# Cisco UCS Manager System Monitoring Guide Using the CLI, Release 4.2

**First Published:** 2021-06-25

**Last Modified:** 2022-02-15

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

# はじめに



## 対象読者

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

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

## 表記法

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

| テキストのタイプ | 説明 |
|---|---|
| システム出力 | システムが表示するターミナルセッションおよび情報は、courierフォントで示しています。 |
| CLI コマンド | CLI コマンドのキーワードは、**this font**で示しています。<br>CLI コマンド内の変数は、このフォント で示しています。 |
| [ ] | 角カッコの中の要素は、省略可能です。 |
| {x \| y \| z} | どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。 |
| [x \| y \| z] | どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。 |
| string | 引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。 |
| < > | パスワードのように出力されない文字は、山カッコで囲んで示しています。 |
| [ ] | システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。 |
| !、# | コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。 |

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

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

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

警告 安全上の重要事項

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

これらの注意事項を保管しておいてください。

# Cisco UCS の関連資料

### ドキュメント ロードマップ

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

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

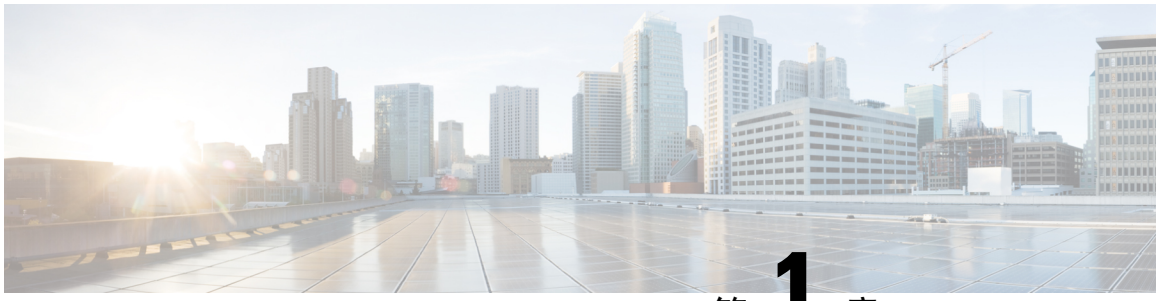
管理用の UCS Manager に統合されたラック サーバでサポートされるファームウェアと UCS Manager のバージョンについては、『Release Bundle Contents for Cisco UCS Software』[英語] を参照してください。

### その他のマニュアル リソース

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

# マニュアルに関するフィードバック

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



第 1 章

# このリリースの新規情報および変更情報



# New and Changed Information for This Release

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

***Table 1: New Features and Changed Behavior in Cisco UCS Manager, Release 4.2(1k)***

| Feature | Description | Where Documented |
|---|---|---|
| Support for Cisco UCS C225 M6 サーバs | Cisco UCS Manager now supports some monitoring functions with the Cisco UCS C225 M6サーバ. | -- |

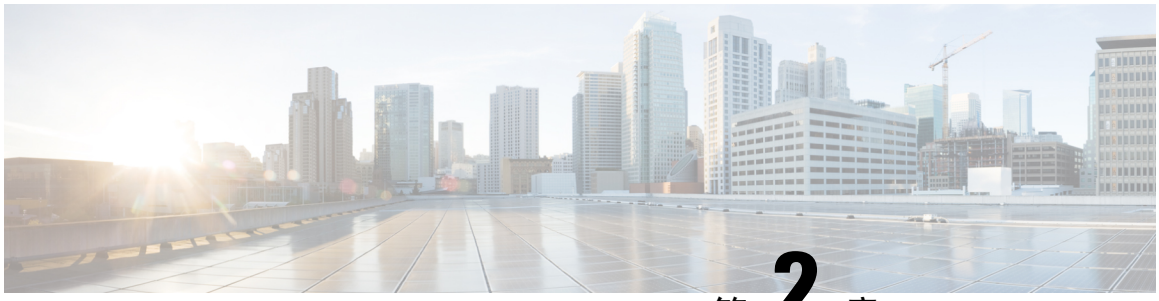
***Table 2: New Features and Changed Behavior in Cisco UCS Manager, Release 4.2(1i)***

| Feature | Description | Where Documented |
|---|---|---|
| Support for Cisco UCS C245 M6 サーバs | Cisco UCS Manager now supports some monitoring functions with the Cisco UCS C245 M6サーバ. | -- |

***Table 3: New Features and Changed Behavior in Cisco UCS Manager, Release 4.2(1d)***

| Feature | Description | Where Documented |
|---|---|---|
| Security Protocol and Data Model (SPDM) monitoring | Cisco UCS Manager now allows you to configure security alert settings for removable devices through a SPDM policy. Three alert levels of monitoring are available. | SPDM Security, on page 81 |

| Feature | Description | Where Documented |
| --- | --- | --- |
| Support for Cisco UCS C220 M6 サーバs and Cisco UCS C240 M6 サーバs | Cisco UCS Manager now supports Cisco UCS Cisco UCS C220 M6 サーバ and Cisco UCS C240 M6 サーバ | -- |



第 2 章

# システム モニタリングの概要



# システム モニタリングの概要

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

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

- マイナーの障害および警告には緊急のアクションは必要ないため、クリティカルまたはメジャーの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

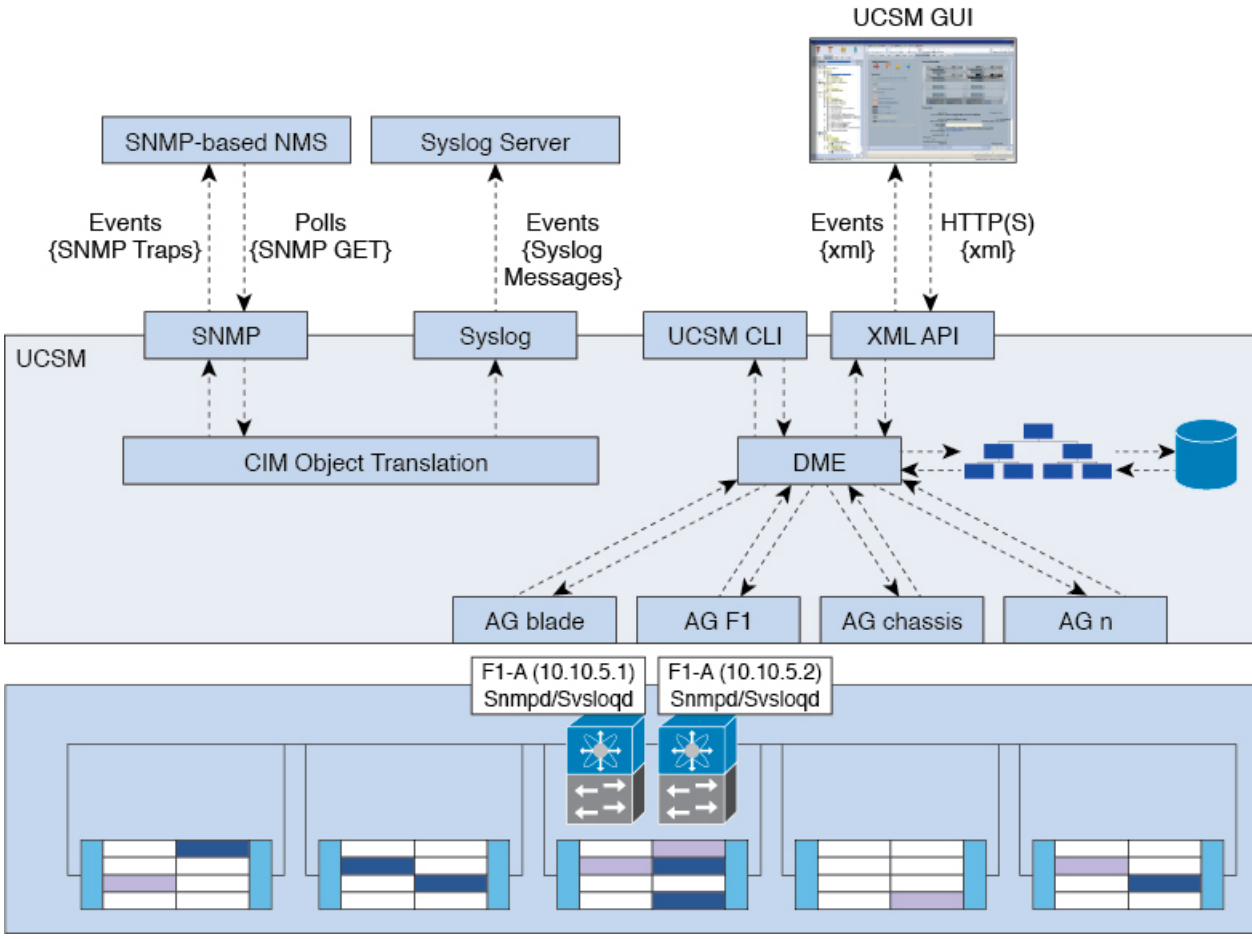
  - 中央のネットワーク管理ステーションからデバイスをモニタリングするための SNMP および、ホストとユーザの設定
  - SNMP トラップ、Call Home 通知、および特定デバイスでの障害抑制ポリシー
- Core File Exporter および、Syslog、監査ログ、システム イベント ログなどのログ
- アダプタ、シャーシ、ホスト、ポート、およびサーバに対する統計情報の収集およびしきい値ポリシー
- Call Home および Smart Call Home の Cisco 組み込みデバイスのサポート
- Cisco UCS Manager ユーザ インターフェイスを使用した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

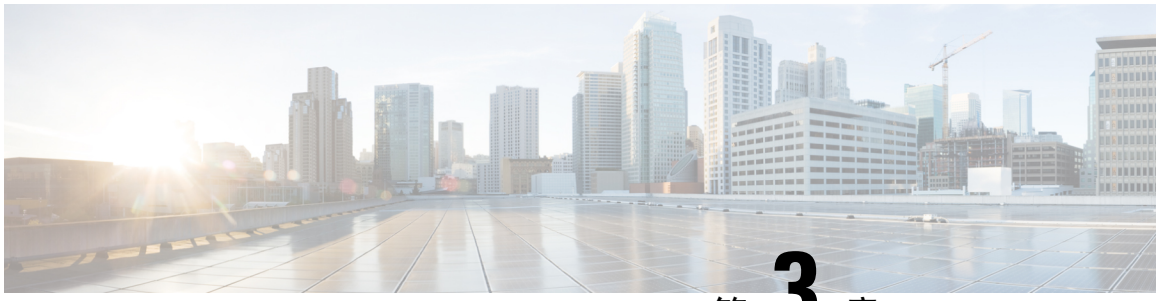
SNMP インフォームおよびトラップは、 Cisco UCSXML データベースに格納された障害情報から直接変換されます。SNMP GET 要求は、同じオブジェクト変換エンジンを介して逆方向に送信され、そこでオブジェクト変換エンジンからの要求を DME が受信します。データは、XML データベースから取得され、SNMP応答に変換されます。

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 マニュアル

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 Getting Started Guide | Cisco UCS アーキテクチャのほか、Cisco UCS Manager の初期設定や構成のベスト プラクティスなど、稼働前に必要な操作について説明しています。 |
| Cisco UCS Manager Administration Guide | パスワード管理、ロールベースのアクセスの設定、リモート認証、通信サービス、CIMC セッション管理、組織、バックアップと復元、スケジュール オプション、BIOS トークンおよび遅延展開について説明しています。 |
| Cisco UCS Manager Infrastructure Management Guide | Cisco UCS Manager によって使用および管理される物理インフラストラクチャと仮想インフラストラクチャのコンポーネントについて説明します。 |
| 『Cisco UCS Manager Firmware Management Guide』 | ファームウェアのダウンロードと管理、自動インストール によるアップグレード、サービス プロファイルによるアップグレード、ファームウェアの自動同期によるエンドポイントでの直接アップグレード、機能カタログの管理、展開シナリオ、および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 Server Management Guide』 | 新しいライセンス、Cisco UCS Central への Cisco UCS ドメインの登録、電力制限、サーバのブート、サーバプロファイルおよびサーバ関連ポリシーについて説明しています。 |
| 『Cisco UCS Manager Storage Management Guide』 | Cisco UCS Manager の SAN や VSAN など、ストレージ管理のあらゆる側面について説明しています。 |
| 『Cisco UCS Manager Network Management Guide』 | Cisco UCS Manager の LAN や VLAN 接続など、ネットワーク管理のあらゆる側面について説明しています。 |
| 『Cisco UCS Manager System Monitoring Guide』 | Cisco UCS Manager における、システム統計を含むシステムおよびヘルス モニタリングのあらゆる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 を使用して管理される UCS S シリーズ サーバの管理のあらゆる側面について説明しています。 |



第 3 章

# Syslog



## Syslog

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

- 定期的なシステム操作
- 障害およびエラー
- 重大なおよび緊急な事態

syslog のエントリには、障害、イベント、監査の 3 種類があります。

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

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

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

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

- イベント コード別または障害コード別：モニタする特定のコードだけを含めるための解析ルールを使ったフィルタを定義します。これらの条件に一致しないメッセージは廃棄されます。
- 重大度別：特定の重大度を持つ 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。

# Enabling Syslog Messages to Store In a Local File

**Procedure**

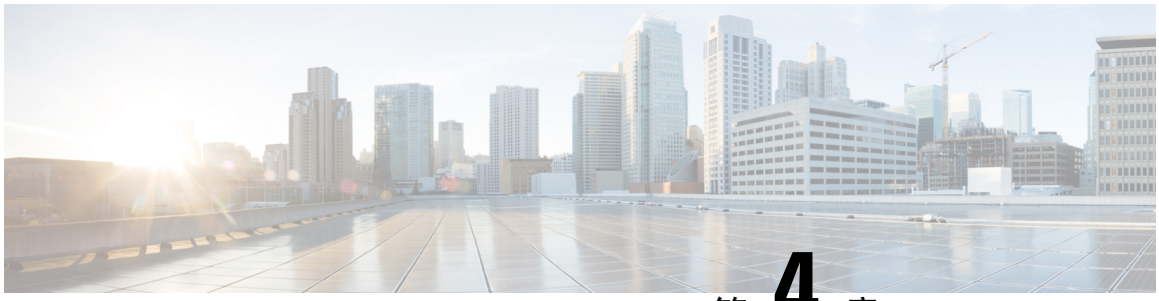
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # {**enable** \| **disable**} **syslog console** | Enables or disables the sending of syslogs to the console. |
| **Step 3** | (Optional) UCS-A /monitoring # **set syslog console level** {**emergencies** \| **alerts** \| **critical**} | Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the console. The level options are listed in order of decreasing urgency.The default level is Critical. |
| **Step 4** | UCS-A /monitoring # {**enable** \| **disable**} **syslog monitor** | Enables or disables the monitoring of syslog information by the operating system. |
| **Step 5** | (Optional) UCS-A /monitoring # **set syslog monitor level** {**emergencies** \| **alerts** \| **critical** \| **errors** \| **warnings** \| **notifications** \| **information** \| **debugging**} | Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency.The default level is Critical.<br>**Note** Messages at levels below Critical are displayed on the terminal monitor only if you have entered the **terminal monitor** command. |
| **Step 6** | UCS-A /monitoring # {**enable** \| **disable**} **syslog file** | Enables or disables the writing of syslog information to a syslog file. |
| **Step 7** | UCS-A /monitoring # **set syslog file name** *filename* | The name of the file in which the messages are logged. Up to 16 characters are allowed in the file name. |
| **Step 8** | (Optional) UCS-A /monitoring # **set syslog file level** {**emergencies** \| **alerts** \| **critical** \| **errors** \| **warnings** \| **notifications** \| **information** \| **debugging**} | Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency.The default level is Critical. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | (Optional) UCS-A /monitoring # **set syslog file size** *filesize* | The maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes. |
| **Step 10** | UCS-A /monitoring # {**enable** \| **disable**} **syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} | Enables or disables the sending of syslog messages to up to three external syslog servers. |
| **Step 11** | (Optional) UCS-A /monitoring # **set syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} **level**{**emergencies** \| **alerts** \| **critical** \| **errors** \| **warnings** \| **notifications** \| **information** \| **debugging**} | Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency.The default level is Critical. |
| **Step 12** | UCS-A /monitoring # **set syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} **hostname** *hostname* | The hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname. |
| **Step 13** | (Optional) UCS-A /monitoring # **set syslog remote-destination** {**server-1** \| **server-2** \| **server-3**} **facility** {**local0** \| **local1** \| **local2** \| **local3** \| **local4** \| **local5** \| **local6** \| **local7**} | The facility level contained in the syslog messages sent to the specified remote syslog server. |
| **Step 14** | UCS-A /monitoring # {**enable** \| **disable**} **syslog source** {**audits** \| **events** \| **faults**} | This can be one of the following:<br>• **audits**—Enables or disables the logging of all audit log events.<br>• **events**—Enables or disables the logging of all system events.<br>• **faults**—Enables or disables the logging of all system faults. |
| **Step 15** | UCS-A /monitoring # **commit-buffer** | Commits the transaction. |

### Example

This example shows how to enable the storage of syslog messages in a local file and commits the transaction:

```
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

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。

# Viewing the System Event Log for a Server

## Viewing the System Event Log for an Individual Server

### SUMMARY STEPS

1. UCS-A# **show sel** *chassis-id* / *blade-id*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **show sel** *chassis-id* / *blade-id* | Displays the system event log for the specified server. |

#### Example

The following example displays the system event log for blade 3 in chassis 1.

```
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
```

## Viewing the System Event Log for All of the Servers in a Chassis

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *blade-id*
2. UCS-A /chassis/server # **show sel**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id / blade-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show sel** | Displays the system event log. |

#### Example

The following example displays the system event log from chassis server mode for blade 3 in chassis 1.

