシ プロファイルの関連付け

このステージでは、シャーシ プロファイルにシャーシ ファームウェア パッケージを含め、シャーシ プロファイルとシャーシとの関連付けを形成します。システムによって、選択したファームウェア バージョンがエンドポイントにプッシュされます。ファームウェア パッケージで指定したバージョンがエンドポイントで確実に実行されるように、シャーシを再認識させる必要があります。

既存のシャーシ プロファイル

シャーシに関連付けられたシャーシプロファイルの場合、[Pending Activities] をクリックして変更を確認した後で、Cisco UCS Manager がファームウェアをアップグレードします。

シャーシ プロファイルのファームウェア パッケージに対するアップデートの影響

シャーシ プロファイルのシャーシ ファームウェア パッケージを使用してファームウェアをアップデートするには、パッケージ内のファームウェアをアップデートする必要があります。ファームウェア パッケージへの変更を保存した後の動作は、Cisco UCS ドメインの設定によって異なります。

次の表に、シャーシ プロファイルのファームウェア パッケージを使用するシャーシのアップグレードに対する最も一般的なオプションを示します。

シャーシ プロファイル	メンテナンス ポリシー	アップグレード処理
シャーシのファームウェア パッケージが 1 つ以上のシャーシ プロファイルに含まれており、各シャーシ プロファイルが、1つのシャーシに関連付けられています。 または シャーシ ファームウェア パッケージがアップデート中のシャーシ プロファイル テンプレートに含まれており、このテンプレートから作成されたシャーシ プロファイルが 1 つのサーバに関連付けられています。	ユーザ確認応答に関して設定済み	シャーシ ファームウェア パッケージをアップデートすると、次のようになります。 1 Cisco UCS によって、変更を確認するように要求され、シャーシのユーザ確認が必要であることが通知されます。 2 点滅している [Pending Activities] ボタンをクリックし、再認識するシャーシを選択し、新しいファームウェアを適用します。 3 Cisco UCS によって、このポリシーを含むシャーシ プロファイルに関連付けられているすべてのシャーシが照合され、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりシャーシが再認識され、ファームウェアがアップデートされます。 シャーシを手動で再認識しても、Cisco UCS によってシャーシ ファームウェア パッケージが適用されたり、保留中のアクティビティがキャンセルされることはありません。[Pending Activities] ボタンを使用して、保留中のアクティビティを確認応答するか、またはキャンセルする必要があります。

シャーシ ファームウェア パッケージの作成

ヒント 同じシャーシ ファームウェア パッケージに複数のタイプのファームウェアを含めることができます。たとえば、1 つのシャーシ ファームウェア パッケージに、異なる 2 つのアダプタのモデル用のボード コントローラ ファームウェアとシャーシ アダプタ ファームウェアの両方を含めることができます。ただし、同じ種類、ベンダー、モデル番号に対しては1つのファームウェア バージョンしか使用できません。システムはエンドポイントで必要なファームウェア バージョンを認識し、それ以外のファームウェア バージョンは無視します。

また、新しいシャーシファームウェアパッケージを作成するとき、または既存のシャーシファームウェアパッケージを変更するときに、シャーシファームウェアパッケージから特定のコンポーネントのファームウェアを除外できます。

はじめる前に

ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [ポリシー（Policies）] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 [Chassis Firmware Packages] を右クリックして [Create Chassis Firmware Package] を選択します。

ステップ 5 [Create Chassis Firmware Package] ダイアログボックスで、パッケージの一意の名前と説明を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

ステップ 6 [Chassis Package] および [Service Pack] の各ドロップダウン リストから、ファームウェア パッケージを選択します。
[Service Pack] のイメージは、[Chassis Package] のイメージよりも優先されます。

ステップ 7 [Excluded Components] 領域で、このシャーシ ファームウェア パッケージから除外するコンポーネントに対応するチェックボックスをオンにします。
コンポーネント チェックボックスを 1 つもオンにしない場合は、リスト内のすべてのコンポーネントがシャーシ ファームウェア パッケージに含まれます。

（注） [Local Disk] は、デフォルトでシャーシ ファームウェア パックから除外されます。

ステップ 8 [OK] をクリックします。

次の作業

ポリシーをシャーシ プロファイルまたはシャーシ プロファイル テンプレートに含めます

シャーシ ファームウェア パッケージのアップデート

同じシャーシファームウェアパッケージに複数のタイプのファームウェアを含めることができます。たとえば、1 つのシャーシ ファームウェア パッケージに、異なる 2 つのアダプタのモデル用のボード コントローラ ファームウェアとシャーシ アダプタ ファームウェアの両方を含めることができます。ただし、同じ種類、ベンダー、モデル番号に対しては 1 つのファームウェア バー

ジョンしか使用できません。システムはエンドポイントで必要なファームウェア バージョンを認識し、それ以外のファームウェア バージョンは無視します。

また、新しいシャーシファームウェアパッケージを作成するとき、または既存のシャーシファームウェアパッケージを変更するときに、シャーシファームウェアパッケージから特定のコンポーネントのファームウェアを除外できます。

重要　各シャーシ ファームウェア パッケージは除外コンポーネントの 1 つのリストと関連付けられます。

はじめる前に

ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認します。

手順

ステップ 1　[ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2　[シャーシ（Chassis）] > [ポリシー（Policies）] の順に展開します。

ステップ 3　アップデートするポリシーを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4　[Chassis Firmware Packages] を展開し、アップデートするポリシーを選択します。

ステップ 5　[ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 6　シャーシ ファームウェア パッケージのコンポーネントを変更するには、[Modify Package Versions] をクリックします。
[Modify Package Versions] ウィンドウが表示されます。

ステップ 7　シャーシ パッケージを変更するには、[Chassis Package] ドロップダウン リストから、シャーシ パッケージのバージョンを選択します。

ステップ 8　サービス パックを変更するには、[Service Pack] ドロップダウン リストから、サービス パックのバージョンを選択します。
サービス パックを削除するには、[<not set>] を選択します。

ステップ 9　[Excluded Components] 領域で、このシャーシ ファームウェア パッケージから除外するコンポーネントに対応するチェックボックスをオンにします。
コンポーネント チェックボックスを 1 つもオンにしない場合は、リスト内のすべてのコンポーネントがシャーシ ファームウェア パッケージに含まれます。

（注）　[Local Disk] は、デフォルトでシャーシ ファームウェア パックから除外されます。

ステップ 10　[OK] をクリックします。

既存のシャーシ プロファイルへのシャーシ ファームウェア パッケージの追加

シャーシ プロファイルがシャーシに関連付けられると、Cisco UCS Manager は、ユーザの確認後に、新しいバージョンのシャーシのファームウェアを更新し、アクティブ化します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [シャーシ（Chassis）] タブをクリックします。

