



## **Cisco UCS Manager** トラブルシューティング リファレンス ガイド

初版：2016年01月20日

最終更新：2017年01月24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/](http://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、すべてユーザー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 Cisco Systems, Inc. All rights reserved.



## 目次

### はじめに ix

対象読者 ix

表記法 ix

Cisco UCSの関連ドキュメント xi

マニュアルに関するフィードバック xi

### 概要 1

概要 1

### 一般的なトラブルシューティングの解決策 3

トラブルシューティングのガイドライン 3

### 障害 4

障害の重大度 5

障害の状態 5

障害の種類 6

障害のプロパティ 7

障害のライフサイクル 8

Cisco UCS Manager GUI の障害 8

Cisco UCS Manager CLI の障害 8

障害収集ポリシー 9

### Event 9

イベントのプロパティ 9

Cisco UCS Manager GUI のイベント 10

Cisco UCS Manager CLI のイベント 10

### 監査ログ 10

監査ログ エントリのプロパティ 11

Cisco UCS Manager GUI の監査ログ 11

Cisco UCS Manager CLI の監査ログ 12

システム イベント ログ	12
SEL ファイル	12
SEL ポリシー	12
Syslog	13
syslog エントリの形式	13
syslog エントリの重大度	13
syslog エントリのパラメータ	14
syslog サービス	15
テクニカル サポート ファイル	15
Cisco UCS Manager GUI でのテクニカル サポート ファイルの作成	16
Cisco UCS Manager CLI でのテクニカル サポート ファイルの作成	19
Cisco UCS ドメインの電源切断	20
LDAP 設定の確認	21
LDAP プロバイダー設定の確認	21
LDAP プロバイダーのグループ設定の確認	22
<b>Cisco UCS B シリーズでの問題のトラブルシューティング</b>	<b>25</b>
Cisco UCS Manager の初期設定のトラブルシューティング	25
コンソール設定の確認	25
ブートの問題のトラブルシューティング	27
リポート警告が表示されない	27
eUSB にインストールされている OS からサーバがブートしない	27
RAID1 クラスタの移行後にサーバがブートしない	28
KVM の問題のトラブルシューティング	29
KVM ビューアの起動時の BadFieldException	29
KVM コンソールの障害	29
KVM を開けない	30
VM の問題のトラブルシューティング	30
分散仮想スイッチでポートを使用できない	30
Cisco UCS Manager の問題のトラブルシューティング	31
DME プロセスがタイムアウト	31
イベントのシーケンス処理で致命的なエラー	32
ファブリック インターコネクトの問題のトラブルシューティング	33

ブートローダプロンプトからのファブリック インターコネクットの回復	33
ファブリック インターコネクットのクラスタ ID 不一致の解決	33
サーバのディスク ドライブの検出およびモニタリングのトラブルシューティング	34
ローカルストレージモニタリングのサポート	34
ローカルストレージモニタリングの前提条件	36
ディスク ドライブのステータスの確認	36
Cisco UCS Manager GUI でのローカルストレージコンポーネントのステータスの表示	36
監視対象ディスク ドライブのステータスの解釈	36
Cisco UCS Manager GUI で HDD メトリックが更新されない	38
ディスク ドライブの障害検出テストに失敗する	38
Cisco UCS Managerで、使用可能なスロットの合計数よりもサーバ内のディスク数が多く報告される	39
Post-Upgrade IQN の問題のトラブルシューティング	39
重複した IQN の障害のクリアと IQN 発信側名の再設定	39
Cisco UCS PowerToolの取得と重複した IQN スクリプトの実行	41
更新中のサービス プロファイル テンプレートにバインドされているサービス プロファイルの IQN 発信側名の再設定	43
Cisco UCS Central への Cisco UCS ドメインの登録に関する問題のトラブルシューティング	44
...	44
SAN の起動および SAN の接続のトラブルシューティング	45
SAN の接続のチェックリスト	45
SAN アレイの設定のチェックリスト	46
SAN の起動中の問題に関する推奨される解決策	46
サーバのハードウェア問題のトラブルシューティング	49
診断ボタンと LED	49
DIMM メモリの問題	50
メモリの用語および略語	51
DIMM のエラーのトラブルシューティング	51
DIMM の正しい取り付け	51

Cisco UCS Manager CLI を使用した場合の DIMM エラーのトラブルシューティング	52
Cisco UCS Manager GUI を使用した DIMM エラーのトラブルシューティング	54
DIMM の低下エラーのトラブルシューティング	55
動作不能な DIMM エラーのトラブルシューティング	56
DIMM の問題に関する推奨される解決策	56
CPU の問題	58
CLI を使用した CPU の問題のトラブルシューティング	58
GUI を使用した CPU の問題のトラブルシューティング	59
DIMM の問題に関する推奨される解決策	59
CPU CATERR_N の詳細	61
ディスク ドライブと RAID に関する問題	62
RAID コントローラ	62
Quiet Boot のディセーブル化	63
ROM ベースのコントローラ ユーティリティへのアクセス	63
B200 M3 サーバ間での RAID クラスタの移動	64
RAID クラスタ内の障害の発生したドライブの交換	64
ローカルストレージの一貫性チェック操作が失敗する	66
アダプタの問題	66
GUI を使用したアダプタ エラーのトラブルシューティング	67
CLI を使用したアダプタ エラーのトラブルシューティング	67
アダプタの問題に関する推奨される解決策	68
電源の問題	69
Cisco UCS B440 サーバの FET 障害のトラブルシューティング	69
Cisco TAC に連絡するときに必要なとなる情報	70
ファームウェアのトラブルシューティング	73
アップグレード中のファブリック インターコネクットの回復	73
ファブリック インターコネクットまたはブートフラッシュに稼働中のイメージがない場合のファブリック インターコネクットの回復	73
ブートフラッシュに稼働中のイメージがある場合のアップグレード中のファブリック インターコネクットの回復	77

アップグレードまたはフェールオーバー中の無応答のファブリック インターコネクトの回復	78
ファームウェア アップグレード中の IO モジュールの回復	80
ピア I/O モジュールからの I/O モジュールのリセット	80
<b>Cisco IPMI Extensions で発生する問題のトラブルシューティング</b>	<b>81</b>
はじめに	81
シスコ ESR 詳細	82
高レベルの一般的なアルゴリズム	82
バイトの順序付け	83
Cisco ESR IPMI コマンドの定義	83
レコード形式	92
IPMI センサー情報に基づいた推奨される解決策	97
ダウングレード後の IPMI 設定で発生する問題の防止	110
<b>IOM の問題のトラブルシューティング</b>	<b>111</b>
IOM の用語	111
シャーシのブート シーケンス	112
リンクのピン接続とフェールオーバーの動作	114
IOM の問題に関する推奨される解決策	115
<b>その他のトラブルシューティング用マニュアル</b>	<b>121</b>
その他のトラブルシューティング用マニュアル	121





## はじめに

- [対象読者, ix ページ](#)
- [表記法, ix ページ](#)
- [Cisco UCSの関連ドキュメント, 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	説明
GUI 要素	タブの見出し、領域名、フィールドラベルなどのGUI要素は、イタリック体 ( <i>italic</i> ) で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトル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 ( <i>italic</i> ) で示しています。

テキストのタイプ	説明
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、ボールド体 ( <b>bold</b> ) で示しています。 CLI コマンド内の変数は、イタリック体 ( <i>italic</i> ) 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の関連ドキュメント

### 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、<http://www.cisco.com/go/unifiedcomputing/b-series-doc> で入手可能な『Cisco UCS B-Series Servers Documentation Roadmap』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、[Cisco UCS Docs on Twitter](#) 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@cisco.com](mailto:ucs-docfeedback@cisco.com) までご連絡ください。ご協力をよろしくお願いいたします。





# 第 1 章

## 概要

この章は、次の項で構成されています。

- [概要, 1 ページ](#)

## 概要

### Cisco Unified Computing System の機能プレーンのトラブルシューティング

Cisco Unified Computing System (Cisco UCS) は、管理、制御、データの各プレーンを明確に分離するよう設計されています。この項では、3つのプレーン全体へのプロセスのディストリビューションにより発生する、一意に特定および解決すべきトラブルシューティングシナリオについての概要を説明します。

Cisco UCS Manager は、システムを構成した後、管理プレーンとのやり取りなしで動作します。システムは、コントロールプレーンとのやり取りのみで、仮想マシンとともにネットワークプロファイルを移動するなどの作業を遂行します。2つのファブリックインターコネクト間が同期状態かつフェイルオーバーの可用性の高い構成で、Cisco UCS Manager は、ソフトウェアのアップグレード中に失敗またはサービス停止する可能性があります。データおよびコントロールプレーンに影響を与えずにシャットダウンし、新しいバージョンにアップグレードすることができます。Cisco Manager が無効になっている場合でも、OS とアプリケーションは、LAN および SAN のトラフィックを送受信できます。

### トラブルシューティングリファレンスガイドの概要

このガイドでは、Cisco UCS の 3つの機能プレーンに関する一般的な問題のトラブルシューティングに役立つ情報を示します。次の表に、このガイドの全体的な構成を示します。

章	説明
概要	管理、制御、データの 3つの操作の機能プレーンに基づいて、Cisco Unified Computing System の概要を説明します。

章	説明
一般的なトラブルシューティングの解決策	Cisco UCS Manager でトラブルシューティングに使用できるツールに関する情報です。
管理プレーン	
Cisco UCS B シリーズでの問題のトラブルシューティング	サーバの起動、KVM、ファブリックインターコネクタの問題などの Cisco UCS B シリーズの操作に関連する問題のトラブルシューティング情報です。また、Cisco UCS Manager の初期設定に関するトラブルシューティング情報を提供します。
制御およびデータ プレーン	
Cisco UCS SAN 接続のトラブルシューティング	SAN の起動および SAN の接続に関連する問題のトラブルシューティング情報です。
Cisco UCS Manager でのトラブルシューティングおよびアップグレード	ファームウェアのアップグレードプロセスに関連する問題のトラブルシューティング情報です。
サーバのハードウェア問題のトラブルシューティング	DIMM メモリ、CPU、RAID およびアダプタの問題など、サーバのハードウェアに関連する問題のトラブルシューティング情報です。
IOM の問題のトラブルシューティング	IOM 関連の問題のトラブルシューティング情報です。
その他のトラブルシューティング情報	その他のトラブルシューティング ドキュメントへのリンクです。



## 第 2 章

# 一般的なトラブルシューティングの解決策

この章は、次の項で構成されています。

- [トラブルシューティングのガイドライン, 3 ページ](#)
- [障害, 4 ページ](#)
- [Event, 9 ページ](#)
- [監査ログ, 10 ページ](#)
- [システム イベント ログ, 12 ページ](#)
- [Syslog, 13 ページ](#)
- [テクニカル サポート ファイル, 15 ページ](#)
- [Cisco UCS ドメインの電源切断, 20 ページ](#)
- [LDAP 設定の確認, 21 ページ](#)

## トラブルシューティングのガイドライン

Cisco UCS Managerの問題、またはそれが管理するコンポーネントの問題のトラブルシューティングを行うには、次の表に記載するガイドラインに従う必要があります。

表 1: トラブルシューティングのガイドライン

ガイドライン	説明
リリースノートをチェックして、この問題が既知の問題かどうかを確認する。	リリース ノートは、から入手できます。 <a href="http://www.cisco.com/go/unifiedcomputing/b-series-doc">http://www.cisco.com/go/unifiedcomputing/b-series-doc</a> で入手可能な『Cisco UCS B-Series Servers Documentation Roadmap』

ガイドライン	説明
障害またはエラーメッセージのダイアログボックス、コンポーネントのFSM、およびその他の関連する領域のスクリーンショットを取得する。	これらのスクリーンショットは、問題が発生したときのCisco UCS Managerの状態に関する、目に見える手掛かりになります。コンピュータにスクリーンショットを撮るソフトウェアがない場合は、オペレーティングシステムのマニュアルをチェックしてください。このような機能が含まれている場合があります。
問題が発生する前に自分が直接実行した手順を記録する。	画面またはキー入力を記録するソフトウェアにアクセスできる場合は、実行した手順を繰り返して、Cisco UCS Managerで発生した内容を記録します。  このようなソフトウェアを持っていない場合は、実行した手順を繰り返して、その手順およびそれぞれの手順の後に Cisco UCS Managerで発生した内容を詳しくメモします。
テクニカルサポートファイルを作成する。	Cisco UCS ドメインの現在の状態に関する情報は、シスコサポートにとって非常に役立ちます。そのため、問題の原因を識別するために必要な情報を頻繁に提供します。

## 障害

Cisco UCSでは、障害はCisco UCS Managerによって管理される可変オブジェクトです。障害は、Cisco UCS ドメインの障害や、発生したしきい値のアラームを表します。障害のライフサイクルの間に、障害の状態または重大度が変化する場合があります。

各障害には、障害の発生時に影響を受けたオブジェクトの動作状態に関する情報が含まれます。障害の状態が移行して解決すると、そのオブジェクトは機能状態に移行します。

障害は、障害収集ポリシーの設定に従ってクリアおよび削除されるまでCisco UCS Manager内に維持されます。

Cisco UCS ドメイン内のすべての障害は、Cisco UCS Manager CLI またはCisco UCS Manager GUI を使用して表示できます。また、障害収集ポリシーを設定して、Cisco UCS ドメインが障害を収集および保持する方法を決定することもできます。



(注) すべての Cisco UCS障害は MIB に含まれ、SNMP によるトラップが可能です。

## 障害の重大度

Cisco UCS ドメインで発生した障害は、ライフサイクルの中で複数の重大度に移行する場合があります。次の表に、発生する可能性がある障害の重大度を示します。

重大度	説明
Critical	サービスに影響する状態であり、すぐに修正処理が必要です。たとえばこの重大度は、管理対象オブジェクトがアウトオブサービスであり、機能を回復させる必要があることを示している場合があります。
Major	サービスに影響する状態であり、緊急の修正処理が必要です。たとえばこの重大度は、管理対象オブジェクトの機能が著しく低下しており、機能を完全に回復させる必要があることを示している場合があります。
Minor	サービスには影響しない障害の状態であり、より深刻な障害が発生するのを防ぐために修正処理が必要です。たとえばこの重大度は、検出されたアラーム条件が、管理対象オブジェクトの能力を低下させていないことを示している場合があります。
警告	潜在的に、あるいは近い将来に発生する可能性のある、サービスに影響する障害であり、システムに大きな影響を与えていません。必要に応じて、さらに詳しく診断して問題を修正し、サービスに影響を与えるより深刻な障害が発生するのを防ぐ必要があります。
Condition	状態に関する情報メッセージで、単独では重要ではありません。
Info	基本的な通知または情報メッセージで、単独では重要ではありません。

## 障害の状態

Cisco UCS ドメインで発生した障害は、ライフサイクルの中で複数の状態に移行します。次の表に、発生する可能性がある障害の状態をアルファベット順に示します。

状態	説明
クリア済み	解決してクリアされた状態。
Flapping	短い間隔で障害が発生し、クリアされ、再び発生しました。これはフラッピング間隔と呼ばれます。

状態	説明
Soaking	短い間隔で障害が発生してクリアされました。これはフラッピング間隔と呼ばれます。この状態は Flapping 状態の可能性があるので、障害の重大度は元のアクティブな値のままですが、この状態は障害が発生した状態がクリアされたことを示します。

## 障害の種類

Cisco UCS ドメインで発生する障害は、次の表で説明する種類のいずれかになります。

タイプ	説明
fsm	FSM タスクが正常に完了しなかったか、または Cisco UCS Manager が FSM のいずれかの段階を再実行しています。
equipment	Cisco UCS Manager が、物理コンポーネントが動作不能であるか、または物理コンポーネントに別の機能上の問題があることを検出しました。
サーバ	Cisco UCS Manager が、サーバタスク（例：サービスプロファイルをサーバに関連付ける）を完了できません。
設定	Cisco UCS Manager がコンポーネントを正常に設定できません。
環境	Cisco UCS Manager が、電力問題、熱問題、電圧問題、CMOS 設定の喪失を検出しました。
管理	Cisco UCS Manager が、次のような重大な管理上の問題を検出しました。 <ul style="list-style-type: none"> <li>重要なサービスを開始できなかった</li> <li>プライマリ ファブリック インターコネクトを識別できなかった</li> <li>Cisco UCS ドメイン内のコンポーネントに互換性のないファームウェアバージョンが含まれている</li> </ul>
接続性	Cisco UCS Manager が接続に関する問題（例：アダプタに到達できない）を検出しました。
network	Cisco UCS Manager がネットワークに関する問題（例：リンクのダウン）を検出しました。

タイプ	説明
動作中	Cisco UCS Managerが動作に関する問題（例：ログキャパシティの問題、サーバディスクバリの失敗）を検出しました。

## 障害のプロパティ

Cisco UCS Managerは、Cisco UCS ドメイン で発生した各障害に関する詳細な情報を提供します。次の表では、Cisco UCS Manager CLIまたはCisco UCS Manager GUI で表示できる障害のプロパティについて説明します。

プロパティ名	説明
Severity	障害の現在の重大度レベル。これは、 <a href="#">障害の重大度</a> 、（5 ページ）に記載されている重大度のいずれかになります。
Last Transition	障害の重大度が最後に変更された日時。障害が発生してから重大度が変わっていない場合、このプロパティは元の作成日を表します。
Affected Object	障害が発生した状態によって影響を受けるコンポーネント。
説明	障害の説明。
ID	障害に割り当てられた固有識別子。
タイプ	発生した障害の種類。これは、 <a href="#">障害の種類</a> 、（6 ページ）に記載されている種類のいずれかになります。
Cause	障害を発生させた状態に関連付けられている固有識別子。
Created at	障害が発生した日時。
コード	障害に割り当てられた固有識別子。
Number of Occurrences	障害が発生したイベントの発生回数。
Original Severity	障害が最初に発生したときに割り当てられた重大度。
Previous Severity	以前の重大度。このプロパティは、障害の重大度がライフサイクル中に変更された場合にのみ使用されます。
Highest Severity	この問題で発生した一番深刻な重大度。

## 障害のライフサイクル

Cisco UCSの障害はステートフルです。各オブジェクトには、特定の障害のインスタンスが1つだけ存在できます。同じ障害が2度発生すると、Cisco UCSは発生回数を1つずつ増やします。

障害のライフサイクルは次のとおりです。

- 1 ある状況がシステムで発生し、Cisco UCS Managerで障害が発生します。これはアクティブな状態です。
- 2 障害が軽減されると、フラッピングまたはフラッピングを防ぐことを目的としたソーキング間隔になります。障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。フラッピング間隔のうち、障害収集ポリシーに指定されている期間は、障害の重要度が保持されます。
- 3 フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。
- 4 クリアされた障害は保持期間になります。この期間があるため、障害が発生した状態が改善され、さらに障害が早々に削除されていない場合でも管理者が障害に気付くことができます。保持期間のうち、障害収集ポリシーに指定された期間はクリアされた障害が保持されます。
- 5 この状況が保持間隔中に再発生する場合は、障害がアクティブ状態に戻ります。この状況が再発生しない場合は、障害が削除されます。

## Cisco UCS Manager GUI の障害

システム内の1つのオブジェクトの障害を表示する場合は、Cisco UCS Manager GUIでそのオブジェクトにナビゲートして、[Work]ペインの[Faults]タブをクリックします。システム内のすべてのオブジェクトの障害を表示するには、[Faults, Events and Audit Log]の下の[Admin]タブにある[Faults]ノードにナビゲートします。

また、Cisco UCS Manager GUIの左上の[Fault Summary]領域には、Cisco UCS ドメインのすべての障害の要約を表示できます。この領域には、Cisco UCS ドメインで発生したすべての障害の要約が表示されます。

障害の重大度は、それぞれ異なるアイコンで表示されます。各アイコンの下の数字は、システム内でその重大度の障害が発生した回数を示します。アイコンをクリックすると、Cisco UCS Manager GUIによって[Work]ペインの[Faults]タブが開き、その重大度のすべての障害の詳細が表示されます。

## Cisco UCS Manager CLI の障害

システム内のすべてのオブジェクトの障害を表示する場合は、最上位レベルのスコープから **show fault** コマンドを入力します。特定のオブジェクトの障害を表示する場合は、そのオブジェクトのスコープに移動して、**show fault** コマンドを実行します。

障害について入手可能なすべての詳細を表示するには、**show fault detail** コマンドを入力します。

## 障害収集ポリシー

障害収集ポリシーは、フラッピング間隔や保持期間に障害を保持する時間など、Cisco UCS ドメインでの障害のライフサイクルを制御します。



ヒント

障害収集ポリシーの設定方法については、[Cisco UCS B-Series Servers Documentation Roadmap](#) で、Cisco UCS Manager の設定ガイドを参照してください。

## Event

Cisco UCSでは、イベントはCisco UCS Manager によって管理される不変オブジェクトです。各イベントは、Cisco UCS ドメインインスタンスの非永続状態を表します。Cisco UCS Managerがイベントを作成してログに記録した後は、イベントは変更されません。たとえば、サーバの電源を投入すると、Cisco UCS Managerは、その要求の始まりと終わりのイベントを作成して、ログに記録します。

Cisco UCS Manager CLIまたはCisco UCS Manager GUIを使用して、1つのオブジェクトのイベントを表示したり、Cisco UCS ドメインのすべてのイベントを表示したりできます。イベントは、イベントログがいっぱいになるまでCisco UCSに残ります。ログがいっぱいになると、Cisco UCS Managerはログおよびログの中のすべてのイベントを削除します。

## イベントのプロパティ

Cisco UCS Managerでは、Cisco UCS ドメインで作成および記録された各イベントに関する詳細な情報が提供されます。次の表に、Cisco UCS Manager CLIまたはCisco UCS Manager GUI で表示可能な障害のプロパティに関する説明を示します。

表 2: イベントのプロパティ

プロパティ名	説明
Affected Object	イベントを作成したコンポーネント。
説明	イベントの説明
Cause	イベントに関連付けられた固有識別子。
Created at	イベントが作成された日付と時刻。

プロパティ名	説明
User	イベントを作成したユーザの種類。次のような種類があります。 <ul style="list-style-type: none"> <li>• admin</li> <li>• internal</li> <li>• blank</li> </ul>
コード	イベントに割り当てられた固有識別子。

## Cisco UCS Manager GUI のイベント

システム内の1つのオブジェクトのイベントを表示する場合は、Cisco UCS Manager GUI でそのオブジェクトにナビゲートして、[Work] ペインの [Events] タブをクリックします。システム内のすべてのオブジェクトのイベントを表示するには、[Faults, Events and Audit Log] の下の [Admin] タブにある [Events] ノードにナビゲートします。

## Cisco UCS Manager CLI のイベント

システム内のすべてのオブジェクトのイベントを表示する場合は、最上位レベルのスコープから **show event** コマンドを入力します。特定のオブジェクトのイベントを表示する場合は、そのオブジェクトのスコープに移動して、**show event** コマンドを入力します。

イベントについて入手可能なすべての詳細を表示するには、**show event detail** コマンドを入力します。

## 監査ログ

監査ログには、ユーザが Cisco UCS Manager で実行するアクション（直接行うアクションおよび間接的なアクションを含む）が記録されます。監査ログの各エントリは、1つの非永続処理を表します。たとえば、ユーザがログインまたはログアウトしたり、サービスプロファイルなどのオブジェクトを作成、変更、削除したりすると、Cisco UCS Manager はそのアクションのエントリを監査ログに追加します。

監査ログのエントリは、Cisco UCS Manager CLI、Cisco UCS Manager GUI、または Cisco UCS Manager から出力したテクニカル サポート ファイルで表示できます。

## 監査ログ エントリのプロパティ

Cisco UCS Manager では、監査ログの各エントリに関する詳細な情報を提供しています。次の表では、Cisco UCS Manager GUI または Cisco UCS Manager CLI で表示できる障害のプロパティについて説明します。

表 3: 監査ログ エントリのプロパティ

プロパティ名	説明
ID	監査ログ メッセージに関連付けられた固有識別子。
Affected Object	ユーザのアクションによって影響を受けるコンポーネント。
Severity	監査ログメッセージに関連付けられたユーザアクションの現在の重大度。障害の重大度、(5 ページ) で説明しているように、これらの重大度は障害にも使用されます。
Trigger	メッセージを発生したユーザに関連付けられているユーザの役割。
User	イベントを作成したユーザのタイプ。次のタイプがあります。 <ul style="list-style-type: none"> <li>• admin</li> <li>• internal</li> <li>• blank</li> </ul>
説明	監査ログ メッセージが示す処理。次のいずれかの値をとります。 <ul style="list-style-type: none"> <li>• creation : コンポーネントがシステムに追加されました。</li> <li>• modification : 既存のコンポーネントが変更されました。</li> </ul>
説明	ユーザ アクションの説明。

## Cisco UCS Manager GUI の監査ログ

Cisco UCS Manager GUI では、[Faults, Events and Audit Log] ノードの下の [Admin] タブにある [Audit Log] ノードで監査ログを確認できます。