```
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
```

# Configuring the SEL Policy

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope ep-log-policy sel**
3. (Optional) UCS-A /org/ep-log-policy # **set description** *description*
4. UCS-A /org/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**]
5. UCS-A /org/ep-log-policy # **set backup clear-on-backup** {**no** | **yes**}
6. UCS-A /org/ep-log-policy # **set backup destination** *URL*
7. UCS-A /org/ep-log-policy # **set backup format** {*ascii* | *binary*}
8. UCS-A /org/ep-log-policy # **set backup hostname** {*hostname* | *ip-addr*}

9. UCS-A /org/ep-log-policy # **set backup interval** {**1-hour** | **2-hours** | **4-hours** | **8-hours** | **24-hours** | **never**}
10. UCS-A /org/ep-log-policy # **set backup password** *password*
11. UCS-A /org/ep-log-policy # **set backup protocol** {**ftp** | **scp** | **sftp** | **tftp**}
12. UCS-A /org/ep-log-policy # **set backup remote-path** *path*
13. UCS-A /org/ep-log-policy # **set backup user** *username*
14. UCS-A /org/ep-log-policy # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type **/** as the *org-name* . |
| **Step 2** | UCS-A /org # **scope ep-log-policy sel** | Enters organization endpoint log policy mode and scopes the SEL policy. |
| **Step 3** | (Optional) UCS-A /org/ep-log-policy # **set description** *description* | Provides a description for the policy.<br>**Note** If your description includes spaces, special characters, or punctuation, begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output. |
| **Step 4** | UCS-A /org/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**] | Specifies an action or actions that will trigger a backup operation. |
| **Step 5** | UCS-A /org/ep-log-policy # **set backup clear-on-backup** {**no** \| **yes**} | Specifies whether to clear the system event log after a backup operation occurs. |
| **Step 6** | UCS-A /org/ep-log-policy # **set backup destination** *URL* | Specifies the protocol, user, password, remote hostname, and remote path for the backup operation. Depending on the protocol used, specify the URL using one of the following syntaxes:<br>• **ftp://** *username***@***hostname* **/** *path*<br>• **scp://** *username* **@** *hostname* **/** *path*<br>• **sftp://** *username* **@** *hostname* **/** *path*<br>• **tftp://** *hostname* **:** *port-num* **/** *path*<br>**Note** You can also specify the backup destination by using the **set backup hostname** , **set backup password** , **set backup protocol** , **set backup remote-path** , **set backup user** commands, or by using the **set backup destination** command. Use either method to specify the backup destination. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | UCS-A /org/ep-log-policy # **set backup format** {*ascii* \| *binary*} | Specifies the format for the backup file. |
| **Step 8** | UCS-A /org/ep-log-policy # **set backup hostname** {*hostname* \| *ip-addr*} | Specifies the hostname or IP address of the remote server. |
| **Step 9** | UCS-A /org/ep-log-policy # **set backup interval** {**1-hour** \| **2-hours** \| **4-hours** \| **8-hours** \| **24-hours** \| **never**} | Specifies the time interval for the automatic backup operation. Specifying the **never** keyword means that automatic backups will not be made. |
| **Step 10** | UCS-A /org/ep-log-policy # **set backup password** *password* | Specifies the password for the username. This step does not apply if the TFTP protocol is used. |
| **Step 11** | UCS-A /org/ep-log-policy # **set backup protocol** {**ftp** \| **scp** \| **sftp** \| **tftp**} | Specifies the protocol to use when communicating with the remote server. |
| **Step 12** | UCS-A /org/ep-log-policy # **set backup remote-path** *path* | Specifies the path on the remote server where the backup file is to be saved. |
| **Step 13** | UCS-A /org/ep-log-policy # **set backup user** *username* | Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used. |
| **Step 14** | UCS-A /org/ep-log-policy # **commit-buffer** | Commits the transaction. |

### Example

The following example configures the SEL policy to back up the system event log (in ASCII format) every 24 hours or when the log is full, clears the system event log after a backup operation occurs, and commits the transaction:

```
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 #
```

# Backing Up the System Event Log for a Server

## Backing Up the System Event Log for an Individual Server

### Before you begin

Configure the system event log policy. The manual backup operation uses the remote destination configured in the system event log policy.

### SUMMARY STEPS

1. UCS-A /chassis/server # **backup sel** *chassis-id* / *blade-id*
2. UCS-A# **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /chassis/server # **backup sel** *chassis-id* / *blade-id* | Backs up the system event log. |
| **Step 2** | UCS-A# **commit-buffer** | Commits the transaction. |

### Example

The following example backs up the system event log for blade 3 in chassis 1 and commits the transaction.

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

## Backing Up the System Event Log for All of the Servers in a Chassis

### Before you begin

Configure the system event log policy. The manual backup operation uses the remote destination configured in the system event log policy.

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *blade-id*
2. UCS-A /chassis/server # **backup sel**
3. UCS-A /chassis/server # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *blade-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **backup sel** | Backs up the system event log. |
| **Step 3** | UCS-A /chassis/server # **commit-buffer** | Commits the transaction. |

#### Example

The following example backs up the system event log from chassis server mode for blade 3 in chassis 1 and commits the transaction.

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

# Clearing the System Event Log for a Server

## Clearing the System Event Log for an Individual Server

### SUMMARY STEPS

1. UCS-A# **clear sel** *chassis-id* / *blade-id*
2. UCS-A# **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **clear sel** *chassis-id* / *blade-id* | Clears the system event log. |
| **Step 2** | UCS-A# **commit-buffer** | Commits the transaction. |

#### Example

The following example clears the system event log for blade 3 in chassis 1 and commits the transaction:

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

# Clearing the System Event Log for All of the Servers in a Chassis

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *blade-id*
2. UCS-A /chassis/server # **clear sel**
3. UCS-A /chassis/server # **commit-buffer**

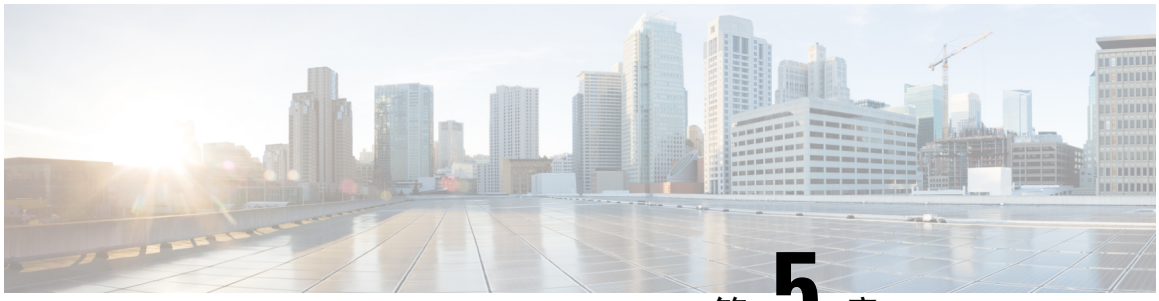
### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *blade-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **clear sel** | Clears the system event log. |
| **Step 3** | UCS-A /chassis/server # **commit-buffer** | Commits the transaction. |

#### Example

The following example clears the system event log from chassis server mode for blade 3 in chassis 1 and commits the transaction:

```
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

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

## Viewing Audit Logs

### SUMMARY STEPS

1. UCS-A# **scope security**
2. UCS-A /security # **show audit-logs**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope security** | Enters security mode. |
| **Step 2** | UCS-A /security # **show audit-logs** | Displays the audit logs.<br>**Note** Use the *id* option to view a specific audit-log. Use the detail option to view more detailed information in the audit log output. |

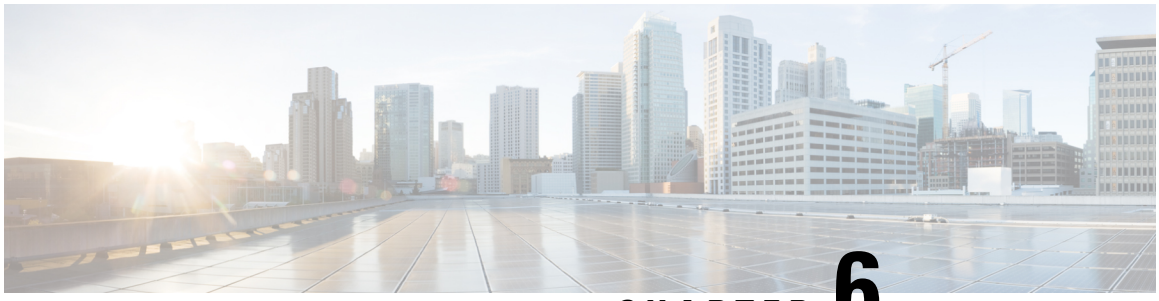
### Example

The following example displays the audit logs:

```
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 #
```



CHAPTER 6

# Log File Exporter



## Log File Exporter

Cisco UCS Manager generates log files for each executable. The log files can be up to 20 MB in size, and up to five backups can be stored on the server. The log file exporter allows you to export the log files to a remote server before they are deleted. The log file names contain the following information:

- The name of the process
- Timestamp
- The name and ID of the fabric interconnect

**Note** If you do not enable log exporting, the oldest log files are deleted whenever the maximum backup file limit is reached.

### Guidelines and Limitations

- We recommend that you use tftp or password-less scp or sftp for log export. When standard scp or sftp is used, the user password is stored in the configuration file in encrypted format.
- On a HA setup, the log files from each side are exported separately. If one side fails to export logs, the other side does not compensate.

## Exporting Log Files to a Remote Server

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope sysdebug**
3. UCS-A /monitoring/sysdebug # **scope log-export-policy**

4. UCS-A /monitoring/sysdebug/log-export-policy # **set admin-state** {**disabled** | **enabled**}
5. (Optional) UCS-A /monitoring/sysdebug/log-export-policy # **set desc** *description*
6. UCS-A /monitoring/sysdebug/log-export-policy # **set hostname** *hostname*
7. UCS-A /monitoring/sysdebug/log-export-policy # **set passwd**
8. UCS-A /monitoring/sysdebug/log-export-policy # **set passwordless-ssh** {**no** | **yes**}
9. UCS-A /monitoring/sysdebug/log-export-policy # **set proto** {**scp** | **ftp** | **sftp** | **tftp**}
10. UCS-A /monitoring/sysdebug/log-export-policy # **set path** *path*
11. UCS-A /monitoring/sysdebug/log-export-policy # **set user** *username*
12. UCS-A /monitoring/sysdebug/log-export-policy # **commit-buffer**

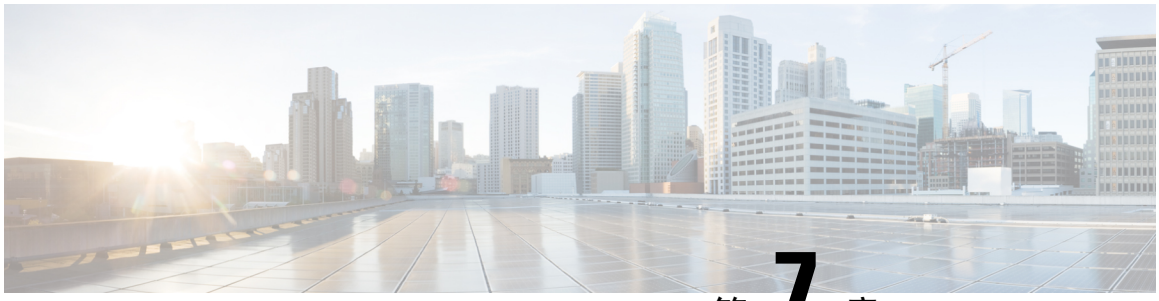
## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope sysdebug** | Enters monitoring system debug mode. |
| **Step 3** | UCS-A /monitoring/sysdebug # **scope log-export-policy** | Enters log file export mode. |
| **Step 4** | UCS-A /monitoring/sysdebug/log-export-policy # **set admin-state** {**disabled** \| **enabled**} | Whether log file exporting is enabled. |
| **Step 5** | (Optional) UCS-A /monitoring/sysdebug/log-export-policy # **set desc** *description* | Provides a description for the log export policy |
| **Step 6** | UCS-A /monitoring/sysdebug/log-export-policy # **set hostname** *hostname* | Specifies the hostname of the remote server. |
| **Step 7** | UCS-A /monitoring/sysdebug/log-export-policy # **set passwd** | After you press Enter, you are prompted to enter the password.<br>Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used. |
| **Step 8** | UCS-A /monitoring/sysdebug/log-export-policy # **set passwordless-ssh** {**no** \| **yes**} | Enables SSH login without a password. |
| **Step 9** | UCS-A /monitoring/sysdebug/log-export-policy # **set proto** {**scp** \| **ftp** \| **sftp** \| **tftp**} | Specifies the protocol to use when communicating with the remote server. |
| **Step 10** | UCS-A /monitoring/sysdebug/log-export-policy # **set path** *path* | Specifies the path on the remote server where the log file is to be saved. |
| **Step 11** | UCS-A /monitoring/sysdebug/log-export-policy # **set user** *username* | Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used. |
| **Step 12** | UCS-A /monitoring/sysdebug/log-export-policy # **commit-buffer** | Commits the transaction. |

### Example

The following example shows how to enable the log file exporter, specify the remote server hostname, set the protocol to scp, enable passwordless login, and commit the transaction.

```
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

ファブリック インターコネクトや I/O モジュールなどの Cisco UCS コンポーネントで重大な障害が発生すると、システムはコアダンプ ファイルを作成することがあります。 Cisco UCS Manager では、この Core File Exporter で TFTP からネットワーク上の指定ロケーションに直ちにコア ダンプ ファイルを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。

## Configuring the Core File Exporter

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope sysdebug**
3. UCS-A /monitoring/sysdebug # **enable core-export-target**
4. UCS-A /monitoring/sysdebug # **set core-export-target path** *path*
5. UCS-A /monitoring/sysdebug # **set core-export-target port** *port-num*
6. UCS-A /monitoring/sysdebug # **set core-export-target server-description** *description*
7. UCS-A /monitoring/sysdebug # **set core-export-target server-name** *hostname*
8. UCS-A /monitoring/sysdebug # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope sysdebug** | Enters monitoring system debug mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | UCS-A /monitoring/sysdebug # **enable core-export-target** | Enables the core file exporter. When the core file exporter is enabled and an error causes the server to perform a core dump, the system exports the core file via TFTP to the specified remote server. |
| **Step 4** | UCS-A /monitoring/sysdebug # **set core-export-target path** *path* | Specifies the path to use when exporting the core file to the remote server. |
| **Step 5** | UCS-A /monitoring/sysdebug # **set core-export-target port** *port-num* | Specifies the port number to use when exporting the core file via TFTP. The range of valid values is 1 to 65,535. |
| **Step 6** | UCS-A /monitoring/sysdebug # **set core-export-target server-description** *description* | Provides a description for the remote server used to store the core file. |
| **Step 7** | UCS-A /monitoring/sysdebug # **set core-export-target server-name** *hostname* | Specifies the hostname of the remote server to connect with via TFTP. |
| **Step 8** | UCS-A /monitoring/sysdebug # **commit-buffer** | Commits the transaction. |

### Example

The following example enables the core file exporter, specifies the path and port to use when sending the core file, specifies the remote server hostname, provides a description for the remote server, and commits the transaction.

```
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 #
```

# Disabling the Core File Exporter

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope sysdebug**
3. UCS-A /monitoring/sysdebug # **disable core-export-target**
4. UCS-A /monitoring/sysdebug # **commit-buffer**

### DETAILED STEPS

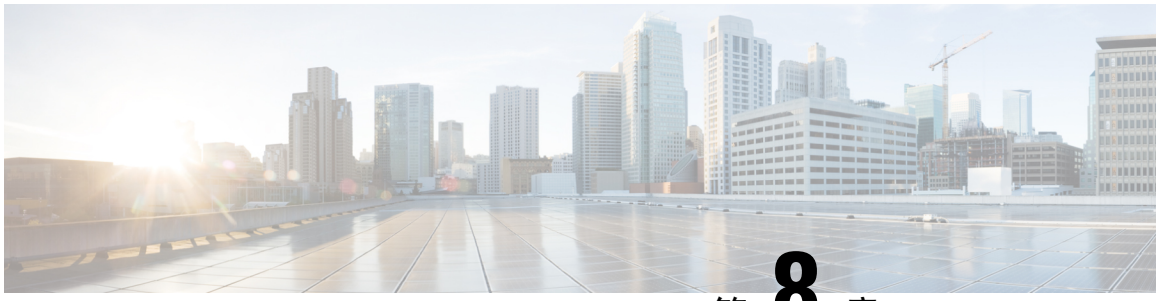
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | UCS-A /monitoring # **scope sysdebug** | Enters monitoring system debug mode. |
| **Step 3** | UCS-A /monitoring/sysdebug # **disable core-export-target** | Disables the core file exporter. When the core file exporter is disabled core files are not automatically exported. |
| **Step 4** | UCS-A /monitoring/sysdebug # **commit-buffer** | Commits the transaction. |

### Example

The following example disables the core file exporter and commits the transaction.

