Cisco UCS Manager システム モニタリング ガイド（CLI 用）、リリース 4.3

最終更新：2025 年 10 月 20 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/

© 2023–2025 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに xi

対象読者 xi

表記法 xi

Cisco UCS の関連ドキュメント xiii

マニュアルに関するフィードバック xiii

第 1 章

このリリースの新規情報および変更情報 1

新機能および変更された機能に関する情報 1

第 2 章

システム モニタリングの概要 5

システム モニタリングの概要 5

Cisco UCS Manager コアと障害の生成 6

Cisco UCS Manager ユーザ CLI ドキュメント 8

第 3 章

Syslog 11

Syslog 11

ローカル ファイルへの Syslog メッセージ保存のイネーブル化 12

第 4 章

システム イベント ログ 17

システム イベント ログ 17

サーバのシステム イベント ログの表示 18

各サーバのシステム イベント ログの表示 18

シャーシ内の全サーバのシステム イベント ログの表示 19

SEL ポリシーの設定 20

サーバのシステム イベント ログのバックアップ 22
個々のサーバのシステム イベント ログのバックアップ 22
シャーシ内の全サーバのシステム イベント ログのバックアップ 23
サーバのシステム イベント ログのクリア 23
個々のサーバのシステム イベント ログのクリア 23
シャーシ内の全サーバのシステム イベント ログのクリア 24

第 5 章 監査ログ 25
監査ログ 25
監査ログの表示 25

第 6 章 ログ ファイル エクスポータ 27
ログ ファイル エクスポータ 27
リモート サーバへのログ ファイルのエクスポート 28

第 7 章 Core File Exporter 31
Core File Exporter 31
Core File Exporter の設定 31
Core File Exporter のディセーブル化 32

第 8 章 システムのモニタリングとデバッグ 35
デバッグ プラグインのロード 35

第 9 章 障害の収集と抑制 37
グローバル障害ポリシー 37
障害収集ポリシーの設定 38
フォールト抑制 39
シャーシに対する障害抑制の設定 40
固定時間間隔を使用したシャーシに対する障害抑制タスクの設定 40
スケジュールを使用したシャーシに対する障害抑制タスクの設定 42
シャーシに対する障害抑制タスクの変更 44

シャーシに対する抑制された障害と障害抑制タスクの表示 46
シャーシに対する障害抑制タスクの削除 47
I/O モジュールに対する障害抑制の設定 47
固定時間間隔を使用した IOM に対する障害抑制タスクの設定 47
スケジュールを使用した IOM に対する障害抑制タスクの設定 49
IOM に対する障害抑制タスクの変更 50
IOM に対する抑制された障害と障害抑制タスクの表示 51
IOM に対する障害抑制タスクの削除 53
FEX に対する障害抑制の設定 53
固定時間間隔を使用した FEX に対する障害抑制タスクの設定 53
スケジュールを使用した FEX に対する障害抑制タスクの設定 55
FEX に対する障害抑制タスクの変更 56
FEX に対する抑制された障害と障害抑制タスクの表示 58
FEX に対する障害抑制タスクの削除 59
サーバに対する障害抑制の設定 59
固定時間間隔を使用したサーバに対する障害抑制タスクの設定 59
スケジュールを使用したサーバに対する障害抑制タスクの設定 60
サーバに対する障害抑制タスクの変更 62
スケジュールの作成 63
サーバに対する抑制された障害と障害抑制タスクの表示 64
サーバに対する障害抑制タスクの削除 65
サービス プロファイルに対する障害抑制の設定 65
固定時間間隔を使用したサービス プロファイルに対する障害抑制タスクの設定 65
スケジュールを使用したサービス プロファイルに対する障害抑制タスクの設定 66
サービス プロファイルに対する障害抑制タスクの変更 68
サービス プロファイルに対する抑制された障害と障害抑制タスクの表示 69
サービス プロファイルに対する障害抑制タスクの削除 70
組織に対する障害抑制の設定 71
固定時間間隔を使用した組織に対する障害抑制タスクの設定 71
スケジュールを使用した組織に対する障害抑制タスクの設定 72
組織に対する障害抑制タスクの変更 73

組織に対する抑制された障害と障害抑制タスクの表示 74
組織に対する障害抑制タスクの削除 75

第 10 章 SNMP の設定 77
SNMP の概要 77
SNMP 機能の概要 77
SNMP 通知 78
SNMP セキュリティ レベルおよび権限 78
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 79
SNMPv3 セキュリティ機能 80
SNMP サポート 80
SNMP の設定 81
SNMP の有効化と SNMP プロパティの設定 81
SNMP トラップの作成 82
SNMP トラップの削除 83
テスト SNMP トラップの生成 84
SNMPv3 ユーザの作成 85
SNMPv3 ユーザの削除 86

第 11 章 統計情報収集ポリシーの設定 89
統計情報収集ポリシー 89
統計情報収集ポリシーの変更 90

第 12 章 Call Home および Smart Call Home の設定 91
UCS の Call Home の概要 91
Call Home の考慮事項とガイドライン 94
Cisco UCSの障害と Call Home のシビラティ（重大度） 95
Cisco Smart Call Home 96
Anonymous Reporting 98
Call Home の設定 98
Call Home のイネーブル化 101

Call Home のディセーブル化 102
システム インベントリ メッセージの設定 103
システム インベントリ メッセージの設定 103
システム インベントリ メッセージの送信 104
Call Home プロファイルの設定 104
Call Home プロファイル 104
Call Home アラート グループ 105
Call Home プロファイルの設定 106
Call Home プロファイルの削除 108
テスト Call Home アラートの送信 108
Call Home ポリシーの設定 110
Call Home ポリシー 110
Call Home ポリシー 110
Call Home ポリシーのディセーブル化 111
Call Home ポリシーのイネーブル化 112
Call Home ポリシーの削除 112
Anonymous Reporting の設定 113
Anonymous Reporting のイネーブル化 113
Anonymous Reporting のディセーブル化 114
Anonymous レポートの表示 115
Smart Call Home の設定 116
Smart Call Home の設定 116
デフォルトの Cisco TAC-1 プロファイルの設定 118
Smart Call Home 用のシステム インベントリ メッセージの設定 119
Smart Call Home の登録 121

第 13 章 データベースのヘルス モニタリング 123
Cisco UCS Manager データベースのヘルス モニタリング 123
内部バックアップの間隔の変更 123
ヘルス チェックのトリガー 124
ヘルス チェックの間隔の変更 124

第 14 章 ハードウェア モニタリング 127

システム モニタリング CLI コマンドのチート シート 127

シャーシの管理 129

シャーシのロケータ LED の電源投入 129

シャーシのロケータ LED の電源切断 129

ブレード サーバの管理 130

ブレード サーバーのロケータ LED の電源投入 130

ブレード サーバーのロケータ LED の電源切断 131

ラックマウント サーバの管理 131

ラックマウント サーバーのロケータ LED の電源投入 131

ラックマウント サーバーのロケータ LED の電源切断 132

ラックマウント サーバーのステータスの表示 132

ラックマウント サーバのホスト イーサネット インターフェイス ステータスのモニタリング 133

PCIe ノードのモニタリング 134

ファン モジュールのモニタリング 135

管理インターフェイスのモニタリング 137

管理インターフェイス モニタリング ポリシー 137

管理インターフェイス モニタリング ポリシーの設定 138

ローカル ストレージのモニタリング 140

ローカル ストレージ モニタリングのサポート 141

ローカル ストレージ モニタリングの前提条件 142

レガシー ディスク ドライブのモニタリング 142

ローカル ディスク ロケータ LED のオン 143

ローカル ディスク ロケータ LED のオフ 143

ローカル ディスク ロケータ LED の状態の表示 144

フラッシュ ライフ ウェア レベル モニタリング 145

Flash 寿命ステータスの表示 145

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 146

ディスク ドライブのステータスの確認 150

RAID コントローラ動作の表示 151
RAID コントローラ統計の表示 152
RAID バッテリ ステータスのモニタリング 152
グラフィックス カードのモニタリング 153
グラフィックス カード サーバ サポート 153
グラフィックス カードのプロパティの表示 154
グラフィックス コントローラのプロパティの表示 155
PCI スイッチのモニタリング 156
PCI スイッチ サーバ サポート 156
PCI スイッチ プロパティの表示 156
Transportable Flash Module と スーパーキャパシタの管理 157
TFM とスーパーキャパシタの注意事項および制約事項 157
TPM モニタリング 158
TPM のプロパティの表示 158

第 15 章 NetFlow のモニタリング 161
NetFlow モニタリング 161
NetFlow に関する制限事項 163
NetFlow のモニタリングの有効化または無効化 164
フロー レコード定義の設定 165
エクスポータ プロファイルの設定 166
NetFlow コレクタの設定 167
フロー エクスポータの設定 168
フロー モニタの設定 169
フロー モニタ セッションの設定 170
NetFlow キャッシュのアクティブおよび非アクティブ タイムアウトの設定 171
vNIC へのフロー モニタ セッションの関連付け 172

第 16 章 トラフィック モニタリング 173
トラフィック モニタリング 173
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 176

トラフィック モニタリング セッション間の選択 178
SPAN のトラフィック モニタリング 179
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 179
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 180
ERSPAN のトラフィック モニタリング 182
発信元インターフェイスの設定 182
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 184
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 185
ERSPAN の切り捨て 187
ERSPAN 切り捨ての設定 187
ERSPAN 切り捨ての表示または変更 189
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 191
モニタリング セッションへのアップリンク ソース ポートの追加 191
モニタリング セッションへの VLAN または VSAN 発信元の追加 192
モニタリング セッションへのストレージ ポート送信元の追加 194
モニタリング セッションへの vNIC 送信元の追加 195
モニタリング セッションへのポート チャネル送信元の追加 196
モニタリング セッションへのブレークアウト インターフェイス送信元の追加 197
モニタリング セッションへの FCoE ポート チャネル送信元の追加 198
モニタリング セッションへの vHBA 発信元の追加 199
モニタリング セッションへの VSAN 発信元（ファイバ チャネル）の追加 200
モニタリング セッションへのソースとしてのポート チャネル（ファイバ チャネル）の追加 201
トラフィック モニタリング セッションのアクティブ化 202
トラフィック モニタリング セッションの削除 203
Cisco UCS Mini の SPAN に関する制約事項 204

はじめに

- 対象読者 （xi ページ）
- 表記法 （xi ページ）
- Cisco UCS の関連ドキュメント （xiii ページ）
- マニュアルに関するフィードバック （xiii ページ）

対象読者

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

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

表記法

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

テキストのタイプ	説明
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、**this font**で示しています。 CLI コマンド内の変数は、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 の関連ドキュメント

ドキュメント ロードマップ

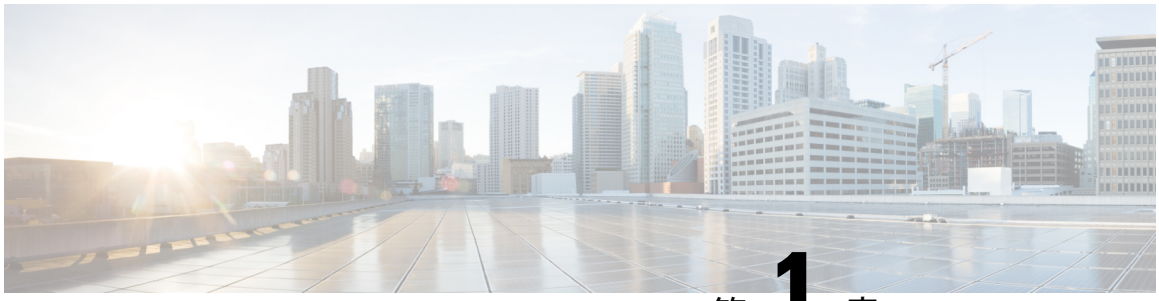
すべての B シリーズ マニュアルの完全なリストについては、次の URL で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

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

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

- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

ここでは、Cisco UCS Manager リリース 4.3 (x) の新機能および変更された動作について説明します。

表 *1 : Cisco UCS Manager* リリース *4.3 (6a)* の新機能と変更された動作

特長	説明	参照先
X シリーズ M8 および C シリーズ M8 サーバのサポート	Cisco UCS Manager は Cisco UCS X210c M8 コンピューティング ノード、Cisco UCS C240 M8 サーバ と Cisco UCS C220 M8 サーバ をサポートするようになりました。	• ローカル ストレージ モニタリングのサポート （141 ページ） • グラフィックス カード サーバ サポート （153 ページ） • TFM とスーパーキャパシタの注意事項および制約事項 （157 ページ）

表 *2 : Cisco UCS Manager* リリース *4.3(5a)* の新機能と変更された動作

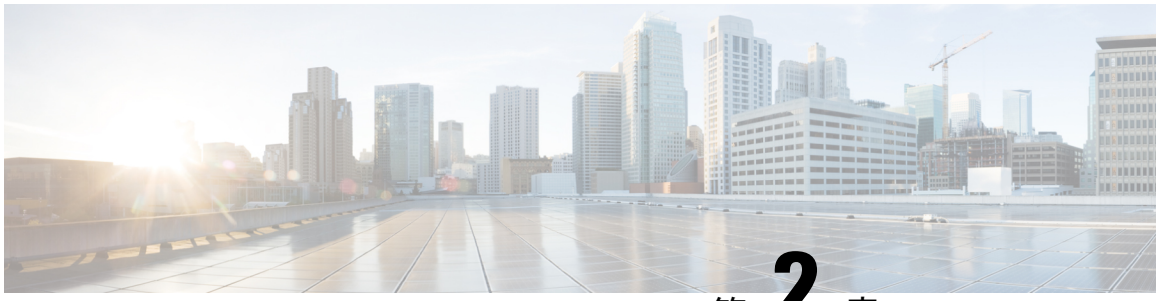
特長	説明	参照先
Cisco UCS X シリーズ M8 サーバのサポート	Cisco UCS Manager が Cisco UCS X215c M8 コンピューティング ノードをサポートするようになりました。	• ローカル ストレージ モニタリングのサポート （141 ページ） • グラフィックス カード サーバ サポート （153 ページ） • TFM とスーパーキャパシタの注意事項および制約事項 （157 ページ）
Cisco UCS C シリーズ M8 サーバのサポート	Cisco UCS Manager が Cisco UCS C225 M8 サーバ をサポートするようになりました。	• ローカル ストレージ モニタリングのサポート （141 ページ） • グラフィックス カード サーバ サポート （153 ページ） • TFM とスーパーキャパシタの注意事項および制約事項 （157 ページ）
ポート ステータスのモニタリングのサポート	Cisco UCS Manager は、ポート ステータスをモニターするためのダイナミック ポーリングをサポートするようになりました。	ラックマウント サーバのホスト イーサネット インターフェイス ステータスのモニタリング （133 ページ）

表 *3 : Cisco UCS Manager* リリース *4.3(4b)* の新機能と変更された動作

特長	説明	参照先
Cisco UCS ファブリック インターコネクト 9108 100G のサポート	Cisco UCS Manager が Cisco UCS ファブリック インターコネクト 9108 100G（Cisco UCS X シリーズ ダイレクト）をサポートするようになりました	• ローカル ファイルへの Syslog メッセージ保存のイネーブル化 （12 ページ） • NetFlow モニタリング （161 ページ）

表 *4 : Cisco UCS Manager* リリース *4.3(4a)* の新機能と変更された動作

特長	説明	参照先
トラフィック モニタリング	Cisco UCS 64108 ファブリック インターコネクトおよび Cisco UCS 6532 ファブリック インターコネクトで ERSPAN トラフィック モニタリングを設定するための Cisco UCS Manager のガイドライン。	トラフィック モニタリング（173 ページ）
PCIe ノード モニタリング	PCIe ノード インベントリのモニタリング	PCIe ノードのモニタリング（134 ページ）



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 （5 ページ）
- Cisco UCS Manager コアと障害の生成 （6 ページ）
- Cisco UCS Manager ユーザ CLI ドキュメント （8 ページ）

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

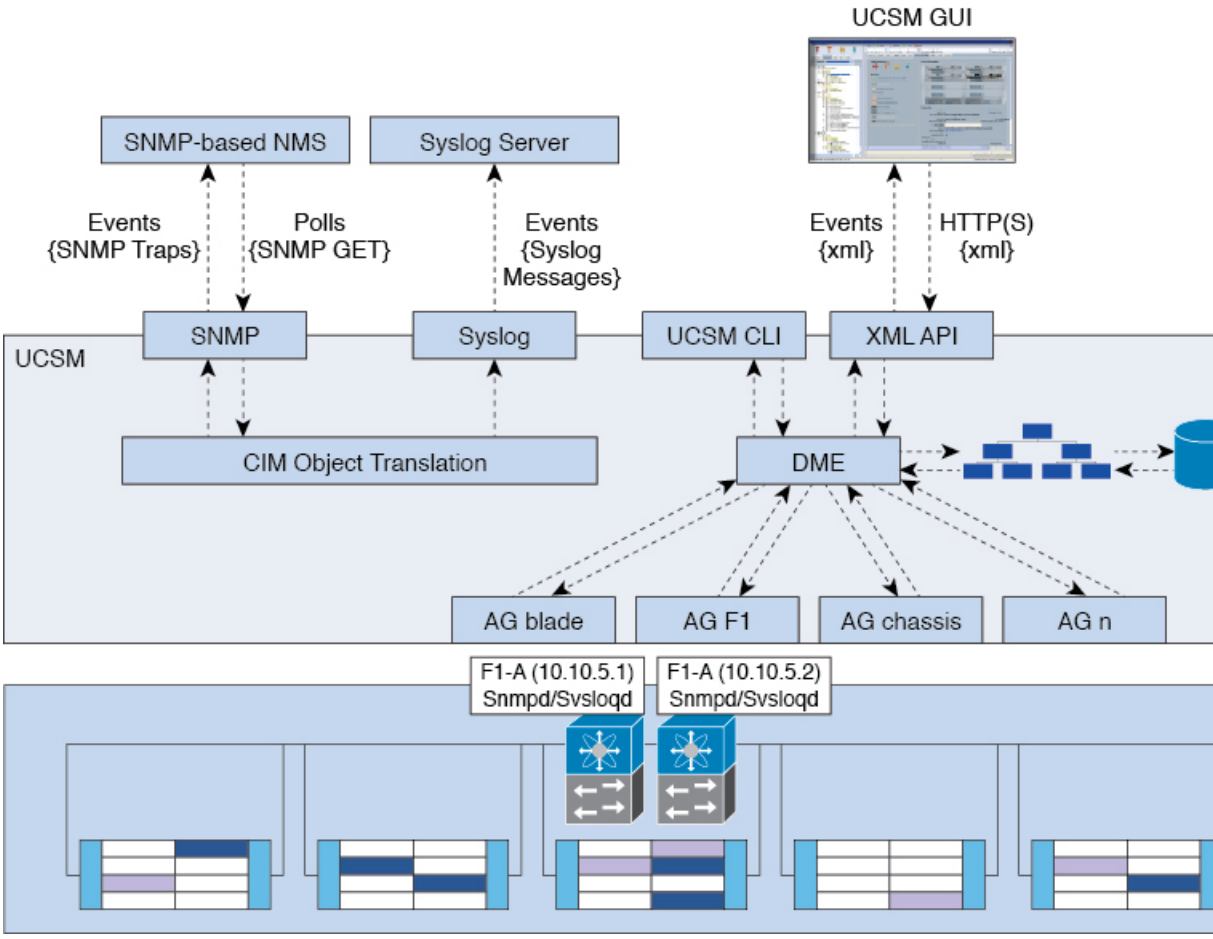
  - 中央のネットワーク管理ステーションからデバイスをモニタリングするためのSNMP および、ホストとユーザの設定
  - SNMP トラップ、Call Home 通知、および特定デバイスでの障害抑制ポリシー
- Core File Exporter および、Syslog、監査ログ、システム イベント ログなどのログ
- アダプタ、シャーシ、ホスト、ポート、およびサーバに対する統計情報の収集およびしきい値ポリシー
- Call Home および Smart Call Home の Cisco 組み込みデバイスのサポート
- Cisco UCS Manager ユーザ インターフェイスを使用したハ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。

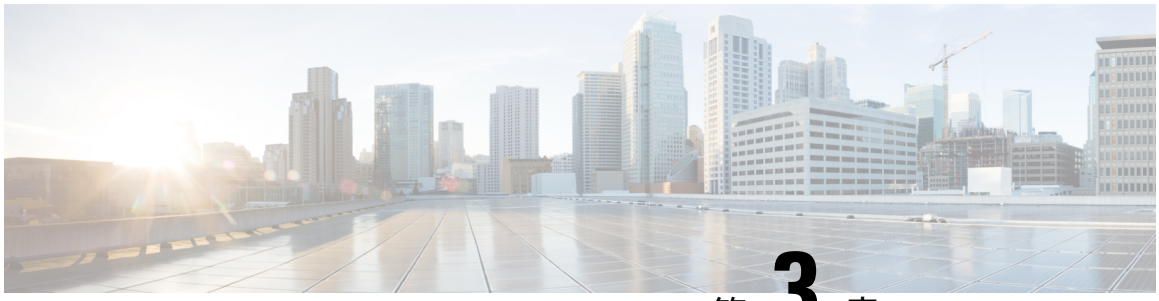
SNMP インフォームおよびトラップは、 Cisco UCSXML データベースに格納された障害情報から直接変換されます。SNMP GET 要求は、同じオブジェクト変換エンジンを介して逆方向に送信され、そこでオブジェクト変換エンジンからの要求を DME が受信します。データは、XML データベースから取得され、SNMP応答に変換されます。

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 CLI ドキュメント

Cisco UCS Manager 次の表に示す、使用例を基本とした従来よりもコンパクトなマニュアル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 Manager の初期構成と構成のベストプラクティスを含め、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。
『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、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 Storage Management Guide』	SUN、VSAN など、Cisco UCS Managerで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 Network Management Guide』	LAN 接続、VLAN 接続など、Cisco UCS Managerで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 System Monitoring Guide』	システム統計を含め、Cisco UCS Managerでの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 （11 ページ）
- ローカル ファイルへの Syslog メッセージ保存のイネーブル化 （12 ページ）

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。

ローカルファイルへのSyslogメッセージ保存のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリングモードを開始します。
ステップ 2	UCS-A /monitoring # {**enable** | **disable**} **syslog console**	コンソールへの Syslog の送信をイネーブルまたはディセーブルにします。
ステップ 3	（任意） UCS-A /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}	表示するメッセージの最低レベルを選択します。syslog が使用可能である場合、システムはそのレベル以上のメッセージをコンソールに表示します。 レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
ステップ 4	UCS-A /monitoring # {**enable** | **disable**} **syslog monitor**	オペレーティング システムによる syslog 情報のモニタリングをイネーブルまたはディセーブルにします。
ステップ 5	（任意） UCS-A /monitoring # **set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	表示するメッセージの最低レベルを選択します。モニタの状態が有効の場合、システムはそのレベル以上のメッセージを表示します。 レベル オプションは緊急性の降順で一覧表示されま

	コマンドまたはアクション	目的
		す。デフォルトのレベルは Critical です。 （注） **terminal monitor** コマンドを入力した場合にだけ、Critical より下のレベルのメッセージが端末のモニタに表示されます。
ステップ 6	UCS-A /monitoring # {**enable** | **disable**} **syslog rfc-5424-compliance**	RFC 5424 フォーマットごとの syslog 情報の書き込みを有効または無効にします。 （注） このオプションは、Cisco UCS ファブリック インターコネクト 9108 100G、Cisco UCS 6500 および 6400 シリーズ ファブリック インターコネクトにのみ適用されます。
ステップ 7	UCS-A /monitoring # {**enable** | **disable**} **syslog file**	syslog ファイルへの syslog 情報の書き込みをイネーブルまたはディセーブルにします。
ステップ 8	UCS-A /monitoring # **set syslog file name** *filename*	メッセージが記録されるファイルの名前。ファイル名は 16 文字まで入力できます。
ステップ 9	（任意） UCS-A /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	ファイルに保存するメッセージの最低レベルを選択します。ファイルの状態が有効の場合、システムはそのレベル以上のメッセージを syslog ファイルに保存します。 レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
ステップ 10	（任意） UCS-A /monitoring # **set syslog file size** *filesize*	最新のメッセージで最も古いものを上書きし始める前の、最大ファイル サイズ（バイト単位）。有効な範囲は 4096 ～ 4194304 バイトです。
ステップ 11	UCS-A /monitoring # {**enable** | **disable**} **syslog remote-destination** {**server-1** | **server-2** | **server-3**}	最大 3 台の外部 syslog サーバへの syslog メッセージの送信をイネーブルまたはディセーブルにします。

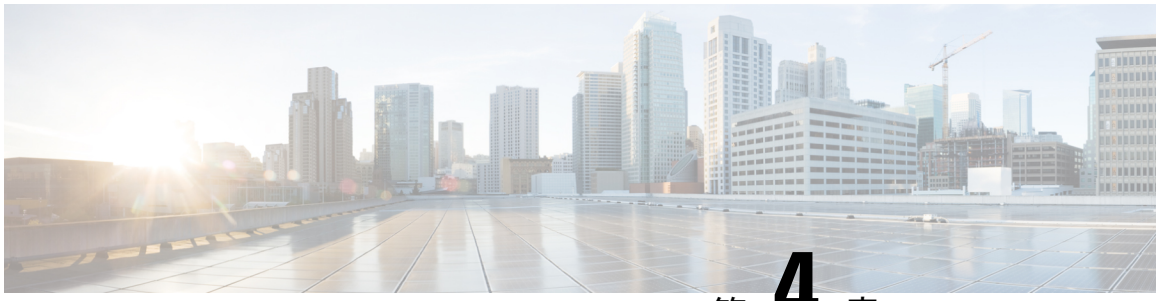
	コマンドまたはアクション	目的
ステップ 12	（任意） UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	外部ログに保存するメッセージの最低レベルを選択します。リモート宛先が有効になっている場合、システムはそのレベル以上のメッセージを外部サーバに送信します。 レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
ステップ 13	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **hostname** *hostname*	指定されたリモート Syslog サーバのホスト名またはIPアドレス。ホスト名は 256 文字まで入力できます。
ステップ 14	（任意） UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**}	指定されたリモート syslog サーバに送信される syslog メッセージに含まれるファシリティ レベル。
ステップ 15	UCS-A /monitoring # {**enable** | **disable**} **syslog source** {**audits** | **events** | **faults**}	次のいずれかになります。 • [監査（audits）] : すべての監査ログイベントのロギングを有効または無効にします。 • [イベント（events）] : すべてのシステムイベントイベントのロギングを有効または無効にします。 • **faults** : すべてのシステム障害のロギングを有効または無効にします。
ステップ 16	UCS-A /monitoring # **commit-buffer**	トランザクションをコミットします。