ステップ 2 [シャーシ（Chassis）] > [シャーシ プロファイル（Chassis Profiles）] の順に展開します。

ステップ 3 アップデートするシャーシ プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[ルート（root）] ノードを展開します。

ステップ 4 シャーシ ファームウェア パッケージを追加するシャーシ プロファイルをクリックします。

ステップ 5 [ワーク（Work）] ペインの [ポリシー（Policies）] タブをクリックします。

ステップ 6 下矢印をクリックして、[Chassis Firmware Package] セクションを展開します。

ステップ 7 シャーシ ファームウェア パッケージを追加するには、[Chassis Firmware Package] ドロップダウンリストから目的のポリシーを選択します。

ステップ 8 [変更の保存（Save Changes）] をクリックします。

Cisco UCS S3260 サーバを使用した UCS ドメインのアップグレード

はじめる前に

- すべてのサーバ ノードがシャットダウンされていることを確認します。
- シャーシ ファームウェア パッケージ ポリシーとシャーシ メンテナンス ポリシーを参照するシャーシ ポリシーが UCS ドメインに割り当てられていることを確認します。

手順

ステップ 1 自動インストールによってインフラストラクチャ ファームウェアをアップグレードします。「自動インストールを使用したインフラストラクチャ ファームウェアのアップグレード」を参照してください。

ステップ 2 シャーシ ファームウェア パッケージ ポリシーを更新します。

- デフォルトのシャーシ ファームウェア パッケージ ポリシーを使用している場合は、新しいパッケージ バージョンでデフォルト シャーシ ファームウェア パッケージ ポリシーを更新し

ます。シャーシ ファームウェア パッケージのアップデート, （71 ページ）を参照してください。

- 新しいシャーシ パッケージ バージョンを使用して新しいシャーシ ファームウェア パッケージポリシーを作成し、既存または割り当て済みのシャーシプロファイル（すべての UserAck を許可）を設定します。新しいシャーシ ファームウェア パッケージポリシーの作成については、シャーシ ファームウェア パッケージの作成, （70 ページ） を参照してください。

このプロセスには 1 ～ 2 時間かかることがあります。シャーシの [FSM] タブでステータスをモニタできます。

ステップ 3 ホストのファームウェアを更新します。「自動インストールによるサーバ ファームウェアのアップグレード」を参照してください。

S3260 シャーシ とサーバ エンドポイントの直接のファームウェア アップグレード

ここでは、S3260 シャーシ とサーバ エンドポイントのアップグレードについて詳しく説明します。

S3260 シャーシ エンドポイント

S3260 シャーシ のファームウェアのアップグレードをトリガーするには、次の順に実行します。

1. CMC 1 ファームウェアの更新
2. CMC 2 ファームウェアの更新
3. シャーシ アダプタ 1 ファームウェアの更新
4. シャーシ アダプタ 2 ファームウェアの更新
5. SAS エクスパンダ 1 ファームウェアの更新
6. SAS エクスパンダ 2 ファームウェアの更新
7. SAS エクスパンダ 1 ファームウェアのアクティブ化
8. SAS エクスパンダ 2 ファームウェアのアクティブ化
9. CMC 1 ファームウェアのアクティブ化
10. CMC 2 ファームウェアのアクティブ化
11. シャーシ アダプタ 1 ファームウェアのアクティブ化
12. シャーシ アダプタ 2 ファームウェアのアクティブ化
13. シャーシ ボード コントローラのアクティブ化

（注） シャーシのローカル ディスクのファームウェアを手動で更新することはできません。ローカル ディスクのファームウェアは、シャーシのファームウェア パッケージに明示的に含めた場合は更新されます。

Cisco UCS S3260 サーバ ノード エンドポイント

サーバ エンドポイントのファームウェアのアップグレードをトリガーするには、次の順に実行します。

1. CIMC の更新
2. CIMC のアクティブ化
3. Update BIOS
4. BIOS のアクティブ化
5. ボード コントローラのアクティブ化
6. ストレージ コントローラのアクティブ化

ファームウェアのアップグレード中は、次の順に実行することを推奨します。

1. インフラストラクチャのアップグレード：Cisco UCS Manager ソフトウェアおよびファブリック インターコネクト
2. シャーシとサーバ エンドポイントのアップグレード

ファームウェアのダウングレード中は、次の順に実行することを推奨します。

1. シャーシとサーバ エンドポイントのダウングレード
2. インフラストラクチャのダウングレード：Cisco UCS Manager ソフトウェアおよびファブリック インターコネクト

シャーシ エンドポイントのファームウェアの直接のアップグレード

S3260 シャーシ の CMC ファームウェアのアップデート

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップパーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* の順に展開します。

ステップ 3 [Work] ペインの [Installed Firmware] タブをクリックして、[Chassis Management Controller] を選択し、[Update Firmware] をクリックします。

ステップ 4 [ファームウェアの更新（Update Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン（Version）] ドロップダウン リストから、エンドポイントをアップデートするファームウェア バージョンを選択します。

b) [OK] をクリックします。
1 つ以上のエンドポイントを直接更新できない場合は、Cisco UCS Manager によって通知メッセージが表示されます。通知メッセージを確認すると、Cisco UCS Manager によって、サーバ上にある直接更新可能な他のすべてのエンドポイントのファームウェアが更新されます。

Cisco UCS Manager によって、選択されたファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまでバックアップとして留まります。

ステップ 5 （任意） [Update Status] 領域でアップデートのステータスをモニタします。
アップデート プロセスは数分かかることがあります。[Installed Firmware] タブの [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

ファームウェアをアクティブにします。

S3260 シャーシ の シャーシ アダプタ ファームウェアのアップデート

両方のファブリック インターコネクトへのアダプタ接続がダウンした場合は、アップグレードはスキップされます。

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [Chassis *Number*] の順に展開します

ステップ 3 [Installed Firmware] タブで [Chassis Adapter] を選択し、[Update Firmware] をクリックします。

ステップ 4 [ファームウェアの更新（Update Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン（Version）] ドロップダウン リストから、エンドポイントをアップデートするファームウェア バージョンを選択します。

b) [OK] をクリックします。
1 つ以上のエンドポイントを直接更新できない場合は、Cisco UCS Manager によって通知メッセージが表示されます。通知メッセージを確認すると、Cisco UCS Manager によって、サーバ上にある直接更新可能な他のすべてのエンドポイントのファームウェアが更新されます。

Cisco UCS Manager によって、選択されたファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまでバックアップとして留まります。

ステップ 5 （任意） [Update Status] 領域でアップデートのステータスをモニタします。
アップデート プロセスは数分かかることがあります。[Installed Firmware] タブの [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

ファームウェアをアクティブにします。

S3260 シャーシ の SAS エクスパンダのファームウェアのアップデート

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップパーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [Chassis *Number*] の順に展開します