```
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

# 障害の収集と抑制



## 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。フラッピング間隔の間、グローバル障害ポリシーに指定されている期間は、障害の重要度が保持されます。
3. フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。
4. クリアされた障害は保持期間になります。この期間があるため、障害が発生した状態が改善され、さらに障害が早々に削除されていない場合でも管理者が障害に気付くことができます。保持期間のうち、グローバル障害ポリシーに指定された期間はクリアされた障害が保持されます。
5. この状況が保持間隔中に再発生する場合は、障害がアクティブ状態に戻ります。この状況が再発生しない場合は、障害が削除されます。

# Configuring the Fault Collection Policy

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope fault policy**
3. UCS-A /monitoring/fault-policy # **set clear-action** {**delete** | **retain**}
4. UCS-A /monitoring/fault-policy # **set flap-interval** *seconds*
5. UCS-A /monitoring/fault-policy # **set retention-interval** {*days hours minutes seconds* | **forever**}
6. UCS-A /monitoring/fault-policy # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope fault policy** | Enters monitoring fault policy mode. |
| **Step 3** | UCS-A /monitoring/fault-policy # **set clear-action** {**delete** \| **retain**} | Specifies whether to retain or delete all cleared messages. If the **retain** option is specified, then the length of time that the messages are retained is determined by the **set retention-interval** command. |
| **Step 4** | UCS-A /monitoring/fault-policy # **set flap-interval** *seconds* | Specifies the time interval (in seconds) the system waits before changing a fault state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change state until the flapping interval has elapsed after the last state change. If the fault is raised again during the flapping interval, it returns to the active state, otherwise, the fault is cleared. |
| **Step 5** | UCS-A /monitoring/fault-policy # **set retention-interval** {*days hours minutes seconds* \| **forever**} | Specifies the time interval the system retains all cleared fault messages before deleting them. The system can retain cleared fault messages forever, or for the specified number of days, hours, minutes, and seconds. |
| **Step 6** | UCS-A /monitoring/fault-policy # **commit-buffer** | Commits the transaction. |

#### Example

This example configures the fault collection policy to retain cleared fault messages for 30 days, sets the flapping interval to 10 seconds, and commits the transaction.

```
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。

# Configuring Fault Suppression for a Chassis

## Configuring Fault Suppression Tasks for a Chassis Using a Fixed Time Interval

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **create fault-suppress-task** *name*
3. UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*
4. UCS-A/chassis/fault-suppress-task # **create local-schedule**
5. UCS-A/chassis/fault-suppress-task/local-schedule # **create occurrence single-one-time**
6. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | 指定したシャーシでシャーシ モードを開始します。 |
| **Step 2** | UCS-A/chassis # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Specifies the fault suppression policy that you want to apply. This can be one of the following:<br>• **default-chassis-all-maint**：シャーシとそのシャーシにインストールされたすべてのコンポーネントの障害を抑制します。コンポーネントには、すべてのサーバ、電源、ファンモジュール、IOMなどが含まれます。<br>• **default-chassis-phys-maint**：シャーシ、すべてのファン モジュール、シャーシに装着された電源の障害を抑制します。<br>• **default-server-maint**：サーバの障害を抑制します。<br>**Note** シャーシに適用された場合、サーバのみが影響を受けます。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 5** | UCS-A/chassis/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 6** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task2 for the chassis, apply the default-chassis-all-maint policy to the task, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
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
```

## Configuring Fault Suppression Tasks for a Chassis Using a Schedule

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **create fault-suppress-task** *name*
3. UCS-A/chassis/fault-suppress-task # **set schedule** *name*
4. UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*
5. UCS-A/chassis/fault-suppress-task # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | 指定したシャーシでシャーシ モードを開始します。 |
| **Step 2** | UCS-A/chassis # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/chassis/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule, on page 56. |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Selects the fault suppression policy you want to apply. This can be one of the following:<br>• **default-chassis-all-maint**：シャーシとそのシャーシにインストールされたすべてのコンポーネン |

| | Command or Action | Purpose |
|---|---|---|
| | | トの障害を抑制します。コンポーネントには、すべてのサーバ、電源、ファンモジュール、IOMなどが含まれます。<br>• **default-chassis-phys-maint**：シャーシ、すべてのファン モジュール、シャーシに装着された電源の障害を抑制します。<br>• **default-server-maint**：サーバの障害を抑制します。<br>**Note** シャーシに適用された場合、サーバのみが影響を受けます。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 |
| **Step 5** | UCS-A/chassis/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task1 for the chassis, apply the scheduler called weekly_maint and the default-chassis-all-maint policy to the task, and commit the transaction:

```
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
```

## Modifying Fault Suppression Tasks for a Chassis

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **scope fault-suppress-task** *name*
3. UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*
4. UCS-A/chassis/fault-suppress-task # **set schedule** *name*
5. UCS-A/chassis/fault-suppress-task # **scope local-schedule**
6. UCS-A/chassis/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
7. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
9. UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | 指定したシャーシでシャーシ モードを開始します。 |
| **Step 2** | UCS-A/chassis # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 3** | UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Modifies the fault suppression policy. This can be one of the following:<br>• **default-chassis-all-maint**：シャーシとそのシャーシにインストールされたすべてのコンポーネントの障害を抑制します。コンポーネントには、すべてのサーバ、電源、ファンモジュール、IOM などが含まれます。<br>• **default-chassis-phys-maint**：シャーシ、すべてのファン モジュール、シャーシに装着された電源の障害を抑制します。<br>• **default-server-maint**：サーバの障害を抑制します。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。<br>**Note** To apply a different schedule to the fault suppression task, go to Step 4. To change the fixed time interval of the fault suppression task, go to Step 5. |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **set schedule** *name* | Applies the schedule you want to use.<br>**Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 5** | UCS-A/chassis/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 6** | UCS-A/chassis/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 7** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
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
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
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
```

## Viewing Suppressed Faults and Fault Suppression Tasks for a Chassis

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **show fault suppressed**
3. UCS-A/chassis # **scope fault-suppress-task** *name*
4. UCS-A/chassis/fault-suppress-task # **show detail expand**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | 指定したシャーシでシャーシ モードを開始します。 |
| **Step 2** | UCS-A/chassis # **show fault suppressed** | Displays the suppressed faults for the chassis.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 3** | UCS-A/chassis # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 4** | UCS-A/chassis/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

### Example

The following example shows how to display the suppressed faults for a chassis:

```
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 #
```

The following example shows how to display the fault suppression task called task1:

```
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 #
```

## Deleting Fault Suppression Tasks for a Chassis

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A/chassis # **delete fault-suppress-task** *name*
3. UCS-A/chassis # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | 指定したシャーシでシャーシ モードを開始します。 |
| **Step 2** | UCS-A/chassis # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 3** | UCS-A/chassis # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to delete the fault suppression task called task1:

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

# Configuring Fault Suppression for an I/O Module

## Configuring Fault Suppression Tasks for an IOM Using a Fixed Time Interval

The **default-iom-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]
2. UCS-A /chassis|fex # **scope iom** *iom-id*
3. UCS-A/chassis|fex/iom # **create fault-suppress-task** *name*
4. UCS-A/chassis|fex/iom/fault-suppress-task # **create local-schedule**
5. UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule # **create occurrence single-one-time**
6. UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope** [**chassis** *chassis-num* \| **fex** *fex-num*] | Enters chassis mode for the specified chassis or FEX. |
| **Step 2** | UCS-A /chassis\|fex # **scope iom** *iom-id* | Enters chassis I/O module mode for the selected I/O module. |
| **Step 3** | UCS-A/chassis\|fex/iom # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the IOM, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 4** | UCS-A/chassis\|fex/iom/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 5** | UCS-A/chassis\|fex/iom/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 6** | UCS-A/chassis\|fex/iom/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/chassis\|fex/iom/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task2 for the IOM on a chassis, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
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
```

The following example shows how to create a fault suppression task called task2 for the IOM on a FEX, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
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
```

## Configuring Fault Suppression Tasks for an IOM Using a Schedule

The **default-iom-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]
2. UCS-A /chassis|fex # **scope iom** *iom-id*
3. UCS-A/chassis|fex/iom # **create fault-suppress-task** *name*
4. UCS-A/chassis|fex/iom/fault-suppress-task # **set schedule** *name*
5. UCS-A/chassis|fex/iom/fault-suppress-task # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope** [**chassis** *chassis-num* \| **fex** *fex-num*] | Enters chassis mode for the specified chassis or FEX. |
| **Step 2** | UCS-A /chassis\|fex # **scope iom** *iom-id* | Enters chassis I/O module mode for the selected I/O module. |
| **Step 3** | UCS-A/chassis\|fex/iom # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the IOM, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブ |

| | Command or Action | Purpose |
|---|---|---|
| | | 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。 |
| **Step 4** | UCS-A/chassis\|fex/iom/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule, on page 56. |
| **Step 5** | UCS-A/chassis\|fex/iom/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task1 for the IOM on a chassis, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
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
```

The following example shows how to create a fault suppression task called task1 for the IOM on a FEX, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
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
```

## Modifying Fault Suppression Tasks for an IOM

### SUMMARY STEPS

1. UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]
2. UCS-A /chassis|fex # **scope iom** *iom-id*
3. UCS-A/chassis|fex/iom # **scope fault-suppress-task** *name*
4. UCS-A/chassis|fex/iom/fault-suppress-task # **set schedule** *name*
5. UCS-A/chassis|fex/iom/fault-suppress-task # **scope local-schedule**
6. UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
7. UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
8. 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*}
9. UCS-A/chassis|fex/iom/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope** [**chassis** *chassis-num* \| **fex** *fex-num*] | Enters chassis mode for the specified chassis or FEX. |
| **Step 2** | UCS-A /chassis\|fex # **scope iom** *iom-id* | Enters chassis I/O module mode for the selected I/O module. |
| **Step 3** | UCS-A/chassis\|fex/iom # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode.<br>**Note** To apply a different schedule to the fault suppression task, go to Step 4. To change the fixed time interval of the fault suppression task, go to Step 5. |
| **Step 4** | UCS-A/chassis\|fex/iom/fault-suppress-task # **set schedule** *name* | Applies a different schedule.<br>**Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 5** | UCS-A/chassis\|fex/iom/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 6** | UCS-A/chassis\|fex/iom/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 7** | UCS-A/chassis\|fex/iom/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 8** | 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 9** | UCS-A/chassis\|fex/iom/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2 for an IOM on a chassis:

```
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
```

The following example shows how to apply a different schedule to the fault suppression task called task1 for an IOM on a FEX:

```
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
```

## Viewing Suppressed Faults and Fault Suppression Tasks for an IOM

### SUMMARY STEPS

1. UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]
2. UCS-A /chassis|fex # **scope iom** *iom-id*
3. UCS-A/chassis|fex/iom # **show fault suppressed**
4. UCS-A/chassis|fex/iom # **scope fault-suppress-task** *name*
5. UCS-A/chassis|fex/iom/fault-suppress-task # **show detail expand**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope** [**chassis** *chassis-num* \| **fex** *fex-num*] | Enters chassis mode for the specified chassis or FEX. |
| **Step 2** | UCS-A /chassis\|fex # **scope iom** *iom-id* | Enters chassis I/O module mode for the selected I/O module. |
| **Step 3** | UCS-A/chassis\|fex/iom # **show fault suppressed** | Displays the suppressed faults for the IOM.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 4** | UCS-A/chassis\|fex/iom # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 5** | UCS-A/chassis\|fex/iom/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

#### Example

The following example shows how to display the suppressed faults for an IOM on a chassis:

```
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 #
```

The following example shows how to display the fault suppression task called task1 for an IOM on a chassis:

```
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 #
```

The following example shows how to display the fault suppression task called task1 for an IOM on a FEX:

```
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 #
```

## Deleting Fault Suppression Tasks for an IOM

### SUMMARY STEPS

1. UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]
2. UCS-A /chassis|fex # **scope iom** *iom-id*
3. UCS-A/chassis|fex/iom # **delete fault-suppress-task** *name*
4. UCS-A/chassis|fex/iom # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope** [**chassis** *chassis-num* \| **fex** *fex-num*] | Enters chassis mode for the specified chassis or FEX. |
| **Step 2** | UCS-A /chassis\|fex # **scope iom** *iom-id* | Enters chassis I/O module mode for the selected I/O module. |
| **Step 3** | UCS-A/chassis\|fex/iom # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 4** | UCS-A/chassis\|fex/iom # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example shows how to delete the fault suppression task called task1 for an IOM on a chassis:

```
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
```

The following example shows how to delete the fault suppression task called task1 for an IOM on a FEX:

```
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
```

# Configuring Fault Suppression for a FEX

## Configuring Fault Suppression Tasks for a FEX Using a Fixed Time Interval

### SUMMARY STEPS

1. UCS-A# **scope fex** *fex-num*
2. UCS-A/fex # **create fault-suppress-task** *name*
3. UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*
4. UCS-A/fex/fault-suppress-task # **create local-schedule**
5. UCS-A/fex/fault-suppress-task/local-schedule # **create occurrence single-one-time**
6. UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fex** *fex-num* | Enters fex mode for the specified FEX. |
| **Step 2** | UCS-A/fex # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the fex, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Specifies the fault suppression policy you want to apply. This can be one of the following:<br>• **default-fex-all-maint**：FEX、すべての電源、ファン モジュール、FEX 内の IOM の障害を抑制します。 |

| | Command or Action | Purpose |
|---|---|---|
| | | • **default-fex-phys-maint**：FEX、FEX 内のすべてのファンモジュールと電源の障害を抑制します。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 |
| **Step 4** | UCS-A/fex/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 5** | UCS-A/fex/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 6** | UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task2 for the FEX, apply the default-fex-all-maint policy to the task, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
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
```

## Configuring Fault Suppression Tasks for a FEX Using a Schedule

### SUMMARY STEPS

1. UCS-A# **scope fex** *fex-num*
2. UCS-A/fex # **create fault-suppress-task** *name*
3. UCS-A/fex/fault-suppress-task # **set schedule** *name*
4. UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*
5. UCS-A/fex/fault-suppress-task # **commit-buffer**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fex** *fex-num* | Enters fex mode for the specified FEX. |
| **Step 2** | UCS-A/fex # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the fex, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/fex/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule, on page 56. |
| **Step 4** | UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Specifies the fault suppression policy that you want to apply. This can be one of the following:<br>• **default-fex-all-maint**：FEX、すべての電源、ファン モジュール、FEX 内の IOM の障害を抑制します。<br>• **default-fex-phys-maint**：FEX、FEX 内のすべてのファンモジュールと電源の障害を抑制します。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。 |
| **Step 5** | UCS-A/fex/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task1 for the FEX, apply the scheduler called weekly_maint and the default-fex-all-maint policy to the task, and commit the transaction:

```
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
```

# Modifying Fault Suppression Tasks for a FEX

### SUMMARY STEPS

1. UCS-A# **scope fex** *fex-num*
2. UCS-A/fex # **scope fault-suppress-task** *name*
3. UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*
4. UCS-A/fex/fault-suppress-task # **set schedule** *name*
5. UCS-A/fex/fault-suppress-task # **scope local-schedule**
6. UCS-A/fex/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
7. UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
9. UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fex** *fex-num* | Enters fex mode for the specified FEX. |
| **Step 2** | UCS-A/fex # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 3** | UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name* | Modifies the fault suppression policy. This can be one of the following:<br>• **default-fex-all-maint**：FEX、すべての電源、ファン モジュール、FEX 内の IOM の障害を抑制します。<br>• **default-fex-phys-maint**：FEX、FEX 内のすべてのファンモジュールと電源の障害を抑制します。<br>• **default-iom-maint**：シャーシまたは FEX 内の IOM の障害を抑制します。<br>**Note** To apply a different schedule to the fault suppression task, go to Step 4. To change the fixed time interval of the fault suppression task, go to Step 5. |
| **Step 4** | UCS-A/fex/fault-suppress-task # **set schedule** *name* | Applies a different schedule.<br>**Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | UCS-A/fex/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 6** | UCS-A/fex/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 7** | UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 9** | UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
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
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
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
```

## Viewing Suppressed Faults and Fault Suppression Tasks for a FEX

### SUMMARY STEPS

1. UCS-A# **scope fex** *fex-num*
2. UCS-A/fex # **show fault suppressed**
3. UCS-A/fex # **scope fault-suppress-task** *name*
4. UCS-A/fex/fault-suppress-task # **show detail expand**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fex** *fex-num* | Enters fex mode for the specified FEX. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | UCS-A/fex # **show fault suppressed** | Displays the suppressed faults for the FEX.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 3** | UCS-A/fex # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 4** | UCS-A/fex/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

### Example

The following example shows how to display the suppressed faults for a FEX:

```
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 #
```

The following example shows how to display the fault suppression task called task1:

```
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 #
```

## Deleting Fault Suppression Tasks for a FEX

### SUMMARY STEPS

1. UCS-A# **scope fex** *fex-num*
2. UCS-A/fex # **delete fault-suppress-task** *name*
3. UCS-A/fex # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fex** *fex-num* | Enters fex mode for the specified FEX. |
| **Step 2** | UCS-A/fex # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 3** | UCS-A/fex # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to delete the fault suppression task called task1:

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

# Configuring Fault Suppression for a Server

## Configuring Fault Suppression Tasks for a Server Using a Fixed Time Interval

The **default-server-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]
2. UCS-A/server # **create fault-suppress-task** *name*
3. UCS-A/server/fault-suppress-task # **create local-schedule**
4. UCS-A/server/fault-suppress-task/local-schedule # **create occurrence single-one-time**
5. UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
7. UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A/server # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the server, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/server/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 4** | UCS-A/server/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 5** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 7** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task2 for the server, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
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
```

## Configuring Fault Suppression Tasks for a Server using a Schedule

The **default-server-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]
2. UCS-A/server # **create fault-suppress-task** *name*
3. UCS-A/server/fault-suppress-task # **set schedule** *name*
4. UCS-A/server/fault-suppress-task # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A/server # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the server, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/server/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule, on page 56. |
| **Step 4** | UCS-A/server/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to creates a fault suppression task called task1 for the server, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
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
```

## Modifying Fault Suppression Tasks for a Server

### SUMMARY STEPS

1. UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]
2. UCS-A/server # **scope fault-suppress-task** *name*
3. UCS-A/server/fault-suppress-task # **set schedule** *name*
4. UCS-A/server/fault-suppress-task # **scope local-schedule**
5. UCS-A/server/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
6. UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A/server # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode.<br>**Note** To apply a different schedule to the fault suppression task, go to Step 3. To change the fixed time interval of the fault suppression task, go to Step 4. |
| **Step 3** | UCS-A/server/fault-suppress-task # **set schedule** *name* | Applies a different schedule. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 4** | UCS-A/server/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 5** | UCS-A/server/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 6** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/server/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
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
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
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
```

## Creating a Schedule

### SUMMARY STEPS

1. UCS-A# **scope system**
2. UCS-A /system # **create scheduler** *sched-name*
3. UCS-A /system/scheduler # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope system** | Enters system mode. |
| **Step 2** | UCS-A /system # **create scheduler** *sched-name* | Creates a scheduler and enters scheduler mode. |
| **Step 3** | UCS-A /system/scheduler # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example creates a scheduler called maintenancesched and commits the transaction:

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

#### What to do next

Create a one time occurrence or recurring occurrence for the schedule.

