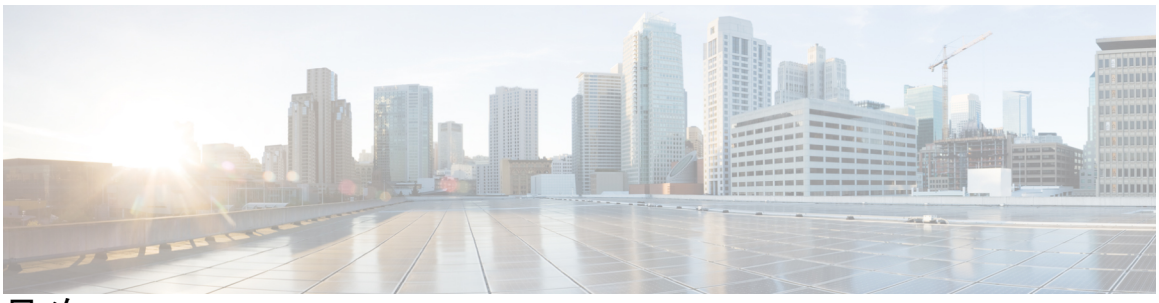
# Cisco UCS Manager リリース 4.2 システム モニタリング ガイド

**初版**：2021 年 6 月 24 日

**最終更新**：2023 年 1 月 9 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/



# 目 次

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

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

Guidance: Reuse the below note in your respective documentation.

（注） The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

# はじめに



## 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、フィールドのラベルのような GUI 要素は、**[GUI 要素]** のように示しています。<br>ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。 |
| マニュアルのタイトル | マニュアルのタイトルは、イタリック体（*italic*）で示しています。 |
| TUI 要素 | テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、`courier` フォントで示しています。 |

| テキストのタイプ | 説明 |
|---|---|
| システム出力 | システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。 |
| CLI コマンド | CLI コマンドのキーワードは、**this font**で示しています。<br>CLI コマンド内の変数は、このフォント 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　安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

# Cisco UCS の関連資料

### ドキュメント ロードマップ

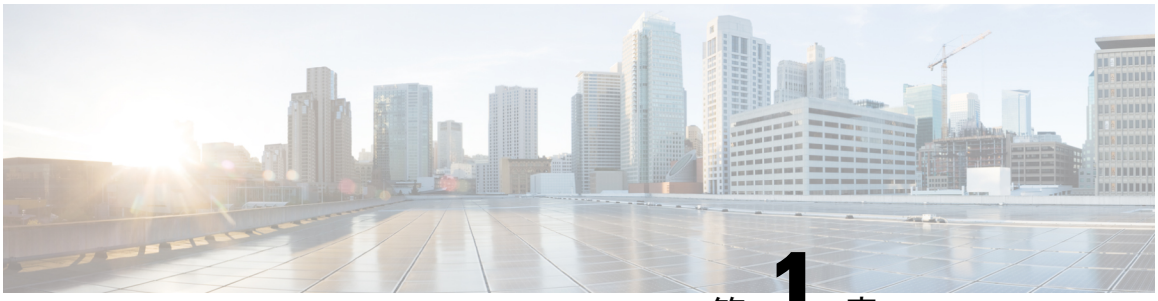
すべての B シリーズ マニュアルの完全なリストについては、次の URL で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

すべての C-Series マニュアルの完全なリストについては、次の URL で入手可能な『『*Cisco UCS C-Series Servers Documentation Roadmap*』』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html

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

# 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、または誤りや記載漏れに関する報告は、ucs-docfeedback@external.cisco.com に送信してください。ご協力をよろしくお願いいたします。



第 1 章

# このリリースの新規情報および変更情報



## このリリースの新規情報および変更情報

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

**表 *1 : Cisco UCS Manager*、リリース *4.2(1l)* の新機能と変更された動作**

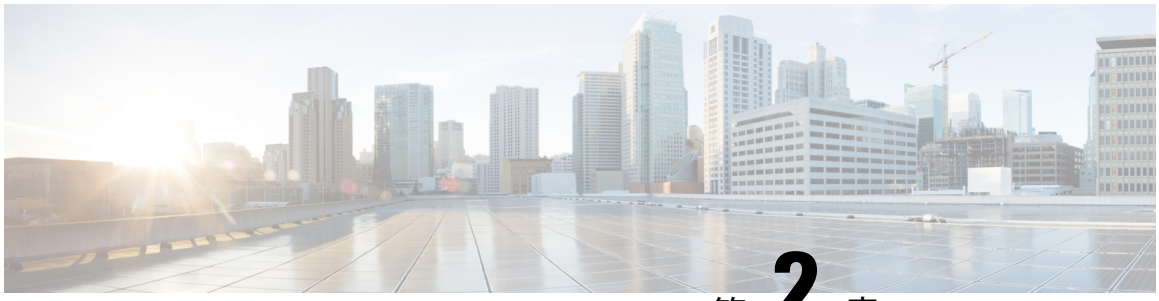
| 特長 | 説明 | 参照先 |
|---|---|---|
| Cisco UCS C225 M6サーバ のサポート | Cisco UCS Managerは、Cisco UCS C225 M6サーバでいくつかの監視機能をサポートするようになりました。 | -- |

**表 *2 : Cisco UCS Manager*、リリース *4.2(1i)* の新機能と変更された動作**

| 特長 | 説明 | 参照先 |
|---|---|---|
| Cisco UCS C245 M6サーバ のサポート | Cisco UCS Manager は、Cisco UCS C245 M6サーバ による一部の監視機能をサポートするようになりました。 | -- |

表 *3 : Cisco UCS Manager*、リリース *4.2(1d)* の新機能と変更された動作

| 特長 | 説明 | 参照先 |
|---|---|---|
| セキュリティ プロトコルおよびデータ モデル（SPDM）の監視 | Cisco UCS Manager は、SPDM ポリシーを介してリムーバブル デバイスのセキュリティ アラート設定を構成できるようになりました。監視には 3 つのアラート レベルが用意されています。 | SPDM セキュリティ （59 ページ） |
| Cisco UCS C220 M6サーバおよび Cisco UCS C240 M6サーバのサポート | Cisco UCS Manager は Cisco UCS Cisco UCS C220 M6サーバおよび Cisco UCS C240 M6サーバ をサポートします。 | -- |



第 2 章

# システム モニタリングの概要



# システム モニタリングの概要

このガイドでは、システムのモニタリングを使用した Cisco UCS Manager 環境の管理と設定方法について説明します。

Cisco UCS Manager は、システム障害（クリティカル、メジャー、マイナー、警告）を検出できます。次のことを行うことを推奨します。

- マイナーの障害および警告には緊急のアクションは必要ないため、クリティカルまたはメジャーのシビラティ（重大度）ステータスのすべての障害をモニタします。
- FSM 障害は時間とともに遷移して解決するため、有限状態マシン（FSM）のタイプでない障害をモニタします。

このガイドは、次の内容で構成されています。

- システム ログ
  - エラー、障害、およびアラームしきい値を含むシステム ログ（Syslog）
  - Syslog には、障害、イベント、および監査の 3 種類のログがあります。
  - Syslog を制御する設定とグローバル障害ポリシー
- システム イベント ログ
  - サーバおよびシャーシコンポーネントとそれらの内部コンポーネントのシステム ハードウェア イベント（システム イベント ログ（SEL）ログ）
  - SEL ログを制御する SEL ポリシー
- 簡易ネットワーク管理プロトコル

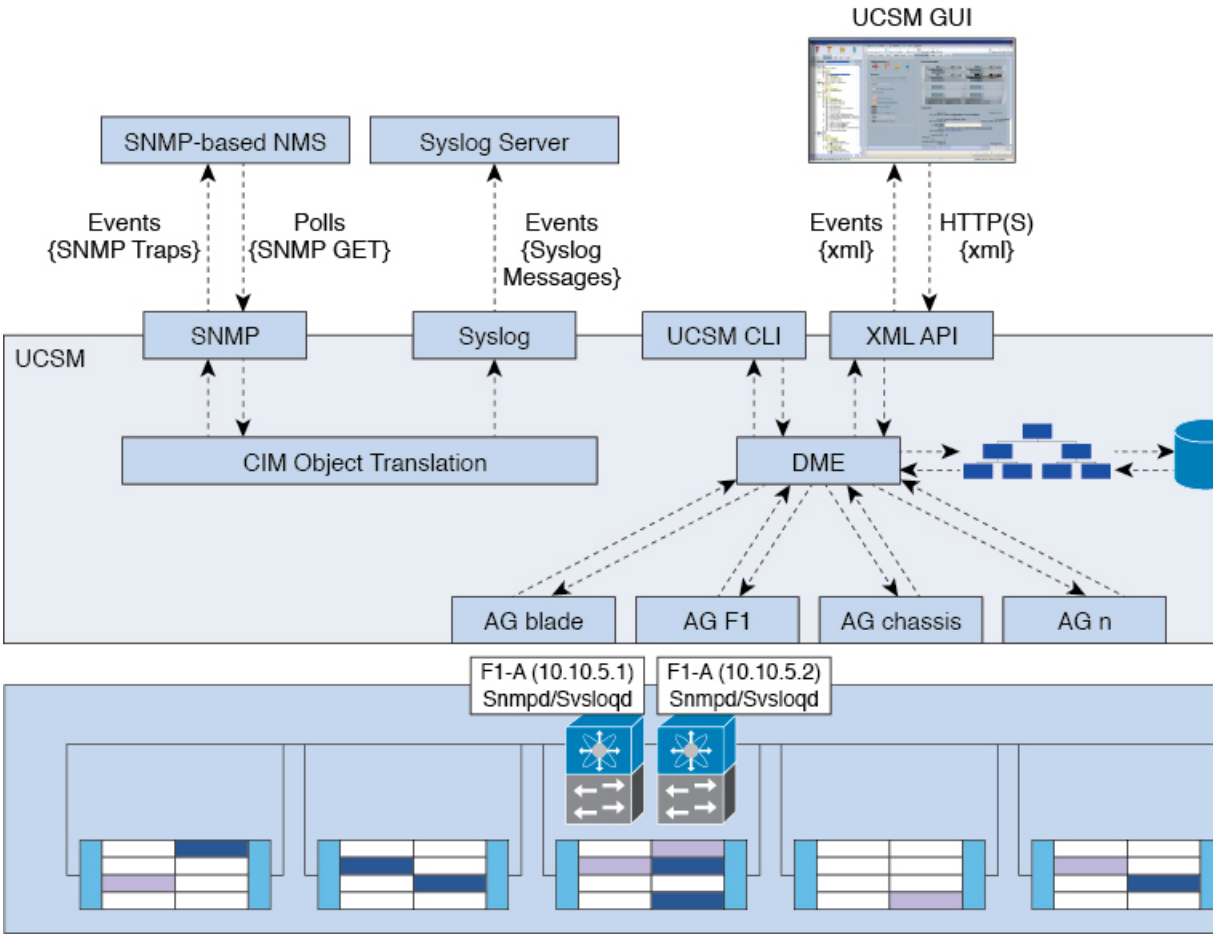
  - 中央のネットワーク管理ステーションからデバイスをモニタリングするためのSNMPおよび、ホストとユーザの設定
  - SNMP トラップ、Call Home 通知、および特定デバイスでの障害抑制ポリシー
- Core File Exporter および、Syslog、監査ログ、システム イベント ログなどのログ
- アダプタ、シャーシ、ホスト、ポート、およびサーバに対する統計情報の収集およびしきい値ポリシー
- Call Home および Smart Call Home の Cisco 組み込みデバイスのサポート
- Cisco UCS Manager ユーザ インターフェイスを使用したハードウェアのモニタリング
- ネットワーク アナライザの分析用トラフィック モニタリング セッション
- IP ネットワーク トラフィックのアカウンティング、使用量に応じたネットワークの課金、ネットワークのプランニング、セキュリティ、Denial of Service（DoS）の監視機能、およびネットワーク モニタリングについての Cisco NetFlow のモニタリング機能

# Cisco UCS Manager コアと障害の生成

Cisco UCS Manager コアは、データ管理エンジン、アプリケーション ゲートウェイ、およびユーザによるアクセスが可能なノースバウンドインターフェイスの3つの要素から構成されています。ノースバウンドインターフェイスは、SNMP、Syslog、XML API、UCSM CLI で構成されています。

Cisco UCS Manager サーバは XML API、SNMP、および Syslog を使用してモニタできます。SNMP と Syslog はどちらも読み取り専用で、モニタリングのみに使用されるインターフェイスであるため、これらのインターフェイスから設定を変更することはできません。また、XML API は読み取り/書き込みモニタリング インターフェイスであるため、Cisco UCS ManagerCisco UCS Managerをモニタしたり、必要に応じて設定を変更することができます。

図 *1 : Cisco UCS Manager* コアおよびモニタリング インターフェイス




### データ管理エンジン（DME）

DME は Cisco UCS Managerシステムの中心であり、次を維持します。

- すべての物理要素（ブレード サーバとラックマウント サーバ、シャーシ、 モジュール、およびファブリック インターコネクト）のインベントリ データベースを収容するCisco UCSXML データベース。
- プロファイル、ポリシー、プール、vNIC および vHBA テンプレートの論理構成データ。
- VLAN、VSAN、ポート チャネル、ネットワーク アップリンク、サーバ ダウンリンク サーバなどのさまざまなネットワーク関連の構成の詳細情報。

DME は以下をモニタします。

- Cisco UCS ドメイン内のすべての物理要素と論理要素のすべてのコンポーネントの現在の完全性と状態。
- 発生したすべての有限状態マシン（FSM）タスクの遷移情報。

管理対象のエンドポイントのインベントリ、完全性、および設定データの現在の情報のみがCisco UCS XMLデータベースに格納されるため、リアルタイムに近い情報となります。デフォルトでは、DME は Cisco UCS ドメイン内で発生した障害の履歴ログを保存しません。エンドポイントで障害状態が発生すると、DME は Cisco UCS XML データベースに障害を作成します。これらの障害が軽減されると、DME は Cisco UCS XML データベースから障害をクリアして削除します。

### アプリケーション ゲートウェイ（AG）

アプリケーション ゲートウェイは、エンドポイントと直接通信するソフトウェア エージェントであり、エンドポイントのヘルスおよび状態を DME にリレーします。AG の管理対象エンドポイントには、サーバ、シャーシ、モジュール、ファブリック エクステンダ、ファブリック インターコネクト、NX-OS が含まれます。AG は Cisco Integrated Management Controller（CIMC）を使用して、IPMI ログおよび SEL ログを通じてアクティブにサーバをモニタします。それらは、デバイスのヘルス、状態、設定、および潜在的な障害状態を DME に提供します。AG は、Cisco UCSXML データベースに変更が加えられると、FSM 遷移時の現在の状態から目的の状態への設定変更を管理します。

モジュール AG およびシャーシ AG は、Chassis Management Controller（CMC）と通信することにより、ヘルス、状態、設定、および障害状態について CMC が把握している情報を取得します。ファブリック インターコネクト NX-OS AG は、NX-OS と直接通信することで、ヘルス、状態、設定、統計情報、および障害状態についてファブリック インターコネクトの NX-OS が把握している情報を取得します。すべての AG は、さまざまな検出プロセス中に、エンドポイントに関するインベントリの詳細を DME に提供します。AG は、FSM がトリガーした遷移中にエンドポイントの設定変更に必要な状態を変化させ、エンドポイントのヘルスおよび状態をモニタし、すべての障害を DME に通知します。

### ノースバウンド インターフェイス

ノースバウンド インターフェイスには、SNMP、Syslog、CLI、および XML API が含まれます。XML API は、Apache Web サーバ レイヤに置かれており、ログイン、ログアウト、クエリー、および設定の要求を HTTP または HTTPS を使用して送信します。SNMP および Syslog は、どちらも DME から得るデータのコンシューマです。

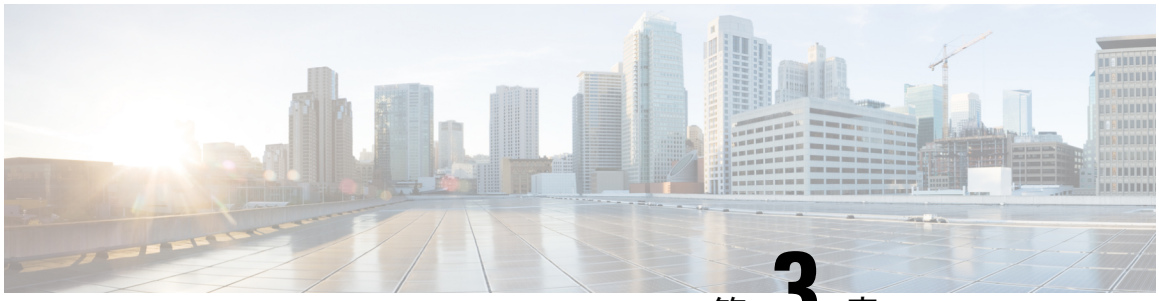
SNMP インフォームおよびトラップは、Cisco UCSXML データベースに格納された障害情報から直接変換されます。SNMP GET 要求は、同じオブジェクト変換エンジンを介して逆方向に送信され、そこでオブジェクト変換エンジンからの要求を DME が受信します。データは、XML データベースから取得され、SNMP応答に変換されます。

syslog メッセージには SNMP と同じオブジェクト変換エンジンが使用されており、データ（障害、イベント、監査ファイル）の発信元は XML からCisco UCS Manager形式の syslog メッセージ に変換されます。

# Cisco UCS Manager ユーザ ドキュメント

Cisco UCS Manager 次の表に記載する、細分化されたユースケース ベースの新しいドキュメントが用意されています。

| ガイド | 説明 |
|---|---|
| Cisco UCS Manager クイック スタート ガイド | Cisco UCS のアーキテクチャと初回操作について説明しています。これにはCisco UCS Manager初期構成と構成のベストプラクティスも含まれます。 |
| Cisco UCS Managerアドミニストレーション ガイド | パスワード管理、ロールベースのアクセス構成、リモート認証、通信サービス、CIMC セッションの管理、組織、バックアップと復元、スケジュール設定オプションに、BIOS トークン、遅延導入について説明しています。 |
| Cisco UCS Manager インフラストラクチャ管理ガイド | Cisco UCS Manager で使用および管理される物理および仮想インフラストラクチャ コンポーネントについて説明しています。 |
| 『Cisco UCS Manager Firmware Management Guide』 | 自動インストールを使用したファームウェアのダウンロード、管理、アップグレード、サービスプロファイルを使用したファームウェアのアップグレード、ファームウェア自動同期を使用したエンドポイントでの直接ファームウェアアップグレード、機能カタログの管理、導入シナリオ、トラブルシューティングについて説明しています。 |
| Cisco UCS Manager サーバ管理ガイド | 新しいランセンス、Cisco UCS Central への Cisco UCS ドメイン の登録、パワー キャッピング、サーバブート、サーバプロファイル、サーバ関連のポリシーについて説明しています。 |
| Cisco UCS Manager ストレージ管理ガイド | Cisco UCS Manager での SUN、VSAN などのストレージ管理のすべての側面について説明しています。 |
| Cisco UCS Manager ネットワーク管理ガイド | Cisco UCS Manager での LAN、VLAN などのネットワーク管理のすべての側面について説明しています。 |
| Cisco UCS Manager システム モニタリング ガイド | Cisco UCS Manager でのシステム統計を含め、システムおよびヘルスモニタリングのすべての側面について説明しています。 |
| Cisco UCS S3260 サーバと Cisco UCS Manager との統合 | Cisco UCS Manager による UCS S シリーズ サーバ管理のすべての側面について説明しています。 |



第 3 章

# Syslog



## Syslog

Cisco UCS Manager はシステム ログ、つまり syslog メッセージを生成して Cisco UCS Manager システム内で発生した次のインシデントを記録します。

- 定期的なシステム操作
- 障害およびエラー
- 重大なおよび緊急な事態

syslog のエントリには、障害、イベント、監査の 3 種類があります。

各 syslog メッセージは、メッセージを生成した Cisco UCS Manager プロセスを特定し、発生したエラーまたはアクションの簡単な説明が提供されします。syslogは、定期的なトラブルシューティングやインシデントへの対処および、管理にも役立ちます。

Cisco UCS Manager は、syslog メッセージを内部的に収集し、記録します。syslog デーモンを実行している外部 syslog サーバにこれらを送信できます。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。モニタされる syslog メッセージには、DIMM の問題、装置の障害、熱の問題、電圧の障害、電源の問題、高可用性（HA）クラスタの問題、およびリンクの障害が含まれます。

（注） FSM の障害、しきい値の障害、および未解決のポリシー イベントは、syslog サーバに送信されません。ただし、しきい値障害イベントに対して SNMP トラップが生成されます。

Syslog メッセージには、イベント コードおよび障害コードが含まれています。Syslog メッセージをモニタするために、Syslog メッセージ フィルタを定義できます。これらのフィルタは、選択した基準に基づいて syslog メッセージを解析できます。フィルタを定義するために、次の条件を使用できます。

- イベントコード別または障害コード別：モニタする特定のコードだけを含めるための解析ルールを使ったフィルタを定義します。これらの条件に一致しないメッセージは廃棄されます。
- シビラティ（重大度）別：特定のシビラティ（重大度）を持つSyslogメッセージをモニタするための解析ルールを使ったフィルタを定義します。syslog のシビラティ（重大度）は OS の機能に応じた個別指定が可能で、簡易的な概要からデバッグ用の詳細情報に至るまでのメッセージのロギングと表示が行えます。

シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslogサービスは、簡単なコンフィギュレーションファイルに従って、メッセージを受信してからファイルに保存するか、出力します。この形式のロギングは、ログの保護された長期的な保存場所を提供できるので、シスコ デバイスでの最適な方法です。

# Cisco UCS Manager GUI を使用した Syslog の設定

**手順**

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[障害、イベント、および監査ログ]**を展開します。

**ステップ 3** [Syslog] をクリックします。

**ステップ 4** [Local Destinations] 領域で、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [コンソール（Console）] セクション | |
| [管理状態（Admin State）] フィールド | Cisco UCSでコンソールに syslog メッセージを表示するかどうかを指定します。次のいずれかになります。<br>• [Enabled]：Syslog メッセージはコンソールに表示され、ログに追加されます。<br>• [Disabled]：Syslog メッセージはログに追加されますが、コンソールには表示されません。 |
| [Level] フィールド | このオプションが [Enabled] である場合、表示する最も低いメッセージ レベルを選択します。Cisco UCS はコンソールのそのレベル以上のメッセージを表示します。レベルは次のいずれかになります。<br>• **緊急（Emergencies）**<br>• **アラート（Alerts）**<br>• **クリティカル（Critical）** |

| 名前 | 説明 |
|---|---|
| [モニタ（Monitor）] セクション | |
| [管理状態（Admin State）] フィールド | Cisco UCSでモニタに syslog メッセージを表示するかどうかを指定します。この状態は次のいずれかになります。<br>• [Enabled]：Syslog メッセージはモニタに表示され、ログに追加されます。<br>• [Disabled]：Syslog メッセージはログに追加されますが、モニタには表示されません。<br>**[管理状態（Admin State）]** が有効になっている場合は、Cisco UCS Manager GUIにこのセクションの残りのフィールドが表示されます。 |
| [Level] ドロップダウン リスト | このオプションが [Enabled] である場合、表示する最も低いメッセージ レベルを選択します。モニタにはそのレベル以上のメッセージが表示されます。レベルは次のいずれかになります。<br>• **緊急（Emergencies）**<br>• **アラート（Alerts）**<br>• **クリティカル（Critical）**<br>• **[Errors]**<br>• **[Warnings]**<br>• **[Notifications]**<br>• **[Information]**<br>• **[Debugging]** |
| [File] セクション | |
| [管理状態（Admin State）] フィールド | Cisco UCSがファブリック インターコネクトのシステム ログにメッセージを保存するかどうかを指定します。この状態は次のいずれかになります。<br>• [Enabled]：メッセージはログ ファイルに保存されます。<br>• [Disabled]：メッセージは保存されません。<br>**[管理状態（Admin State）]** が有効になっている場合は、Cisco UCS Manager GUIにこのセクションの残りのフィールドが表示されます。 |

| 名前 | 説明 |
|---|---|
| [レベル（Level）] ドロップダウン リスト | システムに保存するメッセージの最低レベルを選択します。Cisco UCS は、ファブリック インターコネクトのファイル内に、そのレベル以上のメッセージを保存します。レベルは次のいずれかになります。<br>• **緊急（Emergencies）**<br>• **アラート（Alerts）**<br>• **クリティカル（Critical）**<br>• **[Errors]**<br>• **[Warnings]**<br>• **[Notifications]**<br>• **[Information]**<br>• **[Debugging]** |
| [Name] フィールド | メッセージが記録されるファイルの名前。<br>名前には 16 文字以内の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）が使用できます。デフォルトの名前は**「messages」**です。 |
| [Size] フィールド | ファイルの可能最大サイズ（バイト単位）。ファイルがこのサイズを超えると、Cisco UCS Managerによって最も古いメッセージから最新メッセージへの上書きが開始されます。<br>4096 ～ 4194304 の整数を入力します。 |

**ステップ 5** [Remote Destinations] 領域で、次のフィールドに情報を入力し、Cisco UCSコンポーネントにより生成されたメッセージを保存できる最大 3 つの外部ログを設定します。

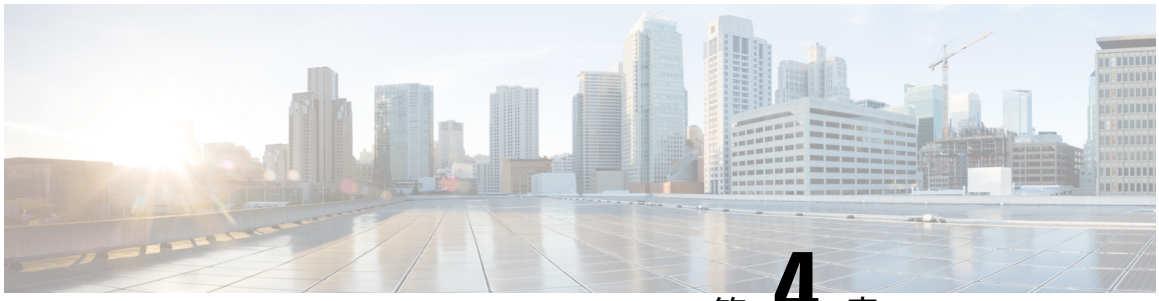
| 名前 | 説明 |
|---|---|
| [管理状態（Admin State）] フィールド | 次のいずれかになります。<br>• **有効**<br>• **無効**<br>**[管理状態（Admin State）]**が有効になっている場合は、Cisco UCS Manager GUIにこのセクションの残りのフィールドが表示されます。 |

| 名前 | 説明 |
|---|---|
| [レベル（Level）] ドロップダウン リスト | システムに保存するメッセージの最低レベルを選択します。リモート ファイルにそのレベル以上のメッセージが保存されます。レベルは次のいずれかになります。<br>• **緊急（Emergencies）**<br>• **アラート（Alerts）**<br>• **クリティカル（Critical）**<br>• **[Errors]**<br>• **[Warnings]**<br>• **[Notifications]**<br>• **[Information]**<br>• **[Debugging]** |
| [Hostname] フィールド | リモート ログ ファイルが存在するホスト名または IP アドレス。<br>（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Managerで DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。 |
| [Facility] ドロップダウン リスト | 次のいずれかになります。<br>• **local0**<br>• **local1**<br>• **local2**<br>• **local3**<br>• **local4**<br>• **local5**<br>• **local6**<br>• **local7** |

**ステップ 6** [Local Sources] エリアで、次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [障害管理状態（Faults Admin State）] フィールド | このフィールドが**[Enabled]**の場合、 Cisco UCS はすべてのシステム障害をログに記録します。 |
| [Audits Admin State] フィールド | このフィールドが **[Enabled]**の場合、Cisco UCS はすべての監査ログ イベントをログに記録します。 |
| [Events Admin State] フィールド | このフィールドが **[Enabled]**の場合、 Cisco UCSはすべてのシステム イベントをログに記録します。 |

**ステップ 7** **[Save Changes]**をクリックします。



第 4 章

# システム イベント ログ



# 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。SEL は、システム正常性に関するトラブルシューティングのために使用されます。過不足電圧のインスタンス、温度イベント、ファン イベント、BIOS 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 によってサポートされるイベントのタイプには、BIOS イベント、メモリ ユニット イベント、プロセッサ イベント、およびマザーボード イベントが含まれます。

SEL ログは SEL ログ ポリシーに従って CIMC NVRAM に保存されます。SEL ログを定期的にダウンロードしてクリアすることがベストプラクティスです。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、定期的に実行されるように設定できます。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。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 という名前になります。