ステップ 3 [Installed Firmware] タブで、更新する SAS エクスパンダを選択して [Update Firmware] をクリックします。

ステップ 4 [ファームウェアの更新（Update Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン（Version）] ドロップダウン リストから、エンドポイントをアップデートするファームウェア バージョンを選択します。

b) [OK] をクリックします。
1 つ以上のエンドポイントを直接更新できない場合は、Cisco UCS Manager によって通知メッセージが表示されます。通知メッセージを確認すると、Cisco UCS Manager によって、サーバ上にある直接更新可能な他のすべてのエンドポイントのファームウェアが更新されます。

Cisco UCS Manager によって、選択されたファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまでバックアップとして留まります。

ステップ 5 （任意） [Update Status] 領域でアップデートのステータスをモニタします。
アップデート プロセスは数分かかることがあります。[Installed Firmware] タブの [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

ファームウェアをアクティブにします。

S3260 シャーシ の SAS エクスパンダ ファームウェアのアクティブ化

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [Chassis *Number*] の順に展開します

ステップ 3 [Installed Firmware] タブで、更新する SAS エクスパンダを選択して [Activate Firmware] をクリックします。

ステップ 4 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン設定（Set Version）] ドロップダウン リストから、該当するバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[バージョン設定（Set Version）] ドロップダウン リストにそのバージョ

ンが表示されません。各エンドポイントについて、[スタートアップ バージョン（Startup Version）] カラムからバージョンを選択する必要があります。

b) [OK] をクリックします。

S3260 シャーシの CMC ファームウェアのアクティブ化

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [Chassis *Number*] の順に展開します

ステップ 3 [Installed Firmware] タブで [Chassis Management Controller] を選択し、[Activate Firmware] をクリックします。

ステップ 4 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン設定（Set Version）] ドロップダウン リストから、該当するバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[バージョン設定（Set Version）] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[スタートアップ バージョン（Startup Version）] カラムからバージョンを選択する必要があります。

b) [OK] をクリックします。

S3260 シャーシの シャーシ アダプタ ファームウェアのアクティブ化

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [Chassis *Number*] の順に展開します

ステップ 3 [Installed Firmware] タブで [Chassis Adapter] を選択し、[Activate Firmware] をクリックします。

ステップ 4 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン設定（Set Version）] ドロップダウン リストから、該当するバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[バージョン設定（Set Version）] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[スタートアップ バージョン（Startup Version）] カラムからバージョンを選択する必要があります。

b) [OK] をクリックします。

S3260 シャーシ のシャーシ ボード コントローラ ファームウェアのアクティブ化

（注） Cisco UCS Manager は、以前のバージョンへのシャーシ ボード コントローラ ファームウェアのアクティブ化をサポートしません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [Chassis *Number*] の順に展開します

ステップ 3 [Installed Firmware] タブで [Board Controller] を選択し、[Activate Firmware] をクリックします。

ステップ 4 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン設定（Set Version）] ドロップダウン リストから、該当するバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[バージョン設定（Set Version）] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[スタートアップ バージョン（Startup Version）] カラムからバージョンを選択する必要があります。

b) [OK] をクリックします。

サーバ エンドポイントのファームウェアの直接のアップグレード

Cisco UCS S3260 サーバ ノードの CIMC ファームウェアの更新

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 CIMC をアップデートするサーバのノードを展開します。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [CIMC] タブをクリックします。

ステップ 6 [Actions] 領域で [Update Firmware] をクリックします。

ステップ 7 [ファームウェアの更新（Update Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン（Version）] ドロップダウン リストから、エンドポイントをアップデートするファームウェア バージョンを選択します。

b) [OK] をクリックします。

Cisco UCS Manager によって、選択されたファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまでバックアップとして留まります。

ステップ 8 （任意） [ステータスの更新（Update Status）] 領域でアップデートのステータスをモニタします。アップデート プロセスは数分かかることがあります。[一般（General）] タブの [ファームウェア（Firmware）] 領域の [バックアップ バージョン（Backup Version）] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

ファームウェアをアクティブにします。

Cisco UCS S3260 サーバ ノードの CIMC ファームウェアのアクティブ化

CIMC のファームウェアのアクティベーションによって、データ トラフィックは中断されませんが、すべての KVM セッションで割り込みが発生するため、サーバに接続しているすべての vMedia が切断されます。

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 アップデートしたファームウェアをアクティブにする対象の Cisco Integrated Management Controller（CIMC）が搭載されているサーバのノードを展開します。

ステップ 4 [Work] ペインで [Inventory] タブをクリックします。

ステップ 5 [CIMC] タブをクリックします。

ステップ 6 [Actions] 領域の [Activate Firmware] をクリックします。

ステップ 7 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、次の操作を実行します。

a) [アクティブ化するバージョン（Version To Be Activated）] ドロップダウン リストから、適切なバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[バージョン設定（Set Version）] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[スタートアップ バージョン（Startup Version）] カラムからバージョンを選択する必要があります。

b) スタートアップ バージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[スタートアップ バージョンのみを設定する（Set Startup Version Only）] チェックボックスをオンにします。
[スタートアップ バージョンのみを設定する（Set Startup Version Only）] を設定した場合は、有効化されたファームウェアが pending-next-boot 状態に移行して、エンドポイントがすぐにリブートしません。有効化されたファームウェアは、エンドポイントがリブートするまで、実行中のファームウェアのバージョンになりません。

c) [OK] をクリックします。

Cisco UCS S3260 サーバ ノードの BIOS ファームウェアの更新

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 BIOS のファームウェアをアップデートするサーバのノードを展開します。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [Motherboard] タブをクリックします。

ステップ 6 [Actions] 領域で [Update BIOS Firmware] をクリックします。

ステップ 7 [Update Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version] ドロップダウン リストから、サーバの BIOS のアップデートの対象となるファームウェア バージョンを選択します。

b) （任意） 互換性のない可能性や、現在実行中のタスクに関係なく、ファームウェアをアップデートする場合は、[Force] チェックボックスをオンにします。

c) [OK] をクリックします。

Cisco UCS Manager により、選択したサーバの BIOS ファームウェア パッケージがバックアップ メモリ スロットにコピーされますが、明示的にアクティブ化されるまで、バックアップのままです。

アップデートが完了すると、[Motherboard] タブの [BIOS] 領域で、[Backup Version] の [Update Status] カラムに [Ready] と表示されます。

次の作業

ファームウェアをアクティブにします。

Cisco UCS S3260 サーバ ノードの BIOS ファームウェアのアクティブ化

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 アップデートした BIOS ファームウェアをアクティブ化するサーバのノードを展開します。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [Motherboard] タブをクリックします。