例

次の例は、ローカル ファイルの syslog メッセージのストレージをイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # disable syslog console
UCS-A /monitoring* # disable syslog monitor
UCS-A /monitoring* # enable syslog file
UCS-A /monitoring* # set syslog file name SysMsgsUCSA
UCS-A /monitoring* # set syslog file level notifications
UCS-A /monitoring* # set syslog file size 4194304
UCS-A /monitoring* # disable syslog remote-destination server-1
UCS-A /monitoring* # disable syslog remote-destination server-2
UCS-A /monitoring* # disable syslog remote-destination server-3
```

```
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```



第 4 章

システム イベント ログ

- システム イベント ログ （17 ページ）
- サーバのシステム イベント ログの表示 （18 ページ）
- SEL ポリシーの設定 （20 ページ）
- サーバのシステム イベント ログのバックアップ （22 ページ）
- サーバのシステム イベント ログのクリア （23 ページ）

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。

サーバのシステム イベント ログの表示

各サーバのシステム イベント ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show sel** *chassis-id / blade-id*	指定したサーバのシステム イベント ログを表示します。

例

次に、シャーシ 1 のブレード 3 のシステム イベント ログを表示する例を示します。

```
UCS-A# show sel 1/3
     1 | 01/01/1970 01:23:27 | System Event 0x83 | Timestamp clock synch | SEL timestamp
 clock updated, event is f
irst of pair | Asserted
     2 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded
 | Asserted
     3 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to On Line
 | Deasserted
     4 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Asserted
     5 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is on | Deasserted
     6 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is on | Asserted
     7 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is off | Deasserted
     8 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Absent | Asserted
     9 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Present | Deasserted
     a | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is on | Asserted
     b | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is green |
Asserted
     c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Deasserted
     d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber |
Deasserted
     e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded
 | Asserted
     f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
    10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted
```

シャーシ内の全サーバのシステム イベント ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / blade-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **show sel**	システム イベント ログを表示します。

例

次に、シャーシ サーバ モードからシャーシ 1 内のブレード 3 のシステム イベント ログを表示する例を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # show sel
     1 | 01/01/1970 01:23:27 | System Event 0x83 | Timestamp clock synch | SEL timestamp
 clock updated, event is f
irst of pair | Asserted
     2 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded
 | Asserted
     3 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to On Line
 | Deasserted
     4 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Asserted
     5 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is on | Deasserted
     6 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is on | Asserted
     7 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is off | Deasserted
     8 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Absent | Asserted
     9 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Present | Deasserted
     a | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is on | Asserted
     b | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is green |
Asserted
     c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Deasserted
     d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber |
Deasserted
     e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded
 | Asserted
     f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
    10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted
```

SEL ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **scope ep-log-policy sel**	組織エンドポイントログポリシーモードを開始し、SEL ポリシーにスコープします。
ステップ 3	（任意） UCS-A /org/ep-log-policy # **set description** *description*	ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括ります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS A/org/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**]	バックアップ操作をトリガーするアクションを指定します。
ステップ 5	UCS-A /org/ep-log-policy # **set backup clear-on-backup** {**no** | **yes**}	バックアップ操作の発生後にシステムイベントログをクリアするかどうかを指定します。
ステップ 6	UCS-A /org/ep-log-policy # **set backup destination** *URL*	バックアップ操作のプロトコル、ユーザ、パスワード、リモートホスト名、リモートパスを指定します。使用するプロトコルに応じて、次の構文のいずれかを使用して URL を指定します。 • **ftp://** *username***@***hostname* **/** *path* • **scp://** *username* **@** *hostname* **/** *path* • **sftp://** *username* **@** *hostname* **/** *path* • **tftp://** *hostname* **:** *port-num* **/** *path*

	コマンドまたはアクション	目的
		（注） **set backup hostname** 、 **set backup password** 、 **set backup protocol** 、 **set backup remote-path** 、 **set backup user** コマンドを使用するか、 **set backup destination** コマンドを使用して、バックアップ先を指定することもできます。いずれかの方法を使用してバックアップ先を指定します。
ステップ 7	UCS-A /org/ep-log-policy # **set backup format** {*ascii* | *binary*}	バックアップ ファイルの形式を指定します。
ステップ 8	UCS-A /org/ep-log-policy # **set backup hostname** {*hostname* | *ip-addr*}	リモート サーバのホスト名または IP アドレスを指定します。
ステップ 9	UCS A/org/ep-log-policy # **set backup interval** {**1-hour** |**2-hours** |**4-hours** |**8-hours** |**24-hours** |**never**\\	自動バックアップ操作の間隔を指定します。 **never** キーワードを指定すると、自動バックアップは実行されません。
ステップ 10	UCS-A /org/ep-log-policy # **set backup password** *password*	ユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 11	UCS A/org/ep-log-policy # **set backup protocol** {**ftp** |**scp** |**sftp** |**tftp**\\	リモート サーバとの通信時に使用するプロトコルを指定します。
ステップ 12	UCS-A /org/ep-log-policy # **set backup remote-path** *path*	バックアップ ファイルが保存されるリモート サーバのパスを指定します。
ステップ 13	UCS-A /org/ep-log-policy # **set backup user** *username*	システムがリモート サーバーへのログインに使用する必要のあるユーザー名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 14	UCS-A /org/ep-log-policy # **commit-buffer**	トランザクションをコミットします。

例

次の例は、システム イベント ログ（ASCII 型式）を 24 時間ごとまたはログがいっぱいになったときにバックアップするよう、またバックアップ操作後にシステム イベン

トログをクリアするよう SEL ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope ep-log-policy sel
UCS-A /org/ep-log-policy # set backup destination scp://user@192.168.1.10/logs
Password:
UCS-A /org/ep-log-policy* # set backup action log-full
UCS-A /org/ep-log-policy* # set backup clear-on-backup yes
UCS-A /org/ep-log-policy* # set backup format ascii
UCS-A /org/ep-log-policy* # set backup interval 24-hours
UCS-A /org/ep-log-policy* # commit-buffer
UCS-A /org/ep-log-policy #
```

サーバのシステム イベント ログのバックアップ

個々のサーバのシステム イベント ログのバックアップ

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A /chassis/server # **backup sel** *chassis-id* / *blade-id*	システム イベント ログをバックアップします。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをコミットします。

例

次の例は、シャーシ 1 内のブレード 3 からシステム イベント ログをバックアップし、トランザクションをコミットします。

```
UCS-A# backup sel 1/3
UCS-A* # commit-buffer
UCS-A#
```

シャーシ内の全サーバのシステム イベント ログのバックアップ

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *blade-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **backup sel**	システム イベント ログをバックアップします。
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをコミットします。

例

次の例は、シャーシ 1 内のブレード 3 のシャーシ サーバ モードからシステム イベント ログをバックアップし、トランザクションをコミットします。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # backup sel
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

サーバのシステム イベント ログのクリア

個々のサーバのシステム イベント ログのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **clear sel** *chassis-id* / *blade-id*	システム イベント ログをクリアします。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをコミットします。

例

次の例は、シャーシ 1 内のブレード 3 からシステム イベント ログをクリアし、トランザクションをコミットします。

```
UCS-A# clear sel 1/3
UCS-A* # commit-buffer
UCS-A#
```

シャーシ内の全サーバのシステム イベント ログのクリア

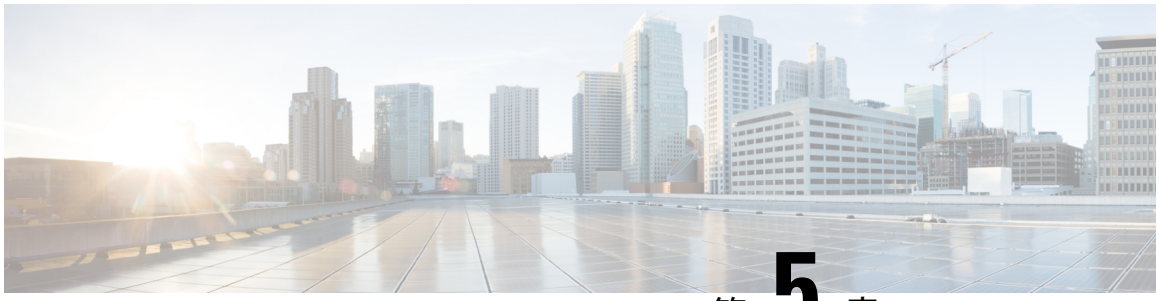
手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *blade-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **clear sel**	システム イベント ログをクリアします。
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをコミットします。

例

次の例は、シャーシ 1 内のブレード 3 のシャーシ サーバ モードからシステム イベント ログをクリアし、トランザクションをコミットします。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # clear sel
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```



第 5 章

監査ログ

- 監査ログ （25 ページ）
- 監査ログの表示 （25 ページ）

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **show audit-logs**	監査ログを表示します。 （注） 特定の監査ログを表示するのにには、*id* オプションを使用します。detail オプションを使用して、監査ログ出力の詳細情報が表示されます。

例

次の例では、監査ログを表示します。

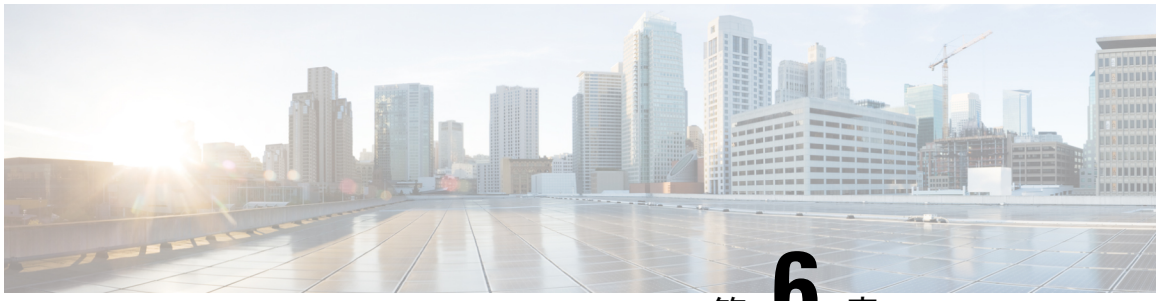
```
UCS-A# scope security
UCS-A /security # show audit-logs

Audit trail logs:
    Creation Time       User       ID       Action          Description
```

```
    ------------------- ---------- -------- ---------------- -----------
    2015-12-24T12:34:02.980
                         internal    6572175 Creation         Web A: local user admin
logged i
    2015-12-22T11:26:33.547
                         admin       6512814 Creation         Server port A/1/21 created

    2015-12-22T11:26:33.547
                         admin       6512816 Deletion         Server Port Channel A/1025
 delet
    2015-12-22T11:26:33.536
                         admin       6512791 Modification     Acknowledged chassis 1.
    2015-12-22T11:25:44.755
                         admin       6512767 Modification     chassis discovery policy
modifie
    2015-12-22T11:25:01.447
                         admin       6512763 Deletion         Server Member Port A/1/23
 remove
    2015-12-22T11:04:22.031
                         admin       6511644 Deletion         Server port A/1/21 deleted

    2015-12-22T11:04:22.030
                         admin       6511638 Creation         Server Port Channel A/1025
 creat
    2015-12-22T11:04:22.030
 UCS-A /security #
```



第 6 章

ログ ファイル エクスポータ

- ログ ファイル エクスポータ （27 ページ）
- リモート サーバへのログ ファイルのエクスポート （28 ページ）

ログ ファイル エクスポータ

Cisco UCS Manager 実行可能ファイルごとにログ ファイルを生成します。ログ ファイルのサイズは最大 20 MB であり、バックアップを 5 回までサーバに保存できます。ログ ファイル エクスポータでは、ログ ファイルが削除される前に、リモート サーバにエクスポートできます。ログ ファイル名には次の情報が含まれます。

- プロセスの名前
- タイムスタンプ
- ファブリック インターコネクトの名前と ID

（注） ログのエクスポートをイネーブルにしない場合は、バックアップ ファイルの最大限度に達するたびに、最も古いログ ファイルが削除されます。

注意事項と制約事項

- ログのエクスポートには、tftp またはパスワードなしの scp か sftp を使用することを推奨します。標準 scp または sftp が使用される場合、ユーザ パスワードは暗号化された形式で設定ファイルに保存されます。
- HA のセットアップでは、各サイドからのログ ファイルが別々にエクスポートされます。1 つのサイドがログのエクスポートに失敗した場合、他のサイドが補償することはありません。

リモート サーバへのログ ファイルのエクスポート

手順

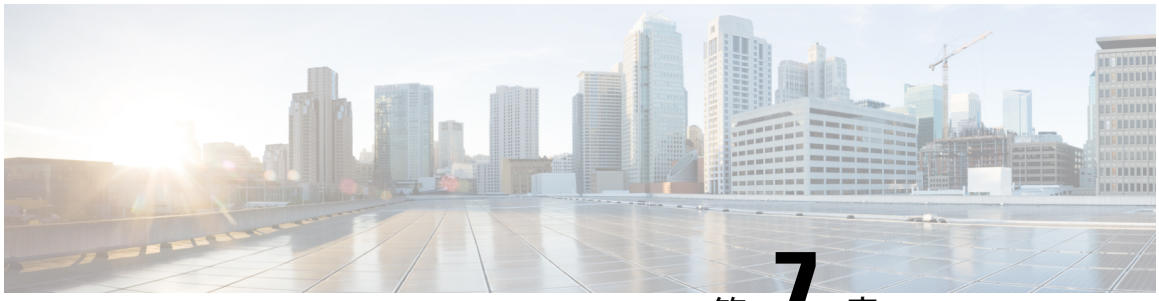
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリングモードを開始します。
ステップ 2	UCS-A /monitoring # **scope sysdebug**	モニタリング システム デバッグ モードを開始します。
ステップ 3	UCS-A /monitoring/sysdebug # **scope log-export-policy**	ログファイルのエクスポートモードを開始します。
ステップ 4	UCS-A /monitoring/sysdebug/log-export-policy # **set admin-state** {**disabled** | **enabled**}	ログファイルのエクスポートが有効かどうか。
ステップ 5	（任意） UCS-A /monitoring/sysdebug/log-export-policy # **set desc** *description*	ログのエクスポートポリシーの説明を入力します。
ステップ 6	UCS-A /monitoring/sysdebug/log-export-policy # **set hostname** *hostname*	リモートサーバのホスト名を指定します。
ステップ 7	UCS-A /monitoring/sysdebug/log-export-policy # **set passwd**	Enter キーを押すと、パスワードを入力するように促されます。 リモートサーバーのユーザー名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 8	UCS-A /monitoring/sysdebug/log-export-policy # **set passwordless-ssh** {**no** | **yes**}	パスワードなしの SSH ログインを有効にします。
ステップ 9	UCS-A /monitoring/sysdebug/log-export-policy # **set proto** {**scp** | **ftp** | **sftp** | **tftp**}	リモートサーバとの通信時に使用するプロトコルを指定します。
ステップ 10	UCS-A /monitoring/sysdebug/log-export-policy # **set path** *path*	ログ ファイルが保存されるリモートサーバのパスを指定します。
ステップ 11	UCS-A /monitoring/sysdebug/log-export-policy # **set user** *username*	システムがリモートサーバーへのログインに使用する必要のあるユーザー名を指定します。この手順は、TFTP プロ

	コマンドまたはアクション	目的
		トコルを使用する場合には適用されません。
ステップ 12	UCS-A /monitoring/sysdebug/log-export-policy # **commit-buffer**	トランザクションをコミットします。

例

次に、ログ ファイルのエクスポータを有効にし、リモート サーバのホスト名を指定し、プロトコルを scp に設定し、パスワードなしのログインを有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # scope log-export-policy
UCS-A /monitoring/sysdebug/log-export-policy # set admin-state enable
UCS-A /monitoring/sysdebug/log-export-policy* # set hostname 10.10.1.1
UCS-A /monitoring/sysdebug/log-export-policy* # set path /
UCS-A /monitoring/sysdebug/log-export-policy* # set user testuser
UCS-A /monitoring/sysdebug/log-export-policy* # set proto scp
UCS-A /monitoring/sysdebug/log-export-policy* # set passwd
password:
UCS-A /monitoring/sysdebug/log-export-policy* # set passwordless-ssh yes
UCS-A /monitoring/sysdebug/log-export-policy* # commit-buffer
UCS-A /monitoring/sysdebug/log-export-policy #
```



第 7 章

Core File Exporter

- Core File Exporter （31 ページ）
- Core File Exporter の設定 （31 ページ）
- Core File Exporter のディセーブル化 （32 ページ）

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope sysdebug**	モニタリング システム デバッグ モードを開始します。
ステップ 3	UCS-A /monitoring/sysdebug # **enable core-export-target**	Core File Exporter のイネーブル化Core File Exporter がイネーブルな状態でエラーによりサーバがコア ダンプを実行する場合、システムはコア ファイルを TFTP 経由で指定されたリモート サーバへエクスポートします。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /monitoring/sysdebug # **set core-export-target path** *path*	コア ファイルをリモート サーバにエクスポートするときに使用するパスを指定します。
ステップ 5	UCS-A /monitoring/sysdebug # **set core-export-target port** *port-num*	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するポート番号を指定します。有効な値の範囲は1 ～ 65,535 です。
ステップ 6	UCS A/モニタリング/sysdebug # **set core-export-target server-description** 説明	コア ファイルを保存するために使用するリモート サーバの説明を加えます。
ステップ 7	UCS A/モニタリング/sysdebug # **set core-export-target server-name** *hostname*	TFTP を介して接続するリモート サーバのホスト名を指定します。
ステップ 8	UCS-A /monitoring/sysdebug # **commit-buffer**	トランザクションをコミットします。

例

次の例では、Core File Exporter をイネーブルにし、コア ファイル送信に使用するパスとポートを指定し、リモート サーバのホスト名を指定し、リモート サーバの説明を加え、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # enable core-export-target
UCS-A /monitoring/sysdebug* # set core-export-target path /root/CoreFiles/core
UCS-A /monitoring/sysdebug* # set core-export-target port 45000
UCS-A /monitoring/sysdebug* # set core-export-target server-description
CoreFile102.168.10.10
UCS-A /monitoring/sysdebug* # set core-export-target server-name 192.168.10.10
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```

Core File Exporter のディセーブル化

手順

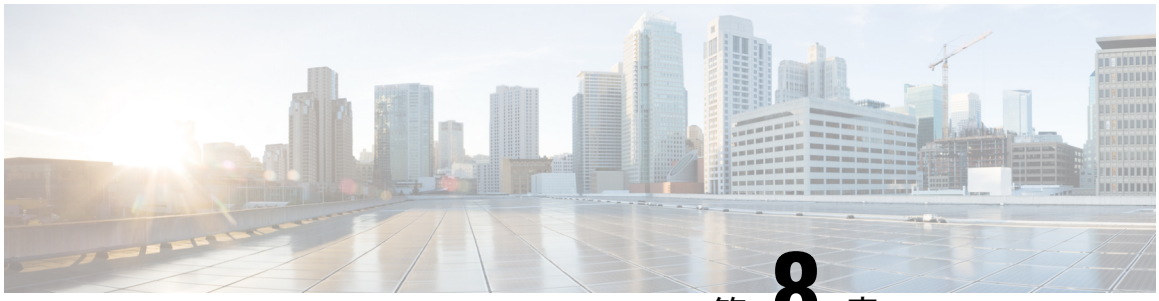
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope sysdebug**	モニタリング システム デバッグ モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /monitoring/sysdebug # **disable core-export-target**	Core File Exporter をディセーブルにします。Core File Exporter がディセーブルの場合、コア ファイルは自動的にエクスポートされません。
ステップ 4	UCS-A /monitoring/sysdebug # **commit-buffer**	トランザクションをコミットします。

例

次に、Core File Exporter をディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # disable core-export-target
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```



第 8 章

システムのモニタリングとデバッグ

• デバッグ プラグインのロード （35 ページ）

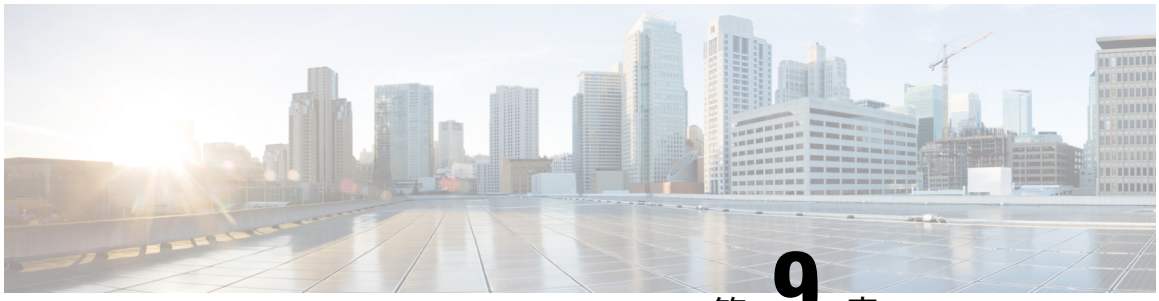
デバッグ プラグインのロード

デバッグ プラグインのロード

`load-debug-plugin` コマンドは、テクニカル アシスタンス センター（TAC）の担当者が使用することを目的としています。このコマンドにより、デバッグプラグインのロードが有効になります。これにより、Cisco UCS Manager で重大な障害およびエラーが発生した際の可視性と診断機能が向上します。これは、Cisco UCS 6300 シリーズ ファブリック インターコネクトとそれより前のバージョンにのみ適用されます。

手順

コマンドまたはアクション	目的
UCS-A# **load *debug-plugin***	デバッグプラグインイメージをロードします。このデバッグプラグインイメージは、TAC と モニタリングとデバッグのためにロードされます。



第 9 章

障害の収集と抑制

- グローバル障害ポリシー （37 ページ）
- フォールト抑制 （39 ページ）

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。

障害収集ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope fault policy**	モニターリング障害ポリシー モードを開始します。
ステップ 3	UCS-A /monitoring/fault-policy # **set clear-action** {**delete** | **retain**}	クリアしたすべてのメッセージを保持するか、削除するかを指定します。 **retain** オプションが指定された場合、メッセージを保持する時間の長さは、 **set retention-interval** コマンドによって決まります。
ステップ 4	UCS-A /monitoring/fault-policy # **set flap-interval** *seconds*	障害状態を変更する前にシステムが待機する間隔を指定します（秒単位）。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。これを回避するために、最後の状態変更後からフラッピング間隔が経過するまで、システムは障害の状態の変更を許可しません。フラッピング間隔中に障害が再発生した場合は、障害がアクティブ状態に戻ります。それ以外の場合は、障害がクリアされます。
ステップ 5	UCS-A /monitoring/fault-policy # **set retention-interval** {*days hours minutes seconds* | **forever**}	システムが、削除する前にクリアしたすべての障害メッセージを保持する時間間隔を指定します。システムは、クリアされた障害メッセージを永続的に保持することも、指定された日数、時間数、分数、秒数保持することもできます。
ステップ 6	UCS-A /monitoring/fault-policy # **commit-buffer**	トランザクションをコミットします。

例

この例では、クリアされた障害メッセージを30日間保持するよう障害収集ポリシーを設定し、フラッピング間隔を 10 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
```

```
UCS-A /monitoring/fault-policy # set clear-action retain
UCS-A /monitoring/fault-policy* # set flap-interval 10
UCS-A /monitoring/fault-policy* # set retention-interval 30 0 0 0
UCS-A /monitoring/fault-policy* # commit-buffer
UCS-A /monitoring/fault-policy #
```

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。

シャーシに対する障害抑制の設定

固定時間間隔を使用したシャーシに対する障害抑制タスクの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **create fault-suppress-task** *name*	シャーシで障害抑制タスクを作成し、障害抑制タスク モードを開始します。

	コマンドまたはアクション	目的
		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。
ステップ 3	UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*	適用する障害抑制ポリシーを指定します。次のいずれかになります。 • **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。 • **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。 • **default-server-maint**：サーバの障害を抑制します。 （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。 • **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 4	UCS-A/chassis/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケジュール モードを開始します。
ステップ 5	UCS-A/chassis/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 6	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 8	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシに対する task2 と呼ばれる障害抑制タスクを作成し、default-chassis-all-maint ポリシーをタスクに適用し、開始日を 2013 年 1 月 1 日 11:00 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # create fault-suppress-task task2
UCS-A/chassis/fault-suppress-task* # set fault-suppress-policy default-chassis-all-maint
UCS-A/chassis/fault-suppress-task* # create local-schedule
UCS-A/chassis/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/chassis/fault-suppress-task/local-schedule* # set date jan 1 2013 11 00 00
UCS-A/chassis/fault-suppress-task/local-schedule* # commit-buffer
```

スケジュールを使用したシャーシに対する障害抑制タスクの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **create fault-suppress-task** *name*	シャーシで障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	UCS-A/chassis/fault-suppress-task # **set schedule** *name*	使用するスケジュールを指定します。 （注）

	コマンドまたはアクション	目的
		すでにあるスケジュールを障害抑制タスクで使用する必要があります。スケジュール作成の詳細については、スケジュールの作成（63 ページ）を参照してください。
ステップ 4	UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*	適用する障害抑制ポリシーを選択します。次のいずれかになります。 • **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。 • **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。 • **default-server-maint**：サーバの障害を抑制します。 （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。 • **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 5	UCS-A/chassis/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシに対するtask1と呼ばれる障害抑制タスクを作成し、weekly_maintおよびdefault-chassis-all-maintポリシーと呼ばれるスケジューラをタスクに適用し、トランザクションをコミットする方法を示します。