# 各サーバのシステム イベント ログの表示

### 手順

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

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

**ステップ 3** システム イベント ログ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 [SEL Logs] タブをクリックします。

Cisco UCS Manager はサーバのシステム イベント ログを取得し、イベントのリストを表示します。

# シャーシ内のサーバのシステム イベント ログの表示

### 手順

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

**ステップ 2** [Equipment] タブで、**[Equipment] > [Chassis] > *[Chassis_Name]*** を展開します。

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

Cisco UCS Manager はサーバのシステム イベント ログを取得し、イベントのリストを表示します。

**ステップ 4** [Server] テーブルで、システム イベント ログを表示するサーバを選択します。

Cisco UCS Manager はサーバのシステム イベント ログを取得し、イベントのリストを表示します。

# SEL ポリシーの設定

### 手順

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

**ステップ 2** **[機器]** ノードをクリックします。

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

**ステップ 4** [SEL Policy] サブタブをクリックします。

**ステップ 5** （任意） [General] 領域で、[Description] フィールドにポリシーの説明を入力します。

この領域の他のフィールドは読み取り専用です。

**ステップ 6** [Backup Configuration] 領域で、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [プロトコル（Protocol）] フィールド | リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。<br>• **FTP**<br>• **TFTP**<br>• **SCP**<br>• **ステップ**<br>• **[USB A]**：ファブリック インターコネクト A に挿入された USB ドライブ。<br>このオプションは特定のシステム設定でのみ使用できます。<br>• **[USB B]**：ファブリック インターコネクト B に挿入された USB ドライブ。<br>このオプションは特定のシステム設定でのみ使用できます。 |
| [Hostname] フィールド | バックアップ設定が存在する場所のサーバのホスト名または IP アドレス。 IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Managerで DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。<br>（注） バックアップ ファイルの名前は、Cisco UCS によって生成されます。名前は次の形式になります。<br>`sel-system-name-chchassis-id-servblade-id-blade-serial-timestamp` |

| 名前 | 説明 |
|---|---|
| [Remote Path] フィールド | 必要に応じて、リモート サーバ上のファイルの絶対パスを指定します。<br>SCP を使用する場合、絶対パスは常に必要です。他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロードフォルダにあれば、リモートパスを指定する必要はありません。ファイル サーバの設定方法の詳細については、システム管理者に問い合わせてください。 |
| [Backup Interval] ドロップダウン リスト | 自動バックアップ間の待機時間。次のいずれかになります。<br>• Never：自動 SEL データ バックアップを実行しません。<br>• **1 Hour**<br>• **2 Hours**<br>• **4 時間**<br>• **8 Hours**<br>• **[24 Hours]**<br>• **1 Week**<br>• **1 Month**<br>（注） システムによって自動バックアップを作成する場合は、[Action] オプション ボックス内の [Timer] チェックボックスがオンになっていることを確認してください。 |
| [Format] フィールド | バックアップ ファイルに使用する形式。次のいずれかになります。<br>• **Ascii**<br>• **2 進数** |
| [Clear on Backup] チェックボックス | オンにすると、Cisco UCSは、バックアップが完了した後に、すべてのシステム イベント ログをクリアします。 |
| [ユーザ（User）] フィールド | システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP の場合、このフィールドは適用されません。 |
| [パスワード（Password）] フィールド | リモート サーバのユーザ名のパスワード。プロトコルが TFTP の場合、このフィールドは適用されません。 |

| 名前 | 説明 |
|---|---|
| [Action] チェックボックス | オンにした各ボックスでは、イベントが発生したときに、システムは SEL のバックアップを作成します。<br>• [Log Full]：ログが許容される最大サイズに到達。<br>• [On Change of Association]：サーバとそのサービス プロファイルの間のアソシエーションが変化。<br>• [On Clear]：システム イベント ログがユーザによって手動でクリア。<br>• [Timer]：[Backup Interval] ドロップダウン リストで指定された時間間隔に到達。 |
| [Reset Configuration] ボタン | バックグラウンドの設定情報をリセットするには、このボタンをクリックします。 |

**ステップ 7** **[Save Changes]**をクリックします。

# システム イベント ログの 1 つ以上のエントリのコピー

このタスクでは、サーバまたはシャーシの [SEL Logs] タブで、サーバのシステム イベント ログが表示されていることを前提にしています。

**手順**

**ステップ 1** Cisco UCS Manager GUI によって [SEL Logs] タブにシステム インベントが表示されたら、マウスを使用して、システムイベントログからコピーするエントリ（複数可）を強調表示します。

**ステップ 2** **Copy** をクリックして、強調表示されたテキストをクリップボードにコピーします。

**ステップ 3** 強調表示されたテキストをテキスト エディタまたは他のドキュメントに貼り付けます。

# システム イベント ログの印刷

このタスクでは、サーバまたはシャーシの [SEL Logs] タブで、サーバのシステム イベント ログが表示されていることを前提にしています。

### 手順

**ステップ 1** Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、[**Print**] をクリックします。

**ステップ 2** [Print] ダイアログボックス で、次の手順を実行します。

a) （任意） デフォルト プリンタ、あるいはその他の任意のフィールドまたはオプションを修正します。

b) [Print] をクリックします。

# システム イベント ログのリフレッシュ

このタスクでは、サーバまたはシャーシの [SEL Logs] タブで、サーバのシステム イベント ログが表示されていることを前提にしています。

### 手順

Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、[**Refresh**] をクリックします。

Cisco UCS Manager はサーバのシステム イベント ログを取得し、アップデートされたイベントのリストを表示します。

# システム イベント ログの手動バックアップ

このタスクでは、サーバまたはシャーシの [SEL Logs] タブで、サーバのシステム イベント ログが表示されていることを前提にしています。

### 始める前に

システム イベント ログ ポリシーを設定します。手動によるバックアップ操作では、システム イベント ログ ポリシーで設定されたリモート宛先を使用します。

### 手順

Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、[**[Backup]**] をクリックします。

Cisco UCS Manager は、SEL ポリシーで指定された場所にシステム イベント ログをバックアップします。

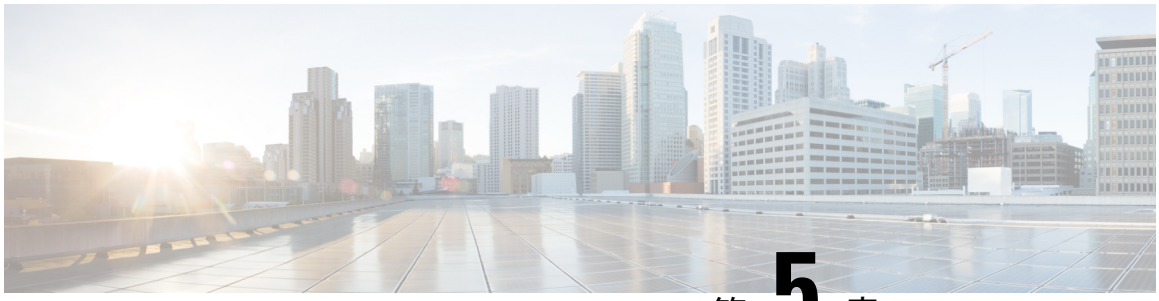
# システム イベント ログの手動クリア

このタスクでは、サーバまたはシャーシの [SEL Logs] タブで、サーバのシステム イベント ログが表示されていることを前提にしています。

**手順**

Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、[**Clear**] をクリックします。

（注） SEL ポリシーの [Action] オプション ボックスで [Clear] がイネーブルになっていると、この処理によって自動バックアップが実行されます。



第 5 章

# Core File Exporter



## Core File Exporter

ファブリック インターコネクトまたは I/O モジュールなどの Cisco UCS のコンポーネントでの重大なエラーによって、システムにコアダンプ ファイルが作成される場合があります。Cisco UCS Manager は、Core File Exporter を使用して、コアダンプ ファイルを TFTP 経由でネットワーク上の指定された場所にエクスポートします。この機能を使用することにより、tar ファイルをコア ダンプ ファイルのコンテンツと一緒にエクスポートできます。Core File Exporter は、システムをモニタリングし、TAC Case に含める必要のあるコア ダンプ ファイルを自動的にエクスポートします。

## Core File Exporter の設定

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[障害、イベント、および監査ログ]**を展開します。

**ステップ 3** [Settings] をクリックします。

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

**ステップ 5** [TFTP Core Exporter] タブで、次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [管理状態（Admin State）] フィールド | 次のいずれかになります。<br>• **[Enabled]**：エラーによってサーバがコア ダンプを実行した場合、 Cisco UCS は所定の場所にコア ダンプ ファイルを FTP を使用して自動的に送信します。このオプションを選択すると、Cisco UCS Manager GUIには、FTP エクスポート オプションを指定できる他のフィールドが表示されます。Core File Exporter は、システムをモニタリングし、TAC Case に含める必要があるコア ファイルを自動的にエクスポートします。<br>• [Disabled]：コア ダンプ ファイルは自動的にエクスポートされません。 |
| [Description] フィールド | コア ファイルのユーザ定義による説明。<br>256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。 |
| [Port] フィールド | TFTP を介してコア ダンプ ファイルをエクスポートするときに使用されるポート番号。 |
| [Hostname] フィールド | TFTP を介して接続されるホスト名か IPv4 アドレスまたは IPv6 アドレス。<br>（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Managerで DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。 |
| [Path] フィールド | リモート システムにコア ダンプ ファイルを保存するときに使用するパス。 |

**ステップ 6** **[Save Changes]**をクリックします。

# Core File Exporter のディセーブル化

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

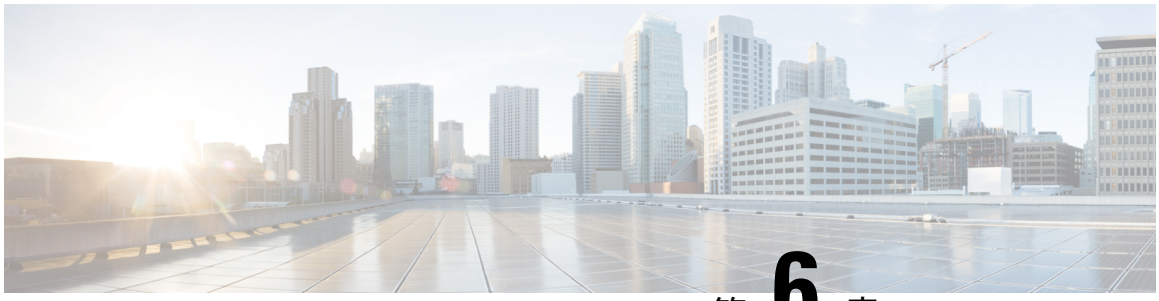
**ステップ 2** **[すべて]** > **[障害、イベント、および監査ログ]**を展開します。

**ステップ 3** [Settings] をクリックします。

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

**ステップ 5** [TFTP Core Exporter] 領域で、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。

**ステップ 6** **[Save Changes]**をクリックします。



第 6 章

# 監査ログ



## 監査ログ

監査ログは、発生したシステム イベント、発生した場所、開始したユーザーを記録します。

## 監査ログの表示

[Audit Logs] ページに表示される監査ログを参照、エクスポート、印刷、または更新できます。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

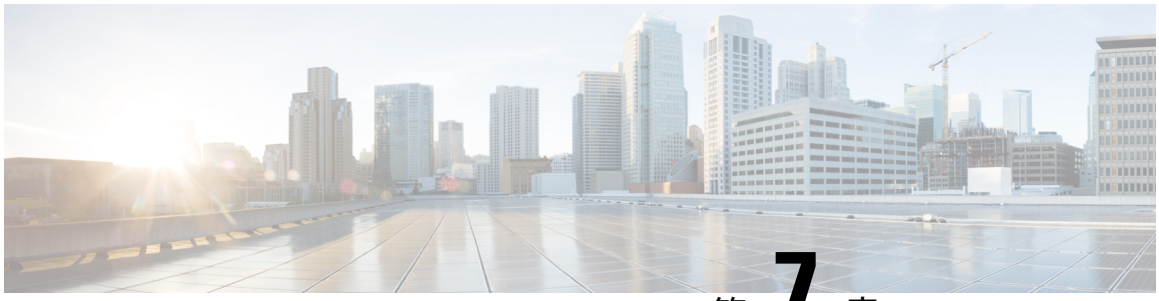
**ステップ 2** **[すべて]** > **[障害、イベント、および監査ログ]**を展開します。

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

**ステップ 4** [Work] ペインに監査ログが表示されます。

| 名前 | 説明 |
|---|---|
| [ID] カラム | メッセージに関連付けられた固有識別情報。 |
| [影響を受けるオブジェクト（Affected Object）] カラム | この問題で影響を受けるコンポーネント。<br>オブジェクト名をクリックすると、そのプロパティが表示されます。 |
| [トリガー（Trig）] カラム | イベントを発生させたユーザに関連付けられたユーザ ロール。 |
| [ユーザ（User）] カラム | ユーザのタイプ。 |

| 名前 | 説明 |
|---|---|
| [Session ID] カラム | イベント発生時にセッションと関連付けられたセッション ID。 |
| [発生場所（Created at）] カラム | 障害が発生した日時。 |
| [識別（Indication）] カラム | 次のいずれかになります。<br>• **[作成（Creation）]**：コンポーネントがシステムに追加された。<br>• **[変更（Modification）]**：既存のコンポーネントが変更された。 |
| **[説明（Description）]** カラム | 障害についての詳細情報。 |
| [Modified Properties] カラム | イベントによって変更されたシステム プロパティ。 |



第 7 章

# 障害の収集と抑制



# 障害収集ポリシーの設定

## グローバル障害ポリシー

グローバル障害ポリシーは、障害がクリアされた日時、フラッピング間隔（障害発生とクリア状態の間の時間）、および保持間隔（システムで障害が発生していた時間）など、Cisco UCS ドメイン内の障害のライフサイクルを制御します。

Cisco UCS の障害には次のライフサイクルがあります。

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。フラッピング間隔中に、グローバル障害ポリシーで指定された期間にわたり、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、グローバル障害ポリシーで指定された期間にわたり、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。

# グローバル障害ポリシーの構成

## 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[障害、イベント、および監査ログ]**を展開します。

**ステップ 3** [設定（Settings）] をクリックします。

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

**ステップ 5** [グローバル障害ポリシー（Global Fault Policy）] タブで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [フラッピング間隔（Flapping Interval）] フィールド | 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。これを防止するため、Cisco UCS Managerでは、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。<br>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。その時点で何が発生するかは、[クリア処理（Clear Action）] フィールドの設定によって異なります。<br>5 ～ 3,600 の範囲の整数を入力します。デフォルトは 10 です。 |
| [当初のシビラティ（重大度）（Initial Severity）] フィールド | 次のいずれかになります。<br>• **情報**<br>• **条件**<br>• **警告** |
| [確認時のアクション（Action on Acknowledgment）] フィールド | 認識されたアクションはログがクリアされると必ず削除されます。このオプションは変更できません。 |
| [クリア処理（Clear Action）] フィールド | エラーがクリアされるときに Cisco UCS Manager が実行するアクション。次のいずれかになります。<br>• [保持（Retain）]：Cisco UCS Manager GUI に [クリア済み障害の保持期間（Length of time to retain cleared faults）] セクションが表示されます。<br>• [削除（Delete）]：障害メッセージにクリアのマークが付いた時点で、Cisco UCS Managerはすぐに障害メッセージを削除します。 |

| 名前 | 説明 |
|---|---|
| [クリア間隔（Clear Interval）] フィールド | Cisco UCS Manager によって特定の間隔で自動的に障害をクリアするかどうかを指定します。次のいずれかになります。<br>• [不可（Never）]：Cisco UCS Manager は自動的に障害をクリアしません。<br>• [その他（other）]：Cisco UCS Manager GUI に [dd:hh:mm:ss] フィールドが表示されます。 |
| [dd:hh:mm:ss] フィールド | Cisco UCS Manager が障害にクリア済みのマークを付けるまでの経過時間（日、時、分、および秒）。その時点で何が発生するかは、[クリア処理（Clear Action）] フィールドの設定によって異なります。 |

**ステップ 6** **[Save Changes]**をクリックします。

# 障害抑制の設定

## フォールト抑制

障害抑制によって、予定されたメンテナンス時間中に SNMP トラップおよび Call Home 通知を抑制することができます。障害抑制タスクを作成し、一時的な障害が発生またはクリアされるたびに通知が送信されることを防止できます。

障害は、期限切れになるか、フォールト抑制タスクが手動で停止されるまで抑制されたままになります。フォールト抑制が終了した後に、Cisco UCS Manager がクリアされていない未処理の抑制された障害の通知を送信します。

次の方法を使用して障害抑制を設定することができます。

#### Fixed Time Intervals（固定時間間隔）または Schedules（スケジュール）

以下を使用して、障害を抑制するメンテナンス ウィンドウを指定することができます。

- 固定時間間隔を使用すると、開始時刻と障害抑制をアクティブにする期間を指定できます。固定時間間隔は繰り返し使用できません。
- スケジュールは、1 回限り、または繰り返される期間で使用されます。スケジュールは保存して再利用することができます。

### 抑制ポリシー

これらのポリシーは、抑制する要因と障害タイプを定義します。タスクに割り当てることができるポリシーは 1 つだけです。次のポリシーが Cisco UCS Managerによって定義されます。

- **default-chassis-all-maint**：シャーシとそのシャーシにインストールされたすべてのコンポーネントの障害を抑制します。コンポーネントには、すべてのサーバ、電源、ファンモジュール、IOM などが含まれます。

  このポリシーは、シャーシにのみ適用されます。

- **default-chassis-phys-maint**：シャーシ、すべてのファン モジュール、シャーシに装着された電源の障害を抑制します。

  このポリシーは、シャーシにのみ適用されます。

- **default-fex-all-maint**：FEX、すべての電源、ファン モジュール、FEX 内の IOM の障害を抑制します。

  このポリシーは、FEX にのみ適用されます。

- **default-fex-phys-maint**：FEX、FEX 内のすべてのファン モジュールと電源の障害を抑制します。

  このポリシーは、FEX にのみ適用されます。

- **default-server-maint**：サーバの障害を抑制します。

  このポリシーは、シャーシ、組織およびサービス プロファイルに適用されます。

（注） シャーシに適用された場合、サーバのみが影響を受けます。

（注） データセンターで使用される高性能な高信頼性サーバ アクセス スイッチをサポートするように設計された NX-OS ネットワーク オペレーティング システムで生成される SNMP MIB-2 障害を、Cisco UCS Manager は抑制しません。これらの SNMP MIB-2 障害は、この障害抑制ポリシーに関連付けられていません。

- **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。

  このポリシーは、シャーシ、FEX および IOM にのみ適用されます。

### 抑制タスク

これらのタスクを使用して、スケジュール設定または固定時間間隔と抑制ポリシーをコンポーネントに関連付けることができます。

（注） 抑制タスクの作成後は、タスクの固定時間間隔またはスケジュールを Cisco UCS Manager GUI と Cisco UCS Manager CLI の両方で編集できるようになります。ただし、Cisco UCS Manager CLI で変更できるのは、固定時間間隔を使用するかスケジュールを使用するかの切り替えのみです。

# 抑制された障害の表示

手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[障害、イベント、および監査ログ]**を展開します。

**ステップ 3** [Faults] をクリックします。

**ステップ 4** [Work] ペインで、[Severity] 領域にある [Suppressed] アイコンを選択します。

抑制された障害のみを表示するには、[Severity] 領域にある他のアイコンの選択を解除します。

# シャーシに対する障害抑制の設定

## シャーシに対する障害抑制タスクの設定

手順

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

**ステップ 2** **[機器]** > **[シャーシ]**を展開します。

**ステップ 3** 障害抑制タスクを作成するシャーシをクリックします。

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

**ステップ 5** [Actions] エリアで、[Start Fault Suppression] をクリックします。

ヒント 複数のシャーシに対して障害抑制タスクを設定するには、[Navigation] ペインで、Ctrl キーを使用して複数のシャーシを選択します。選択したシャーシのいずれかを右クリックして、[Start Fault Suppression] を選択します。

**ステップ 6** [Start Fault Suppression] ダイアログボックスで、次のフィールドに入力します。

| | |
|---|---|
| [Name] フィールド | 障害抑制タスクの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [Select Fixed Time Interval/Schedule] フィールド | 障害抑制タスクを実行するタイミングを指定します。次のいずれかになります。<br>• [Fixed Time Interval]：障害抑制タスクの開始時間と期間を指定するには、このオプションを選択します。<br>[Start Time] フィールドに、障害抑制タスクを開始する日付と時間を指定します。このフィールドの終わりにある下向き矢印をクリックして、ポップアップ カレンダーから開始時間を選択します。<br>[Task Duration] フィールドに、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行させる場合は、このフィールドに「**00:00:00:00**」と入力します。<br>• [Schedule] ：事前に定義されたスケジュールを使用して開始時間と期間を設定するには、このオプションを選択します。<br>[Schedule] ドロップダウン リストからスケジュールを選択します。新しいスケジュールを作成するには、[Create Schedule] をクリックします。 |
| [Policy] ドロップダウン リスト | ドロップダウン リストから、次の抑制ポリシーを選択します。<br>• **default-chassis-all-maint**：シャーシとそのシャーシにインストールされたすべてのコンポーネントの障害を抑制します。コンポーネントには、すべてのサーバ、電源、ファン モジュール、IOM などが含まれます。<br>• **default-chassis-phys-maint**：シャーシ、すべてのファン モジュール、シャーシに装着された電源の障害を抑制します。<br>• **default-server-maint**：サーバの障害を抑制します。<br>（注） シャーシに適用された場合、サーバのみが影響を受けます。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 |

**ステップ 7** **[OK]** をクリックします。

## シャーシに対する障害抑制タスクの表示

### 手順

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

**ステップ 2** **[機器]** > **[シャーシ]**を展開します。

**ステップ 3** 障害抑制タスク プロパティを表示するシャーシをクリックします。

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

**ステップ 5** [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスでは、新しい障害抑制タスクの追加、既存の障害抑制タスクの削除、既存の障害抑制タスクの変更を行うことができます。

## シャーシに対する障害抑制タスクの削除

この手順では、シャーシに対する障害抑制タスクをすべて削除します。タスクを個別に削除するには、[Suppression Tasks] ダイアログボックスで、[Delete] ボタンを使用します。シャーシに対する障害抑制タスクの表示 （35 ページ）を参照してください。

### 手順

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

**ステップ 2** **[機器]** > **[シャーシ]**を展開します。

**ステップ 3** すべての障害抑制タスクを削除するシャーシをクリックします。

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

**ステップ 5** [Actions] 領域で、[Stop Fault Suppression] をクリックします。

**ヒント** 複数のシャーシに対して障害抑制タスクを削除するには、[Navigation] ペインで、Ctrl キーを使用して複数のシャーシを選択します。選択したシャーシのいずれかを右クリックして、[Stop Fault Suppression] を選択します。

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

# I/O モジュールに対する障害抑制の設定

## IOM に対する障害抑制タスクの設定

### 手順

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

**ステップ 2** （任意） シャーシ内の IOM モジュールを選択するには、**[Equipment]** > **[Chassis]** > **[*Chassis Number*]** > **[IO Modules]** の順に展開します。

**ステップ 3** （任意） FEX 内の IOM モジュールを選択するには、**[Equipment]** > **[Chassis]** > **[*FEX Number*]** > **[IO Modules]** の順に展開します。

**ステップ 4** 障害抑制タスクを作成する IOM をクリックします。

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

**ステップ 6** [Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント　複数の IOM の障害抑制タスクを設定するには、[Navigation] ペインで、**Ctrl** キーを使用して複数の IOM を選択します。選択したいずれかの IOM を右クリックし、[Start Fault Suppression] を選択します。

シャーシか FEX またはその両方で IOM を選択できます。

**ステップ 7** [Start Fault Suppression] ダイアログボックスで、次のフィールドに入力します。

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

| | |
|---|---|
| [Select Fixed Time Interval/Schedule] フィールド | 障害抑制タスクを実行するタイミングを指定します。次のいずれかになります。<br>• [Fixed Time Interval]：障害抑制タスクの開始時間と期間を指定するには、このオプションを選択します。<br>[Start Time] フィールドに、障害抑制タスクを開始する日付と時間を指定します。このフィールドの終わりにある下向き矢印をクリックして、ポップアップ カレンダーから開始時間を選択します。<br>[Task Duration] フィールドに、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行させる場合は、このフィールドに「**00:00:00:00**」と入力します。<br>• [Schedule] ：事前に定義されたスケジュールを使用して開始時間と期間を設定するには、このオプションを選択します。<br>[Schedule] ドロップダウン リストからスケジュールを選択します。新しいスケジュールを作成するには、[Create Schedule] をクリックします。 |
| [Policy] ドロップダウン リスト | デフォルトでは、次の抑制ポリシーが選択されます。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 |

**ステップ 8** **[OK]** をクリックします。

## IOM に対する障害抑制タスクの表示

### 手順

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

**ステップ 2** （任意） シャーシ内の IOM モジュールを選択するには、**[Equipment]** > **[Chassis]** > **[*Chassis Number*]** > **[IO Modules]** の順に展開します。

**ステップ 3** （任意） FEX 内の IOM モジュールを選択するには、**[Equipment]** > **[Chassis]** > **[*FEX Number*]** > **[IO Modules]** の順に展開します。

**ステップ 4** 障害抑制タスク プロパティを表示する IOM をクリックします。

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

**ステップ 6** [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスでは、新しい障害抑制タスクの追加、既存の障害抑制タスクの削除、既存の障害抑制タスクの変更を行うことができます。

## IOM に対する障害抑制タスクの削除

この手順は、IOM の障害抑制タスクをすべて削除します。タスクを個別に削除するには、[Suppression Tasks] ダイアログボックスで、[Delete] ボタンを使用します。IOM に対する障害抑制タスクの表示 （37 ページ）を参照してください。

### 手順

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

**ステップ 2** （任意） シャーシ内の IOM モジュールを選択するには、**[Equipment]** > **[Chassis]** > **[*Chassis Number*]** > **[IO Modules]** の順に展開します。

**ステップ 3** （任意） FEX 内の IOM モジュールを選択するには、**[Equipment]** > **[Chassis]** > **[*FEX Number*]** > **[IO Modules]** の順に展開します。

**ステップ 4** 障害抑制タスクをすべて削除する IOM をクリックします。

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

**ステップ 6** [Actions] 領域で、[Stop Fault Suppression] をクリックします。

ヒント　複数の IOM の障害抑制タスクを削除するには、[Navigation] ペインで、**Ctrl** キーを使用して複数の IOM を選択します。選択したいずれかの IOM を右クリックし、[Stop Fault Suppression] を選択します。

シャーシか FEX またはその両方で IOM を選択できます。

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

# FEX に対する障害抑制の設定

## FEX に対する障害抑制タスクの設定

### 手順

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

**ステップ 2** **[Equipment]** > **[Rack Mounts]** > **[FEX]** の順に展開します。

**ステップ 3** 障害抑制タスクを作成する FEX をクリックします。

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

**ステップ 5** [Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント　複数の FEX に対して障害抑制タスクを設定するには、[Navigation] ペインで、Ctrl キーを使用して複数の FEX を選択します。選択したいずれかの FEX を右クリックし、[Start Fault Suppression] を選択します。

**ステップ 6** [Start Fault Suppression] ダイアログボックスで、次のフィールドに入力します。

| | |
|---|---|
| [Name] フィールド | 障害抑制タスクの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [Select Fixed Time Interval/Schedule] フィールド | 障害抑制タスクを実行するタイミングを指定します。次のいずれかになります。<br>• [Fixed Time Interval]：障害抑制タスクの開始時間と期間を指定するには、このオプションを選択します。<br>[Start Time] フィールドに、障害抑制タスクを開始する日付と時間を指定します。このフィールドの終わりにある下向き矢印をクリックして、ポップアップ カレンダーから開始時間を選択します。<br>[Task Duration] フィールドに、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行させる場合は、このフィールドに「**00:00:00:00**」と入力します。<br>• [Schedule] ：事前に定義されたスケジュールを使用して開始時間と期間を設定するには、このオプションを選択します。<br>[Schedule] ドロップダウン リストからスケジュールを選択します。新しいスケジュールを作成するには、[Create Schedule] をクリックします。 |
| [Policy] ドロップダウン リスト | ドロップダウン リストから、次の抑制ポリシーを選択します。<br>• **default-fex-all-maint**：FEX、すべての電源、ファン モジュール、FEX 内の IOM の障害を抑制します。<br>• **default-fex-phys-maint**：FEX、FEX 内のすべてのファン モジュールと電源の障害を抑制します。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 |

**ステップ 7** **[OK]** をクリックします。

## FEX に対する障害抑制タスクの表示

### 手順

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

**ステップ 2** **[Equipment]** > **[Rack Mounts]** > **[FEX]** の順に展開します。

**ステップ 3** 障害抑制タスク プロパティを表示する FEX をクリックします。

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

**ステップ 5** [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスでは、新しい障害抑制タスクの追加、既存の障害抑制タスクの削除、既存の障害抑制タスクの変更を行うことができます。

## FEX に対する障害抑制タスクの削除

この手順では、FEXに対する障害抑制タスクをすべて削除します。タスクを個別に削除するには、[Suppression Tasks] ダイアログボックスで、[Delete] ボタンを使用します。FEX に対する障害抑制タスクの表示 （40 ページ）を参照してください。

### 手順

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

**ステップ 2** **[Equipment]** > **[Rack Mounts]** > **[FEX]** の順に展開します。

**ステップ 3** すべての障害抑制タスクを削除する FEX をクリックします。

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

**ステップ 5** [Actions] 領域で、[Stop Fault Suppression] をクリックします。

**ヒント** 複数の FEX に対して障害抑制タスクを削除するには、[Navigation] ペインで、Ctrl キーを使用して複数の FEX を選択します。選択した FEX のいずれかを右クリックし、[Stop Fault Suppression] を選択します。

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

# サーバに対する障害抑制の設定

## ブレード サーバに対する障害抑制タスクの設定

### 手順

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

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

**ステップ 3** 障害抑制タスクを作成するサーバをクリックします。

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

**ステップ 5** [Actions] エリアで、[Start Fault Suppression] をクリックします。

**ヒント** 複数のブレード サーバに対して障害抑制タスクを設定するには、[Navigation] ペインで、**Ctrl** キーを使用して複数のブレード サーバを選択します。選択したサーバのいずれかを右クリックして、[Start Fault Suppression] を選択します。