ステップ 6 [Actions] 領域で [Activate BIOS Firmware] をクリックします。

ステップ 7 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version To Be Activated] ドロップダウン リストから、適切なサーバ BIOS のバージョンを選択します。
b) スタートアップ バージョンを設定し、サーバで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。
[Set Startup Version Only] を設定した場合は、アクティブ化されたファームウェアが pending-next-boot 状態に移行し、サーバはすぐにはリブートされません。アクティブ化されたファームウェアは、サーバがリブートされるまでは、実行されているバージョンのファームウェアへ変更されません。
c) [OK] をクリックします。

Cisco UCS S3260 サーバ ノードのボード コントローラ ファームウェアのアクティブ化

（注） このアクティブ化手順を実行すると、サーバはリブートされます。サーバに関連付けられているサービス プロファイルにメンテナンス ポリシーが含まれているかどうかに応じて、リブートはただちに行われることがあります。ボード コントローラ ファームウェアをアップグレードする際は、サーバ BIOS のアップグレードと同時に、（Cisco UCS ドメイン のアップグレードの最後の手順として）サービス プロファイル内のホスト ファームウェア パッケージから行うことをお勧めします。これによって、アップグレード プロセス中にサーバをリブートする回数を低減できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] ノードをクリックします。

ステップ 3 [ワーク（Work）] ペインの [ファームウェア管理（Firmware Management）] タブをクリックします。

ステップ 4 [インストールされているファームウェア（Installed Firmware）] タブで、[ファームウェアの有効化（Activate Firmware）] をクリックします。
Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 [Activate Firmware] ダイアログボックスのメニュー バーにある [Filter] ドロップダウン リストから、[Board Controller] を選択します。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスにボード コントローラを備えたすべてのサーバが表示されます。

ステップ 6 更新するボード コントローラに合わせて、[Startup Version] ドロップダウン リストからバージョンを選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 （任意） 異なるアーキテクチャの CPU にアップグレードする場合には、[Force Board Controller Activation] オプションを使用してファームウェア バージョンを更新することもできます。

Cisco UCS S3260 サーバノードのストレージコントローラ ファームウェアのアクティブ化

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 アクティブ化するストレージ コントローラが存在するサーバを選択します。

ステップ 4 [Installed Firmware] タブで [Storage Controller] を選択し、[Activate Firmware] をクリックします。

ステップ 5 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、次の操作を実行します。

a) [バージョン設定（Set Version）] ドロップダウン リストから、該当するバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[バージョン設定（Set Version）] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[スタートアップ バージョン（Startup Version）] カラムからバージョンを選択する必要があります。

b) [OK] をクリックします。

第 8 章

シャーシ管理

- Cisco UCS S3260 シャーシ，87 ページ
- シャーシの確認，88 ページ
- シャーシの稼働中止，89 ページ
- シャーシの削除，89 ページ
- シャーシのロケータ LED の電源投入，90 ページ
- シャーシのロケータ LED の電源切断，90 ページ
- インベントリからのゾーン分割ポリシーの作成，90 ページ
- シャーシの POST 結果の表示，91 ページ

Cisco UCS S3260 シャーシ

Cisco UCS Manager リリース 3.1(2) では、Cisco UCS 6300 シリーズの Cisco UCS S3260 シャーシ のサポート、6200 シリーズ ファブリック インターコネクト設定が導入されました。

Cisco UCS S3260 シャーシ は、スタンドアロン環境でも、または Cisco Unified Computing System の一部としてでも動作するように設計された、4U シャーシです。次の主要なコンポーネントがあります。

- 4 つの 1050 W AC 電源モジュール（2 + 2 共有および動作の冗長モード）
- 2 つのシステム I/O コントローラ（SIOC）スロット
- 2 つのストレージ スロット、そのうちの 1 つは拡張ストレージに使用可能

（注） シャーシの 2 番目のサーバ スロットは、追加の 4 台の 3.5 インチ ドライブ用の HDD 拡張トレイ モジュールで利用できます。

- 2 番目のサーバの代わりに、オプションの 4 台の 3.5 インチ HDD 拡張トレイ モジュールを含む 56 個の 3.5 インチ ドライブ ベイ
- 6TB HDD を使用した最大 360TB のストレージ容量
- 個々のサーバ モジュールに 3.5 インチ ドライブを割り当てるように設定できるシリアル接続 SCSI（SAS）エクスパンダ
- シャーシの 2 台のサーバは、IO エクスパンダを含む 1 台のダブルハイト サーバと交換可能です

シャーシの確認

シャーシをファブリック インターコネクトに接続するポートを変更した場合は、次の手順を実行します。Cisco UCS Managerがポートの変更を認識していることをシャーシに確認します。

シャーシをファブリック インターコネクトに接続するポートを変更した後、少なくとも 1 分間待ってからシャーシを再確認します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。

ステップ 3 確認するシャーシを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [Actions] 領域の [Acknowledge Chassis] をクリックします。

ステップ 6 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[Yes] をクリックします。
Cisco UCS Managerによって、シャーシの接続が解除され、システム内にシャーシとファブリック インターコネクトとの接続が再確立されます。

シャーシの稼働中止

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。
ステップ 3 稼働を停止するシャーシを選択します。
ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 5 [Actions] 領域で、[Decommission Chassis] をクリックします。
ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。
稼働停止処理が完了するまでには、数分かかる場合があります。

シャーシの削除

はじめる前に

次の手順を実行する前に、シャーシを物理的に取り外します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。
ステップ 3 削除するシャーシを選択します。
ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 5 [Actions] 領域で [Remove Chassis] をクリックします。
ステップ 6 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[Yes] をクリックします。
削除が完了するまでに数分かかる場合があります。

シャーシのロケータ LED の電源投入

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。
ステップ 3 位置を特定する必要があるシャーシをクリックします。
ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 5 [Actions] 領域で [Turn on Locator LED] をクリックします。
ロケータ LED の電源がすでにオンになっている場合、この処理は実行できません。
シャーシの LED が点滅を開始します。

シャーシのロケータ LED の電源切断

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。
ステップ 3 ロケータ LED の電源をオフにするシャーシを選択します。
ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 5 [Actions] 領域で [Turn off Locator LED] をクリックします。
ロケータ LED の電源がすでにオフになっている場合、この処理は実行できません。
シャーシの LED の点滅が停止します。

インベントリからのゾーン分割ポリシーの作成

既存のインベントリとディスクの所有権からディスク ゾーン分割ポリシーを作成できます。

（注） 既存のインベントリからディスク ゾーン分割ポリシーを作成すると、Cisco UCS S3260 シャーシ でのみサポートされます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。
ステップ 3 ゾーン分割ポリシーを作成するシャーシを選択します。
ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 5 [Actions] 領域で、[Create Zoning Policy from Inventory] をクリックします。
ステップ 6 表示された [Create Zoning Policy from Inventory] ダイアログボックスで、次を実行します。
a) [Disk Zoning Policy Name] を入力します。
b) ポリシーを作成する組織を選択します。
c) [OK] をクリックします。
ステップ 7 表示される確認ダイアログボックスで [OK] をクリックします。