```
UCS-A# scope chassis 2
UCS-A/chassis # create fault-suppress-task task1
UCS-A/chassis/fault-suppress-task* # set schedule weekly_maint
UCS-A/chassis/fault-suppress-task* # set fault-suppress-policy default-chassis-all-maint
UCS-A/chassis/fault-suppress-task* # commit-buffer
```

シャーシに対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 3	UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*	障害抑制ポリシーを変更します。次のいずれかになります。 • **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。 • **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。 • **default-server-maint**：サーバの障害を抑制します。 • **default-iom-maint**：シャーシまたはFEX 内の IOM の障害を抑制します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ4に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/chassis/fault-suppress-task # **set schedule** *name*	使用するスケジュールを適用します。 （注） 一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。

	コマンドまたはアクション	目的
		スケジュールから一定時間間隔に変更すると、スケジュールへの参照がコミットするときにクリアされます。
ステップ 5	UCS-A/chassis/fault-suppress-task # **scope local-schedule**	ローカル スケジュール モードを開始します。
ステップ 6	UCS-A/chassis/fault-suppress-task/local-schedule # **scope occurrence single-one-time**	single-one-time モードを開始します。
ステップ 7	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 8	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 9	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task2 と呼ばれる障害抑制タスクの日付と障害抑制ポリシーを変更する方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope fault-suppress-task task2
UCS-A/chassis/fault-suppress-task # set fault-suppress-policy default-server-maint
UCS-A/chassis/fault-suppress-task* # scope local-schedule
UCS-A/chassis/fault-suppress-task/local-schedule* # scope occurrence single-one-time
UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time* # set date dec 31 2013
 11 00 00
UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

次の例では、task1 と呼ばれる障害抑制タスクに別のスケジュールを適用する方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope fault-suppress-task task1
UCS-A/chassis/fault-suppress-task # set schedule monthly-maint
UCS-A/chassis/fault-suppress-task* # commit-buffer
```

シャーシに対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **show fault suppressed**	シャーシに対する抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 3	UCS-A/chassis # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 4	UCS-A/chassis/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

例

次に、シャーシに対する抑制された障害を表示する例を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # show fault suppressed
Fault Suppress Task:

Name                Status              Global Schedule Suppress Policy Name
------------------- ------------------- --------------- --------------------
task1               Active              test_schedule1  Default Chassis Phys Maint

UCS-A/chassis #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope fault-suppress-task task1
UCS-A/chassis/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Chassis Phys Maint

UCS-A/chassis/fault-suppress-task #
```

シャーシに対する障害抑制タスクの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **delete fault-suppress-task** *name*	指定された障害抑制タスクを削除します。
ステップ 3	UCS-A/chassis # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # delete fault-suppress-task task1
UCS-A/chassis* # commit-buffer
```

I/O モジュールに対する障害抑制の設定

固定時間間隔を使用した IOM に対する障害抑制タスクの設定

default-iom-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **create fault-suppress-task** *name*	IOM で障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できませ

	コマンドまたはアクション	目的
		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。
ステップ 4	UCS-A/chassis|fex/iom/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケジュール モードを開始します。
ステップ 5	UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 6	UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 7	UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 8	UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシ上の IOM に対する task2 と呼ばれる障害抑制タスクを作成し、開始日を 2013 年 1 月 1 日 11:00 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # create fault-suppress-task task2
UCS-A/chassis/iom/fault-suppress-task* # create local-schedule
UCS-A/chassis/iom/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/chassis/iom/fault-suppress-task/local-schedule/single-one-time* # set date jan 1
2013 11 00 00
UCS-A/chassis/iom/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

次の例では、FEX 上の IOM に対する task2 と呼ばれる障害抑制タスクを作成し、開始日を 2013 年 1 月 1 日 11:00 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fex 1
UCS-A/fex # scope iom a
UCS-A/fex/iom # create fault-suppress-task task2
UCS-A/fex/iom/fault-suppress-task* # create local-schedule
UCS-A/fex/iom/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/fex/iom/fault-suppress-task/local-schedule/single-one-time* # set date jan 1 2013
 11 00 00
UCS-A/fex/iom/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

スケジュールを使用した IOM に対する障害抑制タスクの設定

default-iom-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **create fault-suppress-task** *name*	IOM で障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 4	UCS-A/chassis|fex/iom/fault-suppress-task # **set schedule** *name*	使用するスケジュールを指定します。 （注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。スケジュール作成の詳細については、スケジュールの作成（63 ページ）を参照してください。
ステップ 5	UCS-A/chassis|fex/iom/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシ上の IOM に対する task1 と呼ばれる障害抑制タスクを作成し、weekly_maint と呼ばれるスケジューラをタスクに適用し、トランザクションをコミットする方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # create fault-suppress-task task1
UCS-A/chassis/iom/fault-suppress-task* # set schedule weekly_maint
```

```
UCS-A/chassis/iom/fault-suppress-task* # commit-buffer
```

次の例では、FEX 上の IOM に対する task1 と呼ばれる障害抑制タスクを作成し、weekly_maint と呼ばれるスケジューラをタスクに適用し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fex 1
UCS-A/fex # scope iom a
UCS-A/fex/iom # create fault-suppress-task task1
UCS-A/fex/iom/fault-suppress-task* # set schedule weekly_maint
UCS-A/fex/iom/fault-suppress-task* # commit-buffer
```

IOM に対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 4 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/chassis|fex/iom/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。 （注） 一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。 スケジュールから一定時間間隔に変更すると、スケジュールへの参照がコミットするときにクリアされます。
ステップ 5	UCS-A/chassis|fex/iom/fault-suppress-task # **scope local-schedule**	ローカル スケジュール モードを開始します。
ステップ 6	UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule # **scope occurrence single-one-time**	single-one-time モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A/chassis/iom/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 8	UCS-A/chassis/iom/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 9	UCS-A/chassis/iom/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシ上の IOM に対する task2 と呼ばれる障害抑制タスクの日付と障害抑制ポリシーを変更する方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # scope fault-suppress-task task2
UCS-A/chassis/iom/fault-suppress-task # scope local-schedule
UCS-A/chassis/iom/fault-suppress-task/local-schedule # scope occurrence single-one-time
UCS-A/chassis/iom/fault-suppress-task/local-schedule/single-one-time # set date dec 31
2013 11 00 00
UCS-A/chassis/iom/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

次の例では、FEX 上の IOM に対する task1 と呼ばれる障害抑制タスクに別のスケジュールを適用する方法を示します。

```
UCS-A# scope fex 3
UCS-A/fex # scope iom a
UCS-A/fex/iom # scope fault-suppress-task task1
UCS-A/fex/iom/fault-suppress-task # set schedule monthly-maint
UCS-A/fex/iom/fault-suppress-task* # commit-buffer
```

IOM に対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **show fault suppressed**	IOM の抑制された障害を表示します。

	コマンドまたはアクション	目的
		（注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 4	UCS-A/chassis|fex/iom # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 5	UCS-A/chassis|fex/iom/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

例

次に、シャーシ上の IOM の抑制された障害を表示する例を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # show fault suppressed
Fault Suppress Task:

Name                Status              Global Schedule Suppress Policy Name
------------------- ------------------- --------------- --------------------
task1               Active              test_schedule1  Default Iom Maint

UCS-A/chassis/iom #
```

次の例では、シャーシ上の IOM の task1 と呼ばれる障害抑制タスクを表示する方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # scope fault-suppress-task task1
UCS-A/chassis/iom/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Iom Maint

UCS-A/chassis/iom/fault-suppress-task #
```

次の例では、FEX 上の IOM の task1 と呼ばれる障害抑制タスクを表示する方法を示します。

```
UCS-A# scope fex 3
UCS-A/fex # scope iom a
UCS-A/fex/iom # scope fault-suppress-task task1
UCS-A/fex/iom/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Iom Maint

UCS-A/chassis/iom/fault-suppress-task #
```

IOM に対する障害抑制タスクの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **delete fault-suppress-task** *name*	指定された障害抑制タスクを削除します。
ステップ 4	UCS-A/chassis|fex/iom # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシ上の IOM に対する task1 と呼ばれる障害抑制タスクを削除する方法を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # delete fault-suppress-task task1
UCS-A/chassis/iom* # commit-buffer
```

次の例では、FEX 上の IOM に対する task1 と呼ばれる障害抑制タスクを削除する方法を示します。

```
UCS-A# scope fex 3
UCS-A/fex # scope iom a
UCS-A/fex/iom # delete fault-suppress-task task1
UCS-A/fex/iom* # commit-buffer
```

FEX に対する障害抑制の設定

固定時間間隔を使用した FEX に対する障害抑制タスクの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fex** *fex-num*	指定された FEX の fex モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A/fex # **create fault-suppress-task** *name*	fex で障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*	適用する障害抑制ポリシーを指定します。次のいずれかになります。 • **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。 • **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。 • **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 4	UCS-A/fex/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケジュール モードを開始します。
ステップ 5	UCS-A/fex/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 6	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 7	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 8	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、FEXに対するtask2と呼ばれる障害抑制タスクを作成し、default-fex-all-maintポリシーをタスクに適用し、開始日を2013年1月1日11:00に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fex 1
UCS-A/fex # create fault-suppress-task task2
UCS-A/fex/fault-suppress-task* # set fault-suppress-policy default-fex-all-maint
UCS-A/fex/fault-suppress-task* # create local-schedule
UCS-A/fex/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/fex/fault-suppress-task/local-schedule/single-one-time* # set date jan 1 2013 11
00 00
UCS-A/fex/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

スケジュールを使用した FEX に対する障害抑制タスクの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fex** *fex-num*	指定された FEX の fex モードを開始します。
ステップ 2	UCS-A/fex # **create fault-suppress-task** *name*	fex で障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	UCS-A/fex/fault-suppress-task # **set schedule** *name*	使用するスケジュールを指定します。 （注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。スケジュール作成の詳細については、スケジュールの作成（63ページ）を参照してください。
ステップ 4	UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*	適用する障害抑制ポリシーを指定します。次のいずれかになります。

	コマンドまたはアクション	目的
		• **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。 • **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。 • **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 5	UCS-A/fex/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、FEX に対する task1 と呼ばれる障害抑制タスクを作成し、weekly_maint および default-fex-all-maint ポリシーと呼ばれるスケジューラをタスクに適用し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fex 1
UCS-A/fex # create fault-suppress-task task1
UCS-A/fex/fault-suppress-task* # set schedule weekly_maint
UCS-A/fex/fault-suppress-task* # set fault-suppress-policy default-fex-all-maint
UCS-A/fex/fault-suppress-task* # commit-buffer
```

FEX に対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fex** *fex-num*	指定された FEX の fex モードを開始します。
ステップ 2	UCS-A/fex # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 3	UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*	障害抑制ポリシーを変更します。次のいずれかになります。 • **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。

	コマンドまたはアクション	目的
		• **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。 • **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 4 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/fex/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。 （注） 一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。 スケジュールから一定時間間隔に変更すると、スケジュールへの参照がコミットするときにクリアされます。
ステップ 5	UCS-A/fex/fault-suppress-task # **scope local-schedule**	ローカル スケジュール モードを開始します。
ステップ 6	UCS-A/fex/fault-suppress-task/local-schedule # **scope occurrence single-one-time**	single-one-time モードを開始します。
ステップ 7	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 8	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 9	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task2 と呼ばれる障害抑制タスクの日付と障害抑制ポリシーを変更する方法を示します。

```
UCS-A# scope fex 1
UCS-A/fex # scope fault-suppress-task task2
UCS-A/fex/fault-suppress-task # set fault-suppress-policy default-iom-maint
UCS-A/fex/fault-suppress-task* # scope local-schedule
UCS-A/fex/fault-suppress-task/local-schedule* # scope occurrence single-one-time
UCS-A/fex/fault-suppress-task/local-schedule/single-one-time* # set date dec 31 2013 11
 00 00
UCS-A/fex/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

次の例では、task1 と呼ばれる障害抑制タスクに別のスケジュールを適用する方法を示します。

```
UCS-A# scope fex 1
UCS-A/fex # scope fault-suppress-task task1
UCS-A/fex/fault-suppress-task # set schedule monthly-maint
UCS-A/fex/fault-suppress-task* # commit-buffer
```

FEX に対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fex** *fex-num*	指定された FEX の fex モードを開始します。
ステップ 2	UCS-A/fex #**show fault suppressed**	FEX に対する抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 3	UCS-A/fex # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 4	UCS-A/fex/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

例

次に、FEX に対する抑制された障害を表示する例を示します。

```
UCS-A# scope fex 1
UCS-A/fex # show fault suppressed
Fault Suppress Task:

Name                Status              Global Schedule Suppress Policy Name
------------------- ------------------- --------------- --------------------
task1               Active              test_schedule1  Default FEX Phys Maint

UCS-A/fex #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

```
UCS-A# scope fex 1
UCS-A/fex # scope fault-suppress-task task1
UCS-A/fex/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default FEX Phys Maint

UCS-A/fex/fault-suppress-task #
```

FEX に対する障害抑制タスクの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fex** *fex-num*	指定された FEX の fex モードを開始します。
ステップ 2	UCS-A/fex # **delete fault-suppress-task** *name*	指定された障害抑制タスクを削除します。
ステップ 3	UCS-A/fex #**commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

```
UCS-A# scope fex 1
UCS-A/fex # delete fault-suppress-task task1
UCS-A/fex* # commit-buffer
```

サーバに対する障害抑制の設定

固定時間間隔を使用したサーバに対する障害抑制タスクの設定

default-server-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A/server # **create fault-suppress-task** *name*	サーバで障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	UCS-A/server/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケジュール モードを開始します。
ステップ 4	UCS-A/server/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 5	UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 6	UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 7	UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、サーバに対する task2 と呼ばれる障害抑制タスクを作成し、開始日を 2013 年 1 月 1 日 11:00 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope server 1/1
UCS-A/server # create fault-suppress-task task2
UCS-A/server/fault-suppress-task* # create local-schedule
UCS-A/server/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/server/fault-suppress-task/local-schedule/single-one-time* # set date jan 1 2013
11 00 00
UCS-A/server/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

スケジュールを使用したサーバに対する障害抑制タスクの設定

default-server-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A/server # **create fault-suppress-task** *name*	サーバで障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	UCS-A/server/fault-suppress-task # **set schedule** *name*	使用するスケジュールを指定します。 （注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。スケジュール作成の詳細については、スケジュールの作成（63 ページ）を参照してください。
ステップ 4	UCS-A/server/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、サーバに対する task1 と呼ばれる障害抑制タスクを作成し、weekly_maint と呼ばれるスケジューラをタスクに適用し、トランザクションをコミットする方法を示します。

```
UCS-A# scope server 1/1
UCS-A/server # create fault-suppress-task task1
UCS-A/server/fault-suppress-task* # set schedule weekly_maint
UCS-A/server/fault-suppress-task* # commit-buffer
```

サーバに対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A/server # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ3に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 4 に進みます。
ステップ 3	UCS-A/server/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。 （注） 一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。 スケジュールから一定時間間隔に変更すると、スケジュールへの参照がコミットするときにクリアされます。
ステップ 4	UCS-A/server/fault-suppress-task # **scope local-schedule**	ローカル スケジュール モードを開始します。
ステップ 5	UCS-A/server/fault-suppress-task/local-schedule # **scope occurrence single-one-time**	single-one-time モードを開始します。
ステップ 6	UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 7	UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 8	UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task2と呼ばれる障害抑制タスクの日付と障害抑制ポリシーを変更する方法を示します。

```
UCS-A# scope server 1/1
UCS-A/server # scope fault-suppress-task task2
UCS-A/server/fault-suppress-task # scope local-schedule
UCS-A/server/fault-suppress-task/local-schedule # scope occurrence single-one-time
UCS-A/server/fault-suppress-task/local-schedule/single-one-time # set date dec 31 2013
11 00 00
UCS-A/server/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

次の例では、task1と呼ばれる障害抑制タスクに別のスケジュールを適用する方法を示します。

```
UCS-A# scope server 1/1
UCS-A/server # scope fault-suppress-task task1
UCS-A/server/fault-suppress-task # set schedule monthly-maint
UCS-A/server/fault-suppress-task* # commit-buffer
```

スケジュールの作成

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 モードを開始します。
ステップ2	UCS-A /system # **create scheduler** *sched-name*	スケジューラを作成し、スケジューラ モードを開始します。
ステップ3	UCS-A /system/scheduler # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、maintenanceschedというスケジューラを作成し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # create scheduler maintenancesched
UCS-A /system/scheduler* # commit-buffer
UCS-A /system/scheduler #
```

次のタスク

スケジュールのワンタイム オカレンスまたは繰り返しオカレンスを作成します。

サーバに対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	5 UCS-A/server # **show fault suppressed**	サーバに対する抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 3	UCS-A/server # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 4	UCS-A/server/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

例

次に、サーバに対する抑制された障害を表示する例を示します。

```
UCS-A# scope server 1/1
UCS-A/server # show fault suppressed
Fault Suppress Task:

Name                Status              Global Schedule Suppress Policy Name
------------------- ------------------- --------------- --------------------
task1               Active              test_schedule1  Default Server Maint

UCS-A/server #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

```
UCS-A# scope server 1/1
UCS-A/server # scope fault-suppress-task task1
UCS-A/server/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Server Maint

UCS-A/server/fault-suppress-task #
```

サーバに対する障害抑制タスクの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A/server # **delete fault-suppress-task** *name*	指定された障害抑制タスクを削除します。
ステップ 3	5 UCS-A/server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

```
UCS-A# scope server 1/1
UCS-A/server # delete fault-suppress-task task1
UCS-A/server* # commit-buffer
```

サービス プロファイルに対する障害抑制の設定

固定時間間隔を使用したサービス プロファイルに対する障害抑制タスクの設定

default-server-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create fault-suppress-task** *name*	シャーシで障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以

	コマンドまたはアクション	目的
		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。
ステップ 4	UCS-A/org/service-profile/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケジュール モードを開始します。
ステップ 5	UCS-A/org/service-profile/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 6	UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 7	UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 8	UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、アカウンティング サービス プロファイル下で task2 と呼ばれる障害抑制タスクを作成し、開始日を 2013 年 1 月 1 日 11:00 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # create fault-suppress-task task2
UCS-A/org/service-profile/fault-suppress-task* # create local-schedule
UCS-A/org/service-profile/fault-suppress-task/local-schedule* # create occurrence
single-one-time
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time* # set date
 jan 1 2013 11 00 00
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time* #
commit-buffer
```

スケジュールを使用したサービス プロファイルに対する障害抑制タスクの設定

default-server-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create fault-suppress-task** *name*	シャーシで障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 4	UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name*	使用するスケジュールを指定します。 （注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。スケジュール作成の詳細については、スケジュールの作成 （63 ページ）を参照してください。
ステップ 5	UCS-A/org/service-profile/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、アカウンティング サービス プロファイル下で task1 と呼ばれる障害抑制タスクを作成し、weekly_maint と呼ばれるスケジューラをタスクに適用し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # create fault-suppress-task task1
UCS-A/org/service-profile/fault-suppress-task* # set schedule weekly_maint
UCS-A/org/service-profile/fault-suppress-task* # commit-buffer
```

サービス プロファイルに対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A/org/service-profile # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 4 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。 （注） 一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。 スケジュールから一定時間間隔に変更すると、スケジュールへの参照がコミットするときにクリアされます。
ステップ 5	UCS-A/org/service-profile/fault-suppress-task # **scope local-schedule**	ローカル スケジュール モードを開始します。
ステップ 6	UCS-A/org/service-profile/fault-suppress-task/local-schedule # **scope occurrence single-one-time**	single-one-time モードを開始します。
ステップ 7	UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 8	UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 9	UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task2と呼ばれる障害抑制タスクの日付と障害抑制ポリシーを変更する方法を示します。

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # scope fault-suppress-task task2
UCS-A/org/service-profile/fault-suppress-task # scope local-schedule
UCS-A/org/service-profile/fault-suppress-task/local-schedule # scope occurrence
single-one-time
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # set date
 dec 31 2013 11 00 00
UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time* #
commit-buffer
```

次の例では、task1と呼ばれる障害抑制タスクに別のスケジュールを適用する方法を示します。

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # scope fault-suppress-task task1
UCS-A/org/service-profile/fault-suppress-task # set schedule monthly-maint
UCS-A/org/service-profile/fault-suppress-task* # commit-buffer
```

サービス プロファイルに対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A/org/service-profile # **show fault suppressed**	サーバに対する抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 4	UCS-A/org/service-profile # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 5	UCS-A/org/service-profile/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

例

次に、サービス プロファイルに対する抑制された障害を表示する例を示します。

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # show fault suppressed
UCS-A/org/service-profile #
Fault Suppress Task:

Name                Status              Global Schedule Suppress Policy Name
------------------- ------------------- --------------- --------------------
task1               Active              test_schedule1  Default Server Maint

UCS-A/org/service-profile #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # scope fault-suppress-task task1
UCS-A/org/service-profile/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Server Maint

UCS-A/org/service-profile/fault-suppress-task #
```

サービス プロファイルに対する障害抑制タスクの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A/org/service-profile # **delete fault-suppress-task** *name*	指定された障害抑制タスクを削除します。
ステップ 4	UCS-A/org/service-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

```
UCS-A# scope org /
UCS-A/org # scope service-profile accounting
UCS-A/org/service-profile # delete fault-suppress-task task1
UCS-A/org/service-profile* # commit-buffer
```

組織に対する障害抑制の設定

固定時間間隔を使用した組織に対する障害抑制タスクの設定

default-server-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A/org # **create fault-suppress-task** *name*	組織の障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	UCS-A/org/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケジュール モードを開始します。
ステップ 4	UCS-A/org/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 5	UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 6	UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ルート組織下で task2 と呼ばれる障害抑制タスクを作成し、開始日を 2013 年 1 月 1 日 11:00 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A/org # create fault-suppress-task task2
UCS-A/org/fault-suppress-task* # create local-schedule
UCS-A/org/fault-suppress-task/local-schedule* # create occurrence single-one-time
UCS-A/org/fault-suppress-task/local-schedule/single-one-time* # set date jan 1 2013 11
00 00
UCS-A/org/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

スケジュールを使用した組織に対する障害抑制タスクの設定

default-server-maint 抑制ポリシーがデフォルトで選択されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A/org # **create fault-suppress-task** *name*	組織の障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	UCS-A/org/fault-suppress-task # **set schedule** *name*	使用するスケジュールを指定します。 （注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。スケジュール作成の詳細については、スケ

	コマンドまたはアクション	目的
		ジュールの作成 （63 ページ）を参照してください。
ステップ 4	UCS-A/org/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ルート組織下で task1 と呼ばれる障害抑制タスクを作成し、weekly_maint と呼ばれるスケジューラをタスクに適用し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A/org # create fault-suppress-task task1
UCS-A/org/fault-suppress-task* # set schedule weekly_maint
UCS-A/org/fault-suppress-task* # commit-buffer
```

組織に対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A/org # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 3 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 4 に進みます。
ステップ 3	UCS-A/org/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。 （注） 一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。 スケジュールから一定時間間隔に変更すると、スケジュールへの参照がコミットするときにクリアされます。

	コマンドまたはアクション	目的
ステップ 4	UCS-A/org/fault-suppress-task # **scope local-schedule**	ローカル スケジュール モードを開始します。
ステップ 5	UCS-A/org/fault-suppress-task/local-schedule # **scope occurrence single-one-time**	single-one-time モードを開始します。
ステップ 6	UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 7	UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 8	UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task2 と呼ばれる障害抑制タスクの日付と障害抑制ポリシーを変更する方法を示します。

```
UCS-A# scope org /
UCS-A/org # scope fault-suppress-task task2
UCS-A/org/fault-suppress-task* # scope local-schedule
UCS-A/org/fault-suppress-task/local-schedule # scope occurrence single-one-time
UCS-A/org/fault-suppress-task/local-schedule/single-one-time # set date dec 31 2013 11
00 00
UCS-A/org/fault-suppress-task/local-schedule/single-one-time* # commit-buffer
```

次の例では、task1 と呼ばれる障害抑制タスクに別のスケジュールを適用する方法を示します。

```
UCS-A# scope org
UCS-A/org # scope fault-suppress-task task1
UCS-A/org/fault-suppress-task # set schedule monthly-maint
UCS-A/org/fault-suppress-task* # commit-buffer
```

組織に対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / 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/org # **show fault suppressed**	組織に対する抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 3	UCS-A/org # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 4	UCS-A/org/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

例

次に、組織に対する抑制された障害を表示する例を示します。

```
UCS-A# scope org Finance
UCS-A/org # show fault suppressed
UCS-A/org #
Fault Suppress Task:

Name                Status              Global Schedule Suppress Policy Name
------------------- ------------------- --------------- --------------------
task1               Active              test_schedule1  Default Server Maint

UCS-A/org #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

```
UCS-A# scope org Finance
UCS-A/org # scope fault-suppress-task task1
UCS-A/org/fault-suppress-task # show detail expand
Fault Suppress Task:
    Name: task1
    Status: Active
    Global Schedule: test_schedule1
    Suppress Policy Name: Default Server Maint

UCS-A/org/fault-suppress-task #
```