**ステップ 6** [Start Fault Suppression] ダイアログボックスで、次のフィールドに入力します。

| | |
|---|---|
| [Name] フィールド | 障害抑制タスクの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [Select Fixed Time Interval/Schedule] フィールド | 障害抑制タスクを実行するタイミングを指定します。次のいずれかになります。<br>• [Fixed Time Interval]：障害抑制タスクの開始時間と期間を指定するには、このオプションを選択します。<br>[Start Time] フィールドに、障害抑制タスクを開始する日付と時間を指定します。このフィールドの終わりにある下向き矢印をクリックして、ポップアップ カレンダーから開始時間を選択します。<br>[Task Duration] フィールドに、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行させる場合は、このフィールドに「**00:00:00:00**」と入力します。<br>• [Schedule] ：事前に定義されたスケジュールを使用して開始時間と期間を設定するには、このオプションを選択します。<br>[Schedule] ドロップダウン リストからスケジュールを選択します。新しいスケジュールを作成するには、[Create Schedule] をクリックします。 |

| | |
|---|---|
| [Policy] ドロップダウン リスト | デフォルトでは、次の抑制ポリシーが選択されます。<br>• **default-server-maint**：サーバの障害を抑制します。 |

**ステップ 7** **[OK]** をクリックします。

## ブレード サーバの障害抑制タスクの表示

**手順**

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

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

**ステップ 3** 障害抑制タスク プロパティを表示するサーバをクリックします。

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

**ステップ 5** [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスでは、新しい障害抑制タスクの追加、既存の障害抑制タスクの削除、既存の障害抑制タスクの変更を行うことができます。

## ブレード サーバに対する障害抑制タスクの削除

この手順では、ブレードサーバのすべての障害抑制タスクを削除します。タスクを個別に削除するには、[Suppression Tasks] ダイアログボックスで、[Delete] ボタンを使用します。ブレードサーバの障害抑制タスクの表示 （42 ページ）を参照してください。

**手順**

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

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

**ステップ 3** すべての障害抑制タスクを削除するサーバをクリックします。

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

**ステップ 5** [Actions] 領域で、[Stop Fault Suppression] をクリックします。

**ヒント** 複数のブレード サーバの障害抑制タスクを削除するには、[Navigation] ペインで、**Ctrl** キーを使用して複数のブレード サーバを選択します。選択したサーバのいずれかを右クリックし、[Stop Fault Suppression] を選択します。

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

## ラック サーバに対する障害抑制タスクの設定

### 手順

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

**ステップ 2** **[機器]** > **[ラックマウント]** > **[サーバ]**を展開します。

（注） Cisco UCS C125 M5 サーバ では、**[機器（Equipment）]** > **[ラックマウント（Rack Mounts）]** > **[エンクロージャ（Enclosures）]** > **[ラック エンクロージャ *rack_enclosure_number*（Rack Enclosure rack_enclosure_number）]** > **[サーバ（Servers）]** の順に展開します。

**ステップ 3** 障害抑制タスクを作成するサーバをクリックします。

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

**ステップ 5** [Actions] エリアで、[Start Fault Suppression] をクリックします。

ヒント 複数のラック サーバに対して障害抑制タスクを設定するには、[Navigation] ペインで、**Ctrl** キーを使用して複数のラック サーバを選択します。選択したサーバのいずれかを右クリックして、[Start Fault Suppression] を選択します。

**ステップ 6** [Start Fault Suppression] ダイアログボックスで、次のフィールドに入力します。

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

| | |
|---|---|
| [Select Fixed Time Interval/Schedule] フィールド | 障害抑制タスクを実行するタイミングを指定します。次のいずれかになります。<br>• [Fixed Time Interval]：障害抑制タスクの開始時間と期間を指定するには、このオプションを選択します。<br>[Start Time] フィールドに、障害抑制タスクを開始する日付と時間を指定します。このフィールドの終わりにある下向き矢印をクリックして、ポップアップ カレンダーから開始時間を選択します。<br>[Task Duration] フィールドに、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行させる場合は、このフィールドに「**00:00:00:00**」と入力します。<br>• [Schedule] ：事前に定義されたスケジュールを使用して開始時間と期間を設定するには、このオプションを選択します。<br>[Schedule] ドロップダウン リストからスケジュールを選択します。新しいスケジュールを作成するには、[Create Schedule] をクリックします。 |
| [Policy] ドロップダウン リスト | デフォルトでは、次の抑制ポリシーが選択されます。<br>• **default-server-maint**：サーバの障害を抑制します。 |

**ステップ 7** **[OK]** をクリックします。

## ラック サーバの障害抑制タスクの表示

### 手順

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

**ステップ 2** **[機器]** > **[ラックマウント]** > **[サーバ]**を展開します。

（注） Cisco UCS C125 M5 サーバ では、**[機器（Equipment）]** > **[ラックマウント（Rack Mounts）]** > **[エンクロージャ（Enclosures）]** > **[ラック エンクロージャ *rack_enclosure_number*（Rack Enclosure rack_enclosure_number）]** > **[サーバ（Servers）]** の順に展開します。

**ステップ 3** 障害抑制タスク プロパティを表示するサーバをクリックします。

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

**ステップ 5** [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスでは、新しい障害抑制タスクの追加、既存の障害抑制タスクの削除、既存の障害抑制タスクの変更を行うことができます。

## ラック サーバに対する障害抑制タスクの削除

この手順では、ラック サーバのすべての障害抑制タスクを削除します。タスクを個別に削除するには、[Suppression Tasks] ダイアログボックスで、[Delete] ボタンを使用します。ラック サーバの障害抑制タスクの表示 （44 ページ）を参照してください。

### 手順

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

**ステップ 2** **[機器]** > **[ラックマウント]** > **[サーバ]**を展開します。

（注） Cisco UCS C125 M5 サーバ では、**[機器（Equipment）]** > **[ラックマウント（Rack Mounts）]** > **[エンクロージャ（Enclosures）]** > **[ラック エンクロージャ *rack_enclosure_number*（Rack Enclosure rack_enclosure_number）]** > **[サーバ（Servers）]** の順に展開します。

**ステップ 3** すべての障害抑制タスクを削除するサーバをクリックします。

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

**ステップ 5** [Actions] 領域で、[Stop Fault Suppression] をクリックします。

ヒント 複数のラック サーバの障害抑制タスクを削除するには、[Navigation] ペインで、**Ctrl** キーを使用して複数のラック サーバを選択します。選択したサーバのいずれかを右クリックし、[Stop Fault Suppression] を選択します。

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

# サービス プロファイルに対する障害抑制の設定

## サービス プロファイルに対する障害抑制タスクの設定

### 手順

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

**ステップ 2** **[サーバ]** > **[サービスプロファイル]**を展開します。

**ステップ 3** 障害抑制タスクを作成するサービス プロファイルをクリックします。

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

**ステップ 5** [Actions] エリアで、[Start Fault Suppression] をクリックします。

ヒント　複数のサービスプロファイルに対して障害抑制タスクを設定するには、[Navigation] ペインで、Ctrl キーを使用して複数のサービス プロファイルを選択します。選択したいずれかのサービス プロファイルを右クリックし、[Start Fault Suppression] を選択します。

**ステップ 6** [Start Fault Suppression] ダイアログボックスで、次のフィールドに入力します。

| | |
|---|---|
| [Name] フィールド | 障害抑制タスクの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [Select Fixed Time Interval/Schedule] フィールド | 障害抑制タスクを実行するタイミングを指定します。次のいずれかになります。<br>• [Fixed Time Interval]：障害抑制タスクの開始時間と期間を指定するには、このオプションを選択します。<br>[Start Time] フィールドに、障害抑制タスクを開始する日付と時間を指定します。このフィールドの終わりにある下向き矢印をクリックして、ポップアップ カレンダーから開始時間を選択します。<br>[Task Duration] フィールドに、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行させる場合は、このフィールドに「**00:00:00:00**」と入力します。<br>• [Schedule] ：事前に定義されたスケジュールを使用して開始時間と期間を設定するには、このオプションを選択します。<br>[Schedule] ドロップダウン リストからスケジュールを選択します。新しいスケジュールを作成するには、[Create Schedule] をクリックします。 |
| [Policy] ドロップダウン リスト | デフォルトでは、次の抑制ポリシーが選択されます。<br>• **default-server-maint**：サーバの障害を抑制します。 |

**ステップ 7** **[OK]** をクリックします。

## サービス プロファイルに対する障害抑制タスクの削除

この手順では、サービスプロファイルに対する障害抑制タスクをすべて削除します。タスクを個別に削除するには、[Suppression Tasks] ダイアログボックスで、[Delete] ボタンを使用しま

す。サービス プロファイルに対する障害抑制タスクの表示 （47 ページ）を参照してください。

**手順**

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

**ステップ 2** **[サーバ]** > **[サービスプロファイル]**を展開します。

**ステップ 3** すべての障害抑制タスクを削除するサービス プロファイルをクリックします。

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

**ステップ 5** [Actions] 領域で、[Stop Fault Suppression] をクリックします。

**ヒント** 複数のサービス プロファイルに対して障害抑制タスクを削除するには、[Navigation] ペインで、Ctrl キーを使用して複数のサービス プロファイルを選択します。選択したサービス プロファイルのいずれか右クリックし、[Stop Fault Suppression] を選択します。

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

## サービス プロファイルに対する障害抑制タスクの表示

**手順**

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

**ステップ 2** **[サーバ]** > **[サービスプロファイル]**を展開します。

**ステップ 3** 障害抑制タスク プロパティを表示するサービス プロファイルをクリックします。

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

**ステップ 5** [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスでは、新しい障害抑制タスクの追加、既存の障害抑制タスクの削除、既存の障害抑制タスクの変更を行うことができます。

# 組織に対する障害抑制の設定

## 組織に対する障害抑制タスクの設定

### 手順

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

**ステップ 2** **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

**ステップ 3** 障害抑制タスクを作成する組織をクリックします。

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

**ステップ 5** [Actions] エリアで、[Start Fault Suppression] をクリックします。

**ステップ 6** [Start Fault Suppression] ダイアログボックスで、次のフィールドに入力します。

| | |
|---|---|
| [Name] フィールド | 障害抑制タスクの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [Select Fixed Time Interval/Schedule] フィールド | 障害抑制タスクを実行するタイミングを指定します。次のいずれかになります。<br>• [Fixed Time Interval]：障害抑制タスクの開始時間と期間を指定するには、このオプションを選択します。<br>[Start Time] フィールドに、障害抑制タスクを開始する日付と時間を指定します。このフィールドの終わりにある下向き矢印をクリックして、ポップアップ カレンダーから開始時間を選択します。<br>[Task Duration] フィールドに、このタスクの継続時間を指定します。手動で停止するまでこのタスクを実行させる場合は、このフィールドに「**00:00:00:00**」と入力します。<br>• [Schedule] ：事前に定義されたスケジュールを使用して開始時間と期間を設定するには、このオプションを選択します。<br>[Schedule] ドロップダウン リストからスケジュールを選択します。新しいスケジュールを作成するには、[Create Schedule] をクリックします。 |
| [Policy] ドロップダウン リスト | デフォルトでは、次の抑制ポリシーが選択されます。<br>• **default-server-maint**：サーバの障害を抑制します。 |

**ステップ 7** **[OK]** をクリックします。

## 組織に対する障害抑制タスクの削除

この手順では、組織に対する障害抑制タスクをすべて削除します。タスクを個別に削除するには、[Suppression Tasks] ダイアログボックスで、[Delete] ボタンを使用します。組織に対する障害抑制タスクの表示 （49 ページ）を参照してください。

### 手順

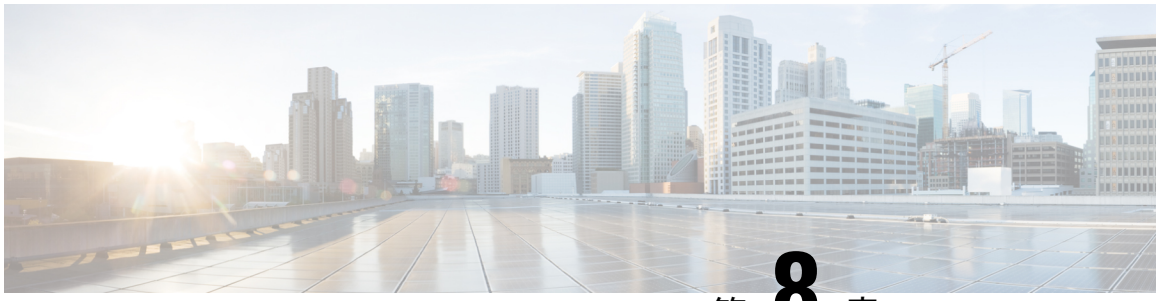
**ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。
**ステップ 2** **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
**ステップ 3** すべての障害抑制タスクを削除する組織をクリックします。
**ステップ 4** [Work] ペインで、[General] タブをクリックします。
**ステップ 5** [Actions] 領域で、[Stop Fault Suppression] をクリックします。
**ステップ 6** 確認ダイアログボックスが表示されたら、**[はい]**をクリックします。

## 組織に対する障害抑制タスクの表示

### 手順

**ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。
**ステップ 2** **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
**ステップ 3** 障害抑制タスク プロパティを表示する組織をクリックします。
**ステップ 4** [Work] ペインで、[General] タブをクリックします。
**ステップ 5** [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスでは、新しい障害抑制タスクの追加、既存の障害抑制タスクの削除、既存の障害抑制タスクの変更を行うことができます。



第 8 章

# SNMP の設定



## SNMP の概要

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP はネットワークデバイスのモニタリングや管理のための標準化されたフレームワークと共通言語を提供します。

### SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMPマネージャ：SNMPを使用してネットワークデバイスのアクティビティを制御し、モニタリングするシステム
- [SNMP エージェント（SNMP agent）]：Cisco UCS 内のソフトウェア コンポーネントであり、Cisco UCS のデータを維持し、必要に応じて SNMP マネージャにデータをレポートする管理対象デバイスです。Cisco UCS には、エージェントと MIB 収集が含まれます。SNMP エージェントを有効にしてマネージャとエージェント間のリレーションシップを作成するには、Cisco UCS Manager で SNMP を有効にして設定します。
- 管理情報ベース：SNMP エージェントの一連の管理対象オブジェクト。Cisco UCS リリース 1.4(1) 以降では、以前よりも多くの MIB をサポートしています。

Cisco UCS は、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。SNMP は次のように定義されています。

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）
- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

# SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco UCS Manager は、トラップまたはインフォームとして SNMP 通知を生成します。SNMP マネージャはトラップ受信時に確認応答を送信せず、Cisco UCS Manager はトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコルデータユニット（PDU）でメッセージの受信を確認します。Cisco UCS Manager が PDU を受信しない場合、インフォーム要求を再送できます。

# SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。セキュリティ モデルと選択したセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限のレベルによって、メッセージが情報開示の保護を必要とするか、またはメッセージが認証されるかが決定されます。サポートされるセキュリティ レベルは、実装されているセキュリティ モデルによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

# SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせを示します。

**表 *4 : SNMP* セキュリティ モデルおよびセキュリティ レベル**

| モデル | レベル | 認証 | 暗号化 | 結果 |
|---|---|---|---|---|
| v1 | noAuthNoPriv | コミュニティ ストリング | なし | コミュニティ ストリングの照合を使用して認証します。 |
| v2c | noAuthNoPriv | コミュニティ ストリング | なし | コミュニティ ストリングの照合を使用して認証します。 |
| v3 | noAuthNoPriv | ユーザ名 | 未対応 | ユーザ名の照合を使用して認証します。 |
| v3 | authNoPriv | HMAC-MD5 または HMAC-SHA | 未対応 | Hash-Based Message Authentication Code（HMAC）メッセージ ダイジェスト 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。 |
| v3 | authPriv | HMAC-MD5 または HMAC-SHA | DES | HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。 |

# SNMPv3 セキュリティ機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 は、管理操作および暗号化 SNMP メッセー

ジを実行するために、設定されているユーザーのみを承認します。SNMPv3 ユーザーベース セキュリティ モデル（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないこと、悪意なく起こり得る範囲を超えてデータ シーケンスが変更されていないことを保証します。
- メッセージの発信元の認証：メッセージ送信者の ID を確認できることを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

# Cisco UCS での SNMP サポート

Cisco UCS は、SNMP に対して以下のサポートを提供します。

### MIB のサポート

Cisco UCS は、MIB への読み取り専用アクセスをサポートします。

Cisco UCS で使用可能な特定の MIB およびその入手先については、B シリーズ サーバーは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html を、C シリーズは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html を参照してください。

### SNMPv3 ユーザーの認証プロトコル

Cisco UCS は、SNMPv3 ユーザーに次の認証プロトコルをサポートします。

- HMAC-MD5-96（MD5）
- HMAC-SHA-96（SHA）

### SNMPv3 ユーザーの AES プライバシー プロトコル

Cisco UCS は、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠しています。

プライバシー パスワード（priv オプション）では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。AES-128 の設定を有効にして、SNMPv3 ユーザー用のプライバシー パスワードを含めると、Cisco UCS Manager はそのプライバシー パスワードを使用して 128 ビット AES キーを生成します。AES priv パスワードは、8 文字以上にします。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

このようなユーザーを展開するには、[AES-128] 暗号化を有効にします。

# SNMP の有効化と SNMP プロパティの設定

Cisco UCS ドメインからの SNMP メッセージには、システム名ではなくファブリック インターコネクト名が表示されます。

### Procedure

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。

**ステップ 3** [通信サービス（Communication Services）] タブを選択します。

**ステップ 4** [SNMP] 領域で、次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [管理状態（Admin State）] フィールド | 次のいずれかになります。<br>• **有効**<br>• **無効**<br>システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。<br>**[管理状態（Admin State）]** が有効になっている場合は、Cisco UCS Manager GUIにこのセクションの残りのフィールドが表示されます。 |

**ステップ 5** **[Save Changes]**をクリックします。

### What to do next

SNMP トラップおよびユーザを作成します。

# SNMP トラップの作成

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。

**ステップ 3** [Communication Services] タブを選択します。

**ステップ 4** [SNMP Traps] 領域で、[+] をクリックします。

**ステップ 5** [Create SNMP Trap] ダイアログボックスで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [ホスト名（または IP アドレス）（Hostname (or IP Address)）] フィールド | Cisco UCS Manager がトラップを送信する SNMP ホストのホスト名または IP アドレス。<br>SNMP ホストには IPv4 アドレスまたは IPv6 アドレスを使用できます。ホスト名を IPv4 アドレスの完全修飾ドメイン名にすることもできます。 |
| [コミュニティ/ユーザ名（Community/Username）] フィールド | Cisco UCS Manager が SNMP ホストにトラップを送信するときに含める、SNMP v1 または v2c コミュニティ名、または SNMP v3 ユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。<br>1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?(疑問符)、&（アンパサンド）、または空のスペースは使用しないでください。 |
| [ポート（Port）] フィールド | トラップのために Cisco UCS Manager が SNMP ホストと通信するポート。<br>1 ～ 65535 の整数を入力します。デフォルトのポートは 162 です。 |
| **[バージョン（Version）]** フィールド | トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。<br>• **V1**<br>• **V2c**<br>• **V3** |
| [タイプ（Type）] フィールド | 送信するトラップのタイプ。バージョンに **V2c** または **V3** を選択する場合、送信するトラップのタイプは次のいずれかになります。<br>• **[Traps]**<br>• **情報** |
| [v3 特権（v3 Privilege）] フィールド | バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。<br>• [認証（Auth）]：認証あり、暗号化なし<br>• [認証なし（Noauth）]：認証なし、暗号化なし<br>• [秘密（Priv）]：認証あり、暗号化あり |

（注）　最大 8 つのホストを SNMP トラップに追加できます。

**ステップ 6** [OK] をクリックします。
**ステップ 7** **[Save Changes]**をクリックします。

# SNMP トラップの削除

手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。
**ステップ 2** **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。
**ステップ 3** [Communication Services] タブを選択します。
**ステップ 4** [SNMP Traps] 領域で、削除するユーザに対応するテーブルの行をクリックします。
**ステップ 5** テーブルの右側の [Delete] アイコンをクリックします。
**ステップ 6** 確認ダイアログボックスが表示されたら、**[はい]**をクリックします。
**ステップ 7** **[Save Changes]**をクリックします。

# SNMPv3 ユーザの作成

手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。
**ステップ 2** **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。
**ステップ 3** [Communication Services] タブを選択します。
**ステップ 4** [SNMP Users] 領域で、[+] をクリックします。
**ステップ 5** [Create SNMP User] ダイアログボックスで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [名前（Name）] フィールド | SNMP ユーザーに割り当てられるユーザー名。<br>32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、-（ハイフン）も指定できます。<br>（注）　ローカル側で認証されたユーザ名と同一の SNMP ユーザ名を作成することはできません。 |

| 名前 | 説明 |
|---|---|
| [Auth Type] フィールド | 許可タイプ。これはできるだけ**SHA**です。 |
| **Use aes-128** ] フィールド | かどうか、ユーザは、aes-128 暗号化を使用します。 |
| [パスワード（Password）] フィールド | このユーザのパスワード。 |
| [Confirm Password] フィールド | 確認のためのパスワードの再入力。 |
| [Privacy Password] フィールド | このユーザのプライバシー パスワード。 |
| [Confirm Privacy Password] フィールド | 確認のためのプライバシー パスワードの再入力。 |

**ステップ 6** [OK] をクリックします。

**ステップ 7** **[Save Changes]**をクリックします。

# SNMPv3 ユーザの削除

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。

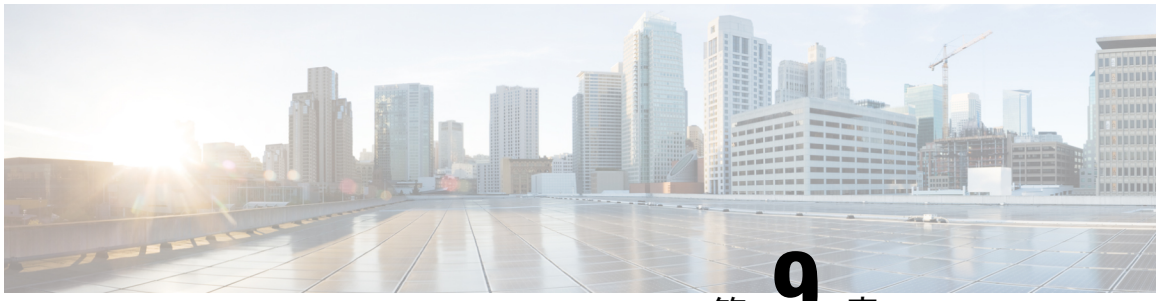
**ステップ 3** [Communication Services] タブを選択します。

**ステップ 4** [SNMP Users] 領域で、削除するユーザに対応するテーブルの行をクリックします。

**ステップ 5** テーブルの右側の [Delete] アイコンをクリックします。

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

**ステップ 7** **[Save Changes]**をクリックします。



第 9 章

# SPDM セキュリティ



# SPDM セキュリティ

Cisco UCS M6 サーバーには、デバイス自体に対する攻撃のベクトルを提供したり、デバイスを使用してシステム内の別のデバイスを攻撃したりする可能性のある可変コンポーネントが含まれている場合があります。これらの攻撃を防御するために、セキュリティ プロトコルおよびデータ モデル （SPDM）仕様では、デバイスがその ID と変更可能なコンポーネント構成の正確さを証明するように要求する安全なトランスポートの実装が可能になっています。この機能は、Cisco UCS Manager リリース 4.2(1d) 以降の Cisco UCS C220 および C240 M6 サーバーでサポートされています。

（注） SPDM は現在、Cisco UCS C225 M6サーバ および Cisco UCS C245 M6サーバ ではサポートされていません。

SPDMは、さまざまなトランスポートおよび物理メディアを介してデバイス間でメッセージ交換を実行するためのメッセージ、データ オブジェクト、およびシーケンスを定義します。これは、管理コンポーネント トランスポート プロトコル（MCTP）を介したベースボード管理コントローラ（BMC）とエンドポイント デバイス間のメッセージ交換を調整します。メッセージ交換には、BMC にアクセスするハードウェア ID の認証が含まれます。SPDM は、デバイス認証、ファームウェア測定、および証明書管理の管理レベルを指定することにより、低レベルのセキュリティ機能と操作へのアクセスを可能にします。エンドポイント デバイスは、認証を提供するように求められます。 BMC はエンドポイントを認証し、信頼できるエンティティのアクセスのみを許可します。

UCS Manager では、オプションで外部セキュリティ証明書を BMC にアップロードできます。ネイティブの内部証明書を含め、最大 40 の SPDM 証明書が許可されます。制限に達すると、

証明書をアップロードできなくなります。ユーザーがアップロードした証明書は削除できますが、内部/デフォルトの証明書は削除できません。

SPDM セキュリティ ポリシーでは、3 つのセキュリティ レベル設定のいずれかを指定できます。セキュリティは、次の 3 つのレベルのいずれかで設定できます。

- フル セキュリティ：

  これは、最高の MCTP セキュリティ設定です。この設定を選択した場合、エンドポイントの認証またはファームウェアの測定が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証またはファームウェア測定がサポートされていない場合にも、障害が生成されます。

- 部分的なセキュリティ (デフォルト):

  この設定を選択した場合、エンドポイントの認証またはファームウェアの測定が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証またはファームウェア測定がサポートされていない場合には、障害が生成されません。

- No Security

  この設定を選択した場合（エンドポイント測定やファームウェア測定が失敗しても）障害は発生しません。

1 つ以上の外部/デバイス証明書のコンテンツを BMC にアップロードすることもできます。SPDM ポリシーを使用すると、必要に応じてセキュリティ証明書または設定を変更または削除できます。証明書は、不要になったときに削除または置き換えることができます。

証明書は、システムのすべてのユーザー インターフェイスに一覧表示されます。

# SPDM セキュリティ ポリシーの作成

この手順では、SPDM ポリシーを作成します。

（注） 最大 40 の SPDM 証明書 (ネイティブ証明書を含む) をアップロードできます。

**手順**

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

**ステップ 2** **[ポリシー（Policies）]** に移動します。[root] ノードを展開します。

**ステップ 3** **[SPDM 証明書ポリシー（SPDM Certificate Policies）]** を右クリックして **[SPDM ポリシー（SPDM Policies の作成）]** を選択します。

**ステップ 4** このポリシーの名前を入力し、セキュリティ レベルとして **[障害アラート設定（Fault Alert Setting）]** を選択します：これは **[無効（Disabled）]**、**[一部（Partial）]**、または **[完全（Full）]** のいずれかです。

デフォルトは **[一部（Partial）]** です。

**ステップ 5** **[追加（Add）]**（**[ポリシーの作成（Create Policy）]** ウィンドウ）をクリックします。**[SPDM 証明書の追加（Add SPDM Certificate)]** ウィンドウが開きます。

**ステップ 6** 証明書に名前を付けます。

UCS Manager は、**Pem** 証明書のみをサポートします。

**ステップ 7** [証明書（Certificate）] フィールドに証明書の内容を貼り付けます。

**ステップ 8** **[OK]** をクリックして証明書を追加し、**[SPDM ポリシーの作成（Create SPDM Policy）]** ウィンドウに戻ります。

最大 40 件の証明書を追加できます。

**ステップ 9** **[SPDM ポリシーの作成（Create SPDM Policy）]** メニューで、**[OK]** をクリックします。

SPDMポリシーを作成してから、サーバールートポリシーの下で**SPDM証明書ポリシー（SPDM Certificate Policy）]** を選択すると、アラート設定とともにすぐにリストに表示されます。

### 次のタスク

証明書をサービス プロファイルに割り当てます。サービス プロファイルを有効にするには、サービス プロファイルをサーバーに関連付ける必要があります。

# セキュリティ ポリシーとサーバーの関連付け

### 始める前に

SPDM セキュリティ ポリシーの作成

### 手順

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

**ステップ 2** **[サービス プロファイル（Service Profiles）]** に移動します。[root] ノードを展開します。

**ステップ 3** 作成したポリシーに関連付けるサービス プロファイルを選択します。

a) **[ポリシー（Policies）]** タブで、下にスクロールして **[SPDM 証明書ポリシー（SPDM Certificate Policy）]**を展開します。**[SPDM 証明書ポリシー（SPDM Certificate Policy）]** ドロップダウンで、このサービスプロファイルに関連付ける目的のポリシーを選択します。