## Cisco UCS Manager CLI の監査ログ

Cisco UCS Manager CLI で、次のコマンドを使用して監査ログを表示できます。

- `scope security`
- `show audit-logs`

## システム イベント ログ

システム イベント ログ (SEL) は、NVRAM 内の CIMC に存在します。過不足の電圧、温度イベント、ファン イベント、BIOS からのイベントなど、ほとんどのサーバ関連イベントが記録されます。SEL は、主にトラブルシューティングのために使用します。

SEL ファイルのサイズは約 40KB で、ファイルがいっぱいになるとそれ以上イベントを記録できません。新たなイベントを記録できるようにするには、ファイルの中身をクリアする必要があります。

SEL ポリシーを使用して、SEL をリモート サーバにバックアップできます。また、必要に応じて、バックアップ操作後に SEL をクリアすることもできます。バックアップ操作は、特定のアクションに基づいて起動するか、定期的に行うことができます。SEL のバックアップやクリアは、手動で行うこともできます。

バックアップ ファイルは、自動的に生成されます。このファイル名の形式は、`sel-SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp` です。たとえば、`sel-UCS-A-ch01-serv01-QCI12522939-20091121160736` となります。

## SEL ファイル

SEL ファイルのサイズは約 40 KB です。SEL ファイルがいっぱいになると、それ以上イベントを記録できません。新たなイベントを記録できるようにするには、ファイルの中身をクリアする必要があります。

## SEL ポリシー

SEL ポリシーを使用して、SEL をリモート サーバにバックアップできます。また、必要に応じて、バックアップ操作後に SEL をクリアすることもできます。バックアップ操作は、特定のアクションに基づいて起動するか、定期的に行うことができます。SEL のバックアップやクリアは、手動で行うこともできます。

Cisco UCS Manager は、SEL ポリシーの設定に従って、SEL のバックアップ ファイルを自動的に生成します。ファイル名の形式は、`sel-SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp` です。

たとえば、ファイル名は sel-UCS-A-ch01-serv01-QCI12522939-20091121160736 のようになります。

## Syslog

syslog は、Cisco UCS ドメインのトラブルシューティングや監査に使用できるシステム ログの収集と処理を一元的に行います。Cisco UCS Manager では、NX-OS syslog メカニズムと API、およびプライマリ ファブリック インターコネクタの syslog 機能を使用して、syslog エントリを収集して処理します。

Cisco UCS Manager は、Cisco UCS ドメインの syslog コレクタを管理および設定し、その設定を 1 つまたは複数のファブリック インターコネクタに展開します。この設定は、Cisco NX-OS または Cisco UCS Manager によって、Cisco UCS ドメインで生成されるすべての syslog エントリに影響します。

syslog および syslog エントリを使用して次の 1 つまたは複数の操作を実行するように Cisco UCS Manager を設定できます。

- syslog エントリをコンソールまたはモニタに表示する
- syslog エントリをファイルに格納する
- syslog エントリを、Cisco UCS ドメインの syslog が格納されている外部ログ コレクタに転送する（最大 3 つまで）

## syslog エントリの形式

Cisco UCS コンポーネントによって生成される各 syslog エントリの形式は、次のとおりです。

```
Year month date hh:mm:ss hostname %facility-severity-MNEMONIC description
```

例：2007 Nov 1 14:07:58 excal-113 %MODULE-5-MOD\_OK: Module 1 is online

## syslog エントリの重大度

syslog エントリには、Cisco UCS Manager によって Cisco UCS の重大度が割り当てられます。次の表に、Cisco UCS の重大度が syslog の重大度にどのようにマップされるかを示します。

表 4: Cisco UCS での syslog エントリの重大度

Cisco UCS の重大度	Syslog の重大度
CRIT	CRIT
MAJOR	ERR
MINOR	WARNING

Cisco UCS の重大度	Syslog の重大度
WARNING	NOTICE
INFO	INFO

## syslog エントリのパラメータ

次の表に、各 syslog エントリに含まれる情報についての説明を示します。

表 5: *syslog* メッセージの内容

名前	説明
ファシリティ	<p>その syslog エントリを生成して送信したログギングファシリティ。このファシリティは大きく分類され、整数で表されます。これらのソースは、次の Linux の標準的なファシリティのいずれかになります。</p> <ul style="list-style-type: none"> <li>• local0</li> <li>• local1</li> <li>• local2</li> <li>• local3</li> <li>• local4</li> <li>• local5</li> <li>• local6</li> <li>• local7</li> </ul>
Severity	<p>syslog エントリが生成される原因となった、イベント、アラート、または問題の重大度。重大度は次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• emergencies</li> <li>• critical</li> <li>• alerts</li> <li>• errors</li> <li>• warnings</li> <li>• 情報</li> <li>• 通知</li> <li>• debugging</li> </ul>

名前	説明
Hostname	<p>エントリの発生元となるコンポーネントに依存する syslog エントリに含まれるホスト名。次のようになります。</p> <ul style="list-style-type: none"> <li>ファブリック インターコネクト、Cisco UCS Manager、または Cisco UCS ドメイン</li> <li>その他すべてのコンポーネントの場合は、仮想インターフェイス（VIF）に関連付けられたホスト名</li> </ul>
Timestamp	syslog エントリが生成された日時。
メッセージ	syslog エントリが生成される原因となった、イベント、アラート、または問題の説明。

## syslog サービス

次の Cisco UCS コンポーネントでは、Cisco NX-OS syslog サービスを使用して、システム情報とアラートに関する syslog エントリを生成します。

- I/O モジュール：syslogd によって、すべての syslog エントリは、接続しているファブリック インターコネクトに送信されます。
- CIMC：すべての syslog エントリは、クラスタ設定内のプライマリ ファブリック インターコネクトに送信されます。
- アダプタ：NIC-Tools/Syslog によって、すべての syslog エントリは、両方のファブリック インターコネクトに送信されます。
- Cisco UCS Manager：syslog の設定に従って、自己生成された syslog エントリがログに記録されます。

## テクニカル サポート ファイル

Cisco Technical Assistance Center（Cisco Technical Assistance Center）によるトラブルシューティングやサポートが必要な問題が発生した場合は、影響を受ける UCS ドメインに関して、できるだけ多くの情報を収集します。Cisco UCS Manager はこの情報をテクニカル サポート ファイルに出力します。このファイルをシスコに送信できます。

テクニカル サポート ファイルは、Cisco UCS ドメインの次のコンポーネントについて作成することができます。

- UCSM：Cisco UCS ドメイン全体のテクニカル サポート データが含まれます。

- UCSM 管理サービス：Cisco UCS Manager 管理サービスのテクニカル サポート データが含まれます（ただし、ファブリック インターコネクトを除きます）。
- シャーシ：特定のシャーシのブレード サーバ上の I/O モジュールまたは CIMC のテクニカル サポート データが含まれます。
- ファブリック エクステンダ：特定の FEX のテクニカル サポート データが含まれます。
- ラック サーバ：特定のラックマウント サーバまたはアダプタのテクニカル サポート データが含まれます。
- サーバ メモリ：特定のラックマウント サーバとブレード サーバに関するサーバ メモリのテクニカル サポート データが含まれます。

## Cisco UCS Manager GUI でのテクニカル サポート ファイルの作成



(注) Cisco UCS Manager Release 1.4(1) よりも前のリリースでは、Cisco UCS Manager CLI でのみテクニカル サポート ファイルを作成できました。

### 手順

- ステップ 1** [Navigation] ペインで [Admin] をクリックします。
- ステップ 2** [All] を展開します。
- ステップ 3** [Work] ペインで、[Create and Download Tech Support] をクリックします。
- ステップ 4** [Create and Download a Tech Support File] ダイアログボックスの [Path] フィールドで、テクニカル サポート ファイルを作成する場所のフルパスを入力します。  
このパスはローカルでアクセスできる必要があります。パスが不明である場合は、[Browse] ボタンをクリックして場所にナビゲートします。

名前	説明
[Path] フィールド	テクニカル サポート ファイルが保存されるフルパス。このパスはローカルでアクセスできる必要があります。

- ステップ 5** [Options] 領域で、次のオプション ボタンのいずれかをクリックします。

オプション	説明
ucsm	<p>Cisco UCS ドメインのテクニカルサポートデータ全体が含まれるファイルを作成します。</p> <p>ucsm を選択すると、Cisco UCS Manager GUI に次のオプションが表示されます。</p> <ul style="list-style-type: none"> <li>• [コマンドの除外 (Exclude Commands) ] : すべての CLI コマンドを除外することによって、テクニカルサポートファイルのサイズを縮小します。</li> <li>• [ファブリック インターコネクト トレース ログを含む (Include Fabric Interconnect Trace Logs) ] : ファブリック インターコネクトにより生成されたトレース ログを含みます。</li> </ul> <p>Cisco Technical Assistance Centerからの指示がある場合にのみ、これらのオプションをチェックする必要があります。</p>
ucsm-mgmt	<p>ファブリック インターコネクトを除く Cisco UCS管理サービスのテクニカル サポート データが含まれるファイルを作成します。</p> <p>ucsm-mgmt を選択すると、Cisco UCS Manager GUI に次のオプションが表示されます。</p> <ul style="list-style-type: none"> <li>• [コマンドの除外 (Exclude Commands) ] : すべての CLI コマンドを除外することによって、テクニカルサポートファイルのサイズを縮小します。</li> <li>• [ファブリック インターコネクト トレース ログを含む (Include Fabric Interconnect Trace Logs) ] : ファブリック インターコネクトにより生成されたトレース ログを含みます。</li> </ul> <p>Cisco Technical Assistance Centerからの指示がある場合にのみ、これらのオプションをチェックする必要があります。</p>

オプション	説明
chassis	<p>指定されたシャーシ内の CIMC または I/O モジュールのいずれかのテクニカルサポートデータが含まれるファイルを作成します。このオプションを選択すると、Cisco UCS Manager GUIには次のフィールドが表示されます。</p> <ul style="list-style-type: none"> <li>• [Chassis ID]フィールド：テクニカル サポート データを取得するシャーシ。</li> <li>• [CIMC]オプションボタン：このオプションを選択すると、CIMC のテクニカル サポート データを取得できます。シャーシ内の1つのサーバのデータを取得するには、そのサーバの ID を [CIMC ID]フィールドに入力します。シャーシ内のすべてのサーバの CIMC データを取得するには、このフィールドに all と入力します。</li> <li>• [IOM]オプション ボタン：このオプションを選択すると、I/O モジュールのテクニカルサポートデータを取得できます。シャーシ内の1つのサーバのデータを取得するには、そのサーバの ID を [IOM ID]フィールドに入力します。シャーシ内のすべてのサーバの I/O モジュールデータを取得するには、このフィールドに all と入力します。</li> </ul>
fabric-extender	<p>ファブリック エクステンダのテクニカルサポートデータが含まれるファイルを作成します。このオプションを選択すると、Cisco UCS Manager GUIには [FEX ID] フィールドが表示されます。このフィールドでは、テクニカルサポートデータを取得する FEX の固有識別子を入力できます。</p>
rack-server	<p>C シリーズ サーバのテクニカルサポートデータが含まれるファイルを作成します。このオプションを選択すると、Cisco UCS Manager GUIには次のフィールドが表示されます。</p> <ul style="list-style-type: none"> <li>• [Rack Server ID]フィールド：テクニカル サポート データを取得するラック サーバの固有識別子。</li> <li>• [Rack Server Adapter ID]フィールド：テクニカル サポート データを取得するアダプタの固有識別子。サーバ内のすべてのアダプタのデータを取得するには、このフィールドに all と入力します。</li> </ul>

オプション	説明
server-memory	<p>B シリーズおよび C シリーズ サーバのサーバ メモリ テクニカル サポート データが含まれるファイルを、指定されたディレクトリに保存します。このオプションを選択すると、Cisco UCS Manager GUI に次のフィールドが表示されます。</p> <p>[Sever IDs] フィールド：詳細なサーバメモリ テクニカル サポート データを必要とするブレードサーバとラックサーバの固有識別子をコンマで区切って記載したリスト。</p>

ステップ 6 [OK] をクリックします。

## Cisco UCS Manager CLI でのテクニカル サポート ファイルの作成

Cisco Technical Assistance Center に送信できる、Cisco UCS ドメインに関する情報を出力するには、**show tech-support** コマンドを使用します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# <b>connect local-mgmt {a   b}</b>	ローカル管理モードを開始します。
ステップ 2	UCS-A(local-mgmt) # <b>show tech-support {chassis chassis-id {all   cimcslot [adapter adapter-id]   iom iom-id}   fex fex-id   server server-id [adapter adapter-id]   server-memory {server-list   all}   ucs   ucs-mgmt} [brief   detail]</b>	<p>選択したオブジェクトに関する情報をファイルに出力します。このファイルを Cisco Technical Assistance Center に送信できます。次のオプションを使用できます。</p> <ul style="list-style-type: none"> <li>• <b>chassis</b> : 指定されたシャーシ内の CIMC または I/O モジュールのいずれかのテクニカル サポート データが含まれるファイルを作成します。</li> <li>• <b>fex</b> : ファブリック エクステンダのテクニカル サポート データが含まれるファイルを作成します。</li> <li>• <b>server</b> : C シリーズ サーバのテクニカル サポート データが含まれるファイルを作成します。</li> <li>• <b>server-memory</b> : すべてのサーバメモリ関連の情報とテクニカル サポート ファイルを作成</li> </ul>

	コマンドまたはアクション	目的
		<p>します。次の場合に、<b>server-memory</b> コマンドを実行できます。</p> <ul style="list-style-type: none"> <li>• 1つのブレードサーバまたはラックマウントサーバ</li> <li>• 複数のブレードサーバ</li> <li>• 複数のラックマウントサーバ</li> <li>• ブレードサーバとラックマウントサーバの組み合わせ</li> <li>• すべてのサーバ</li> </ul> <p><b>重要</b> <code>server-list</code> で複数のサーバを指定する場合は、カンマで区切る必要があります。このコマンドは、サーバの範囲では実行できません。</p> <p><b>detail</b> オプションを併用して <b>server-memory</b> オプションを使用する場合、メモリに関する詳細情報がファイルに保存され、そのファイル名とパスが表示されます。</p> <ul style="list-style-type: none"> <li>• <b>ucsm</b> : Cisco UCS ドメイン全体のテクニカルサポートデータを含むファイルを作成します。</li> <li>• <b>ucsm-mgmt</b> : ファブリックインターコネクトを除く Cisco UCS 管理サービスのテクニカルサポートデータが含まれるファイルを作成します。</li> </ul>
ステップ 3	<pre>UCS-A (local-mgmt) # copyworkspace:techsupport/filename.tar {scp ftp}:user_name@IP_address Enter username's password: password</pre>	<p>SCP または FTP を使用して、出力ファイルを外部の場所にコピーします。</p> <p>SCP および FTP コマンドにはコピー先の場所の絶対パスが必要です。home ディレクトリのパスには、「~」などの特殊記号を含めることはできません。</p>

## Cisco UCS ドメインの電源切断

たとえば、計画停電の一環として、Cisco UCS ドメイン全体の稼働を中止できます。

## 手順

- 
- ステップ 1** 設定バックアップを作成します。  
詳細については、使用しているCisco UCS Managerのリリース用のCisco UCS Manager コンフィギュレーションガイドを参照してください。コンフィギュレーションガイドは、<http://www.cisco.com/go/unifiedcomputing/b-series-doc> で入手可能な『Cisco UCS B-Series Servers Documentation Roadmap』から入手できます。
- ステップ 2** インストールされているオペレーティングシステムから、すべてのブレードまたはラック サーバの電源を正常に切断します。  
サーバ上の OS から、または Cisco UCS Managerを使用して、サーバの電源を切断できます。
- ステップ 3** すべてのサーバの電源を切断してから、シャーシの電源またはラック サーバの電源を取り外します。  
サーバの電源を切断すると、電源 LED が緑色ではなくオレンジ色になります。
- ステップ 4** 次の順序で電源コードを取り外して、各ファブリック インターコネクットの電源を切断します。
- 従属ファブリック インターコネクットを取り外します。
  - プライマリ ファブリック インターコネクットを取り外します。
- 

## LDAP 設定の確認



(注) この手順は、Cisco UCS Manager CLI を使用した場合にのみ実行できます。

Cisco UCS Manager CLI の **test** コマンドにより、Lightweight Directory Access Protocol (LDAP) プロバイダーまたは LDAP プロバイダー グループの設定が確認されます。

## LDAP プロバイダー設定の確認



(注) **test aaa server ldap** コマンドにより、LDAP グローバル設定に関係ない、サーバ固有の設定を確認できます。このコマンドでは、LDAP プロバイダー レベルで設定された、ベース DN、フィルタ、属性、およびタイムアウトの値を使用します。プロバイダー レベルのベース DN またはフィルが空である場合は、LDAP 検索が失敗します。

**test aaa server ldap** コマンドを入力すると、次のように Cisco UCS Manager が LDAP プロバイダーと通信できる場合には、次の情報を確認できます。

- 正しいユーザ名とパスワードが指定されている場合、サーバは認証要求に応答します。
- LDAP のユーザ オブジェクトに対して定義されたロールとロケールがダウンロードされます。
- LDAP グループ許可がオンになっている場合、LDAP グループがダウンロードされます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>connect nxos</b>	nxos モードを開始します。
ステップ 2	<b>test aaa server ldap</b>	LDAP プロバイダー設定を確認します。

応答の例を次に示します。

```
UCS-A# /security # connect nxos
UCS-A#(nxos)# test aaa server ldap 10.193.23.84 kjohn Nbv12345
user has been authenticated
Attributes downloaded from remote server:
User Groups:
CN=g3,CN=Users,DC=ucsm CN=g2,CN=Users,DC=ucsm CN=group-2,CN=groups,DC=ucsm
CN=group-1,CN=groups,DC=ucsm CN=Domain Admins,CN=Users,DC=ucsm
CN=Enterprise Admins,CN=Users,DC=ucsm CN=g1,CN=Users,DC=ucsm
CN=Administrators,CN=Builtin,DC=ucsm
User profile attribute:
shell:roles="server-security,power"
shell:locales="L1,abc"
Roles:
server-security power
Locales:
L1 abc
```

## LDAP プロバイダーのグループ設定の確認



(注) **test aaa group** コマンドにより、LDAP グローバル設定に関係ない、グループ固有の設定を確認できます。

**test aaa group** コマンドを入力すると、次のように Cisco UCS Manager が LDAP グループと通信できる場合には、次の情報を確認できます。

- 正しいユーザ名とパスワードが指定されている場合、サーバは認証要求に応答します。
- LDAP のユーザ オブジェクトに対して定義されたロールとロケールがダウンロードされます。
- LDAP グループ許可がオンになっている場合、LDAP グループがダウンロードされます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>connect nxos</b>	nxos モードを開始します。
ステップ 2	<b>test aaa group</b>	LDAP グループ設定を確認します。

応答の例を次に示します。

```
UCS-A# /security # connect nxos
UCS-A#(nxos)# test aaa group grp-ad1 kjohn Nbv12345
user has been authenticated
Attributes downloaded from remote server:
User Groups:
CN=g3,CN=Users,DC=ucsm CN=g2,CN=Users,DC=ucsm CN=group-2,CN=groups,DC=ucsm
CN=group-1,CN=groups,DC=ucsm CN=Domain Admins,CN=Users,DC=ucsm
CN=Enterprise Admins,CN=Users,DC=ucsm CN=g1,CN=Users,DC=ucsm
CN=Administrators,CN=Builtin,DC=ucsm
User profile attribute:
shell:roles="server-security,power"
shell:locales="L1,abc"
Roles:
server-security power
Locales:
L1 abc
```





## 第 3 章

# Cisco UCS B シリーズでの問題のトラブルシューティング

この章は、次の項で構成されています。

- [Cisco UCS Manager の初期設定のトラブルシューティング](#), 25 ページ
- [ブートの問題のトラブルシューティング](#), 27 ページ
- [KVM の問題のトラブルシューティング](#), 29 ページ
- [VM の問題のトラブルシューティング](#), 30 ページ
- [Cisco UCS Manager の問題のトラブルシューティング](#), 31 ページ
- [ファブリック インターコネクトの問題のトラブルシューティング](#), 33 ページ
- [サーバのディスク ドライブの検出およびモニタリングのトラブルシューティング](#), 34 ページ
- [Post-Upgrade IQN の問題のトラブルシューティング](#), 39 ページ

## Cisco UCS Manager の初期設定のトラブルシューティング

### コンソール設定の確認

両方のファブリック インターコネクトの設定が確実に行われていることを確認するために、SSH を使用してファブリック インターコネクトにログインしたり、CLI を使用してクラスタの状態を確認したりすることができます。この手順については、「[Cisco UCS Manager Initial Setup part 3](#)」をご覧ください。

クラスタの状態を確認するには、次のコマンドを使用します。

コマンド	目的	出力の例
<b>show cluster state</b>	ハイ アベイラビリティ クラスターの両方のファブリック インターコネクタの動作状態およびリーダーシップ ロールを表示します。	次の例の表示では、両方のファブリック インターコネクタが Up 状態、HA が Ready 状態、ファブリック インターコネクタ A がプライマリ ロール、ファブリック インターコネクタ B が従属ロールです。  UCS-A# show cluster state Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4  A: UP, PRIMARY B: UP, SUBORDINATE HA READY
<b>show cluster extended-state</b>	クラスタの状態を詳細に表示します。通常は問題をトラブルシューティングする場合に使用します。	次に、クラスタの状態を詳細に表示する例を示します。  UCSC# show cluster extended-state 0x2e95eaccd0f11e2-0x8ff35147e84f3de2Start time: Thu May 16 06:54:22 2013Last election time: Thu May 16 16:29:28 2015System Management Viewing the Cluster State A: UP, PRIMARY B: UP, SUBORDINATE  A: memb state UP, lead state PRIMARY, mgmt services state: UP B: memb state UP, lead state SUBORDINATE, mgmt services state: UP heartbeat state PRIMARY_OK HA READY Detailed state of the device selected for HA quorum data:  Device 1007, serial: a66b4c20-8692-11df-bd63-1b72ef3ac801, state: active Device 1010, serial: 00e3e6d0-8693-11df-9e10-0f4428357744, state: active Device 1012, serial: 1d8922c8-8693-11df-9133-89fa154e3fa1, state: active

# ブートの問題のトラブルシューティング

## リポート警告が表示されない

問題：依存関係をリストするリポート警告の生成に失敗します。

考えられる原因：この問題は、vNIC テンプレートまたは vHBA テンプレートへの変更が原因で発生する可能性があります。リポート警告は、バックエンドが依存関係のリストを返すときに発生します。vNIC または vHBA テンプレートのテンプレートタイプをアップデートし、ステップ間の変更を適用せずにブート関連プロパティを変更すると、依存関係のリストを返すバックエンドシステムが起動されません。

### 手順

- 
- ステップ 1** Cisco UCS Manager GUI を起動します。
- ステップ 2** サービス プロファイルに含まれる vNIC テンプレートまたは vHBA テンプレートで、次の手順を実行します。
- テンプレートタイプを [Initial Template] から [Updating Template] に変更します。
  - [Save Changes] をクリックします。
- ステップ 3** リポート関連値に追加の変更を加えて、[Save Changes] をクリックします。リポート警告および依存関係のリストが表示されます。
- 

## eUSB にインストールされている OS からサーバがブートしない

問題：Cisco UCS サーバ内に組み込みの eUSB にはオペレーティングシステムが含まれています。けれども、サーバがそのオペレーティングシステムからブートしません。

考えられる原因：この問題は、サーバをサービス プロファイルに関連付けた後、eUSB がサーバの実際のブート順序の 1 番目になっていない場合に発生する可能性があります。

### 手順

- 
- ステップ 1** Cisco UCS Manager GUI を起動します。
- ステップ 2** [サーバ (Servers)] で次の手順を実行して、ブート ポリシー設定を確認します。
- サーバに関連付けられているサービス プロファイルに移動します。
  - [Work] ペインで [Boot Order] タブをクリックします。
  - [Local Disk] がブート ポリシーの 1 番目のデバイスとして設定されていることを確認します。
- ステップ 3** [設備 (Equipment)] で次の手順を実行して、サーバの実際のブート順序を確認します。

- a) サーバに移動します。
- b) [General]タブで [Boot Order Details] 領域を展開し、[Actual Boot Order] タブで eUSB が 1 番目のデバイスとしてリストされていることを確認します。  
たとえば、1 番目のデバイスが [VM eUSB DISK]になっている必要があります。

**ステップ 4** eUSB が実際のブート順序の 1 番目のデバイスでない場合は、次の手順を実行します。

- a) サーバの [General]タブで、[Actions] 領域の次のリンクをクリックします。
  - [KVM Console]をクリックし、KVM コンソールを起動します。
  - [Boot Server]をクリックし、サーバをブートします。
- b) KVM コンソールで、サーバがブートしている間に F2を押して、BIOS 設定を開始します。
- c) BIOS ユーティリティで、[Boot Options]タブをクリックします。
- d) [Hard Disk Order]をクリックします。
- e) [Boot Option #1]を eUSB に設定します。  
たとえば、このオプションを [VM eUSB DISK]に設定します。
- f) F10を押して、設定を保存し、終了します。