組織に対する障害抑制タスクの削除

手順

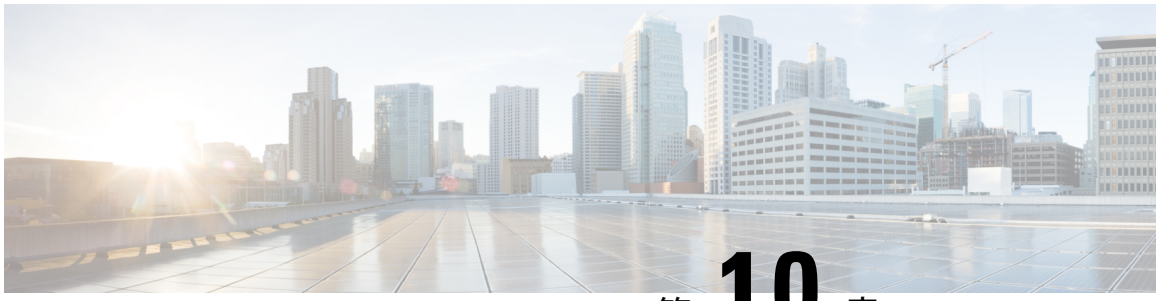
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A/org # **delete fault-suppress-task** *name*	指定された障害抑制タスクを削除します。
ステップ 3	UCS-A/org # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

```
UCS-A# scope org /
UCS-A/org # delete fault-suppress-task task1
UCS-A/org* # commit-buffer
```



第 10 章

SNMP の設定

- SNMP の概要 （77 ページ）
- SNMP 機能の概要 （77 ページ）
- SNMP 通知 （78 ページ）
- SNMP セキュリティ レベルおよび権限 （78 ページ）
- 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 （79 ページ）
- SNMPv3 セキュリティ機能 （80 ページ）
- SNMP サポート （80 ページ）
- SNMP の設定 （81 ページ）

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 *5 : 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。

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。

SNMP の設定

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP を有効にします。
ステップ 3	UCS-A /monitoring # **set snmp community**	snmp コミュニティ モードを開始します。
ステップ 4	UCS-A /monitoring # **Enter a snmp community:** *community-name*	SNMP コミュニティを指定します。パスワードとしてコミュニティ名を使用します。コミュニティ名は、最大 32 文字の英数字で指定できます。
ステップ 5	UCS-A /monitoring # **set snmp syscontact** *system-contact-name*	SNMP 担当者のシステムの連絡先を指定します。システムの連絡先名（電子メール アドレスや、名前と電話番号など）は、最大 255 文字の英数字で指定できます。
ステップ 6	UCS-A /monitoring # **set snmp syslocation** *system-location-name*	SNMP エージェント（サーバー）が実行されるホストの場所を指定します。システム ロケーション名は、最大 512 文字の英数字で指定できます。
ステップ 7	UCS-A /monitoring # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、SNMP を有効にし、SnmpCommSystem2 という名前の SNMP コミュニティを設定し、contactperson という名前のシステム連絡先を設定し、systemlocation という名前の連絡先ロケーションを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # set snmp community
```

```
UCS-A /monitoring* # Enter a snmp community: SnmpCommSystem2
UCS-A /monitoring* # set snmp syscontact contactperson1
UCS-A /monitoring* # set snmp syslocation systemlocation
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP を有効にします。
ステップ 3	UCS-A /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}	指定したホスト名、IPv4 アドレス、または IPv6 アドレスで SNMP トラップ ホストを作成します。 ホスト名は IPv4 アドレスの完全修飾ドメイン名にすることができます。
ステップ 4	UCS-A /monitoring/snmp-trap # **set community** *community-name*	SNMP トラップに使用する SNMP コミュニティ名を指定します。
ステップ 5	UCS-A /monitoring/snmp-trap # **set port** *port-num*	SNMP トラップに使用するポートを指定します。
ステップ 6	UCS-A /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}	トラップに使用する SNMP のバージョンとモデルを指定します。
ステップ 7	（任意） UCS-A /monitoring/snmp-trap # **set notificationtype** {**traps** | **informs**}	送信するトラップのタイプ。バージョンとして v2c または v3 を選択した場合、以下の可能性があり得ます。 • **[トラップ（traps）]**：SNMP トラップ通知 • **[インフォーム（informs）]**：SNMP インフォーム通知
ステップ 8	（任意） UCS-A /monitoring/snmp-trap # **set v3 privilege** {**auth** | **noauth** | **priv**}	バージョンに [V3] を選択した場合、トラップに関連付けられる権限は次のいずれかになります。

	コマンドまたはアクション	目的
		• **auth**：認証あり、暗号化なし • **noauth**：認証なし、暗号化なし • **priv**：認証あり、暗号化あり
ステップ 9	UCS-A /monitoring/snmp-trap # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、SNMP を有効にし、IPv4 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem2 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap 100.10.111.112
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem2
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

次の例は、SNMP をイネーブルにし、IPv6 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem3 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap  2001::1
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem3
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

SNMP トラップの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}	指定したホスト名または IP アドレスの指定した SNMP トラップ ホストを削除します。
ステップ 3	UCS-A /monitoring # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、IP アドレス 192.168.100.112 で SNMP トラップを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-trap 192.168.100.112
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

テスト SNMP トラップの生成

ソフトウェアまたはシステムの物理構成を変更せずに、テスト SNMP トラップを生成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	connect nxos	NX-OS オペレーティング システム ソフトウェアに接続します。
ステップ 2	(nxos)# **test pfm snmp test-trap** ?	テスト トラップ オプションのリストを返します。
ステップ 3	(nxos)# **test pfm snmp test-trap** {fan | powersupply | temp_sensor}	テスト SNMP トラップを生成します。 • fan - ファンのテスト SNMP トラップを生成します • power supply - 電源のテスト用 SNMP トラップを生成します。 • temp_sensor - 温度のテスト用 SNMP トラップを生成します。

次のタスク

NX-OS コマンドの実行中に、ファブリック インターコネクトへの別の SSH セッションを開き、SNMPパケットがファブリック インターコネクトの管理インターフェイスから送信されることを確認できます。

完全なパケットの場合：

```
(nxos)# ethanalyzer local interface mgmt capture-filter "udp port 162"
limit-captured-frames 0 detail
```

パケット ヘッダーだけをキャプチャするには

```
(nxos)# ethanalyzer local interface mgmt capture-filter "udp port 162"
limit-captured-frames 0
```

SNMPv3 ユーザの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP を有効にします。
ステップ 3	UCS-A /monitoring # **create snmp-user** *user-name*	指定された SNMPv3 ユーザーを作成します。 SNMPユーザー名は、ローカルユーザー名と同じにはできません。ローカルユーザー名と一致しない SNMP ユーザー名を選択します。
ステップ 4	UCS-A /monitoring/snmp-user # **set aes-128** {**no** | **yes**}	AES-128暗号化の使用を有効または無効にします。
ステップ 5	UCS-A /monitoring/snmp-user # **set auth** {**md5** | **sha**}	MD5またはDHA認証の使用を指定します。
ステップ 6	UCS-A /monitoring/snmp-user # **set password**	ユーザー パスワードを指定します。 **set password** コマンドを入力すると、パスワードの入力と確認を促すプロンプトが表示されます。 （注） • *[*パスワード強度チェック（*Password Strength Check*）*]* オプションは、ローカルで認証されたユーザーに対してのみサポートさ

	コマンドまたはアクション	目的
		れ、SNMPv3 ユーザーに対してはサポートされません。 • パスワードのガイドラインの詳細については、『Cisco UCS Manager Administration Management Guide』の「*Cisco UCS Passwords* のガイドライン」セクションを参照してください。
ステップ 7	UCS-A /monitoring/snmp-user # **set priv-password**	ユーザー プライバシー パスワードを指定します。 **set priv-password** コマンドを入力すると、プライバシー パスワードの入力と確認を促すプロンプトが表示されます。
ステップ 8	UCS-A /monitoring/snmp-user # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、SNMP を有効にし、snmp-user14 という名前の SNMPv3 ユーザーを作成し、AES-128 暗号化を無効にし、MD5 認証の使用を指定し、パスワードおよびプライバシー パスワードを設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-user snmp-user14
UCS-A /monitoring/snmp-user* # set aes-128 no
UCS-A /monitoring/snmp-user* # set auth md5
UCS-A /monitoring/snmp-user* # set password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # commit-buffer
UCS-A /monitoring/snmp-user #
```

SNMPv3 ユーザの削除

手順

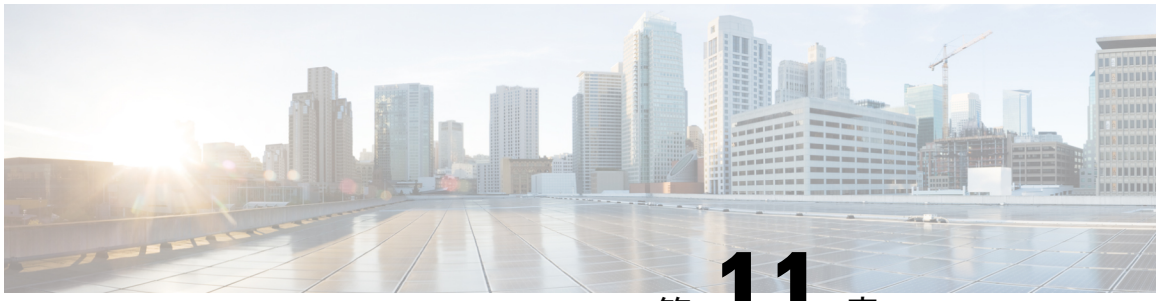
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring # **delete snmp-user** *user-name*	指定した SNMPv3 ユーザーを削除します。
ステップ 3	UCS-A /monitoring # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、snmp user14 という名前の SNMPv3 ユーザを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-user snmp-user14
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```



第 11 章

統計情報収集ポリシーの設定

- 統計情報収集ポリシー （89 ページ）
- 統計情報収集ポリシーの変更 （90 ページ）

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A/monitoring # **scope stats-collection-policy** {**adapter** |**chassis** |**host** |**port** |**server**}	指定されたポリシー タイプの統計情報収集ポリシー モードを開始します。
ステップ 3	UCS-A /monitoring/stats-collection-policy # **set collection-interval** {**1minute** | **2minutes** | **30seconds** | **5minutes**}	統計情報をシステムから収集する間隔を指定します。
ステップ 4	UCS-A /monitoring/stats-collection-policy # **set reporting-interval** {**15minutes** | **30minutes** | **60minutes**}	収集された統計情報の報告間隔を指定します。
ステップ 5	UCS-A /monitoring/stats-collection-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ポートの統計情報収集ポリシーを作成し、収集間隔を 1 分、レポート間隔を 30 分に設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope stats-collection-policy port
UCS-A /monitoring/stats-collection-policy* # set collection-interval 1minute
UCS-A /monitoring/stats-collection-policy* # set reporting-interval 30minutes
UCS-A /monitoring/stats-collection-policy* # commit-buffer
UCS-A /monitoring/stats-collection-policy #
```

CHAPTER 12

Call Home および Smart Call Home の設定

- UCS の Call Home の概要 （91 ページ）
- Call Home の考慮事項とガイドライン （94 ページ）
- Cisco UCSの障害と Call Home のシビラティ（重大度） （95 ページ）
- Cisco Smart Call Home （96 ページ）
- Anonymous Reporting （98 ページ）
- Call Home の設定 （98 ページ）
- Call Home のイネーブル化 （101 ページ）
- Call Home のディセーブル化 （102 ページ）
- システム インベントリ メッセージの設定, on page 103
- Call Home プロファイルの設定, on page 104
- テスト Call Home アラートの送信 （108 ページ）
- Call Home ポリシーの設定, on page 110
- Anonymous Reporting の設定, on page 113
- Smart Call Home の設定, on page 116

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。

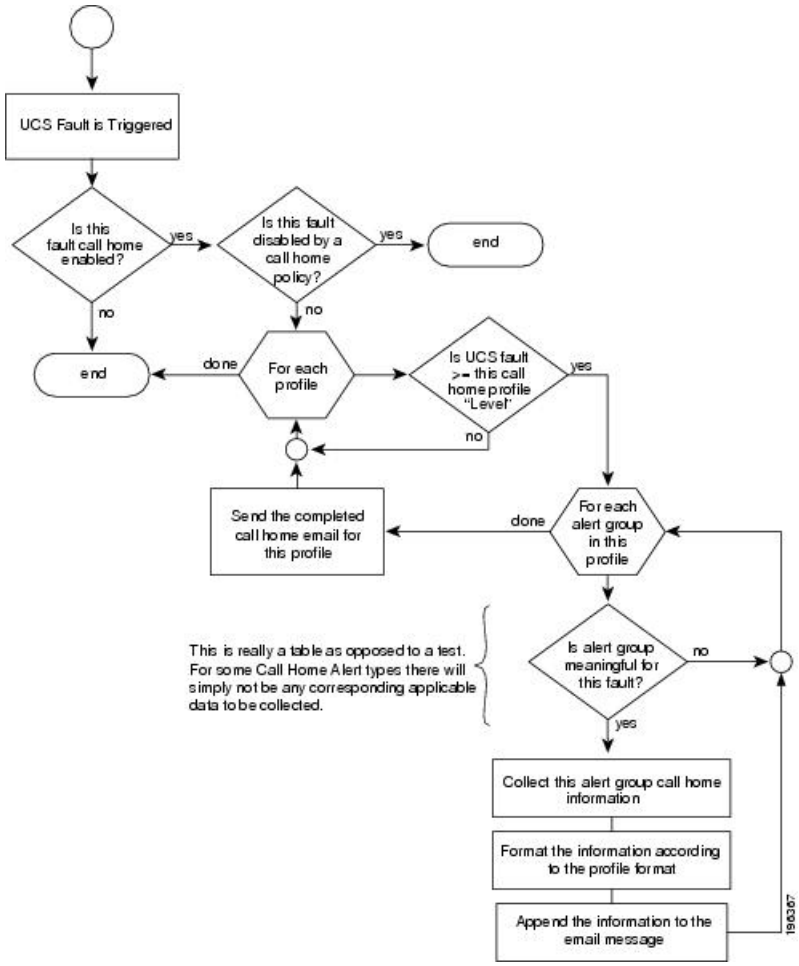
Cisco UCS では、Call Home メッセージが次のフォーマットで配信されます。

- 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



SMTP 認証

リリース 4.2(3b) 以降、UCS Manager は SMTP サーバーを使用した転送電子メールのセキュアな認証をサポートしています。

[SMTP 認証（SMTP Authentication）] を切り替えることができます。

- **[オフ（Off）]**：SMTP 認証はこの Cisco UCS ドメイン に使用されません。
- **[オン（On）]**：SMTP 認証はこの Cisco UCS ドメイン に使用されます。

（注） SMTP サーバーは、STARTTLS、SSL ベースの SMTP 通信をサポート可能である必要があります。

また、SSL から SMTP-AUTH サーバーへの接続を成功させるには、サーバーのルート CA 証明書を SMTP クライアント（スイッチ）にインストールする必要があります。

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。

SMTP 認証

リリース 4.2(3b) 以降、UCS Manager は SMTP サーバーを使用した転送電子メールのセキュアな認証をサポートしています。

[SMTP 認証（SMTP Authentication）] を切り替えることができます。

- **[オフ（Off）]**：SMTP 認証はこの Cisco UCS ドメイン に使用されません。
- **[オン（On）]**：SMTP 認証はこの Cisco UCS ドメイン に使用されます。

（注） SMTP サーバーは、STARTTLS、SSL ベースの SMTP 通信をサポート可能である必要があります。

また、SSL から SMTP-AUTH サーバーへの接続を成功させるには、サーバーのルート CA 証明書を SMTP クライアント（スイッチ）にインストール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 *6*：障害と *Call Home* のシビラティ（重大度）のマッピング

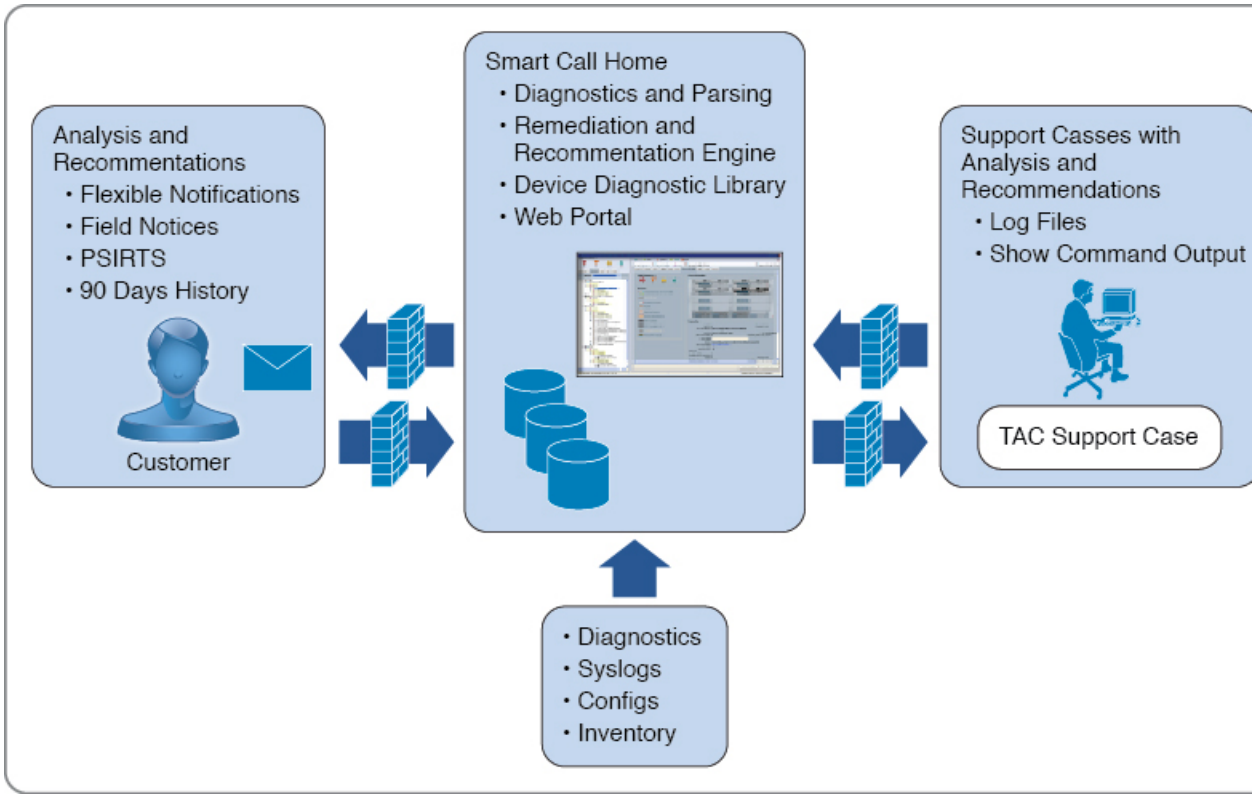
Call Home のシビラティ（重大度）	Cisco UCS の障害	Call Home での意味
(9) Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
(8) Disaster	該当なし	ネットワークに重大な影響が及びます。
(7) Fatal	該当なし	システムが使用不可能な状態。
(6) Critical	Critical	クリティカルな状態、ただちに注意が必要。
(5) Major	Major	重大な状態。
(4) Minor	Minor	軽微な状態。

Call Home のシビラティ（重大度）	Cisco UCS の障害	Call Home での意味
(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。

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
- リリース 4.2(3b) 以降、UCS Manager は SMTP サーバーを使用した転送電子メールのセキュアな認証をサポートしています。STARTTLS、SSL ベースの SMTP 通信をサポートできる SMTP サーバーが必要です。

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。

SMTP 認証

リリース 4.2(3b) 以降、UCS Manager は SMTP サーバーを使用した転送電子メールのセキュアな認証をサポートしています。

[SMTP 認証（SMTP Authentication）] を切り替えることができます。

- **[オフ（Off）]**：SMTP 認証はこの Cisco UCS ドメイン に使用されません。
- **[オン（On）]**：SMTP 認証はこの Cisco UCS ドメイン に使用されます。

（注） SMTP サーバーは、STARTTLS、SSL ベースの SMTP 通信をサポート可能である必要があります。

また、SSL から SMTP-AUTH サーバーへの接続を成功させるには、サーバーのルート CA 証明書を SMTP クライアント（スイッチ）にインストールする必要があります。

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。

Call Home の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **enable**	Call Home をイネーブルにします。
ステップ 4	UCS-A /monitoring/callhome # **set contact** *name*	主要 Call Home 連絡先の名前を指定します。
ステップ 5	UCS-A /monitoring/callhome # **set email** *email-addr*	主要 Call Home 連絡先の電子メールアドレスを指定します。

	コマンドまたはアクション	目的
		（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。
ステップ 6	UCS-A /monitoring/callhome # **set phone-contact** *phone-num*	主要 Call Home 連絡先の電話番号を指定します。+（プラス記号）と国番号から始まる国際形式の番号を入力する必要があります。 （注） Cisco Cisco UCS ファブリック インターコネクト 9108 100G、Cisco UCS 6536 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 インターコネクトで、電話番号を 17 文字以内に制限してください。電話番号の制限が 17 文字を超えると、Cisco UCS Manager システムで障害が発生する場合があります。
ステップ 7	UCS-A /monitoring/callhome # **set street-address** *email-addr*	主要 Call Home 連絡先の住所を指定します。 255 文字以下の ASCII 文字で入力します。
ステップ 8	UCS-A /monitoring/callhome # **set customer-id** *id-num*	ライセンス上のサポート契約の契約番号を含む CCO ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 9	UCS-A /monitoring/callhome # **set contract-id** *id-num*	サービス契約の契約ID番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 10	UCS-A /monitoring/callhome # **set site-id** *id-num*	サービス契約のサイトID番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。

	コマンドまたはアクション	目的
ステップ 11	UCS-A /monitoring/callhome # **set from-email** *email-addr*	Call Home メッセージの **[From]**フィールドで使用する電子メールアドレスを指定します。
ステップ 12	UCS-A /monitoring/callhome # **set reply-to-email** *email-addr*	Call Home メッセージの **Reply To** フィールドで使用する電子メールアドレスを指定します。
ステップ 13	UCS-A /monitoring/callhome # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	電子メールメッセージを送信するために Call Home が使用する SMTP サーバのホスト名、IPv4 または IPv6アドレスを指定します。
ステップ 14	UCS-A /monitoring/callhome # **set port** *port-num*	電子メールメッセージを送信するために Call Home が使用する SMTP サーバポートを指定します。有効なポート番号は 1 ～ 65535 です。
ステップ 15	UCS-A /monitoring/callhome # **set throttling** {**off** | **on**}	Call Home スロットリングをイネーブルまたはディセーブルにします。イネーブルにされると、スロットリングはあまりにも多くの Call Home 電子メールメッセージが同じイベントに対して送信されるのを防ぎます。デフォルトでは、スロットリングはイネーブルです。
ステップ 16	UCS-A /monitoring/callhome # **set urgency** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **information** | **notifications** | **warnings**}	Call Home 電子メール メッセージの緊急性レベルを指定します。ファブリックインターコネクトのペアが複数存在する大規模な UCS 配置のコンテキストでは、緊急性レベルによってある特定の Cisco UCS ドメイン からの Call Home メッセージに別のものより高い重要性を付与することが可能になります。2 つのファブリックインターコネクトだけを含む小さい UCS 配置のコンテキストでは、緊急性レベルはほとんど意味を持ちません。
ステップ 17	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、IPv4 ホスト名を持つ Call Home を設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 192.168.100.12
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

次に、IPv6 ホスト名を持つ Call Home を設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 2001::25
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Call Home のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **enable**	Call Home をイネーブルにします。
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # enable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Call Home のディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **disable**	Call Home をイネーブルにします。
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

システム インベントリ メッセージの設定

システム インベントリ メッセージの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **scope inventory**	モニタリング Call Home インベントリ モードを開始します。
ステップ 4	UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** | **on**}	インベントリ メッセージの送信をイネーブルまたはディセーブルにします。 **on** キーワードを指定すると、インベントリ メッセージは Call Home データベースに自動的に送信されます。
ステップ 5	UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num*	インベントリ メッセージが送信される間隔を指定します（日数）。
ステップ 6	UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour*	インベントリ メッセージが送信される時刻を指定します（24 時間形式を使用）。
ステップ 7	UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute*	インベントリ メッセージが送信される時刻の後の分数を指定します。
ステップ 8	UCS-A /monitoring/callhome/inventory # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home システム インベントリ メッセージを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # scope inventory
UCS-A /monitoring/callhome/inventory* # set send-periodically on
UCS-A /monitoring/callhome/inventory* # set interval-days 15
UCS-A /monitoring/callhome/inventory* # set timeofday-hour 21
```

```
UCS-A /monitoring/callhome/inventory* # set timeofday-minute 30
UCS-A /monitoring/callhome/inventory* # commit-buffer
UCS-A /monitoring/callhome/inventory #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **scope inventory**	モニタリング Call Home インベントリ モードを開始します。
ステップ 4	UCS-A /monitoring/callhome/inventory # **send**	Call Home データベースにシステム インベントリ メッセージを送信します。