**ステップ 4** [OK] をクリックします。

SPDM ポリシーがこのサービス プロファイルに関連付けられます。

### 次のタスク

障害アラート レベルをチェックして、目的の設定に設定されていることを確認します。

# 障害アラート設定の表示

特定のシャーシに関連付けられている障害アラート設定を表示できます。

### 始める前に

ポリシーを作成して、それとサービス プロファイルを関連付けることができます。

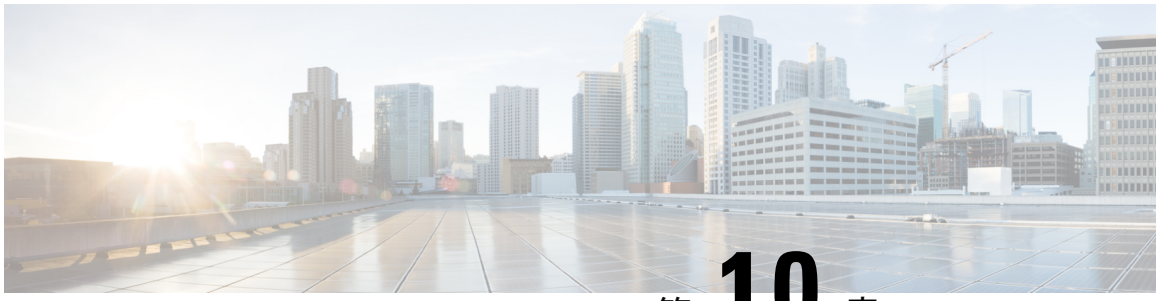
### 手順

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

**ステップ 2** ラックマウント サーバーを選択します。

**ステップ 3** **[インベントリ（Inventory）]** タブで **[CIMC]** を選択します。.

ユーザーがアップロードした証明書が一覧表示され、特定の証明書の情報を選択して表示できます。



第 10 章

# 統計情報収集ポリシーの設定



# 統計情報収集ポリシーの設定

## 統計情報収集ポリシー

統計情報収集ポリシーは、統計情報を収集する頻度（収集インターバル）、および統計情報を報告する頻度（報告インターバル）を定義します。複数の統計データ ポイントが報告インターバル中に収集できるように、報告インターバルは収集インターバルよりも長くなっています。これにより、最小値、最大値、および平均値を計算して報告するために十分なデータが Cisco UCS Manager に提供されます。

NIC 統計情報の場合、Cisco UCS Manager は最後の統計情報収集以降の平均値、最小値、最大値の変化を表示します。値が 0 の場合、最後の収集以降変化はありません。

統計情報は、Cisco UCS システムの次の 5 種類の機能エリアについて収集し、報告できます。

- アダプタ：アダプタに関連した統計情報
- シャーシ：シャーシに関連した統計情報
- ホスト：このポリシーは、将来サポートされる機能のためのプレースホルダで
- ポート：サーバ ポート、アップリンク イーサネット ポート、およびアップリンク ファイバ チャネル ポートを含むポートに関連した統計情報
- サーバ：サーバに関連した統計情報

（注） Cisco UCS Managerには、5 つの機能エリアそれぞれについて、デフォルト統計情報収集ポリシーが 1 つずつあります。追加で統計情報収集ポリシーを作成できません。また、既存のデフォルト ポリシーを削除できません。デフォルト ポリシーを変更することだけが可能です。

Cisco UCS Manager のデルタ カウンタに表示される値は、収集間隔内の最後の 2 つのサンプル間の差として計算されます。さらに、Cisco UCS Manager は、収集間隔内のサンプルの平均値、最小値、および最大値も表示します。

# 統計情報収集ポリシーの変更

## 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[All]** > **[Stats Management]** > **[Collection Policies]** の順に展開します。

**ステップ 3** 作業ウィンドウで、変更するポリシーを右クリックし、[Modify Collection Policy] を選択します。

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

| 名前 | 説明 |
|---|---|
| [名前（Name）] フィールド | 収集ポリシーの名前。<br>この名前は Cisco UCS によって割り当てられ、変更できません。 |
| **[Collection Interval]** フィールド | データのレコーディングから次のレコーディングまでファブリック インターコネクトが待機する時間の長さ。次のいずれかになります。<br>• **30 秒**<br>• **1 分**<br>• **2 分**<br>• **5 分** |

| 名前 | 説明 |
|---|---|
| **[Reporting Interval]** フィールド | カウンタについて収集されたデータが Cisco UCS Manager に送信されるまでファブリック インターコネクトが待機する時間の長さ。次のいずれかになります。<br>• **2 分**<br>• **15 分**<br>• **30 分**<br>• **60 分**<br>• **2 Hours**<br>• **4 時間**<br>• **8 Hours**<br>この時間が経過すると、ファブリック インターコネクトによって、Cisco UCS Manager に最後に情報を送信してから収集されたすべてのデータがグループ化され、そのグループから次の 4 種類の情報が抽出されて Cisco UCS Manager に送信されます。<br>• 最後に収集された統計情報<br>• このグループの統計情報の平均値<br>• このグループ内の最大値<br>• このグループ内の最小値<br>たとえば、収集インターバルを 1 分に設定し、報告インターバルを 15 分に設定した場合、ファブリック インターコネクトによって 15 分の報告インターバルに 15 個のサンプルが収集されます。Cisco UCS Manager に 15 個の統計情報が送信される代わりに、グループ全体の平均値、最小値、および最大値と一緒に最新のレコーディングだけが送信されます。 |
| [状態（States）] セクション | |
| [現在のタスク（Current Task）] フィールド | このコンポーネントの代わりに実行中のタスク。詳細については、関連する **[FSM]** タブを参照してください。<br>（注） 現在のタスクが存在しない場合、このフィールドは表示されません。 |

**ステップ 5** [OK] をクリックします。

# 統計情報しきい値ポリシーの設定

## 統計情報しきい値ポリシー

統計情報しきい値ポリシーは、システムの特定の側面についての統計情報をモニタし、しきい値を超えた場合にはイベントを生成します。最小値と最大値の両方のしきい値を設定できます。たとえば、CPUの温度が特定の値を超えた場合や、サーバを過度に使用していたり、サーバの使用に余裕がある場合には、アラームを発生するようにポリシーを設定できます。

これらのしきい値ポリシーが、CIMC などのエンドポイントに適用される、ハードウェアやデバイス レベルのしきい値を制御することはありません。このしきい値は、製造時にハードウェア コンポーネントに焼き付けられます。

Cisco UCSを使用して、次のコンポーネントに対して統計情報のしきい値ポリシーを設定できます。

- サーバおよびサーバ コンポーネント
- アップリンクのイーサネット ポート
- イーサネット サーバ ポート、シャーシ、およびファブリック インターコネクト
- ファイバ チャネル ポート

**Note** イーサネットサーバポート、アップリンクのイーサネットポート、またはアップリンクのファイバ チャネル ポートには、統計情報のしきい値ポリシーを作成したり、削除できません。既存のデフォルト ポリシーの設定だけを行うことができます。

Cisco UCS を使用して、サーバおよびサーバ コンポーネントに対して統計情報のしきい値ポリシーを設定できます。

## サーバおよびサーバ コンポーネントのしきい値ポリシーの作成

**ヒント** この手順では、[Server] タブでサーバおよびサーバ コンポーネントのしきい値ポリシーを作成する方法について説明します。これらのしきい値は、[LAN] タブ、[SAN] タブの [Policies] ノードの適切な組織内、および [Admin] タブの [Stats Management] ノードでも作成し、設定できます。

### 手順

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

**ステップ 2** **[サーバ]** > **[ポリシー]**を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、**[root]** ノードを展開します。

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

**ステップ 5** [Create Threshold Policy] ウィザードの [Define Name and Description] ページで、次の手順を実行します。

a) 次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [名前（Name）] フィールド | ポリシーの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **[説明（Description）]** フィールド | ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。<br>256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。 |
| [Owner] フィールド | 次のいずれかになります。<br>• [ローカル（Local）]：このポリシーは、この Cisco UCS ドメイン内のサービス プロファイルとサービス プロファイル テンプレートでのみ使用できます。<br>• [グローバル移行中（Pending Global）]：このポリシーの制御は、Cisco UCS Centralに移行中です。移行が完了すると、このポリシーは（Cisco UCS Centralに登録されている）すべての Cisco UCS ドメインで使用可能になります。<br>• [グローバル（Global）]：このポリシーは Cisco UCS Central で管理されます。このポリシーを変更する場合は、必ず Cisco UCS Central を使用してください。 |

b) [Next] をクリックします。

**ステップ 6** [Create Threshold Policy] ウィザードの [Threshold Classes] ページで、次の手順を実行します。

a) [Add] をクリックします。
b) [Choose Statistics Class] ダイアログボックスの [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。
c) [Next] をクリックします。

**ステップ 7** [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。

[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。
c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。
d) **[Alarm Triggers (Above Normal Value)]** フィールドで、次のチェックボックスの 1 つ以上をオンにします。

- **[Critical]**
- **メジャー**
- **マイナー**
- **警告**
- **条件**
- **Info**

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
f) **[Alarm Triggers (Below Normal Value)]** フィールドで、次のチェックボックスの 1 つ以上をオンにします。

- **情報**
- **条件**
- **警告**
- **Minor**
- **Major**
- **[Critical]**

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。

- クラスに別のしきい値のプロパティを定義するには、ステップ 7 を繰り返します。
- クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

**ステップ 8** [Create Threshold Policy] ウィザードの [Threshold Classes] ページで、次の手順を実行します。

- ポリシーの別のしきい値クラスを設定するには、ステップ 6 および 7 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

**ステップ 9** [OK] をクリックします。

# サーバおよびサーバ コンポーネントのしきい値ポリシーの削除

### 手順

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

**ステップ 2** **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

**ステップ 3** [Threshold Policies] ノードを展開します。

**ステップ 4** 削除するポリシーを右クリックし、[Delete] を選択します。

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

# 既存のサーバおよびサーバコンポーネントしきい値ポリシーへのしきい値クラスの追加

ヒント この手順では、[Server] タブでサーバおよびサーバ コンポーネントのしきい値ポリシーにしきい値クラスを追加する方法を示します。これらのしきい値は、[LAN] タブ、[SAN] タブの [Policies] ノードの適切な組織内、および [Admin] タブの [Stats Management] ノードでも作成し、設定できます。

### 手順

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

**ステップ 2** **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

**ステップ 3** [Threshold Policies] ノードを展開します。

**ステップ 4** しきい値クラスを追加するポリシーを右クリックして、[Create Threshold Class] を選択します。

**ステップ 5** [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。

b) [Next] をクリックします。

**ステップ 6** [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。

[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- **[Critical]**
- **メジャー**
- **マイナー**
- **警告**
- **条件**
- **Info**

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- **情報**
- **条件**
- **警告**
- **Minor**
- **Major**
- **[Critical]**

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

h) [Finish Stage] をクリックします。

i) 次のいずれかを実行します。

- クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
- クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

**ステップ 7** [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次のいずれかの手順を実行します。

- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

**ステップ 8** [OK] をクリックします。

# アップリンク イーサネット ポートしきい値ポリシーへのしきい値クラスの追加

ヒント　アップリンク イーサネット ポートしきい値ポリシーは作成できません。デフォルト ポリシーを修正または削除するだけです。

## 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[LANクラウド]**を展開します。

**ステップ 3** [Threshold Policies] ノードを展開します。

**ステップ 4** [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。

**ステップ 5** [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。

b) [Next] をクリックします。

**ステップ 6** [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。

[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- **[Critical]**
- メジャー
- マイナー
- 警告
- 条件
- **Info**

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - **情報**
   - **条件**
   - **警告**
   - **Minor**
   - **Major**
   - **[Critical]**

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。
   - クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
   - クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

**ステップ 7** [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。
- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

# イーサネット サービス ポート、シャーシ、およびファブリック インターコネクトのしきい値ポリシーへのしきい値クラスの追加

**ヒント** イーサネット サーバ ポート、シャーシ、およびファブリック インターコネクトのしきい値ポリシーは作成できません。デフォルト ポリシーを修正または削除するだけです。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。
**ステップ 2** **[LAN]** > **[Internal LAN]** の順に展開します。
**ステップ 3** [Threshold Policies] ノードを展開します。
**ステップ 4** [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。
**ステップ 5** [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。
b) [Next] をクリックします。

**ステップ 6** [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。

[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。
c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。
d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- **[Critical]**
- **メジャー**
- **マイナー**
- **警告**
- **条件**
- **Info**

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- **情報**
- **条件**
- **警告**
- **Minor**
- **Major**
- **[Critical]**

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。

- クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
- クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

**ステップ 7** [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。

- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。

• ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

# ファイバ チャネル ポートしきい値ポリシーへのしきい値クラスの追加

ファイバ チャネル ポートしきい値ポリシーは作成できません。デフォルト ポリシーを修正または削除するだけです。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。

**ステップ 2** **[SAN]** > **[SANクラウド]**を展開します。

**ステップ 3** [Threshold Policies] ノードを展開します。

**ステップ 4** [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。

**ステップ 5** [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。

b) [Next] をクリックします。

**ステップ 6** [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。

[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- **[Critical]**
- **メジャー**
- **マイナー**
- **警告**
- **条件**
- **Info**

e) [Up]フィールドおよび[Down]フィールドに、アラームを発行する値の範囲を入力します。

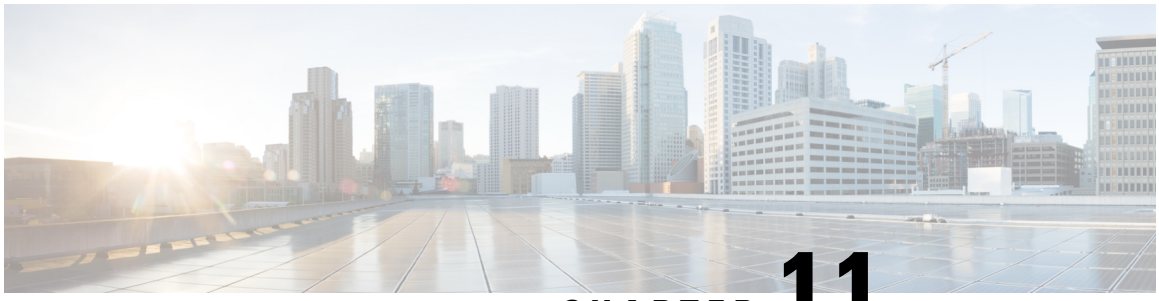
f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- **情報**
- **条件**
- **警告**
- **Minor**
- **Major**
- **[Critical]**

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。
   - クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
   - クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

**ステップ 7** [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。

- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。



CHAPTER 11

# Call Home および Smart Call Home の設定




# Call Home および Smart Call Home の設定


## UCS の Call Home の概要

Call Home では、重要なシステム ポリシーに対して電子メールベースの通知が提供されます。ポケットベル サービスや XML ベースの自動解析アプリケーションに対応可能なさまざまなメッセージ フォーマットが用意されています。この機能を使用して、ネットワーク サポート エンジニアにポケットベルで連絡したり、ネットワーク オペレーション センターに電子メールを送信したりできます。また、Cisco Smart Call Home サービスを使用して TAC のケースを生成できます。

Call Home 機能では、診断情報および環境の障害とイベントに関する情報が含まれるアラート メッセージを配信できます。

Call Home機能では、複数の受信者（Call Home宛先プロファイルと呼びます）にアラートを配信できます。各プロファイルには、設定可能なメッセージ フォーマットとコンテンツ カテゴリが含まれます。Cisco TAC へアラートを送信するための宛先プロファイルが事前に定義されていますが、独自の宛先プロファイルを定義することもできます。

メッセージを送信するようにCall Home を設定すると、Cisco UCS Manager によって適切な CLI **show** コマンドが実行され、コマンド出力がメッセージに添付されます。

Cisco UCS では、Call Home メッセージが次のフォーマットで配信されます。

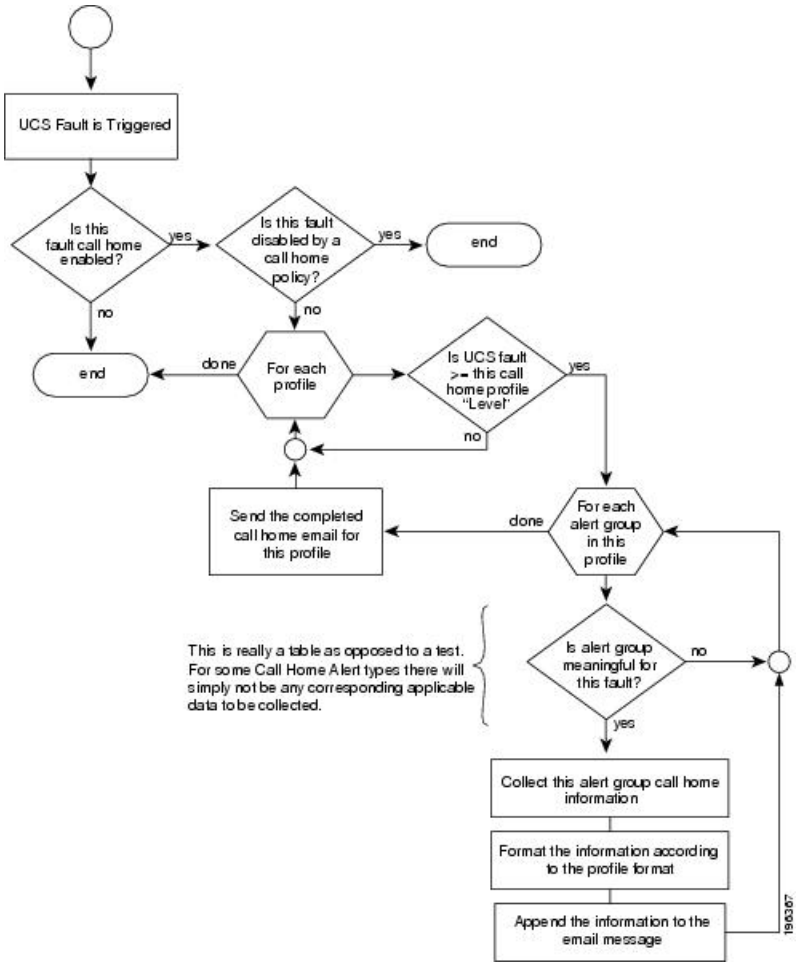
- 1 または 2 行で障害を説明する、ポケットベルや印刷レポートに適したショート テキスト フォーマット。
- 詳細な情報を十分に書式が整えられたメッセージで提供する、ユーザが読むのに適したフル テキスト フォーマット。
- Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用する、コンピュータで読み取り可能な XML フォーマット。AML

XSD は Cisco.com の Web サイトで公開されています。XML 形式は、シスコ Technical Assistance Center とのやり取りの中でも使用されます。

Call Home電子メールアラートをトリガする可能性がある障害についての情報は、『*Cisco UCS Faults and Error Messages Reference*』を参照してください。

次の図に、Call Home が設定されたシステムで Cisco UCS 障害がトリガーされた後のイベントの流れを示します。

**図 *2:* 障害発生後のイベントの流れ**




# Call Home の考慮事項とガイドライン

Call Home の設定方法は、機能の使用目的によって異なります。Call Home を設定する前に考慮すべき情報には次のものがあります。

### 宛先プロファイル

少なくとも 1 つの宛先プロファイルを設定する必要があります。使用する 1 つまたは複数の宛先プロファイルは、受信エンティティがポケットベル、電子メール、または自動化されたサービス（Cisco Smart Call Home など）のいずれであるかによって異なります。

宛先プロファイルで電子メール メッセージ配信を使用する場合は、Call Home を設定するときにシンプル メール転送プロトコル（SMTP）サーバーを指定する必要があります。

### 連絡先情報

受信者が Cisco UCS ドメインからの受信メッセージの発信元を判別できるように、連絡先の電子メール、電話番号、および所在地住所の情報を設定する必要があります。

システム インベントリを送信して登録プロセスを開始した後、Cisco Smart Call Home はこの電子メール アドレスに登録の電子メールを送信します。

電子メールアドレスに#(ハッシュ記号)、スペース、&(アンパサンド)などの特殊文字が含まれていると、電子メールサーバが電子メールメッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メール アドレスを使用することをお勧めします。

### 電子メール サーバーまたは HTTP サーバーへの IP 接続

ファブリック インターコネクトに、電子メール サーバーまたは宛先 HTTP サーバーへの IP 接続を与える必要があります。クラスタ設定の場合は、両方のファブリック インターコネクトに IP 接続を与える必要があります。この接続により、現在のアクティブなファブリック インターコネクトで Call Home 電子メール メッセージを送信できることが保証されます。これらの電子メール メッセージの発信元は、常にファブリック インターコネクトの IP アドレスになります。クラスタ設定で Cisco UCS Manager に割り当てられた仮想 IP アドレスが、電子メールの発信元になることはありません。

（注） SMTP サーバに必ず各ファブリック インターコネクト IP を追加してください。ファブリック インターコネクト IP が SMTP サーバに設定されていない場合、Call Home 電子メールメッセージは配信できません。

### Smart Call Home

Cisco Smart Call Home を使用する場合は、次のことが必要です。

- 設定するデバイスが、有効なサービス契約でカバーされている必要があります。
- Cisco UCS 内で Smart Call Home 設定と関連付けられるカスタマー ID は、Smart Call Home が含まれるサポート契約と関連付けられている CCO（Cisco.com）アカウント名にする必要があります。

# Cisco UCSの障害と Call Home のシビラティ（重大度）

Call Home は複数の Cisco 製品ラインにまたがって存在するため、独自に標準化されたシビラティ（重大度）があります。次の表に、基礎をなす Cisco UCS の障害レベルと Call Home のシビラティ（重大度）とのマッピングを示します。Call Home のプロファイルにレベルを設定するときには、このマッピングを理解しておくことが必要です。

**表 *5:* 障害と *Call Home* のシビラティ（重大度）のマッピング**

| Call Home のシビラティ（重大度） | Cisco UCS の障害 | Call Home での意味 |
|---|---|---|
| (9) Catastrophic | 該当なし | ネットワーク全体に壊滅的な障害が発生しています。 |
| (8) Disaster | 該当なし | ネットワークに重大な影響が及びます。 |
| (7) Fatal | 該当なし | システムが使用不可能な状態。 |
| (6) Critical | Critical | クリティカルな状態、ただちに注意が必要。 |
| (5) Major | Major | 重大な状態。 |
| (4) Minor | Minor | 軽微な状態。 |
| (3) Warning | Warning | 警告状態。 |
| (2) Notification | Info | 基本的な通知と情報メッセージ。他と関係しない、重要性の低い障害です。 |
| (1) Normal | Clear | 通常のイベント。通常の状態に戻ることを意味します。 |
| (0) debug | 該当なし | デバッグ メッセージ。 |

## Anonymous Reporting

Cisco UCS Managerの最新リリースにアップグレードすると、デフォルトでは、Anonymous Reporting をイネーブルにするようにダイアログボックスで指示されます。

Anonymous Reporting をイネーブルにするには、SMTP サーバおよびファブリック スイッチに保存するデータ ファイルの詳細を入力する必要があります。このレポートは7日ごとに生成され、同じレポートの以前のバージョンと比較されます。Cisco UCS Manager がレポートでの変更を識別すると、レポートが電子メールとして送信されます。

## Anonymous Reporting のイネーブル化

（注） Anonymous Reporting は、Call Home がディセーブルである場合でもイネーブルにできます。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Actions] 領域で、[Anonymous Reporting Data] をクリックしてサンプルまたは既存のレポートを表示します。

**ステップ 5** [Properties] ペインで、[Anonymous Reporting] フィールドの次のいずれかのオプション ボタンをクリックします。

- [On] ：サーバが匿名レポートを送信できるようにします。
- [Off] ：サーバが匿名レポートを送信できないようにします。

**ステップ 6** [SMTP Server] 領域で、anonymous reporting が電子メール メッセージを送信する SMTP サーバに関する情報を次のフィールドに入力します。

- [Host (IP Address or Hostname)]：SMTP サーバの IPv4 または IPv6 アドレス、あるいはホスト名。
- [Port]：システムが SMTP サーバとの通信で使用するポート番号。

  1 ～ 65535 の整数を入力します。デフォルトは 25 です。

**ステップ 7** **[Save Changes]**をクリックします。

## Call Home の設定

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Admin] 領域で、次のフィールドに入力して [Call Home] をイネーブルにします。

| 名前 | 説明 |
|---|---|
| [状態（State）] フィールド | 次のいずれかになります。<br>• [オフ（Off）]：Call Home はこの Cisco UCS ドメインには使用されません。<br>• [オン（On）]：Cisco UCSでは、システムで定義されている Call Home ポリシーやプロファイルに基づいて Call Home アラートが生成されます。<br>（注） このフィールドを [オン（On）] に設定すると、Cisco UCS Manager GUIはこのタブに残りのフィールドを表示します。 |
| [スイッチの優先順位（Switch Priority）] ドロップダウン リスト | 次のいずれかになります。<br>• **アラート（Alerts）**<br>• **クリティカル（Critical）**<br>• **デバッグ（Debugging）**<br>• **緊急事態（Emergencies）**<br>• **エラー（Errors）**<br>• **情報（Information）**<br>• **通知（Notifications）**<br>• **警告（Warnings）** |
| [スロットリング（Throttling）] フィールド | 同じイベントについて重複して受信するメッセージの数を制限するかどうかを指定します。次のいずれかになります。<br>• [オン（ON）]：送信された重複メッセージの数が 2 時間以内に 30 件を超えると、そのアラート タイプに関するそれ以降のメッセージは破棄されます。<br>• [オフ（Off）]:検出された数に関係なく、重複するメッセージのすべてが送信されます。 |

a) [状態（State）] フィールド で、[On] をクリックします。

（注） このフィールドを [オン（On）] に設定すると、Cisco UCS Manager GUIはこのタブに残りのフィールドを表示します。

b) [スイッチの優先順位（Switch Priority）] ドロップダウン リストから、次のいずれかのレベルを選択します。

• **アラート（Alerts）**

- クリティカル（Critical）
- デバッグ（Debugging）
- 緊急事態（Emergencies）
- エラー（Errors）
- 情報（Information）
- 通知（Notifications）
- 警告（Warnings）

ファブリック インターコネクトの複数のペアがある大規模な Cisco UCS の展開の場合は、メッセージの受信者がメッセージの優先順位を判断できるようこのフィールドを使用して特定の 1 つの Cisco UCS ドメインからのメッセージにシビラティ（重大度）を割り当てることができます。このフィールドは、小規模な Cisco UCS の展開（単一の Cisco UCS ドメイン など）には有用でないことがあります。

**ステップ 5** [Contact Information] 領域で、次のフィールドに必要な連絡先情報を入力します。

| 名前 | 説明 |
|---|---|
| [連絡先（Contact）] フィールド | 主要 Call Home 連絡先。<br>255 文字以下の ASCII 文字で入力します。 |
| [電話（Phone）] フィールド | 主要連絡先の電話番号。<br>+（プラス記号）と国番号から始まる国際形式の番号を入力します。ハイフンは使用できますが、カッコは使用できません。 |
| [電子メール（Email）] フィールド | 主要連絡先の電子メール アドレス。<br>Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。<br>（注） 電子メールアドレスに# (ハッシュ記号)、スペース、& (アンパサンド)などの特殊文字が含まれていると、電子メールサーバが電子メールメッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メール アドレスを使用することをお勧めします。 |
| [アドレス（Address）] フィールド | 主要連絡先の住所。<br>255 文字以下の ASCII 文字で入力します。 |

**ステップ 6** [Ids] 領域で、Call Home が使用する ID 情報を次のフィールドに入力します。

ヒント Smart Call Home を設定しない場合は、この手順を省略できます。

| 名前 | 説明 |
|---|---|
| [顧客 ID（Customer Id）] フィールド | ライセンス上のサポート契約の契約番号を含む Cisco.com ID。<br>510 文字以下の ASCII 文字を入力します。 |
| [連絡先 ID（Contract Id）] フィールド | お客様の Call Home 契約番号。<br>510 文字以下の ASCII 文字を入力します。 |
| [サイト ID（Site Id）] フィールド | お客様のサイトに固有の Call Home ID。<br>510 文字以下の ASCII 文字を入力します。 |

**ステップ 7** [Email Addresses] 領域で、Call Home アラート メッセージの電子メール情報を次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| **[開始]** フィールド | システムによって送信される Call Home アラート メッセージの [送信者（From）] フィールドに表示される電子メール アドレス。 |
| [返信先（Reply To）] フィールド | システムによって送信される Call Home アラート メッセージの [宛先（To）] フィールドに表示される電子メール アドレス。 |

**ステップ 8** [SMTP Server] 領域で、Call Home が電子メール メッセージを送信する SMTP サーバーに関する情報を次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [ホスト（IP アドレスまたはホスト名）（Host (IP Address or Hostname)）] フィールド | SMTP サーバの IPv4 または IPv6 アドレスまたはホスト名。<br>（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Managerで DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。 |
| [ポート（Port）] フィールド | SMTP サーバとの通信に使用されるポート番号。<br>1 ～ 65535 の整数を入力します。デフォルトは 25 です。 |

**ステップ 9** **[Save Changes]**をクリックします。

## Call Home のディセーブル化

この手順は任意です。

Cisco UCS ドメインをアップグレードすると、アップグレードプロセスを完了するために Cisco UCS Manager によってコンポーネントが再起動されます。この再起動によって、サービスの中断およびコンポーネントの障害と同じイベントが発生し、Call Home アラートの送信がトリガーされます。アップグレードの開始前に Call Home をディセーブルにしない場合は、アップグレードに関連したコンポーネントの再起動によって生成されるアラートを無視してください。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Admin] 領域で、[状態（State）] フィールド で [Off] をクリックします。

（注） このフィールドを [Off] に設定すると、Cisco UCS Manager はこのタブの残りのフィールドを非表示にします。

**ステップ 5** **[Save Changes]**をクリックします。

## Call Home のイネーブル化

この手順は任意です。ファームウェアのアップグレードを開始する前に Call Home をディセーブルにした場合にのみ、イネーブルにする必要があります。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Admin] 領域で、[状態（State）] フィールド [On] をクリックします。