シャーシの POST 結果の表示

シャーシ内のすべてのサーバおよびアダプタに対する Power On Self-Test プロセスで収集されたすべてのエラーを表示できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] の順に展開します。
ステップ 3 Power On Self-Test（POST）の結果を表示するシャーシを選択します。
ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 5 [Actions] 領域で [View POST Results] をクリックします。
[POST Results] ダイアログボックスに、シャーシ内の各サーバとそのアダプタに対する POST の結果が一覧表示されます。
ステップ 6 （任意） アダプタのプロパティを表示するには、[Affected Object] カラムをクリックします。
ステップ 7 [OK] をクリックして [POST Results] ダイアログボックスを閉じます。

第 9 章

サーバ管理

- Cisco UCS S3260 サーバ ノード管理，94 ページ
- Cisco UCS S3260 サーバ ノードのブート，94 ページ
- サービス プロファイルからの Cisco UCS S3260 サーバ ノードのブート，95 ページ
- Cisco UCS S3260 サーバ ノードのブート順序の決定，95 ページ
- Cisco UCS S3260 サーバ ノードのシャットダウン，96 ページ
- サービス プロファイルからの Cisco UCS S3260 サーバ ノードのシャットダウン，97 ページ
- Cisco UCS S3260 サーバ ノードのリセット，97 ページ
- Cisco UCS S3260 サーバ ノードの出荷時の初期状態へのリセット，98 ページ
- Cisco UCS S3260 サーバ ノードの再確認，99 ページ
- シャーシからの Cisco UCS S3260 サーバ ノードの削除，100 ページ
- Cisco UCS S3260 サーバ ノードからのインバンド設定の削除，101 ページ
- Cisco UCS S3260 ノードの使用停止，101 ページ
- Cisco UCS S3260 サーバ ノードの再稼働，102 ページ
- S3260 シャーシ 内のサーバ スロットの再認識，102 ページ
- 設定データベースからの存在しない Cisco UCS S3260 サーバ ノードの削除，103 ページ
- Cisco UCS S3260 サーバ ノードのロケータ LED のオン/オフ切り替え，104 ページ
- Cisco UCS S3260 サーバ ノードのローカル ディスク ロケータ LED のオン/オフ切り替え，104 ページ
- Cisco UCS S3260 サーバ ノードの CIMC のリセット，105 ページ
- Cisco UCS S3260 サーバ ノードの CMOS のリセット，105 ページ
- Cisco UCS S3260 サーバ ノードからの NMI の発行，106 ページ
- Cisco UCS S3260 サーバ ノードの POST 結果の表示，107 ページ

- Cisco UCS S3260 サーバ ノードのヘルス イベントの表示，107 ページ
- ヘルス LED アラーム，109 ページ

Cisco UCS S3260 サーバ ノード管理

Cisco UCS Manager では、Cisco UCS ドメインのすべての Cisco UCS S3260 サーバ ノードを管理、モニタできます。電源状態の変更など一部のサーバ管理タスクは、サーバおよびサービス プロファイルから実行できます。

残りの管理タスクは、サーバ上でだけ実行できます。

シャーシ内のサーバ スロットが空の場合、そのスロットに関する情報、エラー、および障害が Cisco UCS Manager から提供されます。サーバ ミスマッチ エラーを解決し、そのスロット内のサーバを再検出するために、スロットを再認識させることもできます。

Cisco UCS S3260 サーバ ノードのブート

[Actions] 領域で [Boot Server] リンクがグレー表示されている場合は、まず、サーバをシャットダウンする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 ブートするサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [Actions] 領域の [Boot Server] をクリックします。

ステップ 6 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

サーバがブートされると、[General] タブの [Overall Status] フィールドに [OK] ステータスが表示されます。

サービス プロファイルからの Cisco UCS S3260 サーバ ノードのブート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [サーバ（Servers）] をクリックします。

ステップ 2 [サービス（Servers）] > [サービス プロファイル（Service Profiles）] の順に展開します。

ステップ 3 サービスプロファイルを作成する組織、または適切なサービスプロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 関連付けられたサーバをブートする必要があるサービス プロファイルを選択します。

ステップ 5 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 6 [Actions] 領域の [Boot Server] をクリックします。

ステップ 7 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

ステップ 8 [Boot Server] ダイアログボックスで [OK] をクリックします。
サーバがブートした後は、[General] タブの [Overall Status] フィールドに [ok] ステータスまたは [up] ステータスが表示されます。

Cisco UCS S3260 サーバ ノードのブート順序の決定

ヒント サーバに関連付けられているサービス プロファイルの [General] タブからもブート順序タブを表示できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 ブート順序を決定するサーバをクリックします。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [Boot Order Details] 領域が展開されていない場合は、見出しの右側の [Expand] アイコンをクリックします。

ステップ 6 サーバに割り当てられているブート順序を表示するには、[Configured Boot Order] タブをクリックします。

ステップ 7 物理サーバ構成内のさまざまなデバイスから何がブートされるかを表示するには、[Actual Boot Order] タブをクリックします。

Cisco UCS S3260 サーバ ノードのシャットダウン

この手順を使用して、インストールされているオペレーティング システムによりサーバをシャットダウンする場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown Server] リンクがグレー表示されている場合、そのサーバは動作していません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 シャットダウンするサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

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

ステップ 6 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに電源オフ状態が表示されます。

サービス プロファイルからの Cisco UCS S3260 サーバ ノードのシャットダウン

この手順を使用して、インストールされているオペレーティング システムによりサーバをシャットダウンする場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown Server] リンクがグレー表示されている場合、そのサーバは動作していません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [サーバ（Servers）] をクリックします。
ステップ 2 [サービス（Servers）] > [サービス プロファイル（Service Profiles）] の順に展開します。
ステップ 3 関連付けられているサービス プロファイルを含む組織のノードを展開します。
ステップ 4 シャットダウンするサーバと関連付けられたサービス プロファイルを選択します。
ステップ 5 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 6 [Actions] 領域で、[Shutdown Server] をクリックします。
ステップ 7 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに [down] ステータスまたは [power-off] ステータスが表示されます。

Cisco UCS S3260 サーバ ノードのリセット

サーバをリセットすると、Cisco UCS Manager により、リセット ライン上にパルスが送信されます。オペレーティング システムのグレースフル シャットダウンを選択することができます。オペレーティング システムがグレースフル シャットダウンをサポートしていない場合は、サーバの電源を切ってから入れ直します。Cisco UCS Manager に、サーバをリセットする前にすべての管理操作を完了させるオプションでは、これらの操作がサーバのリセット前に完了するかどうかは保証されていません。