例

次に、Call Home データベースにシステム インベントリ メッセージを送信する例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope inventory
UCS-A /monitoring/callhome/inventory* # send
```

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。

アラート グループ	説明
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。 （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 プロファイルの設定

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。ただし、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電子メールアラートを送信するために、追加プロファイルを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **create profile** *profile-name*	モニタリング Call Home プロファイル モードを開始します。
ステップ 4	UCS-A /monitoring/callhome/profile # **set level** {**critical** | **debug** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}	プロファイルのイベント レベルを指定します。各プロファイル固有のイベント レベルを設定できます。 そのイベント レベル以上の Cisco UCS 障害が、このプロファイルをトリガーします。
ステップ 5	UCS-A /monitoring/callhome/profile # **set alertgroups** *group-name* • **ciscotac** • **diagnostic** • **environmental** • **inventory** • **license** • **lifecycle** • **linecard** • **supervisor**	プロファイルに基づいてアラートを受け取る 1 つ以上のグループを指定します。*group-name* 引数には、同一コマンドラインで入力される、次のキーワードを 1 つ以上設定できます。

	コマンドまたはアクション	目的
	• **syslogport** • **system** • **test**	
ステップ 6	（任意） UCS-A /monitoring/callhome/profile # **add alertgroups** *group-names*	Call Home プロファイルに基づいて警告を受け取るグループの既存のリストに 1 つ以上のグループを追加します。 （注） 既存のアラート グループ リストに、さらにアラート グループを追加する場合は、 **add alertgroups** コマンドを使用する必要があります。**set alertgroups** コマンドを使用すると、新しいグループ リストで既存のアラート グループを置き換えます。
ステップ 7	UCS-A /monitoring/callhome/profile # **set format** {**shorttxt** | **xml**}	電子メール メッセージに使用するフォーマット方法を指定します。
ステップ 8	UCS-A /monitoring/callhome/profile # **set maxsize** *id-num*	電子メール メッセージの最大サイズ（文字数）を指定します。
ステップ 9	UCS-A /monitoring/callhome/profile # **create destination** *email-addr*	Call Home アラートを送信する電子メール アドレスを入力します。この電子メールアドレスに Call Home のアラートと障害が送信されます。複数の電子メール受信者を指定するには、モニタリング Call Home プロファイル モードで複数の **create destination** コマンドを使用します。指定された電子メール受信者を削除するには、モニタリング Call Home プロファイル モードで **delete destination** コマンドを使用します。
ステップ 10	UCS-A /monitoring/callhome/profile/destination # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home プロファイルを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # create profile TestProfile
```

```
UCS-A /monitoring/callhome/profile* # set level normal
UCS-A /monitoring/callhome/profile* # set alertgroups test diagnostic
UCS-A /monitoring/callhome/profile* # set format xml
UCS-A /monitoring/callhome/profile* # set maxsize 100000
UCS-A /monitoring/callhome/profile* # create destination admin@MyCompany.com
UCS-A /monitoring/callhome/profile/destination* # commit-buffer
UCS-A /monitoring/callhome/profile/destination #
```

Call Home プロファイルの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **delete profile** *profile-name*	指定されたプロファイルを削除します。
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、TestProfile という名前の Call Home プロファイルを削除し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # delete profile TestProfile
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

テスト Call Home アラートの送信

始める前に

Call Home と Call Home プロファイルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A/monitoring/callhome # **send-test-alert** {[**alert-group** {**diagnostic** |**environmental**}] [**alert-level** {**critical** |**debug** |**fatal** |**major** |**minor** |**normal** |**notify** |**warning**}] [**alert-message-type** {**conf** |**diag** |**env** |**inventory** |**syslog** |**test**}] [**alert-message-subtype** {**delta** |**full** |**goldmajor** |**goldminor** |**goldnormal** |**major** |**minor** |**nosubtype** |}] [**alert-description** 説明*]}* **test**	テスト Call Home アラートを送信します。テスト Call Home アラートは、すべての **alert-*** パラメータを指定する必要があり、そうしなければ Cisco UCS Manager はテスト メッセージを生成できません。**alert-*** パラメータには、次のものがあります。 • **alert-description**—アラートの説明 • **alert-group**—アラート グループ • **alert-level**—イベントのシビラティ（重大度）レベル • **alert-message-type**—メッセージ タイプ • **alert-message-subtype**—メッセージ サブタイプ Call Home テスト アラートを送信されると、Call Home は他のアラートと同様に応答し、設定された宛先電子メール アドレスにこれを転送します。

例

次に、環境アラート グループの設定済み宛先電子メール アドレスに、Call Home テスト アラートを発信する例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # send-test-alert alert-group diagnostic
alert-level critical alert-message-type test alert-message-subtype major
alert-description "This is a test alert"
```

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、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。しかし、必要に応じて、Call Home ポリシーで、その他の重要なシステム イベントに対するアラート メールの送信をイネーブルにするか、ディセーブルにするかを設定することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **create policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}	指定されたポリシーを作成し、モニタリング Call Home ポリシー モードを開始します。
ステップ 4	UCS-A /monitoring/callhome/policy # {**disabled** | **enabled**}	指定されたポリシーの電子メール アラートの送信をイネーブルまたはディセーブルにします。
ステップ 5	UCS-A /monitoring/callhome/policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、電圧の問題に関するシステムイベントについての電子メールアラート送信をディセーブルにする Call Home ポリシーを作成し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # create policy voltage-problem
UCS-A /monitoring/callhome/policy* # disabled
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

Call Home ポリシーのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}	指定したポリシーでモニタリング Call Home ポリシー モードを開始します。
ステップ 4	UCS-A /monitoring/callhome/policy # **disable**	指定したポリシーをディセーブルにします。
ステップ 5	UCS-A /monitoring/callhome/policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、voltage-problem という名前の Call Home ポリシーをディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope policy voltage-problem
UCS-A /monitoring/callhome/policy # disable
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

Call Home ポリシーのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}	指定したポリシーでモニタリング Call Home ポリシー モードを開始します。
ステップ 4	UCS-A /monitoring/callhome/policy # **enable**	指定したポリシーをイネーブルにします。
ステップ 5	UCS-A /monitoring/callhome/policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、voltage-problem という名前の Call Home ポリシーをイネーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope policy voltage-problem
UCS-A /monitoring/callhome/policy # enable
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

Call Home ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **delete policy** {**equipment-inoperable** |	指定されたポリシーを削除します

	コマンドまたはアクション	目的
	fru-problem | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}	
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、voltage-problem という名前の Call Home ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # delete policy voltage-problems
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Anonymous Reporting の設定

Anonymous Reporting のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A/monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	（任意） UCS-A/monitoring/callhome # **show anonymous-reporting**	Anonymous Reporting がイネーブルかディセーブルかを表示します。
ステップ 4	UCS-A/monitoring/callhome # **enable anonymous-reporting**	Smart Call Home で Anonymous Reporting をイネーブルにします。
ステップ 5	UCS-A/monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home サーバで Anonymous Reporting をイネーブルにする例を示します。

```
UCS-A # scope monitoring
UCS-A/monitoring #scope callhome
UCS-A/mnitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
    Off
UCS-A/monitoring/callhome* # enable anonymous-reporting
UCS-A/monitoring/callhome # commit-buffer
UCS-A/monitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
    On
```

Anonymous Reporting のディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A/monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	（任意） UCS-A/monitoring/callhome # **show anonymous-reporting**	Anonymous Reporting がイネーブルかディセーブルかを表示します。
ステップ 4	UCS-A/monitoring/callhome # **disable anonymous-reporting**	Smart Call Home サーバで Anonymous Reporting をディセーブルにします。
ステップ 5	UCS-A/monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home サーバで Anonymous Reporting をディセーブルにする例を示します。

```
UCS-A # scope monitoring
UCS-A/monitoring # scope callhome
UCS-A/mnitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
    On
UCS-A/monitoring/callhome* # disable anonymous-reporting
UCS-A/monitoring/callhome # commit-buffer
UCS-A/monitoring/callhome # show anonymous-reporting
Anonymous Reporting:
    Admin State
    -----------
```

```
Off
```

Anonymous レポートの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A/monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A/monitoring/callhome # **scope anonymous-reporting**	Anonymous Reporting モードを開始します。
ステップ 4	UCS-A/monitoring/callhome/anonymous-reporting # **show detail**	SMTP サーバのアドレスおよびサーバ ポートを表示します。
ステップ 5	UCS-A/monitoring/callhome/anonymous-reporting # **show inventory**	Anonymous Reporting の情報を表示します。
ステップ 6	UCS-A/monitoring/callhome/anonymous-reporting # **show content**	Anonymous レポート サンプル情報を表示します。

例

次に、Call Home サーバで Anonymous レポートを表示する例を示します。

```
UCS-A # scope monitoring
UCS-A/monitoring # scope callhome
UCS-A/monitoring/callhome # scope anonymous-reporting
UCS-A/monitoring/callhome/anonymous-reporting # show detail
UCS-A/monitoring/callhome/anonymous-reporting # show inventory
UCS-A/monitoring/callhome/anonymous-reporting # show content
<anonymousData>
<discreteData
smartCallHomeContract="false"
ethernetMode="EndHost"
fcMode="EndHost"
disjointL2Used="false"
fabricFailoverUsed="false"
numVnicAdaptTempl="3"
numServiceProfiles="7"
updatingSPtemplUsed="false"
initialSPtemplUsed="true"
lanConnPolicyUsed="true"
sanConnPolicyUsed="false"
updatingAdaptTemplUsed="false"
initialAdaptTemplUsed="true"
numMsoftVMnets="10"
numOfVMs="3"
```

```
discreteFEX="false"
ucsCentralConnected="false"/>
<bladeUnit
chassisId="1"
slotId="4"
…..
```

Smart Call Home の設定

Smart Call Home の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリングモードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **enable**	Call Home をイネーブルにします。
ステップ 4	UCS-A /monitoring/callhome # **set contact** *name*	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。
ステップ 5	UCS-A /monitoring/callhome # **set email** *email-addr*	主要 Call Home 連絡先の電子メールアドレスを指定します。 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。
ステップ 6	UCS-A /monitoring/callhome # **set phone-contact** *phone-num*	主要 Call Home 連絡先の電話番号を指定します。+（プラス記号）と国番号から始まる国際形式の番号を入力する必要があります。
ステップ 7	UCS-A /monitoring/callhome # **set street-address** *email-addr*	主要 Call Home 連絡先の住所を指定します。
ステップ 8	UCS-A /monitoring/callhome # **set customer-id** *id-num*	ライセンス上のサポート契約の契約番号を含む CCO ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。

	コマンドまたはアクション	目的
ステップ 9	UCS-A /monitoring/callhome # **set contract-id** *id-num*	サービス契約の契約ID番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 10	UCS-A /monitoring/callhome # **set site-id** *id-num*	サービス契約のサイトID番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 11	UCS-A /monitoring/callhome # **set from-email** *email-addr*	Call Home メッセージの [From] フィールドで使用する電子メールアドレスを指定します。
ステップ 12	UCS-A /monitoring/callhome # **set reply-to-email** *email-addr*	Call Home メッセージの [Reply To] フィールドで使用する電子メールアドレスを指定します。
ステップ 13	UCS-A /monitoring/callhome # **set hostname** {*hostname* | *ip-addr*}	電子メールメッセージを送信するために Call Home が使用する SMTP サーバのホスト名またはIPアドレスを指定します。
ステップ 14	UCS-A /monitoring/callhome # **set port** *port-num*	電子メールメッセージを送信するために Call Home が使用する SMTP サーバポートを指定します。有効なポート番号は 1 ～ 65535 です。
ステップ 15	UCS-A /monitoring/callhome # **set throttling** {**off** | **on**}	Call Home スロットリングをイネーブルまたはディセーブルにします。イネーブルにされると、スロットリングはあまりにも多くのCall Home電子メールメッセージが同じイベントに対して送信されるのを防ぎます。デフォルトでは、スロットリングはイネーブルです。
ステップ 16	UCS-A /monitoring/callhome # **set urgency** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **information** | **notifications** | **warnings**}	Call Home 電子メール メッセージの緊急性レベルを指定します。
ステップ 17	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home を設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 192.168.100.12
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

次のタスク

Smart Call Homeで使用するよう Call Home プロファイルを設定するには、「デフォルトの Cisco TAC-1 プロファイルの設定 （118 ページ）」へ進みます。

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

始める前に

「Smart Call Home の設定 （116 ページ）」セクションを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /monitoring/callhome # **scope profile CiscoTac-1**	デフォルト Cisco TAC-1 プロファイルのモニタリング Call Home プロファイル モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring/callhome/profile # **set level normal**	プロファイルの **normal** イベント レベルを指定します。
ステップ 3	UCS-A /monitoring/callhome/profile # **set alertgroups ciscotac**	プロファイルに **ciscotac** アラート グループを指定します。
ステップ 4	UCS-A /monitoring/callhome/profile # **set format xml**	電子メール メッセージのフォーマットを **xml** に指定します。
ステップ 5	UCS-A /monitoring/callhome/profile # **set maxsize 5000000**	電子メール メッセージに最大サイズ **5000000** を指定します。
ステップ 6	UCS-A /monitoring/callhome/profile # **create destination callhome@cisco.com**	電子メール受信者を **callhome@cisco.com** に指定します。
ステップ 7	UCS-A /monitoring/callhome/profile/destination # **exit**	モニタリング Call Home プロファイル モードを終了します。
ステップ 8	UCS-A /monitoring/callhome/profile # **exit**	モニタリング Call Home モードを終了します。

例

次の例では、Smart Call Home で使用するデフォルト Cisco TAC-1 プロファイルを設定します。

```
UCS-A /monitoring/callhome* # scope profile CiscoTac-1
UCS-A /monitoring/callhome/profile* # set level normal
UCS-A /monitoring/callhome/profile* # set alertgroups ciscotac
UCS-A /monitoring/callhome/profile* # set format xml
UCS-A /monitoring/callhome/profile* # set maxsize 5000000
UCS-A /monitoring/callhome/profile* # create destination callhome@cisco.com
UCS-A /monitoring/callhome/profile/destination* # exit
UCS-A /monitoring/callhome/profile* # exit
UCS-A /monitoring/callhome* #
```

次のタスク

Smart Call Home で使用するシステム インベントリ メッセージを設定するには、「Smart Call Home 用のシステム インベントリ メッセージの設定 （119 ページ）」に進みます。

Smart Call Home 用のシステム インベントリ メッセージの設定

始める前に

「デフォルトの Cisco TAC-1 プロファイルの設定 （118 ページ）」セクションを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /monitoring/callhome # **scope inventory**	モニタリング Call Home インベントリ モードを開始します。
ステップ 2	UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** | **on**}	インベントリ メッセージの送信をイネーブルまたはディセーブルにします。 **on** キーワードを指定すると、インベントリ メッセージは Call Home データベースに自動的に送信されます。
ステップ 3	UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num*	インベントリ メッセージが送信される時間間隔（日数）を指定します。
ステップ 4	UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour*	インベントリ メッセージが送信される時刻を指定します（24 時間形式を使用）。
ステップ 5	UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute*	インベントリ メッセージが送信される時刻の後の分数を指定します。
ステップ 6	UCS-A /monitoring/callhome/inventory # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home システム インベントリ メッセージを設定し、トランザクションをコミットする例を示します。

```
UCS-A /monitoring/callhome* # scope inventory
UCS-A /monitoring/callhome/inventory* # set send-periodically on
UCS-A /monitoring/callhome/inventory* # set interval-days 15
UCS-A /monitoring/callhome/inventory* # set timeofday-hour 21
UCS-A /monitoring/callhome/inventory* # set timeofday-minute 30
UCS-A /monitoring/callhome/inventory* # commit-buffer
UCS-A /monitoring/callhome/inventory #
```

次のタスク

Smart Call Home 登録プロセスを開始するインベントリ メッセージを送信するには、「Smart Call Home の登録 （121 ページ）」に進みます。

Smart Call Home の登録

始める前に

「Smart Call Home 用のシステム インベントリ メッセージの設定 （119 ページ）」セクションを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /monitoring/callhome/inventory # **send**	Smart Call Home データベースにシステム インベントリ メッセージを送信します。 シスコがシステム インベントリを受信すると、Smart Call Home 登録電子メールが、Smart Call Home メイン連絡先の電子メール アドレスとして設定した電子メール アドレスに送信されます。

例

次に、Smart Call Home データベースにシステム インベントリ メッセージを送信する例を示します。

```
UCS-A /monitoring/callhome/inventory # send
```

次のタスク

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。

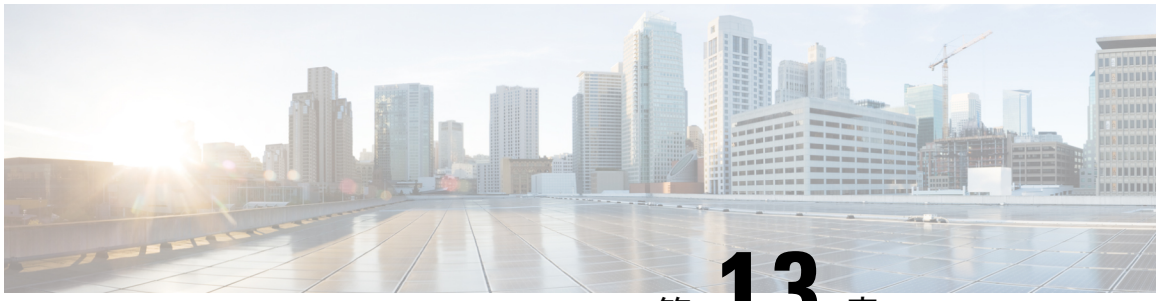
1. 電子メール内のリンクをクリックします。

   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。

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

3. 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 13 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 （123 ページ）
- 内部バックアップの間隔の変更 （123 ページ）
- ヘルス チェックのトリガー （124 ページ）
- ヘルス チェックの間隔の変更 （124 ページ）

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 （124 ページ）、およびヘルス チェックの間隔の変更 （124 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 （123 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。

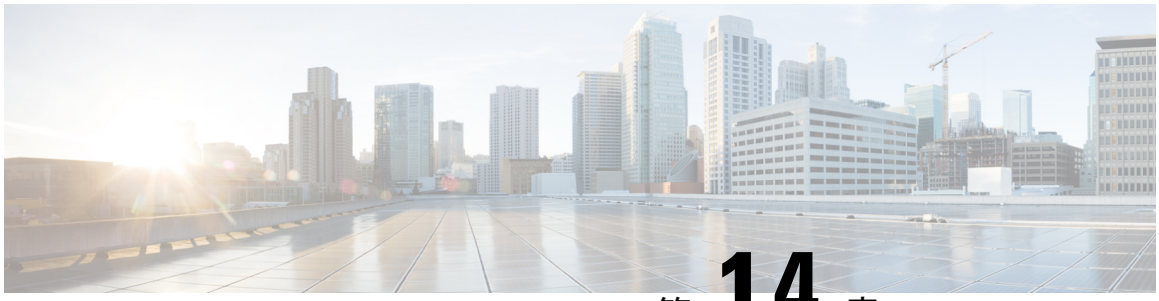
手順

	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。
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 14 章

ハードウェア モニタリング

- システム モニタリング CLI コマンドのチート シート （127 ページ）
- シャーシの管理 （129 ページ）
- ブレード サーバの管理 （130 ページ）
- ラックマウント サーバの管理 （131 ページ）
- PCIe ノードのモニタリング （134 ページ）
- ファン モジュールのモニタリング （135 ページ）
- 管理インターフェイスのモニタリング （137 ページ）
- ローカル ストレージのモニタリング （140 ページ）
- グラフィックス カードのモニタリング （153 ページ）
- PCI スイッチのモニタリング （156 ページ）
- Transportable Flash Module と スーパーキャパシタの管理 （157 ページ）
- TPM モニタリング （158 ページ）

システム モニタリング CLI コマンドのチート シート

次の表に、システム内の管理対象オブジェクトをモニタするために使用する Cisco UCS Manager CLI コマンドの要約を記載します。

管理対象オブジェクト	モニタリング コマンド	説明
ハードウェア		
シャーシ	**show chassis [adaptor |cmc |decommissioned |detail |environment |fabric |fi-iom |firmware |fsm |inventory |psu |version]**	シャーシ情報を表示します。
ファブリック インターコネクト	**show fabric-interconnect[a |b] [detail |environment |firmware |fsm |inventory |mac-aging |mode |version]**	ファブリック インターコネクトの情報を表示します。

管理対象オブジェクト	モニタリング コマンド	説明
FEX	**show fex** [**detail** | **firmware** | **fsm** | **inventory** | **version**]	ファブリック エクステンダの情報を表示します。
IOM	**show iom**[**firmware** |**health** |**version**]	ファブリック入出力モジュールの情報を表示します。
サーバ	**show server**[**actual-boot-order adapter** |**assoc** |**bios** |**boot-order** |**cpu** |**decommissioned** |**environment** |**firmware** |**health** |**identity** |**inventory** |**memory** |**status** |**storage** |**version**]	サーバ情報を表示します。
システム	**show system**[**detail** |**firmware** |**version**]	システム情報を表示します。
システム	**scope monitoring**[**show**] [**baseline-faults** |**callhome** |**event** |**fault** |**fault-suppress-policy** |**fsm** |**mgmt-if-mon-policy** |**new-faults** |**snmp** |**snmp-trap** |**snmp-user** |**stats-collection-policy** |**stats-threshold-policy** |**syslog**]	モニタリング モードのコマンドに関する情報を表示します。
ログ		
Event	**show event** [*event-id* | **detail**]	イベント ログを表示します。
Fault	**show fault** [*fault-id* | **cause** | **detail** | **severity** | **suppressed**]	障害ログを表示します。
SEL	**show sel** [*chassis-id*/*blade-id* | *rack-id*]	シャーシ、ブレード、またはラックマウント サーバのシステム イベント ログを表示します。
Syslog	**scope monitoring**[**show**] [**syslog**]	Syslog を表示します。

シャーシの管理

シャーシのロケータ LED の電源投入

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope chassis**　シャーシ番号	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **enable locator-led**	シャーシ ロケータ LED の電源を投入します。
ステップ 3	UCS-A /chassis # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、シャーシ 2 のロケータ LED の電源を投入し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2
UCS-A /chassis # enable locator-led
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```

シャーシのロケータ LED の電源切断

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope chassis**　シャーシ番号	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **disable locator-led**	シャーシ ロケータ LED の電源を切断します。
ステップ 3	UCS-A /chassis # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、シャーシ 2 のロケータ LED の電源を切断し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2
UCS-A /chassis # disable locator-led
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```

ブレード サーバの管理

ブレード サーバーのロケータ LED の電源投入

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope server** *chassis-num / server-num*	指定したシャーシでシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **enable locator-led** [**multi-master** | **multi-slave**]	ブレード サーバーのロケータ LED の電源を投入します。
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、シャーシ 2 のブレード サーバ 4 のロケータ LED の電源を投入し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # enable  locator-led
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ブレード サーバーのロケータ LED の電源切断

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope server** *chassis-num* / *server-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis/server # **disable locator-led** [**multi-master** | **multi-slave**]	ブレード サーバーのロケータ LED の電源を切断します。
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Example

次に、シャーシ 2 のブレード サーバ 4 のロケータ LED の電源を切断し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2/4
UCS-A /chassis/server # disable locator-led
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ラックマウント サーバの管理

ラックマウント サーバーのロケータ LED の電源投入

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したラックマウント サーバーでサーバー モードを開始します。
ステップ 2	UCS-A /server # **enable locator-led**	ラックマウント サーバーのロケータ LED の電源を投入します。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ラックマウント サーバー 2 のロケータ LED の電源を投入し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2
UCS-A /server # enable  locator-led
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバーのロケータ LED の電源切断

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したラックマウントサーバーでサーバー モードを開始します。
ステップ 2	UCS-A /server # **disable locator-led**	ラックマウント サーバーのロケータ LED の電源を切断します。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ラックマウント サーバー 2 のロケータ LED の電源を切断し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2
UCS-A /server # disable  locator-led
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバーのステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show server status**	Cisco UCS ドメイン内にあるすべてのサーバーのステータスを表示します。

例

次に、Cisco UCS ドメイン 内にあるすべてのサーバーのステータスを表示する例を示します。番号が 1 および 2 のサーバーは、ラックマウント サーバーであるため、表にスロットが示されていません。

```
Server Slot  Status    Availability  Overall Status  Discovery
------------------------------------------------------------------------
1/1          Equipped  Unavailable   Ok              Complete
1/2          Equipped  Unavailable   Ok              Complete
1/3          Equipped  Unavailable   Ok              Complete
1/4          Empty     Unavailable   Ok              Complete
1/5          Equipped  Unavailable   Ok              Complete
1/6          Equipped  Unavailable   Ok              Complete
1/7          Empty     Unavailable   Ok              Complete
1/8          Empty     Unavailable   Ok              Complete
1            Equipped  Unavailable   Ok              Complete
2            Equipped  Unavailable   Ok              Complete
```

ラックマウントサーバのホストイーサネットインターフェイスステータスのモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-num*	指定したサーバを開始します。
ステップ 2	UCS-A server / # **scope adapter** *adapter-num*	指定されたアダプタを開始します。
ステップ 3	UCS-A server / adapter # **show host-eth-if-detail** *adapter-num*	指定されたアダプタのホストイーサネット インターフェイスの詳細が表示されます。

例

以下の例では、アダプタのホストイーサネットインターフェイスの詳細が表示されます。

```
UCS-A server / adapter # show host-eth-if-detail
ID:1
Dynamic MAC address: B4:96:91:89:5B:48
Burned-In MAC address: B4:96:91:89:5B:48
Model: Device 1593
Name:
Cdn Name:
Admin State: Enabled
Operability: Operable
Order: Unspecified
```

```
PCI Addr: 168:00.0
Side: Left
Host Interface Ethernet MTU: 1500
Fabric ID: None
Port ID: 1
Slot ID: 0
Peer Port ID: 0
Peer Slot ID: 0
Peer Chassis ID: N/A
Virtualization Preference: None
Port State: Up
Port Speed: 10000 Mbps
Current Task:
```

PCIe ノードのモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A# **Show pcie-node detail**	PCIe ノードの詳細を表示します。

例

次に、シャーシ 1 の PCIe モジュールに関する情報を表示する例を示します。

```
UCS-A# scope chassis 1
UCS-A# show pcie-node detail
PCIe Node:
    Slot Id: 1
    Model: UCSX-440P
    Vendor: Cisco Systems Inc
    Serial (SN): FCH26xxxxxxK
    Type: Gpu
    Peer Dn: sys/chassis-1/blade-2
    Overall Status: Operable
    Presence: Equipped

    Slot Id: 3
    Model: UCSX-440P
    Vendor: Cisco Systems Inc
    Serial (SN): FCHxxxxxxxx3
    Type: Gpu
    Peer Dn: sys/chassis-1/blade-4
    Overall Status: Operable
    Presence: Equipped