## Viewing Suppressed Faults and Fault Suppression Tasks for a Server

### SUMMARY STEPS

1. UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]
2. UCS-A/server # **show fault suppressed**
3. UCS-A/server # **scope fault-suppress-task** *name*
4. UCS-A/server/fault-suppress-task # **show detail expand**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A/server # **show fault suppressed** | Displays the suppressed faults for the server.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 3** | UCS-A/server # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 4** | UCS-A/server/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

#### Example

The following example shows how to display the suppressed faults for a server:

```
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 #
```

The following example shows how to display the fault suppression task called task1:

```
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 #
```

## Deleting Fault Suppression Tasks for a Server

### SUMMARY STEPS

1. UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]
2. UCS-A/server # **delete fault-suppress-task** *name*
3. UCS-A/server # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A/server # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 3** | UCS-A/server # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example shows how to delete the fault suppression task called task1:

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

# Configuring Fault Suppression for a Service Profile

## Configuring Fault Suppression Tasks for a Service Profile Using a Fixed Time Interval

The **default-server-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A /org/service-profile # **create fault-suppress-task** *name*
4. UCS-A/org/service-profile/fault-suppress-task # **create local-schedule**
5. UCS-A/org/service-profile/fault-suppress-task/local-schedule # **create occurrence single-one-time**
6. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A /org/service-profile # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 4** | UCS-A/org/service-profile/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 6** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task2 under the accounting service profile, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
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
```

## Configuring Fault Suppression Tasks for a Service Profile Using a Schedule

The **default-server-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A /org/service-profile # **create fault-suppress-task** *name*
4. UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name*
5. UCS-A/org/service-profile/fault-suppress-task # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A /org/service-profile # **create fault-suppress-task** *name* | Creates a fault-suppress-task on the chassis, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule, on page 56. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task1 under the accounting service profile, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
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
```

## Modifying Fault Suppression Tasks for a Service Profile

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A/org/service-profile # **scope fault-suppress-task** *name*
4. UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name*
5. UCS-A/org/service-profile/fault-suppress-task # **scope local-schedule**
6. UCS-A/org/service-profile/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
7. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
9. UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A/org/service-profile # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** To apply a different schedule to the fault suppression task, go to Step 4. To change the fixed time interval of the fault suppression task, go to Step 5. |
| **Step 4** | UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name* | Applies a different schedule.<br>**Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 6** | UCS-A/org/service-profile/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 7** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 9** | UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
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
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
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
```

# Viewing Suppressed Faults and Fault Suppression Tasks for a Service Profile

## SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A/org/service-profile # **show fault suppressed**
4. UCS-A/org/service-profile # **scope fault-suppress-task** *name*
5. UCS-A/org/service-profile/fault-suppress-task # **show detail expand**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A/org/service-profile # **show fault suppressed** | Displays the suppressed faults for the server.<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 4** | UCS-A/org/service-profile # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 5** | UCS-A/org/service-profile/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

### Example

The following example shows how to display the suppressed faults for a service profile:

```
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 #
```

The following example shows how to display the fault suppression task called task1:

```
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 #
```

## Deleting Fault Suppression Tasks for a Service Profile

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A/org/service-profile # **delete fault-suppress-task** *name*
4. UCS-A/org/service-profile # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters service profile organization mode for the service profile. |
| **Step 3** | UCS-A/org/service-profile # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 4** | UCS-A/org/service-profile # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example shows how to delete the fault suppression task called task1:

```
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
```

# Configuring Fault Suppression for an Organization

## Configuring Fault Suppression Tasks for an Organization Using a Fixed Time Interval

The **default-server-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **create fault-suppress-task** *name*
3. UCS-A/org/fault-suppress-task # **create local-schedule**

4. UCS-A/org/fault-suppress-task/local-schedule # **create occurrence single-one-time**
5. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
7. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A/org # **create fault-suppress-task** *name* | Creates a fault-suppress-task for the organization, and enters fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/org/fault-suppress-task # **create local-schedule** | Creates a local schedule and enters local-schedule mode. |
| **Step 4** | UCS-A/org/fault-suppress-task/local-schedule # **create occurrence single-one-time** | Creates a one-time occurrence, and enters single-one-time mode. |
| **Step 5** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 7** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task2 under the Root organization, set the start date to January 1, 2013 at 11:00, and commit the transaction:

```
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
```

# Configuring Fault Suppression Tasks for an Organization Using a Schedule

The **default-server-maint** suppression policy is selected by default.

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **create fault-suppress-task** *name*
3. UCS-A/org/fault-suppress-task # **set schedule** *name*
4. UCS-A/org/fault-suppress-task # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A/org # **create fault-suppress-task** *name* | Creates a fault-suppress-task for the organization, and enters the fault-suppress-task mode.<br>この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 |
| **Step 3** | UCS-A/org/fault-suppress-task # **set schedule** *name* | Specifies the schedule that you want to use.<br>**Note** The schedule must exist before you can use it in a fault suppression task. For more information about creating schedules, see Creating a Schedule, on page 56. |
| **Step 4** | UCS-A/org/fault-suppress-task # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a fault suppression task called task1 under the Root organization, apply the scheduler called weekly_maint to the task, and commit the transaction:

```
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
```

# Modifying Fault Suppression Tasks for an Organization

## SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **scope fault-suppress-task** *name*
3. UCS-A/org/fault-suppress-task # **set schedule** *name*
4. UCS-A/org/fault-suppress-task # **scope local-schedule**
5. UCS-A/org/fault-suppress-task/local-schedule # **scope occurrence single-one-time**
6. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*
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*}
8. UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A/org # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode.<br>**Note** To apply a different schedule to the fault suppression task, go to Step 3. To change the fixed time interval of the fault suppression task, go to Step 4. |
| **Step 3** | UCS-A/org/fault-suppress-task # **set schedule** *name* | Applies a different schedule.<br>**Note** If you change from a fixed time interval to a schedule, the fixed time interval is deleted when you commit.<br>If you change from a schedule to a fixed time interval, the reference to the schedule is cleared when you commit. |
| **Step 4** | UCS-A/org/fault-suppress-task # **scope local-schedule** | Enters local-schedule mode. |
| **Step 5** | UCS-A/org/fault-suppress-task/local-schedule # **scope occurrence single-one-time** | Enters single-one-time mode. |
| **Step 6** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds* | Specifies the date and time that this occurrence should run. |
| **Step 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*} | Specifies the maximum length of time that this task can run. To run the task until it is manually stopped, enter none or omit this step. |
| **Step 8** | UCS-A/org/fault-suppress-task/local-schedule/single-one-time # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to change the date and the fault suppression policy of the fault suppression task called task2:

```
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
```

The following example shows how to apply a different schedule to the fault suppression task called task1:

```
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
```

## Viewing Suppressed Faults and Fault Suppression Tasks for an Organization

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **show fault suppressed**
3. UCS-A/org # **scope fault-suppress-task** *name*
4. UCS-A/org/fault-suppress-task # **show detail expand**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A/org # **show fault suppressed** | Displays the suppressed faults for the organization<br>**Note** Only faults owned by the selected component are displayed. |
| **Step 3** | UCS-A/org # **scope fault-suppress-task** *name* | Enters fault-suppress-task mode. |
| **Step 4** | UCS-A/org/fault-suppress-task # **show detail expand** | Displays the schedule or fixed time interval for the task. |

### Example

The following example shows how to display the suppressed faults for an organization:

```
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 #
```

The following example shows how to display the fault suppression task called task1:

```
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 #
```

## Deleting Fault Suppression Tasks for an Organization

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A/org # **delete fault-suppress-task** *name*
3. UCS-A/org # **commit-buffer**

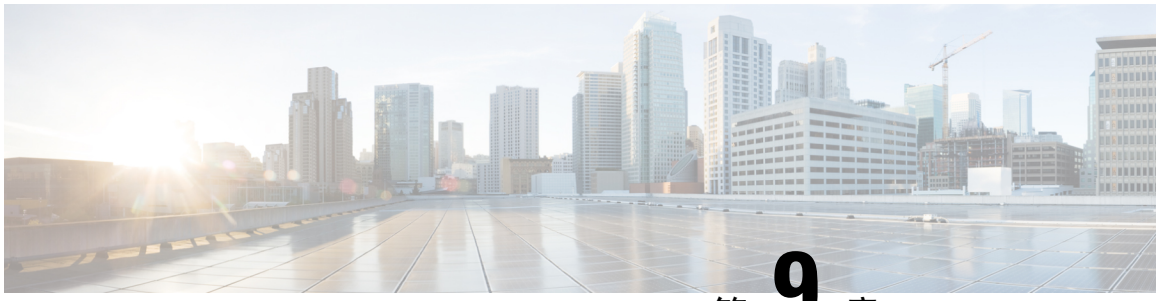
### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |
| **Step 2** | UCS-A/org # **delete fault-suppress-task** *name* | Deletes the specified fault suppression task. |
| **Step 3** | UCS-A/org # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example shows how to delete the fault suppression task called task1:

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



第 9 章

# SNMP の設定



## SNMP の概要

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

## SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム。
- SNMP エージェント： Cisco UCS 内のソフトウェア コンポーネント。 Cisco UCS のデータを維持し、必要に応じて SNMP マネージャにレポートします。Cisco UCS にはエージェントと MIB のコレクションが含まれます。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。
- Managed Information Base（MIB）：SNMPエージェントの管理対象オブジェクトの集合。 Cisco UCS リリース 1.4(1) 以降では、それ以前のリリースより大量の 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 モデルは選択されたセキュリティ レベルと組み合わされ、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

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権限を決定します。権限のレベルによって、メッセージが情報開示の保護を必要とするか、またはメッセージが認証されるかが決定されます。サポートされるセキュリティ レベルは、実装されているセキュリティ モデルによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

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

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

# SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせを示します。

表 *4: SNMP* セキュリティ モデルおよびセキュリティ レベル

| モデル | レベル | 認証 | 暗号化 | 結果 |
|---|---|---|---|---|
| v1 | noAuthNoPriv | コミュニティ ストリング | 未対応 | 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 | 未対応 | 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のみを承認します。SNMPv3 ユーザベース 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 Support

Cisco UCS provides the following support for SNMP:

### Support for MIBs

Cisco UCS supports read-only access to MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html for B-series servers, and http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html C-series servers.

### Authentication Protocols for SNMPv3 Users

Cisco UCS supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

### AES Privacy Protocol for SNMPv3 Users

Cisco UCS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Manager uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

# Configuring SNMP

## Enabling SNMP and Configuring SNMP Properties

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。

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **enable snmp**
3. UCS-A /monitoring # **set snmp community**
4. UCS-A /monitoring # **Enter a snmp community:** *community-name*
5. UCS-A /monitoring # **set snmp syscontact** *system-contact-name*
6. UCS-A /monitoring # **set snmp syslocation** *system-location-name*
7. UCS-A /monitoring # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **enable snmp** | Enables SNMP. |
| **Step 3** | UCS-A /monitoring # **set snmp community** | Enters snmp community mode. |
| **Step 4** | UCS-A /monitoring # **Enter a snmp community:** *community-name* | Specifies SNMP community. Use the community name as a password. The community name can be any alphanumeric string up to 32 characters. |
| **Step 5** | UCS-A /monitoring # **set snmp syscontact** *system-contact-name* | Specifies the system contact person responsible for the SNMP. The system contact name can be any alphanumeric string up to 255 characters, such as an email address or name and telephone number. |
| **Step 6** | UCS-A /monitoring # **set snmp syslocation** *system-location-name* | Specifies the location of the host on which the SNMP agent (server) runs. The system location name can be any alphanumeric string up to 512 characters. |
| **Step 7** | UCS-A /monitoring # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example enables SNMP, configures an SNMP community named SnmpCommSystem2, configures a system contact named contactperson, configures a contact location named systemlocation, and commits the transaction:

```
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

Create SNMP traps and users.

# Creating an SNMP Trap

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **enable snmp**
3. UCS-A /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}
4. UCS-A /monitoring/snmp-trap # **set community** *community-name*
5. UCS-A /monitoring/snmp-trap # **set port** *port-num*
6. UCS-A /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}
7. (Optional) UCS-A /monitoring/snmp-trap # **set notificationtype** {**traps** | **informs**}
8. (Optional) UCS-A /monitoring/snmp-trap # **set v3 privilege** {**auth** | **noauth** | **priv**}
9. UCS-A /monitoring/snmp-trap # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **enable snmp** | Enables SNMP. |
| **Step 3** | UCS-A /monitoring # **create snmp-trap** {*hostname* \| *ip-addr* \| *ip6-addr*} | Creates an SNMP trap host with the specified host name, IPv4 address, or IPv6 address.<br>The host name can be a fully qualified domain name of an IPv4 address. |
| **Step 4** | UCS-A /monitoring/snmp-trap # **set community** *community-name* | Specifies the SNMP community name to be used for the SNMP trap. |
| **Step 5** | UCS-A /monitoring/snmp-trap # **set port** *port-num* | Specifies the port to be used for the SNMP trap. |
| **Step 6** | UCS-A /monitoring/snmp-trap # **set version** {**v1** \| **v2c** \| **v3**} | Specifies the SNMP version and model used for the trap. |
| **Step 7** | (Optional) UCS-A /monitoring/snmp-trap # **set notificationtype** {**traps** \| **informs**} | The type of trap to send. If you select v2c or v3 for the version, this can be:<br>• **traps**—SNMP trap notifications |

| | Command or Action | Purpose |
|---|---|---|
| | | • **informs**—SNMP inform notifications |
| **Step 8** | (Optional) UCS-A /monitoring/snmp-trap # **set v3 privilege** {**auth** \| **noauth** \| **priv**} | If you select v3 for the version, the privilege associated with the trap can be<br>• **auth**—Authentication but no encryption<br>• **noauth**—No authentication or encryption<br>• **priv**—Authentication and encryption |
| **Step 9** | UCS-A /monitoring/snmp-trap # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example enables SNMP, creates an SNMP trap using an IPv4 address, specifies that the trap will use the SnmpCommSystem2 community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
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 #
```

The following example enables SNMP, creates an SNMP trap using an IPv6 address, specifies that the trap will use the SnmpCommSystem3 community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
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 #
```

# Deleting an SNMP Trap

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}
3. UCS-A /monitoring # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **delete snmp-trap** {*hostname* \| *ip-addr*} | Deletes the specified SNMP trap host with the specified hostname or IP address. |
| **Step 3** | UCS-A /monitoring # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example deletes the SNMP trap at IP address 192.168.100.112 and commits the transaction:

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

# Generating Test SNMP Traps

You can generate a test SNMP trap without making any software or physical configuration change to the system.

### SUMMARY STEPS

1. connect nxos
2. (nxos)# **test pfm snmp test-trap** ?
3. (nxos)# **test pfm snmp test-trap**{fan | powersupply | temp_sensor}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | connect nxos | Connects to the NX-OS operating system software. |
| **Step 2** | (nxos)# **test pfm snmp test-trap** ? | Returns the list of test trap options. |
| **Step 3** | (nxos)# **test pfm snmp test-trap**{fan \| powersupply \| temp_sensor} | Generates a test SNMP trap.<br>• fan - Generate a test SNMP Trap for fan<br>• powersupply -Generate a test SNMP Trap for Power Supply.<br>• temp_sensor - Generate a test SNMP Trap for Temperature. |

### What to do next

While you run the NX-OS command, you can open another SSH session to the fabric interconnect and verify that SNMP packets are sent out from the fabric interconnect's management interface.

**For complete packet:**

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

**To capture just packet headers**

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

# Creating an SNMPv3 User

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **enable snmp**
3. UCS-A /monitoring # **create snmp-user** *user-name*
4. UCS-A /monitoring/snmp-user # **set aes-128** {**no** | **yes**}
5. UCS-A /monitoring/snmp-user # **set auth** {**md5** | **sha**}
6. UCS-A /monitoring/snmp-user # **set password**
7. UCS-A /monitoring/snmp-user # **set priv-password**
8. UCS-A /monitoring/snmp-user # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **enable snmp** | Enables SNMP. |
| **Step 3** | UCS-A /monitoring # **create snmp-user** *user-name* | Creates the specified SNMPv3 user.<br>An SNMP username cannot be the same as a local username. Choose an SNMP username that does not match a local username. |
| **Step 4** | UCS-A /monitoring/snmp-user # **set aes-128** {**no** \| **yes**} | Enables or disables the use of AES-128 encryption. |
| **Step 5** | UCS-A /monitoring/snmp-user # **set auth** {**md5** \| **sha**} | Specifies the use of MD5 or DHA authentication. |
| **Step 6** | UCS-A /monitoring/snmp-user # **set password** | Specifies the user password. After you enter the **set password** command, you are prompted to enter and confirm the password. |
| **Step 7** | UCS-A /monitoring/snmp-user # **set priv-password** | Specifies the user privacy password. After you enter the **set priv-password** command, you are prompted to enter and confirm the privacy password. |
| **Step 8** | UCS-A /monitoring/snmp-user # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example enables SNMP, creates an SNMPv3 user named snmp-user14, disables AES-128 encryption, specifies the use of MD5 authentication, sets the password and privacy password, and commits the transaction:

```
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 #
```

# Deleting an SNMPv3 User

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **delete snmp-user** *user-name*
3. UCS-A /monitoring # **commit-buffer**

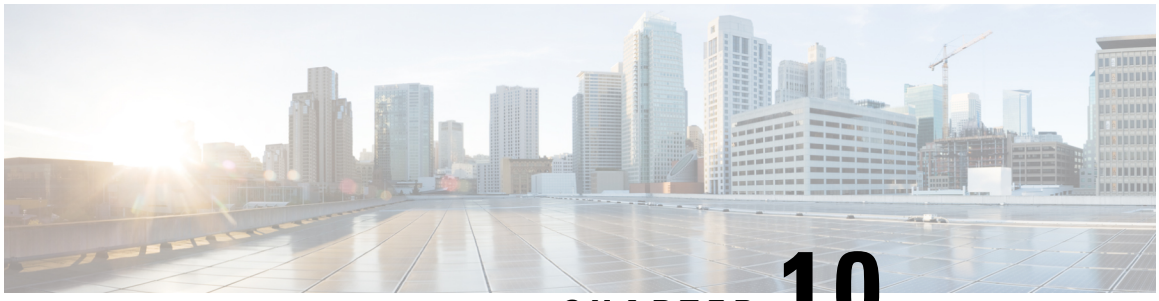
### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **delete snmp-user** *user-name* | Deletes the specified SNMPv3 user. |
| **Step 3** | UCS-A /monitoring # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example deletes the SNMPv3 user named snmp-user14 and commits the transaction:

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



CHAPTER 10

# SPDM Security



## SPDM Security

Cisco UCS M6 Servers can contain mutable components that could provide vectors for attack against a device itself or use of a device to attack another device within the system. To defend against these attacks, the Security Protocol and Data Model (SPDM) Specification enables a secure transport implementation that challenges a device to prove its identity and the correctness of its mutable component configuration. This feature is supported on Cisco UCS C220 and C240 M6 Servers starting with in Cisco UCS Manager, Release 4.2(1d).