## RAID1 クラスタの移行後にサーバがブートしない

**問題：** RAID1 クラスタの移行後に、サーバがオペレーティング システムからブートしません。RAID LUN は、サービス プロファイルのアソシエーション中もアソシエーション後も、「非アクティブ」状態のままになります。その結果、サーバは起動できなくなります。

**考えられる問題：** この問題は、サーバ上のサービス プロファイルのローカル ディスク設定ポリシーが、RAID1 ではなく [Any Configuration]モードで設定されていることが原因で発生する可能性があります。

### 手順

**ステップ 1** Cisco UCS Manager GUIで、[サーバ (Servers) ] をクリックします。

**ステップ 2** サーバに関連付けられているサービス プロファイルに移動し、[Storage]タブをクリックします。

**ステップ 3** 次のいずれかを実行します。

- 次のように、移行する前に、サービス プロファイルに含まれているローカル ディスク設定ポリシーを、サーバに関連付けられているサービス プロファイルのローカル ディスク設定ポリシーと同じポリシーに変更します。
  - [Actions]領域で、[Change Local Disk Configuration Policy] をクリックします。
  - [Select the Local Disk Configuration Policy] ドロップダウン リストから、適切なポリシーを選択します。

- [OK] をクリックします。
- サービス プロファイルに含まれているローカル ディスク設定ポリシーのモード プロパティを、次のように変更します。
  - [Storage] タブの [Local Disk Configuration Policy] 領域で、[Local Disk Policy Instance] フィールド内のリンクをクリックします。
  - [Mode] フィールドで、[Raid 1 Mirrored] オプションが選択されていることを確認します。
  - [Save Changes] をクリックします。

## KVM の問題のトラブルシューティング

### KVM ビューアの起動時の `BadFieldException`

問題：KVM ビューアを起動するとき、`BadFieldException` エラーが発生します。

考えられる原因：ネイティブ ライブラリを使用するアプリケーションと共に `Java Web Start` を使用すると、デフォルトでキャッシュがディセーブルになることによって、この問題が発生することがあります。

#### 手順

- ステップ 1 [Start] > [Control Panel] > [Java] を選択します。
- ステップ 2 [General] タブをクリックします。
- ステップ 3 [Temporary Internet Files] 領域で、[Settings] をクリックします。
- ステップ 4 [Keep temporary files on my computer] チェックボックスをクリックします。
- ステップ 5 [OK] をクリックします。

### KVM コンソールの障害

問題：KVM コンソールが起動に失敗し、JRE によって次のメッセージが表示されます。

```
Unable to launch the application.
```

考えられる原因：この問題は、複数の KVM コンソールが同時に起動された場合に発生する可能性があります。

## 手順

- 
- ステップ 1 可能な場合には、開いているすべての KVM コンソールを閉じます。
- ステップ 2 KVM コンソールを一度に 1 つずつ再起動します。
- 

## KVM を開けない

問題：初めてサーバで KVM を開こうとすると、KVM が起動に失敗します。

考えられる原因：この問題は、JRE バージョンの非互換性が原因で発生する可能性があります。

## 手順

- 
- ステップ 1 JRE 1.6\_11 にアップグレードします。
- ステップ 2 サーバをリブートします。
- ステップ 3 KVM コンソールを起動します。
- 

## VM の問題のトラブルシューティング

### 分散仮想スイッチでポートを使用できない

問題：次のエラーが表示されます。

```
Currently connected network interface x uses Distributed Virtual Switch (uusid:y) which is
accessed on the host via a switch that has no free ports.
```

考えられる原因：この問題は、次のいずれかが原因で発生する可能性があります。

- VM の電源をオフにした後、またはあるホストから別のホストに VM を移行した後、vSphere サーバが hostProxySwitch オブジェクトの numPortsAvailable プロパティの再計算に失敗しています。
- ESX ホスト上で電源がオンになっている VM の vNIC の累積数が、サーバのサービス プロファイルに設定されている動的 nVINC の数と一致しているかまたは上回っています。
- あるデータストアから同じサーバ上の別のデータストアに VM を移行した後、ホスト上で電源がオンになっているすべての VM で使用されている DVS ポート数の増加が、サーバによって誤って検出されています。

## 手順

- 
- ステップ 1** エラーが表示されていたときに実行していた操作を特定します。
- ステップ 2** エラーが、VM の電源をオフにしたことで発生したか、またはあるホストから別のホストに VM を移行したことで発生した場合は、次の手順を実行します。
- 2 番目の VM を ESX ホストから別のシステムに移行します。
  - 2 番目のポートが使用可能になった後、次のいずれかを実行します。
    - VM の電源をオンにします。
    - VM を ESX ホストに再び移行します。
- ステップ 3** エラーが、あるデータストアから同じサーバ上の別のデータストアに VM インスタンスを移行したことで発生した場合は、次の手順を実行します。
- ESX ホスト上のすべての VM をシャットダウンします。
  - 移行を再試行します。
- 

# Cisco UCS Manager の問題のトラブルシューティング

## DME プロセスがタイムアウト

問題 : Cisco UCS Manager CLI コマンドを実行すると、Cisco UCS Manager CLI に次のメッセージが表示されます。

Software Error: Exception during execution: [Error: Timed out communicating with DME]

理由 : この問題は、プライマリ ファブリック インターコネクトの DME プロセスが応答しないか、クラッシュして実行状態にない場合に発生します。DME がダウンした場合に発生する他の症状は次のとおりです。

- Cisco UCS Manager GUI が応答しない
- 仮想 IP の接続がダウンする

## 手順

- 
- ステップ 1** システムがこの状態に至るまでの一連のイベントについての情報を収集します (Cisco UCS Manager のアップグレードや設定の変更など)。
- ステップ 2** 個々の IP アドレスを使用して、各ファブリック インターコネクトに接続し、次のコマンドを使用して、クラスタ ステータス、プロセスおよびコアのダンプを確認します。
- UCS-A# **connect local-mgmt**

クラスタのローカル管理モードを開始します。

- b) UCS-A (local-mgmt) # **show cluster extended-state**  
クラスタ内のファブリック インターコネクトの状態と、クラスタが HA レディであるかどうかを表示します。
- c) UCS-A(local-mgmt)# **show pmon state**  
Cisco UCS Manager内のすべてのプロセスのステータスを表示します。
- d) UCS-A(local-mgmt)# **ls workspace:/cores**  
ワークスペースのすべてのコア ダンプの一覧が表示されます。

**ステップ 3** プライマリ ファブリック インターコネクトを特定し、さらに HA の選択が不完全であるかどうかを確認します。

**ステップ 4** 次のコマンドを使用して、NXOS のログでファブリック インターコネクトのハードウェアの問題を確認します。

- a) UCS-A# **connect nxos {a | b}**  
ファブリック インターコネクトの NX-OS モードを開始します。
- b) UCS-A(nxos)# **show logg**  
ログ ファイルの詳細を表示します。

**ステップ 5** 次のコマンドを使用して、local-mgmt CLI から Cisco UCS Managerのテクニカル サポート情報を収集します。

- a) UCS-A# **connect local-mgmt**  
クラスタのローカル管理モードを開始します。
- b) UCS-A(local-mgmt)# **show tech-support ucsman detail**  
Cisco UCS Managerのテクニカル サポート情報が表示されます。

### 次の作業

障害の詳細について調査するには、これらのログと情報を収集して TAC にお問い合わせください。

## イベントのシーケンス処理で致命的なエラー

問題：スリープ モードから復帰した後、Cisco UCS Manager GUI によって次のメッセージが表示されます。

Fatal error: event sequencing is skewed.

考えられる原因：この問題は、コンピュータがスリープ状態に入るときに Cisco UCS Manager GUI が実行中だった場合に発生する可能性があります。JRE にはスリープ検出メカニズムがないため、システムでは、スリープ モードに入る前に受信したすべてのメッセージを再追跡することはできません。複数回再試行した後、このイベント シーケンス エラーがログに記録されます。



(注) コンピュータをスリープにするときは、必ず Cisco UCS Manager GUI をシャットダウンします。

#### 手順

Cisco UCS Manager GUI で、[Connection Error]ダイアログボックスが表示された場合は、次のいずれかをクリックします。

- [Re-login]をクリックし、Cisco UCS Manager GUI に再度ログインします。
- [Exit]をクリックし、Cisco UCS Manager GUI を終了します。

## ファブリック インターコネクトの問題のトラブルシューティング

### ブート ロード プロンプトからのファブリック インターコネクトの回復

ファブリック インターコネクトの起動に失敗した場合は、次のいずれかの問題が発生している可能性があります。

- キックスタート イメージが破損しているか、その他の理由で機能していない
- ブートフラッシュ メモリのファイル システムが破損している

これらの問題のいずれかが存在する場合、ブートローダプロンプトを使用して、ファブリック インターコネクトを回復することが必要になる場合があります。

#### 手順

Cisco Technical Assistance Centerに問い合わせして、ファームウェア リカバリ イメージと、ブートローダ プロンプトからファブリック インターコネクトを回復する方法の情報を取得します。

### ファブリック インターコネクトのクラスタ ID 不一致の解決

問題：ハイアベイラビリティ クラスタをサポートするように2つのファブリック インターコネクトを設定してL1ポートとL2ポートを接続した場合に、ファブリック インターコネクトのクラスタ ID で不一致が発生する可能性があります。このタイプの不一致は、クラスタで障害が発生したために、Cisco UCS Manager を初期化できないことを意味します。

## 手順

- 
- ステップ 1** Cisco UCS Manager CLI で、ファブリック インターコネク ト B に接続して **erase configuration** を実行します。  
ファブリック インターコネク ト上のすべての設定が消去されます。
- ステップ 2** ファブリック インターコネク ト B をリブートします。  
リブート後、ファブリック インターコネク ト B はファブリック インターコネク ト A のプレゼン スを検出し、ファブリック インターコネク ト A からクラスタ ID をダウンロードします。クラスタ の設定で従属ファブリック インターコネク トを設定する必要があります。
- ステップ 3** 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。 **console** と入力して、コンソール CLI を使用した初期設定を続行します。  
(注) ファブリック インターコネク トによって、クラスタ内のピア ファブリック インターコネク トが検出されます。検出されなかった場合は、L1 ポートと L2 ポート間の物理接続を調べ、ピア ファブリック インターコネク トがクラスタ設定でイネーブルになっていることを確認します。
- ステップ 4** **y** と入力して、従属ファブリック インターコネク トをクラスタに追加します。
- ステップ 5** ピア ファブリック インターコネク トの管理パスワードを入力します。
- ステップ 6** 従属ファブリック インターコネク ト上の管理ポートの IP アドレスを入力します。
- ステップ 7** 設定の要約を確認し、 **yes** と入力して設定を保存および適用するか、 **no** と入力して設定ウィザードを再びやり直し、設定を一部変更します。  
設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、 **Enter** を押します。
- 

# サーバのディスクドライブの検出およびモニタリングの トラブルシューティング

## ローカルストレージモニタリングのサポート

サポートされるモニタリングのタイプは、Cisco UCSサーバによって異なります。

### ローカルストレージモニタリングについてサポートされる Cisco UCSサーバ

Cisco UCS Managerを使用して、次のサーバについてローカルストレージコンポーネントをモニタできます。

- Cisco UCSB200 M3 ブレードサーバ
- Cisco UCSB420 M3 ブレードサーバ

- Cisco UCSB22 M3 ブレード サーバ
- Cisco UCSB200 M4 ブレード サーバ
- Cisco UCSB260 M4 ブレード サーバ
- Cisco UCSB460 M4 ブレード サーバ
- Cisco UCSC460 M2 ラック サーバ
- Cisco UCSC420 M3 ラック サーバ
- Cisco UCSC260 M2 ラック サーバ
- Cisco UCSC240 M3 ラック サーバ
- Cisco UCSC220 M3 ラック サーバ
- Cisco UCSC24 M3 ラック サーバ
- Cisco UCSC22 M3 ラック サーバ
- Cisco UCSC220 M4 ラック サーバ
- Cisco UCSC240 M4 ラック サーバ
- Cisco UCSC460 M4 ラック サーバ



(注) すべてのサーバがすべてのローカルストレージコンポーネントをサポートするわけではありません。Cisco UCSラックサーバの場合は、マザーボードに組み込まれたオンボード SATA RAID 0/1 コントローラはサポートされません。

#### レガシー ディスク ドライブのモニタリングについてサポートされる Cisco UCSサーバ

レガシーディスクドライブモニタリングのみが、次のサーバでCisco UCS Managerを介しサポートされます。

- Cisco UCSB200 M1/M2 ブレード サーバ
- Cisco UCSB250 M1/M2 ブレード サーバ



(注) Cisco UCS Managerがディスクドライブをモニタするには、1064Eストレージコントローラは、パッケージバージョンが2.0(1)以上のUCSバンドルに含まれるファームウェアレベルが必要です。

## ローカルストレージモニタリングの前提条件

これらの前提条件は、有益なステータス情報を提供するため行われるローカルストレージモニタリングやレガシー ディスク ドライブ モニタリングの際に満たす必要があります。

- ドライブがサーバ ドライブ ベイに挿入されている必要があります。
- サーバの電源が投入されている。
- サーバが検出を完了している。
- BIOS POST の完了結果が正常である。

## ディスク ドライブのステータスの確認

### Cisco UCS Manager GUI でのローカルストレージコンポーネントのステータスの表示

#### 手順

- 
- ステップ 1 [Navigation]ペインで [Equipment] をクリックします。
  - ステップ 2 [Equipment] > [Chassis] > [Chassis Number] > [Servers] の順に展開します。
  - ステップ 3 ローカルストレージコンポーネントのステータスを表示するサーバをクリックします。
  - 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 [Storage]サブタブをクリックして、RAID コントローラと FlexFlash コントローラのステータスを表示します。
  - ステップ 6 下矢印をクリックして[Local Disk Configuration Policy]、[Actual Disk Configurations]、[Disks]、[Firmware] バーの順に展開し、追加のステータス情報を表示します。
- 

## 監視対象ディスク ドライブのステータスの解釈

Cisco UCS Managerでは、モニタリング対象のディスク ドライブごとに次のプロパティが表示されます。

- [Operability] : ドライブの動作状態。
- [Presence] : ディスク ドライブのプレゼンス（サーバ ドライブ ベイ内で検出されるかどうかであり、動作状態は関係ない）。

監視対象のディスク ドライブのステータスを判断するには、両方のプロパティを確認する必要があります。次の表に、これらプロパティ値の組み合わせの一般的な解釈を示します。

[Operability]のステータス	Presence Status	解釈
Operable	Equipped	障害が発生していない状態。ディスクドライブは、サーバ内に存在し、使用できます。
Inoperable	Equipped	障害が発生している状態。ディスクドライブはサーバ内に存在していますが、次のいずれかが原因で操作可能性の問題が発生している可能性があります。 <ul style="list-style-type: none"> <li>不良ブロックなどのハードウェアの問題が原因でディスクドライブを使用できません。</li> <li>ストレージコントローラへの IPMI リンクに問題が発生しています。</li> </ul>
該当なし	Missing	障害が発生している状態。サーバドライブベイにディスクドライブが搭載されていません。
該当なし	Equipped	障害が発生している状態。ディスクドライブはサーバ内に存在していますが、次のいずれかが原因で操作可能性の問題が発生している可能性があります。 <ul style="list-style-type: none"> <li>サーバの電源がオフになっています。</li> <li>ストレージコントローラファームウェアは、バージョンが不適切なため、ディスクドライブモニタリングをサポートしていません。</li> <li>サーバでディスクドライブモニタリングがサポートされていません。</li> </ul>



(注) [Operability]フィールドは、ディスクが破損した RAID セットの一部分である、または BIOS POST (電源投入時自己診断テスト) が完了していないなどの理由で不正な状態を表示する場合があります。

## Cisco UCS Manager GUI で HDD メトリックが更新されない

問題：ハードドライブのホットスワップ、取り外し、または追加の後、更新されたハードディスクドライブ (HDD) メトリックが Cisco UCS Manager GUI に表示されません。

考えられる原因：この問題は、Cisco UCS Manager が、システムブート中のみ HDD メトリックを収集することによって発生する場合があります。システムブートの後にハードドライブの追加または取り外しを行った場合、Cisco UCS Manager GUI では HDD メトリックが更新されません。

### 手順

サーバをリブートします。

## ディスク ドライブの障害検出テストに失敗する

問題：サーバディスク ドライブで障害 LED が点灯または点滅していますが、Cisco UCS Manager にはディスク ドライブ障害が示されません。

考えられる原因：次のうちの 1 つ以上の条件に該当することによって、ディスク ドライブの障害検出テストが失敗しました。

- ディスク ドライブには障害が発生しておらず、再構築が進行中です。
- ドライブの予測可能な障害
- B200、B230 または B250 ブレードのディスク 2 における、ドライブ障害
- B200、B230 または B250 ブレードのディスク 1 における、ドライブ障害

### 手順

---

**ステップ 1** エラーが発生したサーバにおける各ディスク ドライブの障害 LED をモニタリングします。

**ステップ 2** サーバの障害 LED がオレンジなどの何らかの色になっているか、または点滅しており、その理由が明らかでない場合は、エラーが発生したそれぞれのサーバについてテクニカルサポートファイルを作成し、Cisco Technical Assistance Centerにご連絡ください。

---

## Cisco UCS Managerで、使用可能なスロットの合計数よりもサーバ内のディスク数が多く報告される

問題：Cisco UCS Managerで、サーバ内で使用可能なディスク スロットの合計数よりも、サーバのディスク数が多く報告されます。たとえば次のように、Cisco UCS Managerで、ディスク スロットが2つあるサーバに対して3つのディスクが報告されます。

```
RAID Controller 1:
  Local Disk 1:
    Product Name: 73GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted
    PID: A03-D073GC2
    Serial: D3B0P99001R9
    Presence: Equipped
  Local Disk 2:
    Product Name:
    Presence: Equipped
    Size (MB): Unknown
  Local Disk 5:
    Product Name: 73GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted
    Serial: D3B0P99001R9
    HW Rev: 0
    Size (MB): 70136
```

考えられる原因：この問題は一般的に、Cisco UCS Managerと不正確な情報を報告しているサーバ間の通信障害が原因で発生します。

### 手順

- 
- ステップ1 Cisco UCS ドメインを最新リリースの Cisco UCS ソフトウェアおよびファームウェアにアップグレードします。
  - ステップ2 サーバの稼働を中止する。
  - ステップ3 サーバを再稼働します。
- 

## Post-Upgrade IQN の問題のトラブルシューティング

### 重複した IQN の障害のクリアと IQN 発信側名の再設定

問題：Cisco UCS Release 2.0(1) から Release 2.0(2) にアップグレードした後、サービス プロファイルでホストファームウェアパッケージの変更などのアクションを実行しようとする、Cisco UCS Manager によって1つ以上のサービス プロファイルで IQN 関連の障害が発生します。

考えられる原因：単一のサービスプロファイルまたは複数のサービスプロファイルで使用されている1つ以上の iSCSI vNICs に、一意の IQN 発信側名が指定されていません。

## 手順

- 
- ステップ 1** Cisco UCS Manager CLI にログインします。
- ステップ 2** 次のコマンドを実行して、Cisco UCS ドメイン内の IQN のリストを表示します。  
UCS-A# **show identity iqn | include iqn name**
- ステップ 3** Cisco UCS PowerTool でスクリプトを実行して、重複する IQN を含む iSCSI vNIC を特定します。
- ステップ 4** IQN 発信側名が登録されていないサービス プロファイルで、発信側 ID をデフォルトの IQN プールに変更するか、または手動で一意的 IQN を割り当てます。
- ステップ 5** 発信側 ID を変更したサービス プロファイルで、次のように発信側割り当てを割り当てた名前またはプールに変更します。
- UCS-A # **scope org org-name**  
指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
  - UCS-A /org # **scope service-profile profile-name**  
サービス プロファイルのサービス プロファイル組織モードを開始します。
  - UCS-A/org# **scope vnic-iscsi iscsi\_vnic\_name**  
指定した iSCSI vNIC のモードを開始します。  
  
(注) この vNIC は未登録であり、**show identity iqn** で表示されません。
  - UCS-A /org/service-profile/vnic-iscsi\* # **set iscsi-identity {initiator-name initiator-name | initiator-pool-name iqn-pool-name}**  
iSCSI 発信側の名前または iSCSI 発信側名の提供元の IQN プール名を指定します。iSCSI 発信側名には最大 223 文字を使用できます。
  - UCS-A /org/service-profile/vnic-iscsi # **commit-buffer**  
トランザクションをシステムの設定にコミットします。  
  
(注) 発信側名の変更にはストレージ側の設定も関係しますが、これについてはこのマニュアルでは説明していません。
- ステップ 6** サービス プロファイルに対するアクションを実行して、Cisco UCS データベースにイニシエータ名を登録します。  
たとえば、関連付けされたサーバ上のファームウェアをアップグレードしたり、サービス プロファイルの説明またはラベルを変更できます。
- ステップ 7** 次のコマンドを実行して、IQN 変更が登録されたことを確認します。  
UCS-A# **show identity iqn | include iqn name**
-

## Cisco UCS PowerToolの取得と重複した IQN スクリプトの実行

Cisco UCS ドメインが iSCSI ブート用に設定されている場合は、Cisco UCS リリース 2.0(1) から Cisco UCS リリース 2.0(2) 以降にアップグレードする前に、複数のサービス プロファイルで使用される iSCSI vNIC がすべて一意のイニシエータ名を持っていることを確認する必要があります。

Cisco UCS PowerTool内で実行するスクリプトを使用して、iSCSI ブート用の Cisco UCS 設定に重複する IQN が含まれているかどうかを確認します。

### 手順

- ステップ 1** Cisco UCS PowerToolをダウンロードするには、次の手順を実行します。
- お使いの Web ブラウザで、Web サイト <http://developer.cisco.com/web/unifiedcomputing/microsoft> に移動します。
  - [Cisco UCS PowerTool (PowerShell Toolkit) Beta Download]領域まで下にスクロールします。
  - CiscoUcs-PowerTool-0.9.6.0.zip ファイルをダウンロードします。
  - ファイルを解凍し、プロンプトに従って Cisco UCS PowerToolをインストールします。  
Cisco UCS PowerToolは、任意の Windows コンピュータにインストールできます。Cisco UCS Managerへのアクセスに使用しているコンピュータにインストールする必要はありません。

- ステップ 2** Cisco UCS PowerToolを起動するには、コマンドラインに次のように入力します。  
**C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUcs sPS.ps1**

例 :

次に、Cisco UCS PowerToolを起動した場合の処理の例を示します。

```
C:\Program Files (x86)\Cisco\Cisco UCS
PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe
-NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

- ステップ 3** Cisco UCS PowerToolで、次の手順を実行します。
- 次のように、Cisco UCS Managerに接続します。  
**PS C:\>Connect-Ucs IP\_address**
  - 次の例のように、クレデンシャルを求めるプロンプトが表示された場合には、ユーザ名とパスワードを入力します。  
cmdlet Connect-Ucs at command pipeline position 1  
Supply values for the following parameters:  
Credential  
Cisco UCS PowerToolによって、ログイン後の画面に次のような内容が出力されます。

```
Cookie           : 1331303969/2af0afde-6627-415c-b85f-a7cae6233de3
Domains          :
LastUpdateTime   : 3/9/2012 6:20:42 AM
Name             : 209.165.201.15
NoSsl            : False
```

```

NumPendingConfigs      : 0
NumWatchers            : 0
Port                   : 443
Priv                   : {admin, read-only}
RefreshPeriod          : 600
SessionId              : web_49846_A
TransactionInProgress  : False
Ucs                    : ucs-4
Uri                    : https://209.165.201.15
UserName               : admin
VirtualIpv4Address     : 209.165.201.15
Version                : 2.0 (2i) 3.0 (1a)
WatchThreadStatus     : None

```

**ステップ 4** Cisco UCS PowerToolで次のスクリプトを実行して、iSCSI 起動設定を検証し、重複した IQN がな  
いかどうかを確認します。

```

PS C:\>Get-UcsServiceProfile -type instance | Get-UcsVnicIscsi | ? { $_.InitiatorName -ne "" } | select
Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $Obj = New-Object PSObject ; $Obj
| Add-Member NoteProperty Count $_.Count; $Obj | Add-Member NoteProperty InitiatorName $_.Name;
$Obj | Add-Member NoteProperty Dn ($_ | select -exp Group | % { $_.Dn } ); $Obj }

```

Cisco UCS PowerToolによって、次のように、画面に結果が表示されます。

```

Count InitiatorName          Dn
-----
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_1_6/is...
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_1/is...
2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_41/i...
4 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_7/is...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub1/ls-...
2 iqn.2012-01.cisco.com:s... {org-root/org-sub2/ls-...

```

**ステップ 5** (任意) .NET Framework 3.5 Service Pack 1 がインストールされている場合は、次のスクリプト  
を使用して GUI で結果を表示できます。

```

PS C:\>Get-UcsServiceProfile -type instance | Get-UcsVnicIscsi | ? { $_.InitiatorName -ne "" } | select
Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $Obj = New-Object PSObject ; $Obj
| Add-Member NoteProperty Count $_.Count; $Obj | Add-Member NoteProperty InitiatorName $_.Name;
$Obj | Add-Member NoteProperty Dn ($_ | select -exp Group | % { $_.Dn } ); $Obj } | ogv

```

**ステップ 6** 次のように、Cisco UCS Managerから切断します。