（注） このフィールドを [オン（On）] に設定すると、Cisco UCS Manager GUIはこのタブに残りのフィールドを表示します。

**ステップ 5** **[Save Changes]**をクリックします。

### 次のタスク

Call Home が完全に設定されていることを確認します。

## システム インベントリ メッセージの設定

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Properties] 領域で、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Send Periodically] フィールド | このフィールドを **[on]** に設定すると、Cisco UCS によってシステム インベントリが Call Home データベースに送信されます。この情報がいつ送信されるかは、この領域の他のフィールドによって決まります。 |
| [Send Interval] フィールド | 自動システム インベントリ データ収集の間隔（日数）。<br>1 ～ 30 の整数を入力します。 |
| [Hour of Day to Send] フィールド | データを送信する時間（24 時間時計形式）。 |
| [Minute of Hour] フィールド | データを送信する時間（分数）。 |
| [Time Last Sent] フィールド | 情報が最後に送信された日時。<br>（注） このフィールドは、最初のインベントリが送信された後に表示されます。 |
| [Next Scheduled] フィールド | 次のデータ収集の日時。<br>（注） このフィールドは、最初のインベントリが送信された後に表示されます。 |

**ステップ 5** **[Save Changes]**をクリックします。

## システム インベントリ メッセージの送信

スケジュール済みメッセージ以外のシステム インベントリ メッセージを手動で送信する必要がある場合は、この手順を使用します。

（注） システム インベントリ メッセージは、CiscoTAC-1 プロファイルで定義された受信者だけに送信されます。

**手順**

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Actions] 領域で [Send System Inventory Now] をクリックします。

Cisco UCS Manager は、ただちに Call Home に設定された受信者にシステム インベントリ メッセージを送信します。

## Call Home プロファイルの設定

### Call Home プロファイル

Call Home プロファイルは、指定した受信者に送信されるアラートを決定します。プロファイルを設定して、必要なシビラティ（重大度）のイベントと障害に対する電子メール アラート、およびアラートのカテゴリを表す特定のアラート グループに対する電子メール アラートを送信できます。また、これらのプロファイルを使用して特定の受信者およびアラート グループのセットに対してアラートの形式を指定することもできます。

アラート グループおよびCall Homeプロファイルによって、アラートをフィルタリングし、特定のプロファイルがアラートの特定のカテゴリだけを受信できるようにすることができます。たとえば、データセンターにはファンおよび電源の問題を処理するハードウェア チームがある場合があります。このハードウェア チームは、サーバのPOST障害やライセンスの問題は扱いません。ハードウェア チームが関連したアラートだけを受信するようにするには、ハードウェア チームの Call Home プロファイルを作成し、「環境」アラート グループだけをチェックします。

デフォルトでは、Cisco TAC-1 プロファイルを設定する必要があります。指定したレベルのイベントが発生したときに電子メール アラートを 1 つ以上のアラート グループに送るための追加プロファイルを作成し、それらのアラートについて適切な量の情報とともに受信者を指定することもできます。

たとえば、高いシビラティ（重大度）の障害に対して次の 2 つのプロファイルを設定できます。

- アラート グループにアラートを送信する短いテキスト形式のプロファイル。このグループのメンバーは、障害に関する 1 ～ 2 行の説明を受け取ります（この説明を使用して問題を追跡できます）。

- CiscoTAC アラート グループにアラートを送信する XML 形式のプロファイル。このグループのメンバーは、マシンが読み取り可能な形式で詳細なメッセージを受け取ります（Cisco Systems Technical Assistance Center 推奨）。

## Call Home アラート グループ

アラート グループは、事前定義された Call Home アラートのサブセットです。アラート グループを使用すると、事前定義されたまたはカスタムの Call Home プロファイルに送信する一連の Call Home アラートを選択できます。Cisco UCS Manager は、次の条件下でのみ、接続先プロファイルの電子メール接続先に Call Home アラートを送信します。

- Call Home アラートが、その宛先プロファイルに関連付けられているアラート グループのいずれかに属する場合。
- 宛先プロファイルに設定されているメッセージの重要度以上の Call Home メッセージの重要度をアラートが持つ場合。

Cisco UCS Manager が生成する各アラートは、アラート グループによって表されるカテゴリに分けられます。次の表では、それらのアラート グループについて説明します。

| アラート グループ | 説明 |
|---|---|
| Cisco TAC | Smart Call Home 宛ての、他のアラート グループからのすべてのクリティカル アラート。 |
| Diagnostic | サーバの POST の完了など診断によって生成されたイベント。 |
| 環境 | 電源、ファン、および温度アラームなどの環境検知要素に関連するイベント。<br>（注） ファンまたは PSU がシャーシから手動で取り外された場合、Call Home アラートは生成されません。これは設計によるものです。 |

## Call Home プロファイルの作成

デフォルトでは、Cisco TAC-1 プロファイルを設定する必要があります。しかし、プロファイルを追加作成することにより、指定したレベルでイベントが発生したときに、指定された 1 つ以上のグループにアラート メールを送信することもできます。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** テーブルの右側のアイコン バーで、[+] をクリックします。

[+] アイコンが無効になっている場合、テーブルのいずれかのエントリをクリックして、有効にします。

**ステップ 5** [Call Home プロファイルの作成（Create Call Home Profile）] ダイアログボックスで、次の情報フィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [名前（Name）] フィールド | このプロファイルのユーザ定義名。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| [レベル（Level）] フィールド | Cisco UCS の障害がこのレベル以上の場合は、プロファイルがトリガーされます。次のいずれかになります。<br>• **クリティカル（Critical）**<br>• **[デバッグ（Debug）]**<br>• **障害**<br>• **[致命的（Fatal）]**<br>• **メジャー**<br>• **マイナー**<br>• **標準**<br>• **通知**<br>• **警告** |
| [アラート グループ（Alert Groups）] フィールド | この Call Home プロファイルに基づいて警告されるグループ。次の中から 1 つ以上選択できます。<br>• [Cisco Tac]：Cisco TAC の受信者<br>• [診断（Diagnostic）]：POST 完了サーバ障害通知の受信者<br>• [環境（Environmental）]：PSU、ファンなどの問題に関する通知の受信者 |

**ステップ 6** [E メールの設定（Email Configuration）] 領域で、次のフィールドに値を入力して電子メールアラートを設定します。

| 名前 | 説明 |
|---|---|
| [形式（Format）] フィールド | 次のいずれかになります。<br>• [xml]：Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用するマシンが読み取り可能な形式。この形式により、Cisco Systems Technical Assistance Center との通信が可能になります。<br>• [フル テキスト（Full Txt）]：人間が判読するのに適している完全にフォーマットされた、詳細な情報を含むメッセージ。<br>• [ショート テキスト（Short Txt）：ポケットベルまたは印刷されたレポートに適している 1 ～ 2 行の障害の説明。 |
| [最大メッセージサイズ（Max Message Size）] フィールド | 指定された Call Home 受信者に送信される最大メッセージ サイズ。<br>1 ～ 5,000,000 の範囲の整数を入力します。デフォルト値は 5,000,000 です。<br>フルテキスト メッセージおよび XML メッセージの推奨最大サイズは 5,000,000 です。ショートテキスト メッセージの推奨最大サイズは 100,000 です。Cisco TAC アラート グループの場合、最大メッセージ サイズは 5,000,000 に制限されます。 |

**ステップ 7** [受信者（Recipients）] 領域で次の操作を行って電子メール アラートの受信者を 1 つ以上追加します。

a) テーブルの右側のアイコン バーで、[+] をクリックします。

b) [メール受信者を追加（Add Email Recipients）] ダイアログボックスで、[電子メール（Email）] フィールドで Call Home アラートを送信する宛先メール アドレスを入力します。

入力したメール アドレスで Callhome アラート/障害を受信するようになります。

保存した電子メール アドレスは削除できますが、変更はできません。

c) [OK] をクリックします。

**ステップ 8** [OK] をクリックします。

## Call Home プロファイルの削除

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** 削除するプロファイルを右クリックし、[削除（Delete）] を選択します。

**ステップ 5** **[Save Changes]**をクリックします。

## Call Home ポリシーの設定

### Call Home ポリシー

Call Home ポリシーは、特定の種類の障害またはシステム イベントに対して Call Home アラートを送信するかどうかを決定します。デフォルトでは、特定の種類の障害およびシステム イベントに対してアラートを送信するよう Call Home がイネーブルになります。

（注） デフォルトの障害やシステム イベントを処理しないように Cisco UCS Manager を設定できます。

ある種類の障害またはイベントに対してアラートを無効にするには、まず最初にその種類に対して Call Home ポリシーを作成し、次にそのポリシーを無効にします。

### Call Home ポリシー

ヒント デフォルトでは、すべての Call Home ポリシーが有効になっており、重要なシステム イベントすべてについてアラートが電子メールで送信されます。

**手順**

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** テーブルの右側のアイコン バーで、[+] をクリックします。

[+] アイコンが無効になっている場合、テーブルのいずれかのエントリをクリックして、有効にします。

**ステップ 5** [Call Home ポリシーの作成（Create Call Home Policy）] ダイアログボックスで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [状態（State）] フィールド | このフィールドが **[有効（Enabled）]** の場合、関連付けられた原因と一致するエラーが発生した際にシステムはこのポリシーを使用します。それ以外の場合、一致するエラーが発生しても、システムはこのポリシーを無視します。デフォルトでは、すべてのポリシーが有効になります。 |
| [原因（Cause）] フィールド | このアラートをトリガーするイベント。各ポリシーは、アラートをイベント タイプごとに送信するかを定義します。 |

**ステップ 6** [OK] をクリックします。

**ステップ 7** 異なる種類の障害またはイベントに Call Home ポリシーを設定する場合は、ステップ 4 および 5 を繰り返します。

## Call Home ポリシーのディセーブル化

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** ディセーブルにするポリシーを右クリックし、[Show Navigator] を選択します。

**ステップ 5** [State] フィールドで、[Disabled] をクリックします。

**ステップ 6** [OK] をクリックします。

## Call Home ポリシーのイネーブル化

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** イネーブルにするポリシーを右クリックし、[Show Navigator] を選択します。

**ステップ 5** [State] フィールドで、[Enabled] をクリックします。

**ステップ 6** [OK] をクリックします。

### Call Home ポリシーの削除

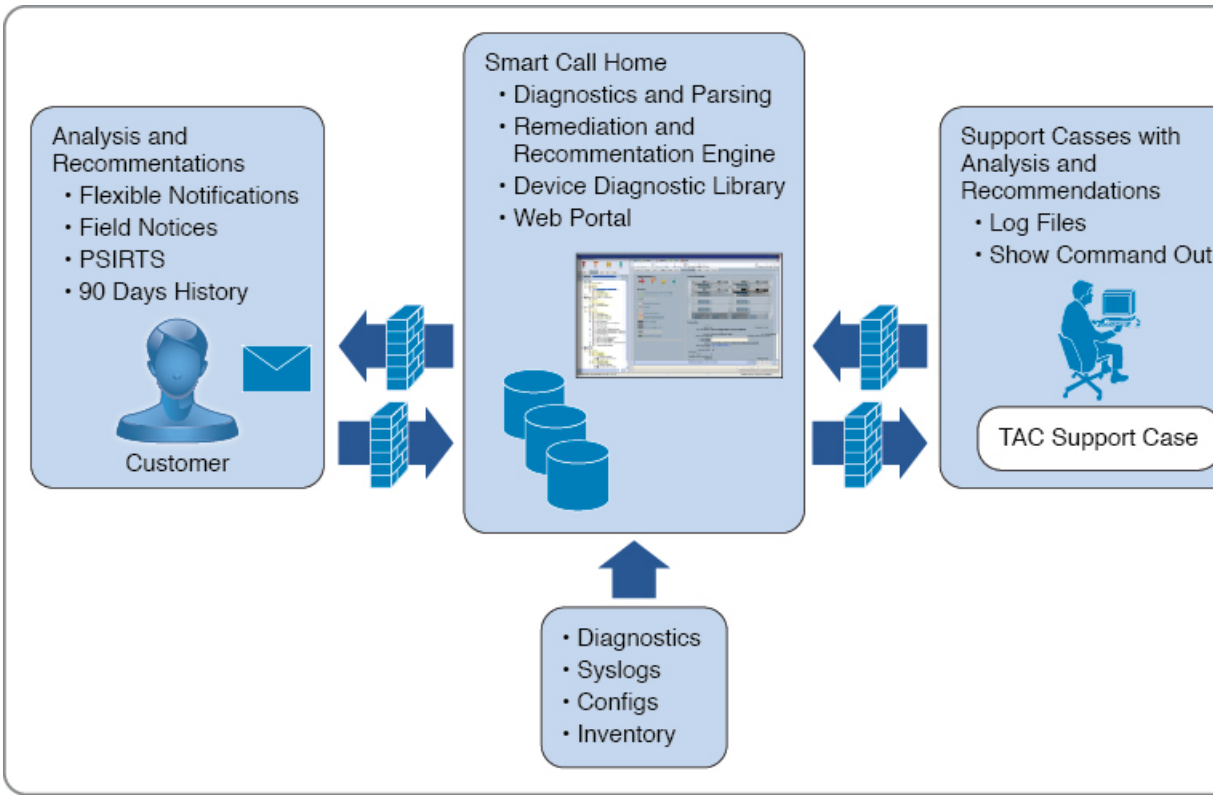
手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。
**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。
**ステップ 3** [Work] ペインの [Call Home Policies] タブをクリックします。
**ステップ 4** 無効にするポリシーを右クリックし、[削除（Delete）] を選択します。
**ステップ 5** **[Save Changes]**をクリックします。

## Cisco Smart Call Home

Cisco Smart Call Home は、Cisco UCS の Call Home 機能を強化する Web アプリケーションです。Smart Call Home により、予防的な診断および重要なシステム イベントのリアルタイムの電子メール アラートが提供されます。それにより、ネットワークの可用性が高まり、運用効率が向上します。Smart Call Home は、Cisco UCS の Cisco Unified Computing Support Service と Cisco Unified Computing Mission Critical Support Service によって提供されるセキュア接続のサービスです。

図 *3 : Cisco Smart Call Home* の機能



（注） Smart Call Home を使用するには、次のものが必要です。

- 対応する Cisco Unified Computing Support Service 契約または Cisco Unified Computing Mission Critical Support Service 契約と関連付けられた Cisco.com ID。
- 登録されるデバイス用の Cisco Unified Computing Support Service または Cisco Unified Computing Mission Critical Support Service

Smart Call Home 電子メール アラートを Smart Call Home System またはセキュアな Transport Gateway のいずれかに送信するように、Cisco UCS Manager を設定し、登録できます。セキュアな Transport Gateway に送信された電子メール アラートは、HTTPS を使用して Smart Call Home System に転送されます。

（注） セキュリティ上の理由から、Transport Gateway オプションの使用を推奨します。Transport Gateway は、Cisco.com からダウンロードできます。

Smart Call Home を設定するには、次の手順を実行します。

- Smart Call Home 機能をイネーブルにします。
- 連絡先情報を設定します。
- 電子メール情報を設定します。
- SMTP サーバ情報を設定します。
- デフォルトの CiscoTAC-1 プロファイルを設定します。

（注） Callhome sendtestAlert 機能を適用するには、電子メールの接続先の少なくとも 1 つを CiscoTAC-1 以外のプロファイルに設定する必要があります。

- Smart Call Home インベントリ メッセージを送信して、登録プロセスを開始します。
- Call Home カスタマー ID として Cisco UCS ドメイン に使用する予定の Cisco.com ID にその資格として登録の契約番号が追加されていることを確認します。この ID は、Cisco.com の Profile Manager の [Additional Access] の下にある [Account Properties] 内で更新できます。

# Smart Call Home の設定

手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Admin] 領域で次の作業を行い、Call Home をイネーブルにします。

a) [状態（State）] フィールド で、[On] をクリックします。

（注） このフィールドを [オン（On）] に設定すると、Cisco UCS Manager GUIはこのタブに残りのフィールドを表示します。

b) [スイッチの優先順位（Switch Priority）] ドロップダウン リストから、次のいずれかの緊急度レベルを選択します。

- **アラート（Alerts）**
- **クリティカル（Critical）**
- **デバッグ（Debugging）**
- **緊急事態（Emergencies）**
- **エラー（Errors）**
- **情報（Information）**
- **通知（Notifications）**
- **警告（Warnings）**

**ステップ 5** 同じイベントについて重複して受信するメッセージの数を制限するかどうかを指定します。次のいずれかになります。

- [オン（ON）] : 送信された重複メッセージの数が 2 時間以内に 30 件を超えると、そのアラート タイプに関するそれ以降のメッセージは破棄されます。
- [オフ（Off）]:検出された数に関係なく、重複するメッセージのすべてが送信されます。

**ステップ 6** [Contact Information] 領域で、次のフィールドに必要な連絡先情報を入力します。

| 名前 | 説明 |
|---|---|
| [連絡先（Contact）] フィールド | 主要 Call Home 連絡先。<br>255 文字以下の ASCII 文字で入力します。 |

| 名前 | 説明 |
|---|---|
| [電話（Phone）] フィールド | 主要連絡先の電話番号。<br>+（プラス記号）と国番号から始まる国際形式の番号を入力します。ハイフンは使用できますが、カッコは使用できません。 |
| [電子メール（Email）] フィールド | 主要連絡先の電子メール アドレス。<br>Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。<br>（注） 電子メールアドレスに# (ハッシュ記号)、スペース、& (アンパサンド)などの特殊文字が含まれていると、電子メールサーバが電子メールメッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メール アドレスを使用することをお勧めします。 |
| [アドレス（Address）] フィールド | 主要連絡先の住所。<br>255 文字以下の ASCII 文字で入力します。 |

**ステップ 7** [Ids] 領域で、次のフィールドに Smart Call Home ID 情報を入力します。

| 名前 | 説明 |
|---|---|
| [顧客 ID（Customer Id）] フィールド | ライセンス上のサポート契約の契約番号を含む Cisco.com ID。<br>510 文字以下の ASCII 文字を入力します。 |
| [連絡先 ID（Contract Id）] フィールド | お客様の Call Home 契約番号。<br>510 文字以下の ASCII 文字を入力します。 |
| [サイト ID（Site Id）] フィールド | お客様のサイトに固有の Call Home ID。<br>510 文字以下の ASCII 文字を入力します。 |

**ステップ 8** [Email Addresses] 領域で、次のフィールドに Smart Call Home アラート メッセージの電子メール情報を入力します。

| 名前 | 説明 |
|---|---|
| **[開始]** フィールド | システムによって送信される Call Home アラート メッセージの [送信者（From）] フィールドに表示される電子メール アドレス。 |
| [返信先（Reply To）] フィールド | システムによって送信される Call Home アラート メッセージの [宛先（To）] フィールドに表示される電子メール アドレス。 |

**ステップ 9** [SMTP Server] 領域で、次のフィールドに Call Home が電子メール メッセージを送信するために使用する SMTP サーバに関する情報を入力します。

| 名前 | 説明 |
|---|---|
| [ホスト（IP アドレスまたはホスト名）（Host (IP Address or Hostname)）] フィールド | SMTP サーバの IPv4 または IPv6 アドレスまたはホスト名。<br>（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。 |
| [ポート（Port）] フィールド | SMTP サーバとの通信に使用されるポート番号。<br>1 ～ 65535 の整数を入力します。デフォルトは 25 です。 |

**ステップ 10** **[Save Changes]**をクリックします。

## デフォルトの Cisco TAC-1 プロファイルの設定

CiscoTAC-1 プロファイルのデフォルト設定は次のとおりです。

（注） Callhome sendtestAlert 機能を適用するには、電子メールの接続先の少なくとも 1 つを CiscoTAC-1 以外のプロファイルに設定する必要があります。

- レベルは標準です
- CiscoTAC 警報グループだけが選択されています
- 形式は xml です
- 最大メッセージ サイズは 5000000 です

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。
**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。
**ステップ 3** [Work] ペインで、[Profiles] タブをクリックします。

**ステップ 4** Cisco TAC-1 プロファイルを右クリックし、[Recipient] を選択します。

**ステップ 5** [Add Email Recipients] ダイアログボックスで、次の手順を実行します。

a) [電子メール（Email）] フィールドで、Call Home アラートの送信先の電子メール アドレスを入力します。

たとえば、「callhome@cisco.com」と入力します。

保存した電子メール アドレスは削除できますが、変更はできません。

b) [OK] をクリックします。

## Smart Call Home に対するシステム インベントリ メッセージの設定

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Properties] 領域で、次のフィールドに値を入力して、システム インベントリ メッセージを Smart Call Home に送信する方法を指定します。

| 名前 | 説明 |
|---|---|
| [Send Periodically] フィールド | このフィールドを **[on]** に設定すると、Cisco UCS によってシステム インベントリが Call Home データベースに送信されます。この情報がいつ送信されるかは、この領域の他のフィールドによって決まります。 |
| [Send Interval] フィールド | 自動システム インベントリ データ収集の間隔（日数）。<br>1 ～ 30 の整数を入力します。 |
| [Hour of Day to Send] フィールド | データを送信する時間（24 時間時計形式）。 |
| [Minute of Hour] フィールド | データを送信する時間（分数）。 |
| [Time Last Sent] フィールド | 情報が最後に送信された日時。<br>（注） このフィールドは、最初のインベントリが送信された後に表示されます。 |
| [Next Scheduled] フィールド | 次のデータ収集の日時。<br>（注） このフィールドは、最初のインベントリが送信された後に表示されます。 |

**ステップ 5** **[Save Changes]**をクリックします。

## Smart Call Home の登録

### 手順

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]** > **[Call Home]**を展開します。

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

**ステップ 4** [Actions] 領域で [Send System Inventory Now] をクリックし、登録プロセスを開始します。

シスコがシステム インベントリを受信すると、Smart Call Home の登録電子メールが、[General] タブの [Contact Information] 領域で設定した電子メール アドレスに送信されます。

**ステップ 5** シスコから登録電子メールを受信したら、Smart Call Home の登録を完了するために、次の手順を実行します。

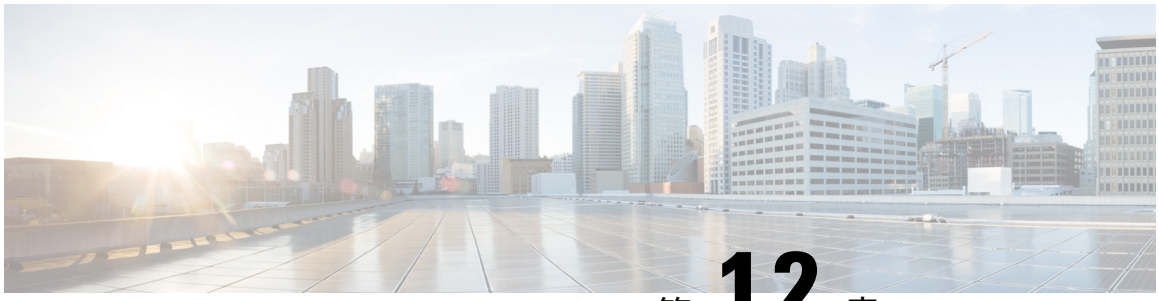
a) 電子メール内のリンクをクリックします。

リンクにより Web ブラウザで Cisco Smart Call Home ポータルが開きます。

b) Cisco Smart Call Home ポータルにログインします。

c) Cisco Smart Call Home によって示される手順に従います。

条項および条件に同意したら、Cisco UCS ドメインの Cisco Smart Call Home 登録は完了です。



第 12 章

# データベースのヘルス モニタリング



## Cisco UCS Manager データベースのヘルス モニタリング

Cisco UCS Manager は、ファブリック インターコネクトに保存された SQLite データベースを使用して、設定およびインベントリを保持します。フラッシュと NVRAM ストレージ デバイスの両方でデータが破損すると、障害が発生して顧客の設定データが失われる可能性があります。Cisco UCS Manager には、Cisco UCS Manager のデータベースの整合性を向上させるために、複数のプロアクティブなヘルス チェックおよびリカバリ メカニズムが備わっています。これらのメカニズムはデータベース ヘルスのアクティブなモニタリングを有効にします。

- **定期的なヘルス チェック**：データベースの整合性を定期的にチェックすることで、あらゆる破損を検知してプロアクティブに回復させることができます。ヘルス チェックのトリガー （102 ページ）、およびヘルス チェックの間隔の変更 （102 ページ）を参照してください。
- **定期的なバックアップ**：システムの定期的な内部 Full State バックアップにより、回復不可能なエラーが発生した場合に、よりスムーズに復旧できます。「内部バックアップの間隔の変更 （101 ページ）」を参照してください。

## 内部バックアップの間隔の変更

内部バックアップを実行する間隔を変更できます。バックアップを無効にするには、値を 0 に設定します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | UCS-A# **scope system** | システムを入力します。 |
| ステップ 2 | UCS-A /system# **set mgmt-db-check-policy internal-backup-interval** *days* | 整合性バックアップ（日数）を実行する時間間隔を指定します。 |
| ステップ 3 | UCS-A /system* # **commit-buffer** | トランザクションをコミットします。 |

例

この例では、チェックを実行する時間間隔を2日に変更し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # set mgmt-db-check-policy health-check-interval 2
UCS-A /system* # commit-buffer
UCS-A /system #
```

# ヘルス チェックのトリガー

次のコマンドを使用して、即時のデータベースの完全な整合性チェックをトリガーします。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | UCS-A# **scope system** | システムを入力します。 |
| ステップ 2 | UCS-A /system # **start-db-check** | ヘルス チェックをトリガーします。 |
| ステップ 3 | UCS-A /system # **commit-buffer** | トランザクションをコミットします。 |

# ヘルス チェックの間隔の変更

整合性チェックを実行する間隔を変更できます。定期的なチェックを完全に無効にするには、値を 0 に設定します。

手順

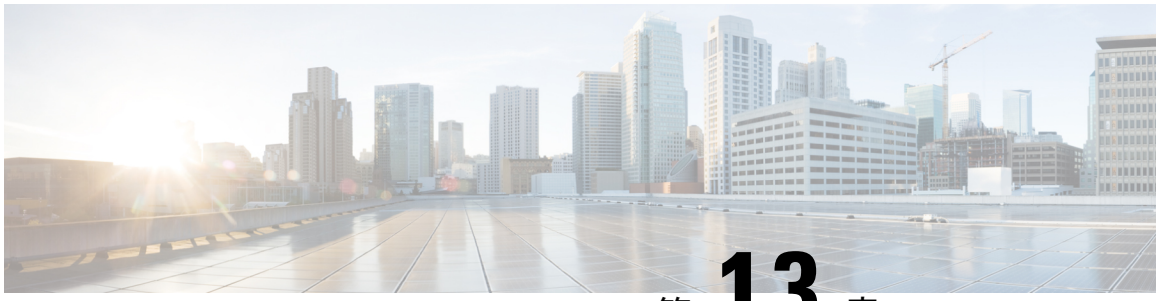
| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | UCS-A# **scope system** | システムを入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 2** | UCS A/system# **set mgmt-db-check-policy health-check-interval** *hours* | 整合性チェック（時間）を実行する時間間隔を指定します。 |
| **ステップ 3** | UCS-A /system* # **commit-buffer** | トランザクションをコミットします。 |

### 例

この例では、チェックを実行する時間間隔を 2 時間に変更し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # set mgmt-db-check-policy health-check-interval 2
UCS-A /system* # commit-buffer
UCS-A /system #
```



第 13 章

# ハードウェア モニタリング



## ファブリック インターコネクトのモニタリング

### 手順

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

**ステップ 2** **[機器]** > **[ファブリックインターコネクト]**を展開します。

**ステップ 3** モニタするファブリック インターコネクトのノードをクリックします。

**ステップ 4** [Work]ペインで次のタブのいずれかをクリックして、ファブリック インターコネクトのステータスを表示します。

| オプション | 説明 |
|---|---|
| [General] タブ | 障害の概要、ファブリック インターコネクト プロパティの概要、ファブリック インターコネクトとそのコンポーネントの物理表示など、ファブリック インターコネクトのステータスの概要が示されます。 |

| オプション | 説明 |
|---|---|
| [Physical Ports] タブ | ファブリック インターコネクトのすべてのポートのステータスが表示されます。このタブには次のサブタブが含まれます。<br>• [Ethernet Ports] タブ<br>• [FC Ports] タブ |
| [Fans] タブ | ファブリックインターコネクトのすべてのファンモジュールのステータスが表示されます。 |
| [PSUs] タブ | ファブリック インターコネクトのすべての電源モジュールのステータスが表示されます。 |
| [Physical Display] タブ | ファブリック インターコネクトとすべてのポートおよびその他のコンポーネントがグラフィック表示されます。コンポーネントに障害がある場合、そのコンポーネントの横に障害アイコンが表示されます。 |
| [FSM] タブ | タスクのステータスなど、サーバで実行されている現在の FSM タスクに関する詳細情報が表示されます。この情報を使用して、これらのタスクにおけるエラーを診断できます。 |
| [Faults] タブ | ファブリック インターコネクトで発生した障害の詳細が表示されます。 |
| [Events] タブ | ファブリック インターコネクトで発生したイベントの詳細が表示されます。 |
| [Neighbors] タブ | ファブリック インターコネクトの LAN、SAN、および LLDP ネイバーの詳細が表示されます。<br>（注） [Neighbors] の詳細を表示するには、[Info Policy] を有効にします。 |
| [Statistics] タブ | ファブリック インターコネクトとそのコンポーネントに関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |

# ブレード サーバのモニタリング

### 手順

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

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

**ステップ 3** モニタするサーバをクリックします。

**ステップ 4** [Work] ペインで次のタブのいずれかをクリックして、サーバのステータスを表示します。

| オプション | 説明 |
|---|---|
| [General] タブ | 障害の概要、サーバプロパティの概要、サーバとそのコンポーネントの物理表示など、サーバのステータスの概要が示されます。 |
| [Inventory] タブ | サーバのコンポーネントのプロパティとステータスに関する詳細情報が次のサブタブに表示されます。<br>• [Motherboard]：マザーボードとサーバ BIOS 設定に関する情報。このサブタブから、破損した BIOS ファームウェアを復旧させることもできます。<br>• [CIMC]：CIMC とそのファームウェアに関する情報。サーバの SEL にもアクセスできます。スタティックまたはプールされた管理 IP アドレスを割り当てて、このサブタブから CIMC ファームウェアを更新およびアクティブ化することもできます。<br>• [CPUs]：サーバの各 CPU に関する情報。<br>• [Memory]：サーバの各メモリ スロットと、スロットの DIMM に関する情報。<br>• [Adapters]：サーバに取り付けられた各アダプタに関する情報。<br>• [HBAs]：各 HBA のプロパティと、サーバに関連付けられたサービス プロファイルでの HBA の設定。<br>• [NICs]：各 NIC のプロパティと、サーバに関連付けられたサービス プロファイルでの NIC の設定。各行を展開すると、関連する VIF および vNIC に関する情報を表示できます。<br>• [iSCSI vNICs]：各 iSCSI vNIC のプロパティと、サーバに関連付けられたサービス プロファイルでのこの vNIC の設定。<br>• [Storage]：ストレージ コントローラのプロパティ、サーバに関連付けられたサービスプロファイルでのローカルディスク設定ポリシー、サーバの各ハード ディスクに関する情報。 |

| オプション | 説明 |
|---|---|
| | **ヒント** ハードディスク ドライブやソリッド ステート ドライブなどの SATA デバイスがサーバに 1 つ以上搭載されている場合、Cisco UCS Manager GUI の [Vendor] フィールドにはその SATA デバイスのベンダー名が表示されます。<br><br>ただし Cisco UCS Manager CLI では、[Vendor] フィールドに ATA が表示され、ベンダー名などのベンダー情報は [Vendor Description] フィールドに表示されます。この 2 番目のフィールドは Cisco UCS Manager GUI にはありません。 |
| [Virtual Machines] タブ | サーバでホストされている仮想マシンの詳細情報が表示されます。 |
| [Installed Firmware] タブ | CIMC、アダプタ、その他のサーバ コンポーネントのファームウェア バージョンが表示されます。このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。 |
| [CIMC Sessions] タブ | サーバの CIMC セッションに関するデータを提供します。 |
| [SEL Logs] タブ | サーバのシステム イベント ログが表示されます。 |
| [VIF Paths] タブ | サーバでのアダプタの VIF パスが表示されます。 |
| [Faults] タブ | サーバで発生した障害の概要が表示されます。任意の障害をクリックすれば、詳細情報を表示できます。 |
| [Events] タブ | サーバで発生したイベントの概要が表示されます。任意のイベントをクリックすれば、詳細情報を表示できます。 |
| [FSM] タブ | タスクのステータスなど、サーバで実行されている現在の FSM タスクに関する詳細情報が表示されます。この情報を使用して、これらのタスクにおけるエラーを診断できます。 |
| [Health] タブ | サーバとそのコンポーネントのヘルス ステータスに関する詳細が表示されます。 |
| [Statistics] タブ | サーバとそのコンポーネントに関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |
| [Temperatures] タブ | サーバのコンポーネントの温度に関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |
| [Power] タブ | サーバのコンポーネントの電力に関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |

**ステップ 5** [Navigation] ペインで、**[*Server_ID*]** > **[Adapters]** > **[*Adapter_ID*]** を展開します。

**ステップ 6** [Navigation] ペインで、次のアダプタのコンポーネントを 1 つ以上クリックしてナビゲータを開き、コンポーネントのステータスを表示します。

- 
- DCE インターフェイス
- HBA
- NIC
- iSCSI vNIC

**ヒント** 子ノードを表示するには、テーブル内のノードを展開します。たとえば、[NIC] ノードを展開すると、その NIC で作成された各 VIF を表示できます。

# ラックマウント サーバのモニタリング

**手順**

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

**ステップ 2** **[機器]** > **[ラックマウント]** > **[サーバ]**を展開します。

（注） Cisco UCS C125 M5 サーバ では、**[機器（Equipment）]** > **[ラックマウント（Rack Mounts）]** > **[エンクロージャ（Enclosures）]** > **[ラック エンクロージャ *rack_enclosure_number*（Rack Enclosure rack_enclosure_number）]** > **[サーバ（Servers）]** の順に展開します。

**ステップ 3** モニタするサーバをクリックします。

**ステップ 4** [Work] ペインで次のタブのいずれかをクリックして、サーバのステータスを表示します。

| オプション | 説明 |
|---|---|
| [General] タブ | 障害の概要、サーバ プロパティの概要、サーバとそのコンポーネントの物理表示など、サーバのステータスの概要が示されます。 |
| [Inventory] タブ | サーバのコンポーネントのプロパティとステータスに関する詳細情報が次のサブタブに表示されます。<br>• [Motherboard]：マザーボードとサーバ BIOS 設定に関する情報。このサブタブから、破損した BIOS ファームウェアを復旧させることもできます。<br>• [CIMC]：CIMC とそのファームウェアに関する情報。サーバの SEL にもアクセスできます。スタティックまたはプールされた管理 IP ア |

| オプション | 説明 |
|---|---|
| | ドレスを割り当てて、このサブタブからCIMCファームウェアを更新およびアクティブ化することもできます。<br>• [CPU]：サーバの各 CPU に関する情報。<br>• [Memory]：サーバの各メモリ スロットと、スロットの DIMM に関する情報。<br>• [Adapters]：サーバに取り付けられた各アダプタに関する情報。<br>• [HBAs]：各 HBA のプロパティと、サーバに関連付けられたサービス プロファイルでの HBA の設定。<br>• [NICs]：各 NIC のプロパティと、サーバに関連付けられたサービス プロファイルでの NIC の設定。各行を展開すると、関連する VIF および vNIC に関する情報を表示できます。<br>• [iSCSI vNICs]：各 iSCSI vNIC のプロパティと、サーバに関連付けられたサービス プロファイルでのこの vNIC の設定。<br>• [Storage]：ストレージ コントローラのプロパティ、サーバに関連付けられたサービス プロファイルでのローカル ディスク設定ポリシー、サーバの各ハード ディスクに関する情報。<br>（注） C シリーズ/S シリーズ サーバのファームウェアを Cisco UCSM リリース 2.2(6) から 3.1(2) 以降のリリースにアップグレードした場合は、プラットフォーム コントローラ ハブ（PCH）のストレージ コントローラは（SSD ブート ドライブとともに）UCSM GUI に表示されません。<br>ヒント ハード ディスク ドライブやソリッド ステート ドライブなどの SATA デバイスがサーバに 1 つ以上搭載されている場合、Cisco UCS Manager GUI の [Vendor] フィールドにはその SATA デバイスのベンダー名が表示されます。<br>ただし Cisco UCS Manager CLI では、[Vendor] フィールドに ATA が表示され、ベンダー名などのベンダー情報は [Vendor Description] フィールドに表示されます。この 2 番目のフィールドは Cisco UCS Manager GUI にはありません。 |
| [Virtual Machines] タブ | サーバでホストされている仮想マシンの詳細情報が表示されます。 |
| [Installed Firmware] タブ | CIMC、アダプタ、その他のサーバ コンポーネントのファームウェア バージョンが表示されます。このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。 |
| [SEL Logs] タブ | サーバのシステム イベント ログが表示されます。 |

| オプション | 説明 |
|---|---|
| [VIF Paths] タブ | サーバでのアダプタの VIF パスが表示されます。 |
| [Faults] タブ | サーバで発生した障害の概要が表示されます。任意の障害をクリックすれば、詳細情報を表示できます。 |
| [Events] タブ | サーバで発生したイベントの概要が表示されます。任意のイベントをクリックすれば、詳細情報を表示できます。 |
| [FSM] タブ | タスクのステータスなど、サーバで実行されている現在の FSM タスクに関する詳細情報が表示されます。この情報を使用して、これらのタスクにおけるエラーを診断できます。 |
| [Statistics] タブ | サーバとそのコンポーネントに関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |
| [Temperatures] タブ | サーバのコンポーネントの温度に関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |
| [Power] タブ | サーバのコンポーネントの電力に関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |

**ステップ 5** [Navigation] ペインで、**[*Server_ID*]** > **[Adapters]** > **[*Adapter_ID*]** を展開します。

**ステップ 6** [Work] ペインで、次のアダプタのコンポーネントを 1 つ以上右クリックしてナビゲータを開き、コンポーネントのステータスを表示します。

- アダプタ
- DCE インターフェイス
- HBA
- NIC

**ヒント** 子ノードを表示するには、テーブル内のノードを展開します。たとえば、[NIC] ノードを展開すると、その NIC で作成された各 VIF を表示できます。

# I/O モジュールのモニタリング

**手順**

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

**ステップ 2** **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [IO モジュール（IO Modules）]** の順に展開します。

**ステップ 3** モニタするモジュールをクリックします。

**ステップ 4** 次のタブのいずれかをクリックして、モジュールのステータスを表示します。

| オプション | 説明 |
|---|---|
| [General] タブ | 障害の概要、モジュール プロパティの概要、モジュールとそのコンポーネントの物理表示など、IO モジュールのステータスの概要が示されます。 |
| [Fabric Ports] タブ | I/O モジュールのすべてのファブリック ポートのステータスおよび選択されたプロパティが表示されます。 |
| [Backplane Ports] タブ | モジュールのすべてのバックプレーン ポートのステータスおよび選択されたプロパティが表示されます。 |
| [Faults] タブ | モジュールで発生した障害の詳細が表示されます。 |
| [Events] タブ | モジュールで発生したイベントの詳細が表示されます。 |
| [FSM] タブ | モジュールに関連する FSM タスクの詳細およびステータスが表示されます。この情報を使用して、これらのタスクにおけるエラーを診断できます。 |
| [Health] タブ | モジュールのヘルス ステータスの詳細が表示されます。 |
| [Statistics] タブ | モジュールとそのコンポーネントに関する統計情報が表示されます。これらの統計情報は図表形式で表示できます。 |

# Crypto Card のモニタリング

## ブレード サーバでの Cisco Crypto Card 管理

Cisco UCS Manager では、Cisco UCSB-B200-M4 ブレード サーバでのメザニン Crypto Card（UCSB-MEZ-INT8955）のインベントリ管理が行えます。Cisco Crypto Card の中心的な機能は、UCS ブレード サーバに対して、特定のアプリケーション用のハードウェア ベース暗号化機能を提供することです。

Cisco B200 M4 ブレード サーバでは、オプションとして、ホットプラグ対応の SAS、SATA ハード ディスク ドライブ（HDD）またはソリッド ステート ドライブ（SSD）を計 2 台利用可能で、広範な IT ワークロードに適しています。Crypto Card は、ブレード サーバのスロット 2 に設置します。

Cisco UCS Manager は、ブレード サーバに設置された Crypto Card を検出すると、モデル、リビジョン、ベンダー、シリアル番号を、[Equipment] > [Chassis] > [Server_Number] > [Inventory] > [Security] サブタブに表示します。サポートされていないブレード サーバに Crypto Card を追加すると、Crypto Card の検出に失敗します。

Cisco UCS Manager は、Crypto Card のファームウェア管理をサポートしていません。

Crypto Card の挿入時または取り外し時は、詳細なディスカバリがトリガーされます。Crypto Card を他の Crypto Card、アダプタ、Fusion I/O またはパス スルー カードと交換した場合、動作しているサーバでの詳細なディスカバリがトリガーされます。Crypto Card の交換については、次のようなシナリオが想定されます。

- Crypto Card を別の Crypto Card と交換する。
- Crypto Card をアダプタと交換する。
- Crypto Card を Fusion I/O と交換する。
- Crypto Card を GPU カードと交換する。
- Crypto Card をパス スルー カードと交換する。
- アダプタを Crypto Card と交換する。
- ストレージ メザニンを Crypto Card と交換する。
- GPU カードを Crypto Card と交換する。

Cisco UCS Manager を以前のバージョンにダウングレードする場合、クリーンアップは必要ではありません。ダウングレード後に UCS Manager をアップグレードする場合は、カードを再検出してインベントリに登録させる必要があります。Crypto Card をサポートしていないサーバでも、検出は中断されずに続行されます。

Crypto Card の検出、関連付け、関連付け解除、および解放は、Cisco UCS Manager で処理されます。

# Crypto Card のプロパティの表示

**手順**

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

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

**ステップ 3** [Work] ペインで [Inventory] タブをクリックし、[Security] サブタブをクリックします。

| 名前 | 説明 |
|---|---|
| [ID] フィールド | |

| 名前 | 説明 |
|---|---|
| [Slot ID] フィールド | メザニン カードが設置されているスロット ID を指定します。 |
| [Magma Expander Slot Id] フィールド | PCI スロットの ID 番号を指定します。 |
| [Is Supported] フィールド | カードがサポートされているかどうかを指定します。 |
| [Vendor] フィールド | カードのベンダーを指定します。 |
| [Model] フィールド | カードのモデル番号を指定します。 |
| [Serial] フィールド | カードのシリアル番号を指定します。 |
| [Firmware Version] フィールド | Crypto Card のシリアル番号を指定します。 |

# NVMe PCIe SSD デバイスのモニタリング

## NVMe PCIe SSD ストレージ デバイス インベントリ

Cisco UCS Manager GUI は、Non-Volatile Memory Express（NVMe）Peripheral Component Interconnect Express（PCIe）SSD ストレージ デバイスのインベントリを検出、識別、および表示します。サーバ内のストレージ デバイスの状態を表示できます。NVMe 対応 PCIe SSD ストレージ デバイスは、SAS または SATA の SSD と比較して、遅延を短縮し、1 秒あたりの入出力操作数（IOPS）を増加させ、電力消費を削減できます。

オプションの Intel VMD 対応 NVMe ドライバおよび Intel VMD 対応 LED コマンド ライン インターフェイス ツールは、ルート ポートに接続されている NVMe PCIe SSD デバイスを集約することにより、追加の機能を提供します。これにより、Suprise ホットプラグが有効になり、Intel VMD が有効になっているドメインに接続された PCIe SSD ストレージで LED 点滅パターンのオプション設定が可能になります。

## NVMe PCIe SSD ストレージ インベントリの表示

**手順**

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

**ステップ 2** **[機器（Equipment）]** > **[ラックマウント（Rack Mounts）]** > **[サーバ（Servers）]** > ***[サーバ番号（Server Number）]*** の順に展開します。

**ステップ 3** [Inventory] タブをクリックします。

**ステップ 4** 次のいずれかを実行します。

a) [Storage] タブをクリックします。

[Storage Controller NVME *ID number*] という名前の NVMe PCIe SSD ストレージ デバイスの一覧が表示されます。名前、サイズ、シリアル番号、動作ステータス、状態、その他の詳細を表示できます。

b) NVMe PCIe SSD ストレージ デバイスをクリックします。

次のインベントリの詳細が表示されます。

| 名前 | 説明 |
|---|---|
| [Actions] 領域 | |
| [ID] フィールド | サーバで設定されている NVMe PCIe SSD ストレージ デバイス。 |
| [Description] フィールド | サーバで設定されている NVMe PCIe SSD ストレージ デバイスの簡単な説明。 |
| [Model] フィールド | NVMe PCIe SSD ストレージ デバイスのモデル。 |
| [Revision] フィールド | NVMe PCIe SSD ストレージ デバイスのリビジョン。 |
| **サブタイプ**()] フィールド | NVMe PCIe SSD ストレージ デバイスのベンダー名。 |
| [RAID Support] フィールド | NVMe PCIe SSD ストレージ デバイスが RAID 対応かどうかが示されます。 |
| [OOB Interface Support] フィールド | NVMe PCIe SSD ストレージ デバイスがアウトオブバンド管理をサポートしているかどうかを示します。 |
| [PCIe Address] フィールド | 仮想インターフェイス カード（VIC）上の NVMe PCIe SSD ストレージ デバイス。 |
| [Number of Local Disks] フィールド | NVMe PCIe SSD ストレージ デバイスに含まれているディスク数。 |

| 名前 | 説明 |
|---|---|
| [Rebuild Rate] フィールド | ディスク障害発生時のストレージデバイスの RAID 再構築の所要時間。 |
| **SubOemID** | 仮想インターフェイス カード（VIC）上の NVMe PCIe SSD ストレージ デバイスの OME ID。 |
| **ストリップ サイズのサポート**()] フィールド | NVMe PCIe SSD ストレージ デバイスでサポートされているストリップ サイズ。 |
| [Sub Device ID] フィールド | コントローラのサブデバイス ID |
| **[Sub Ventor ID]** フィールド | コントローラのサブベンダー ID |
| [Name] フィールド | コントローラの名前。 |
| [PID] フィールド | NVMe PCIe SSD ストレージ デバイスの製品 ID（製品名、モデル名、製品番号とも呼ばれます）。 |
| [Serial] フィールド | ストレージ デバイスのシリアル番号。 |
| [Vendor] フィールド | NVMe PCIe SSD ストレージ デバイスを製造したベンダー。 |
| [PCI Slot] フィールド | ストレージ デバイスの PCI スロット。 |

| 名前 | 説明 |
|---|---|
| [Controller Status] フィールド | CIMC で報告されたコントローラの現在のステータス。次のいずれかになります。<br>• [Optimal]：コントローラは正しく機能しています。<br>• [Failed]：コントローラは機能していません。<br>• [Unresponsive]：CIMC はコントローラと通信できません。 |
| **キャッシュのステータスを固定**()] フィールド | ストレージ デバイスのピン キャッシュ ステータス。 |
| **[Default Strip Size]** フィールド | デフォルトのストリップ サイズ ストレージ デバイスをサポートできます。 |
| [Device ID] フィールド | ストレージ デバイスの ID。 |
| [Vendor ID] フィールド | 製造業者の ID。 |
| **[Security]** フィールド | デバイスのセキュリティがストレージ デバイスに適用します。 |
| **[Embedded Storage]** 領域 | |
| [Presence] フィールド | かどうか、ストレージが組み込まれています。 |
| [Operability] フィールド | デバイスの動作のステータス。 |
| [Block Size] フィールド | デバイスのメモリ。 |
| **サイズ (MB)** ] フィールド | MB でデバイスの小数メモリ。 |
| **[Connection Protocol]** フィールド | 接続プロトコルが後。 |
| **運用修飾子の理由** | デバイスの [operability 理由 |
| [Number of Blocks] フィールド | メモリ ブロックの数。 |

| 名前 | 説明 |
|---|---|
| [Firmware] 領域 | |
| [Boot-loader Version] フィールド | コンポーネント上のブートローダ ソフトウェアに関連付けられたファームウェアバージョンを表示します。 |
| [Running Version] フィールド | コンポーネントで使用されるファームウェアバージョン。 |
| [Package Version] フィールド | ファームウェアが含まれているファームウェア パッケージのバージョン。 |
| [Startup Version] フィールド | コンポーネントの次回リブート時に有効にするファームウェアのバージョン。 |
| [Activate Status] フィールド | 次のいずれかになります。<br>• [Ready]：アクティベーションが成功し、コンポーネントが新しいバージョンを実行中です。<br>• [Activating]：システムは新しいファームウェアバージョンをアクティブにしています。<br>• [Failed]：ファームウェアのアクティベーションに失敗しました。詳細については、失敗したコンポーネントをダブルクリックして、ステータスのプロパティを確認してください。 |

# NVMe PCIe SSD ストレージ統計情報の表示

## 手順

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

**ステップ 2** **[機器（Equipment）] > [ラックマウント（Rack Mounts）] > [サーバ（Servers）] > *[サーバ番号（Server Number）]*** の順に展開します。

**ステップ 3** [Inventory] タブをクリックします。

**ステップ 4** [Storage] タブをクリックします。

**ステップ 5** [Controller] タブをクリックします。

**ステップ 6** 統計情報を表示したい NVMe PCIe SSD ストレージ デバイスをクリックします。

**ステップ 7** [Statistics] タブをクリックします。

次の統計情報が表示されます。

| 名前 | 説明 |
|---|---|
| **履歴テーブルのトグル**ボタン | 右側のペインを左右に分割して、ウィンドウの下部で**履歴**テーブルを表示します。ウィンドウの上部で、カウンタを選択すると、**履歴**テーブルには、そのカウンタからデータを収集したたびに記録された情報が表示されます。 |
| **コレクションポリシーの変更**]ボタン | 収集と報告、カウンタの間隔を指定できますが、選択したカウンタは、の**[全般]** タブを開きます。<br>（注） このオプションは、カウンタが選択されている場合に使用可能なだけです。 |

| 名前 | 説明 |
|---|---|
| [名前（Name）] カラム | 統計のカウンタは使用可能なシステム コンポーネントを示すツリー ビューです。コンポーネントに関連付けられているカウンタを表示するには、ナビゲーション ツリーの一部を展開します。すべてのカウンタを表示するには、グラフの上部にあるボタンを+をクリックします (プラス記号)。<br><br>ファブリック インターコネクトのシステムの統計情報およびFEX を使用できます。これには次が含まれます。<br><br>• CPU 使用率<br>• メモリ使用率の低いカーネル メモリを含む<br><br>（注） ファブリックインターコネクトの主要な障害が発生した使用可能なカーネル メモリが 100 MB 未満の場合<br><br>• ECC エラー<br><br>PCH、SAS、および SATA のストレージ コントローラには、ディスクの統計情報が表示されます。<br><br>NVMe ドライブには、NVMe 統計情報が表示されます。これには次が含まれます。<br><br>• **DriveLifeUsedPercentage**:、NVMe ドライブを読み書き使用 life パーセンテージで表示されます。<br>• **LifeLeftInDays**:、NVMe ドライブ読み書き残量ワークロードに基づくものです。されると、完全なドライブが読み取りにのみ使用できます。<br>• **温度**: ドライブの温度。 |

| 名前 | 説明 |
|---|---|
| [Value] カラム | 最上位のコンポーネントは、この列は、カウンタが最後に更新された日時を示します。実際のカウンタは、この列は、カウンタの現在の値を示します。<br>値では、ユニットは、カウンタの名前に付加コードによって決定できます。<br>• **(A)**]: アンペア<br>• **(babbles)**<br>• **(bytes)**: バイト数<br>• **©)**: 摂氏<br>• **(コリジョン)**]: ネットワークのコリジョンが発生した回数<br>• **(廃棄)**]:、転送中にパケットがドロップされました回数<br>• **(エラー)**]: 発生したエラーの数<br>• **(lostCarrier)**: 送信中にキャリアが失われた回数。<br>• **(MB)**: メガバイト<br>• **(noCarrier)**]: キャリアが見つかりませんでした回数<br>• **(packets))**]: 転送されるパケットの数<br>• **(一時停止)**]: データ伝送中に発生した一時停止の数<br>• **(リセット)**]: 番号またはデータ伝送中に発生したのリセット<br>• **(V)**: ボルト<br>• **(W)**: ワット<br>• **(**blank**)** |
| 平均] カラム | カウンタの平均値。<br>（注） 集約カウンタは、これは平均デルタ レポート期間内で。 |
| [Max] カラム | 最大では、カウンタの値を記録します。<br>（注） 集約カウンタは、これは最大デルタ レポート期間内で。 |

| 名前 | 説明 |
|---|---|
| [Min] カラム | 最小値は、カウンタの値を記録します。<br>（注） 集約カウンタは、これは最小デルタ レポート期間内で。 |
| **デルタ**] カラム | 最大の変更は、カウンタの記録されます。 |

# ヘルス モニタリング

## ファブリックインターコネクトのメモリ不足統計情報および修正可能なパリティ エラーのモニタリング

Cisco UCSファブリック インターコネクト システムの統計情報と障害をモニタできるため、次のようなシステムの全体的な完全性を管理できます。

- **カーネル メモリ不足**：これは Linux カーネルが直接対処するセグメントです。Cisco UCS Manager は、カーネルのメモリが 100 MB を下回った場合に、ファブリック インターコネクトで重大な障害を生成します。ファブリック インターコネクトのメモリ不足障害のモニタリング （123 ページ）を参照してください。メモリ不足しきい値に到達すると、KernelMemFree と KernelMemTotal の 2 つの統計情報アラームが出されます。KernelMemFree および KernelMemTotal 統計情報は、ユーザが独自のしきい値を定義できるシステム統計情報のしきい値ポリシーに追加されます。

  メモリ不足の障害については、次の Cisco UCS ファブリック インターコネクトでサポートされています。

  - UCS 6248-UP
  - UCS 6296-UP
  - UCS Mini
  - UCS-FI-6332
  - UCS-FI-6332-16UP

- [Correctable Parity Errors]：（UCS 6300 ファブリック インターコネクトの場合のみ）これらのエラーをシステムで収集し、報告するには、[Statistics] > [sysstats] > [CorrectableParityError] の順に選択します。
- **修正不可能なパリティ エラー**（UCS 6300 ファブリック インターコネクトのみ）：これらのエラーは [Faults] タブでファブリック インターコネクトの重大な障害を生成して、CallHome をトリガーします。これらの重大な障害では、ファブリック インターコネクト

のリブートが必要になる場合があります。ファブリック インターコネクトの修正不可能なパリティ エラーによる重大な障害のモニタリング （124 ページ）を参照してください。

ファブリック インターコネクトのメモリ不足および修正可能なメモリに関する統計情報の表示法：

**手順**

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

**ステップ 2** **[機器（Equipment）] > [ファブリック インターコネクト（Fabric Interconnects）] > *[Fabric_Interconnect_Name]*** の順に展開します。

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

**ステップ 4** [Statistics] タブで [sysstats] ノードを展開して、ファブリック インターコネクトのメモリ不足および修正可能なパリティ エラーに関する統計情報をモニタします。

重大な障害は、カーネルの空きメモリ（KernelMemFree）が 100 MB を下回ると発生します。修正不可能なパリティ エラーが発生した場合も、システムは重大な障害を生成します。

# ファブリック インターコネクトのメモリ不足障害のモニタリング

Cisco UCS Manager システムは、カーネルの空きメモリが 100 MB を下回った場合に、ファブリック インターコネクトで高いシビラティ（重大度）の障害を生成します。

メモリ不足の障害については、次の Cisco UCS ファブリック インターコネクトでサポートされています。

- UCS 6248-UP
- UCS 6296-UP
- UCS Mini
- UCS-FI-6332
- UCS-FI-6332-16UP

ファブリック インターコネクトのメモリ不足障害を表示するには：

**手順**

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

**ステップ 2** **[機器（Equipment）] > [ファブリック インターコネクト（Fabric Interconnects）] > *[Fabric_Interconnect_Name]*** の順に展開します。

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

**ステップ 4** **[Faults]** タブで、次のように説明されている高いシビラティ（重大度）の障害を探します：*Fabric Interconnect_Name* kernel low memory free reached critical level: ## (MB)

# ファブリック インターコネクトの修正不可能なパリティ エラーによる重大な障害のモニタリング

修正不可能なパリティ エラーの発生は、[Faults] タブにあるファブリック インターコネクトに重大な障害を生成して、Call Home をトリガーします。重大な障害は、ファブリック インターコネクトのリブートを必要とする場合があります。

（注） これは、UCS 6300 ファブリック インターコネクトにのみ適用されます。

修正不可能なパリティ エラーの障害の監視法：

**手順**

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

**ステップ 2** **[機器（Equipment）]** > **[ファブリック インターコネクト（Fabric Interconnects）]** > ***[Fabric_Interconnect_Name]*** の順に展開します。

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

**ステップ 4** **[Faults]** タブで、次のように説明されている高いシビラティ（重大度）の障害を探します：SER、訂正不可能なエラー：回復不可能なエラーが見つかりました。おそらくファイルシステムが壊れています。Reboot FI for recovery.