**Note** SPDM is currently not supported on the Cisco UCS C225 M6サーバ and Cisco UCS C245 M6サーバ.

SPDM defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. It orchestrates message exchanges between Baseboard Management Controllers (BMC) and end-point devices over a Management Component Transport Protocol (MCTP). Message exchanges include authentication of hardware identities accessing the BMC. The SPDM enables access to low-level security capabilities and operations by specifying a managed level for device authentication, firmware measurement, and certificate management. Endpoint devices are challenged to provide authentication. and BMC authenticates the endpoints and only allows access for trusted entities.

The UCS Manager optionally allows uploads of external security certificates to BMC. A maximum of 40 SPDM certificates is allowed, including native internal certificates. Once the limit is reached, no more certificates can be uploaded. User uploaded certificates can be deleted but internal/default certificates cannot.

A SPDM security policy allows you to specify one of three Security level settings. Security can be set at one of the three levels listed below:

- Full Security:

  This is the highest MCTP security setting. When you select this setting, a fault is generated when any endpoint authentication failure or firmware measurement failure is detected. A fault will also be generated if any of the endpoints do not support either endpoint authentication or firmware measurements.

- Partial Security (default):

  When you select this setting, a fault is generated when any endpoint authentication failure or firmware measurement failure is detected. There will NOT be a fault generated when the endpoint doesn't support endpoint authentication or firmware measurements.

- No Security

  When you select this setting, there will NOT be a fault generated for any failure (either endpoint measurement or firmware measurement failures).

You can also upload the content of one or more external/device certificates into BMC. Using a SPDM policy allows you to change or delete security certificates or settings as desired. Certificates can be deleted or replaced when no longer needed.

Certificates are listed in all user interfaces on a system.

# Creating and Configuring a SPDM Security Certificate Policy using CLI

A Security Protocol and Data Model (SPDM) policy can be created to present security alert-level and certificate contents to BMC for authentication.

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **create spdm-certificate-policy** *policy-name*
3. UCS-A /org/spdm-certificate-policy* # **set fault-alert** {**full** | **partial** | **no**}
4. (Optional) UCS-A /org/spdm-certificate-policy* # **set descr** *description*
5. UCS-A /org/spdm-certificate-policy* # **create certificate** *certificate-name*
6. UCS-A /org/spdm-certificate-policy* # **set content**
7. UCS-A /org/spdm-certificate-policy # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type **/** as the *org-name* . |
| **Step 2** | UCS-A /org # **create spdm-certificate-policy** *policy-name* | Creates a SPDM security certificate policy with the specified policy name, and enters organization SPDM certificate policy mode.<br>**Note** The only supported certificate type is **pem**. |
| **Step 3** | UCS-A /org/spdm-certificate-policy* # **set fault-alert** {**full** \| **partial** \| **no**} | Configures the fault alert level for this policy. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | (Optional) UCS-A /org/spdm-certificate-policy* # **set descr** *description* | Provides a description for the SPDM security certificate policy.<br>**Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output. |
| **Step 5** | UCS-A /org/spdm-certificate-policy* # **create certificate** *certificate-name* | |
| **Step 6** | UCS-A /org/spdm-certificate-policy* # **set content** | This prompts for the content of the outside certificate. Enter certificate content one line at a time. After End of Certificate, enter ENDOFBUF at the prompt to return to the command line.<br>**Note** To exit without commiting the certificate content, enter **C**. |
| **Step 7** | UCS-A /org/spdm-certificate-policy # **commit-buffer** | Commits the transaction to the system configuration. |

### What to do next

Assign outside security certificates, if desired.

# Displaying the Security Policy Fault Alert Level

After the policy is created, you can check the alert level for the SPDM policy.

### SUMMARY STEPS

1. UCS-A /org/spdm-certificate-policy # **show fault-alert**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /org/spdm-certificate-policy # **show fault-alert**<br>**Example:**<br>`UCS-A /server/cimc/spdm-certificate #show fault-alert` | The returned result shows that the setting for this SPDM policy is Partial, the default.<br>`SPDM Fault Alert Setting: Partial` |

# Loading an Outside SPDM Security Certificate Policy

The SPDM allows you to download an outside security certificate.

### Before you begin

Create a SPDM security certificate policy.

### SUMMARY STEPS

1. UCS-A /org # **scope spdm-certificate-policy**
2. UCS-A org/spdm-certificate-policy# **create spdm-cert** *Certificate name*
3. UCS-A /org/spdm-certificate-policy* # **set** {*certificate* }
4. UCS-A /org/spdm-certificate-policy # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /org # **scope spdm-certificate-policy** | Enters SPDM security certificate policy mode. |
| **Step 2** | UCS-A org/spdm-certificate-policy# **create spdm-cert** *Certificate name* | Creates a SPDM security certificate policy for the specified external certificate,. |
| **Step 3** | UCS-A /org/spdm-certificate-policy* # **set** {*certificate* } | Specifying certificate prompts for the content of the outside certificate. The only supported certificate type is **pem**. |
| **Step 4** | UCS-A /org/spdm-certificate-policy # **commit-buffer** | Commits the transaction to the system configuration. |

The following example shows loading a certificate for Broadcom of type PEM.

### Example

```
UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert?
Name - Certificate name

UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert Broadcom
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set?
certificate - Certificate content

UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set certificate
{enter certificate content}
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # commit-buffer
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert# show detail
SPDM Certificate:
Name: Broadcom
Certificate Type: pem
Certificate Content:
```

# Viewing the Certificate Inventory

You can view what SPDM certificates have been uploaded and also request further details for a specified certificate.

## SUMMARY STEPS

1. UCS-A # **scope server** *server*
2. UCS-A/server # **scope cimc** *server*
3. UCS-A/server/cimc # **scope spdm** *server*
4. UCS-A/server/cimc/spdm # **show certificate**
5. UCS-A/server/cimc/spdm # **show certificate** *certificate-id***detail**
6. UCS-A /org/spdm-certificate-policy/certificate # **show**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope server** *server* | |
| **Step 2** | UCS-A/server # **scope cimc** *server* | |
| **Step 3** | UCS-A/server/cimc # **scope spdm** *server* | |
| **Step 4** | UCS-A/server/cimc/spdm # **show certificate** | The returned result shows the certificate inventory. |
| **Step 5** | UCS-A/server/cimc/spdm # **show certificate** *certificate-id***detail**<br>**Example:**<br>`UCS-A /server/cimc/spdm-certificate #show certificate 3 detail`<br>`Certificate Information`<br>`Certificate Id : 3`<br>`Subject Country Code (C) : US`<br>`Subject State (ST) : Colorado`<br>`Subject Organization (O) : Broadcom Inc.`<br>`Subject Organization Unit(OU) : NA`<br>`Subject Common Name (CN) : NA`<br>`Issuer Country Code (C) : US`<br>`Issuer State (ST) : Colorado`<br>`Issuer City (L) : Colorado Springs`<br>`Issuer Organization (O) : Broadcom Inc.`<br>`Issuer Organization Unit(OU) : NA`<br>`Issuer Common Name (CN) : NA`<br>`Valid From : Oct 23 00:25:13 2019 GMT`<br>`Valid To : Apr 8 10:36:14 2021 GMT`<br>`UserUploaded : Yes`<br>`Certificate Content : <Certificate String>`<br>`Certificate Type : PEM` | The returned result shows the certificate ID, identifiers, and expiration date. |
| **Step 6** | UCS-A /org/spdm-certificate-policy/certificate # **show**<br>**Example:**<br>`SPDM Certificate:`<br>`Name SPDM Certificate Type`<br>`---------- ------------------------------`<br>`cert1 Pem`<br>**Example:** | The returned result shows the type of certificate details.<br>The returned result shows the fault alert setting. |

| | Command or Action | Purpose |
|---|---|---|
| | UCS-A /server/cimc/spdm-certificate/certificate #up<br>UCS-A /server/cimc/spdm-certificate #show<br><br>SPDM Certificate Policy:<br>Name Fault Alert Setting<br>---------- ----------<br><br>Broadcom Full | |

# Deleting a SPDM Policy

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **delete spdm-certificate-policy** *policy-name*
3. UCS-A /org # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name. |
| **Step 2** | UCS-A /org # **delete spdm-certificate-policy** *policy-name* | Deletes the specified SPDM control policy. |
| **Step 3** | UCS-A /org # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example deletes a power control policy called VendorPolicy2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete spdm-certificate-policy VendorPolicy2
UCS-A /org* # commit-buffer
UCS-A /org #
```

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

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。

# Configuring a Statistics Collection Policy

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A/monitoring # **scope stats-collection-policy** {**adapter** | **chassis** | **host** | **port** | **server**}
3. UCS-A /monitoring/stats-collection-policy # **set collection-interval** {**1minute** | **2minutes** | **30seconds** | **5minutes**}
4. UCS-A /monitoring/stats-collection-policy # **set reporting-interval** {**15minutes** | **30minutes** | **60minutes**}
5. UCS-A /monitoring/stats-collection-policy # **commit-buffer**

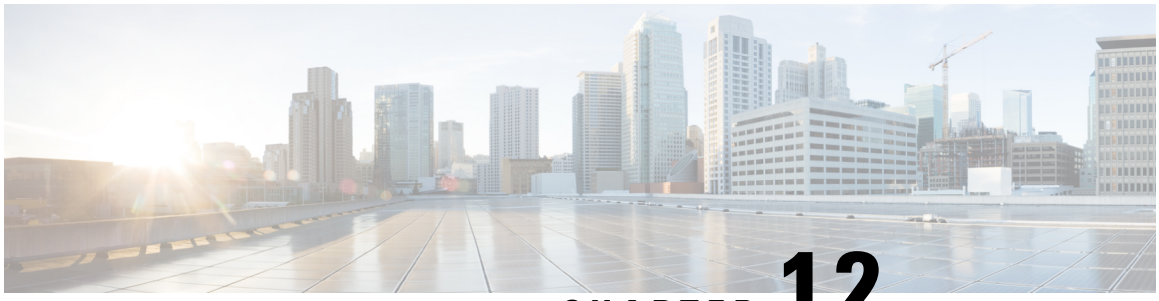
### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope stats-collection-policy** {**adapter** \| **chassis** \| **host** \| **port** \| **server**} | Enters statistics collection policy mode for the specified policy type. |
| **Step 3** | UCS-A /monitoring/stats-collection-policy # **set collection-interval** {**1minute** \| **2minutes** \| **30seconds** \| **5minutes**} | Specifies the interval at which statistics are collected from the system. |
| **Step 4** | UCS-A /monitoring/stats-collection-policy # **set reporting-interval** {**15minutes** \| **30minutes** \| **60minutes**} | Specifies the interval at which collected statistics are reported. |
| **Step 5** | UCS-A /monitoring/stats-collection-policy # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example creates a statistics collection policy for ports, sets the collection interval to one minute, the reporting interval to 30 minutes, and commits the transaction:

```
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

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 ベースの自動化された解析アプリケーションとの互換性のために、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。

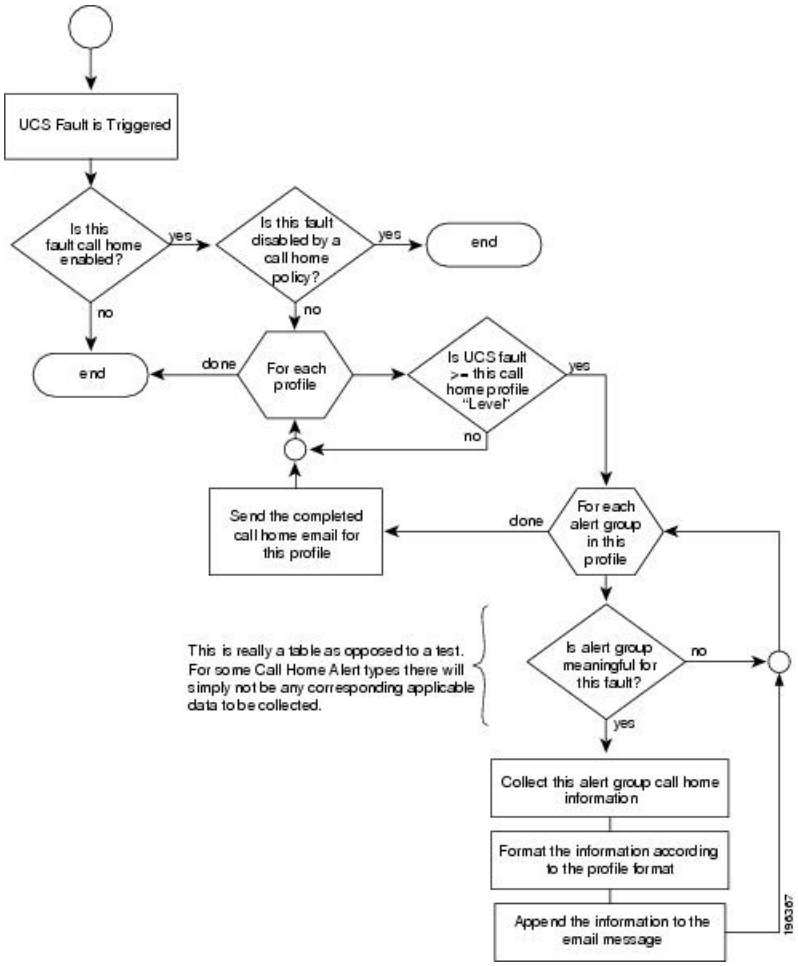
Cisco UCS では、Call Home メッセージが次のフォーマットで配信されます。

- 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 フォーマットでは、シスコの TAC との通信が可能になります。

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

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

図 *2:* 障害発生後のイベントの流れ




# Call Home の考慮事項とガイドライン

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

### 宛先プロファイル

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

宛先プロファイルで電子メール メッセージ配信を使用する場合は、Call Home を設定するときにシンプル メール転送プロトコル（SMTP）サーバ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 サーバまたは HTTP サーバへの IP 接続

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

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

### Smart Call Home

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

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

# Cisco UCSの障害と Call Home の重大度

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 の重大度とのマッピングを示します。Call Home のプロファイルにレベルを設定するときには、このマッピングを理解しておくことが必要です。

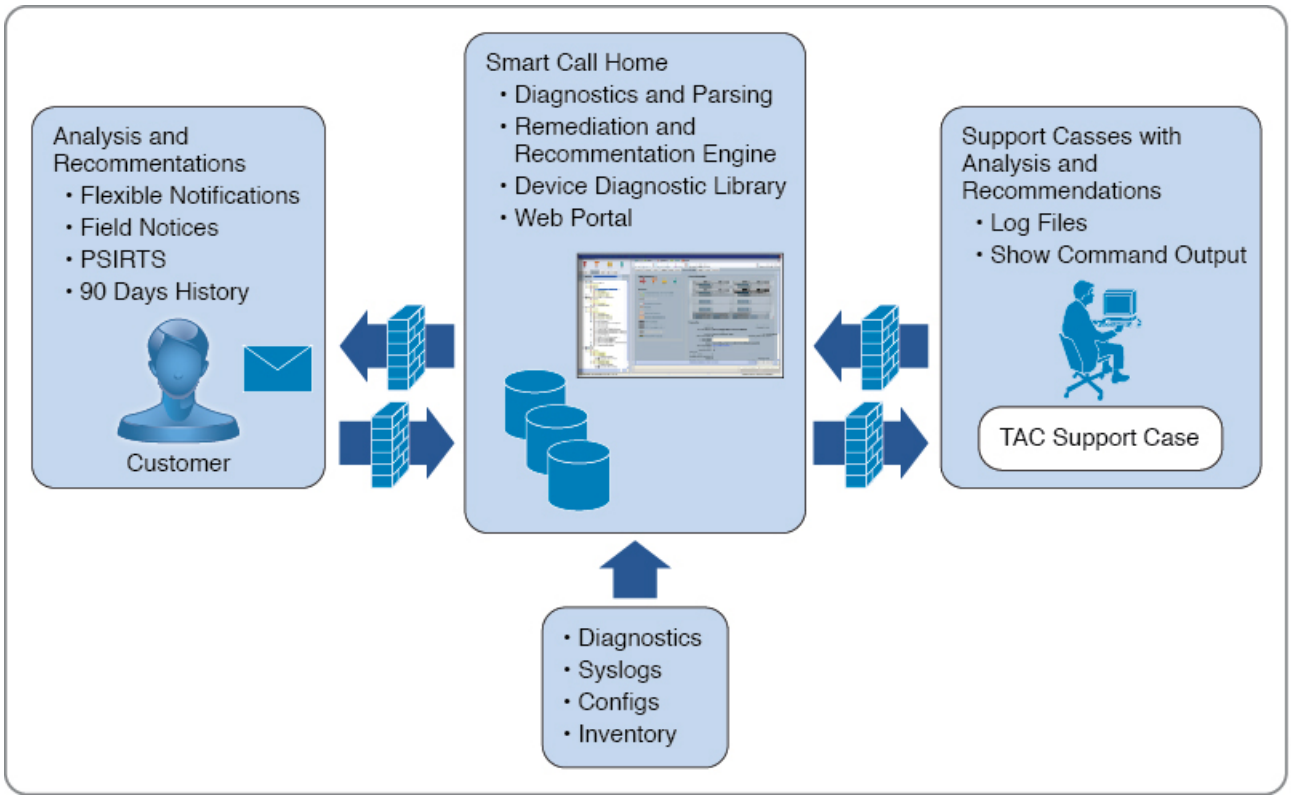
表 *5:* 障害と *Call Home* の重大度のマッピング

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

# Cisco Smart Call Home

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

図 *3 : Cisco Smart Call Home* の機能




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

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

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

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

Smart Call Home を設定するには、次の手順を実行します。

- Smart Call Home 機能をイネーブルにします。

- 連絡先情報を設定します。
- 電子メール情報を設定します。
- SMTP サーバ情報を設定します。
- デフォルトの CiscoTAC-1 プロファイルを設定します。
- 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。