```

PS C:\>Disconnect-Ucs

```

## 次の作業

Cisco UCS ドメインの複数のサービス プロファイルで IQN が重複している場合は、Cisco UCS リ  
リース 2.1 以降にアップグレードする前に、Cisco UCS Manager で iSCSI vNIC を再設定し、それぞ  
れが一意的な IQN を持つようにします。

アップグレード前に、Cisco UCS ドメインのサービス プロファイル全体においてすべての iSCSI  
vNICが一意的であることを確認しなかった場合は、IQNの重複を警告するために、Cisco UCS Manager  
で iSCSI vNIC に関するエラーが発生します。また、サービス プロファイル内に重複した IQN 名

(同じ名前が両方の iSCSI vNIC で使用されている場合など) がないことを確認しなかった場合は、Cisco UCSによってサービス プロファイルが再設定され、1つの IQN を持つようになります。この障害をクリアして重複した IQN を再設定する方法の詳細については、『[Cisco UCS B-Series Troubleshooting Guide](#)』を参照してください。

## 更新中のサービス プロファイルテンプレートにバインドされているサービス プロファイルの IQN 発信側名の再設定

問題：Cisco UCS Release 2.0(1) から Release 2.0(2) にアップグレードした後、Cisco UCS Manager によって 1つ以上のサービス プロファイルで IQN 関連の障害が発生し、サービス プロファイル上の重複した IQN 発信側名を再設定できません。

考えられる原因：一意の IQN 発信側名を持っていないサービス プロファイルが、更新中のサービス プロファイルテンプレートに基づいています。

### 手順

- ステップ 1 Cisco UCS Manager CLIにログインします。
- ステップ 2 `UCS-A # scope org org-name`  
指定した組織の組織モードを開始します。ルート組織モードを開始するには、`org-name` に / と入力します。
- ステップ 3 `UCS-A /org # scope service-profile profile-name`  
サービス プロファイルのサービス プロファイル組織モードを開始します。
- ステップ 4 `UCS-A/org# scope vnic-iscsi iscsi_vnic1_name`  
サービス プロファイルに割り当てられている最初の iSCSI vNIC のモードを開始します。
- ステップ 5 `UCS-A /org/service-profile/vnic-iscsi* # set iscsi-identity {initiator-name initiator-name | initiator-pool-name iqn-pool-name}`  
iSCSI 発信側の名前または iSCSI 発信側名の提供元の IQN プール名を指定します。iSCSI 発信側名には最大 223 文字を使用できます。
- ステップ 6 `UCS-A /org/service-profile/vnic-iscsi* # exit`  
指定した iSCSI vNIC のモードを終了します。
- ステップ 7 `UCS-A/org# scope vnic-iscsi iscsi_vnic2_name`  
サービス プロファイルに割り当てられている 2 番目の iSCSI vNIC のモードを開始します。
- ステップ 8 `UCS-A /org/service-profile/vnic-iscsi* # set iscsi-identity {initiator-name initiator-name | initiator-pool-name iqn-pool-name}`  
iSCSI 発信側の名前または iSCSI 発信側名の提供元の IQN プール名を指定します。iSCSI 発信側名には最大 223 文字を使用できます。
- ステップ 9 `UCS-A /org/service-profile/vnic-iscsi # commit-buffer`  
トランザクションをシステムの設定にコミットします。

- ステップ 10** Cisco UCS Manager GUIで、更新中のサービス プロファイル テンプレートからサービス プロファイルをアンバインドします。

## Cisco UCS Central への Cisco UCS ドメインの登録に関する問題のトラブルシューティング

...

日時の不一致が、登録に関する最も一般的な問題です。

Cisco UCS Centralと Cisco UCS ドメイン の間の日時が同期していることを確認するには、次の事柄を行います。

- Cisco UCS Centralと Cisco UCS ドメイン で有効な NTP 設定が行われていることを確認します。
- Cisco UCS Centralが、Cisco UCS ドメイン の時間より遅れて実行していることを確認します。これにより、Cisco UCS Centralによって発行された証明書の開始日が将来にならないように確実に設定されます。
- 証明書が有効でない場合は、次のコマンドを使用して Cisco UCS Centralからデフォルトのキーリング証明書を再生成します。

```
UCSC # connect policy-mgr
UCSC (policy-mgr) # scope org
UCSC (policy-mgr) /org# scope device-profile
UCSC (policy-mgr) /org/device-profile # scope security
UCSC (policy-mgr) /org/device-profile/security # scope keyring default
UCSC (policy-mgr) /org/device-profile/security/keyring* # set regenerate yes
UCSC (policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

- 設定を修正した後に問題が発生した場合は、Cisco UCS Managerの共有秘密の更新が必要な可能性があります。

```
UCSM# scope system
UCSM /system # scope control-ep policy
UCSM /system/control-ep # set shared-secret
Shared Secret for Registration:
UCSM /system/control-ep* # commit-buffer
```



**重要** Cisco TAC に連絡する前に、次のことを確認してください。

- Cisco UCS Centralと、登録されている Cisco UCS ドメイン の日時が同期していること。
- Cisco UCS ドメインが一時停止になっていたり、表示状態になっていないこと。
- ドメインの登録ステータスが [Registered] になっていること。



## 第 4 章

# SAN の起動および SAN の接続のトラブルシューティング

この章は、次の項で構成されています。

- [SAN の接続のチェックリスト, 45 ページ](#)
- [SAN アレイの設定のチェックリスト, 46 ページ](#)
- [SAN の起動中の問題に関する推奨される解決策, 46 ページ](#)

## SAN の接続のチェックリスト

SANアレイへの接続の問題によって、SANの起動の問題が発生する可能性があります。その他の解決策で問題が解消されない場合は、次の内容を検討します。

- Cisco UCS Managerにファイバチャネルのアップリンク ポートが設定されていますか。
- Cisco UCS Managerの仮想ストレージエリア ネットワーク (VSAN) に割り当てられた番号がファイバチャネルスイッチに設定された番号と一致していますか。
- ファイバチャネルスイッチでNポートID仮想化 (NPIV) がイネーブルになっていますか。
- Cisco UCSのファブリック インターコネクトはファイバチャネルスイッチにログインしていますか。ファイバチャネルスイッチはファブリック インターコネクトを NPIV デバイスとして表示します。たとえば、マルチレイヤディレクタスイッチ (MDS) で **show fcns data** コマンドを使用して、Cisco UCS のファブリック インターコネクトがスイッチにログインしているかどうかを判別できます。
- Cisco UCS Managerの World Wide Name (WWN) は正しい形式ですか。
- 最新のファームウェアを使用するために、Cisco UCS ドメイン (サーバアダプタを含む) をアップグレードしましたか。
- ブートポリシーの SAN の起動および SAN のブート ターゲットの設定に、サーバと関連付けられたサービス プロファイルが含まれていることを確認しましたか。

- ブートポリシー内のvNICとvHBAは、サービスプロファイルに割り当てられているvNICとvHBAに一致していますか。
- アレイはアクティブまたはパッシブですか。
- アレイでアクティブなコントローラをブーティングしていますか。
- アレイは正しく設定されていますか。たとえば、[SANアレイの設定のチェックリスト](#)、(46ページ)の項目を確認しましたか。

## SAN アレイの設定のチェックリスト

SANアレイの間違った設定やその他の問題によってSANの起動の問題が発生する可能性があります。その他の解決策で問題が解消されない場合は、次のSANアレイの基本的な設定内容を確認します。

- ホストがアレイによって認識または登録されていますか。
- ホストが論理ユニット番号(LUN)にアクセスできるようにアレイが設定されていますか。たとえば、LUNのセキュリティまたはLUNのマスキングが設定されていますか。
- Cisco UCSドメインで割り当てられたワールドワイドポート名(WWPN)を使用してLUNの割り当てが正しく設定されていますか。ワールドワイドノード名(WWNN)を使用して割り当ておよび設定を行うと、問題が発生する可能性があります。
- Cisco UCSのブートポリシーに設定された番号と同じLUN番号に、アレイのバックアップ用LUNをマップしましたか。

## SANの起動中の問題に関する推奨される解決策

SANの起動の問題のトラブルシューティングに役立つ問題と推奨される解決策のリストを示します。SANアレイから起動しようとした際に障害が発生した場合は、次の解決策を導入する必要があります。

問題	推奨される解決策
SANの起動が断続的に失敗する。	サービスプロファイルに含まれている起動ポリシーのSAN起動ターゲットの設定を確認します。たとえば、SAN起動ターゲットに有効なWWPNが含まれていることを確認します。

問題	推奨される解決策
<p>サーバが SAN ではなくローカル ディスクから起動しようとする。</p>	<p>サービス プロファイルで設定したブート順序で、SAN が最初のブート デバイスになっていることを確認します。</p> <p>サービス プロファイルのブート順序が正しい場合は、サーバの実際のブート順序に、SAN が最初のブート デバイスとして組み込まれていることを確認します。</p> <p>実際のブート順序が正しくない場合は、サーバをリブートします。</p>
<p>ブート順序が正しいが、サーバが SAN から起動できない。</p>	<p>Windows および Linux の場合は、ブート LUN の番号が 0 になっていることを確認します。これにより、LUN が最初のディスクとしてマウントされ、そこからサーバが起動します。</p> <p>ESX の場合、複数の LUN が存在するときは、ブート LUN が最も小さい番号の LUN になっていることを確認します。</p>





## 第 5 章

# サーバのハードウェア問題のトラブルシューティング

この章は、次の項で構成されています。

- [診断ボタンと LED, 49 ページ](#)
- [DIMM メモリの問題, 50 ページ](#)
- [CPU の問題, 58 ページ](#)
- [ディスク ドライブと RAID に関する問題, 62 ページ](#)
- [アダプタの問題, 66 ページ](#)
- [電源の問題, 69 ページ](#)
- [Cisco TAC に連絡するときに必要なとなる情報, 70 ページ](#)

## 診断ボタンと LED

ブレードの起動時に、POST 診断によって CPU、DIMM、HDD、およびアダプタ カードがテストされます。エラー通知がある場合は、Cisco UCS Manager に送信されます。通知はシステム イベント ログ (SEL) または `show tech-support` コマンド出力で確認できます。エラーが検出されると、障害が発生したコンポーネントの横にある LED がオレンジに点灯します。実行時に、ブレード BIOS、コンポーネントドライバ、および OS によってハードウェアの障害がモニタされます。修正できないエラーまたは規定値を超える修正できるエラー (ホスト ECC エラーなど) が発生すると、ハードウェアのコンポーネントの診断 LED がオレンジに点灯します。

LED の状態は保存されます。シャーシからブレードを取り外すと、LED の値は最大 10 分間継続されます。マザーボードの LED 診断ボタンを押すと、コンポーネントに障害が発生していることを示す LED が最大 30 秒間点灯します。シャーシにブレードを取り付け直して起動すると、LED の障害値がリセットされます。

DIMM 挿入エラーが検出されると、ブレードの検出に失敗する場合があります。エラーはサーバの POST 情報でレポートされます。これらのエラーは、Cisco UCS Manager CLI または Cisco UCS

Manager GUI で確認できます。ブレードサーバに DIMM を取り付けるときは、特定のルールに従う必要があります。このルールはブレードサーバのモデルによって異なります。ルールについてはブレードサーバの各マニュアルを参照してください。

HDD ステータス LED は HDD の前面にあります。CPU、DIMM、またはアダプタカードで障害が発生すると、サーバヘルス LED は、軽微な障害ではオレンジに点灯し、重大な障害ではオレンジに点滅します。

## DIMM メモリの問題

### DIMM エラーのタイプ

Cisco UCS サーバは、修正可能および訂正不能な DIMM エラーを検出し、報告できます。

#### 修正可能な DIMM エラー

修正可能なエラーのある DIMM はディセーブルにならず、OS で利用できます。合計メモリと実効メモリは同じです（メモリのミラーリングが考慮されます）。これらの訂正可能なエラーは、所定のエラーしきい値を超えると、低下エラーとしてで報告されます。

#### 訂正不能な DIMM エラー

一般に、訂正不能なエラーは修復できず、アプリケーションやオペレーティングシステムは処理を続行できなくなる場合があります。訂正不能なエラーの DIMM は、DIMM のブラケットリストへの追加が有効な場合、または DIMM が BIOS POST 中に再起動に失敗し、OS でメモリを確認できない場合に無効になります。この場合、の **operState** では DIMM は動作不能となります。

DIMM メモリに問題が発生すると、サーバの起動に失敗したり、サーバがその能力以下で動作したりする場合があります。DIMM の問題が疑われる場合は、次の内容を検討します。

- システムでサポートされる DIMM は、シスコによりテストされ、シスコの基準を満たし、シスコにより販売される DIMM のみです。サードパーティ製の DIMM はサポートされません。このような DIMM が存在する場合、これらの DIMM をシスコが販売する DIMM に交換してから、問題のトラブルシューティングを続行してください。
- 不具合がある DIMM が、使用しているサーバのモデルでサポートされているかどうかを確認します。サーバのインストールガイドおよび技術仕様を参照して、サーバ、CPU、および DIMM を正しく組み合わせて使用しているかどうかを確認します。
- 不具合がある DIMM がスロットに確実に装着されていることを確認します。DIMM を取り外してからもう一度装着します。
- すべての Cisco サーバには必須または推奨の DIMM 取り付け順序があります。サーバのインストールガイドおよび技術仕様を参照して、所定のサーバタイプに対して DIMM を適切に追加していることを確認します。
- 交換用の DIMM の最大速度が以前に取り付けられていたメモリの速度より遅い場合、サーバ内のすべての DIMM の速度が低下するか、場合によっては完全に動作しなくなります。サー

バ内の DIMM はすべて同じタイプである必要があります。最適なパフォーマンスを得るために、サーバ内の DIMM はすべて同じタイプである必要があります。

- DIMM の数およびサイズは、サーバ内のすべての CPU について同一である必要があります。DIMM の構成に不一致があると、システムのパフォーマンスが低下する場合があります。

## メモリの用語および略語

表 6: メモリの用語および略語

略語	意味
DIMM	Dual In-line Memory Module (デュアル インライン メモリ モジュール)
DRAM	ダイナミック ランダム アクセス メモリ
ECC	Error Correction Mode (エラー訂正モード)
LVDIMM	Low Voltage DIMM (低電圧 DIMM)
MCA	Machine Check Architecture (マシーン チェック アーキテクチャ)
MEMBIST	Memory Built-In Self Test (メモリ組み込み自己テスト)
MRC	Memory Reference Code (メモリ リファレンス コード)
POST	Power On Self Test (電源投入時自己診断テスト)
SPD	Serial Presence Detect (シリアル プレゼンス検出)
DDR	Double Data Rate (ダブル データ レート)
CAS	Column Address Strobe (コラム アドレス ストローベ)
RAS	Row Address Strobe (行アドレス ストローベ)

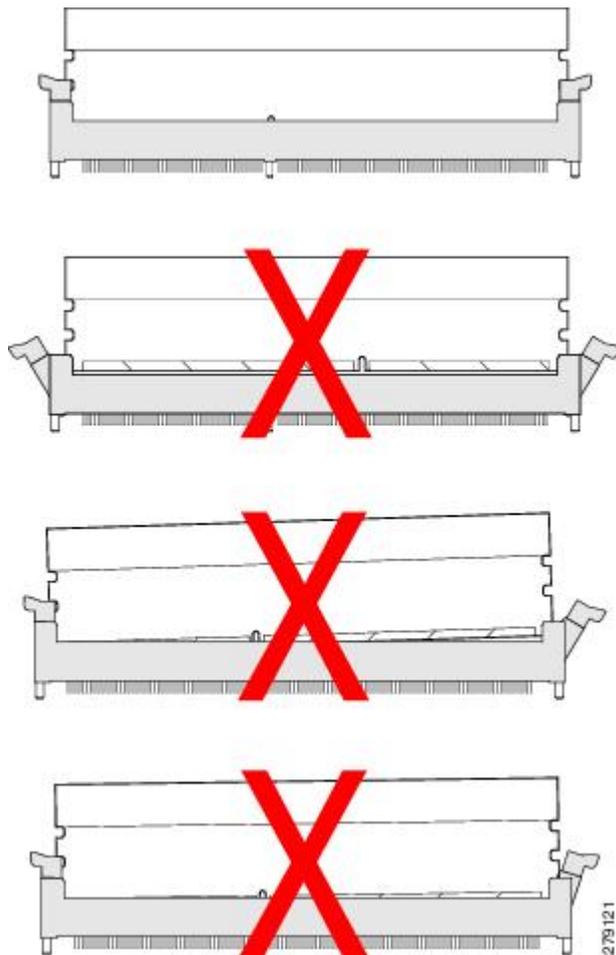
## DIMM のエラーのトラブルシューティング

### DIMM の正しい取り付け

DIMM が正しく取り付けられていることを確認します。

次の図に示す最初の例では、DIMM が正常に挿入され、固定されています。少量のほこりによっていずれかの接点が塞がれていない限り、この DIMM は正常に機能します。2 番目の例は、DIMM の向きがスロットのキーの向きと合っていない場合を示しています。DIMM はこの方向に挿入することはできないため、スロットに合うよう向きを変える必要があります。3 番目の例では、DIMM の左側は正しく装着され、ラッチがしっかりとかかっていますが、右側はスロットにわずかに接触しているだけで、ラッチが DIMM のノッチに固定されていません。4 番目の例では、左側はしっかりと挿入されて固定されていますが、右側は挿入が不完全で、ラッチがしっかりと固定されていません。

図 1 : DIMM の取り付け



## Cisco UCS Manager CLI を使用した場合の DIMM エラーのトラブルシューティング

Cisco UCS Manager CLI でメモリ情報を確認して、発生する可能性のある DIMM エラーを識別します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# <b>scope server</b> x/y	指定したサーバのサーバモードを開始します。
ステップ 2	UCS-A /chassis/server # <b>show memory detail</b>	サーバのメモリ情報が表示されます。
ステップ 3	UCS-A /chassis/server # <b>show memory-array detail</b>	メモリアレイの詳細情報が表示されません。
ステップ 4	UCS-A /chassis/server # <b>scope memory-array</b> x	指定したレイのレイモードを開始します。
ステップ 5	UCS-A /chassis/server/memory-array # <b>show stats</b>	メモリアレイの統計が表示されます。

次に、Cisco UCS Manager CLI を使用してメモリ情報を確認する例を示します。

```
UCS-A# scope server 1/5
UCS-A /chassis/server # show memory detail
Server 1/5:
  Array 1:
    CPU ID: 1
    Current Capacity (GB): 393216
    Error Correction: Undisc
    Max Capacity (GB): 393216
    Max Devices: 48
    Populated: 48

    DIMMS:

    ID 1:
      Location: DIMM_A0
      Presence: Equipped
      Overall Status: Operable
      Operability: Operable
      Visibility: Yes
      Product Name: 8GB DDR3-1333MHz RDIMM/PC3-10600/dual rank 2Gb DRAM
      PID: N01-M308GB2
      VID: V01
      Vendor: 0xCE00
      Vendor Description: Samsung Electronics, Inc.
      Vendor Part Number: M393B1K70BH1-CH9
      Vendor Serial (SN): 0x46185EC2
      HW Revision: 0
      Form Factor: Dimm
      Type: Other
      Capacity (MB): 8192
      Clock: 1067
      Latency: 0.900000
      Width: 64
    .
    .
    .
UCS-A /chassis/server # show memory-array detail

Memory Array:
  ID: 1
```

```

Current Capacity (GB): 384
Max Capacity (GB): 384
Populated: 48
Max Devices: 48
Error Correction: Undisc
Product Name:
PID:
VID:
Vendor:
Serial (SN):
HW Revision: 0
Threshold Status: N/A
Power State: N/A
Thermal Status: N/A
Voltage Status: N/A

UCS-A /chassis/server # scope memory-array 1
UCS-A /chassis/server/memory-array # show stats

Memory Array Env Stats:
Time Collected: 2011-09-27T20:15:52.858
Monitored Object: sys/chassis-1/blade-5/board/memarray-1/array-env-stats
Suspect: No
Input Current (A): 62.400002
Thresholded: 0

Memory Error Stats:
Time Collected: 2011-09-27T20:15:43.821
Monitored Object: sys/chassis-1/blade-5/board/memarray-1/mem-1/error-stats
Suspect: No
Address Parity Errors: 0
Mismatch Errors: 0
Ecc Multibit Errors: 0
Ecc Singlebit Errors: 0
Thresholded: 0

Time Collected: 2011-09-27T20:15:43.821
Monitored Object: sys/chassis-1/blade-5/board/memarray-1/mem-2/error-stats
Suspect: No
Address Parity Errors: 0
Mismatch Errors: 0
Ecc Multibit Errors: 0
Ecc Singlebit Errors: 0
Thresholded: 0

Time Collected: 2011-09-27T20:15:43.821
Monitored Object: sys/chassis-1/blade-5/board/memarray-1/mem-3/error-stats
Suspect: No
Address Parity Errors: 0
Mismatch Errors: 0
Ecc Multibit Errors: 0
Ecc Singlebit Errors: 0
Thresholded: 0
.
.
.
UCS-A /chassis/server/memory-array #

```

## Cisco UCS Manager GUIを使用した DIMM エラーのトラブルシューティング

Cisco UCS Manager GUIを使用して、発生している DIMM エラーの種類を特定できます。

## 手順

- ステップ 1** ナビゲーション ペインで、正しいシャーシを展開し、サーバを選択します。
- ステップ 2** [Inventory] タブで、[Memory] タブをクリックします。  
サーバのメモリ エラーが表示されます。
- ステップ 3** サーバの [Statistics] タブで、[Chart] タブをクリックします。  
関連するメモリ アレイを展開して、そのアレイに関する情報を表示できます。
- ステップ 4** OS 側から見たメモリの容量が、サーバに関連付けられたサービス プロファイルにリストされているメモリの容量と一致していることを確認します。  
たとえば、OS からすべてのメモリが見えているか、または一部のメモリしか見えていないかを確認します。可能な場合には、OS からメモリ診断ツールを実行します。

## DIMM の低下エラーのトラブルシューティング

修正可能なエラーのある DIMM はディセーブルにならず、OS で利用できます。合計メモリと実効メモリは同じです（メモリのミラーリングが考慮されます）。これらの修正可能なエラーは、Cisco UCS Manager において、低下としてレポートされます。

前述の情報に一致する修正可能なエラーがレポートされている場合、その問題は、ブレードサーバを装着し直したり、リセットしたりするのではなく、BMC をリセットすることによって修正できます。次の Cisco UCS Manager CLI コマンドを使用します。



(注) BMC のリセットは、ブレード上で実行されている OS に影響を及ぼしません。

## 手順

	コマンドまたはアクション	目的
ステップ 1	UCS1-A# <b>scope server x/y</b>	サーバコンフィギュレーションモードを開始します。
ステップ 2	UCS1-A /chassis/server # <b>scope bmc</b>	BMC のコンフィギュレーションモードを開始します。
ステップ 3	UCS1-A /chassis/server/bmc # <b>reset</b>	BMC サーバをハードリセットします。
ステップ 4	UCS1-A /chassis/server/bmc* # <b>commit-buffer</b>	トランザクションをシステムの設定にコミットします。

次の例では、BMC をリセットする方法を示します。

```
UCS1-A# scope server x/y
UCS1-A /chassis/server # scope bmc
UCS1-A /chassis/server/bmc # reset
UCS1-A /chassis/server/bmc* # commit-buffer
```

## 動作不能な DIMM エラーのトラブルシューティング

修正不可能なエラーが発生している DIMM はディセーブルになり、そのメモリはサーバの OS から認識されません。システムが稼働しているときに DIMM で障害が発生した場合、OS が予期せずクラッシュする可能性があります。修正不可能な DIMM エラーの場合、DIMM は動作不能として表示されます。これらのエラーは、ソフトウェアでは修正できません。不良 DIMM を特定して取り外すと、サーバをブートできます。たとえば、1 つ以上の DIMM が不良であるために、BIOS で POST を渡せなくなります。

### 手順

- 
- ステップ 1** 1 つの DIMM（できればテスト済みの良好な DIMM）または DIMM ペアを、1 つ目のプロセッサの 1 つ目の使用可能スロットに取り付けます（POST を成功させるための最小要件）。
  - ステップ 2** システムのブートを再試行します。
  - ステップ 3** それでもなお BIOS POST に失敗する場合は、ステップ 2 で別の DIMM を使用してステップ 1 ～ 3 を繰り返します。
  - ステップ 4** BIOS POST に成功し、続けてメモリを追加します。そのサーバモデルの装着規則に従います。一部のメモリ構成では BIOS POST を正しく渡せるが、他のメモリ構成では渡せないという場合は、その情報を使用して、問題の原因の特定に役立てます。
- 