    Slot Id: 5
    Model: UCSX-440P
    Vendor: Cisco Systems Inc
    Serial (SN): FCHxxxxxxxYP
    Type: Gpu
```

```
    Peer Dn: sys/chassis-1/blade-6
    Overall Status: Operable
    Presence: Equipped
UCS-A /chassis #
```

ファン モジュールのモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **show environment fan**	シャーシ内のすべてのファンの環境ステータスを表示します。 これには次の情報が含まれます。 • 全体のステータス • 運用性 • 電源の状態 • 温度ステータス • しきい値ステータス • 電圧ステータス
ステップ 3	UCS-A /chassis # **scope fan-module** *tray-num module-num*	指定したファン モジュールでモジュール シャーシ モードを開始します。 （注） 各シャーシには、1つのトレイが含まれるため、このコマンドのトレイ番号は常に 1 です。
ステップ 4	UCS A/chassis/fan-module # **show** [**detail** | **expand**]	指定したファンモジュールの環境ステータスを表示します。

例

次に、シャーシ 1 のファン モジュールに関する情報を表示する例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # show environment fan
Chassis 1:
```

```
Overall Status: Power Problem
Operability: Operable
Power State: Redundancy Failed
Thermal Status: Upper Non Recoverable

Tray 1 Module 1:
    Threshold Status: OK
    Overall Status: Operable
    Operability: Operable
    Power State: On
    Thermal Status: OK
    Voltage Status: N/A

    Fan Module Stats:
         Ambient Temp (C): 25.000000

    Fan 1:
        Threshold Status: OK
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: OK
        Voltage Status: N/A

    Fan 2:
        Threshold Status: OK
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: OK
        Voltage Status: N/A

Tray 1 Module 2:
    Threshold Status: OK
    Overall Status: Operable
    Operability: Operable
    Power State: On
    Thermal Status: OK
    Voltage Status: N/A

    Fan Module Stats:
         Ambient Temp (C): 24.000000

    Fan 1:
        Threshold Status: OK
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: OK
        Voltage Status: N/A

    Fan 2:
        Threshold Status: OK
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: OK
        Voltage Status: N/A
```

次に、シャーシ 1 のファン モジュール 2 に関する情報を表示する例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope fan-module 1 2
```

```
UCS-A /chassis/fan-module # show detail
Fan Module:
    Tray: 1
    Module: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Product Name: Fan Module for UCS 5108 Blade Server Chassis
    PID: N20-FAN5
    VID: V01
    Vendor: Cisco Systems Inc
    Serial (SN): NWG14350B6N
    HW Revision: 0
    Mfg Date: 1997-04-01T08:41:00.000
```

管理インターフェイスのモニタリング

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 モニタリング モードを開始します。

UCS-A# **scope monitoring**

ステップ 2 管理インターフェイス モニタリング ポリシーをイネーブルにするか、ディセーブルにします。

UCS-A /monitoring # **set mgmt-if-mon-policy admin-state** {**enabled** | **disabled**}

ステップ 3 システムがデータの記録の間で待機する秒数を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy poll-interval**

90 ～ 300 の整数を入力します。

ステップ 4 管理インターフェイス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を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy max-fail-reports** *num: mon*-試行

2 ～ 5 の整数を入力します。

ステップ 5 システムが使用するモニタリング メカニズムを指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy monitor-mechanism** {**mii-status** | **ping-arp-targets** | **ping-gateway**

- **mii-status**—システム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。
- **ping-arp-targets** —システムは Address Resolution Protocol（ARP）を使用して指定されたターゲットに ping を送信します。
- **ping-gateway**—システムは管理インターフェイスでこの Cisco UCS ドメイン インスタンスに指定されたデフォルト ゲートウェイ アドレスに ping を送信します。

ステップ 6 モニタリング メカニズムとして **mii-status** を選択した場合、次のプロパティを設定します。

a) 前回の試行が失敗したとき、もう一度 MII からの応答を要求する前にシステムが待機する秒数を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy mii-retry-interval** *num-seconds*

3 ～ 10 の範囲の整数を入力します。

b) インターフェイスが使用不能であるとシステムが判断するまでにシステムが MII をポーリングする回数を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy mii-retry-count** *num-retries*

1 ～ 3 の整数を入力します。

ステップ 7 モニタリング メカニズムとして **ping-arp-targets** を選択した場合、次のプロパティを設定します。

a) システムが ping する最初の IPv4 または IPv6 アドレスを指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp target1* | *ndisc target1*} {*ipv4 addr* | *ipv6 addr*}

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。

b) システムが ping する第 2 の IPv4 または IPv6 アドレスを指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp target2* | *ndisc target2*} {*ipv4 addr* | *ipv6 addr*}

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。

c) システムが ping する第 3 の IPv4 または IPv6 アドレスを指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp target3* | *ndisc target3*\\{*ipv4 addr* | *ipv6 addr*}

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。

（注）
ping IPv4 ARP または IPv6 N ディスク ターゲットは、ファブリック インターコネクトと同じサブネットまたはプレフィクスにそれぞれある必要があります。

d) ターゲット IP アドレスに送信する ARP 要求の数を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy arp-requests** *num* 要求

1 ～ 5 の整数を入力します。

e) 使用不能と見なす前にシステムが ARP ターゲットからの応答を待機する秒数を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy arp-deadline** *num-seconds*

5 ～ 15 の範囲内の数を入力してください。

ステップ 8 モニタリング メカニズムとして **ping-gateway** wo選択した場合、次のプロパティを設定します。

a) システムがゲートウェイに ping を実行する必要がある回数を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy ping-requests**

1 ～ 5 の整数を入力します。

b) アドレスが使用不能であるとシステムが判断するまでゲートウェイからの応答を待機する秒数を指定します。

UCS-A /monitoring # **set mgmt-if-mon-policy ping-deadline**

5 ～ 15 の整数を入力します。

ステップ 9 UCS-A /monitoring # **commit-buffer**

トランザクションをシステムの設定にコミットします。

例

次に、メディア独立型インターフェイス（MII）モニタリング メカニズムを使用してモニタリング インターフェイス管理ポリシーを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # set mgmt-if-mon-policy admin-state enabled
UCS-A /monitoring* # set mgmt-if-mon-policy poll-interval 250
UCS-A /monitoring* # set mgmt-if-mon-policy max-fail-reports 2
UCS-A /monitoring* # set mgmt-if-mon-policy monitor-mechanism set mii-status
UCS-A /monitoring* # set mgmt-if-mon-policy mii-retry-count 3
UCS-A /monitoring* # set mgmt-if-mon-policy mii-retry-interval 7
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

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 X210c M8 コンピューティング ノード
- Cisco UCS X215c M8 コンピューティング ノード
- Cisco UCS X210c M7 コンピューティング ノード
- Cisco UCS X210c M6 コンピューティングノード
- Cisco UCS B200 M6サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS C240 M8 サーバ
- Cisco UCS C220 M8 サーバ
- Cisco UCS C245 M8 サーバ

- Cisco UCS C225 M8 サーバ
- Cisco UCS C240 M7 サーバ
- Cisco UCS C220 M7 サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C245 M6サーバ
- Cisco UCS C220 M6サーバ
- Cisco UCS C225 M6サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS C220 M5 サーバ

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。

レガシー ディスク ドライブのモニタリング

（注） 以下の情報は、B200 M1/M2 および B250 M1/M2 ブレード サーバにのみ適用されます。

Cisco UCS のディスク ドライブのモニタリングは、Cisco UCS ドメイン 内のサポートされているブレードサーバについて、ブレードに存在するディスク ドライブのステータスをCisco UCS Managerに提供します。ディスク ドライブ モニタリングは、ステータス情報提供のためにLSI ファームウェアから Cisco UCS Manager への単方向障害の信号を提供します。

次のサーバ コンポーネントおよびファームウェア コンポーネントが、サーバ内のディスク ドライブ ステータスに関する情報の収集、送信、および集約を行います。

- 物理的なプレゼンス センサー：ディスク ドライブがサーバ ドライブ ベイに挿入されているかどうかを調べます。

- 物理的な障害センサー：ディスク ドライブの LSI ストレージ コントローラ ファームウェアからレポートされる操作可能性のステータスを調べます。
- IPMI ディスク ドライブの障害およびプレゼンス センサー：センサーの結果を Cisco UCS Manager に送信します。
- ディスク ドライブの障害 LED 制御および関連する IPMI センサー：ディスク ドライブの障害 LED の状態（オン/オフ）を制御し、それらの状態を Cisco UCS Manager に伝えます。

ローカル ディスク ロケータ LED のオン

手順

ステップ 1 UCS-A # **scope server** *id*

指定したサーバのサーバ モードを開始します。

ステップ 2 UCS-A/server # **scope local-disk** *id*

指定されたローカル ディスクの RAID コントローラを入力します。

ステップ 3 UCS-A /server/local-disk # **enable locator-led**

ディスク ロケータ LED をオンにします。

ステップ 4 UCS-A/server/local-disk* # **commit-buffer**

コマンドをシステムの設定にコミットします。

例

次に、ローカル ディスク ロケータ LED をオンにする例を示します。

```
UCS-A# scope server 1
UCS-A /server/raid-controller # scope local-disk 2
USA-A /server/raid-controller/local-disk # enable locator-led
USA-A /server/raid-controller/local-disk* # commit-buffer
```

ローカル ディスク ロケータ LED のオフ

手順

ステップ 1 UCS-A# **scope server** *id*

指定したサーバのサーバ モードを開始します。

ステップ 2 UCS-A/server # **scope local-disk** *id*

指定されたローカル ディスクの RAID コントローラを入力します。

ステップ 3 UCS-A/server/local-disk # **disable locator-led**

ディスク ロケータ LED をオフにします。

ステップ 4 UCS-A/server/raid-controller/local-disk* # **commit-buffer**

コマンドをシステムの設定にコミットします。

例

次に、ローカル ディスク ロケータ LED を無効化する例を示します。

```
UCS-A# server 1
UCS-A /server # scope local-disk 2
USA-A /server/local-disk # disable locator-led
USA-A /server/local-disk* # commit-buffer
```

ローカル ディスク ロケータ LED の状態の表示

手順

ステップ 1 UCS-A# **scope server** *id*

指定したサーバのサーバ モードを開始します。

ステップ 2 UCS-A/server # **scope local-disk** *id*

指定されたローカル ディスクの RAID コントローラを入力します。

ステップ 3 UCS-A/server/local-disk # **show locator-led**

ディスク ロケータ LED の状態を表示します。

例

次の例は、ローカル ディスク ロケータ LED の状態がオンになっていることを示しています。

```
USA-A# scope server 1
USA-A /server # scope local-disk 2
USA-A /serverlocal-disk # show locator-led
Locator LED:
    Equipment        Operational State
```

```
---------------- -----------------
1/SAS-1/2        On
```

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 M6サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 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。

Flash 寿命ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **show raid-controller detail expand**	RAID コントローラの詳細を表示します。

例

次に、サーバ 3 の Flash 寿命ステータスを表示する例を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # show raid-controller detail expand

RAID Controller:
    ID: 1
    Type: FLASH
    PCI Addr: 131:00.0
    Vendor: Cisco Systems Inc
    Model: UCSC-F-FIO-1205M
```

```
    Serial: 1315D2B52
    HW Rev: FLASH
    Raid Support: No
    OOB Interface Supported: No
    Rebuild Rate: N/A
    Controller Status: Unknown

    Flash Life:
    Flash Percentage: N/A
    FLash Status: Error(244)

UCS-A /chassis/server #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *server-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **show inventory storage**	サーバのローカルおよび仮想ストレージの情報を表示します。

例

次に、サーバ 2 のローカル ディスク ステータスを表示する例を示します。

```
UCS-A# scope server 1/2
UCS-A /chassis/server # show inventory storage
Server 1/2:
    Name:
    User Label:
    Equipped PID: UCSB-B200-M3
    Equipped VID: V01
    Equipped Serial (SN): FCH16207KXG
    Slot Status: Equipped
    Acknowledged Product Name: Cisco UCS B200 M3
    Acknowledged PID: UCSB-B200-M3
    Acknowledged VID: V01
    Acknowledged Serial (SN): FCH16207KXG
    Acknowledged Memory (MB): 98304
    Acknowledged Effective Memory (MB): 98304
    Acknowledged Cores: 12
    Acknowledged Adapters: 1
    Motherboard:
        Product Name: Cisco UCS B200 M3
        PID: UCSB-B200-M3
        VID: V01
        Vendor: Cisco Systems Inc
        Serial (SN): FCH16207KXG
        HW Revision: 0

        RAID Controller 1:
            Type: SAS
```

```
  Vendor: LSI Logic   Symbios Logic
  Model: LSI MegaRAID SAS 2004 ROMB
  Serial: LSIROMB-0
  HW Revision: B2
  PCI Addr: 01:00.0
  Raid Support: RAID0, RAID1
  OOB Interface Supported: Yes
  Rebuild Rate: 31
  Controller Status: Optimal

Local Disk 1:
     Product Name: 146GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted
     PID: A03-D146GA2
     VID: V01
     Vendor: SEAGATE
     Model: ST9146803SS
     Vendor Description: Seagate Technology LLC
     Serial: 3SD31S4X
     HW Rev: 0
     Block Size: 512
     Blocks: 285155328
     Operability: Operable
     Oper Qualifier Reason: N/A
     Presence: Equipped
     Size (MB): 139236
     Drive State: Online
     Power State: Active
     Link Speed: 6 Gbps
     Device Type: HDD

  Local Disk 2:
     Product Name: 600G AL12SE SAS Hard Disk Drive
     PID: A03-D600GA2
     VID: V01
     Vendor: TOSHIBA
     Model: MBF2600RC
     Vendor Description: Toshiba Corporation
     Serial: EA00PB109T4A
     HW Rev: 0
     Block Size: 512
     Blocks: 1169920000
     Operability: Operable
     Oper Qualifier Reason: N/A
     Presence: Equipped
     Size (MB): 571250
     Drive State: Online
     Power State: Active
     Link Speed: 6 Gbps
     Device Type: HDD

  Local Disk Config Definition:
     Mode: RAID 1 Mirrored
     Description:
     Protect Configuration: No

  Virtual Drive 0:
     Type: RAID 1 Mirrored
     Block Size: 512
     Blocks: 285155328
     Operability: Operable
     Presence: Equipped
     Size (MB): 139236
     Lifecycle: Allocated
     Drive State: Optimal
```

```
                Strip Size (KB): 64
                Access Policy: Read Write
                Read Policy: Normal
                Configured Write Cache Policy: Write Through
                Actual Write Cache Policy: Write Through
                IO Policy: Direct
                Drive Cache: No Change
                Bootable: False

UCS-A /chassis/server #
```

次に、PCIe\NVMeフラッシュ ストレージを備えたサーバ2のローカルディスク ステータスを表示する例を示します。

```
UCS-A# scope server 1/2
UCS-A /chassis/server # show inventory storage
Server 1/2:
Name:
    Acknowledged Serial (SN): FCH1901V0FK
    Acknowledged Product Name: Cisco UCS C240 M4S2
    Acknowledged PID: UCSC-C240-M4S2
    Acknowledged VID: 0
    Acknowledged Memory (MB): 16384
    Acknowledged Effective Memory (MB): 16384
    Acknowledged Cores: 24
    Acknowledged Adapters: 4
    Motherboard:
        Product Name: Cisco UCS C240 M4S2
        PID: UCSC-C240-M4S2
        VID: V01
        Vendor: Cisco Systems Inc
        Serial (SN): FCH1901V0FK
        HW Revision: 0

        Raid Controller 1:
            Type: NVMe
            Vendor: HGST
            Model: HUSPR3280ADP301
            Serial: STM0001A74F2
            HW Revision:
            PCI Addr: 42:00.0
            Raid Support: No
            OOB Interface Supported: Yes
            Rebuild Rate: 0
            Controller Status: Optimal


            Local Disk 2:
                Product Name: Cisco UCS 800GB 2.5 in NVMe based PCIeSSD
                PID: UCS-SDHPCIE800GB
                VID:
                Vendor: HGST
                Model: HUSPR3280ADP301
                Vendor Description:
                Serial: 14310CF8E975
                HW Rev: 0
                Block Size: 512
                Blocks: 285155328
                Operability: NA
                Oper Qualifier Reason: N/A
                Presence: Equipped
                Size: 94413
                Drive State: NA
                Power State: NA
```

```
                Link Speed: NA
                Device Type: SSD
                Thermal: N/A
UCS-A /chassis/server #
```

次に、Cisco UCS（P3600）2.5 インチ 800 GB NVMe ベース PCIe SSD のローカル ディスク ステータスを表示する例を示します。

```
RAID Controller:
    ID: 1
    Type: NVME
    PCI Addr: 69:00.0
    Vendor: Intel
    Model: SSDPE2ME800G4K
    Serial: CVMD6083003D800GGN
    HW Rev:
    Raid Support: No
    OOB Interface Supported: Yes
    Mode: NVME
    Rebuild Rate: 0
    Controller Status: Optimal
    Config State: Not Applied
    Pinned Cache Status: Disabled
    Sub OEM ID: 0
    Supported Strip Sizes: Not Applicable
    Default Strip Size: Unknown
   PCI Slot: FrontPCIe5
    Product Variant: default
    Product Name: Cisco UCS (P3600) 2.5 inches 800 GB NVMe based PCIe SSD
    PID: UCS-PCI25-8003
    VID:
    Part Number:
    Storage Controller Admin State: Unspecified
    Vendor Id: 0x8086
    Subvendor Id: 0x1137
    Device Id: 0x953
    Subdevice Id: 0x15b
    Current Task:

    Local Disk:
        ID: 5
        Block Size: 512
        Physical Block Size: Unknown
        Blocks: 1562822656
        Size: 763097
        Technology:
        Operability: N/A
        Oper Qualifier Reason: N/A
        Presence: Equipped
        Connection Protocol: NVME
        Product Variant: default
        Product Name: Cisco UCS (P3600) 2.5 inches 800 GB NVMe based PCIe SSD
        PID: UCS-PCI25-8003
        VID:
        Vendor: Intel
        Model: SSDPE2ME800G4K
        Vendor Description:
        Serial: CVMD6083003D800GGN
        HW Rev: 0
        Drive State: Unknown
        Power State: Unknown
        Link Speed: Unknown
        Enclosure Association Type: Unknown
        Device Version: N/A
```

```
        Device Type: SSD
        Thermal: N/A
        Admin State Type: N/A
        Admin Virtual Drive ID: Unspecified
        Current Task:
```

次に、Cisco UCS（P3600）HHHL 2000 GB NVMe ベース PCIe SSD のステータスを表示する例を示します。

```
RAID Controller:
    ID: 3
    Type: NVME
    PCI Addr: 01:00.0
    Vendor: Intel
    Model: SSDPEDME020T401
    Serial: CVMD543200AQ2P0EGN
    HW Rev:
    Raid Support: No
    OOB Interface Supported: Yes
    Mode: NVME
    Rebuild Rate: 0
    Controller Status: Optimal
    Config State: Not Applied
    Pinned Cache Status: Disabled
    Sub OEM ID: 0
    Supported Strip Sizes: Not Applicable
    Default Strip Size: Unknown
    PCI Slot: 2
    Product Variant: default
    Product Name: Cisco UCS (P3600) HHHL 2000 GB NVMe based PCIe SSD
    PID: UCSC-F-I20003
    VID:
    Part Number:
    Storage Controller Admin State: Unspecified
    Vendor Id: 0x8086
    Subvendor Id: 0x1137
    Device Id: 0x953
    Subdevice Id: 0x1ac
    Current Task:

    Embedded Storage:
        Size: 2000000
        Block Size: 512
        Number Of Blocks: 3906250000
```

ディスク ドライブのステータスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope server** *server-num*	サーバー シャーシ モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}	RAID コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/raid-controller # **show local-disk** [*local-disk-id* | **detail** | **expand**]	

例

次の例は、ディスク ドライブのステータスを示しています。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 6
UCS-A /chassis/server # scope raid-controller 1 sas
UCS-A /chassis/server/raid-controller # show local-disk 1

Local Disk:
    ID: 1
    Block Size: 512
    Blocks: 60545024
    Size (MB): 29563
    Operability: Operable
    Presence: Equipped
```

RAID コントローラ動作の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **show raid-controller operation**	RAID コントローラの長期実行動作が表示されます。

例

次に、サーバ 3 の RAID コントローラ動作を表示する例を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # show raid-controller operation

    Name: Rebuild
    Affected Object: sys/chassis-1/blade-3/board/storage-SAS-1/disk-1
    State: In Progress
    Progress: 4
    Start Time: 2013-11-05T12:02:10.000
    End Time: N/A

UCS-A /chassis/server #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* **{flash | sas | sata | sd | unknown}**	RAID コントローラ サーバ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server/raid-controller # **show stats**	RAID コントローラ統計を表示します。

例

次に、RAID コントローラ統計を表示する例を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope raid-controller
UCS-A /chassis/server/raid-controller # show stats

Nvme Stats:
    Time Collected: 2016-06-22T12:37:55.043
    Monitored Object: sys/rack-unit-6/board/storage-NVME-1/nvme-stats
    Suspect: Yes
    Temperature (C): 27.000000
    Life Used Percentage: 0
    Thresholded: 0

UCS-A /chassis/server/raid-controller #
```

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。バッテリ バックアップ ユニット（BBU）が故障した場合、または故障すると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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** シャーシ番号	指定したシャーシでシャーシ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /chassis # **scope server** *server-num*	サーバー シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**flash** | **sas** | **sata** | **sd** | **unknown**}	RAID コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/raid-controller # **show raid-battery expand**	RAID バッテリ ステータスを表示します。

例

この例では、サーバの BBU に関する情報の表示方法を示します。

```
UCS-A # scope chassis 1
UCS-A /chassis #scope server 3
UCS-A /chassis/server #scope raid-controller 1 sas
UCS-A /chassis/server/raid-controller # show raid-battery expand
RAID Battery:
    Battery Type: Supercap
    Presence: Equipped
    Operability: Operable
    Oper Qualifier Reason:
    Vendor: LSI
    Model: SuperCaP
    Serial: 0
    Capacity Percentage: Full
    Battery Temperature (C): 54.000000

    Transportable Flash Module:
        Presence: Equipped
        Vendor: Cisco Systems Inc
        Model: UCSB-RAID-1GBFM
        Serial: FCH164279W6
```

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 X210c M8 コンピューティング ノード
- Cisco UCS X215c M8 コンピューティング ノード
- Cisco UCS X410c M7 コンピューティングノード
- Cisco UCS X210c M7 コンピューティング ノード

- Cisco UCS X210c M6 コンピューティングノード
- Cisco UCS C240 M8 サーバ
- Cisco UCS C220 M8 サーバ
- Cisco UCS C245 M8 サーバ
- Cisco UCS C225 M8 サーバ
- Cisco UCS C240 M7 サーバ
- Cisco UCS C220 M7 サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C220 M6サーバ
- Cisco UCS C245 M6サーバ
- Cisco UCS C225 M6サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS B200 M6サーバ
- Cisco UCS B480 M6 サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 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。

グラフィックス カードのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-# **scope server** *blade-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **show graphics-card detail**	グラフィックス カードに関する情報を表示します。

例

次に、サーバ 1 のグラフィックス カードのプロパティを表示する例を示します。

```
UCS-A# scope server 1
UCS-A /server # show graphics-card detail

ID: 1
Slot Id: 2
Magma Expander Slot Id:
Is Supported: Yes
Vendor: Cisco Systems Inc
Model: UCSB-GPU-M6
Serial: FHH1924002B
Mode: Graphics
PID: UCSB-GPU-M6
Firmware Version: 84.04.89.00.01|2754.0200.01.02
Vendor Id: 0x10de
Subvendor Id: 0x10de
Device Id: 0x13f3
Subdevice Id: 0x1143

UCS-A /server #
```

グラフィックス コントローラのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-# **scope server** *blade-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope graphics-card** *card-id*	指定したグラフィックス カードのグラフィックス カード モードを開始します。
ステップ 3	UCS A/server/graphics-card # **show graphics-controller detail**	グラフィックス コントローラに関する情報を表示します。

例

次に、サーバ 1 にあるグラフィックス カード 1 のグラフィックス コントローラのプロパティを表示する例を示します。

```
UCS-A# scope server 1
UCS-A /server # scope graphics-card 1
UCS-A /server/graphics-card # show graphics-controller detail
Graphics Controller:
    ID: 1
    Pci Address: 07:00.0
```

```
    ID: 2
    Pci Address: 08:00.0
UCS-A /server/graphics-card #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **show pci-switch**	PCI スイッチに関する情報を表示します。
ステップ 3	UCS A/server # **scope pci-switch** *pci-switch-number*	指定された PCI スイッチの PCI スイッチ モードを開始します。
ステップ 4	UCS-A /server # **show detail**	

例

次の例では、PCI スイッチのプロパティを表示する方法を示します。

```
UCS-A# scope server 1
UCS-A /server # show pci-switch
Pci Switch:
ID Pci Switch name Firmware Version
--- --------------- ----------------
1 PCI-Switch-1 xxxx
2 PCI-Switch-2 xxxxxxx
3 PCI-Switch-3 xxx
4 PCI-Switch-4 xxxxx
UCS-A /server # scope pci-switch 1
UCS-A /server/pci-switch #show detail
```

```
Pci Switch:
ID: 1
Pci Switch name: PCI-Switch-1
No of Adapters: 3
Switch Status: Good
Switch Temperature (C): 45.000000
Switch Product Revision: 0XxB
Firmware Version: xxxx
Vendor Id: xxx
Subvendor Id: xxx
Device Id: xxxx
Subdevice Id: xxxx
Switch Vendor: xxxxx
Pci Address: xx:00.0
UCS-A /server/pci-switch #
```

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 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 X210c M8 コンピューティング ノード
- Cisco UCS X215c M8 コンピューティング ノード
- Cisco UCS X410c M7 コンピューティングノード
- Cisco UCS X210c M7 コンピューティング ノード
- Cisco UCS X210c M6 コンピューティングノード
- Cisco UCS C240 M8 サーバ
- Cisco UCS C220 M8 サーバ