**ステップ 5** ファブリック インターコネクトをリブートします。

# ブレード サーバとラックマウント サーバでの CIMC メモリ使用率のモニタリング

Cisco Integrated Management Controller（CIMC）は、ブレード サーバとラックマウント サーバについて、次のメモリ使用量イベントを報告します。

- メモリが 1 MB を下回り、メモリ使用量が致命的と CIMC が判断。リセットが差し迫った状況。
- メモリが 5 MB を下回り、メモリ使用量が過度に高いと CIMC が判断。
- メモリが 10 MB を下回り、メモリ使用量が高いと CIMC が判断。

CIMC のメモリ使用量イベントの表示法：

**手順**

次のいずれかを実行します。

- **ブレード サーバの場合**：
  1. [Equipment] タブの **[Equipment]** > **[Chassis]** > **[*Chassis Number*]** > **[Servers]** を展開します。
  2. [Server_Number] をクリックします。
  3. [Work] ペインで、[Health] タブをクリックします。
- **ラックマウント サーバの場合**：
  1. [Equipment] タブで、**[Equipment]** > **[Rack-Mounts]** > **[Servers]** の順に展開します。
  2. [Server_Number] をクリックします。
  3. [Work] ペインで、[Health] タブをクリックします。

CIMC が 2 つのヘルス イベントを報告し、その一方のシビラティ（重大度）が高くもう一方のシビラティ（重大度）が低い場合、システムは高いシビラティ（重大度）の障害を 1 つ生成して、[Health] タブの [Management Services] サブタブに詳細を表示します。個々のヘルス イベントは個別の障害に変換されません。最も高いシビラティ（重大度）のヘルス イベントが 1 つの障害に変換されます。障害は ***[Server_Number]*** > **[Faults]** タブに表示されます。

# 入出力モジュールでの CMC メモリ使用率のモニタリング

Cisco Chassis Management Controller（CMC）は、IOM およびシャーシについてメモリ使用量イベントを報告します。

システムは、報告されたヘルス ステータスを集約して 1 つの障害を生成します。

CMC のメモリ使用量イベントの表示方法：

**手順**

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

**ステップ 2** **[機器（Equipment）]** > **[シャーシ（Chassis）]** > ***[*シャーシ番号（*Chassis Number*）*]*** > **[IO モジュール（IO Modules）]** の順に展開します。

**ステップ 3** [IO Module_Number] をクリックします。

[Health] タブの [Management Services] サブタブが表示されます。

個々のイベントは個別の障害に変換されません。最も高いシビラティ（重大度）のイベントが障害に変換されます。障害は ***[IO Module_Number]*** > **[Faults]** タブに表示されます。

# FEX 統計情報のモニタリング

Cisco UCS Manager は、System Stats に集計された次の Cisco ファブリック エクステンダ（FEX）に関する統計情報を報告します。

- 負荷
- 使用可能なメモリ
- キャッシュされたメモリ
- カーネル
- メモリ合計
- カーネル メモリの空き容量

Cisco 2200 シリーズおよび 2300 シリーズ FEX は、統計情報モニタリングをサポートしています。

（注） Cisco UCS ミニ プラットフォームでは、FEX 統計情報はサポートされていません。

すべての FEX 統計は FexSystemStats として、ユーザ独自のしきい値を定義できるしきい値ポリシーに追加されます。

**手順**

**ステップ 1** [Equipment] タブで **[Equipment]** > **[Rack Mounts]** > **[FEX]** > ***[FEX Number]*** の順に展開します。

[Statistics] タブが表示されます。統計情報は図表形式で表示できます。

**ステップ 2** [sys-stats] ノードを展開して、FEX 統計情報をモニタします。

# 管理インターフェイス モニタリング ポリシー

管理インターフェイス モニタリング ポリシーでは、ファブリック インターコネクトの mgmt0 イーサネット インターフェイスをモニタする方法を定義します。Cisco UCS Managerによって管理インターフェイスの障害が検出されると、障害レポートが生成されます。障害レポートの数が設定された数に達した場合、システムは管理インターフェイスが使用不能であると見な

し、障害を生成します。デフォルトでは、管理インターフェイス モニタリング ポリシーは有効です。

その時点で管理インスタンスであるファブリック インターコネクトの管理インターフェイスに障害が発生した場合、 Cisco UCS Manager はまず、下位のファブリック インターコネクトがアップ状態であるかどうかを確認します。さらに、ファブリック インターコネクトに対して記録されている障害レポートがその時点でない場合、 Cisco UCS Managerはエンドポイントの管理インスタンスを変更します。

影響を受けるファブリック インターコネクトがハイ アベイラビリティ設定でプライマリに設定されている場合、管理プレーンのフェールオーバーがトリガーされます。このフェールオーバーはデータ プレーンに影響しません。管理インターフェイスのモニタリングに関連している次のプロパティを設定できます。

- 管理インターフェイスのモニタに使用されるメカニズムのタイプ。
- 管理インターフェイスのステータスがモニタされる間隔。
- 管理が使用できないと判断し障害メッセージを生成する前にシステムの失敗を許容するモニタリングの最大試行回数。

**重要** ファブリック インターコネクトの管理インターフェイスに障害が発生した場合、次のいずれかが発生したときは、管理インスタンスを変わらないことがあります。

- 従属ファブリック インターコネクト経由のエンド ポイントへのパスが存在しない。
- 従属ファブリック インターコネクトの管理インターフェイスが失敗した。
- 従属ファブリック インターコネクト経由のエンド ポイントへのパスが失敗した。

# 管理インターフェイス モニタリング ポリシーの設定

**手順**

**ステップ 1** [ナビゲーション]ペインで、[管理者]をクリックします。

**ステップ 2** **[すべて]** > **[通信管理]**を展開します。

**ステップ 3** [Management Interfaces] をクリックします。

**ステップ 4** [Work] ペインの [Management Interfaces Monitoring Policy] タブをクリックします。

**ステップ 5** 次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [Admin Status] フィールド | モニタリング ポリシーを管理インターフェイスに対して有効にするか無効にするかを示します。 |

| 名前 | 説明 |
|---|---|
| [Poll Interval] フィールド | データ記録の間に Cisco UCSが待機する秒数。<br>90 ～ 300 の整数を入力します。 |
| [Max Fail Report Count] フィールド | Cisco UCS が管理インターフェイスを使用できないと判断し、障害メッセージを生成するまでのモニタリングの最大失敗回数。<br>2 ～ 5 の整数を入力します。 |
| [Monitoring Mechanism] フィールド | Cisco UCSで使用するモニタリングのタイプ。次のいずれかになります。<br>• **[MII Status]**：Cisco UCS はメディア独立型インターフェイス（MII）のアベイラビリティをモニタします。このオプションを選択すると、Cisco UCS Manager GUI は **[Media Independent Interface Monitoring]** 領域を表示します。<br>• **[Ping Arp Targets]**：Cisco UCSは指定されたターゲットを Address Resolution Protocol（ARP）を使用して ping します。このオプションを選択すると、 Cisco UCS Manager GUI は **[ARP Target Monitoring]** 領域を表示します。<br>• **[Ping Gateway]**：Cisco UCS は、**[Management Interfaces]** タブでこのCisco UCS ドメインに指定されたデフォルト ゲートウェイ アドレスを ping します。このオプションを選択すると、 Cisco UCS Manager GUIは **[Gateway Ping Monitoring]** 領域表示します。 |

**ステップ 6** モニタリング メカニズムに **[MII Status]** を選択する場合、**[Media Independent Interface Monitoring]** 領域 の次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [Retry Interval] フィールド | 前の試行が失敗した場合に、MII から別の応答を要求するまでに Cisco UCS が待機する秒数。<br>3 ～ 10 の範囲の整数を入力します。 |
| [Max Retry Count] フィールド | システムがインターフェイスを使用できないと判断するまでに Cisco UCS が MII をポーリングする回数。<br>1 ～ 3 の整数を入力します。 |

**ステップ 7** モニタリング メカニズムに **[Ping Arp Targets]** を選択する場合、**[ARP Target Monitoring]** 領域の該当するタブのフィールドに入力します。

IPv4 アドレスを使用している場合は、[IPv4] サブタブの次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [Target IP 1] フィールド | 最初の IPv4アドレスCisco UCSが、ping します。 |
| [Target IP 2] フィールド | 2 番目の IPv4アドレスCisco UCSが、ping します。 |
| [Target IP 3] フィールド | 3 番目の IPv4アドレスCisco UCSが、ping します。 |
| [Number of ARP Requests] フィールド | Cisco UCS がターゲット IP アドレスに送信する ARP 要求数。<br>1 ～ 5 の整数を入力します。 |
| [Max Deadline Timeout] フィールド | システムが ARP ターゲットを使用できないと判断するまでに、Cisco UCS が ARP ターゲットからの応答を待機する秒数。<br>5 ～ 15 の整数を入力します。 |

IPv6 アドレスを使用している場合は、[IPv6] サブタブの次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [Target IP 1] フィールド | 最初の IPv6 アドレスCisco UCSが、ping します。 |
| [Target IP 2] フィールド | 2 番目の IPv6 アドレスCisco UCSが、ping します。 |
| [Target IP 3] フィールド | 3 番目の IPv6 アドレスCisco UCSが、ping します。 |
| [Number of ARP Requests] フィールド | Cisco UCS がターゲット IP アドレスに送信する ARP 要求数。<br>1 ～ 5 の整数を入力します。 |
| [Max Deadline Timeout] フィールド | システムが ARP ターゲットを使用できないと判断するまでに、Cisco UCS が ARP ターゲットからの応答を待機する秒数。<br>5 ～ 15 の整数を入力します。 |

IPv4 アドレスに 0.0.0.0 と入力すると、ARP ターゲットが削除されます。または IPv6 アドレスの場合は N-disc ターゲットが削除されます。

**ステップ 8** モニタリング メカニズムに **[Ping Gateway]** を選択する場合、**[Gateway Ping Monitoring]** 領域の次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [Number of ping Requests] フィールド | Cisco UCSがゲートウェイを ping する回数。<br>1 ～ 5 の整数を入力します。 |
| [Max Deadline Timeout] フィールド | Cisco UCS がアドレスを使用できないと判断するまでに、Cisco UCSがゲートウェイからの応答を待機する秒数。<br>5 ～ 15 の整数を入力します。 |

**ステップ 9** **[Save Changes]**をクリックします。

# ローカル ストレージのモニタリング

Cisco UCS でのローカル ストレージのモニタリングでは、ブレードまたはラック サーバに物理的に接続されているローカル ストレージに関するステータス情報を提供します。これには、RAID コントローラ、物理ドライブおよびドライブ グループ、仮想ドライブ、RAID コントローラ バッテリ（バッテリ バックアップ ユニット）、Transportable Flash Module（TFM）、スーパーキャパシタ、FlexFlash コントローラおよび SD カードが含まれます。

Cisco UCS Manager は、アウトオブバンド インターフェイスを使用して LSI MegaRAID コントローラおよび FlexFlash コントローラと直接通信するため、リアルタイムの更新が可能になります。表示される情報には次のようなものがあります。

- RAID コントローラ ステータスと再構築レート。
- 物理ドライブのドライブの状態、電源状態、リンク速度、運用性およびファームウェア バージョン。
- 仮想ドライブのドライブの状態、運用性、ストリップのサイズ、アクセス ポリシー、ドライブのキャッシュおよびヘルス。
- BBU の運用性、それがスーパーキャパシタまたはバッテリであるか、および TFM に関する情報。

  LSI ストレージ コントローラは、スーパーキャパシタを備えた Transportable Flash Module（TFM）を使用して RAID キャッシュ保護を提供します。
- SD カードおよび FlexFlash コントローラに関する情報（RAID のヘルスおよび RAID の状態、カード ヘルスおよび運用性を含む）。
- 再構築、初期化、再学習などストレージ コンポーネント上で実行している操作の情報。

（注） CIMC のリブートまたはビルドのアップグレード後は、ストレージ コンポーネント上で実行している操作のステータス、開始時刻および終了時刻が正しく表示されない場合があります。

- すべてのローカル ストレージ コンポーネントの詳細な障害情報。

（注） すべての障害は、[Faults] タブに表示されます。

# 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、次のブレード 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 UCS B200 M6サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS B200 M4 ブレード サーバ
- Cisco UCS B260 M4 ブレード サーバ
- Cisco UCS B460 M4 ブレード サーバ
- Cisco UCS B200 M3 ブレード サーバ
- Cisco UCS B420 M3 ブレード サーバ
- Cisco UCS B22 M3 ブレード サーバ

Cisco UCS Manager を使用して、次のラック 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 UCS C420 M3 ラック サーバ
- Cisco UCS C240 M3 ラック サーバ
- Cisco UCS C220 M3 ラック サーバ
- Cisco UCS C24 M3 ラック サーバ
- Cisco UCS C22 M3 ラック サーバ
- Cisco UCS C220 M4 ラック サーバ
- Cisco UCS C240 M4 ラック サーバ
- Cisco UCS C460 M4 ラック サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS C220 M6サーバ
- Cisco UCS C240 M6サーバ

- Cisco UCS C225 M6サーバ
- Cisco UCS C245 M6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。

# 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。
- 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。

# フラッシュ ライフ ウェア レベル モニタリング

フラッシュ ライフ ウェア レベル モニタリングによって、ソリッド ステート ドライブの寿命をモニタできます。フラッシュ ライフ残量の割合とフラッシュ ライフの状態の両方を表示できます。ウェア レベル モニタリングは次の Cisco UCS ブレード サーバのフュージョン IO メザニン カードでサポートされます。

- Cisco UCS B200 M4 ブレード サーバ
- Cisco UCS B260 M4 ブレード サーバ
- Cisco UCS B460 M4 ブレード サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS B200 M6サーバ

（注） ウェア レベル モニタリングの必須事項は次のとおりです。

- Cisco UCS Manager がリリース 2.2(2a) 以降である。
- フュージョン IO メザニン カードのファームウェアのバージョンが 7.1.15 以降である。

## 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** [ナビゲーション]ペインで、[機器]をクリックします。

**ステップ 2** **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [サーバ（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。

## RAID 0 一貫性チェックの制限

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。一貫性チェックを実行するには、ローカル ディスク設定ポリシーを変更する必要があります。詳細は『*UCS Manager Server Management Guide*』の「Server Related Policies」の章にある「Changing a Local Disk Policy」のトピックを参照してください。

# グラフィックス カードのモニタリング

## グラフィックス カード サーバ サポート

Cisco UCS Managerを使用すると、特定のグラフィックス カードとコントローラのプロパティを表示できます。グラフィックス カードは、次のサーバでサポートされています。

- Cisco UCS C460 M4 ラック サーバ
- Cisco UCS B200M4 ブレード サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ

- Cisco UCS C225 M6サーバ
- Cisco UCS C245 M6サーバ

（注） 特定の NVIDIA グラフィック処理ユニット（GPU）では、エラー訂正コード（ECC）と vGPU の組み合わせはサポートされません。シスコでは、NVIDIA が公開しているそれぞれの GPU のリリース ノートを参照して、ECC と vGPU の組み合わせがサポートされているかどうか確認することを推奨しています。

# ブレード サーバでの GPU メザニン グラフィックス モジュール管理

Cisco UCS Manager では、Cisco B200 M4 ブレード サーバで使用する NVIDIA Graphics Processing Unit（GPU）メザニン グラフィックス モジュール（N16E-Q5）の、インベントリおよびファームウェア管理が行えます。GPU を利用することで、科学計算、分析、エンジニアリング、コンシューマ、企業アプリケーションでの計算処理が高速化されます。Cisco B200 M4 ブレード サーバでは、オプションとして、ホットプラグ対応の SAS、SATA ハード ディスク ドライブ（HDD）またはソリッド ステート ドライブ（SSD）を計 2 台利用可能で、広範な IT ワークロードに適しています。

Cisco UCS Manager は、現場交換可能ユニットとしてブレード サーバーの GPU グラフィックス カードの存在を検出し、モデル、ベンダー、シリアル番号、PCI スロットおよびアドレス、ファームウェアなどのデバイス インベントリ情報を収集します。Cisco UCS Manager は、[機器（Equipment）]>[シャーシ（Chassis）]>*[Server_Number]*>[インベントリ（Inventory）]>[GPU] サブタブで GPU カード インベントリを表示します。

GPU カードのファームウェア管理には、ファームウェアのアップグレードおよびダウングレードが含まれます。既存の Cisco UCS Manager サービス プロファイルを使用して、GPU ファームウェアをアップグレードします。クリーンアップが必要であるため、古いバージョンのファームウェアを使用した GPU ファームウェアのダウングレードは行わないでください。

GPU カードは、ブレード サーバのスロット 2 に設置します。サポートされていないブレード サーバにカードを挿入すると、GPU カードの検出に失敗します。

GPU カードを交換すると、動作しているサーバでの詳細なディスカバリがトリガーされます。詳細なディスカバリをトリガーする GPU カードの交換シナリオは、次のように各種存在します。

- GPU カードを別の GPU カードと交換する。
- GPU カードをアダプタと交換する。
- GPU カードをストレージ メザニンと交換する。
- アダプタを GPU カードと交換する。
- ストレージ メザニンを GPU カードと交換する。
- GPU カードを Crypto Card と交換する。

- Crypto Card を GPU カードと交換する。

Cisco UCS Manager は、GPU グラフィックス カードを検出、関連付け、関連付け解除、および解放します。GPU グラフィックス カードを表示させるには「グラフィックス カードのプロパティの表示 （135 ページ）」を参照してください。

（注） GPU グラフィックス カードのメモリ（DIMM）には最大 1 TB の制限があります。

# グラフィックス カードのプロパティの表示

## 手順

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

**ステップ 2** 次のいずれかを実行します。

- **[Equipment]** > **[Chassis]** > ***[Chassis_Number]*** > **[Servers]** > ***[Server_Number]*** の順に展開します。
- **[Equipment]** > **[Rack-Mounts]** > **[Servers]** > ***[Server_Number]*** の順に展開します。

**ステップ 3** [Work] ペインで [Inventory] タブをクリックし、[GPU] サブタブをクリックします。

| 名前 | 説明 |
|---|---|
| **[ID]** フィールド | グラフィックス カードの固有識別子。 |
| [PCI Slot] フィールド | グラフィックス カードがインストールされている PCI スロット番号。 |
| [Expander Slot ID] フィールド | エクスパンダ スロット ID。 |
| [PID] フィールド | グラフィックス カードの製品 Id。 |
| [Is Supported] フィールド | グラフィックス カードがサポートされているかどうか。次のいずれかになります。<br>• 〇<br>• **[いいえ（No）]** |
| [Vendor] フィールド | 製造元の名前。 |
| [Model] フィールド | グラフィックス カードのモデル番号。 |
| [Serial] フィールド | コンポーネントのシリアル番号。 |
| [Running Version] フィールド | グラフィックス カードのファームウェア バージョン。 |

| 名前 | 説明 |
|---|---|
| **Activate Status** | グラフィックス カード ファームウェア アクティベーションのステータス:<br>• **[対応（Ready）]**：アクティベーションが成功し、コンポーネントが新しいバージョンを実行中です。<br>• **[アクティブ化中（Activating）]**：システムは新しいファームウェア バージョンをアクティブにしています。<br>• **[失敗（Failed）]**：ファームウェアのアクティベーションに失敗しました。詳細については、失敗したコンポーネントをダブルクリックして、ステータスのプロパティを確認してください。 |
| [Mode] フィールド | 設定されたグラフィックス カードのモード。次のいずれかになります。<br>• **コンピューティング**<br>• **グラフィック**<br>• **任意構成** |
| **部品の詳細** | |
| [Vendor ID] フィールド | グラフィックス カードのベンダー ID。 |
| [Sub Vendor ID] フィールド | グラフィックス カードのサブ ベンダー ID。 |
| [Device ID] フィールド | グラフィックス カードのデバイス ID。 |
| [Sub Device ID] フィールド | グラフィックス カードのサブ デバイス ID。 |

# PCI スイッチのモニタリング

## PCI スイッチ サーバ サポート

Cisco UCS Manager、PCI スイッチのプロパティを表示することができます。PCI スイッチは、次のサーバでサポートされます。

- Cisco UCS C480 M5 ML サーバー

# PCI スイッチ プロパティの表示

スイッチの PCI のプロパティは、PCI スイッチがサポートされているサーバのみに表示されます。

### 手順

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

**ステップ 2** **[Equipment]** > **[Rack-Mounts]** > **[Servers]** > ***[Server_Number]*** の順に展開します。

**ステップ 3** **[Work]** ペインで **[Inventory]** タブをクリックし、**[PCI Switch]** サブタブをクリックします。

| 名前 | 説明 |
|---|---|
| [Device ID] フィールド | PCI スイッチのデバイス ID。 |
| [ID] フィールド | PCI スイッチの固有 ID。 |
| [PCI Slot] フィールド | PCI スイッチがインストールされている PCI スロット番号。 |
| **PCI Address** | 特定 PCI スイッチの PCI アドレス。 |
| [PID] フィールド | Cisco 製品識別子 (PID) の PCI スイッチ。 |
| **[Switch Name]** フィールド | PCI スイッチの名前。これには、スイッチの ID には通常が含まれます。たとえば、PCI スイッチ 2。 |
| **スイッチ ステータス** | PCI スイッチが正しく動作しているかどうかを示します。スイッチのステータスは、次のいずれかになります。<br>• 適切な: と PCI スイッチが正常に動作します。<br>• Degraded]: と PCI スイッチが修正不可能な重大なエラーです。 |
| [Vendor] フィールド | 製造元の名前。 |
| [Vendor ID] フィールド | PCI スイッチのベンダー ID。 |
| [Model] フィールド | PCI スイッチのモデル番号。 |
| [Sub Device ID] フィールド | PCI スイッチのサブデバイス ID。 |
| [Sub Vendor ID] フィールド | PCI スイッチのサブベンダーID。 |
| [Temperature] フィールド | PCI スイッチの現在の温度 |
| [PCI リンクの詳細 | |
| [Link Speed] フィールド | [PCI リンクの速度。 |

| 名前 | 説明 |
|---|---|
| [リンクステータス（Link Status）] フィールド | [PCI リンクのステータス |
| **[Link Width]** フィールド | [PCI リンクの幅 |
| [Slot Status] フィールド | PCI スロットが正しく動作しているかどうかを示します。 |
| [PCI Slot] フィールド | PCI スロット番号 |

# Transportable Flash Module と スーパーキャパシタの管理

LSI ストレージ コントローラは、スーパーキャパシタを備えた Transportable Flash Module（TFM）を使用して RAID キャッシュ保護を提供します。Cisco UCS Manager を使用すると、これらのコンポーネントをモニタしてバッテリ バックアップ ユニット（BBU）の状態を決定できます。BBU の動作状態は次のいずれかになります。

- [Operable]：BBU は正常に動作しています。
- [Inoperable]：TFM または BBU が欠落している、または BBU に障害が発生しており交換する必要があります。
- [Degraded]：BBU に障害が発生すると予測されます。

TFM およびスーパーキャパシタ機能は Cisco UCS Manager リリース 2.1(2) 以降でサポートされています。

## TFM とスーパーキャパシタの注意事項および制約事項

### TFM とスーパーキャパシタの制約事項

- Cisco UCS B420 M3 ブレード サーバの TFM およびスーパーキャパシタの CIMC センサーは、Cisco UCS Manager によってポーリングされません。
- TFM およびスーパーキャパシタが Cisco UCS B420 M3 ブレード サーバに搭載されていない、または搭載後にブレード サーバから取り外した場合、障害は生成されません。
- TFM は Cisco UCS B420 M3 ブレード サーバに搭載されていないが、スーパーキャパシタが搭載されている場合、Cisco UCS Manager によって BBU システム全体が欠落していると報告されます。TFM とスーパーキャパシタの両方がブレード サーバに存在することを物理的に確認する必要があります。

### TFM およびスーパーキャパシタについてサポートされる Cisco UCS サーバ

次の Cisco UCS サーバは TFM およびスーパーキャパシタをサポートしています。

- Cisco UCS B420 M3 ブレード サーバ
- Cisco UCS C22 M3 ラック サーバ
- Cisco UCS C24 M3 ラック サーバ
- Cisco UCS C220 M3 ラック サーバ
- Cisco UCS C240 M3 ラック サーバ
- Cisco UCS C420 M3 ラック サーバ
- Cisco UCS C460 M4 ラック サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS C220 M3 ラック サーバ
- Cisco UCS C240 M3 ラック サーバ

# RAID コントローラ統計の表示

次の手順は、PCIe\NVMe フラッシュ ストレージを備えたサーバの RAID コントローラ統計を表示するための方法を示しています

### 手順

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

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

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

**ステップ 4** **[Storage]** > **[Controller]** > **[General]** サブタブをクリックしてコントローラ統計を表示します。

# RAID バッテリ ステータスのモニタリング

この手順は、RAID 設定および TFM をサポートする Cisco UCS サーバにのみ該当します。BBU に障害が発生した場合、または障害が予測される場合には、そのユニットをできるだけ早く交換する必要があります。

**手順**

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

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

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

**ステップ 4** [Storage] サブタブをクリックして、[RAID Battery (BBU)] 領域を表示します。

# RAID バッテリ障害の表示

（注） これは、RAID 設定および TFM をサポートする Cisco UCS サーバにのみ適用されます。

**手順**

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

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

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

**ステップ 4** 状態に関する詳細情報を表示するバッテリを選択します。

# TPM モニタリング

Cisco UCS M3 以降のすべてのブレード サーバとラックマウント サーバに信頼されたプラットフォーム モジュール（TPM）が搭載されています。オペレーティング システムでの暗号化に TPM を使用することができます。たとえば、Microsoft の BitLocker ドライブ暗号化は Cisco UCS サーバ上で TPM を使用して暗号キーを保存します。

Cisco UCS Manager では、TPM が存在しているか、イネーブルになっているか、有効またはアクティブになっているかどうかを含めた TPM のモニタリングが可能です。

# TPM のプロパティの表示

手順

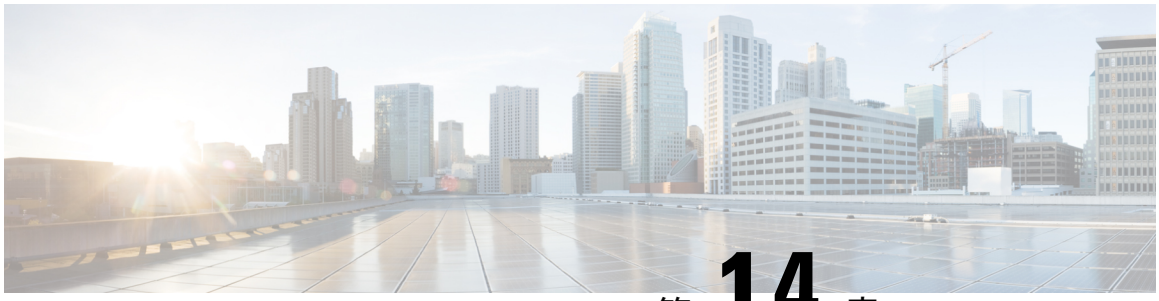
**ステップ 1** [ナビゲーション]ペインで、[機器]をクリックします。

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

**ステップ 3** TPM 設定を表示するサーバを選択します。

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

**ステップ 5** [Motherboard] サブタブをクリックします。



第 14 章

# トラフィック モニタリング



# トラフィック モニタリング

トラフィック モニタリングでは、1 つまたは複数の送信元ポートからのトラフィックをコピーし、コピーされたトラフィックを分析用の専用宛先ポートに送信してネットワーク アナライザに分析させます。この機能は、Switched Port Analyzer（SPAN）としても知られています。

### トラフィック モニタリング セッションの種類

モニタリング セッションが 2 種類あります。

- イーサネット
- ファイバチャネル

宛先ポートの種類により、どのようなモニタリング セッションを必要とするかが決まります。イーサネットのトラフィック モニタリング セッションの場合、宛先ポートは未設定の物理ポートであることが必要です。、Cisco UCS 6454 ファブリック インターコネクト、Cisco UCS 6400 シリーズ ファブリック インターコネクト および 6300 ファブリック インターコネクトを使用

している場合を除いて、ファイバチャネルのトラフィックモニタリングセッションの場合、宛て先ポートはファイバチャネル アップリンクポートであることが必要です。

（注） Cisco UCS 6332、6332-16UP、64108、6454 ファブリック インターコネクトについては、ファイバチャネル宛て先ポートを選択できません。宛先ポートは、未設定の物理イーサネット ポートである必要があります。

### イーサネット全体のトラフィック モニタリング

イーサネット トラフィック モニタリング セッションでは、次のトラフィックの送信元ポートおよび宛先ポートのいずれかをモニタできます。

| 送信元ポート | 宛先のポート |
|---|---|
| • アップリンク イーサネット ポート<br>• イーサネット ポート チャネル<br>• VLAN<br>• サービス プロファイル vNIC<br>• サービス プロファイル vHBA<br>• FCoE ポート<br>• ポート チャネル<br>• ユニファイド アップリンク ポート<br>• VSAN | 未設定のイーサネット ポート |

（注） すべてのトラフィックの送信元は宛先ポートと同じスイッチ内にある必要があります。宛先ポートとして設定されたポートは、送信元ポートとして設定できません。ポート チャネルのメンバ ポートを個別に送信元として設定することはできません。ポート チャネルが送信元として設定されている場合、すべてのメンバ ポートが送信元ポートです。

サーバー ポートは、非仮想化ラックサーバー アダプタへのポートの場合にのみ送信元にすることができます。

### Cisco UCS 6400 シリーズ ファブリック インターコネクトのトラフィックモニタリング

- Cisco UCS 6400 シリーズ ファブリック インターコネクトは、宛て先ポートとしてのファイバチャネルポートをサポートしません。したがって、イーサネット ポートは、このファブリック インターコネクトでトラフィック モニタリング セッションを設定するための唯一のオプションです。

- Cisco UCS 6400 シリーズ ファブリック インターコネクトでは、ファブリック インターコネクトごとに2つ以上の送信元に対する送信方向のトラフィックのモニタリングをサポートします。
- 送信方向と受信方向のトラフィックについて、ポート チャネル送信元で SPAN をモニタまたは使用できます。
- 1 つのモニタ セッションの宛先ポートとしてポートを設定できます。
- 送信方向の送信元としてポート チャネルをモニタできます。
- 送信方向の送信元として vEth をモニタすることはできません。

### Cisco UCS 6300 ファブリック インターコネクトのトラフィック モニタリング

- Cisco UCS 6300 ファブリック インターコネクトはポートベースのミラーリングをサポートしています。
- Cisco UCS 6300 ファブリック インターコネクトは、VLAN SPAN を受信方向でのみサポートします。
- イーサネット SPAN は Cisco UCS 6300 ファブリック インターコネクトに基づいたポートです。

### Cisco UCS 6200 ファブリック インターコネクトのトラフィック モニタリング

- Cisco UCS 6200 および 6324 ファブリック インターコネクトでは、ファブリック インターコネクトごとに最大2つの送信元で「送信」方向のモニタリング トラフィックがサポートされています。
- Cisco UCS 6200 では、SPAN トラフィックは SPAN 宛先ポートの速度により レート制限されています。これは 1 Gbps または 10 Gbps のいずれかです。