## DIMM の問題に関する推奨される解決策

次の表に、DIMM の問題のトラブルシューティングを行うためのガイドラインおよび推奨される解決策を示します。

表 7: DIMM の問題

問題	推奨される解決策
DIMM が認識されない。	<p>DIMM が、アクティブ CPU をサポートするスロットに装着されていることを確認します。</p> <p>DIMM が Cisco 製品であることを確認します。サードパーティ製のメモリは Cisco UCS ではサポートされていません。</p>

問題	推奨される解決策
DIMM がスロットに合わない。	<p>DIMM がそのサーバモデルでサポートされていることを確認します。</p> <p>スロットに対して DIMM の向きが正しいことを確認します。DIMM とそのスロットにはキーが付いており、2 方向のうちのいずれか一方でのみ固定できます。</p>
DIMM が SEL、POST、または LED で不良としてレポートされるか、または Cisco IMC で動作不能としてレポートされる。	<p>DIMM がそのサーバモデルでサポートされていることを確認します。</p> <p>DIMM が、そのサーバモデルの装着規則に従ってスロットに装着されていることを確認します。</p> <p>DIMM がスロットにしっかりと装着されていることを確認します。アダプタが確実に接触するように装着し直し、POST を再度実行します。</p> <p>DIMM を、正常に機能することがわかっているスロットに取り付けて、DIMM に問題があることを確認します。</p> <p>正常に機能することがわかっている DIMM をスロットに取り付けて、DIMM のスロットが損傷していないことを確認します。</p> <p>BMC をリセットします。</p>
DIMM が GUI または CLI で低下としてレポートされるか、または予期した速度よりも遅い。	<p>BMC をリセットします。</p> <p>シャーシ内のサーバを装着し直します。</p>
DIMM が過熱としてレポートされる。	<p>DIMM がスロットにしっかりと装着されていることを確認します。アダプタが確実に接触するように装着し直し、POST を再度実行します。</p> <p>空気が設計どおりに流れるように、空の HDD ベイ、サーバスロット、電源装置ベイのすべてでブランキングカバーが使用されていることを確認します。</p> <p>空気が設計どおりに流れるように、サーバエアバッフルが取り付けられていることを確認します。</p> <p>空気が設計どおりに流れるように、必要な CPU エアブロックが取り付けられていることを確認します。</p>

## CPUの問題

すべての Cisco UCS サーバは、1～2基または1～4基の CPU をサポートしています。1基の CPU に問題が発生すると、サーバのブート失敗、非常に低速な動作、または重大なデータ損失やデータ破損の原因となり得ます。CPU の問題が疑われる場合は、次の内容を検討します。

- サーバ内のすべての CPU は、同じタイプである必要があります、同じ速度で動作し、同数および同じサイズの DIMM を使用している必要があります。
- 新しく CPU を交換またはアップグレードした場合は、その CPU がサーバに対して互換性があり、その CPU をサポートしている BIOS がインストールされていることを確認します。サポートされる Cisco モデルおよび製品 ID については、サーバのマニュアルを参照してください。シスコ提供の CPU のみを使用してください。BIOS バージョンの情報は、ソフトウェアリリースのリリース ノートで確認できます。
- CPU を交換する際は、ヒートシンクを確実に接着し、放熱を行ってください。CPU が加熱すると、Cisco UCS Manager で障害メッセージが表示されます。また、CPU の損傷を防ぐためにパフォーマンスが低下する場合があります。
- CPU の過熱が疑われる場合は、シャーシ内のすべてのサーバのバッフルおよびエアフローを確認します。隣接サーバのエアフロー問題により、別のサーバの CPU 冷却が不十分になる可能性があります。
- CPU 速度とメモリ速度は一致している必要があります。一致しない場合、サーバは2つの速度のうちの遅い方の速度で動作します。
- 1基の CPU に障害が発生した場合、残りのアクティブな CPU は、障害が発生した CPU に割り当てられているメモリにはアクセスできません。

## CLI を使用した CPU の問題のトラブルシューティング

Cisco UCS Manager CLI を使用して CPU 情報を確認できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# <b>scope server x/y</b>	サーバモードを開始します。
ステップ 2	UCS-A# <b>show cpu</b>	サーバの CPU 情報が表示されます。
ステップ 3	UCS-A# <b>show bios</b>	サーバの BIOS 情報が表示されます。
ステップ 4	UCS-A# <b>show cimc</b>	サーバの CIMC 情報が表示されます。

次に、サーバ 1/5 の CPU、BIOS、および CIMC に関する情報を表示する例を示します。

```
jane-A# scope server 1/5
UCS-A /chassis/server # show cpu

CPU:
  ID  Presence           Architecture      Socket Cores      Speed (GHz)
  ---  -
  1   Equipped           Xeon              CPU1   6                 3.333000
  2   Equipped           Xeon              CPU2   6                 3.333000
UCS-A /chassis/server # show bios

Bios Firmware:
Server Model      Vendor              Running-Vers Package-Vers
-----
1/5      N20-B6625-2 Cisco Systems, In S5500.1.3.1c.0.052020102031
UCS-A /chassis/server # show cimc

CIMC:
  PID              Serial (SN)        HW Revision
  ---
  N20-B6625-2     QCI140200D4       0
UCS-A /chassis/server #
```

## GUI を使用した CPU の問題のトラブルシューティング

Cisco UCS Manager GUI を使用して、発生している CPU エラーのタイプを判別できます。

### 手順

- 
- ステップ 1** ナビゲーション ペインで、正しいシャーシを展開し、サーバを選択します。
  - ステップ 2** [Inventory] ウィンドウの [CPU] タブをクリックします。  
そのサーバの CPU エラーが表示されます。
- 

## DIMM の問題に関する推奨される解決策

次の表に、DIMM の問題のトラブルシューティングを行うためのガイドラインおよび推奨される解決策を示します。

表 8: DIMM の問題

問題	推奨される解決策
DIMM が認識されない。	<p>DIMM が、アクティブ CPU をサポートするスロットに装着されていることを確認します。</p> <p>DIMM が Cisco 製品であることを確認します。サードパーティ製のメモリは Cisco UCS ではサポートされていません。</p>

問題	推奨される解決策
DIMM がスロットに合わない。	<p>DIMM がそのサーバ モデルでサポートされていることを確認します。</p> <p>スロットに対して DIMM の向きが正しいことを確認します。DIMM とそのスロットにはキーが付いており、2 方向のうちのいずれか一方でのみ固定できます。</p>
DIMM が SEL、POST、または LED で不良としてレポートされるか、または Cisco IMC で動作不能としてレポートされる。	<p>DIMM がそのサーバ モデルでサポートされていることを確認します。</p> <p>DIMM が、そのサーバ モデルの装着規則に従ってスロットに装着されていることを確認します。</p> <p>DIMM がスロットにしっかりと装着されていることを確認します。アダプタが確実に接触するように装着し直し、POST を再度実行します。</p> <p>DIMM を、正常に機能することがわかっているスロットに取り付けて、DIMM に問題があることを確認します。</p> <p>正常に機能することがわかっている DIMM をスロットに取り付けて、DIMM のスロットが損傷していないことを確認します。</p> <p>BMC をリセットします。</p>
DIMM が GUI または CLI で低下としてレポートされるか、または予期した速度よりも遅い。	<p>BMC をリセットします。</p> <p>シャーシ内のサーバを装着し直します。</p>
DIMM が過熱としてレポートされる。	<p>DIMM がスロットにしっかりと装着されていることを確認します。アダプタが確実に接触するように装着し直し、POST を再度実行します。</p> <p>空気が設計どおりに流れるように、空の HDD ベイ、サーバ スロット、電源装置ベイのすべてでブランキングカバーが使用されていることを確認します。</p> <p>空気が設計どおりに流れるように、サーバエアバップルが取り付けられていることを確認します。</p> <p>空気が設計どおりに流れるように、必要な CPU エアブロッカが取り付けられていることを確認します。</p>

## CPU CATERR\_Nの詳細

CATERR\_N 信号は、1 つ以上のプロセッサに致命的なメモリ エラーが発生したことを示します。これは、修正不可能なメモリ エラーが発生したことを示しているか、QPI リンクのエラーを表しています。CATERR\_N 信号は CATERR\_N センサーによって監視されます。信号が通常の動作を示している場合またはエラーが発生した場合に、システム イベント ログ (SEL) にイベントが生成されます。

CATERR\_N センサーは 2 ビットを使用し、通常の動作であるか障害が発生したかを示すセンサーの読み取り値を表します。

- ビット 0 は、Predictive Failure Deasserted を示します (センサーで障害は示されていません)。
- ビット 1 は、Predictive Failure Asserted を示します (障害が発生したことを示します)。

センサーがセンサーのスキャンマネージャにより初期化されると、通常、システム イベント ログ (SEL) に、障害がないことを示すビットが設定されたことを示すイベントが表示されます。これはビット 0 で、イベントは次のように表示されます。

```
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Deasserted | Asserted
```

これは、障害なしを示すビット、「Predictive Failure Deasserted」ビット (ビット 0) がアサートされたことを示します。これは肯定的な表示です。

システムに致命的なエラーが発生すると、センサー マネージャは CATERR\_N センサーを Bit0 設定から Bit1 設定に移行します。これは「Predictive Failure Deasserted」ビット (ビット 0) をアサート停止し、「Predictive Failure Asserted」ビット (ビット 1) をアサートします。この状況が発生すると、システム イベント ログ (SEL) に次のようにイベントが表示されます。

```
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Deasserted | Deasserted
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Asserted | Asserted
```

ビット 0 は「オフ」、ビット 1 は現在「オン」を示します。一部のログでは「オフ」 (アサート停止) のメッセージをフィルターで非表示にし、ログの 2 番目のイベントのみを表示することができます。センサーが通常状態に戻ると、次のように、fault ビット (ビット 1) がアサート停止され、no-fault ビット (ビット 0) がアサートされます。

```
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Asserted | Deasserted
| CIMC | Processor CATERR_N #0x8e | Predictive
Failure Deasserted | Asserted
```

ここでも、ログ ファイルの「オン」になっているビット (Predictive Failure Deasserted | Asserted) のイベントのみを表示することができます。この場合は、non-fault ビット (ビット 0) のアサートが表示されます。

## ディスクドライブと RAID に関する問題

ディスクドライブまたは RAID コントローラに問題が発生すると、サーバの起動に失敗したり、重大なデータ損失またはデータ破損が生じる可能性があります。ドライブの問題が疑われる場合は、次の内容を検討します。

- OS ツールを定期的を使用して、ドライブの問題（不良セクターなど）を検出および修正します。Cisco UCS Manager では、サーバの OS と同じように効果的にドライブの問題を修正することはできません。
- 各ディスクドライブに装備されているアクティビティ LED により、ドライブに対する未処理の I/O 処理が示されます。また、ドライブに障害が検出されると、ヘルス LED がオレンジに点灯します。ドライブの障害は、BIOS POST で検出できます。SEL メッセージには、これらの問題を見つけるのに役立つ重要な情報が含まれている場合があります。
- ディスクドライブは、システムシャーシからブレードを取り外さなくてもサーバから取り外すことができる唯一の主要コンポーネントです。
- ディスクドライブには、さまざまな容量のものがあります。ドライブに空き容量がない、またはドライブに OS で解決できない問題が存在するためにディスクドライブのパフォーマンスが低下した場合、ドライブの内容をバックアップして、より大容量のハードドライブまたは新しいハードドライブを取り付ける必要があります。

## RAID コントローラ

次の RAID コントローラ オプション付きの B シリーズサーバを発注または設定できます。

- Cisco UCS B200 および B250 サーバでは、LSI 1064E コントローラがマザーボードに搭載されています。このコントローラは、最大 2 台の SAS ドライブまたは SATA ドライブに対して RAID 0 および 1 をサポートします。このコントローラは、RAID を設定する前に Cisco UCS Manager でイネーブルにしておく必要があります。すべての RAID オプションを Cisco UCS Manager から設定できます。
- Cisco UCS B440 サーバには、LSI MegaRAID コントローラ（サーバによってモデルは異なる）が搭載されています。インストールされたライセンスキーに応じて、これらのコントローラは、最大 4 台の SAS ドライブまたは SATA ドライブに対する RAID 0、1、5、6、および 10 のサポートを提供します。
- Cisco B200 M3 サーバでは、LSI SAS 2004 RAID コントローラがマザーボードに搭載されています。このコントローラは、最大 2 台の SAS ドライブまたは SATA ドライブに対して RAID 0 および 1 をサポートします。



- (注) RAID クラスタをサーバ間で移動させる必要がある場合は、そのクラスタの新旧両方のサーバで同じ LSI コントローラが使用されている必要があります。たとえば、LSI 1064E を搭載したサーバから LSI MegaRAID を搭載したサーバへの移行はサポートされていません。

サーバで使用されているオプションについての記録がない場合は、Quiet Boot 機能をディセーブルにし、システムのブート時に表示されるメッセージから読み取ります。搭載されている RAID コントローラのモデルに関する情報は、冗長ブート機能の一部として表示されます。それらのコントローラの構成ユーティリティを起動するため、Ctrl を押した状態で H を押すように求めるプロンプトが表示されます。

## Quiet Boot のディセーブル化

Quiet Boot 機能がディセーブルになっている場合、ブートアップ時にコントローラの情報と、オプションの ROM ベースの LSI ユーティリティのプロンプトが表示されます。この機能をディセーブルにするには、次の手順を実行します。

### 手順

- ステップ 1 サーバをブートし、ブートプロセス中に F2 キー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 2 BIOS セットアップユーティリティを起動するために、プロンプトが表示されたら F2 を押します。
- ステップ 3 BIOS セットアップユーティリティのメインページで、[Quiet Boot] をディセーブルに設定します。これにより、ブートアップ時にシスコのロゴ画面ではなく、デフォルトではないメッセージ、プロンプト、および POST メッセージが表示されるようになります。
- ステップ 4 F10 を押して変更内容を保存し、ユーティリティを終了します。

## ROM ベースのコントローラ ユーティリティへのアクセス

ハードドライブの RAID 設定を変更するには、ホスト OS の上にインストールされたホストベースのユーティリティを使用します。また、サーバ上にインストールされている LSI オプションの ROM ベースのユーティリティを使用することもできます。

### 手順

- ステップ 1 Quiet モードをディセーブルにしてサーバを起動します。（「Quiet Boot のディセーブル化」の項 (P.6 ~ 11) を参照）。  
LSI オプションの ROM ベース ユーティリティを起動するためのキーの組み合わせを示すプロンプトと共に、コントローラに関する情報が表示されます。

**ステップ 2** 冗長ブートプロセス中に、目的のコントローラのプロンプトが表示されたら、次のいずれかの制御コマンドを入力します。

- プロンプトが表示されたら、Ctrl+H (LSI 1064E コントローラの場合)、または Ctrl+C (LSI MegaRAID コントローラの場合)、または Ctrl+M (Intel ICH10R の場合) と入力して、コントローラカードユーティリティを入力します。

## B200 M3 サーバ間での RAID クラスタの移動

別のサーバ上で作成された RAID クラスタを認識するようにサーバを設定できます。また、RAID クラスタ上のデータをサーバ間で移動させなければならなくなったときにも使用できます。

### はじめる前に

移動元と移動先の両方のサーバのサービスプロファイルが、まったく同じローカルディスク設定ポリシーを持ち、正常に起動できることを確認します。

### 手順

- 
- ステップ 1** 移動元サーバのオペレーティングシステムをそのオペレーティングシステム内からシャットダウンします。  
先に進む前に、OS が完全にシャットダウンし、自動で再起動していないことを確認します。
- ステップ 2** B200M3 サーバに現在適用されているサービスプロファイルの関連付けを解除します。
- ステップ 3** アレイ内のドライブを移動先のサーバに物理的に移します。  
サーバを変更する場合は、新しいサーバでも元のサーバと同じスロットにドライブを装着する必要があります。
- ステップ 4** 前に使用していたのと同じ論理ドライブ設定ポリシーが維持されるように、サービスプロファイルを新しいブレードに再関連付けします。
- ステップ 5** 各サーバの前面にある電源スイッチを押して、サーバの電源をオンにします。
- ステップ 6** 新しいサーバへの KVM 接続を開き、Storage Web BIOS Utility が起動するのを待ちます。
- ステップ 7** この Web BIOS ユーティリティのプロンプトに従って、RAID LUN を「移行」します。
- 

## RAID クラスタ内の障害の発生したドライブの交換

RAID ボリュームを作成する際は、業界の標準的なプラクティスに従って、容量が同じドライブを使用することを推奨します。容量の異なるドライブを使用すると、最も容量の小さいドライブで使用可能な容量が、RAID ボリュームを編成するすべてのドライブで使用されることとなります。

## はじめる前に

障害の発生した HDD または SSD を、同じサイズ、モデル、メーカーのドライブと交換します。稼働中のシステムで HDD を交換する前に、UCS Manager でサービス プロファイルを確認し、新しいハードウェア設定が、サービス プロファイルで設定されているパラメータの範囲内になることを確認します。

## 手順

- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
- ステップ 2 [Equipment] > [Chassis] > [Chassis Number] > [Servers] の順に展開します。
- ステップ 3 ローカルストレージ コンポーネントのステータスを表示するサーバをクリックします。
- 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 [Storage] サブタブをクリックして、RAID コントローラと FlexFlash コントローラのステータスを表示します。
- ステップ 6 下矢印をクリックして [Local Disk Configuration Policy]、[Actual Disk Configurations]、[Disks]、[Firmware] バーの順に展開し、追加のステータス情報を表示します。
- ステップ 7 障害の発生したドライブを物理的に交換します。  
必要に応じて、お使いのサーバモデルのサービスノートを参照します。通常、ほとんどのモデルで同様の手順になります。
- ステップ 8 サーバの前面にある電源スイッチを使用して、サーバを起動します。  
必要ならば、Quiet Boot 機能をディセーブルにし、再起動します（[Quiet Boot のディセーブル化](#)、[63 ページ](#)）を参照）。
- ステップ 9 LSI Configuration Utility バナーが表示されるのを待ちます。
- ステップ 10 LSI Configuration Utility を起動するために、Ctrl+C を押します。
- ステップ 11 [SAS Adapter List] 画面から、サーバ内で使用される SAS アダプタを選択します。  
使用されている RAID コントローラを確認するには、[RAID コントローラ](#)、[\(62 ページ\)](#) を参照してください。
- ステップ 12 [RAID Properties] を選択します。  
[View Array] 画面が表示されます。
- ステップ 13 [Manage Array] を選択します。  
[Manage Array] 画面が表示されます。
- ステップ 14 [Activate Array] を選択します。  
アクティベーションが完了すると、RAID ステータスが [Optimal] に変化します。
- ステップ 15 [Manage Array] 画面で、[Synchronize Array] を選択します。
- ステップ 16 ミラー同期化が完了するまで待ちます（表示されている経過表示バーを監視します）。  
(注) 同期化が完了するまでの時間は、RAID アレイ内のディスクのサイズによって異なります。

**ステップ 17** ミラー同期化が完了したら、Escキーを数回押して画面を順番に戻り（一度に1つ）、LSI Configuration Utility を終了します。

**ステップ 18** [reboot] オプションを選択して、変更を完了します。

## ローカルストレージの一貫性チェック操作が失敗する

問題：一貫性チェック操作が仮想ドライブで、次のエラーメッセージを表示して失敗します。

Adapter 0: Check Consistency is not possible on Virtual Drive at this time

原因：RAID 0 ボリュームでは、一貫性チェック操作はサポートされていません。

回避策：RAID 1 ボリュームとして構成された仮想ディスクで一貫性チェック操作を実行します。

## アダプタの問題

イーサネットアダプタまたは FCoE アダプタでの問題によって、サーバがネットワークに接続できず、Cisco UCS Manager から到達不能になる場合があります。すべてのアダプタはシスコ独自の設計であり、シスコ以外のアダプタはサポートされていません。アダプタの問題が疑われる場合は、次のことを検討してください。

- そのシスコのアダプタが正規品であるかどうかを確認します。
- 使用しているソフトウェアリリースで、そのアダプタタイプがサポートされているかどうかを確認します。Cisco UCS Manager のリリースノートにある内部的な依存性の表には、すべてのアダプタに対する、最小および推奨ソフトウェアバージョンが示されています。
- アダプタに適したファームウェアがサーバにロードされているかどうかを確認します。リリースバージョン 1.0(1) ~ 2.0 では、Cisco UCS Manager のバージョンとアダプタファームウェアのバージョンが一致する必要があります。Cisco UCS ソフトウェアとファームウェアをアップデートするには、インストール環境に適した [Cisco UCS のアップグレード](#) のドキュメントを参照してください。
- ソフトウェアバージョンのアップデートが完全でなく、ファームウェアバージョンが Cisco UCS Manager のバージョンに一致しなくなった場合は、インストール環境に適した [Cisco UCS Manager の設定ガイド](#) に従い、アダプタファームウェアをアップデートします。
- 2 枚の Cisco UCS M81KR 仮想インターフェイスカードを、ESX 4.0 を実行する Cisco UCS B250 拡張メモリブレードサーバに装着する場合、パッチ 5 (ESX4.0u1p5) 以降のリリースの ESX 4.0 にアップグレードする必要があります。
- あるアダプタタイプから別のアダプタタイプに移行する場合は、新しいアダプタタイプのドライバを入手できることを確認します。新しいアダプタタイプに合わせてサービスプロファイルをアップデートします。そのアダプタタイプに適したサービスを設定します。
- デュアルアダプタを使用する場合は、サポートされる組み合わせにいくつかの制限があることに注意してください。次の組み合わせがサポートされます。

サーバ	同一タイプのデュアルカード	混合タイプのデュアルカード
Cisco UCS B250	すべて (All)	M71KR-Q または -E + M81KR M72KR-Q または -E + M81KR
Cisco UCS B440	82598KR-CI を除くすべて	M72KR-Q または -E + M81KR

## GUI を使用したアダプタ エラーのトラブルシューティング

アダプタでネットワークリンクを1つも確立できなかった場合、サーバ正面のリンク LED がオフになります。1つ以上のリンクがアクティブになっている場合は、緑色になります。アダプタエラーは、マザーボード上の LED で報告されます。「診断ボタンと LED」 (P.6-1) を参照してください。

次の手順を使用して、発生しているアダプタ エラーの種類を特定します。

### 手順

- 
- ステップ 1** ナビゲーション ペインでシャーシを展開し、目的のサーバを選択します。
- ステップ 2** [Inventory] ウィンドウで、[Interface Cards] タブを選択します。  
そのサーバのアダプタ エラーが画面に表示されます。
- 

## CLI を使用したアダプタ エラーのトラブルシューティング

アダプタでネットワークリンクを1つも確立できなかった場合、サーバ正面のリンク LED がオフになります。1つ以上のリンクがアクティブになっている場合は、緑色になります。アダプタエラーは、マザーボード上の LED で報告されます。

次の手順を使用して、CLI でアダプタの状態情報を確認できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# <b>scope serverchassis-id/server-id</b>	
ステップ 2	UCS-A /chassis/server # <b>show adapter [detail]</b>	

次に、シャーシ ID 1、サーバ ID 5 のアダプタの詳細を表示する例を示します。

```
UCS-A# scope server 1/5
UCS-A /chassis/server # show adapter detail

Adapter:
  Id: 2
  Product Name: Cisco UCS 82598KR-CI
  PID: N20-AI0002
  VID: V01
  Vendor: Cisco Systems Inc
  Serial: QCI132300GG
  Revision: 0
  Mfg Date: 2009-06-13T00:00:00.000
  Slot: N/A
  Overall Status: Operable
  Conn Path: A,B
  Conn Status: Unknown
  Managing Instance: B
  Product Description: PCI Express Dual Port 10 Gigabit Ethernet Server Adapter
UCS-A /chassis/server #
```

## アダプタの問題に関する推奨される解決策

次の表に、アダプタの問題のトラブルシューティングに役立つガイドラインおよび推奨される解決策を示します。

表 9: アダプタの問題

問題	推奨される解決策
アダプタが SEL、POST、または LED で不良としてレポートされるか、または Cisco UCS Manager で動作不能としてレポートされる。	<p>アダプタがそのサーバモデルでサポートされていることを確認します。</p> <p>使用中の Cisco UCS Manager のバージョンで動作するのに必要なファームウェアバージョンが、アダプタに組み込まれていることを確認します。</p> <p>アダプタが、マザーボードのスロットおよびミッドプレーンの接点にしっかりと装着されていることを確認します。アダプタが確実に接触するように装着し直し、サーバを再度取り付けてから、POST を再度実行します。</p> <p>アダプタを、正常に機能することがわかっており、同じ種類のアダプタを使用しているサーバに取り付けて、アダプタに問題があることを確認します。</p>
アダプタが GUI または CLI で低下としてレポートされる。	シャーシ内のブレードサーバを装着し直します。

問題	推奨される解決策
アダプタが過熱としてレポートされる。	<p>アダプタがスロットにしっかりと装着されていることを確認します。アダプタが確実に接触するように装着し直し、POST を再度実行します。</p> <p>空気が設計どおりに流れるように、空のHDDベイ、サーバスロット、電源装置ベイのすべてでブランキングカバーが使用されていることを確認します。</p> <p>空気が設計どおりに流れるように、サーバエアバフフルが取り付けられていることを確認します。</p>