（注） 電源切断状態からサーバをブートする場合は、[Reset] を使用しないでください。

この手順を使用して電源投入を続けると、サーバの望ましい電源状態が実際の電源状態と同期しなくなり、サーバが後で予期せずシャットダウンすることがあります。選択したサーバを電源切断状態から安全にリブートするには、[Cancel] をクリックし、[Boot Server] アクションを選択します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 リセットするサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

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

ステップ 6 [Reset Server] ダイアログボックスで、次の手順を実行します。

a) [Power Cycle] オプションをクリックします。

b) （任意） このサーバの保留中の管理操作を Cisco UCS Manager によってすべて完了させる場合は、チェックボックスをオンにします。

c) [OK] をクリックします。

リセットが完了するまでに数分かかる場合があります。サーバがリセットされると、[General] タブの [Overall Status] フィールドに OK ステータスが表示されます。

Cisco UCS S3260 サーバ ノードの出荷時の初期状態へのリセット

Cisco UCS S3260 サーバ ノードを出荷時の設定にリセットできるようになりました。デフォルトでは、出荷時へのリセット操作は、ストレージ ドライブに影響しません。これはデータの損失を防止するためです。ただし、これらのデバイスを既知の状態にリセットすることもできます。

次のガイドラインは、スクラブ ポリシーを使用する場合に Cisco UCS S3260 サーバ ノードに適用されます。

- Cisco UCS S3260 サーバ ノードでは、スクラブ ポリシーを使用してストレージを削除することはできません。
- Cisco UCS S3260 サーバ ノードでは、FlexFlash ドライブはサポートされていません。
- Cisco UCS S3260 サーバ ノードでは、スクラブ ポリシーを使用して BIOS だけをリセットできます。

重要 ストレージ デバイスをリセットすると、データが失われる可能性があります。

サーバを出荷時のデフォルト設定にリセットするには、次の手順を実行します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 出荷時のデフォルト設定にリセットするサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [アクション（Actions）] 領域で、[サーバ メンテナンス（Server Maintenance）] をクリックします。

ステップ 6 [メンテナンス（Maintenance）] ダイアログボックスで、次の手順を実行します。

a) [Reset to Factory Default] をクリックします。

b) [OK] をクリックします。

ステップ 7 表示される [Maintenance Server] ダイアログ ボックスから適切なオプションを選択します。

- すべてのストレージを削除するには、[Scrub Storage] チェックボックスを選択します。

  （注） Cisco UCS S3260 サーバ ノードでは、スクラブ ポリシーを使用してストレージを削除することはできません。

- すべてのストレージを削除してからすべてのディスクを初期状態に戻すには、[Create Initial Volumes] チェックボックスを選択します。

  [Scrub Storage] チェックボックスを選択した場合のみ、このチェックボックスを選択できます。JBOD をサポートするサーバの場合、ディスクは JBOD 状態になります。JBOD をサポートしないサーバの場合、各ディスクはディスク内のすべての領域を占有する単一 R0 ボリュームで初期化されます。

  重要 ストレージ プロファイルを使用するには、[Create Initial Volumes] ボックスを選択しないでください。ストレージ プロファイルを使用しているときに初期ボリュームを作成すると、設定エラーが発生する可能性があります。

Cisco UCS Manager は、サーバを出荷時のデフォルト設定にリセットします。

Cisco UCS S3260 サーバ ノードの再確認

サーバ、およびそのサーバのエンドポイントすべてを再検出する必要がある場合は、次の手順を実行します。たとえば、サーバがディスカバリ状態など、予期していなかった状態から抜け出せなくなっている場合に、この手順を使用します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 再確認するサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [アクション（Actions）] 領域で、[サーバ メンテナンス（Server Maintenance）] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Re-acknowledge] をクリックし、次に [OK] をクリックします。
Cisco UCS Manager はサーバを接続解除してから、サーバとシステム内の 1 つまたは複数のファブリック インターコネクトとの接続を確立します。確認が終了するまでに数分かかる場合があります。サーバが確認されると、[General] タブの [Overall Status] フィールドに OK ステータスが表示されます。

シャーシからの Cisco UCS S3260 サーバ ノードの削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 シャーシから削除するサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

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

ステップ 6 [Maintenance] ダイアログボックスで、[Decommission] をクリックし、[OK] をクリックします。
サーバが Cisco UCS構成から削除されます。

ステップ 7 シャーシの物理的な配置場所で、スロットからサーバ ハードウェアを取り外します。
サーバ ハードウェアの取り外し方法については、お使いのシャーシの『*Cisco UCS Hardware Installation Guide*』を参照してください。

次の作業

サーバを物理的に取り付けなおす場合は、スロットを再認識して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

Cisco UCS S3260 サーバ ノードからのインバンド設定の削除

この手順では、ブレード サーバからインバンド管理 IP アドレスの設定を削除します。このアクションがグレー表示されている場合、インバンド設定は完了していません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [サーバ（Servers）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [*Chassis Number*] > [Servers] > [*Server Name*] の順に展開します。

ステップ 3 [Work] 領域の [Inventory] タブをクリックします。

ステップ 4 [CIMC] サブタブをクリックします。

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

ステップ 6 [Delete] の確認ダイアログボックスで [Yes] をクリックします。
サーバのインバンド設定が削除されます。

（注） Cisco UCS Manager でインバンド サービス プロファイルがデフォルト VLAN とプール名で設定されている場合、ここでインバンド設定を削除した約 1 分後、サーバ CIMC が自動的にインバンド プロファイルからインバンド設定を取得します。

Cisco UCS S3260 ノードの使用停止

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 稼働を停止するサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

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

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [Decommission] をクリックします。

b) [OK] をクリックします。

サーバが Cisco UCS構成から削除されます。

次の作業

サーバを物理的に取り付けなおす場合は、Cisco UCS Managerにスロットを再認識させ、そのサーバを再検出させる必要があります。

Cisco UCS S3260 サーバ ノードの再稼働

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [シャーシ（Chassis）] ノードをクリックします。

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

ステップ 4 再稼動する各サーバの行で、[Recommission] カラムのチェックボックスをオンにしてから、[Save Changes] をクリックします。

ステップ 5 確認ダイアログボックスが表示されたら、[はい（Yes）] をクリックします。

ステップ 6 （任意） サーバの再稼動と検出の進行状況を、そのサーバの [FSM] タブでモニタします。

S3260 シャーシ 内のサーバ スロットの再認識

物理ハードウェアをシャーシから取り外さずにサーバの稼働を中止した場合、Cisco UCS Managerにサーバを再検出させ、再認識させるには、次の手順を実行します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 スロットを再確認するサーバを選択します。