**重要** (6200 および 6324 ファブリック インターコネクトの場合) 入力トラフィック専用ポート チャネル上で SPAN の使用またはモニタができます。

### ファイバ チャネル全体のトラフィック モニタリング

ファイバチャネル トラフィック アナライザまたはイーサネット トラフィック アナライザを使用して、ファイバチャネル トラフィックをモニタできます。ファイバチャネル トラフィックが、イーサネット宛先ポートでイーサネット トラフィック モニタリング セッションでモニタされる場合、宛先トラフィックは FCoE になります。Cisco UCS 6300 ファブリック インターコネクトは、FC SPAN を、入力側でのみサポートします。Cisco UCS 6248 ファブリック インターコネクトのファイバ チャネル ポートは送信元ポートとして設定できません。

ファイバ チャネル トラフィック モニタリング セッションでは、次のトラフィックの送信元ポートおよび宛先ポートのいずれかをモニタできます。

| 送信元ポート | 宛先のポート |
|---|---|
| • FC ポート<br>• FCポートチャネル<br>• アップリンク ファイバ チャネル ポート<br>• SAN ポート チャネル<br>• VSAN<br>• サービス プロファイル vHBA<br>• ファイバ チャネル ストレージ ポート | • ファイバ チャネル アップリンク ポート<br>• 未構成のイーサネット ポート（Cisco UCS 64108、6454、6332、および 6332-16UP ファブリック インターコネクト） |

# トラフィック モニタリングに関するガイドラインと推奨事項

トラフィック モニタリングを設定するか、アクティブにする場合は、次のガイドラインを考慮してください。

### トラフィックモニタリングセッション

トラフィック モニタリング セッションは作成時にはデフォルトでディセーブルです。トラフィック モニタリングを開始するには、まずセッションをアクティブにします。トラフィック モニタリング セッションは、Cisco UCSポッド内のどのファブリック インターコネクトでも固有である必要があります。一意の名前と一意の VLAN ソースを使用して各モニタリング セッションを作成します。サーバからのトラフィックを監視するには、サーバに対応するサービス プロファイルからすべての vNIC を追加します。

（注） 1 つの SPAN モニタリング セッションに追加できる VLAN は 32 までです。

### ファブリック インターコネクトごとにサポートされるアクティブ トラフィック モニタリング セッションの最大数

トラフィック モニタリング セッションは最大 16 まで作成し保存できますが、同時にアクティブにできるのは 4 つだけです。各 Cisco UCS 6400 シリーズ ファブリック インターコネクトおよび 6300 ファブリック インターコネクトについては、最大 4 個のトラフィック方向のみをモニタできます。受信および送信方向は、それぞれ 1 モニタリング セッションとしてカウントされます。一方、双方向モニタリング セッションは、2 モニタリング セッションとしてカウントされます。次に例を示します。

- 4 つのアクティブ セッション：各セッションが 1 方向だけでトラフィックをモニタするように設定されている場合。
- 2 アクティブ セッション：各セッションが双方向のトラフィックをモニタリングするように設定されている場合。
- 3 アクティブ セッション：1 つのセッションが単方向で、もう 1 つのセッションが双方向の場合。

（注） トラフィック モニタリングは、システム リソースにかなりの負荷をかけることがあります。負荷を最小限にするには、不必要なトラフィックができるだけ少ない送信元を選択し、不必要なときにはトラフィック モニタリングをディセーブルにします。

### vNIC

トラフィック モニタリングの宛先は単一の物理ポートであるため、トラフィック モニタリング セッションは 1 つのファブリックだけを監視できます。ファブリック フェールオーバーにわたって中断されない vNIC トラフィックをモニタリングするには、ファブリックごとに 1 つ、合計 2 つのセッションを作成し、2 台のアナライザを接続します。両方のセッションでまったく同じ名前を使用して、トラフィックの送信元として vNIC を追加します。仮想コンピュータのポート プロファイルを変更すると、送信元ポートとして使用されている、関連付けられた vNIC はモニタリングから削除され、モニタリング セッションを再設定する必要があります。トラフィック モニタリング セッションが Cisco UCS Manager リリース 2.0 より前のリリースのもとでダイナミック vNIC で設定された場合、アップグレード後にトラフィック モニタリング セッションを再設定する必要があります。Cisco UCS 6200 は、送信方向での vNIC からのトラフィック モニタリングをサポートします。ただし、Cisco UCS 6400 シリーズ ファブリック インターコネクトは、送信方向で vNIC からのトラフィックモニタリング トラフィックをサポートしていません。

### vHBA

vHBA はイーサネットまたはファイバ チャネルのどちらのモニタリング セッションの送信元としても設定できますが、同時に両方の送信元とすることはできません。VHBA が SPAN 送信元として設定されている場合、 SPAN 宛先は、VN タグが付いたフレームのみを受信します。これは、直接 FC フレームを受信しません。Cisco UCS 6200 では、送信方向 vHBA からのトラフィック モニタリングをサポートします。ただし、Cisco UCS 6400 シリーズ ファブリック インターコネクトは、送信方向で vHBA からのトラフィックモニタリング トラフィックをサポートしていません。

# イーサネット トラフィック モニタリング セッションの作成

## 手順

**ステップ 1** [Create Traffic Monitoring Session] ダイアログボックスで、次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| [名前（Name）] フィールド | トラフィック モニタリング セッションの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **[Admin State]** フィールド | [Destination] フィールドで選択された物理ポートのトラフィックをモニタするかどうかを示します。次のいずれかになります。<br>• **[Enabled]**：ソース コンポーネントがセッションに追加されるとすぐに、Cisco UCS によって、ポート アクティビティのモニタリングが開始されます。<br>• **[Disabled]**：Cisco UCS によるポート アクティビティのモニタリングは実行されません。 |
| **[Span Control Packets]**フィールド | CPU から送信された発信制御パケットをモニタリングするかどうかを示します。次のいずれかになります。<br>• **[Enabled]**：Cisco UCSポート上の発信制御パケットをモニタリングします。<br>• **[Disabled]**—Cisco UCSポート上の発信の制御パケットをモニタリングしません。 |
| **[Destination]** ドロップダウン リスト | モニタされている物理ポート。<br>ポートのプロパティを表示するには、このフィールドのリンクをクリックします。 |

| 名前 | 説明 |
|---|---|
| **[Admin Speed]** フィールド | モニタされるポート チャネルのデータ転送速度。<br>使用可能なデータ速度は、Cisco UCS ドメインにインストールされているファブリック インターコネクトによって異なります。6332 および 6332-16UP FI のイーサネット トラフィック モニタリング セッションでは、設定済みのイーサネット宛先ポートに 1 Gbps の速度設定を使用することはできません。 |

**ステップ 2** [OK] をクリックします。

### 次のタスク

- トラフィック モニタリング セッションにトラフィック ソースを追加します。
- トラフィック モニタリング セッションをアクティブ化します。

# 既存のイーサネット トラフィック モニタリング セッションの宛先の設定

### 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** [LAN] タブで、**[LAN]** > **[Traffic Monitoring Sessions]** > **[*Fabric_Interconnect_Name*]** > **[*Monitor_Session_Name*]** の順に展開します。

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

**ステップ 4** [Actions] 領域で、[Set Destination] をクリックします。

**ステップ 5** [Set Destination] ダイアログボックスで、次のフィールドに入力します。

**例：**

| 名前 | 説明 |
|---|---|
| **[Destination]** ドロップダウン リスト | ソースからのすべての通信をモニタする物理ポート。 |

| 名前 | 説明 |
|---|---|
| **[Admin Speed]** フィールド | モニタされるポート チャネルのデータ転送速度。<br>使用可能なデータ速度は、Cisco UCS ドメインにインストールされているファブリック インターコネクトによって異なります。6332 および 6332-16UP FI のイーサネット トラフィック モニタリング セッションでは、設定済みのイーサネット宛先ポートに 1 Gbps の速度設定を使用することはできません。 |

**ステップ 6** **[OK]** をクリックします。

# 既存のイーサネット トラフィック モニタリング セッションの宛先のクリア

**手順**

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[トラフィック モニタリング セッション（Traffic Monitoring Sessions）]** > ***[Fabric_Interconnect_Name]*** > ***[Monitor_Session_Name]*** の順に展開します。

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

**ステップ 4** [Actions] 領域で、[Clear Destination] をクリックします。

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

# ファイバ チャネル トラフィック モニタリング セッションの作成

**手順**

**ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。

**ステップ 2** **[SAN]** > **[Traffic Monitoring Sessions]** > **[Fabric_Interconnect_Name]** の順に展開します

**ステップ 3** ***[Fabric_Interconnect_Name***]を右クリックし、**[トラフィックモニタリングセッションの作成]**を選択します。

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

| 名前 | 説明 |
|---|---|
| [名前（Name）] フィールド | トラフィック モニタリング セッションの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **[Admin State]** フィールド | [Destination] フィールドで選択された物理ポートのトラフィックをモニタするかどうかを示します。次のいずれかになります。<br>• **[Enabled]**：ソース コンポーネントがセッションに追加されるとすぐに、Cisco UCS によって、ポート アクティビティのモニタリングが開始されます。<br>• **[Disabled]**：Cisco UCS によるポート アクティビティのモニタリングは実行されません。 |
| **[Span Control Packets]**フィールド | CPU から送信された発信制御パケットをモニタリングするかどうかを示します。次のいずれかになります。<br>• **[Enabled]**：Cisco UCSポート上の発信制御パケットをモニタリングします。<br>• **[Disabled]**—Cisco UCSポート上の発信の制御パケットをモニタリングしません。 |
| **[Destination]** ドロップダウン リスト | ソースからのすべての通信をモニタする物理ポートを選択します。 |
| **[Admin Speed]** ドロップダウン リスト | モニタされるポート チャネルのデータ転送速度。使用可能なデータ速度は、Cisco UCS ドメインにインストールされているファブリック インターコネクトによって異なります。次のいずれかになります。<br>• **1 Gbps**<br>• **10 Gbps**<br>• **25Gbps**<br>• **[Auto]**：Cisco UCSがデータ転送速度を決定します。 |

**ステップ 5** [OK] をクリックします。

### 次のタスク

- トラフィック モニタリング セッションにトラフィック ソースを追加します。
- トラフィック モニタリング セッションをアクティブ化します。

# 既存のファイバ チャネル モニタリング セッションの宛先の設定

### 手順

**ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。

**ステップ 2** **[SAN]** > **[Traffic Monitoring Sessions]** > ***[Fabric_Interconnect_Name]*** > ***[Monitor_Session_Name]*** の順に展開します

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

**ステップ 4** [Actions] 領域で、[Set Destination] をクリックします。

**ステップ 5** [Set Destination] ダイアログボックスで、次のフィールドに入力します。

| 名前 | 説明 |
|---|---|
| **[Destination]** ドロップダウン リスト | ソースからのすべての通信をモニタする物理ポートを選択します。 |
| **[Admin Speed]** ドロップダウン リスト | モニタされるポート チャネルのデータ転送速度。使用可能なデータ速度は、Cisco UCS ドメインにインストールされているファブリック インターコネクトによって異なります。次のいずれかになります。<br>• **1 Gbps**<br>• **2 Gbps**<br>• **[4 Gbps]**<br>• **[8 Gbps]**<br>• **[Auto]**：Cisco UCSがデータ転送速度を決定します。 |

**ステップ 6** **[OK]** をクリックします。

# 既存のファイバチャネル トラフィック モニタリング セッションの宛先のクリア

### 手順

**ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。

**ステップ 2** **[SAN]** > **[Traffic Monitoring Sessions]** > **[Fabric_Interconnect_Name]** > **[Monitor_Session_Name]** の順に展開します

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

**ステップ 4** [Actions] 領域で、[Clear Destination] をクリックします。

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

# モニタリング セッションへのトラフィック送信元の追加

トラフィック モニタリング セッションがモニタする複数の送信元タイプから複数の送信元を選択できます。選択できる送信元は、Cisco UCS ドメインに設定したコンポーネントによって異なります。

（注） この手順では、イーサネット トラフィックのモニタリング セッションに対して送信元を追加する方法について説明します。ファイバ チャネルのモニタリング セッションに送信元を追加する場合は、ステップ 2 の [LAN] タブの代わりに [SAN] タブを選択します。

### 始める前に

トラフィック モニタリング セッションが作成されている必要があります。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[トラフィック モニタリング セッション（Traffic Monitoring Sessions）]** > ***[Fabric_Interconnect_Name]*** の順に展開します。

**ステップ 3** ***[Fabric_Interconnect_Name]*** を展開し、設定するモニタ セッションをクリックします。

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

**ステップ 5** [Sources] 領域で、追加するトラフィック送信元のタイプのセクションを展開します。

**ステップ 6** モニタリングに使用できるコンポーネントを確認するには、テーブルの右端にある [+] ボタンをクリックして [Add Monitoring Session Source] ダイアログボックスを開きます。

**ステップ 7** 送信元コンポーネントを選択して [OK] をクリックします。

必要に応じて、上記の3つの手順を繰り返して、複数の送信元タイプから複数の送信元を追加できます。

**ステップ 8** **[Save Changes]**をクリックします。

### 次のタスク

トラフィック モニタリング セッションをアクティブ化します。セッションがすでにアクティブ化されている場合、送信元を追加すると、トラフィックはモニタリングの宛先に転送されます。

# トラフィック モニタリング セッションのアクティブ化

（注） この手順では、イーサネット トラフィックのモニタリング セッションをアクティブにする方法について説明します。ファイバチャネルモニタリングセッションをアクティブ化するには、ステップ 2 で [LAN] タブの代わりに [SAN] タブを選択します。

### 始める前に

トラフィック モニタリング セッションが作成されている必要があります。

### 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[トラフィック モニタリング セッション（Traffic Monitoring Sessions）]** > ***[Fabric_Interconnect_Name]*** の順に展開します。

**ステップ 3** ***[Fabric_Interconnect_Name]*** を展開し、アクティブにするモニタ セッションをクリックします。

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

**ステップ 5** [Properties] 領域で、[Admin State] の [enabled] オプション ボタンをクリックします。

**ステップ 6** **[Save Changes]**をクリックします。

トラフィック モニタの送信元が設定されている場合、トラフィック モニタリングの宛先ポートにトラフィックのフローが始まります。

# トラフィック モニタリング セッションの削除

（注） この手順では、イーサネット トラフィックのモニタリング セッションを削除する方法について説明します。ファイバ チャネル モニタリング セッションを削除するには、ステップ 2 で [LAN] タブの代わりに [SAN] タブを選択します。

## 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

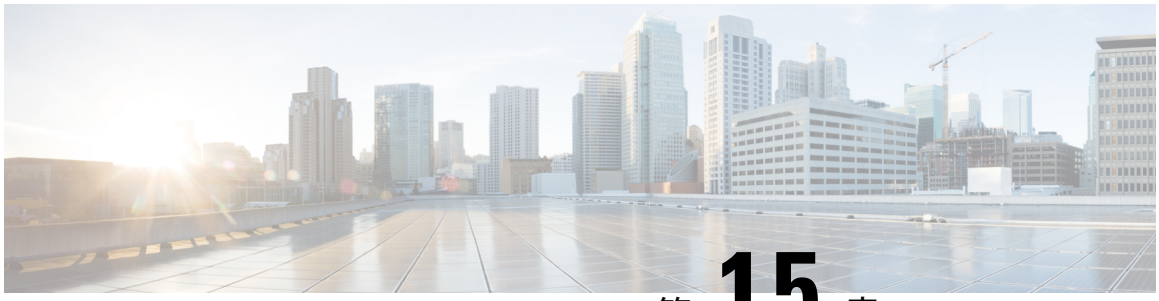
**ステップ 2** **[LAN]** > **[トラフィック モニタリング セッション（Traffic Monitoring Sessions）]** > ***[Fabric_Interconnect_Name]*** の順に展開します。

**ステップ 3** ***[Fabric_Interconnect_Name]*** を展開し、削除するモニタ セッションをクリックします。

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

**ステップ 5** [Actions] 領域で、[Delete] アイコンをクリックします。

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



第 15 章

# NetFlow モニタリング



# NetFlow モニタリング

NetFlow は、IP トラフィック データを収集するための標準ネットワーク プロトコルです。NetFlowにより、特定の特性を共有する単方向IPパケットに関して、フローを定義することができます。フロー定義に一致するすべてのパケットが収集され、1 つ以上の外部 NetFlow コレクタにエクスポートされます。そこでは、アプリケーション固有の処理のために、さらに集約、分析、および使用されます。

Cisco UCS Manager は、Netflow 対応アダプタ（Cisco UCS VIC 1200 シリーズ、Cisco UCS VIC 1300 シリーズ、Cisco UCS VIC 1400 シリーズ）を使用して、フロー情報を収集し、エクスポートするルータおよびスイッチと通信します。

（注）
- NetFlow モニタリングは、Cisco UCS 6400 シリーズ ファブリック インターコネクトではサポートされていません。
- リリース 3.0(2) では、NetFlow モニタはエンド ホスト モードでのみサポートされます。

### ネットワーク フロー

フローとは、トラフィックの送信元または送信先、ルーティング情報、使用されているプロトコルなど、共通のプロパティを持つ一連の単方向 IP パケットです。フローは、フロー レコード定義での定義に一致する場合に収集されます。

### フロー レコード定義

フロー レコード定義は、フロー定義で使用されるプロパティに関する情報で構成され、特性プロパティと測定プロパティの両方を含めることができます。フローキーとも呼ばれる特性プロパティは、フローを定義するプロパティです。 Cisco UCS Manager では IPv4、IPv6,、およびレイヤ 2 のキーがサポートされています。フロー値または非キーとも呼ばれる測定された特性は、フローのすべてのパケットに含まれるバイト数またはパケットの合計数などの、測定できる値です。

フロー レコード定義は、フロー キーとフロー値の特定の組み合わせです。次の 2 つのタイプのフロー レコード定義があります。

- **[System-defined]**：Default flow record definitions supplied by Cisco UCS Managerが提供するデフォルトのフロー レコード定義。
- [User-defined]：ユーザが独自に作成できるフロー レコード定義。

### フロー エクスポータ、フロー エクスポータ プロファイル、およびフロー コレクタ

フロー エクスポータは、フロー エクスポータ プロファイルの情報に基づき、フロー コネクタにフローを転送します。フロー エクスポータ プロファイルには、NetFlow パケットをエクスポートする際に使用されるネットワーキング プロパティが含まれます。ネットワーキング プロパティには、各ファブリック インターコネクトの VLAN、送信元 IP アドレス、およびサブネット マスクが含まれます。

（注） Cisco UCS Manager GUIでは、ネットワーキング プロパティは、プロファイルに含まれているエクスポータ インターフェイスで定義されます。Cisco UCS Manager CLIでは、プロパティはプロファイルで定義されます。

フロー コレクタは、フロー エクスポータからフローを受信します。各フロー コレクタには、フローの送信先を定義する、IP アドレス、ポート、外部ゲートウェイ IP、VLAN が含まれます。

### フロー モニタおよびフロー モニタ セッション

フローモニタは、フロー定義、1つまたは2つのフローエクスポータ、タイムアウトポリシーで構成されます。フローモニタを使用することで、どのフロー情報をどこから収集するかを指定できます。各フロー モニタは、出力または入力のどちらかの方向で動作します。

フロー モニタ セッションには、次の 4 つまでのフロー モニタが含まれます。入力方向の 2 つのフロー モニタと出方向の 2 つのフロー モニタ。また、フロー モニタ セッションは、vNIC に関連付けることができます。

# NetFlow に関する制限事項

NetFlow モニタリングには、次の制限事項が適用されます。

- NetFlow モニタリングは、Cisco UCS 6400 シリーズ ファブリック インターコネクトではサポートされていません。
- NetFlow モニタリングは、Cisco UCS 1200、1300、1400 VIC アダプタでサポートされています。ただし、1200 シリーズの VIC アダプタでは、FCoE トラフィックに対して NetFlow を使用することは推奨されません。
- 最大 64 のフロー レコード定義、フロー エクスポータ、フロー モニタを使用できます。
- NetFlow は、vNIC テンプレート オブジェクトではサポートされません。
- PVLAN およびローカル VLAN は、サービス VLAN に対してサポートされません。
- すべての VLAN は公開されており、両方のファブリック インターコネクトに共通である必要があります。
- VLAN はフロー コレクタと併用する前に、エクスポータ インターフェイスとして定義する必要があります。
- NetFlow は、usNIC、仮想マシン キュー、RoCE、Geneve、または vNIC が有効化された Linux ARFS と併用できません。

# NetFlow モニタリングの有効化

機能を動作させるには、NetFlow モニタリングを有効にする必要があります。

**手順**

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** を展開します。

**ステップ 3** [General] タブをクリックします。

**ステップ 4** **[Admin State]** フィールドで **[Enabled]** ラジオ ボタンをクリックして NetFlow モニタリングを有効にします。

**ステップ 5** **[Save Changes]** をクリックして、設定変更を保存します。

# フロー レコード定義の作成

## 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** を展開します。

**ステップ 3** [Flow Record Definitions] を右クリックし、[Create Flow Record Definition] を選択します。

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

| フィールド | 説明 |
|---|---|
| **名前（Name）** | フロー レコード定義の名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Description** | フロー レコード定義のユーザ定義の説明。 |
| **Keys** | 使用するキーのオプション ボタンを選択します。次のいずれかになります。<br>• [IPv4]：IPv4 キーで選択ウィンドウに入力します。<br>• [IPv6]：IPv6 キーで選択ウィンドウに入力します。<br>• [Layer 2 Switched]：レイヤ 2 キーで選択ウィンドウに入力します。<br>フローに含まれるプロパティのチェックボックスをオンにします。 |
| **Measured Properties** | フローの対象とする非キー フィールドのチェックボックスをオンにします。これは次のいずれか、または複数の値になります。<br>• **Counter Bytes Long**<br>• **Counter Packets Long**<br>• **Sys Uptime First**<br>• **Sys Uptime Last** |

**ステップ 5** [OK] をクリックします。

# フロー レコード定義の表示

**手順**

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** を展開します。

**ステップ 3** すべてのフロー定義のリストを表示するには、[Flow Record Definitions] を選択します。

**ステップ 4** 指定したフロー定義のプロパティを表示するには、フロー定義の名前をダブルクリックします。

[Properties] ウィンドウで、フローに使用するキーおよび非キーを変更できます。

# エクスポータ プロファイルの定義

**手順**

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** > **[フロー エクスポータ（Flow Exporters）]** > **[フロー エクスポータ プロファイル（Flow Exporter Profiles）]** を展開します。

**ステップ 3** [Flow Exporter Profile default] をクリックします。

**ステップ 4** [Properties] 領域で、[Exporter Interface(s)] テーブルの横にある [Add] をクリックします。

**ステップ 5** [Create Exporter Interface] ダイアログボックスで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| **VLAN** | エクスポータ インターフェイスと関連付ける VLAN を選択するか、[Create VLANs] をクリックして新しい VLAN を作成します。<br><br>PVLAN とローカル VLAN はサポートされません。すべての VLAN は公開されており、両方のファブリック インターコネクトに共通である必要があります。 |

| 名前 | 説明 |
|---|---|
| **Fabric A Source IP** | ファブリック A でのエクスポータ インターフェイスの送信元 IP。<br>**重要** 指定する IP アドレスが Cisco UCS ドメイン内で固有であることを確認します。すでに Cisco UCS Manager で使用されている IP アドレスを指定すると、IP アドレスの競合が発生する可能性があります。 |
| **Fabric A Subnet Mask** | ファブリック A でのエクスポータ インターフェイスのサブネット マスク。 |
| **Fabric B Source IP** | ファブリック B でのエクスポータ インターフェイスの送信元 IP。<br>**重要** 指定する IP アドレスが Cisco UCS ドメイン内で固有であることを確認します。すでに Cisco UCS Manager で使用されている IP アドレスを指定すると、IP アドレスの競合が発生する可能性があります。 |
| **Fabric B Subnet Mask** | ファブリック B でのエクスポータ インターフェイスのサブネット マスク。 |

**ステップ 6** [OK] をクリックします。

# フロー コレクタの作成

手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。
**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** を展開します。
**ステップ 3** [Work] ペインで、[Flow Collectors] タブをクリックします。
**ステップ 4** [Flow Collectors] テーブルの横にある [Add] をクリックします。
**ステップ 5** [Create Flow Collectors] ダイアログボックスで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| 名前（**Name**） | フロー コレクタの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Description** | フロー コレクタのユーザ定義の説明。 |
| **Collector IP** | フロー コレクタの IP アドレス。 |
| **Port** | フロー コレクタのポート。1 ～ 65535 の値を入力します。 |
| **Exporter Gateway IP** | フロー コレクタの外部ゲートウェイ IP。 |
| **VLAN** | フロー コレクタに関連付けられた VLAN。<br>VLAN はフロー コレクタと併用する前に、[Create Exporter Interface] ダイアログボックスで定義する必要があります。 |

**ステップ 6** [OK] をクリックします。

# フロー エクスポータの作成

手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** を展開します。

**ステップ 3** [Flow Exporters] を右クリックし、[Create Flow Exporter] を選択します。

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

| 名前 | 説明 |
|---|---|
| 名前（**Name**） | フロー エクスポータの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Description** | フロー エクスポータのユーザ定義の説明。 |

| 名前 | 説明 |
|---|---|
| **DSCP** | DiffServ コード ポイント（DSCP）値。値の範囲は、0 ～ 63 です。 |
| **Version** | エクスポータのバージョン。デフォルトでは、これはバージョン 9 になります。 |
| **Exporter Profile** | フロー エクスポータに関連付けるエクスポータ プロファイル。 |
| **Flow Collector** | フローエクスポータに関連付けるフローコレクタを選択するか、[Create Flow Exporter] をクリックして新規に作成します。 |
| **Template Data Timeout** | NetFlow テンプレート データ再送信のタイムアウト期間。<br>1 ～ 86400 の範囲で値を入力します。 |
| **Option Exporter Stats Timeout** | NetFlow フロー エクスポータ データ再送信のタイムアウト期間。<br>1 ～ 86400 の範囲で値を入力します。 |
| **Option Interface Table Timeout** | NetFlow フロー エクスポータ インターフェイス テーブル再送信のタイムアウト期間。<br>1 ～ 86400 の範囲で値を入力します。 |

**ステップ 5** [OK] をクリックします。

# フロー モニタの作成

### 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。
**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** を展開します。
**ステップ 3** [Flow Monitors] を右クリックし、[Create Flow Monitor] を選択します。
**ステップ 4** [Create Flow Monitor] ダイアログボックスで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| 名前（**Name**） | フロー モニタの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Description** | フロー モニタのユーザ定義の説明。 |
| **Flow Definition** | 値のリストから使用するフロー 定義を選択するか、[Create Flow Record Definition] をクリックして新規に作成します。 |
| **Flow Exporter 1** | 値のリストから使用するフロー エクスポータを選択するか、[Create Flow Record Exporter] をクリックして新規に作成します。 |
| **Flow Exporter 2** | 値のリストから使用するフロー エクスポータを選択するか、[Create Flow Record Exporter] をクリックして新規に作成します。 |
| **Timeout Policy** | 使用するタイムアウト ポリシーを値のリストから選択します。 |

**ステップ 5** [OK] をクリックします。

# フロー モニタ セッションの作成

### 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。
**ステップ 2** **[LAN]** > **[ネットフロー モニタリング（Netflow Monitoring）]** を展開します。
**ステップ 3** [Flow Monitor Sessions] を右クリックし、[Create Flow Monitor Session] を選択します。
**ステップ 4** [Create Flow Monitor Session] ダイアログボックスで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| 名前（**Name**） | フロー モニタ セッションの名前。<br>この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Description** | フロー モニタ セッションのユーザ定義の説明。 |
| **Host Receive Direction Monitor 1** | 値のリストから使用するフロー モニタを選択するか、[Create Flow Monitor] をクリックして新規に作成します。 |
| **Host Receive Direction Monitor 2** | 値のリストから使用するフロー モニタを選択するか、[Create Flow Monitor] をクリックして新規に作成します。 |
| **Host Transmit Direction Monitor 1** | 値のリストから使用するフロー モニタを選択するか、[Create Flow Monitor] をクリックして新規に作成します。 |
| **Host Transmit Direction Monitor 2** | 値のリストから使用するフロー モニタを選択するか、[Create Flow Monitor] をクリックして新規に作成します。 |

**ステップ 5** [OK] をクリックします。

# vNIC へのフロー モニタ セッションの関連付け

### 手順

**ステップ 1** [ナビゲーション]ペインで、[LAN]をクリックします。

**ステップ 2** **[LAN]** > **[ネットフローモニタリング（Netflow Monitoring）]** > **[フロー モニタ セッション（Flow Monitor Sessions）]** を展開します。

**ステップ 3** 関連付けるフロー モニタ セッションをクリックします。

**ステップ 4** [Flow Exporter Profile default] をクリックします。

**ステップ 5** [Properties] 領域で、[vNICs] を展開します。

**ステップ 6** テーブルの横にある [Add] をクリックします。

**ステップ 7** [Add Monitoring Session Source] ダイアログボックスで、フロー モニタ セッションと関連付ける vNIC を選択します。

**ステップ 8** [OK] をクリックして、ダイアログボックスを閉じます。

**ステップ 9** [Save] をクリックして、ダイアログボックスを閉じます。

翻訳について
このドキュメントは、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。