## 電源の問題

サーバのオンボード電源システムの問題が原因で、警告なしでサーバがシャットダウンしたり、電源オンに失敗したり、検出プロセスに失敗したりする場合があります。

### Cisco UCS B440 サーバの FET 障害のトラブルシューティング

Cisco UCS B440 サーバの電源部における電界効果トランジスタ (FET) の障害によって、サーバのシャットダウン、電源投入の障害、または検出プロセスの障害が発生する場合があります。サーバによって障害が検出された場合は、前面パネルの電源ボタンを使用しても、サーバの電源をオンにできません。

FET 障害が発生しているかどうかを判断するには、次の手順を実行します。

#### 手順

- 
- ステップ 1** 「障害」の項 (P.1 ~ 2) の手順を使用し、レポートされた障害で障害コード F0806、「Compute Board Power Fail.」の有無を確認します。この障害によって、サーバの全体的なステータスが [Inoperable] になります。
- ステップ 2** システム イベント ログ (SEL) で、この例に示すタイプの電源システム障害の有無を確認します。
- ```
58f | 06/28/2011 22:00:19 | BMC | Power supply POWER_SYS_FLT #0xdb | Predictive Failure deasserted | Asserted
```
- ステップ 3** ファブリック インターコネクットの CLI から、障害が発生したサーバの CIMC にアクセスし、**connect cimc chassis/server** と入力することによって、障害センサーを表示します。

例：

次の例では、シャーシ 1、サーバ 5 の CIMC に接続する方法を示します。

```
Fabric Interconnect-A# connect cimc 1/5
```

```

Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^]'.
CIMC Debug Firmware Utility Shell
[ help ]# sensors fault
HDD0_INFO | 0x0 | discrete | 0x2181| na | na | na | na | na | na
HDD1_INFO | 0x0 | discrete | 0x2181| na | na | na | na | na | na
.
.[lines removed for readability]
.
LED_RTC_BATT_FLT | 0x0 | discrete | 0x2180| na | na | na | na | na | na
POWER_SYS_FLT | 0x0 | discrete | 0x0280| na | na | na | na | na | na
[ sensors fault]#

```

POWER\_SYS\_FLT センサーで 0x0280 が示されている場合は、FET 障害があります。通常動作においては、このセンサーでは 0x0180 が示されます。

**ステップ 4** FET 障害が発生したと判断した場合は、次の手順を実行します。

a) Cisco UCS Manager CLI で、次のコマンドの出力を収集します。

- **show tech-support ucsm detail**
- **show tech-support chassis *chassis-id* all detail**

b) Cisco Technical Assistance Center (TAC) に問い合わせて障害があることを確認してください。

c) Cisco UCS Manager で Recover Server アクションを使用して、交換するサーバを設置してください。

## Cisco TAC に連絡するときに必要なとなる情報

問題を切り分けてコンポーネントを特定できない場合は、次の質問について検討してください。これらの質問は、Cisco Technical Assistance Center (TAC) に連絡するとき役に立ちます。

- 問題が発生する前は、ブレードは動作していましたか。サービスプロファイルが関連付けられた状態でブレードが実行中に問題が発生しましたか。
- これは新しく挿入したブレードですか。
- このブレードは、現地で組み立てられたものですか。それともシスコから組み立てられた状態で到着したものですか。
- メモリを装着し直しましたか。
- ブレードの電源は切れていましたか、またはブレードをスロット間で移動しましたか。
- Cisco UCS Manager を最近アップグレードしましたか。アップグレードした場合は、BIOS もアップグレードしましたか。

Cisco UCS の問題に関して Cisco TAC に連絡するときは、Cisco UCS Manager および問題が発生しているシャーシから tech-support 出力を取得することが重要です。詳細については、[テクニカルサポート ファイル](#)、[\(15 ページ\)](#) を参照してください。





## 第 6 章

# ファームウェアのトラブルシューティング

- [アップグレード中のファブリック インターコネクットの回復](#), 73 ページ
- [ファームウェア アップグレード中の IO モジュールの回復](#), 80 ページ

## アップグレード中のファブリック インターコネクットの回復

1つまたは両方のファブリック インターコネクットがフェールオーバーまたはファームウェア アップグレード中に失敗した場合は、次のいずれかのアプローチを使用してこれらのファブリック インターコネクットを回復できます。

- ファブリック インターコネクットに稼働中のイメージがない場合にファブリック インターコネクットを回復する。
- ファブリック インターコネクットに稼働中のイメージがある場合にファブリック インターコネクットを回復する。
- アップグレードまたはフェールオーバー中に無応答のファブリック インターコネクットを回復する。

## ファブリック インターコネクットまたはブートフラッシュに稼働中のイメージがない場合のファブリック インターコネクットの回復

両方または一方のファブリック インターコネクットがファームウェア アップグレード中にダウンし、レポートされ、ローダープロンプトで停止した場合、かつファブリック インターコネクットに稼働中のイメージがない場合は、次の手順を実行できます。

ファブリック インターコネクトまたはブートフラッシュに稼働中のイメージがない場合のファブリック  
インターコネクトの回復

## 手順

**ステップ 1** スイッチをリブートし、コンソールで **Ctrl+L** キーを押して、起動時にローダー プロンプトを表示させます。

(注) ローダー プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

例 :

```
loader>
```

**ステップ 2** TFTP を通じてキックスタート イメージを受信するようにインターフェイスを設定します。

a) loader> プロンプトでシステムのローカル IP アドレスとサブネット マスクを入力して、**Enter** キーを押します。

例 :

```
loader> set ip 10.104.105.136 255.255.255.0
```

b) デフォルト ゲートウェイの IP アドレスを指定します。

例 :

```
loader> set gw 10.104.105.1
```

c) 必要なサーバからキックスタート イメージ ファイルを起動します。

例 :

```
loader> boot  
tftp://10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin  
switch(boot)#
```

(注) ブートフラッシュにキックスタート イメージがある場合は、このステップは不要です。

**ステップ 3** switch(boot)# プロンプトで **init system** コマンドを入力します。  
このコマンドによって、ファブリック インターコネクトが再フォーマットされます。

例 :

```
switch(boot)# init system
```

**ステップ 4** 管理インターフェイスを設定します。

a) 設定モードに変更し、**mgmt0** インターフェイスの IP アドレスを設定します。

例 :

```
switch(boot)# config t  
switch(boot) (config)# interface mgmt0
```

b) **ip address** コマンドを入力して、システムのローカル IP アドレスとサブネット マスクを設定します。

例 :

```
switch(boot) (config-if) # ip address 10.104.105.136 255.255.255.0
```

- c) **no shutdown** コマンドを入力して、システムで mgmt0 インターフェイスを有効にします。

例 :

```
switch(boot) (config-if) # no shutdown
```

- d) **ip default-gateway** コマンドを入力して、デフォルトゲートウェイの IP アドレスを設定します。

例 :

```
switch(boot) (config-if) # exit  
switch(boot) (config) # ip default-gateway 10.104.105.1
```

- e) **exit** を入力して、EXEC モードを終了します。

例 :

```
switch(boot) (config) # exit
```

- ステップ 5** キックスタート、システム、および Cisco UCS Manager 管理イメージを TFTP サーバからブートフラッシュにコピーします。

例 :

```
switch(boot) # copy  
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin  
bootflash://  
switch(boot) # copy  
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin  
bootflash://  
switch(boot) # copy  
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-manager-k9.3.0.2d56.bin bootflash://
```

- ステップ 6** (任意) ブートフラッシュに installables および installables/switch ディレクトリを個別に作成します。

例 :

```
switch(boot) # mkdir bootflash:installables  
switch(boot) # mkdir bootflash:installables/switch
```

- ステップ 7** キックスタート、システム、および Cisco UCS Manager イメージを installables/switch ディレクトリにコピーします。

例 :

```
switch(boot) # copy ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin bootflash:installables/switch/  
switch(boot) # copy ucs-6300-k9-system.5.0.2.N1.3.02d56.bin bootflash:installables/switch/  
switch(boot) # copy ucs-manager-k9.3.02d56.bin bootflash:installables/switch/
```

- ステップ 8** 管理イメージが nova-sim-mgmt-nsg.0.1.0.001.bin にリンクされていることを確認します。  
nova-sim-mgmt-nsg.0.1.0.001.bin は予約済みシステム イメージが使用し、管理イメージを Cisco UCS Manager 準拠にするための名前です。

ファブリック インターコネクトまたはブートフラッシュに稼働中のイメージがない場合のファブリック  
インターコネクトの回復

例 :

```
switch(boot)# copy bootflash:installables/switch/ucs-manager-k9.3.02d56.bin
nuova-sim-mgmt-nsg.0.1.0.001.bin
```

**ステップ 9** スイッチをリロードします。

例 :

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
```

**ステップ 10** キックスタート イメージから起動します。

例 :

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
loader> boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

**ステップ 11** システム イメージをロードします。

システム イメージが完全にロードされたら、[Basic System Configuration Dialog]ウィザードが表示  
されます。このウィザードを使用してファブリック インターコネクトを設定します。

例 :

```
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
Uncompressing system image: bootflash:/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
```

...

```
---- Basic System Configuration Dialog ----
```

```
This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the Fabric interconnect and its clustering mode is performed through these steps.
```

...

```
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.
```

```
Configuration file - Ok
```

**ステップ 12** Cisco UCS Managerにログインし、ファームウェアをダウンロードします。

例 :

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<infra bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<b-series bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<c-series bundle name>
Password:
UCS-A /firmware # show download-task
```

```

Download task:
File Name Protocol Server          Userid          State
-----
ucs-k9-bundle-b-series.3.0.2.B.bin
Scp          10.104.105.22  abcdefgh       Downloading
ucs-k9-bundle-c-series.3.0.2.C.bin
Scp          10.104.105.22  abcdefgh       Downloading
ucs-k9-bundle-infra.3.0.2.A.bin
Scp          10.104.105.22  abcdefgh       Downloading
UCS-A /firmware #
    
```

**ステップ 13** ファームウェアのダウンロードが完了したら、ファブリックインターコネク  
トファームウェアと Cisco UCS Managerファームウェアをアクティブ化します。  
このステップにより、Cisco UCS Managerおよびファブリック インターコネク  
トが目的のバージョンに更新されてリブートされます。

例 :

```

UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect* # activate firmware kernel-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
UCS-A /fabric-interconnect* # activate firmware system-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect # exit
    
```

```

UCS-A# scope system
UCS-A /system # show image
    
```

```

Name                                     Type          Version
-----
ucs-manager-k9.3.02d56.bin              System        3.0(2d)
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system #
    
```

## ブートフラッシュに稼働中のイメージがある場合のアップグレード中 のファブリック インターコネク トの回復

次の手順は、両方または一方のファブリック インターコネク  
トがファームウェアアップグレード  
中にダウンし、リブートされ、ローダー プロンプトで停止した場合に実行できます。

### はじめる前に

次の手順を実行するには、ブートフラッシュに稼働中のイメージが存在する必要があります。

### 手順

**ステップ 1** スイッチをリブートし、コンソールで Ctrl+L キーを押して、起動時にローダー プロンプトを表示  
させます。

(注) ローダー プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

例：  
loader>

**ステップ 2** **dir** コマンドを実行します。  
ブートフラッシュ内の使用可能なカーネル、システム、および Cisco UCS Manager イメージのリストが表示されます。

例：  
loader> **dir**  
nuova-sim-mgmt-nsg.0.1.0.001.bin  
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin  
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin  
ucs-manager-k9.3.02d56.bin

**ステップ 3** ブートフラッシュからカーネル ファームウェア バージョンを起動します。  
(注) ここで使用できるカーネル イメージが、起動できる稼動イメージです。

例：  
loader> **boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin**

**ステップ 4** 管理イメージが `nuova-sim-mgmt-nsg.0.1.0.001.bin` にリンクされていることを確認します。  
`nuova-sim-mgmt-nsg.0.1.0.001.bin` は予約済みシステム イメージが使用し、管理イメージを Cisco UCS Manager 準拠にするための名前です。

例：  
switch (boot) # **copy ucs-manager-k9.1.4.1k.bin nuova-sim-mgmt-nsg.0.1.0.001.bin**

**ステップ 5** システム イメージをロードします。

例：  
switch (boot) # **load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin**

**ステップ 6** Cisco UCS Manager にログインし、ファブリック インターコネクと Cisco UCS Manager ソフトウェアを必要なバージョンにアップデートします。

---

## アップグレードまたはフェールオーバー中の無応答のファブリック インターコネクットの回復

アップグレードまたはフェールオーバー中は、新たなリスクを避けるため、次のタスクを実行しないでください。

- Pmon の停止と開始
- FI のリブート（電源の再投入または CLI）
- HA フェールオーバー

## 手順

- ステップ 1** CSCup70756 で説明されているように `httpd_cimc.sh` プロセスが失われた場合、KVM にアクセスできなくなります。フェールオーバーを続けるか、Cisco テクニカル サポートに連絡します。
- ステップ 2** プライマリ側で KVM にアクセスできなくなった場合は、フェールオーバーを続行して問題を解決します。
- ステップ 3** セカンダリ側で KVM が必要であるか、またはダウンしている場合は、デバッグ プラグインを使用してそのサービスのみを開始します。デバッグ イメージを実行するには、TAC にお問い合わせください。
- ステップ 4** CSCuo50049 で説明されている `/dev/null` 問題が発生した場合は、必要に応じて両方のステップでデバッグ プラグインを使用して権限を 666 に修正します。Cisco テクニカル サポートに連絡してデバッグ コマンドを実行します。
- ステップ 5** CSCup70756 および CSCuo50049 の両方が発生した場合、VIP が失われる可能性があります。VIP が失われた場合は、次の手順を実行します。
- 1 GUI からプライマリ物理アドレスにアクセスし、GUI を使用して、回復するすべての IO モジュールのバックプレーン ポートを確認します。
  - 2 GUI がダウンしている場合、NXOS `show fex detail` コマンドを使用して、IO モジュールのバックプレーン ポートを確認します。
  - 3 回避策を実行し、両方のファブリック インターコネクットのクラスタの状態が UP になっていることを確認します。
  - 4 両方のファブリック インターコネクットのクラスタの状態が UP になっている場合は、SSH CLI 構文を使用してプライマリ ファブリック インターコネクットのリブートを再確認して、アップグレードを続行します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

# ファームウェア アップグレード中の IO モジュールの回復

ファームウェアのアップグレード中に IO モジュールを回復するには、ピア IO モジュールからその IO モジュールをリセットします。リセット後に、その IO モジュールはファブリック インターコネクトから設定を取得できます。

## ピア I/O モジュールからの I/O モジュールのリセット

I/O モジュールのアップグレードが失敗したり、メモリ リークにより Cisco UCS Manager から I/O モジュールにアクセスできなくなったりする場合があります。このような場合でも、アクセスできない I/O モジュールをそのピア I/O モジュールからリポートできます。

I/O モジュールをリセットすると、I/O モジュールが工場出荷時の設定に復元され、すべてのキャッシュ ファイルと一時ファイルが削除されますが、サイズ制限付きの OBFL ファイルは保持されません。

### 手順

- 
- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
  - ステップ 2 [Equipment] > [Chassis] > [Chassis Number] > [IO Modules] の順に展開します。
  - ステップ 3 リセットする I/O モジュールのピア I/O モジュールを選択します。
  - 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、[Reset Peer IO Module] をクリックします。
-



## 第 7 章

# Cisco IPMI Extensions で発生する問題のトラブルシューティング

この章は、次の項で構成されています。

- [はじめに, 81 ページ](#)
- [シスコ ESR 詳細, 82 ページ](#)
- [高レベルの一般的なアルゴリズム, 82 ページ](#)
- [バイトの順序付け, 83 ページ](#)
- [Cisco ESR IPMI コマンドの定義, 83 ページ](#)
- [レコード形式, 92 ページ](#)
- [IPMI センサー情報に基づいた推奨される解決策, 97 ページ](#)
- [ダウングレード後の IPMI 設定で発生する問題の防止, 110 ページ](#)

## はじめに

この章は、IPMI 2.0 の仕様を理解していることを前提としています。

デバッグを容易にするため、既存および将来の Cisco サーバは、現在の IPMI 仕様で扱える 255 個よりも多くのセンサーを提供できます。したがって、特定の B シリーズおよび C シリーズの Cisco サーバは、IPMI 2.0 仕様のセンサーとセンサー関連機能を拡張します。この章では、IPMI ツールユーザが拡張を効率的に使用できるよう、これらの拡張について説明します。

センサーの数が 255 個以下であるセンサーについては、シスコは IPMI の仕様に準拠しています。センサーの数が 256 個以上であるセンサー（Extended Sensor Range（ESR））については、シスコはシスコ OEM IPMI コマンドとして同等のセンサー関連 IPMI コマンドを追加しています。Extended Sensor Range のセンサーは Cisco Extended センサー（CES）と呼ばれます。また、IPMI 仕様では、すべてのセンサーに付けられた番号が連続している必要はありません。したがって、Cisco サーバ

と CIMC のソフトウェアバージョンによっては、IPMI の範囲に空きがある場合でも、IPMI の範囲ではなく ESR 内にセンサーがある可能性があります。

オープンソースプログラムの IPMITool および OpenIPMI は、シスコの ESR 機能を統合するようには変更されません。ただし、これらのツールで、raw IPMI コマンドを発行することができるため、ESR 機能処理するラッパーを書き込むことができます。

## シスコ ESR 詳細

SDR (センサーデータレコード) および SEL 形式は両方とも、既存の IPMI の標準 8 ビットサイズを超えて、32 ビットセンサー ID に対応できるよう拡大されています。Cisco Extended Sensor Range - Sensor Data Record (ESR-SDR) は、より多くのセンサー、大きいレコードサイズ、長いストリング長を扱うことが可能です。ESR - センサー イベント ログが拡張され、新しい名前のセンサーの読み取り値を取得する機能がサポートされます。

新しい形式が導入されても、核となる CES と関連の SDR および SEL の操作は標準 IPMI 仕様で定義された動作と同じです。つまり、IPMI センサーで予期される動作は Cisco Extended センサーで予期される動作と同じです。

Cisco Extended SEL (ESR-SEL) リポジトリを追加する操作は、通常と若干異なります。サーバ全体のデバッグの簡素化するため、このリポジトリには ESR-SEL 形式に再フォーマットされた標準 IPMI SEL イベントと Cisco Extended センサーの SEL イベントの両方が含まれています。つまり、ESR-SEL はスーパーセットと見なすことができます。

現在の UCS サーバでは、IPMI SEL リポジトリの現在の使用状況をパーセンテージで示し、リポジトリが特定の充足率に達した場合に SEL イベントを生成するためにセンサーがあります。このセンサーは、「SEL\_FULLNESS」という名前が付けられます。ESR-SEL は異なるリポジトリであるため、同等のセンサーが提供されます。従来の「SEL\_FULLNESS」センサーは常に、標準 IPMI リポジトリを参照し、新しい「CISCO\_SEL\_FULLNESS」センサーは ESR-SEL リポジトリを参照します。センサーの名前はリポジトリを区別するキーとなります。その結果、「Clear-SEL-Event」SEL レコードと「SEL-Full-Event」SEL レコードも、SEL 使用率センサーの名前を継承します。これらのセンサーの名前を確認することによって、使用率の現在のパーセンテージ、SEL が最後にクリアされた時刻、SEL がいっぱいになった時刻、これらのイベントが参照しているリポジトリがわかります。

UCS Manager SEL のバックアップ機能を有効にすると、SEL 使用率センサーに基づいてサーバから SEL イベントがバックアップされます。この実装前は、SEL\_FULLNESS センサーのみに基づいていました。ESR 機能が搭載されると、UCS Manager は両方の SEL 使用率センサーを確認し、どちらかが特定の使用レベルに達した場合にイベントをバックアップします。UCS Manager はバックアップ後に両方のリポジトリをクリアします。

## 高レベルの一般的なアルゴリズム

シスコの Extended Sensor の機能を確認および使用するためのアルゴリズムが提供されています。このアルゴリズムは、シスコおよびシスコ以外のすべての IPMI を実装するプラットフォームに安全に適用できます。

- 1 サーバへの **GET Device ID** IPMI コマンドを発行します。製造者 ID が 0x168B の場合、Cisco B シリーズまたは C シリーズサーバです。次の手順に進みます。製造者 ID が 0x168B でない場合、このアルゴリズムを続行しないでください。想定外の動作が発生する可能性があります。
- 2 **Cisco Get ESR Capabilities** IPMI コマンドを発行します。最初の 6 バイトが定義通りで、すべてのバイトが返ることを確認します。エラーコードが返された場合、最初の 6 バイトが不一致であるか、すべてのバイトが返されていません。Cisco B シリーズまたは C シリーズサーバは ESR をサポートしていません。この手順を続行しないでください。
- 3 残りのバイトを、**Cisco Get ESR Capabilities** コマンドで確認します。ESR 対応フラグが設定されていない場合、この手順を続行しないでください。
- 4 この時点で、Cisco B シリーズまたは C シリーズサーバは、ESR をサポートすることが確認されました。Cisco ESR IPMI コマンドのいずれかを発行できます。

ESR 機能をサポートしていることが確認された後に、センサーの読み取り値の取得を行うため、以降の手順を実行することを推奨します。

- 1 IPMI の仕様ごとに、すべての標準 IPMI SDR を取得します。
- 2 **Get ESR-SDR** IPMI コマンドを発行して、すべての Cisco ESR センサーのデータ レコード (ESR-SDR) を取得します。
- 3 本ドキュメントの後半で説明するように、標準 IPMI **Get Sensor Reading** コマンドを発行するか、**Get CES Reading** IPMI コマンドを発行して、目的のセンサー読み取り値を取得します。**Get CES Reading** コマンドは、IPMI センサーを取得するためにも発行できます。
- 4 対応する SDR を使用して、生の読み取り値を人間が読むことのできる形式に復号化します。

## バイトの順序付け

IPMI のマルチバイト フィールドはすべて、リトルエンディアンです。要求または応答フィールドの最下位インデックスに最下位バイトが置かれます。これは IPMI で一貫しています。たとえば、*earth-age* という要求フィールドがあり、インデックス 5 から 8 までの 4 バイトの長さだとします。地球の年齢が約 10 億年である場合、16 進表記では 0x3B9ACA00 です。この場合、要求データのインデックス 5 が 0 になり、インデックス 6 は 0xCA、インデックス 7 は 0x9A、インデックス 8 は 0x3B です。

## Cisco ESR IPMI コマンドの定義

### Get ESR Capabilities コマンド

|            |                      |
|------------|----------------------|
| コマンド名 :    | Get ESR Capabilities |
| ネットワーク機能 : | NF_STO               |
| コマンド番号 :   | 0xF5                 |
|            |                      |

| 要求バイト   | フィールド名                  | 説明                                                                                                                                                                                                          |
|---------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| なし      |                         |                                                                                                                                                                                                             |
| 応答バイト   | フィールド名                  | 説明                                                                                                                                                                                                          |
| [1]     | Completion Code         |                                                                                                                                                                                                             |
| [2]     | ID0                     | 0x43: ASCII 'C'                                                                                                                                                                                             |
| [3]     | ID1                     | 0x49: ASCII 'I'                                                                                                                                                                                             |
| [4]     | ID2                     | 0x53: ASCII 'S'                                                                                                                                                                                             |
| [5]     | ID3                     | 0x43: ASCII 'C'                                                                                                                                                                                             |
| [6]     | ID4                     | 0x4F: ASCII 'O'                                                                                                                                                                                             |
| [7]     | Flags                   | Bit 0 : これは ESR イネーブル フラグです。このビットが設定されている場合、ESR 機能がサポートされます。Bits [7:1] : 予約済み。すべてゼロ。                                                                                                                        |
| [8]     | API Version             | 現在のバージョンは1です。このフィールドで、すべての Cisco ESR IPMI コマンドの要求および応答バイトの定義が決まります。ソフトウェアはこのフィールドを使い、システム上の Cisco ESR の API のバージョンを判断できます。たとえば、タイポなどでドキュメントが更新されると、リビジョン番号は変更されますが、API の形式は変更されません。この場合、ソフトウェアに変更の必要はありません。 |
| [9]     | Document Version, Minor | これは、このドキュメントのマイナーバージョンで、参照に使用します。                                                                                                                                                                           |
| [10]    | Document Version, Major | これは、このドキュメントのメジャーバージョンで、参照に使用します。メジャーバージョンとマイナーバージョンはどちらも、参照に使用するこのドキュメントのバージョンを示します。リビジョンはこのドキュメントのタイトル ページにあります。                                                                                          |
| [11:37] | 予約済み                    | すべてゼロにします。                                                                                                                                                                                                  |

### Get ESR-SDR Repository Info コマンド

このコマンドはリポジトリ情報を取得します。IPMI の **Get SDR Repository Info** コマンドに似ています。

|            |                             |                               |
|------------|-----------------------------|-------------------------------|
| コマンド名 :    | Get ESR-SDR Repository Info |                               |
| ネットワーク機能 : | NF_STO                      |                               |
| コマンド番号 :   | 0xF0                        |                               |
| 要求バイト      | フィールド名                      | 説明                            |
| なし         |                             |                               |
| 応答バイト      | フィールド名                      | 説明                            |
| [1]        | Completion Code             |                               |
| [2]        | 状態                          | 0x1 がまだ初期化中。                  |
| [3:6]      | Starting Record ID          | リポジトリの最初の ESR-SDR を示すレコード ID。 |
| [7:10]     | End Record ID               | リポジトリの最後の ESR-SDR を示すレコード ID。 |
| [11:14]    | SDR Size                    | ESR-SDR リポジトリのサイズ (バイト単位)。    |