ステップ 4 Cisco UCS Managerに [Resolve Slot Issue] ダイアログボックスが表示された場合は、次のいずれかの手順を実行します。

オプション	説明
[Situation] 領域の [here] リンク	このリンクをクリックし、次に確認ダイアログボックスの [Yes] をクリックします。Cisco UCS Managerはスロットを再認識し、スロット内のサーバを検出します。

オプション	説明
[OK]	[General] タブに移動するには、このボタンをクリックします。[Actions] 領域の [Reacknowledge Slot] リンクを使用すると、Cisco UCS Manager でスロットを再確認し、スロット内のサーバを検出できます。

設定データベースからの存在しない Cisco UCS S3260 サーバ ノードの削除

サーバを解放せずにサーバ ハードウェアを物理的に外した場合は、次の手順を実行します。サーバが物理的に存在する場合はこの手順を実行できません。

サーバを物理的に削除するには、シャーシからの Cisco UCS S3260 サーバ ノードの削除, （100 ページ） を参照してください。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 設定データベースから削除するサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

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

ステップ 6 [Maintenance] ダイアログボックスで、[Remove] をクリックし、[OK] をクリックします。
Cisco UCS Manager は、設定データベースからそのサーバに関するすべてのデータを削除します。サーバ スロットは、新しいサーバ ハードウェアの挿入に使用できます。

Cisco UCS S3260 サーバ ノードのロケータ LED のオン/オフ切り替え

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 ロケータ LED のオン/オフを切り替えるサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [Actions] 領域で、次のいずれかをクリックします。

- [Turn on Locator LED]：選択したサーバの LED を点灯します。
- [Turn off Locator LED]：選択したサーバの LED を消灯します。

Cisco UCS S3260 サーバ ノードのローカル ディスク ロケータ LED のオン/オフ切り替え

はじめる前に

- ディスクがゾーン分割されていることを確認します。ゾーン分割されていないディスクでは、ロケータ LED のオンおよびオフはできません。
- ディスクが配置されるサーバの電源が投入されていることを確認します。サーバがオフの場合、ローカル ディスクのロケータ LED のオン/オフを切り替えることはできません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 ローカル ディスクのロケータ LED のオン/オフを切り替えるサーバを選択します。

ステップ 4 [Work] ペインで、[Inventory] > [Storage] > [Disks] タブの順にクリックします。
ストレージ コントローラのインベントリが表示されます。

ステップ 5 ディスクをクリックします。
ディスクの詳細が表示されます。

ステップ 6 [Details] 領域で、[Toggle Locator LED] をクリックします。
[Locator LED] の状態が [On] の場合は、[Off] に切り替わります。[Locator LED] の状態が [Off] の場合は、[On] に切り替わります。

ステップ 7 [Save Changes] をクリックします。

Cisco UCS S3260 サーバ ノードの CIMC のリセット

ファームウェアの場合、サーバのトラブルシューティング時に、CIMC のリセットが必要になることがあります。CIMC のリセットは、通常のサーバ メンテナンスには含まれません。CIMC のリセット後、サーバは、そのサーバで実行されているバージョンのファームウェアを使ってブートされます。

CIMC をリセットすると、CIMC がリブートするまで Cisco UCS の電力モニタリング機能が短時間使用不能になります。通常は20秒しかかかりませんが、その間にピーク電力制限を超える可能性があります。低い電力制限が設定された環境で、設定された電力制限を超えないようにするには、CIMC のリブートまたはアクティブ化を交互に実施することを検討してください。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 CIMC をリセットするサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [アクション（Actions）] 領域の [サーバの復元（Recover Server）] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CIMC (Server Controller)] をクリックし、[OK] をクリックします。

Cisco UCS S3260 サーバ ノードの CMOS のリセット

場合によっては、サーバのトラブルシューティング時に、CMOS のリセットが必要になることがあります。CMOS のリセットは、通常のサーバ メンテナンスには含まれません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 CMOS をリセットするサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [アクション（Actions）] 領域の [サーバの復元（Recover Server）] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CMOS] をクリックし、[OK] をクリックします。

Cisco UCS S3260 サーバ ノードからの NMI の発行

システムが応答しないままになっており、Cisco UCS Manager で、CIMC からマスク不能割り込み（NMI）を BIOS またはオペレーティング システムに発行する必要がある場合は、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 NMI を発行するサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [アクション（Actions）] 領域で、[サーバ メンテナンス（Server Maintenance）] をクリックします。

ステップ 6 [メンテナンス（Maintenance）] ダイアログボックスで、次の手順を実行します。

a) [Diagnostic Interrupt] をクリックします。

b) [OK] をクリックします。

Cisco UCS Manager は BIOS またはオペレーティング システムに NMI を送信します。

Cisco UCS S3260 サーバ ノードの POST 結果の表示

サーバとそのアダプタに対する Power On Self-Test プロセスで収集された任意のエラーを表示できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 POST の結果を表示するサーバを選択します。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [Actions] 領域で [View POST Results] をクリックします。
[POST Results] ダイアログボックスに、サーバとそのアダプタに対する POST の結果が一覧表示されます。

ステップ 6 （任意） アダプタのプロパティを表示するには、[Affected Object] カラムをクリックします。

ステップ 7 [OK] をクリックして [POST Results] ダイアログボックスを閉じます。

Cisco UCS S3260 サーバ ノードのヘルス イベントの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 ヘルス イベントを表示するサーバを選択します。

ステップ 4 [Work] ペインで、[Health] タブをクリックします。
このサーバでトリガーされたヘルス イベントが表示されます。このタブのフィールドは次のとおりです。

名前	説明
[Health Summary] 領域	
[Health Qualifier] フィールド	コンポーネントに対してトリガーされるすべてのヘルス イベントのカンマ区切りの名前。

名前	説明
[Health Severity] フィールド	コンポーネントに対してトリガーされるすべてのステータスイベントの最高重大度。次のいずれかになります。 • critical • major • minor • warning • info • cleared （注） 重大度レベルが最高のものから順に記載されています。
[Health Details] 領域	
[Severity] カラム	ヘルスイベントの重大度。次のいずれかになります。 • critical • major • minor • warning • info • cleared （注） 重大度レベルが最高のものから順に記載されています。
[Name] カラム	ヘルス イベントの名前。
[Description] カラム	ヘルス イベントの詳細。
[Value] カラム	ヘルス イベントの現在の値。
[Details] 領域	[Details] 領域には、[Health Details] 領域で選択するヘルス イベントの [Name] 、[Description] 、[Severity] および [Value] の詳細が表示されます。