- Cisco UCS C245 M8 サーバ
- Cisco UCS C225 M8 サーバ
- Cisco UCS C240 M7 サーバ
- Cisco UCS C220 M7 サーバ
- Cisco UCS B200 M6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

TPM モニタリング

トラステッドプラットフォーム モジュール（TPM）は、すべての Cisco UCS M3 ブレード サーバやラックマウント サーバに搭載されています。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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope tpm** *tpm-id*	指定された TPM ID の TPM モードを開始します。
ステップ 3	UCS-A /chassis/server/tpm # **show**	TPM プロパティを表示します。
ステップ 4	UCS-A /chassis/server/tpm # **show detail**	TPM プロパティの詳細を表示します。

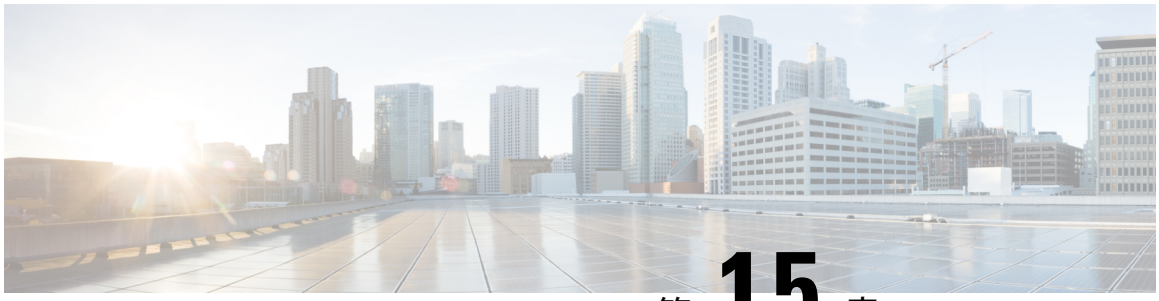
例

次の例では、シャーシ 1 のブレード 3 の TPM のプロパティを表示する方法を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope tpm 1
UCS-A /chassis/server/tpm # show

Trusted Platform Module:
    Presence: Equipped
    Enabled Status: Enabled
    Active Status: Activated
    Ownership: Unowned
UCS-A /chassis/server/tpm # show detail

Trusted Platform Module:
    Enabled Status: Enabled
    Active Status: Activated
    Ownership: Unowned
    Tpm Revision: 1
    Model: UCSX-TPM1-001
    Vendor: Cisco Systems Inc
    Serial: FCH16167DBJ
UCS-A /chassis/server/tpm #
```



第 15 章

NetFlow のモニタリング

- NetFlow モニタリング （161 ページ）
- NetFlow に関する制限事項 （163 ページ）
- NetFlow のモニタリングの有効化または無効化 （164 ページ）
- フロー レコード定義の設定 （165 ページ）
- エクスポータ プロファイルの設定 （166 ページ）
- NetFlow コレクタの設定 （167 ページ）
- フロー エクスポータの設定 （168 ページ）
- フロー モニタの設定 （169 ページ）
- フロー モニタ セッションの設定 （170 ページ）
- NetFlow キャッシュのアクティブおよび非アクティブ タイムアウトの設定 （171 ページ）
- vNIC へのフロー モニタ セッションの関連付け （172 ページ）

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 Cisco UCS VIC 1300 シリーズ、 Cisco UCS VIC 1400 シリーズ、Cisco UCS VIC 14000 シリーズ、Cisco UCS VIC 15000 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。

4.3(2b) リリース以降、NetFlow モニタリングは、Cisco UCS 6400 および 6500 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。

4.3(4b) リリース以降、NetFlow モニタリングは Cisco UCS ファブリック インターコネクト 9108 100G (Cisco UCS X シリーズ ダイレクト) でサポートされます。

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 VIC 1300、1400、14000 および 15000 シリーズ VIC アダプタでサポートされています。Cisco UCS 1200 シリーズのアダプタでは、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。
- Cisco UCS ファブリック インターコネクト 9108 100G、Cisco UCS 6500 シリーズおよび 6400 シリーズ ファブリック インターコネクトの場合
  - NetFlow モニタリングには、ホスト受信方向と送信方向の両方が含まれます。ホスト受信方向モニタに適用される NetFlow モニタリング セッションは送信と受信の両方のモニタリングを有効にしますが、ホスト送信方向モニタに適用される NetFlow モニタリング セッションは NO-OP です。
  - Vethernet インターフェイスの NetFlow モニターでは、**NFM_RECORD_L2_SRC_VLAN** が常に有効になります。
  - **フロー タイムアウト ポリシー**の**アクティブ タイムアウト**と**非アクティブ タイムアウト**の値は変更できません。
- 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、稼働マシン複数キュー、RoCE、SRIOV、Geneve、または vNIC が有効化された Linux ARFS と併用できません。
- NetFlow モニタリングを有効にしても、Cisco UCS Manager ソフトウェアをダウングレードすることはできません。ダウングレードするには、Netflow モニタリング機能を無効にします。

NetFlow のモニタリングの有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # *enable|disable*	NetFlow 機能を有効にし、Cisco UCS Manager に存在する既存の構成を NX-OS に展開します。 または、NetFlow 機能を無効にし、NX-OS から構成を削除します。NetFlow モニタリングを無効にしても、Cisco UCS Manager は NetFlow 構成を保持し、NetFlow モニタリングを有効にすると同じ構成を展開します。 （注） NetFlow を無効にすると、バックエンドからすべての NetFlow 関連の構成が削除されます。使用中のすべてのフロー セッションが削除されます。
ステップ 3	UCS-A /eth-flow-mon # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、NetFlow のモニタリングを無効にする方法を示しています。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # disable
Warning: Disabling Netflow will Remove all Netflow related configuration from backend.
All the flow session which is in use will get cleaned up.
UCS-A /eth-flow-mon* # commit-buffer
UCS-A /eth-flow-mon #
```

フロー レコード定義の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-record** *flow-record-name*	指定されたフロー レコードのフロー レコード モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-record # **set keytype** {**ipv4keys** | **ipv6keys** | **l2keys**}	キー タイプを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-record # **set ipv4keys** {**dest-port** | **ip-protocol** | **ip-tos** | **ipv4-dest-address** | **ipv4-src-address** | **src-port**}	ステップ 3 で選択したキー タイプの属性を指定します。 （注） ステップ 3 で **ipv4keys** を選択した場合にのみ、このコマンドを使用します。
ステップ 5	UCS-A /eth-flow-mon/flow-record # **set ipv6keys** {**dest-port** | **ip-protocol** | **ipv6-dest-address** | **ipv6-src-address** | **src-port**}	ステップ 3 で選択したキー タイプの属性を指定します。 （注） ステップ 3 で **ipv6keys** を選択した場合にのみ、このコマンドを使用します。
ステップ 6	UCS-A /eth-flow-mon/flow-record # **set l2keys** {**dest-mac-address** | **ethertype** | **src-mac-address**}	ステップ 3 で選択したキー タイプの属性を指定します。 （注） ステップ 3 で **l2keys** を選択した場合にのみ、このコマンドを使用します。
ステップ 7	UCS-A /eth-flow-mon/flow-record # **set nonkeys** {**counter-bytes-long** | **counter-packets-long** | **sys-uptime-first** | **sys-uptime-last**}	非キー属性を指定します。
ステップ 8	UCS-A /eth-flow-mon/flow-record # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、レイヤ 2 キーでフロー レコード定義を作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-record r1
UCS-A /eth-flow-mon/flow-record* # set keytype l2keys
UCS-A /eth-flow-mon/flow-record* #set l2keys dest-mac-address src-mac-address
UCS-A /eth-flow-mon/flow-record* # set nonkeys sys-uptime counter-bytes counter-packets
UCS-A /eth-flow-mon/flow-record* # commit-buffer
UCS-A /eth-flow-mon/flow-record #
```

エクスポータ プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **scope flow-profile** *profile-name*	指定されたプロファイルのフロー プロファイル モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-profile # **show config**	フロー プロファイルの設定を表示します。
ステップ 4	UCS-A /eth-flow-mon/flow-profile # **enter vlan** *vlan-name*	エクスポータ プロファイルに関連付けられた VLAN を指定します。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。
ステップ 5	UCS-A /eth-flow-mon/flow-profile/vlan # **enter fabric** {**a** | **b**}	指定されたファブリックのフロー プロファイル モードを開始します。
ステップ 6	UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **set addr** *ip-addr* **subnet** *ip-addr*	ファブリックのエクスポータ プロファイルの送信元 IP アドレスおよびサブネット マスクを指定します。 **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

	コマンドまたはアクション	目的
		ドレスの競合が発生する可能性があります。
ステップ 7	UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、デフォルトのエクスポータ プロファイルを設定し、各ファブリックのエクスポータ インターフェイスの送信元 IP アドレスおよびサブネット マスクを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # scope flow-profile default
UCS-A /eth-flow-mon/flow-profile # enter vlan 100
UCS-A /eth-flow-mon/flow-profile/vlan* # enter fabric a
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # set addr 10.10.10.10 subnet 255.255.255.0
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # up
UCS-A /eth-flow-mon/flow-profile/vlan* # enter fabric b
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # set addr 10.10.10.11 subnet 255.255.255.0
UCS-A /eth-flow-mon/flow-profile/vlan/fabric* # commit-buffer
UCS-A /eth-flow-mon/flow-profile/vlan/fabric #
```

NetFlow コレクタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-collector** *flow-collector-name*	指定されたフロー コレクタのフロー コレクタ モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-collector # **set dest-port** *port_number*	フロー コレクタの宛て先ポートを指定します。
ステップ 4	UCS-A /eth-flow-mon # **set vlan** *flow-collector-name*	フロー コレクタの VLAN ID を指定します。
ステップ 5	UCS-A /eth-flow-mon/flow-collector # **enter ip-if**	IPv4 コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /eth-flow-mon/flow-collector/ip-if # **set addr** *ip-address*	エクスポータ IP アドレスを指定します。
ステップ 7	UCS-A /eth-flow-mon/flow-collector/ip-if # **set exporter-gw** *gw-address*	エクスポータ ゲートウェイ アドレスを指定します。
ステップ 8	UCS-A /eth-flow-mon/flow-collector/ip-if # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、NetFlow コレクタを設定し、エクスポータ IP とゲートウェイ アドレスを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-collector c1
UCS-A /eth-flow-mon/flow-collector* # set dest-port 9999
UCS-A /eth-flow-mon/flow-collector* # set vlan vlan100
UCS-A /eth-flow-mon/flow-collector* # enter ip-if
UCS-A /eth-flow-mon/flow-collector/ip-if* # set addr 20.20.20.20
UCS-A /eth-flow-mon/flow-collector/ip-if* # set exporter-gw 10.10.10.1
UCS-A /eth-flow-mon/flow-collector/ip-if* # commit-buffer
UCS-A /eth-flow-mon/flow-collector/ip-if #
```

フロー エクスポータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-exporter** *flow-exporter-name*	指定されたフローエクスポータのフローエクスポータ モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-exporter # **set dscp** *dscp_number*	DiffServ コードポイントを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-exporter # **set flow-collector** *flow-collector_name*	フロー コレクタを指定します。
ステップ 5	UCS-A /eth-flow-mon/flow-exporter # **set exporter-stats-timeout** *timeout_number*	NetFlow フロー エクスポータ データを再送信する場合のタイムアウト期間を指定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /eth-flow-mon/flow-exporter # **set interface-table-timeout** *timeout_number*	NetFlow フロー エクスポータ インターフェイス テーブルの再送信の時間を指定します。
ステップ 7	UCS-A /eth-flow-mon/flow-exporter # **set template-data-timeout** *timeout_number*	NetFlow テンプレート データを再送信する場合のタイムアウト期間を指定します。
ステップ 8	UCS-A /eth-flow-mon/flow-exporter # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、フローエクスポータを設定して、タイムアウト値を設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-exporter ex1
UCS-A /eth-flow-mon/flow-exporter* # set dscp 6
UCS-A /eth-flow-mon/flow-exporter* # set flow-collector c1
UCS-A /eth-flow-mon/flow-exporter* # set exporter-stats-timeout 600
UCS-A /eth-flow-mon/flow-exporter* # set interface-table-timeout 600
UCS-A /eth-flow-mon/flow-exporter* # set template-data-timeout 600
UCS-A /eth-flow-mon/flow-exporter* # commit-buffer
UCS-A /eth-flow-mon/flow-exporter #
```

フロー モニタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-monitor** *flow-monitor-name*	指定されたフロー モニタのフロー モニタ モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-monitor # **set flow-record** *flow-record-name*	フロー レコードを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter** *flow-exporter-name*	1 番目のフローエクスポータを指定します。
ステップ 5	UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter** *flow-exporter-name*	2 番目のフローエクスポータを指定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /eth-flow-mon/flow-monitor # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、フロー モニタを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-monitor m1
UCS-A /eth-flow-mon/flow-monitor* # set flow-record r1
UCS-A /eth-flow-mon/flow-monitor* # create flow-exporter ex1
UCS-A /eth-flow-mon/flow-monitor* # create flow-exporter ex2
UCS-A /eth-flow-mon/flow-monitor* # commit-buffer
UCS-A /eth-flow-mon/flow-monitor #
```

フロー モニタ セッションの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-mon-session** *flow-monitor-session-name*	指定されたフロー モニタ セッションのフロー モニタ セッション モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-1*	1 番目のフロー モニタを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-2*	2 番目のフロー モニタを指定します。
ステップ 5	UCS-A /eth-flow-mon/flow-mon-session # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、2 つのフロー モニタを使用してフロー モニタ セッションを作成する例を示します。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # enter flow-mon-session s1
UCS-A /eth-flow-mon/flow-mon-session* # create flow-monitor m1
UCS-A /eth-flow-mon/flow-mon-session* # create flow-monitor m2
```

```
UCS-A /eth-flow-mon/flow-mon-session* # commit-buffer
UCS-A /eth-flow-mon/flow-mon-session #
```

NetFlow キャッシュのアクティブおよび非アクティブ タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **scope flow-timeout** *timeout-name*	指定したフロー タイムアウトのフロー タイムアウト モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-timeout # **set cache-timeout-active** *timeout-value*	アクティブなタイムアウト値を指定します。この値は 60 ～ 4092 秒です。デフォルト値は 120 秒です。
ステップ 4	UCS-A /eth-flow-mon/flow-timeout # **set cache-timeout-inactive** *timeout-value*	非アクティブなタイムアウト値を指定します。この値は 15 ～ 4092 秒です。デフォルト値は 15 秒です。
ステップ 5	UCS-A /eth-flow-mon/flow-timeout # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、NetFlow タイムアウト値を変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-flow-mon
UCS-A /eth-flow-mon # scope flow-timeout default
UCS-A /eth-flow-mon/flow-timeout # set cache-timeout-active 1800
UCS-A /eth-flow-mon/flow-timeout* # set cache-timeout-inactive 20
UCS-A /eth-flow-mon/flow-timeout* # commit-buffer
UCS-A /eth-flow-mon/flow-timeout #
```

vNIC へのフロー モニタ セッションの関連付け

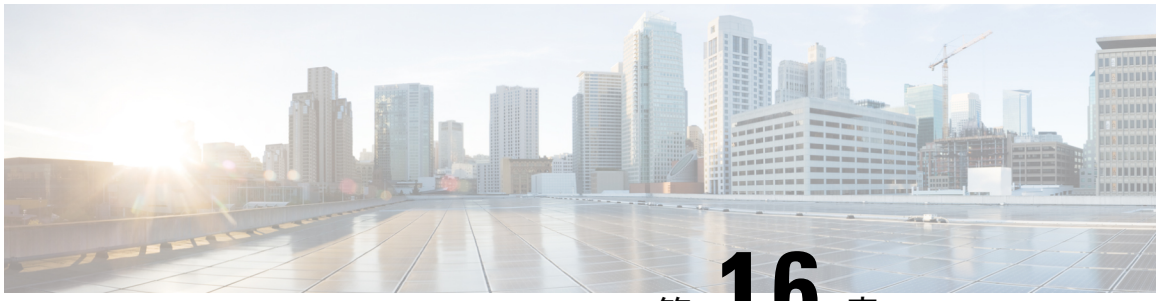
手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	指定した vNIC で組織サービス プロファイル モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **enter flow-mon-src** *flow-monitor-session-name*	vNIC にフロー モニタ セッションを関連付けます。
ステップ 5	UCS-A /org/service-profile/vnic # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、vNIC eth5 にフロー モニタ セッション s1 を関連付ける例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # scope vnic eth5
UCS-A /org/service-profile/vnic # enter flow-mon-src s1
UCS-A /org/service-profile/vnic # commit-buffer
```



第 16 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 （173 ページ）
- 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 （176 ページ）
- トラフィック モニタリング セッション間の選択 （178 ページ）
- SPAN のトラフィック モニタリング （179 ページ）
- ERSPAN のトラフィック モニタリング （182 ページ）
- ERSPAN の切り捨て （187 ページ）
- 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 （191 ページ）
- トラフィック モニタリング セッションのアクティブ化 （202 ページ）
- トラフィック モニタリング セッションの削除 （203 ページ）
- Cisco UCS Mini の SPAN に関する制約事項 （204 ページ）

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。

ただし、このトラフィックの監視は 1 つのスイッチに限定されます。SPAN はスイッチ間でトラフィックを送信できますが、このトラフィックをルーティングすることはできません。この問題を解決するために、Cisco UCS Manager 4.3(4a)から ERSPAN（カプセル化リモート スイッチド ポート アナライザ）のサポートが提供されています。

ERSPAN は GRE カプセル化を使用します。これにより、L3 ネットワークの送信元から宛先に SPAN トラフィックをルーティングできます。

ERSPANは、IPネットワークでミラーリングされたトラフィックを転送するために使用されます。発信元インターフェイスは、L3 ネットワーク上でパケットを転送するために構成された送信元 IP アドレスを持つ各ファブリック インターコネクト上に作成されます。ファブリックごとに一意の IP アドレスが VLAN 情報とともにキャプチャされます。

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 6536 ファブリック インターコネクト、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、および 6536 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 • イーサネット ポート チャネル • VLAN • サービス プロファイル vNIC • サービス プロファイル vHBA • FCoE ポート • ポート チャネル • ユニファイド アップリンク ポート • 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 6500、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 6500、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 6500、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。

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。

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 • FCポートチャネル • アップリンク ファイバ チャネル ポート • SAN ポート チャネル • VSAN • サービス プロファイル vHBA • 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 • 未構成のイーサネット ポート（Cisco UCS 6536、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。

Cisco UCS Manager 4.3(4a)からは、送信または受信モニタリング セッション、またはその両方が 1 つのセッションのみと見なされます。

4つのアクティブセッション：任意のトラフィック方向のイーサネットおよびファイバチャネル トラフィック モニタリング セッションが含まれます。

トラフィック モニタリング セッションの制限は、各ファブリック インターコネクトごとに制限されます。最大16個のセッションを構成できます。ただし、イーサネットまたはファブリック インターコネクトの最大 4 つのモニタリング セッションをアクティブにできます。

（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 ファブリック インターコネクト 9108 100G、Cisco UCS 6500、 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 6500、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 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。

ERSPAN の場合

ERSPAN は次をサポートしています。

- 4G (HD) および 5G ファブリック インターコネクトにのみ適用されます。
- 送信元セッション モニタリングのみ。
- イーサネットと FC ポートは送信元インターフェイスです。
- 両方のファブリック インターコネクトで ERSPAN を設定できます。
- 発信元インターフェイスを作成する前に、VLAN を定義する必要があります。
- IPv4 配信/転送ヘッダーのみサポートされます。

- タイプ II ERSPAN ヘッダーのみサポートします。

ERSPAN 機能は、次をサポートしていません。

- 宛先セッション モニタリング。
- 送信元セッション ACL。
- 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。

制限事項

- ポートチャネルまたは物理ポートで受信した入力パケットは、宛先にスパンされません。これは、アップリンクが1つだけで、セッションの送信元とセッションの出力が同じ場合に発生します。
- 2 つのメンバーが 1 つのアップリンクであるポートチャネルがある場合、パケットはアナライザに 2 回スパンされます。
- モニタリング送信元として複数の VLAN を設定する場合は、システムで更新される時間がかかる可能性があるため、各 VLAN のトラフィック モニタリング送信元を個別にモニタすることを推奨します。これは、より多くの VLAN を持つセットアップがあり、モニタリング送信元として VLAN を構成する場合に発生します。

トラフィック モニタリング セッション間の選択

Cisco UCS Manager 4.3(4a)から、SPAN または ERSPAN トラフィック モニタリング セッションを選択できるようになりました。

制限事項

（注） 既存の SPAN 制限は、ERSPAN にも適用されます。

次に、SPAN または ERSPAN トラフィック モニタリング セッションを選択する場合の制限を示します。

- セッション移行はサポートされていません。セッションタイプを SPAN から ERSPAN に、またはその逆に、作成後に変更することはできません。
- ERSPAN は、元のインターフェイスまたは VLAN 構成を NetFlow と共有しません。

  NetFlow と ERSPAN の両方に同じ送信元 VLAN を使用することはできません。

（注） IP アドレスを Netflow と共有することもできません。

- ERSPANセッションでは、制御パケットのスパンキャプチャをイネーブルにできません。

SPAN 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 セッションの作成

（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 セッションを作成する方法について説明します。ファイバ チャネル トラフィックのモニタリング セッションを作成するには、次の変更が必要になります。

- ステップ 1 で、 **scope fc-traffic-mon** コマンドを **scope eth-traffic-mon** コマンドの代わりに入力します。
- ステップ 3 で、 **create fc-mon-session** コマンドを **create eth-mon-session** コマンドの代わりに入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-traffic-mon**	イーサネット トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /eth-traffic-mon/fabric # **create eth-mon-session** *session-name*	指定した名前で、トラフィック モニタリング セッションを作成します。
ステップ 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session # **create dest-interface** *slot-num port-num*	トラフィック モニタリング セッションのモニタリング先とするために指定したスロットとポート番号でインターフェイスを設定します。そのインターフェイスでコマンド モードを開始します。
ステップ 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **set speed***admin-speed*	モニタされるポート チャネルのデータ転送速度 を設定します。ここに表示される値は次のとおりです。 • 1gbps：1 Gbps • 10gbps：10 Gbps • 20gbps：20 Gbps

	コマンドまたはアクション	目的
		• 40gbps：40 Gbps
ステップ 6	UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、イーサネット トラフィック モニタリング セッションを作成してトラフィックをスロット 2、ポート 12 の宛先ポートにコピーおよび転送し、管理速度を 20 Gbps に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # create eth-mon-session EthMonitor33
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # create dest-interface 2 12
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface* # set speed 20gbps
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface #
```

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。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-traffic-mon**	ファイバ チャネル トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /fc-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル トラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /fc-traffic-mon/fabric # **create fc-mon-session** *session-name*	指定した名前で、ファイバ チャネル トラフィック モニタリング セッションを作成します。
ステップ 4	UCS-A /fc-traffic-mon/fabric/fc-mon-session # **create dest-interface** *slot-num port-num*	ファイバ チャネル トラフィック モニタリング セッションのモニタリング先ス

	コマンドまたはアクション	目的
		ロットおよびポートのコマンド モードを作成してそのモードを開始します。
ステップ 5	UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **set speed***admin-speed*	モニタされるポート チャネルのデータ転送速度 を設定します。ここに表示される値は次のとおりです。 • 1gbps：1 Gbps • 2gbps：2 Gbps • 4gbps：4 Gbps • 8gbps：8 Gbps • 自動：Cisco UCSがデータ転送速度を決定します。
ステップ 6	UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファイバ チャネル トラフィック モニタリング セッションを作成してトラフィックをスロット 1、ポート 10 の宛先ポートにコピーおよび転送し、管理速度を 8 Gbps に設定し、トランザクションをコミットします。

```
UCS-A# scope fc-traffic-mon
UCS-A /fc-traffic-mon # scope fabric a
UCS-A /fc-traffic-mon/fabric # create fc-mon-session FCMonitor
UCS-A /fc-traffic-mon/fabric/fc-mon-session* # create dest-interface 1 10
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface* # set speed 8gbps
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface* # commit-buffer
UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface #
```

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。

ERSPAN のトラフィック モニタリング

発信元インターフェイスの設定

送信元 IP アドレスが設定された各ファブリック インターコネクト上で、パケットを L3 ネットワーク上に転送するための発信元インターフェイスを作成できます。グローバル VLAN と、VLAN 情報とともにキャプチャされるファブリック インターコネクトごとに一意の IP アドレスを設定する必要があります。ERSPAN は、SVI インターフェイスでこれらのアドレスを送信元 IP アドレスとして使用します。

アップリンク スイッチは、トラフィックをファブリック インターコネクトから L3 ネットワーク経由でトラフィック アナライザに転送するように設定する必要があります。ファブリック インターコネクト SVI インターフェイスからトラフィックを受信します。

（注） この手順では、イーサネット トラフィック モニタリング セッションから発信元のインターフェイスを構成する方法について説明します。ファイバ チャネル トラフィック モニタリング セッションから発信元のインターフェイスを構成するには、ステップ 2 で **[LAN]** タブの代わりに **[SAN]** タブを選択します。

（注） 許可される発信元インターフェイスは1つのみです。

始める前に

VLAN が設定されていることを確認します。

VLAN インターフェイス、またはスイッチ仮想インターフェイス（SVI）、は、デバイス上の VLAN を同じデバイス上のレイヤ 3 ルータ エンジンに接続する仮想ルーテッド インターフェイスです。ERSPAN 構成では、接続されたファブリック インターコネクト デバイスの発信元インターフェイスに使用される VLAN ID と一致する VLAN ID を持つアップリンク スイッチに SVI があることが想定されます。アップリンク スイッチで SVI 用に設定された IP アドレスは、リモート モニタリングの発信元インターフェイス設定のデフォルト ゲートウェイ アドレスとして使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope remote-traffic-mon**	リモート トラフィック モニタリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /remote-traffic-mon # **create vlan** <*vlan name*>	VLANを作成し、VLAN名を指定して、リモート トラフィック モニタリング モードを開始します。
ステップ 3	UCS-A /remote-traffic-mon/vlan* # **create origin** {**a** | **b**}	指定したファブリック インターコネクト（AまたはB）の発信元インターフェイスを作成します。
ステップ 4	UCS-A /remote-traffic-mon/vlan/origin* # **set addr** <*IP address*> **subnet** <*subnet-mask*> **def-gw** < *def-gw gateway-ip*>	IP アドレス、サブネット アドレス、およびデフォルト ゲートウェイ アドレスを設定します。
ステップ 5	UCS-A /remote-traffic-mon/vlan/origin* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、発信元のインターフェイスを作成し、トランザクションをコミットする方法を示しています。