**Get Cisco SDR Record**

|            |                      |                        |
|------------|----------------------|------------------------|
| コマンド名 :    | Get Cisco SDR Record |                        |
| ネットワーク機能 : | NF_STO               |                        |
| コマンド番号 :   | 0xF1                 |                        |
| 要求バイト      | フィールド名               | 説明                     |
| [1:4]      | レコード ID              | データを取得する SDR のレコード ID。 |
| [5:6]      | Offset               | レコードのオフセット。            |
| [7]        | Read Bytes           | 読み込むバイト数。33 バイトを超えません。 |
| 応答バイト      | フィールド名               | 説明                     |

|       |                 |                                                        |
|-------|-----------------|--------------------------------------------------------|
| [1]   | Completion Code | 0xCA : 要求の読み込みバイト数とオフセットが SDR のレコード長を超えています。           |
| [2:5] | Next Record ID  | 次の SDR のレコード ID。<br>0xFFFFFFFF は最後のレコードに到達していることを示します。 |
| [6:N] |                 | SDR のデータ。                                              |

### Get ESR-SDR コマンド

このコマンドは ESR-SDR リポジトリから ESR-SDR レコードを取得します。IPMI の **Get SDR** コマンドと同じです。

| コマンド名 :    | Get ESR-SDR     |                                                         |
|------------|-----------------|---------------------------------------------------------|
| ネットワーク機能 : | NF_STO          |                                                         |
| コマンド番号 :   | 0xF1            |                                                         |
|            |                 |                                                         |
| 要求バイト      | フィールド名          | 説明                                                      |
| [1:4]      | レコード ID         | データを取得する SDR のレコード ID。                                  |
| [5:6]      | Offset          | レコードのオフセット。                                             |
| [7]        | Read Bytes      | 読み込むバイト数。最大値は 33 です。                                    |
| 応答バイト      | フィールド名          | 説明                                                      |
| [1]        | Completion Code |                                                         |
| [2:5]      | Next Record ID  | 次のレコードのレコード ID。<br>値 0xFFFFFFFF は最後のレコードに到達していることを示します。 |
| [6:N]      | Data            | 取得する ESR-SDR レコードのデータ。                                  |

**Get CES Reading コマンド**

このコマンドは、CES の未加工の測定値を取得します。標準の IPMI の **Get Sensor Reading** コマンドと同じ機能です。

|            |                 |                                                     |
|------------|-----------------|-----------------------------------------------------|
| コマンド名 :    | Get CES Reading |                                                     |
| ネットワーク機能 : | NF_SEN          |                                                     |
| コマンド番号 :   | 0xF0            |                                                     |
| 要求バイト      | フィールド名          | 説明                                                  |
| [1:4]      | CES number      | Cisco Extended Sensor のセンサー番号。                      |
| 応答バイト      | フィールド名          | 説明                                                  |
| [1]        | Completion Code |                                                     |
| [2]        | Reading         | 標準の IPMI の Get Sensor Reading コマンドのバイト 2 を参照してください。 |
| [3]        | Sensor Status   | 標準の IPMI の Get Sensor Reading コマンドのバイト 3 を参照してください。 |
| [4] オプション  | Sensor Flags 1  | 標準の IPMI の Get Sensor Reading コマンドのバイト 4 を参照してください。 |
| [5] オプション  | Sensor Flags 2  | 標準の IPMI の Get Sensor Reading コマンドのバイト 5 を参照してください。 |

**Get Cisco Extended SEL Repository Information**

このコマンドは SEL リポジトリに関する未加工の測定値を取得します。標準の IPMI の **Get SEL Info** コマンドと同じ機能です。

|            |                                               |
|------------|-----------------------------------------------|
| コマンド名 :    | Get Cisco Extended SEL Repository Information |
| ネットワーク機能 : | NF_STO                                        |

|          |                 |                                                                        |
|----------|-----------------|------------------------------------------------------------------------|
| コマンド番号 : |                 | 0xF2                                                                   |
| 要求バイト    | フィールド名          | 説明                                                                     |
| なし       |                 |                                                                        |
| 応答バイト    | フィールド名          | 説明                                                                     |
| [1]      | Completion Code |                                                                        |
| [2:5]    | Total Entries   | リポジトリ内の Cisco Extended SEL の総数。                                        |
| [6:9]    | Free Space      | CESEL リポジトリの空きバイト数。                                                    |
| [10:13]  | Add Timestamp   | 最後に Cisco SEL を追加したときのタイムスタンプ。                                         |
| [14:17]  | Erase Timestamp | 前回 Cisco SEL をクリアしたときのタイムスタンプ。                                         |
| [18]     | Flags           | Bit 7 : 設定されている場合、SEL のオーバーフローが発生しています。<br>Bits[6:0] : 予約済み。すべてゼロにします。 |

**Get Cisco SEL Repository Info**

|            |                 |                               |
|------------|-----------------|-------------------------------|
| コマンド名 :    |                 | Get Cisco SEL Repository Info |
| ネットワーク機能 : |                 | NF_STO                        |
| コマンド番号 :   |                 | 0xF2                          |
| 要求バイト      | フィールド名          | 説明                            |
| なし         |                 |                               |
| 応答バイト      | フィールド名          | 説明                            |
| [1]        | Completion Code |                               |

|         |                 |                                         |
|---------|-----------------|-----------------------------------------|
| [2:5]   | Total Entries   | リポジトリ内の Cisco SEL の数                    |
| [6:9]   | Free Space      | リポジトリの空きバイト数                            |
| [10:13] | Add Timestamp   | 最後に Cisco SEL を追加したときのタイムスタンプ           |
| [14:17] | Erase Timestamp | 前回 Cisco SEL を消去したときのタイムスタンプ            |
| [18]    | SEL Flags       | Bit 7 : 設定されている場合、SEL のオーバーフローが発生しています。 |

### Get Cisco Extended SEL Record コマンド

このコマンドは SEL リポジトリからエントリを取得します。標準の IPMI の **Get SEL Entry** コマンドと同じ機能です。

|            |                                       |                                                                      |
|------------|---------------------------------------|----------------------------------------------------------------------|
| コマンド名 :    | Get Cisco Extended SEL Record<br>コマンド |                                                                      |
| ネットワーク機能 : | NF_SEN                                |                                                                      |
| コマンド番号 :   | 0xF3                                  |                                                                      |
| 要求バイト      | フィールド名                                | 説明                                                                   |
| [1:4]      | Cisco SEL Record ID                   | 取得する Cisco Extended SEL の<br>レコード ID。                                |
| 応答バイト      | フィールド名                                | 説明                                                                   |
| [1]        | Completion Code                       |                                                                      |
| [2:5]      | Next SEL Record ID                    | 次の SEL のレコード ID。値<br>0xFFFFFFFF は最後の SEL レ<br>コードに到達していることを示<br>します。 |
| [6:9]      | SEL Record ID                         | 取得する SEL ID。                                                         |

|         |                 |                                                                                                   |
|---------|-----------------|---------------------------------------------------------------------------------------------------|
| [10]    | SEL Version     | 現在の SEL レコードのバージョン ID。このフィールドは SEL レコードデータの残りのバイトの解釈方法を示します。詳細については、ESR-SEL レコード形式セクションを参照してください。 |
| [11:29] | SEL Record Data | Cisco Extended SEL のデータ。                                                                          |

**Get Cisco SEL Entry**

|            |                     |                                                                  |
|------------|---------------------|------------------------------------------------------------------|
| コマンド名 :    | Get Cisco SEL Entry |                                                                  |
| ネットワーク機能 : | NF_STO              |                                                                  |
| コマンド番号 :   | 0xF3                |                                                                  |
|            |                     |                                                                  |
| 要求バイト      | フィールド名              | 説明                                                               |
| [1:4]      | SEL ID              | 取得する SEL エントリの番号。                                                |
| 応答バイト      | フィールド名              | 説明                                                               |
| [1]        | Completion Code     | 0xCA : SEL ID は存在しません                                            |
| [2:5]      | Next SEL ID         | 次の SEL の SEL ID。<br>0xFFFFFFFF は最後の SEL レコードに到達していることを示します。      |
| [6:9]      | SEL ID              | 取得する SEL ID。                                                     |
| [10]       | Version             | Cisco SEL 形式のバージョン。<br>現在はバージョン 1 であるため、この後のバイトでバージョン 1 が定義されます。 |
| [11]       | SEL Type            | IPMI の Get SEL Entry Response の同じところを参照してください。                   |
| [12:13]    | 予約済み                | ゼロにします。                                                          |

|         |                 |                                                |
|---------|-----------------|------------------------------------------------|
| [14:17] | Time stamp      | SEL のタイム スタンプ                                  |
| [18:19] | Generator ID    | IPMI の Get SEL Entry Response の同じところを参照してください。 |
| [20]    | EvMRev          | IPMI の Get SEL Entry Response の同じところを参照してください。 |
| [21]    | Sensor Type     | IPMI の Get SEL Entry Response の同じところを参照してください。 |
| [22:25] | Sensor Number   |                                                |
| [26]    | Event Attribute | IPMI の Get SEL Entry Response の同じところを参照してください。 |
| [27:29] | Event Data      | IPMI の Get SEL Entry Response の同じところを参照してください。 |

### Clear Cisco Extended SEL Repository

このコマンドは、リポジトリのすべての既存の SEL イベントをクリアします。IPMI の **Clear SEL** コマンドと同じです。

|            |                                     |    |
|------------|-------------------------------------|----|
| コマンド名 :    | Clear Cisco Extended SEL Repository |    |
| ネットワーク機能 : | NF_SEN                              |    |
| コマンド番号 :   | 0xF4                                |    |
| 要求バイト      | フィールド名                              | 説明 |
| なし         |                                     |    |
| 応答バイト      | フィールド名                              | 説明 |
| [1]        | Completion Code                     |    |

**Get Cisco Sensor Reading**

|            |                          |                                             |
|------------|--------------------------|---------------------------------------------|
| コマンド名 :    | Get Cisco Sensor Reading |                                             |
| ネットワーク機能 : | NF_SEN                   |                                             |
| コマンド番号 :   | 0xF0                     |                                             |
| 要求バイト      | フィールド名                   | 説明                                          |
| [1:4]      | Sensor Number            | 測定値を取得するセンサーの番号。                            |
| 応答バイト      | フィールド名                   | 説明                                          |
| [1]        | Completion Code          |                                             |
| [2]        | Reading                  | IPMI の Get Sensor Reading のバイト 2 を参照してください。 |
| [3]        | Sensor Status            | IPMI の Get Sensor Reading のバイト 3 を参照してください。 |
| [4] オプション  | Sensor Flags             | IPMI の Get Sensor Reading のバイト 4 を参照してください。 |
| [5] オプション  | Sensor Flags             | IPMI の Get Sensor Reading のバイト 5 を参照してください。 |

## レコード形式

**SDR 形式**

| フィールド名      | IPMI 2.0 SDR タイプ 1 のバイト | Cisco SDR のバイト | 説明                                                 |
|-------------|-------------------------|----------------|----------------------------------------------------|
| レコード ID     | [1:2]                   | [1:4]          | これは、IPMI に対応する最後の SDR レコードに 1 を加えたレコード ID から始まります。 |
| SDR Version | 3                       | 5              | Cisco SDR の場合、0x80 になります。                          |

|                                                                       |         |         |                                                 |
|-----------------------------------------------------------------------|---------|---------|-------------------------------------------------|
| レコード タイプ                                                              | 4       | 6       | Cisco Sensor Full Data Record の場合、0xC1 に固定されます。 |
| Record Length                                                         | 5       | [7:10]  |                                                 |
| Sensor Owner ID                                                       | 6       | 11      |                                                 |
| Sensor Owner LUN                                                      | 7       | 12      |                                                 |
| Sensor Number                                                         | 8       | [13:16] |                                                 |
| Entity ID                                                             | 9       | 17      |                                                 |
| Entity Instance                                                       | 10      | 18      |                                                 |
| Sensor Initialization                                                 | 11      | 19      |                                                 |
| Sensor Capabilities                                                   | 12      | 20      |                                                 |
| Sensor Type                                                           | 13      | 21      |                                                 |
| Event/Reading Code                                                    | 14      | 22      |                                                 |
| Assertion Event Mask/Lower Threshold Reading Mask                     | [15:16] | [23:24] |                                                 |
| Deassertion Event Mask/Upper Threshold Reading Mask                   | [17:18] | [25:26] |                                                 |
| Discrete Reading Mask/Settable Threshold Mask/Readable Threshold Mask | [19:20] | [27:28] |                                                 |
| Sensor Units 1                                                        | 21      | 29      |                                                 |
| Sensor Units 2                                                        | 22      | 30      |                                                 |
| Sensor Units 3                                                        | 23      | 31      |                                                 |
| Linearization                                                         | 24      | 32      |                                                 |
| M                                                                     | 25      | 33      |                                                 |
| M and Tolerance                                                       | 26      | 34      |                                                 |
| B                                                                     | 27      | 35      |                                                 |
| B and Accuracy                                                        | 28      | 36      |                                                 |
| Accuracy, Accuracy exponent and Sensor Direction                      | 29      | 37      |                                                 |
| R and B exponents                                                     | 30      | 38      |                                                 |

|                                    |         |        |                                            |
|------------------------------------|---------|--------|--------------------------------------------|
| Analog Characteristic Flag         | 31      | 39     |                                            |
| Normal Reading                     | 32      | 40     |                                            |
| Normal Maximum                     | 33      | 41     |                                            |
| Normal Minimum                     | 34      | 42     |                                            |
| Sensor Max Reading                 | 35      | 43     |                                            |
| Sensosr Min Reading                | 36      | 44     |                                            |
| Upper Non-Recoverable Threshold    | 37      | 45     |                                            |
| Upper Critical Threshold           | 38      | 46     |                                            |
| Upper Non-Critical Threshold       | 39      | 47     |                                            |
| Lower Non-Recoverable Threshold    | 40      | 48     |                                            |
| Lower Critical Threshold           | 41      | 49     |                                            |
| Lower Non-Critical Threshold       | 42      | 50     |                                            |
| Positive Going Threshold Hystersis | 43      | 51     |                                            |
| Negative Going Threshold Hystersis | 44      | 52     |                                            |
| reserved                           | [45:46] | 該当なし   | 削除されました。                                   |
| OEM                                | 47      | 53     |                                            |
| ID String and Len Code             | 48      | 54     | Bits[7:6]はIPMIの仕様に従います。Bits[5:0]はID文字列長です。 |
| ID String                          | [49:64] | [55:N] | 現在、最大48バイトをサポートしています。Nの最大値は102です。          |

### ESR-SEL レコード形式

このセクションでは、ESR-SEL レコード形式で使われる、標準の IPMI SEL のさまざまな領域の形式を定義します。タイムスタンプフィールドは、一般に、エポックからの秒数を示します。

SEL Type 0x2 は、標準の IPMI SEL Type 0x2 と同じですがインデックスが異なります。SEL レコードバージョンと SEL タイプのフィールドからこのレコードのタイプが分かります。

| バイト インデックス | フィールド名                   | 説明                                                  |
|------------|--------------------------|-----------------------------------------------------|
| [1:4]      | レコード ID                  | この ESR-SEL レコードの ID                                 |
| [5]        | Cisco SEL Record Version | この定義の値は 0x1 です。                                     |
| [6]        | SEL Type                 | 値は 0x2 です。                                          |
| [7:8]      | 予約済み                     | 値はすべてゼロです。                                          |
| [9:12]     | Timestamp                | イベントが ESR-SEL リポジット<br>りにログ記録されたときのタイ<br>ムスタンプ。     |
| [13:14]    | Generator ID             | 標準の IPMI SEL Type 2 のバイ<br>ト 8 と 9 を参照してください。       |
| [15]       | EvMRev                   | 標準の IPMI SEL Type 2 のバイ<br>ト 10 を参照してください。          |
| [16]       | Sensor Type              | 標準の IPMI SEL Type 2 のバイ<br>ト 11 を参照してください。          |
| [17:20]    | Sensor Number            | センサー番号このセンサー番号<br>は IPMI センサーまたは CES の<br>いずれかです。   |
| [21]       | Event Attribute          | 標準の IPMI SEL Type 2 のバイ<br>ト 13 を参照してください。          |
| [22:24]    | Event Data 1, 2 and 3    | 標準の IPMI SEL Type 2 のバイ<br>ト 14 ~ 16 を参照してくださ<br>い。 |

SEL Type OEM の領域 0xC0 ~ 0xDF は次のように機能します。

| バイト インデックス | フィールド名                   | 説明                  |
|------------|--------------------------|---------------------|
| [1:4]      | レコード ID                  | この ESR-SEL レコードの ID |
| [5]        | Cisco SEL Record Version | この定義の値は 0x1 です。     |
| [6]        | SEL Type                 | 値 : 0xC0 ~ 0xDF     |
| [7:8]      | 予約済み                     | 値はすべてゼロです。          |

|         |                 |                                                  |
|---------|-----------------|--------------------------------------------------|
| [9:12]  | Timestamp       | イベントが ESR-SEL リポジトリにログ記録されたときのタイムスタンプ。           |
| [13:15] | Manufacturer ID | 標準の IPMI 仕様の OEM SEL レコードのバイト 8 ~ 10 を参照してください。  |
| [16:22] | OEM Defined     | 標準の IPMI 仕様の OEM SEL レコードのバイト 11 ~ 16 を参照してください。 |
| [23:24] | 予約済み            | すべてゼロを返します。                                      |

IPMI 仕様に従って、SEL Type OEM の領域 0xE0 ~ 0xFF はタイムスタンプのない OEM SEL レコードです。ただし、このイベントが ESR-SEL レコード形式に変換されると、タイムスタンプが付けられます。

| バイト インデックス | フィールド名                         | 説明                                                   |
|------------|--------------------------------|------------------------------------------------------|
| [1:4]      | レコード ID                        | この ESR-SEL レコードの ID                                  |
| [5]        | Cisco SEL Record Version       | この定義の値は 0x1 です。                                      |
| [6]        | SEL Type                       | 値 : 0xE0 ~ 0xFF                                      |
| [7]        | OEM Defined Byte 1             | IPMI 仕様の OEM no-timestamps SEL イベントのバイト 4 を参照してください。 |
| [8]        | 予約済み                           | 値は 0 です。                                             |
| [9:12]     | Timestamp                      | イベントが ESR-SEL リポジトリにログ記録されたときのタイムスタンプ。               |
| [13:24]    | OEM Defined Bytes 2 through 13 | 標準の IPMI 仕様の OEM SEL レコード形式のバイト 5 ~ 16 を参照してください。    |

# IPMI センサー情報に基づいた推奨される解決策

## 概要

IPMI センサー情報は、サーバイベントログとエラーメッセージから入手できます。このセクションでは、IPMI センサーによって報告された問題の考えられる解決策を示します。

## 電源センサー

| Sensor Name | 推奨処置                                                                                                                 |
|-------------|----------------------------------------------------------------------------------------------------------------------|
|             | これらいずれかのセンサーの電圧について表示されるステータスが FAIL の場合、または OK 以外の場合、サーバは Cisco に返却して交換する必要があります。CPU、DIMM、ドライブは交換するサーバに付け替えることができます。 |

| Sensor Name   | 推奨処置 |
|---------------|------|
| P5V_STBY      |      |
| P3V3_STBY     |      |
| P1V1_SSB_STBY |      |
| P1V8_STBY     |      |
| P1V0_STBY     |      |
| P1V5_STBY     |      |
| P0V75_STBY    |      |
| P12V          |      |
| P5V           |      |
| P3V3          |      |
| P1V5_SSB      |      |
| P1V1_SSB      |      |
| P1V8_SAS      |      |
| P1V5_SAS      |      |
| P1V0_SAS      |      |
| P1V0A_SAS     |      |
| P3V3_SAS      |      |
| P12V_SAS      |      |
| P0V75_SAS     |      |
| P1V05_VTT_P1  |      |
| P1V05_VTT_P2  |      |
| P1V05_VTT_P3  |      |
| P1V05_VTT_P4  |      |
| P0V9_PVSA_P1  |      |
| P0V9_PVSA_P2  |      |
| P0V9_PVSA_P3  |      |
| P0V9_PVSA_P4  |      |
| P1V8_PLL_P1   |      |
| P1V8_PLL_P2   |      |
| P1V8_PLL_P3   |      |
| P1V8_PLL_P4   |      |
| P1V1_VCCP_P1  |      |
| P1V1_VCCP_P2  |      |
| P1V1_VCCP_P3  |      |
| P1V1_VCCP_P4  |      |

| Sensor Name                                                                                                                                                                                                                                                                          | 推奨処置                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| P1V5_VCC_AB<br>P1V5_VCC_CD<br>P1V5_VCC_EF<br>P1V5_VCC_GH<br>P1V5_VCC_IJ<br>P1V5_VCC_KL<br>P1V5_VCC_MN<br>P1V5_VCC_OP<br>P0V75_DDR3VTT_AB<br>P0V75_DDR3VTT_CD<br>P0V75_DDR3VTT_EF<br>P0V75_DDR3VTT_GH<br>P0V75_DDR3VTT_IJ<br>P0V75_DDR3VTT_KL<br>P0V75_DDR3VTT_MN<br>P0V75_DDR3VTT_OP |                                                                              |
| P3V_BAT_SCALED                                                                                                                                                                                                                                                                       | 障害が見られる場合は、マザーボードのバッテリーを交換します。                                               |
| HP_MAIN_FET_FLT<br>HP_STBY_FET_FLT<br>HW_POWER_FLT<br>POWER_ON_FAIL                                                                                                                                                                                                                  | これらセンサーの1つに障害が見られる場合はブレードの電源に障害があるため、サーバは交換する必要があります。                        |
| P12V_CUR_SENS<br>POWER_USAGE                                                                                                                                                                                                                                                         | これらのセンサーのいずれかに障害が見られる場合は、サーバの負荷を軽減します。UCS Manager で電力上限と電力割り当てオプションをチェックします。 |

| Sensor Name                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 推奨処置                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| VCCP_P1_CUR_SENS<br>VCCP_P2_CUR_SENS<br>VCCP_P3_CUR_SENS<br>VCCP_P4_CUR_SENS<br>PVSA_P1_CUR_SENS<br>PVSA_P2_CUR_SENS<br>PVSA_P3_CUR_SENS<br>PVSA_P4_CUR_SENS<br>VCCD_AB_CUR_SENS<br>VCCD_CD_CUR_SENS<br>VCCD_EF_CUR_SENS<br>VCCD_GH_CUR_SENS<br>VCCD_IJ_CUR_SENS<br>VCCD_KL_CUR_SENS<br>VCCD_MN_CUR_SENS<br>VCCD_OP_CUR_SENS<br>P1_CORE_VRHOT<br>P2_CORE_VRHOT<br>P3_CORE_VRHOT<br>P4_CORE_VRHOT<br>P1_MEM_VRHOT<br>P2_MEM_VRHOT<br>P3_MEM_VRHOT<br>P4_MEM_VRHOT | これらセンサーの1つ以上の障害は、CPU アクティビティの急増を原因として断続的に見られる場合があります。この障害が頻繁に見られる場合は、CPU の負荷を軽減します。 |