# 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。

# Configuring Call Home

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **enable**
4. UCS-A /monitoring/callhome # **set contact** *name*
5. UCS-A /monitoring/callhome # **set email** *email-addr*
6. UCS-A /monitoring/callhome # **set phone-contact** *phone-num*
7. UCS-A /monitoring/callhome # **set street-address** *street-addr*
8. UCS-A /monitoring/callhome # **set customer-id** *id-num*
9. UCS-A /monitoring/callhome # **set contract-id** *id-num*
10. UCS-A /monitoring/callhome # **set site-id** *id-num*
11. UCS-A /monitoring/callhome # **set from-email** *email-addr*
12. UCS-A /monitoring/callhome # **set reply-to-email** *email-addr*
13. UCS-A /monitoring/callhome # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}
14. UCS-A /monitoring/callhome # **set port** *port-num*
15. UCS-A /monitoring/callhome # **set throttling** {**off** | **on**}
16. UCS-A /monitoring/callhome # **set urgency** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **information** | **notifications** | **warnings**}

17. UCS-A /monitoring/callhome # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **enable** | Enables Call Home. |
| **Step 4** | UCS-A /monitoring/callhome # **set contact** *name* | Specifies the name of the main Call Home contact person. |
| **Step 5** | UCS-A /monitoring/callhome # **set email** *email-addr* | Specifies the email address of the main Call Home contact person.<br>**Note** 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。 |
| **Step 6** | UCS-A /monitoring/callhome # **set phone-contact** *phone-num* | Specifies the phone number of the main Call Home contact person. The phone number must be in international format, starting with a + (plus sign) and a country code. |
| **Step 7** | UCS-A /monitoring/callhome # **set street-address** *street-addr* | Specifies the street address of the main Call Home contact person.<br>Enter up to 255 ASCII characters. |
| **Step 8** | UCS-A /monitoring/callhome # **set customer-id** *id-num* | Specifies the CCO identification number that includes the contract numbers for the support contract in its entitlements. The number can be up to 255 alphanumeric characters in free format. |
| **Step 9** | UCS-A /monitoring/callhome # **set contract-id** *id-num* | Specifies the contract identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| **Step 10** | UCS-A /monitoring/callhome # **set site-id** *id-num* | Specifies the site identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| **Step 11** | UCS-A /monitoring/callhome # **set from-email** *email-addr* | Specifies the email address to use for the **From** field in Call Home messages. |
| **Step 12** | UCS-A /monitoring/callhome # **set reply-to-email** *email-addr* | Specifies the email address to use for the **Reply To** field in Call Home messages. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | UCS-A /monitoring/callhome # **set hostname** {*hostname* \| *ip-addr* \| *ip6-addr*} | Specifies the hostname, IPv4 or IPv6 address of the SMTP server that Call Home uses to send email messages. |
| **Step 14** | UCS-A /monitoring/callhome # **set port** *port-num* | Specifies the SMTP server port that Call Home uses to send email messages. Valid port numbers are 1 to 65535. |
| **Step 15** | UCS-A /monitoring/callhome # **set throttling** {**off** \| **on**} | Enables or disables Call Home throttling. When enabled, throttling prevents too many Call Home email messages from being sent for the same event. By default, throttling is enabled. |
| **Step 16** | UCS-A /monitoring/callhome # **set urgency** {**alerts** \| **critical** \| **debugging** \| **emergencies** \| **errors** \| **information** \| **notifications** \| **warnings**} | Specifies the urgency level for Call Home email messages. In the context of a large UCS deployment with several pairs of fabric interconnects, the urgency level potentially allows you to attach significance to Call Home messages from one particular Cisco UCS ドメイン versus another. In the context of a small UCS deployment involving only two fabric interconnects, the urgency level holds little meaning. |
| **Step 17** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example configures Call Home with and IPv4 hostname and commits the transaction:

```
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 #
```

The following example configures Call Home with and IPv6 hostname and commits the transaction:

```
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 #
```

# Enabling Call Home

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **enable**
4. UCS-A /monitoring/callhome # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **enable** | Enables Call Home. |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example enables Call Home and commits the transaction:

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

# Disabling Call Home

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **disable**

4. UCS-A /monitoring/callhome # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **disable** | Enables Call Home. |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

**Example**

The following example disables Call Home and commits the transaction:

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

# Configuring System Inventory Messages

## Configuring System Inventory Messages

**SUMMARY STEPS**

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope inventory**
4. UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** | **on**}
5. UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num*
6. UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour*
7. UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute*
8. UCS-A /monitoring/callhome/inventory # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope inventory** | Enters monitoring call home inventory mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** \| **on**} | Enables or disables the sending of inventory messages. When the **on** keyword is specified, inventory messages are automatically sent to the Call Home database. |
| **Step 5** | UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num* | Specifies the time interval (in days) at which inventory messages will be sent. |
| **Step 6** | UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour* | Specifies the hour (using 24-hour format) that inventory messages are sent. |
| **Step 7** | UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute* | Specifies the number of minutes after the hour that inventory messages are sent. |
| **Step 8** | UCS-A /monitoring/callhome/inventory # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example configures Call Home system inventory messages and commits the transaction:

```
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 #
```

# Sending a System Inventory Message

Use this procedure if you need to manually send a system inventory message outside of the scheduled messages.

**Note** The system inventory message is sent only to those recipients defined in CiscoTAC-1 profile.

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope inventory**
4. UCS-A /monitoring/callhome/inventory # **send**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope inventory** | Enters monitoring call home inventory mode. |
| **Step 4** | UCS-A /monitoring/callhome/inventory # **send** | Sends the system inventory message to the Call Home database. |

**Example**

The following example sends the system inventory message to the Call Home database:

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

# Configuring Call Home Profiles

## 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 グループでは、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 Call Home アラートのセットを選択できます。 Cisco UCS Manager は、次の条件でのみ、宛先プロファイルの電子メールの宛先に Call Home アラートを送信します。

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

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

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

# Configuring a Call Home Profile

By default, you must configure the Cisco TAC-1 profile, However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **create profile** *profile-name*
4. UCS-A /monitoring/callhome/profile # **set level** {**critical** | **debug** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}
5. UCS-A /monitoring/callhome/profile # **set alertgroups** *group-name*

- **ciscotac**
- **diagnostic**
- **environmental**
- **inventory**
- **license**
- **lifecycle**
- **linecard**
- **supervisor**
- **syslogport**
- **system**
- **test**

6. (Optional) UCS-A /monitoring/callhome/profile # **add alertgroups** *group-names*
7. UCS-A /monitoring/callhome/profile # **set format** {**shorttxt** | **xml**}
8. UCS-A /monitoring/callhome/profile # **set maxsize** *id-num*
9. UCS-A /monitoring/callhome/profile # **create destination** *email-addr*
10. UCS-A /monitoring/callhome/profile/destination # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **create profile** *profile-name* | Enters monitoring call home profile mode. |
| **Step 4** | UCS-A /monitoring/callhome/profile # **set level** {**critical** \| **debug** \| **disaster** \| **fatal** \| **major** \| **minor** \| **normal** \| **notification** \| **warning**} | Specifies the event level for the profile. Each profile can have its own unique event level.<br>Cisco UCS faults that are greater than or equal to the event level will trigger this profile. |
| **Step 5** | UCS-A /monitoring/callhome/profile # **set alertgroups** *group-name*<br>• **ciscotac**<br>• **diagnostic**<br>• **environmental**<br>• **inventory**<br>• **license**<br>• **lifecycle**<br>• **linecard**<br>• **supervisor**<br>• **syslogport**<br>• **system**<br>• **test** | Specifies one or more groups that are alerted based on the profile. The *group-name* argument can be one or more of the following keywords entered on the same command line: |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | (Optional) UCS-A /monitoring/callhome/profile # **add alertgroups** *group-names* | Adds one or more groups to the existing list of groups that are alerted based on the Call Home profile.<br>**Note** You must use the **add alertgroups** command to add more alert groups to the existing alert group list. Using the **set alertgroups** command will replace any pre-existing alert groups with a new group list. |
| **Step 7** | UCS-A /monitoring/callhome/profile # **set format** {**shorttxt** \| **xml**} | Specifies the formatting method to use for the e-mail messages. |
| **Step 8** | UCS-A /monitoring/callhome/profile # **set maxsize** *id-num* | Specifies the maximum size (in characters) of the email message. |
| **Step 9** | UCS-A /monitoring/callhome/profile # **create destination** *email-addr* | Specifies the email address to which Call Home alerts should be sent. This email address receives Callhome Alerts/Faults. Use multiple **create destination** commands in monitoring call home profile mode to specify multiple email recipients. Use the **delete destination** command in monitoring call home profile mode to delete a specified email recipient. |
| **Step 10** | UCS-A /monitoring/callhome/profile/destination # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example configures a Call Home profile and commits the transaction:

```
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 #
```

# Deleting a Call Home Profile

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **delete profile** *profile-name*
4. UCS-A /monitoring/callhome # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **delete profile** *profile-name* | Deletes the specified profile. |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example deletes the Call Home profile named TestProfile and commits the transaction:

```
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 #
```

# Sending a Test Call Home Alert

#### Before you begin

Configure Call Home and a Call Home Profile.

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
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** | **test**}] [**alert-description** *description*]}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 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** | Sends a test Call Home alert. The test Call Home alert must specify all **alert-*** parameters or Cisco UCS Manager cannot generate the test message. The **alert-*** parameters include the following:<br>• **alert-description**—Alert description |

| | Command or Action | Purpose |
|---|---|---|
| | \| **full** \| **goldmajor** \| **goldminor** \| **goldnormal** \| **major** \| **minor** \| **nosubtype** \| **test**}] [**alert-description** *description*]} | • **alert-group**—Alert group<br>• **alert-level**—Event severity level<br>• **alert-message-type**—Message type<br>• **alert-message-subtype**—Message subtype<br>When a test Call Home alert is sent, Call Home responds as it would to any other alert and delivers it to the configured destination email addresses. |

**Example**

The following example sends a test Call Home alert to the configured destination email address of the environmental alert group:

```
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"
```

# Configuring Call Home Policies

## 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。

## Configuring a Call Home Policy

**Tip** By default, email alerts are sent for all critical system events. However, you can optionally configure Call Home policies to enable or disable sending email alerts for other critical system events.

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **create policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}
4. UCS-A /monitoring/callhome/policy # {**disabled** | **enabled**}
5. UCS-A /monitoring/callhome/policy # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **create policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Creates the specified policy and enters monitoring call home policy mode. |
| **Step 4** | UCS-A /monitoring/callhome/policy # {**disabled** \| **enabled**} | Disables or enables the sending of email alerts for the specified policy. |
| **Step 5** | UCS-A /monitoring/callhome/policy # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example creates a Call Home policy that disables the sending of email alerts for system events pertaining to voltage problems and commits the transaction:

```
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 #
```

# Disabling a Call Home Policy

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}
4. UCS-A /monitoring/callhome/policy # **disable**
5. UCS-A /monitoring/callhome/policy # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Enters monitoring call home policy mode for the specified policy. |
| **Step 4** | UCS-A /monitoring/callhome/policy # **disable** | Disables the specified policy. |
| **Step 5** | UCS-A /monitoring/callhome/policy # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example disables the Call Home policy named voltage-problem and commits the transaction:

```
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 #
```

# Enabling a Call Home Policy

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}
4. UCS-A /monitoring/callhome/policy # **enable**
5. UCS-A /monitoring/callhome/policy # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Enters monitoring call home policy mode for the specified policy. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A /monitoring/callhome/policy # **enable** | Enables the specified policy. |
| **Step 5** | UCS-A /monitoring/callhome/policy # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example enables the Call Home policy named voltage-problem and commits the transaction:

```
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 #
```

# Deleting a Call Home Policy

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **delete policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}
4. UCS-A /monitoring/callhome # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **delete policy** {**equipment-inoperable** \| **fru-problem** \| **identity-unestablishable** \| **thermal-problem** \| **voltage-problem**} | Deletes the specified policy |
| **Step 4** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example deletes the Call Home policy named voltage-problem and commits the transaction:

```
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 #
```

# Configuring Anonymous Reporting

## Enabling Anonymous Reporting

### SUMMARY STEPS

1. UCS-A # **scope monitoring**
2. UCS-A/monitoring # **scope callhome**
3. (Optional) UCS-A/monitoring/callhome # **show anonymous-reporting**
4. UCS-A/monitoring/callhome # **enable anonymous-reporting**
5. UCS-A/monitoring/callhome # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | (Optional) UCS-A/monitoring/callhome # **show anonymous-reporting** | Displays if anonymous reporting is enabled or disabled. |
| **Step 4** | UCS-A/monitoring/callhome # **enable anonymous-reporting** | Enables anonymous reporting on Smart Call Home. |
| **Step 5** | UCS-A/monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example shows how to enable anonymous reporting on the Call Home server:

```
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
```

# Disabling Anonymous Reporting

### SUMMARY STEPS

1. UCS-A # **scope monitoring**
2. UCS-A/monitoring # **scope callhome**
3. (Optional) UCS-A/monitoring/callhome # **show anonymous-reporting**
4. UCS-A/monitoring/callhome # **disable anonymous-reporting**
5. UCS-A/monitoring/callhome # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | (Optional) UCS-A/monitoring/callhome # **show anonymous-reporting** | Displays if anonymous reporting is enabled or disabled. |
| **Step 4** | UCS-A/monitoring/callhome # **disable anonymous-reporting** | Disables anonymous reporting on the Smart Call Home server. |
| **Step 5** | UCS-A/monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example shows how to disable anonymous reporting on the Call Home server:

```
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
```

# Viewing Anonymous Reports

### SUMMARY STEPS

1. UCS-A # **scope monitoring**
2. UCS-A/monitoring # **scope callhome**

3. UCS-A/monitoring/callhome # **scope anonymous-reporting**
4. UCS-A/monitoring/callhome/anonymous-reporting # **show detail**
5. UCS-A/monitoring/callhome/anonymous-reporting # **show inventory**
6. UCS-A/monitoring/callhome/anonymous-reporting # **show content**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A/monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A/monitoring/callhome # **scope anonymous-reporting** | Enters anonymous reporting mode. |
| **Step 4** | UCS-A/monitoring/callhome/anonymous-reporting # **show detail** | Displays the SMTP server address and server port. |
| **Step 5** | UCS-A/monitoring/callhome/anonymous-reporting # **show inventory** | Displays the anonymous reporting information. |
| **Step 6** | UCS-A/monitoring/callhome/anonymous-reporting # **show content** | Displays the anonymous report sample information. |

### Example

The following example shows how to display anonymous reports from the Call Home server:

```
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"
```

# Configuring Smart Call Home

## Configuring Smart Call Home

### SUMMARY STEPS

1. UCS-A# **scope monitoring**
2. UCS-A /monitoring # **scope callhome**
3. UCS-A /monitoring/callhome # **enable**
4. UCS-A /monitoring/callhome # **set contact** *name*
5. UCS-A /monitoring/callhome # **set email** *email-addr*
6. UCS-A /monitoring/callhome # **set phone-contact** *phone-num*
7. UCS-A /monitoring/callhome # **set street-address** *street-addr*
8. UCS-A /monitoring/callhome # **set customer-id** *id-num*
9. UCS-A /monitoring/callhome # **set contract-id** *id-num*
10. UCS-A /monitoring/callhome # **set site-id** *id-num*
11. UCS-A /monitoring/callhome # **set from-email** *email-addr*
12. UCS-A /monitoring/callhome # **set reply-to-email** *email-addr*
13. UCS-A /monitoring/callhome # **set hostname** {*hostname* | *ip-addr*}
14. UCS-A /monitoring/callhome # **set port** *port-num*
15. UCS-A /monitoring/callhome # **set throttling** {**off** | **on**}
16. UCS-A /monitoring/callhome # **set urgency** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **information** | **notifications** | **warnings**}
17. UCS-A /monitoring/callhome # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope monitoring** | Enters monitoring mode. |
| **Step 2** | UCS-A /monitoring # **scope callhome** | Enters monitoring call home mode. |
| **Step 3** | UCS-A /monitoring/callhome # **enable** | Enables Call Home. |
| **Step 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。 |
| **Step 5** | UCS-A /monitoring/callhome # **set email** *email-addr* | Specifies the email address of the main Call Home contact person.<br>Cisco Smart Call Home sends the registration email to this email address. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A /monitoring/callhome # **set phone-contact** *phone-num* | Specifies the phone number of the main Call Home contact person. The phone number must be in international format, starting with a + (plus sign) and a country code. |
| **Step 7** | UCS-A /monitoring/callhome # **set street-address** *street-addr* | Specifies the street address of the main Call Home contact person. |
| **Step 8** | UCS-A /monitoring/callhome # **set customer-id** *id-num* | Specifies the CCO identification number that includes the contract numbers for the support contract in its entitlements. The number can be up to 255 alphanumeric characters in free format. |
| **Step 9** | UCS-A /monitoring/callhome # **set contract-id** *id-num* | Specifies the contract identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| **Step 10** | UCS-A /monitoring/callhome # **set site-id** *id-num* | Specifies the site identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| **Step 11** | UCS-A /monitoring/callhome # **set from-email** *email-addr* | Specifies the email address to use for the From field in Call Home messages. |
| **Step 12** | UCS-A /monitoring/callhome # **set reply-to-email** *email-addr* | Specifies the email address to use for the Reply To field in Call Home messages. |
| **Step 13** | UCS-A /monitoring/callhome # **set hostname** {*hostname* \| *ip-addr*} | Specifies the hostname or IP address of the SMTP server that Call Home uses to send email messages. |
| **Step 14** | UCS-A /monitoring/callhome # **set port** *port-num* | Specifies the SMTP server port that Call Home uses to send email messages. Valid port numbers are 1 to 65535. |
| **Step 15** | UCS-A /monitoring/callhome # **set throttling** {**off** \| **on**} | Enables or disables Call Home throttling. When enabled, throttling prevents too many Call Home email messages from being sent for the same event. By default, throttling is enabled. |
| **Step 16** | UCS-A /monitoring/callhome # **set urgency** {**alerts** \| **critical** \| **debugging** \| **emergencies** \| **errors** \| **information** \| **notifications** \| **warnings**} | Specifies the urgency level for Call Home email messages. |
| **Step 17** | UCS-A /monitoring/callhome # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example configures Call Home and commits the transaction:

```
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 #
```

### What to do next

Continue to "Configuring the Default Cisco TAC-1 Profile, on page 115" to configure a Call Home profile for use with Smart Call Home.