```
UCS-A  /eth-uplink # scope remote-traffic-mon
UCS-A /remote-traffic-mon # create vlan vlan102
UCS-A /remote-traffic-mon/vlan* # create origin a
UCS-A /remote-traffic-mon/vlan/origin* # set addr 10.10.10.23 subnet 255.255.255.0 def-gw
 10.10.10.2
UCS-A /remote-traffic-mon/vlan/origin* # commit-buffer
UCS-A /remote-traffic-mon/vlan/origin* # up
UCS-A /remote-traffic-mon/vlan # show origin detail

Origin IP:
    Fabric Id: A
    IP address: 10.10.10.23
    Subnet mask: 255.255.255.0
    Default Gateway: 10.10.10.2

    Fabric Id: B
    IP address: 10.10.10.24
    Subnet mask: 255.255.255.0
    Default Gateway: 10.10.10.2

UCS-A /remote-traffic-mon/vlan #
```

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

（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 セッションを作成する方法について説明します。ファイバ チャネル トラフィックのモニタリング セッションを作成するには、次の変更が必要になります。

- ステップ 2 で、 **scope fc-traffic-mon** コマンドを **scope eth-traffic-mon** コマンドの代わりに入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-traffic-mon**	イーサネット トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /eth-traffic-mon/fabric # **create eth-mon-session** <*session name*>	イーサネット モニタリング セッションを作成し、セッション名を指定して、イーサネット トラフィック モニタリング モードを開始します。
ステップ 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session* # **set session-type** <*session-type*> *{span-local|erspan-source}*	セッションタイプを作成します。デフォルトは **span-local**です。
ステップ 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session* # **create remote-config**	イーサネット リモート構成モードを作成します。
ステップ 6	UCS-A /eth-traffic-mon/fabric/eth-mon-session* # **set destination-ip <destination ip>**	宛先 IP アドレスを作成します。
ステップ 7	UCS-A /eth-traffic-mon/fabric/eth-mon-session* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、イーサネット トラフィック モニタリング セッションを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # create eth-mon-session Test2
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # set session-type erspan-source
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # create remote-config
UCS-A /eth-traffic-mon/fabric/eth-mon-session/fc* # set destination-ip 10.193.167.34
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote # show detail

Remote Config:
    ERSPAN ID: 512
    Destination IP: 10.193.167.34
    IP TTL: 64
    IP DSCP: 0
    MTU: 512
    Truncation enabled: Yes
    Fwd drops ingress: Yes
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote #

UCS-A /eth-traffic-mon/fabric # show eth-mon-session

Ethernet Traffic Monitoring Session:

Name       Admin State    Oper State   Oper State Reason Config Success Session type
---------- -------------- ------------ ----------------- -------------- --------
----
A1         Disabled       Down         Session Admin Shut Yes            Erspan Source
demo       Disabled       Down         Session Admin Shut Yes            Erspan Source
```

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。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-traffic-mon**	ファイバ チャネル トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /fc-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル トラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /fc-traffic-mon/fabric # **create fc-mon-session** *<session name>*	ファイバ チャネル モニタリング セッションを作成し、セッション名を指定して、ファイバ チャネル トラフィック モニタリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /fc-traffic-mon/fabric/fc-mon-session* # **set session-type** *<session-type> {span-local|erspan-source}*	セッション タイプを作成します。デフォルトは **span-local**です。
ステップ 5	UCS-A /fc-traffic-mon/fabric/fc-mon-session* # **create remote-config**	ファイバ チャネル リモート構成モードを作成します。
ステップ 6	UCS-A /fc-traffic-mon/fabric/fc-mon-session* # **set destination-ip <destination ip>**	宛先 IP アドレスを作成します。
ステップ 7	UCS-A /fc-traffic-mon/fabric/fc-mon-session* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファイバ チャネル トラフィック モニタリング セッションを作成する方法を示し、トランザクションをコミットする方法を示しています。

```
UCS-A# scope fc-traffic-mon
UCS-A /fc-traffic-mon # scope fabric a
UCS-A /fc-traffic-mon/fabric # create fc-mon-session Test2
UCS-A /fc-traffic-mon/fabric/fc-mon-session* # set session-type
  erspan-source  Erspan Source
  span-local     Span Local

UCS-A /fc-traffic-mon/fabric/fc-mon-session* # set session-type erspan-source
UCS-A /fc-traffic-mon/fabric/fc-mon-session* # create fc-config
UCS-A /fc-traffic-mon/fabric/fc-mon-session/fc* # set destination-ip 10.193.167.34
UCS-A /fc-traffic-mon/fabric/fc-mon-session/fc* # commit-buffer
UCS-A /fc-traffic-mon/fabric/fc-mon-session/fc # show detail

FC Config:
    ERSPAN ID: 512
    Destination IP: 10.193.167.34
    IP TTL: 64
    IP DSCP: 0
    MTU: 512
    Truncation enabled: Yes
    Fwd drops ingress: Yes
UCS-A /fc-traffic-mon/fabric/fc-mon-session/fc #

UCS-A /fc-traffic-mon/fabric # show fc-mon-session

Fibre Channel Traffic Monitoring Session:

Name       Admin State    Oper State   Oper State Reason Config Success Session type
---------- -------------- ------------ ----------------- -------------- --------
----
A1         Disabled       Down         Session Admin Shut Yes            Erspan Source
demo       Disabled       Down         Session Admin Shut Yes            Erspan Source
```

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。

ERSPAN の切り捨て

Cisco UCS Manager 4.3(4a) 以降では、最大伝送ユニット（MTU）のサイズに基づいて各 ERSPAN セッションの送信元パケットの切り捨てを設定できます。切り捨てにより、モニタするパケットのサイズを減らすことで、ERSPAN の帯域幅を効果的に軽減できます。設定された MTU サイズよりも大きいERSPANパケットはすべて、設定されたサイズに切り捨てられます。ERSPAN では、ERSPANヘッダータイプに応じて、切り捨てられたパケットに54ー166バイトのERSPAN ヘッダーが追加されます。たとえば、MTU を 300 バイトに設定すると、ERSPAN ヘッダー タイプの設定に応じて、パケットは 354 ー 466 バイトの ERSPAN ヘッダーサイズで複製されます。

ERSPAN切り捨てはデフォルトでは無効です。切り捨てを使用するには、個々のERSPANセッションで有効にしておく必要があります。

ERSPAN 切り捨ての設定

切り捨ては、ERSPAN 送信元セッションに対してのみ設定できます。

（注） デフォルトでは、ERSPAN セッションはパケット全体（9216 ジャンボ パケット）を転送します。

次の手順では、MTU サイズを切り捨てる方法について説明します。

始める前に

ERSPAN のパケット切り捨てを有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-traffic-mon**	イーサネット トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-traffic-mon/fabric # **create eth-mon-session** <*session name*>	イーサネットモニタリングセッションを作成し、セッション名を指定して、イーサネットトラフィックモニタリング モードを開始します。
ステップ 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session* # **set session-type** <*session type*>	イーサネットモニタリングセッションを作成し、セッション名を指定して、イーサネットトラフィックモニタリング モードを開始します。 デフォルトでは、 **SPAN ローカル**です。サポートされているモニタリングセッションのタイプは**SPAN Local**および **ERSPAN 送信元**です。
ステップ 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session* # **create remote-config**	イーサネットリモート構成モードを作成します。
ステップ 6	UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **set/unset packet-truncation** {**Yes**| **No**}	指定されたイーサネットモニタリングセッションのパケット切り捨てを作成します。
ステップ 7	UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **set mtu** <*size*>	MTUの切り捨てサイズを設定します。設定された MTU サイズよりも大きい ERSPAN パケットはすべて、設定されたサイズに切り捨てられます。 （注） MTU サイズの範囲は 64 ～ 1518 バイトです。許可される最大サイズは 1518MBです。 （注） MTU サイズを変更するには、パケットの切り捨てを有効にする必要があります。
ステップ 8	UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **Set destination-ip** <*destination-ip*>	宛先 IP アドレスを設定します
ステップ 9	(Optional) UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **set erspan-id** <*erspan-id*>	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。

	コマンドまたはアクション	目的
ステップ 10	(Optional) UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **set ip-ttl** *<ttl value>*	ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。
ステップ 11	(Optional) UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **set ip-dscp** *<dscp value>*	ERSPAN トラフィックのパケットの DiffServ コードポイント（DSCP）値を設定します。範囲は 0 ～ 63 です。
ステップ 12	UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、パケットの切り捨てを有効にして、パケット サイズを設定することを許可します。

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # create eth-mon-session TR
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # set session-type erspan-source
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # create remote-config
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set packet-truncation yes
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set mtu 256
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set destination-ip
10.193.167.34
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set erspan-id test1
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set ip-ttl 3
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set ip-dscp 2
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config # show detail

Ether Remote Config:
    ERSPAN ID: 0
    Destination IP: 10.193.167.34
    IP TTL: 64
    IP DSCP: 0
    MTU: 256
    Truncation enabled: Yes
    Fwd drops ingress: No

UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config #
```

ERSPAN 切り捨ての表示または変更

切り捨ては、ERSPAN 送信元セッションに対してのみ設定できます。

（注） デフォルトでは、ERSPAN セッションはパケット全体（9216 個のジャンボ パケット）を転送します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-traffic-mon**	イーサネット トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /eth-traffic-mon/fabric # **scope eth-mon-session** <*session name*>	イーサネット モニタリング セッションを開始し、セッション名を指定して、イーサネット トラフィック モニタリング モードを開始します。
ステップ 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session* # **scope remote-config**	イーサネット リモート構成モードを開始します。
ステップ 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **set packet-truncation** {**Yes**| **No**}	指定されたイーサネット モニタリング セッションのパケットの切り捨てを作成します。
ステップ 6	UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **set mtu** <*size*>	MTU の切り捨てサイズを設定します。設定された MTU サイズよりも大きい ERSPAN パケットはすべて、設定されたサイズに切り捨てられます。 （注） MTU サイズの範囲は 64 ～ 1518 バイトです。許可される最大サイズは1518MBです。
ステップ 7	UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、パケットの切り捨てを有効にして、パケット サイズを設定することを許可します。

```
UCS-A# scope eth-traffic-mon Monitor33
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # scope eth-mon-session
UCS-A /eth-traffic-mon/fabric/eth-mon-session/ # scope remote-config remote3
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set packet-truncation yes
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # set mtu 256
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config* # commit-buffer
```

```
UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config # show detail

Ether Remote Config:
    ERSPAN ID: 0
    Destination IP: 10.193.167.34
    IP TTL: 64
    IP DSCP: 0
    MTU: 256
    Truncation enabled: Yes
    Fwd drops ingress: No

UCS-A /eth-traffic-mon/fabric/eth-mon-session/remote-config #
```

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

モニタリング セッションへのアップリンク ソース ポートの追加

（注） この手順は、トラフィック モニタリング セッションのソースとしてイーサネット アップリンク ポートを追加する方法について説明します。ソースとしてファイバ チャネル アップリンク ポートを追加するには、ステップ 1 で **scope eth-uplink** コマンドの代わりに **scope fc-uplink** コマンドを入力します。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのアップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope interface** *slot-num port-num*	指定されたアップリンク ポートのインターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/interface # **create mon-src** *session-name*	指定されたモニタリング セッションのソースとしてアップリンク ポートを追加します。

	コマンドまたはアクション	目的
ステップ 5	（任意） UCS-A /eth-uplink/fabric/interface/mon-src # **set direction** {**both** | **receive** | **transmit**}	モニタするトラフィックの方向を指定します。 （注） 方向を選択しない場合、デフォルトの方向は Rx です。
ステップ 6	UCS-A /eth-uplink/fabric/interface/mon-src # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、モニタリング セッションのソースとしてファブリック A のスロット 2 のイーサネット アップリンク ポート 3 への入力トラフィックを追加し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope interface 2 3
UCS-A /eth-uplink/fabric/interface # create mon-src Monitor23
UCS-A /eth-uplink/fabric/interface/mon-src* # set direction receive
UCS-A /eth-uplink/fabric/interface/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/interface/mon-src #
```

次のタスク

トラフィック モニタリング セッションにはさらにソースを追加できます。

モニタリング セッションへの VLAN または VSAN 発信元の追加

（注） この手順は、トラフィック モニタリング セッションのソースとして VLAN を追加する方法について説明します。ソースとして VSAN を追加するには、次の変更が必要です。

- ステップ 1 で、 **scope fc-uplink** コマンドを **scope eth-uplink** コマンドの代わりに入力します。
- ステップ 3 で、 **create vsan** コマンドを **create vlan** コマンドの代わりに入力します。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのアップリンク ファブリック モードを開始します。 （注） ローカル VLAN をソースとして追加する場合、この手順は必須です。ソースとしてグローバルな VLAN を追加するには、この手順を省略します。
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *VLAN 名* *VLAN ID*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、アップリンク VLAN モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **create mon-src** *session-name*	指定されたモニタリング セッションのソースとして VLAN を追加します。
ステップ 5	UCS-A /eth-uplink/fabric/vlan/mon-src # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネット モニタリング セッションのソースとしてローカル VLAN を追加し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan vlan23 23
UCS-A /eth-uplink/fabric/vlan # create mon-src Monitor23
UCS-A /eth-uplink/fabric/vlan/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/vlan/mon-src #
```

次のタスク

トラフィック モニタリング セッションにはさらにソースを追加できます。

モニタリング セッションへのストレージ ポート送信元の追加

（注） この手順では、ファイバチャネル トラフィックのモニタリングセッションのソースとしてファイバチャネルストレージポートを追加する方法について説明します。イーサネットトラフィック モニタリング セッションのソースとして FCoE ストレージ ポートを追加するには、ステップ 3 で **scope interface fc** コマンドの代わりに **scope interface fcoe** コマンドを入力します。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ ポートのコマンド モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル ストレージ ポート ファブリック モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **scope interface fc** *slot-num* ポート番号	ファイバチャネル ストレージ ポート インターフェイスを入力し、インターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /fc-storage/fabric/fc # **create mon-src** セッション名	指定されたモニタリング セッションのソースとしてストレージ ポートを追加します。
ステップ 5	UCS-A /fc-storage/fabric/fc/mon-src # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファイバ チャネル モニタリング セッションのソースとしてスロット 2 のポート 3 にあるファイバ チャネル ストレージ ポートを追加し、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric # scope interface fc 2 3
UCS-A /fc-storage/fabric/fc* # create mon-src Monitor23
UCS-A /fc-storage/fabric/fc/mon-src* # commit-buffer
UCS-A /fc-storage/fabric/fc/mon-src #
```

次のタスク

トラフィック モニタリング セッションにはさらにソースを追加できます。

モニタリング セッションへの vNIC 送信元の追加

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **scope service-profile** <*profile-name*>	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic** <*vnic-name*>	指定された vNIC をサービス プロファイルに関連付けます。
ステップ 4	UCS-A /org/service-profile/vnic # **create mon-src** <*session-name*>	指定されたモニタリング セッションの送信元として組織のサービス プロファイルを追加します。
ステップ 5	(Optional) UCS-A /org/service-profile/vnic/mon-src* # **set direction** { **receive** | **transmit** | **both**	モニタするトラフィックの方向を指定します。 （注） vNIC は受信方向でのみモニターできます。
ステップ 6	UCS-A /org/service-profile/vnic/mon-src* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネット トラフィック モニタリング セッションの送信元として vNIC を追加し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # scope service-profile WDC
UCS-A /org/service-profile # scope vnic eth0
UCS-A /org/service-profile/vnic # create mon-src TC-A
UCS-A /org/service-profile/vnic/mon-src* # set direction receive
UCS-A /org/service-profile/vnic/mon-src* # commit-buffer
UCS-A /org/service-profile/vnic/mon-src #
```

モニタリング セッションへのポート チャネル送信元の追加

（注） この手順は、トラフィック モニタリング セッションの送信元としてイーサネット ポート チャネルを追加する方法について説明します。送信元としてファイバ チャネル ポート チャネルを追加するには、ステップ 1 で **scope eth-uplink** コマンドの代わりに **scope fc-uplink** コマンドを入力します。

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **show port-channel**	ポート チャネルの詳細を表示します。
ステップ 4	UCS-A /eth-uplink/fabric # **scope port-channel** <*port-number*>	イーサネット アップリンク ポート チャネル構成モードを開始します。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel # **create aggr-interface member-port mon-src**	集約インターフェイスを作成します。
ステップ 6	UCS-A /eth-uplink/fabric/port-channel* # **create m member-port mon-src**	指定されたモニタリング セッションの送信元としてアップリンク ポートを追加します。
ステップ 7	UCS-A /eth-uplink/fabric/port-channel* # **create mon-src** <*session-name*>	指定されたモニタリング セッションの送信元にセッション名と共にアップリンク ポートを追加します。
ステップ 8	UCS-A /eth-uplink/fabric/port-channel* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、イーサネット モニタリング セッションの送信元としてポート チャネルを追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # show port-channel
UCS-A /eth-uplink/fabric/port-channel # scope port-channel 11
UCS-A /eth-uplink/fabric/port-channel* # create aggr-interface  member-port     mon-src
UCS-A /eth-uplink/fabric/port-channel* # create m member-port  mon-src
UCS-A /eth-uplink/fabric/port-channel* # create mon-src TC-A
UCS-A /eth-uplink/fabric/port-channel/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel/mon-src #
```

モニタリング セッションへのブレークアウト インターフェイス送信元の追加

（注） この手順は、トラフィック モニタリング セッションのソースとしてイーサネット アップリンク ポートを追加する方法について説明します。ソースとしてファイバ チャネル ブレークアウト インターフェイスを追加するには、ステップ 1 で **scope eth-uplink** コマンドの代わりに **scope fc-uplink** コマンドを入力します。

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric #	ファブリック接続モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric # **scope aggr-interface** *<slot-id>* *<port-id>*	インターフェイス構成モードを集約します。
ステップ 5	UCS-A /eth-uplink/fabric/aggr-interface # **scope br-interface** *<id>*	ブリッジ インターフェイス構成モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /eth-uplink/fabric/aggr-interface/br-interface # **create mon-src** *<session name>*	指定されたモニタリング セッションのソースとしてブレークアウト インターフェイス サービスを追加します。
ステップ 7	UCS-A /eth-uplink/fabric/aggr-interface/br-interface* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、イーサネット トラフィック モニタリング セッションのソースとしてブレークアウト インターフェイスを追加し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope aggr-interface 1 4
UCS-A /eth-uplink/fabric/aggr-interface # scope br-interface 1
UCS-A /eth-uplink/fabric/aggr-interface/br-interface # create mon-src TC-A
UCS-A /eth-uplink/fabric/aggr-interface/br-interface/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/aggr-interface/br-interface/mon-src #
```

モニタリング セッションへの FCoE ポート チャネル送信元の追加

（注） この手順は、トラフィック モニタリング セッションの送信元として FCoE ポート チャネルの追加について説明します。送信元としてファイバ チャネル FCoE ポート チャネルを追加するには、ステップ 1 で **scope eth-uplink** コマンドの代わりに **scope fc-uplink** コマンドを入力します。

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/fabric # **scope fcoe-port-channel** <*port-id*>	アップリンク FCoE ポート チャネル構成モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/fcoe-port-channel # **create mon-src** <*session-name*>	指定されたモニタリング セッションに送信元として FCoE ポート チャネル サービス プロファイルを追加します。
ステップ 5	UCS-A /eth-uplink/fabric/fcoe-port-channel* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネット トラフィック モニタリング セッションの送信元として FCoE ポート チャネルを追加し、トランザクションをコミットする方法を示しています。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope fcoe-port-channel 11
UCS-A /eth-uplink/fabric/fcoe-port-channel # create mon-src TC-A
UCS-A /eth-uplink/fabric/fcoe-port-channel/mon-src* # commit-buffer
UCS-A /eth-uplink/fabric/fcoe-port-channel/mon-src #
```

モニタリング セッションへの vHBA 発信元の追加

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **scope service-profile** <*profile name*>	指定されたサービス プロファイル テンプレートを作成し、組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vhba** <*vhba-name*>	指定された vHBA をサービス プロファイルに関連付けます。
ステップ 4	UCS-A /org/service-profile/vnic # **create mon-src** <*session name*>	指定されたモニタリング セッションの送信元として vHBA サービス プロファイルを追加します。

	コマンドまたはアクション	目的
ステップ 5	(Optional) UCS-A /org/service-profile/vnic/mon-src* # **set direction** { **receive** | **transmit** | **both**	モニタするトラフィックの方向を指定します。 （注） vHBA は、受信方向でのみモニターできます。
ステップ 6	UCS-A /org/service-profile/vnic/mon-src* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イーサネット トラフィック モニタリング セッションの送信元として vHBA を追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile WDC
UCS-A /org/service-profile # scope vhba  vhba0
UCS-A /org/service-profile/vhba # create mon-src TC-A
UCS-A /org/service-profile/vhba/mon-src* # set direction receive
UCS-A /org/service-profile/vhba/mon-src* # commit-buffer
UCS-A /org/service-profile/vhba/mon-src #
```

モニタリング セッションへの VSAN 発信元（ファイバ チャネル）の追加

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope vsan** <*vsan-id*>	VSAN 構成モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /fc-uplink/fabric/vsan # **create mon-src** *<session name>*	指定されたモニタリング セッションの送信元として VSAN サービス プロファイルを追加します。
ステップ 5	UCS-A /fc-uplink/fabric/vsan* **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファイバ チャネル トラフィックモニタリング セッションの送信元として VSAN を追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope vsan 100
UCS-A /fc-uplink/fabric/vsan # create mon-src TC-A
UCS-A /fc-uplink/fabric/vsan/mon-src* # commit-buffer
UCS-A /fc-uplink/fabric/vsan/mon-src #
```

モニタリング セッションへのソースとしてのポート チャネル（ファイバ チャネル）の追加

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** *<port-channel id>*	アップリンク ポート チャネル構成モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **create mon-src** *<session name>*	指定されたモニタリング セッションに送信元として、ポート チャネル サービス プロファイルを追加します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /fc-uplink/fabric/port-channel* # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファイバ チャネル トラフィック モニタリング セッションに送信元としてポート チャネルを追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric/port-channel # create mon-src TC-A
UCS-A /fc-uplink/fabric/port-channel/mon-arc* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel/mon-arc
```

トラフィック モニタリング セッションのアクティブ化

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化する方法について説明します。ファイバチャネル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には、次の変更が必要になります。

- ステップ 1 で、**scope fc-traffic-mon** コマンドを **scope eth-traffic-mon** コマンドの代わりに入力します。
- ステップ 3 で、**scope fc-mon-session** コマンドを **scope eth-mon-session** コマンドの代わりに入力します。

始める前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-traffic-mon**	イーサネット トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /eth-traffic-mon/fabric # **scope eth-mon-session** <*session-name*>	指定した名前のトラフィック モニタリング セッションのコマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session # **disable** | **enable**	トラフィックのモニタリング セッションをイネーブルまたはディセーブルにします。
ステップ 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、イーサネット トラフィック モニタリング セッションをアクティブにし、トランザクションをコミットします。

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # scope eth-mon-session Monitor33
UCS-A /eth-traffic-mon/fabric/eth-mon-session # enable
UCS-A /eth-traffic-mon/fabric/eth-mon-session* # commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session # show

Ether Traffic Monitoring Session:
    Name       Admin State       Oper State   Oper State Reason
    ---------- ----------------- ------------ -----------------
    Monitor33  Enabled           Up           Active

UCS-A /eth-traffic-mon/fabric/eth-mon-session #
```

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 トラフィックのモニタリング セッションを削除するには、次の変更が必要です。

- ステップ 1 で、 **scope fc-traffic-mon** コマンドを **scope eth-traffic-mon** コマンドの代わりに入力します。
- ステップ 3 で、 **delete fc-mon-session** コマンドを **delete eth-mon-session** コマンドの代わりに入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-traffic-mon**	イーサネット トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックのトラフィック モニタリング コマンド モードを開始します。
ステップ 3	UCS-A /eth-traffic-mon/fabric # **delete eth-mon-session** *session-name*	指定した名前のトラフィック モニタリング セッションを削除します。
ステップ 4	UCS-A /eth-traffic-mon/fabric # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、イーサネット トラフィックのモニタリング セッションを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-traffic-mon
UCS-A /eth-traffic-mon # scope fabric a
UCS-A /eth-traffic-mon/fabric # delete eth-mon-session Monitor33
UCS-A /eth-traffic-mon/fabric* # commit-buffer
UCS-A /eth-traffic-mon/fabric #
```

Cisco UCS Mini の SPAN に関する制約事項

SPAN機能を設定する際は、次のガイドラインおよび制約事項を考慮してください。 Cisco UCS Mini

- FC ポートは SPAN 宛先としてはサポートされていません。
- VSAN は SPAN 送信元としてはサポートされません。
- FC アップリンク ポートは SPAN 送信元としてはサポートされません。

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。