## デバイス検出センサー

| Sensor Name | 推奨処置                                                                                                                            |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
|             | <p>これらはすべて、対応するコンポーネントが正常に検出されたことを示します。</p> <p>取り付けられているデバイスの検出に失敗する場合は、ソケットへの装着をやり直すか、または動作することが分かっている同じタイプのコンポーネントに交換します。</p> |

| Sensor Name    | 推奨処置 |
|----------------|------|
| HDD0_PRS       |      |
| HDD1_PRS       |      |
| HDD2_PRS       |      |
| HDD3_PRS       |      |
| MEZZ1_PRS      |      |
| MEZZ2_PRS      |      |
| MLOM_PRS       |      |
| TPM_CARD_PRS   |      |
| P1_PRESENT     |      |
| P2_PRESENT     |      |
| P3_PRESENT     |      |
| P4_PRESENT     |      |
| DDR3_P1_A0_PRS |      |
| DDR3_P1_A1_PRS |      |
| DDR3_P1_A2_PRS |      |
| DDR3_P1_B0_PRS |      |
| DDR3_P1_B1_PRS |      |
| DDR3_P1_B2_PRS |      |
| DDR3_P1_C0_PRS |      |
| DDR3_P1_C1_PRS |      |
| DDR3_P1_C2_PRS |      |
| DDR3_P1_D0_PRS |      |
| DDR3_P1_D1_PRS |      |
| DDR3_P1_D2_PRS |      |
| DDR3_P2_E0_PRS |      |
| DDR3_P2_E1_PRS |      |
| DDR3_P2_E2_PRS |      |
| DDR3_P2_F0_PRS |      |
| DDR3_P2_F1_PRS |      |
| DDR3_P2_F2_PRS |      |
| DDR3_P2_G0_PRS |      |
| DDR3_P2_G1_PRS |      |
| DDR3_P2_G2_PRS |      |
| DDR3_P2_H0_PRS |      |
| DDR3_P2_H1_PRS |      |

| Sensor Name     | 推奨処置 |
|-----------------|------|
| DDR3_P2_H2_PRS  |      |
| DDR3_P3_I0_PRS  |      |
| DDR3_P3_I1_PRS  |      |
| DDR3_P3_I2_PRS  |      |
| DDR3_P3_J0_PRS  |      |
| DDR3_P3_J1_PRS  |      |
| DDR3_P3_J2_PRS  |      |
| DDR3_P3_K0_PRS  |      |
| DDR3_P3_K1_PRS  |      |
| DDR3_P3_K2_PRS  |      |
| DDR3_P3_L0_PRS  |      |
| DDR3_P3_L1_PRS  |      |
| DDR3_P3_L2_PRS  |      |
| DDR3_P4_M0_PRS  |      |
| DDR3_P4_M1_PRS  |      |
| DDR3_P4_M2_PRS  |      |
| DDR3_P4_N0_PRS  |      |
| DDR3_P4_N1_PRS  |      |
| DDR3_P4_N2_PRS  |      |
| DDR3_P4_O0_PRS  |      |
| DDR3_P4_O1_PRS  |      |
| DDR3_P4_O2_PRS  |      |
| DDR3_P4_P0_PRS  |      |
| DDR3_P4_P1_PRS  |      |
| DDR3_P4_P2_PRS  |      |
| MAIN_POWER_PRS  |      |
| LSI_FLASH_PRSNT |      |
| BBU_PRES        |      |

**POST センサー**

| Sensor Name     | 推奨処置                                                               |
|-----------------|--------------------------------------------------------------------|
| BIOS_POST_CMPLT | このセンサーは、サーバの電源投入後に BIOS POST が完了したことを示します。情報メッセージであり、何もする必要はありません。 |

| Sensor Name      | 推奨処置                                                                             |
|------------------|----------------------------------------------------------------------------------|
| BIOSPOST_TIMEOUT | POST が予想以上に時間がかかり、完了できませんでした。情報メッセージであり、何もする必要はありません。                            |
| BIST_FAIL        | ホスト CPU の自己テストの失敗を示します。SEL でどのホスト CPU が失敗したのか確認し、Cisco TAC に連絡してください。CPU を交換します。 |
| WILL_BOOT_FAULT  | サーバはおそらく検出に失敗します。UCS Manager で検出の問題を探してください。                                     |

#### 温度センサー

| Sensor Name                                                  | 推奨処置                                                                                                                                                                                                                        |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TEMP_SENS_FRONT                                              | これは吸気温度センサーです。これが高すぎる場合、周囲の室温が必要な範囲内にあることをただちに確認してください。                                                                                                                                                                     |
| TEMP_SENS_REAR                                               | これは排気温度センサーです。これが高すぎる場合、吸気または排気を妨げるものがないか、またサーバ内のエアバッフルが正しく取り付けられているか確認してください。                                                                                                                                              |
| P1_TEMP_SENS<br>P2_TEMP_SENS<br>P3_TEMP_SENS<br>P4_TEMP_SENS | これらのセンサーは CPU の過熱を示します。CPU のサーマルプレートが正しく取り付けられていない、またはヒートシンクが損傷しているか正しく取り付けられていない可能性があります。<br><br>サーマルプレートの交換やヒートシンクの確認後もまだ高すぎる場合は、さらに吸気または排気を妨げるものがないか、またサーバ内のエアバッフルが正しく取り付けられているか確認してください。この状態が長期間続く場合は、CPU を交換する必要があります。 |

| Sensor Name | 推奨処置                                                                                                                                     |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------|
|             | <p>これらのセンサーは、DIMM の過熱を示します。吸気または排気を妨げるものがないか、またサーバ内のエアバップルが正しく取り付けられているか確認してください。</p> <p>問題が解決しない場合は、DIMM が過熱されて破損し、交換が必要になることがあります。</p> |

| Sensor Name    | 推奨処置 |
|----------------|------|
| DDR3_P1_A0_TMP |      |
| DDR3_P1_A1_TMP |      |
| DDR3_P1_A2_TMP |      |
| DDR3_P1_B0_TMP |      |
| DDR3_P1_B1_TMP |      |
| DDR3_P1_B2_TMP |      |
| DDR3_P1_C0_TMP |      |
| DDR3_P1_C1_TMP |      |
| DDR3_P1_C2_TMP |      |
| DDR3_P1_D0_TMP |      |
| DDR3_P1_D1_TMP |      |
| DDR3_P1_D2_TMP |      |
| DDR3_P2_E0_TMP |      |
| DDR3_P2_E1_TMP |      |
| DDR3_P2_E2_TMP |      |
| DDR3_P2_F0_TMP |      |
| DDR3_P2_F1_TMP |      |
| DDR3_P2_F2_TMP |      |
| DDR3_P2_G0_TMP |      |
| DDR3_P2_G1_TMP |      |
| DDR3_P2_G2_TMP |      |
| DDR3_P2_H0_TMP |      |
| DDR3_P2_H1_TMP |      |
| DDR3_P2_H2_TMP |      |
| DDR3_P3_I0_TMP |      |
| DDR3_P3_I1_TMP |      |
| DDR3_P3_I2_TMP |      |
| DDR3_P3_J0_TMP |      |
| DDR3_P3_J1_TMP |      |
| DDR3_P3_J2_TMP |      |
| DDR3_P3_K0_TMP |      |
| DDR3_P3_K1_TMP |      |
| DDR3_P3_K2_TMP |      |
| DDR3_P3_L0_TMP |      |
| DDR3_P3_L1_TMP |      |

| Sensor Name                                                                                                                                                                                                                            | 推奨処置                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DDR3_P3_L2_TMP<br>DDR3_P4_M0_TMP<br>DDR3_P4_M1_TMP<br>DDR3_P4_M2_TMP<br>DDR3_P4_N0_TMP<br>DDR3_P4_N1_TMP<br>DDR3_P4_N2_TMP<br>DDR3_P4_O0_TMP<br>DDR3_P4_O1_TMP<br>DDR3_P4_O2_TMP<br>DDR3_P4_P0_TMP<br>DDR3_P4_P1_TMP<br>DDR3_P4_P2_TMP |                                                                                                                                                                                                                                                                                                                              |
| P1_PROCHOT<br>P2_PROCHOT<br>P3_PROCHOT<br>P4_PROCHOT                                                                                                                                                                                   | <p>これらのセンサーは CPU の過熱を示します。CPU のサーマルプレートが正しく取り付けられていない、またはヒートシンクが損傷しているか正しく取り付けられていない可能性があります。</p> <p>サーマルプレートの交換やヒートシンクの確認後もまだ高すぎる場合は、さらに吸気または排気を妨げるものがないか、またサーバ内のエアパッフルが正しく取り付けられているか確認してください。</p> <p>問題が解決しない場合は、CPU の交換が必要になることがあります。</p> <p>このセンサーは、Intel プロセッサが内部クロックを遅らせ、電流量を下げ、熱の発生を抑えることで温度を自己調整しようとしていることを示します。</p> |

| Sensor Name                                                          | 推奨処置                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P1_THERMTRIP_N<br>P2_THERMTRIP_N<br>P3_THERMTRIP_N<br>P4_THERMTRIP_N | <p>これらのセンサーは CPU の過熱を示します。CPU のサーマルプレートが正しく取り付けられていない、またはヒートシンクが損傷しているか正しく取り付けられていない可能性があります。</p> <p>サーマルプレートの交換やヒートシンクの確認後もまだ高すぎる場合は、さらに吸気または排気を妨げるものがないか、またサーバ内のエアバッフルが正しく取り付けられているか確認してください。</p> <p>問題が解決しない場合は、CPU の交換が必要になることがあります。</p> <p>このセンサーは Intel プロセッサが温度を自己調整し、過熱による損傷をシャットダウンによって防止しようとしていることを示します。これが見られるのは、ほとんどの場合、プロセッサが内部クロックを遅らせ、電流量を下げ、熱の発生を抑えることで温度を自己調整しようとした後です。</p> |

### SuperCap センサー

| Sensor Name    | 推奨処置                                                                                             |
|----------------|--------------------------------------------------------------------------------------------------|
| LSI_SCAP_FAULT | このセンサーは SuperCap を交換する必要があることを示します。                                                              |
| BBU_PRES       | このセンサーは SuperCap が使われていることを示します。情報のみで、何もする必要はありません。                                              |
| BBU_TEMP       | このセンサーは SuperCap の温度を摂氏でレポートします。情報のみで、過熱がレポートされない限り何もする必要はありません。SuperCap が過熱している場合は、サーバの電源を切ります。 |
| BBU_PRED_FAIL  | このセンサーは SuperCap が停止しそうな状態であり、交換する必要があることを示します。                                                  |

| Sensor Name                   | 推奨処置                                                    |
|-------------------------------|---------------------------------------------------------|
| BBU_FAULT<br>BBU_REPLACE_REQD | SuperCap で障害が生じているため、ただちに SuperCap を交換してください。           |
| BBU_DEGRADED                  | SuperCap に注意が必要です。LSI のファームウェアが自動的に処理するため、何もする必要はありません。 |
| BBU_CAPACITANCE               | SuperCap の充電状態を測定し、設計値の % で報告します。                       |

## 標準 IPMI センサー

| Sensor Name        | 推奨処置                                                   |
|--------------------|--------------------------------------------------------|
| SEL_FULLNESS       | 標準 IPMI センサー ログがいっぱいです。何もする必要はありません。情報提供のみです。          |
| CISCO_SEL_FULLNESS | Cisco Extended Sensor ログがいっぱいです。何もする必要はありません。情報提供のみです。 |

## ダウングレード後の IPMI 設定で発生する問題の防止

問題：IPMI の設定に障害が発生します。

考えられる原因：デフォルトでは、LAN 経由 IPMI は、CIMC バージョン 2.2 (2\*) 以上では無効になります。たとえばシステムを 2.2 (1d) にダウングレードしている場合、LAN 経由 IPMI は無効のままです。

ダウングレード後に発生する可能性がある問題を回避するため、ダウングレード前にこの項の手順 ([http://www.cisco.com/web/about/security/intelligence/IPMI\\_security.html#host](http://www.cisco.com/web/about/security/intelligence/IPMI_security.html#host)) に従い、Cisco UCS Manager で、LAN 上の IPMI を有効にします。



## 第 8 章

# IOM の問題のトラブルシューティング

この章の内容は、次のとおりです。

- [IOM の用語, 111 ページ](#)
- [シャーシのブート シーケンス, 112 ページ](#)
- [リンクのピン接続とフェールオーバーの動作, 114 ページ](#)
- [IOM の問題に関する推奨される解決策, 115 ページ](#)

## IOM の用語

IOM の問題の診断でよく見られる略語と用語は次の通りです。

- HR : Host Receive Block (ホスト受信ブロック)
- NR : Network Receive Block (ネットワーク受信ブロック)
- SS : Switching Subsystem (スイッチングサブシステム)
- HI : Host Interface Block (ホストインターフェイスブロック)
- NI : Network Interface Block (ネットワークインターフェイスブロック)
- CI : CPU Interface Block (CPUインターフェイスブロック)
- BI : BMC Interface Block (BMCインターフェイスブロック)
- HIF : Host Interface (ホストインターフェイス)
- NIF : Network Interface (ネットワークインターフェイス)
- CIF : CPU Interface (CPUインターフェイス)
- BIF : BMC Interface (BMCインターフェイス)
- VIF : Virtual Interface (仮想インターフェイス)
- VNTag : Virtual NIC Tag (仮想NICタグ)

- h2n : Host-to-Network (ホスト - ネットワーク) 方向。HI、CI、BI で受信した NI 宛てのトラフィックの説明に使用。
- n2h : Network-to-Host (ネットワーク - ホスト) 方向。NI で受信した HI、CI、BI 宛てのトラフィックの説明に使用。
- Redwood : 2104 IOM に搭載されている ASIC。Redwood ASIC の基本機能は、サーバアダプタカードに接続されている 8 つのホスト側 10G イーサネットポートと 4 つのネットワーク側 10G イーサネットポートでやり取りされるトラフィックを集約することです。
- Woodside : 2204 および 2208 IOM に搭載されている ASIC。32 のホスト側 10G イーサネットポートと 4 つまたは 8 つのネットワーク側 10G イーサネットポートでやり取りされるトラフィックを集約します。
- シャーシ管理スイッチ (CMS : Chassis Management Switch) : IOM に統合されている Marvell 88E6095 イーサネットスイッチ。
- CMC : Redwood または Woodside ASIC と CMS を制御し、必要な IOM ファームウェアを実行し、その他のシャーシ管理機能を実行する CPU。

## シャーシのブートシーケンス

Cisco 5108 シャーシの 2100 および 2200 シリーズ IOM は、シャーシ自体でアクティブな唯一のコンポーネントです。シャーシを稼働するには 1 つの IOM で十分ですが、両方ともクラスタの設定が必要です。

シャーシと IOM に関する問題の一部は、次のブートシーケンスを確認することで追跡できます。

- 1 電源が投入されます。
- 2 ブートローダが呼び出し済み、IOM のメモリが設定済みかつスクラビング処理済みで、ECC が有効化されます。ブートローダで、IOM Health LED がオレンジ色に設定されます。
- 3 カーネルチェックサムおよび起動が開始されます。  
指定したカーネルチェックサムが失敗するか、指定したカーネルが最後の 2 回の起動でユーザプロセス「OHMD」の起動に失敗した場合、代替カーネルが起動します。
- 4 カーネルを起動できない場合、IOM Health LED がオレンジ色で点滅します。IOM は Cisco UCS Manager では認識されません。これが唯一のアクティブ IOM の場合、シャーシ全体が認識されません。

カーネルの起動が成功すると、IOM Health LED が緑色に設定されます。IOM が Cisco UCS Manager で認識されない場合、IOM とファブリックインターコネクタ間に物理的な配線の問題が存在していないか確認します。Cisco UCS Manager で管理するシャーシの場合、物理的な接続が 1 つ機能していなければなりません。配線に問題がない場合、IOM のファームウェアのバージョンが、Cisco UCS Manager のバージョンよりも古い可能性があります。IOM をシスコに返却する必要がある場合があります。

5 Communications ASIC で実行中のプロセス (Redwood または Woodside) および CMC Process Monitor (pmon) で実行中のプロセスを起動し、次の CMC プラットフォームのプロセスを再起動します。

- platform\_ohms -POST およびランタイムのヘルス モニタリング
- dmserver - デバイス マネージャ、seeprom データ キャッシュ、I2C デバイス スキャン
- ipmiserver - センサーおよび UCS Manager への FRU データ送信
- cmc\_manager - シャーシ情報の設定、UCS Manager 要求への応答
- cluster\_manager - ローカル クラスタ マスターおよびクライアント データの転送
- updated - ソフトウェア アップデートの要求のリッスン
- thermal - シャーシ サーマル管理
- pwrmgr - シャーシの電源マネージャ
- pppd - ピア CMC への UART 2 経由の通信パス
- obfllogger - OBFL Flash へのメッセージのログに対するクライアント要求の許可
- rsyslogd - syslog、UCS Manager 宛てにレベル別に送信されたメッセージ

ブート シーケンスのステージ 2 または 3 で障害が検出された場合、関連コンポーネントが主に考えられる原因であり、ほとんどの場合 IOM を返却する必要があります。IOM ブート ロード コンソールを直接監視することができる IOM に HDMI コンソール ポートがありますが、これを使用できるのは、既知の機能しているファームウェア イメージへの読み込みなどの詳細な変更に必要なデバッグ ソフトウェアへのアクセス権を持つ、シスコ社内の技術者に限定されます。

表 10: 予想されるシャーシ IOM および LED の動作

| LED              | Status (ステータス) | LED の状態 |
|------------------|----------------|---------|
| IOM Health LED   | 通常動作中          | グリーン    |
|                  | 起動または軽微なエラー    | オレンジ    |
|                  | 重大なエラー         | オレンジに点滅 |
| Chassis OK LED   | Booting        | 消灯      |
|                  | IOM の制御中       | グリーン    |
| Chassis FAIL LED | エラーなし          | 消灯      |
|                  | 軽微なエラー         | オレンジ    |
|                  | 重大なエラー         | オレンジに点滅 |

## リンクのピン接続とフェールオーバーの動作

IOM とファブリック インターコネクト (IOM HIF ポート) 間のリンクがダウンすると生じる障害は、シャーシ内のサーバに使われる静的ルートのピン設定を理解すると、わかりやすくなります。最も簡単な解決策は、単にシャーシを再確認することですが、このトピックを理解することで、その解決策を実行すべき場合がよくわかるようになります。

表 11: IOM のリンクのピン接続

| アクティブなファブリックリンクの数 | ファブリック リンクにピン接続されるブレード スロット                                                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 1 リンク             | すべての HIF ポートがアクティブ リンクにピン接続されます。                                                                                                             |
| 2 リンク             | 1、3、5、7 はリンク 1 にピン接続<br>2、4、6、8 はリンク 2 にピン接続                                                                                                 |
| 4 リンク             | 1、5 はリンク 1 にピン接続<br>2、6 はリンク 2 にピン接続<br>3、7 はリンク 3 にピン接続<br>4、8 はリンク 4 にピン接続                                                                 |
| 8 リンク (2208XP のみ) | 1 はリンク 1 にピン接続<br>2 はリンク 2 にピン接続<br>3 はリンク 3 にピン接続<br>4 はリンク 4 にピン接続<br>5 はリンク 5 にピン接続<br>6 はリンク 6 にピン接続<br>7 はリンク 7 にピン接続<br>8 はリンク 8 にピン接続 |

1、2、4、8 リンクだけがサポートされます。3、5、6、7 リンクは無効な構成となります。

以下に想定される動作の例を示します。

- 1 各 IOM 上にはアクティブなリンクが 4 つあり、それぞれ対応するファブリック インターコネクトに接続しています。
- 2 IOM-1 とそのファブリック インターコネクト (現在アクティブ) を接続するリンク 4 が、データセンターの従業員に誤って切断されています。

- 3 ブレードスロット 3、4、7、8 を使用した IOM-1 経由の接続は IOM-2 とスタンバイのファブリック インターコネクタにフェイルオーバーします。スロット 4 と 8 だけが影響を受けそうに思われますが、3つのリンク構成はサポートされていないため、リンク 3 も管理上停止します。データのスループットは失われませんが、Cisco UCS Manager で障害が通知されます。
- 4 この時点で、次のいずれかを実行できます。
  - リンク 4 の接続をやり直して接続の問題を解決します。設定されている通常の動作が再開されます。
  - シャーシを再確認します。構成が行われ、2つのファブリックリンクで機能するようにピン設定が再度確立されます。後でリンクを交換または修理する場合は、2番目の再確認が必要になります。

## IOM の問題に関する推奨される解決策

次の表に、IOM の問題のトラブルシューティングを行うためのガイドラインおよび推奨される解決策を示します。

表 12: IOM の問題

| 問題                                          | 推奨される解決策                                                                                                      |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| IOM Health LED が初期ブートアップでオレンジ色に変わり、そのままになる。 | 問題の IOM を取り付け直します。<br>IOM を取り外して交換します。<br>シャーシの両方の IOM が同じ状態を示している場合は、サーバまたはシャーシの使用を停止して Cisco TAC に連絡してください。 |
| IOM Health LED がオレンジ色で点滅したままで、緑色にならない。      | 問題の IOM を取り付け直します。<br>IOM を取り外して交換します。<br>シャーシの両方の IOM が同じ状態を示している場合は、サーバまたはシャーシの使用を停止して Cisco TAC に連絡してください。 |

| 問題                                                                                    | 推奨される解決策                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>CMC は Cisco UCS Manager からシャーシ情報を受け取っているが、1 つ以上のブレードが応答していないか、シャーシ情報を受け取っていない。</p> | <p>IOM ファームウェアと Cisco UCS Manager が同じソフトウェア レベルであることを確認します。</p> <p>問題の IOM を取り付け直します。</p> <p>IOM の Redwood または Woodside ASIC の POST 結果を確認します。</p> <p>ランタイム リンク 停止ステータスを確認します。</p> <p>問題のサーバで POST テストが失敗しているかどうか確認します。シャーシ情報に関する詳細は、CMC Manager のログにあります。CMC クラスタの状態は、次のコマンドを使ってファブリック インターコネクトと比較できます。</p> <p>FI: show cluster state</p> <p>cmc connected directly to the IOM: show platform software cmcctrl dmclient all</p> |
| <p>CMC が Cisco UCS Manager からシャーシ情報を一切受け取らない。</p>                                     | <p>IOM ファームウェアと Cisco UCS Manager が同じソフトウェア レベルであることを確認します。</p> <p>IOM とファブリック インターコネクト間で 1 つ以上の物理ケーブルが正常に機能していることを確認します。</p> <p>ランタイム リンク 停止ステータスを確認します。</p> <p>問題の IOM を取り付け直します。</p>                                                                                                                                                                                                                                         |
| <p>1 つ以上のサーバへのリンクが失われた。</p>                                                           | <p>問題が生じている複数のサーバが同じピン設定グループにあることを確認します。可能であれば、停止しているリンクを隔離して交換します。</p> <p>問題のサーバを取り付け直します。</p> <p>問題の IOM を取り付け直します。</p> <p>シャーシを再確認し、問題のサーバへのピン接続を再度確立します。</p>                                                                                                                                                                                                                                                                |
| <p>IOM-1 が IOM-2 にピア接続していない。</p>                                                      | <p>両方の IOM を取り付け直します。</p>                                                                                                                                                                                                                                                                                                                                                                                                       |



```

0      up <= iBMC slot 1
1      up <= iBMC slot 2
2      down <= iBMC slot 3
3      down <= iBMC slot 4
4      up <= iBMC slot 5
5      down <= iBMC slot 6
6      down <= iBMC slot 7
7      down <= iBMC slot 8
8      up <= CMS/CMC Processor link
9      no_phy <= Redwood link
10     no_phy <= Debug port link
IN_GOOD_OCTETS_LO (p0) : [0x000290AA]
IN_GOOD_OCTETS_HI (p0) : [0x00000000]
...
...
IN_FILTERED      (p10) : [0x0000]
OUT_FILTERED     (p10) : [0x0000]

```

Woodside ASIC のランタイム リンク停止ステータスを確認します。

- NI : ネットワーク インターフェイスはスイッチ側
- HI : ホスト インターフェイスはブレード側

```

cmc-3-A# connect iom 1
fex-1# show platform software woodside sts
Board Status Overview:
  legend:
    ' '= no-connect
    X  = Failed
    -  = Disabled
    :  = Dn
    |  = Up
    [$] = SFP present
    [ ] = SFP not present
    [X] = SFP validation failed

```

```

-----
(FINAL POSITION TBD)      Uplink #:      1  2  3  4  5  6  7  8
Link status:             |  |  |  |  |  |  |  |
SFP:                     +-----+
                        [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
                        +-----+
                        | N  N  N  N  N  N  N  N |
                        | I  I  I  I  I  I  I  I |
                        | 0  1  2  3  4  5  6  7 |
                        |
                        |           NI (0-7)           |
                        +-----+
                        |
-----+-----+-----+-----+
|           |           |           |           |
+-----+-----+-----+-----+
|           |           |           |           |
+-----+-----+-----+-----+
| HI (0-7)  | HI (8-15) | HI (16-23) | HI (24-31) |
|           |           |           |           |
| H  H  H  H  H  H  H  H | | H  H  H  H  H  H  H  H | | H  H  H  H  H  H  H  H | | H  H  H
| I  I  I  I  I  I  I  I | | I  I  I  I  I  I  I  I | | I  I  I  I  I  I  I  I | | I  I  I
| I  I  I  I  I  |
| 0  1  2  3  4  5  6  7 | | 8  9  1  1  1  1  1  1 | | 1  1  1  1  2  2  2  2 | | 2  2  2
| 2  2  2  3  3 |
|           |           |           |           |
|           |           |           |           |
| 7  8  9  0  1 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] | [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] | [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] | [ ] [ ] [ ]
| [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] |

```







## 第 9 章

# その他のトラブルシューティング用マニュアル

---

- [その他のトラブルシューティング用マニュアル](#), 121 ページ

## その他のトラブルシューティング用マニュアル

その他のトラブルシューティング情報は、次のマニュアルに記載されています。

- 『[Cisco UCS Manager Faults and Error Message Reference](#)』 : Cisco UCS Manager の障害および BIOS や CIMC のメッセージなどのシステム イベント ログ メッセージに関する情報が含まれています。
- 『[Cisco UCS C-Series Servers Integrated Management Controller Troubleshooting Guide](#)』 : C シリーズ ラックマウント サーバの問題のトラブルシューティング方法に関する情報が含まれています。
- 『[Cisco UCS Central Troubleshooting Reference Guide](#)』 : Cisco UCS Central を使用して問題をトラブルシューティングする方法に関する情報が含まれています。