ヘルス LED アラーム

サーバ ヘルス LED は、各サーバの前面にあります。Cisco UCS Manager では、センサー故障が発生すると、ブレード ヘルス LED が緑色からオレンジ色またはオレンジ色の点滅に変化します。

ヘルス LED アラームには次の情報が表示されます。

名前	説明
[Severity] カラム	アラームの重大度。次のいずれかになります。 • 重要：サーバのステータス LED がオレンジ色に点滅します。これは赤色のドットで示されます。 • マイナー：サーバのステータス LED がオレンジ色です。これはオレンジ色のドットで示されます。
[Description] カラム	アラームの簡単な説明。
[Sensor ID] カラム	アラームをトリガーしたセンサーの ID。
[Sensor Name] カラム	アラームをトリガーしたセンサーの名前。

ヘルス LED アラームの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [機器（Equipment）] > [シャーシ（Chassis）] > *[Chassis Number]* > [サーバ（Servers）] の順に展開します。

ステップ 3 ヘルス LED アラームを表示する対象のサーバをクリックします。

ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。

ステップ 5 [Actions] 領域で、[View Health LED Alarms] をクリックします。
[View Health LED Alarms] ダイアログボックスに、選択したサーバのヘルス LED アラームが一覧表示されます。

ステップ 6 [OK] をクリックして、[View Health LED Alarms] ダイアログボックスを閉じます。

第 10 章

SIOC 管理

- Cisco UCS Manager での SIOC 管理，111 ページ
- SIOC の認識，112 ページ
- CMC のリセット，113 ページ
- CMC セキュア ブート，113 ページ

Cisco UCS Manager での SIOC 管理

Cisco UCS Manager を使用して Cisco UCS ドメイン内のすべてのシステム I/O コントローラ（SIOC）を管理およびモニタできます。

SIOC の削除または交換

シャーシから SIOC の取り外しや交換ができます。SIOC の取り外しと交換はサービスに影響する操作であるため、シャーシ全体の電源をオフにする必要があります。

SIOC の取り外しのガイドライン

- アクティブな SIOC または両方の SIOC を取り外すには、シャーシ全体をシャットダウンして電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。
- シャーシから SIOC を削除すると、シャーシ全体が Cisco UCS Manager から切断されます。

SIOC の取り外し

SIOC をシステムから取り外すには、次の手順を実行してください。

1 シャットダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。

2 SIOC をシステムに接続しているケーブルを取り外します。

3 システムから SIOC を取り外します。

SIOC の交換

SIOC をシステムから取り外し、別の SIOC に置き換えるには、次の手順を実行してください。

1 シャットダウンして、シャーシ全体の電源を切ります。完全に電源を切るためには、すべての電源コードを抜く必要があります。

2 SIOC をシステムに接続しているケーブルを取り外します。

3 システムから SIOC を取り外します。

4 新しい SIOC をシステムに接続します。

5 ケーブルを SIOC に接続します。

6 電源コードを接続し、システムの電源をオンにします。

7 新しい SIOC を認識させます。

置き換えられた SIOC に接続されているサーバを再度検出します。

（注） 置き換えられた SIOC のファームウェアのバージョンがピア SIOC と異なる場合、シャーシ プロファイルの関連付けを再度トリガーして、置き換えられた SIOC のファームウェアを更新することが推奨されます。

SIOC の認識

Cisco UCS Manager にはシャーシの特定の SIOC を認識する機能もあります。シャーシの SIOC を交換したときには、次の手順を実行します。

注意 この操作では、SIOC とその接続先ファブリック インターコネクトとの間に、ネットワーク接続が再構築されます。この SIOC に対応するサーバは到達不能になり、トラフィックは中断されます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [Equipment] > [Chassis] > [*Chassis Number*] > [SIOC] の順に展開します
ステップ 3 認識する SIOC を選択します。
ステップ 4 [ワーク（Work）] ペインで、[一般（General）] タブをクリックします。
ステップ 5 [Actions] 領域の [Acknowledge SIOC] をクリックします。
ステップ 6 [Acknowledge SIOC] 確認ボックスで、[Yes] をクリックします。

CMC のリセット

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。
ステップ 2 [Equipment] > [Chassis] > [*Chassis Number*] > [SIOC] > [*SIOC Number*] の順に展開します
ステップ 3 [Work] ペインの [Chassis Management Controller] タブをクリックします。
ステップ 4 [Actions] 領域で [Reset CMC] をクリックします。
ステップ 5 [Reset CMC] 確認ボックスで、[Yes] をクリックします。

CMC セキュア ブート

Chassis Management Controller（CMC）のセキュア ブートにより、シスコの署名が付加されたファームウェア イメージのみインストールでき、CMC で実行できます。CMC が更新されると、イメージは、ファームウェアがフラッシュされる前に認証されます。認証に失敗すると、ファームウェアはフラッシュされません。これにより、CMC ファームウェアへの不正アクセスを防止します。

CMC セキュア ブートの注意事項と制約事項

- CMC セキュア ブートは、Cisco UCS S3260 シャーシ 上でのみサポートされます。
- シャーシの関連付けの実行中、1 つの SIOC でセキュア ブートを有効にすると、操作は失敗します。
- CMC セキュア ブートを有効にした後で、無効にすることはできません。

- CMC セキュア ブートはそれが有効にされた SIOC に固有です。CMC セキュア ブートが有効になっている SIOC を置き換えると、[Secure boot operational state] フィールドには新しい SIOC のセキュア ブートのステータスが表示されます。
- CMC セキュア ブートがシャーシで有効にされると、そのシャーシをスタンドアロン モードに戻すことはできず、CMC のファームウェア イメージを Cisco IMC リリース 2.0(13) 以前にダウングレードできなくなります。
- [Secure boot operational state] フィールドには、セキュア ブートのステータスが表示されます。次のいずれかになります。
  - Disabled：CMC セキュア ブートが有効ではありません。これは、デフォルトの状態です。
  - Enabling：CMC セキュア ブートが有効化されています。
  - Enabled： CMC セキュア ブートが有効化されました。

CMC セキュア ブートの有効化

手順

ステップ 1 [ナビゲーション（Navigation）] ペインで [機器（Equipment）] をクリックします。

ステップ 2 [Equipment] > [Chassis] > [*Chassis Number*] > [SIOC] の順に展開します

ステップ 3 CMC セキュア ブートを有効にする SIOC を選択します。

ステップ 4 [Work] ペインの [Chassis Management Controller] タブをクリックします。

ステップ 5 [Actions] 領域で、[Enable Secure Boot] をクリックします。
[Enable Secure Boot] 確認ボックスには次の警告が表示されます。

コミットすると、CMCセキュアブートとインストールが有効になります。この操作は、元に戻すことができません。セキュアブートを有効にしますか。

ステップ 6 [Yes] をクリックします。