# Configuring the Default Cisco TAC-1 Profile

CiscoTAC-1 プロファイルのデフォルト設定は次のとおりです。

- 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

### Before you begin

Complete the "Configuring Smart Call Home, on page 113" section.

## SUMMARY STEPS

1. UCS-A /monitoring/callhome # **scope profile CiscoTac-1**
2. UCS-A /monitoring/callhome/profile # **set level normal**
3. UCS-A /monitoring/callhome/profile # **set alertgroups ciscotac**
4. UCS-A /monitoring/callhome/profile # **set format xml**
5. UCS-A /monitoring/callhome/profile # **set maxsize 5000000**
6. UCS-A /monitoring/callhome/profile # **create destination callhome@cisco.com**
7. UCS-A /monitoring/callhome/profile/destination # **exit**
8. UCS-A /monitoring/callhome/profile # **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /monitoring/callhome # **scope profile CiscoTac-1** | Enters monitoring call home profile mode for the default Cisco TAC-1 profile. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | UCS-A /monitoring/callhome/profile # **set level normal** | Specifies the **normal** event level for the profile. |
| **Step 3** | UCS-A /monitoring/callhome/profile # **set alertgroups ciscotac** | Specifies the **ciscotac** alert group for the profile. |
| **Step 4** | UCS-A /monitoring/callhome/profile # **set format xml** | Specifies the e-mail message format to **xml** . |
| **Step 5** | UCS-A /monitoring/callhome/profile # **set maxsize 5000000** | Specifies the maximum size of **5000000** for email messages. |
| **Step 6** | UCS-A /monitoring/callhome/profile # **create destination callhome@cisco.com** | Specifies the email recipient to **callhome@cisco.com** . |
| **Step 7** | UCS-A /monitoring/callhome/profile/destination # **exit** | Exits to monitoring call home profile mode. |
| **Step 8** | UCS-A /monitoring/callhome/profile # **exit** | Exits to monitoring call home mode. |

### Example

The following example configures the default Cisco TAC-1 profile for use with Smart Call Home:

```
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* #
```

### What to do next

Continue to "Configuring a System Inventory Message for Smart Call Home, on page 116" to configure system inventory messages for use with Smart Call Home.

# Configuring a System Inventory Message for Smart Call Home

### Before you begin

Complete the "Configuring the Default Cisco TAC-1 Profile, on page 115" section.

### SUMMARY STEPS

1. UCS-A /monitoring/callhome # **scope inventory**
2. UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** | **on**}
3. UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num*
4. UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour*
5. UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute*
6. UCS-A /monitoring/callhome/inventory # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /monitoring/callhome # **scope inventory** | Enters monitoring call home inventory mode. |
| **Step 2** | UCS-A /monitoring/callhome/inventory # **set send-periodically** {**off** \| **on**} | Enables or disables the sending of inventory messages. When the **on** keyword is specified, inventory messages are automatically sent to the Call Home database. |
| **Step 3** | UCS-A /monitoring/callhome/inventory # **set interval-days** *interval-num* | Specifies the the time interval (in days) at which inventory messages will be sent. |
| **Step 4** | UCS-A /monitoring/callhome/inventory # **set timeofday-hour** *hour* | Specifies the hour (using 24-hour format) that inventory messages are sent. |
| **Step 5** | UCS-A /monitoring/callhome/inventory # **set timeofday-minute** *minute* | Specifies the number of minutes after the hour that inventory messages are sent. |
| **Step 6** | UCS-A /monitoring/callhome/inventory # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example configures Call Home system inventory messages and commits the transaction:

```
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 #
```

#### What to do next

Continue to "Registering Smart Call Home, on page 117" to send an inventory message that starts the Smart Call Home registration process.

# Registering Smart Call Home

#### Before you begin

Complete the "Configuring a System Inventory Message for Smart Call Home, on page 116" section.

### SUMMARY STEPS

1. UCS-A /monitoring/callhome/inventory # **send**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A /monitoring/callhome/inventory # **send** | Sends the system inventory message to the Smart Call Home database.<br><br>When Cisco receives the system inventory, a Smart Call Home registration email is sent to the email address that you configured as the email address for the main Smart Call Home contact. |

### Example

The following example sends the system inventory message to the Smart Call Home database:

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

### What to do next

When you receive the registration email from Cisco, do the following to complete registration for Smart Call Home:

1. Click the link in the email.

   The link opens the Cisco Smart Call Home portal in your web browser.

2. Log into the Cisco Smart Call Home portal.

3. Follow the steps provided by Cisco Smart Call Home.

   After you agree to the terms and conditions, the Cisco Smart Call Home registration for the Cisco UCS ドメイン is complete.

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

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 （120 ページ）、およびヘルス チェックの間隔の変更 （120 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 （119 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 |
|---|---|---|
| **Step 1** | UCS-A# **scope system** | システムを入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **Step 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。 |
| **Step 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 |
|---|---|---|
| **Step 1** | UCS-A# **scope system** | システムを入力します。 |
| **Step 2** | UCS-A /system # **start-db-check** | ヘルス チェックをトリガーします。 |
| **Step 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 |
|---|---|---|
| **Step 1** | UCS-A# **scope system** | システムを入力します。 |
| **Step 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。 |
| **Step 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



## System Monitoring CLI Command Cheat Sheet

The following table provides a brief summary of Cisco UCS Manager CLI commands you use to monitor managed objects in the system.

| Managed Object | Monitoring Command | Description |
|---|---|---|
| **Hardware** | | |
| Chassis | **show chassis** [**adaptor** \| **cmc** \| **decommissioned** \| **detail** \| **environment** \| **fabric** \| **fi-iom** \| **firmware** \| **fsm** \| **inventory** \| **psu** \| **version**] | Displays chassis information. |
| Fabric Interconnect | **show fabric-interconnect** [**a** \| **b** ] [**detail** \| **environment** \| **firmware** \| **fsm** \| **inventory** \| **mac-aging** \| **mode** \| **version**] | Displays Fabric Interconnect information. |
| FEX | **show fex** [**detail** \| **firmware** \| **fsm** \| **inventory** \| **version**] | Displays Fabric Extender information |

| Managed Object | Monitoring Command | Description |
|---|---|---|
| IOM | **show iom** [**firmware** \| **health** \| **version**] | Displays Fabric Input/Output Module information. |
| Server | **show server** [**actual-boot-order** **adapter** \| **assoc** \| **bios** \| **boot-order** \| **cpu** \| **decommissioned** \| **environment** \| **firmware** \| **health** \| **identity** \| **inventory** \| **memory** \| **status** \| **storage** \| **version**] | Displays server information . |
| System | **show system** [**detail** \| **firmware** \| **version**] | Displays system information. |
| System | **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**] | Displays information about commands in Monitoring mode. |
| **Logs** | | |
| Event | **show event** [*event-id* \| **detail**] | Displays the Event log. |
| Fault | **show fault** [*fault-id* \| **cause** \| **detail** \| **severity** \| **suppressed**] | Displays the Fault log. |
| SEL | **show sel** [*chassis-id*/*blade-id* \| *rack-id*] | Displays the System Event Log for the chassis, blade, or rack-mount server. |
| Syslog | **scope monitoring** [**show** ] [**syslog**] | Displays the Syslog. |

# Managing the Chassis

## Turning On the Locator LED for a Chassis

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **enable locator-led**
3. UCS-A /chassis # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A /chassis # **enable locator-led** | Turns on the chassis locator LED. |
| **Step 3** | UCS-A /chassis # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example turns on the locator LED for chassis 2 and commits the transaction:

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

# Turning Off the Locator LED for a Chassis

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **disable locator-led**
3. UCS-A /chassis # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A /chassis # **disable locator-led** | Turns off the chassis locator LED. |
| **Step 3** | UCS-A /chassis # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example turns off the locator LED for chassis 2 and commits the transaction:

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

# Managing Blade Servers

## Turning On the Locator LED for a Blade Server

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **enable locator-led** [**multi-master** | **multi-slave**]
3. UCS-A /chassis/server # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-num* / *server-num* | Enters chassis server mode for the specified chassis. |
| **Step 2** | UCS-A /chassis/server # **enable locator-led** [**multi-master** \| **multi-slave**] | Turns on the blade server locator LED. |
| **Step 3** | UCS-A /chassis/server # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example turns on the locator LED for blade server 4 in chassis 2 and commits the transaction:

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

## Turning Off the Locator LED for a Blade Server

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **disable locator-led** [**multi-master** | **multi-slave**]
3. UCS-A /chassis/server # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-num* / *server-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A /chassis/server # **disable locator-led** [**multi-master** \| **multi-slave**] | Turns off the blade server locator LED. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | UCS-A /chassis/server # **commit-buffer** | Commits the transaction to the system configuration. |

**Example**

The following example turns off the locator LED for blade server 4 in chassis 2 and commits the transaction:

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

# Managing Rack-Mount servers

## Turning On the Locator LED for a Rack-Mount Server

**SUMMARY STEPS**

1. UCS-A# **scope server** *server-num*
2. UCS-A /server # **enable locator-led**
3. UCS-A /server # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *server-num* | Enters server mode for the specified rack-mount server. |
| **Step 2** | UCS-A /server # **enable locator-led** | Turns on the rack-mount server locator LED. |
| **Step 3** | UCS-A /server # **commit-buffer** | Commits the transaction to the system configuration. |

**Example**

The following example turns on the locator LED for rack-mount server 2 and commits the transaction:

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

# Turning Off the Locator LED for a Rack-Mount Server

### SUMMARY STEPS

1. UCS-A# **scope server** *server-num*
2. UCS-A /server # **disable locator-led**
3. UCS-A /server # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *server-num* | Enters server mode for the specified rack-mount server. |
| **Step 2** | UCS-A /server # **disable locator-led** | Turns off the rack-mount server locator LED. |
| **Step 3** | UCS-A /server # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example turns off the locator LED for rack-mount server 2 and commits the transaction:

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

# Showing the Status for a Rack-Mount Server

### SUMMARY STEPS

1. UCS-A# **show server status**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **show server status** | Shows the status for all servers in the Cisco UCS ドメイン. |

#### Example

The following example shows the status for all servers in the Cisco UCS ドメイン. The servers numbered 1 and 2 do not have a slot listed in the table because they are rack-mount servers.

```
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
```

# Monitoring Fan Modules

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **show environment fan**
3. UCS-A /chassis # **scope fan-module** *tray-num module-num*
4. UCS-A /chassis/fan-module # **show** [**detail** | **expand**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | 指定したシャーシでシャーシ モードを開始します。 |
| **Step 2** | UCS-A /chassis # **show environment fan** | Displays the environment status for all fans within the chassis.<br>This includes the following information:<br>• Overall status<br>• Operability<br>• Power state<br>• Thermal status<br>• Threshold status<br>• Voltage status |
| **Step 3** | UCS-A /chassis # **scope fan-module** *tray-num module-num* | Enters fan module chassis mode for the specified fan module.<br>**Note** Each chassis contains one tray, so the tray number in this command is always 1. |
| **Step 4** | UCS-A /chassis/fan-module # **show** [**detail** \| **expand**] | Displays the environment status for the specified fan module. |

### Example

The following example displays information about the fan modules in chassis 1:

```
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
```

The following example displays information about fan module 2 in chassis 1:

```
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
```

# Monitoring Management Interfaces

## 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。

# Configuring the Management Interfaces Monitoring Policy

### SUMMARY STEPS

1. Enter monitoring mode.
2. Enable or disable the management interfaces monitoring policy.
3. Specify the number of seconds that the system should wait between data recordings.
4. Specify the maximum number of monitoring attempts that can fail before the system assumes that the management interface is unavailable and generates a fault message.
5. Specify the monitoring mechanism that you want the system to use.
6. If you selected **mii-status** as your monitoring mechanism, configure the following properties:
7. If you selected **ping-arp-targets** as your monitoring mechanism, configure the following properties:
8. If you selected **ping-gateway** as your monitoring mechanism, configure the following properties:
9. UCS-A /monitoring # **commit-buffer**

### DETAILED STEPS

**Step 1** Enter monitoring mode.

UCS-A# **scope monitoring**

**Step 2** Enable or disable the management interfaces monitoring policy.

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

**Step 3** Specify the number of seconds that the system should wait between data recordings.

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

Enter an integer between 90 and 300.

**Step 4** Specify the maximum number of monitoring attempts that can fail before the system assumes that the management interface is unavailable and generates a fault message.

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

Enter an integer between 2 and 5.

**Step 5** Specify the monitoring mechanism that you want the system to use.

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

- **mii-status** —The system monitors the availability of the Media Independent Interface (MII).
- **ping-arp-targets** —The system pings designated targets using the Address Resolution Protocol (ARP).
- **ping-gateway** —The system pings the default gateway address specified for this Cisco UCS ドメイン in the management interface.

**Step 6** If you selected **mii-status** as your monitoring mechanism, configure the following properties:

a) Specify the number of seconds that the system should wait before requesting another response from the MII if a previous attempt fails.

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

Enter an integer between 3 and 10.

b) Specify the number of times that the system polls the MII until the system assumes that the interface is unavailable.

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

Enter an integer between 1 and 3.

**Step 7** If you selected **ping-arp-targets** as your monitoring mechanism, configure the following properties:

a) Specify the first IPv4 or IPv6 address the system pings.

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) Specify the second IPv4 or IPv6 address the system pings.

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) Specify the third IPv4 or IPv6 address the system pings.

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。

**Note** The ping IPv4 ARP or IPv6 N-disc targets must be in the same subnet or prefix, respectively, as the fabric interconnect.

d) Specify the number of ARP requests to send to the target IP addresses.

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

Enter an integer between 1 and 5.

e) Specify the number of seconds to wait for responses from the ARP targets before the system assumes that they are unavailable.

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

Enter a number between 5 and 15.

**Step 8** If you selected **ping-gateway** as your monitoring mechanism, configure the following properties:

a) Specify the number of times the system should ping the gateway.

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

Enter an integer between 1 and 5.

b) Specify the number of seconds to wait for a response from the gateway until the system assumes that the address is unavailable.

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

Enter an integer between 5 and 15.

**Step 9** UCS-A /monitoring # **commit-buffer**

Commits the transaction to the system configuration.

### Example

The following example creates a monitoring interface management policy using the Media Independent Interface (MII) monitoring mechanism and commits the transaction:

```
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 B200 M3 ブレード サーバ
- Cisco UCS B420 M3 ブレード サーバ
- Cisco UCS B22 M3 ブレード サーバ
- Cisco UCS B200 M4 ブレード サーバ
- Cisco UCS B260 M4 ブレード サーバ
- Cisco UCS B460 M4 ブレード サーバ
- Cisco UCS C420 M3 ラック サーバ
- Cisco UCS C240 M3 ラック サーバ

- Cisco UCS C220 M3 ラック サーバ
- Cisco UCS C24 M3 ラック サーバ
- Cisco UCS C22 M3 ラック サーバ
- Cisco UCS C220 M4 ラック サーバ
- Cisco UCS C240 M4 ラック サーバ
- Cisco UCS C460 M4 ラック サーバ
- Cisco UCS 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

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

# ローカル ストレージ モニタリングの前提条件

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

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

# Legacy Disk Drive Monitoring

**Note** The following information is applicable only for B200 M1/M2 and B250 M1/M2 blade servers.

The legacy disk drive monitoring for Cisco UCS provides Cisco UCS Manager with blade-resident disk drive status for supported blade servers in a Cisco UCS ドメイン. Disk drive monitoring provides a unidirectional fault signal from the LSI firmware to Cisco UCS Manager to provide status information.

The following server and firmware components gather, send, and aggregate information about the disk drive status in a server:

- Physical presence sensor—Determines whether the disk drive is inserted in the server drive bay.
- Physical fault sensor—Determines the operability status reported by the LSI storage controller firmware for the disk drive.
- IPMI disk drive fault and presence sensors—Sends the sensor results to Cisco UCS Manager.
- Disk drive fault LED control and associated IPMI sensors—Controls disk drive fault LED states (on/off) and relays the states to Cisco UCS Manager.

# Turning On the Local Disk Locator LED

**Step 1** UCS-A# **scope server** *id*

Enters server mode for the specified server.

**Step 2** UCS-A/server # **scope local-disk** *id*

Enters the RAID controller for the specified local disk.

**Step 3** UCS-A /server/local-disk # **enable locator-led**

Turns on the disk locator LED.

**Step 4** UCS-A/server/local-disk* # **commit-buffer**

Commits the command to the system configuration.

### Example

The following example displays how to turn on the local disk Locator LED:

```
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
```

# Turning Off the Local Disk Locator LED

**Step 1** UCS-A# **scope server** *id*

Enters server mode for the specified server.

**Step 2** UCS-A/server # **scope local-disk** *id*

Enters the RAID controller for the specified local disk.

**Step 3** UCS-A/server/local-disk # **disable locator-led**

Turns off the disk locator LED.

**Step 4** UCS-A/server/raid-controller/local-disk* # **commit-buffer**

Commits the command to the system configuration.

### Example

The following example displays how to disable the local disk Locator LED:

```
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
```

# Viewing the Local Disk Locator LED State

**Step 1** UCS-A# **scope server** *id*

Enters server mode for the specified server.

**Step 2** UCS-A/server # **scope local-disk** *id*

Enters the RAID controller for the specified local disk.

**Step 3** UCS-A/server/local-disk # **show locator-led**

Shows the state of the disk locator LED.

### Example

The following example shows that the state of the local disk Locator LED is on:

```
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
```

# Flash Life Wear Level Monitoring

Flash life wear level monitoring enables you to monitor the life span of solid state drives. You can view both the percentage of the flash life remaining, and the flash life status. Wear level monitoring is supported on the Fusion IO mezzanine card with the following Cisco UCS blade servers:

- Cisco UCS B22 M3 blade server
- Cisco UCS B200 M3 blade server

- Cisco UCS B420 M3 blade server
- Cisco UCS B200 M4 blade server
- Cisco UCS B260 M4 blade server
- Cisco UCS B460 M4 blade server

**Note** Wear level monitoring requires the following:

- Cisco UCS Manager must be at release 2.2(2a) or greater.
- The Fusion IO mezzanine card firmware must be at version 7.1.15 or greater.

# Viewing Flash Life Status

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *server-id*
2. UCS-A /chassis/server # **show raid-controller detail expand**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show raid-controller detail expand** | Displays details for the RAID controller. |

#### Example

The following example shows how to display the flash life status for server 3:

```
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 #
```

# Viewing the Status of Local Storage Components

## SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *server-id*
2. UCS-A /chassis/server # **show inventory storage**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show inventory storage** | Displays the local and virtual storage information for the server. |

### Example

The following example shows how to display the local disk status for server 2:

```
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 #
```

The following example shows how to display the local disk status for server 2 with PCIe\NVMe Flash Storage:

```
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 #
```

The following example shows how to display the local disk status for Cisco UCS (P3600) 2.5 inches 800 GB NVMe based PCIe SSD:

```
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:
```

The following example shows how to display the status for Cisco UCS (P3600) HHHL 2000 GB NVMe based PCIe SSD:

```
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
```

# Viewing the Status of a Disk Drive

### SUMMARY STEPS

1. UCS-A# **scope chassis** *chassis-num*
2. UCS-A /chassis # **scope server** *server-num*
3. UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}
4. UCS-A /chassis/server/raid-controller # **show local-disk** [*local-disk-id* | **detail** | **expand**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope chassis** *chassis-num* | 指定したシャーシでシャーシ モードを開始します。 |
| **Step 2** | UCS-A /chassis # **scope server** *server-num* | Enters server chassis mode. |
| **Step 3** | UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**sas** \| **sata**} | Enters RAID controller server chassis mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A /chassis/server/raid-controller # **show local-disk** [*local-disk-id* \| **detail** \| **expand**] | |

### Example

The following example shows the status of a disk drive:

```
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
```

# Viewing RAID Controller Operations

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *server-id*
2. UCS-A /chassis/server # **show raid-controller operation**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **show raid-controller operation** | Displays the long running operations for the RAID controller. |

### Example

The following example shows how to display the RAID controller operations for server 3:

```
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 #
```

# Viewing RAID Controller Stats

The following procedure shows how to display controller stats for a server with PCIe\NVMe Flash Storage:

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *server-id*
2. UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* **{flash | sas | sata | sd | unknown}**
3. UCS-A /chassis/server/raid-controller # **show stats**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* **{flash \| sas \| sata \| sd \| unknown}** | Enters RAID controller server chassis mode. |
| **Step 3** | UCS-A /chassis/server/raid-controller # **show stats** | Displays the raid controller stats. |

#### Example

The following example shows how to display the RAID controller stats:

```
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 #
```

# Monitoring RAID Battery Status

This procedure applies only to Cisco UCS servers that support RAID configuration and TFM. If the Battery Backup Unit (BBU) has failed or is predicted to fail, you should replace the unit as soon as possible.

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A # **scope chassis** *chassis-num* | Enters chassis mode for the specified chassis. |
| **Step 2** | UCS-A /chassis #**scope server** *server-num* | Enters server chassis mode. |
| **Step 3** | UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**flash** \| **sas** \| **sata** \| **sd** \| **unknown**} | Enters RAID controller server chassis mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A /chassis/server/raid-controller # **show raid-battery expand** | Displays the RAID battery status. |

### Example

This example shows how to view information on the BBU of a server:

```
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
```

# Graphics Card Monitoring

## 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 C240 M3 ラック サーバ
- Cisco UCS C460 M4 ラック サーバ
- Cisco UCS B200M4 ブレード サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ

（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。

# Viewing Graphics Card Properties

### SUMMARY STEPS

1. UCS-A# **scope server** *blade-id*
2. UCS-A /server # **show graphics-card detail**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *blade-id* | Enters server mode for the specified server. |
| **Step 2** | UCS-A /server # **show graphics-card detail** | Displays information about the graphics card. |

#### Example

The following example shows how to display the graphics card properties on server 1:

```
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 #
```

# Viewing Graphics Controller Properties

### SUMMARY STEPS

1. UCS-A# **scope server** *blade-id*

2. UCS-A /server # **scope graphics-card** *card-id*
3. UCS-A /server/graphics-card # **show graphics-controller detail**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *blade-id* | Enters server mode for the specified server. |
| **Step 2** | UCS-A /server # **scope graphics-card** *card-id* | Enters graphics card mode for the specified graphics card. |
| **Step 3** | UCS-A /server/graphics-card # **show graphics-controller detail** | Displays information about the graphics controllers. |

**Example**

The following example shows how to display the graphics controller properties for graphics card 1 on server 1:

```
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 Switch Monitoring

## 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

## Viewing PCI Switch Properties

PCI Switch properties are visible only for servers which support PCI switch.

**SUMMARY STEPS**

1. UCS-A# **scope server** *server-num*
2. UCS-A /server # **show pci-switch**
3. UCS-A /server # **scope pci-switch** *pci-switch-number*
4. UCS-A /server # **show detail**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *server-num* | Enters server mode for the specified server. |
| **Step 2** | UCS-A /server # **show pci-switch** | Displays information about the PCI switches. |
| **Step 3** | UCS-A /server # **scope pci-switch** *pci-switch-number* | Enters the PCI switch mode for the specified PCI switch. |
| **Step 4** | UCS-A /server # **show detail** | |

### Example

The following example shows how to display the PCI switch properties:

```
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 とスーパーキャパシタの制約事項

- Cisco UCS B420 M3 ブレード サーバの TFM およびスーパーキャパシタの CIMC センサーは、Cisco UCS Manager によってポーリングされません。
- TFM およびスーパーキャパシタが Cisco UCS B420 M3 ブレード サーバに搭載されていない、または搭載後にブレード サーバから取り外した場合、障害は生成されません。
- TFM は Cisco UCS B420 M3 ブレード サーバに搭載されていないが、スーパーキャパシタが搭載されている場合、Cisco UCS Manager によって BBU システム全体が欠落していると報告されます。TFM とスーパーキャパシタの両方がブレード サーバに存在することを物理的に確認する必要があります。

### TFM およびスーパーキャパシタについてサポートされる Cisco UCS サーバ

次の Cisco UCS サーバは TFM およびスーパーキャパシタをサポートしています。

- Cisco UCS B420 M3 ブレード サーバ
- Cisco UCS C22 M3 ラック サーバ
- Cisco UCS C24 M3 ラック サーバ
- Cisco UCS C220 M3 ラック サーバ
- Cisco UCS C240 M3 ラック サーバ
- Cisco UCS C420 M3 ラック サーバ
- Cisco UCS C460 M4 ラック サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS C220 M3 ラック サーバ
- Cisco UCS C240 M3 ラック サーバ

# TPM Monitoring

Trusted Platform Module (TPM) is included on all Cisco UCS M3 blade and rack-mount servers. Operating systems can use TPM to enable encryption. For example, Microsoft's BitLocker Drive Encryption uses the TPM on Cisco UCS servers to store encryption keys.

Cisco UCS Manager enables monitoring of TPM, including whether TPM is present, enabled, or activated.

## Viewing TPM Properties

### SUMMARY STEPS

1. UCS-A# **scope server** *chassis-id* / *server-id*
2. UCS-A /chassis/server # **scope tpm** *tpm-id*
3. UCS-A /chassis/server/tpm # **show**
4. UCS-A /chassis/server/tpm # **show detail**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope server** *chassis-id* / *server-id* | Enters chassis server mode for the specified server. |
| **Step 2** | UCS-A /chassis/server # **scope tpm** *tpm-id* | Enters TPM mode for the specified TPM ID. |
| **Step 3** | UCS-A /chassis/server/tpm # **show** | Displays the TPM properties. |
| **Step 4** | UCS-A /chassis/server/tpm # **show detail** | Displays detailed TPM properties. |

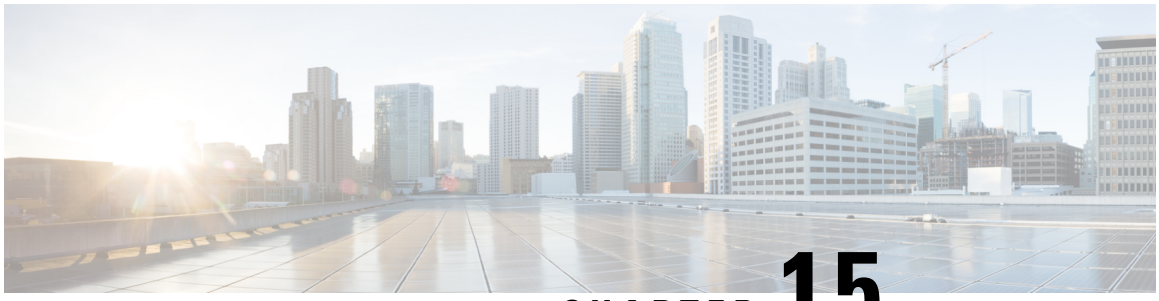
#### Example

The following example shows how to display the TPM properties for blade 3 in chassis 1:

```
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 #
```



CHAPTER 15

# Netflow Monitoring



# NetFlow モニタリング

NetFlowは、IP トラフィック データを収集するための標準ネットワーク プロトコルです。NetFlow により、特定の特性を共有する単方向 IP パケットに関して、フローを定義することができます。フロー定義に一致するすべてのパケットが収集され、1 つ以上の外部 NetFlow コレクタにエクスポートされます。そこでは、アプリケーション固有の処理のために、さらに集約、分析、および使用されます。

Cisco UCS Manager は、Netflow 対応アダプタ (Cisco UCS VIC 1240、Cisco UCS VIC 1280、Cisco UCS VIC 1225、 Cisco UCS VIC 1300 シリーズ、および Cisco UCS VIC 1440 series) を使用して、フロー情報を収集し、エクスポートするルータおよびスイッチと通信します。

（注）

- NetFlow モニタリングは、 Cisco UCS 6400 シリーズ ファブリック インターコネクト ではサポートされません。
- リリース 3.0(2) では、NetFlow モニタはエンド ホスト モードでのみサポートされます。

### ネットワーク フロー

フローとは、トラフィックの送信元または送信先、ルーティング情報、使用されているプロトコルなど、共通のプロパティを持つ一連の単方向IPパケットです。フローは、フロー レコード定義での定義に一致する場合に収集されます。

### フロー レコード定義

フロー レコード定義は、フロー定義で使用されるプロパティに関する情報で構成され、特性プロパティと測定プロパティの両方を含めることができます。フロー キーとも呼ばれる特性プロパティは、フローを定義するプロパティです。 Cisco UCS Manager では IPv4、IPv6,、およびレイヤ2のキーがサポートされています。フロー値または非キーとも呼ばれる測定された特性は、フローのすべてのパケットに含まれるバイト数またはパケットの合計数などの、測定できる値です。

フロー レコード定義は、フロー キーとフロー値の特定の組み合わせです。次の2つのタイプのフロー レコード定義があります。

- **[System-defined]**：Default flow record definitions supplied by Cisco UCS Managerが提供するデフォルトのフロー レコード定義。
- [User-defined]：ユーザが独自に作成できるフロー レコード定義。

### フロー エクスポータ、フロー エクスポータ プロファイル、およびフロー コレクタ

フロー エクスポータは、フロー エクスポータ プロファイルの情報に基づき、フロー コネクタにフローを転送します。フロー エクスポータ プロファイルには、NetFlow パケットをエクスポートする際に使用されるネットワーキングプロパティが含まれます。ネットワーキングプロパティには、各ファブリック インターコネクトの VLAN、送信元 IP アドレス、およびサブネット マスクが含まれます。

（注） Cisco UCS Manager GUIでは、ネットワーキング プロパティは、プロファイルに含まれているエクスポータ インターフェイスで定義されます。Cisco UCS Manager CLIでは、プロパティはプロファイルで定義されます。

フロー コレクタは、フロー エクスポータからフローを受信します。各フロー コレクタには、フローの送信先を定義する、IP アドレス、ポート、外部ゲートウェイ IP、VLAN が含まれます。

### フロー モニタおよびフロー モニタ セッション

フロー モニタは、フロー定義、1つまたは2つのフロー エクスポータ、タイムアウト ポリシーで構成されます。フロー モニタを使用することで、どのフロー情報をどこから収集するかを指定できます。各フロー モニタは、出力または入力のどちらかの方向で動作します。

フロー モニタ セッションには、次の4つまでのフロー モニタが含まれます。入力方向の2つのフロー モニタと出方向の2つのフロー モニタ。また、フロー モニタ セッションは、vNIC に関連付けることができます。

# NetFlow に関する制限事項

NetFlow モニタリングには、次の制限事項が適用されます。

- NetFlow モニタリングは、 Cisco UCS 6400 シリーズ ファブリック インターコネクト ではサポートされません。
- NetFlow モニタリングは、 Cisco UCS 1200、1300、および 1400 シリーズ VIC アダプタでサポートされています。ただし、1200 シリーズの VIC アダプタでは、FCoE トラフィックに対して NetFlow を使用することは推奨されません。
- 最大 64 のフロー レコード定義、フロー エクスポータ、フロー モニタを使用できます。
- NetFlow は、vNIC テンプレート オブジェクトではサポートされません。
- PVLAN およびローカル VLAN は、サービス VLAN に対してサポートされません。
- すべての VLAN は公開されており、両方のファブリック インターコネクトに共通である必要があります。
- VLAN はフロー コレクタと併用する前に、エクスポータ インターフェイスとして定義する必要があります。
- NetFlow は、usNIC、仮想マシン キュー、または Linux ARFS と併用できません。

# Configuring a Flow Record Definition

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-record** *flow-record-name* | Enters flow record mode for the specified flow record. |
| **Step 3** | UCS-A /eth-flow-mon/flow-record # **set keytype** {**ipv4keys** \| **ipv6keys** \| **l2keys**} | Specifies the key type. |
| **Step 4** | UCS-A /eth-flow-mon/flow-record # **set ipv4keys** {**dest-port** \| **ip-protocol** \| **ip-tos** \| **ipv4-dest-address** \| **ipv4-src-address** \| **src-port**} | Specifies the attributes for the key type that you selected in Step 3.<br>**Note** Use this command only if you chose **ipv4keys** in step 3. |
| **Step 5** | UCS-A /eth-flow-mon/flow-record # **set ipv6keys** {**dest-port** \| **ip-protocol** \| **ipv6-dest-address** \| **ipv6-src-address** \| **src-port**} | Specifies the attributes for the key type that you selected in Step 3.<br>**Note** Use this command only if you chose **ipv6keys** in Step 3. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A /eth-flow-mon/flow-record # **set l2keys** {**dest-mac-address** \| **ethertype** \| **src-mac-address**} | Specifies the attributes for the key type that you chose in Step 3.<br>**Note** Use this command only if you selected **l2keys** in step 3. |
| **Step 7** | UCS-A /eth-flow-mon/flow-record # **set nonkeys** {**counter-bytes-long** \| **counter-packets-long** \| **sys-uptime-first** \| **sys-uptime-last**} | Specifies the nonkey attributes. |
| **Step 8** | UCS-A /eth-flow-mon/flow-record # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a flow record definition with Layer 2 keys and commit the transaction:

```
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 #
```

# Configuring an Exporter Profile

### SUMMARY STEPS

1. UCS-A# **scope eth-flow-mon**
2. UCS-A /eth-flow-mon # **scope flow-profile** *profile-name*
3. UCS-A /eth-flow-mon/flow-profile # **show config**
4. UCS-A /eth-flow-mon/flow-profile # **enter vlan** *vlan-name*
5. UCS-A /eth-flow-mon/flow-profile/vlan # **enter fabric** {**a** | **b**}
6. UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **set addr** *ip-addr* **subnet** *ip-addr*
7. UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **scope flow-profile** *profile-name* | Enters the flow profile mode for the specified profile. |
| **Step 3** | UCS-A /eth-flow-mon/flow-profile # **show config** | Displays the flow profile configuration. |
| **Step 4** | UCS-A /eth-flow-mon/flow-profile # **enter vlan** *vlan-name* | Specifies the VLAN associated with the exporter profile. PVLANs and local VLAN are not supported. All VLAN |

| | Command or Action | Purpose |
|---|---|---|
| | | must be public and must be common to both fabric interconnects. |
| **Step 5** | UCS-A /eth-flow-mon/flow-profile/vlan # **enter fabric** {**a** \| **b**} | Enters flow profile mode for the specified fabric. |
| **Step 6** | UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **set addr** *ip-addr* **subnet** *ip-addr* | Specifies the source IP and subnet mask for the exporter profile on the fabric.<br>**Important** Make sure the IP address you specify is unique within the Cisco UCS ドメイン. IP address conflicts can occur if you specify an IP address that is already being used by Cisco UCS Manager. |
| **Step 7** | UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to configure the default exporter profile, set the source IP and subnet mask for the exporter interface on each fabric, and commit the transaction:

```
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 #
```

# Configuring a Netflow Collector

### SUMMARY STEPS

1. UCS-A# **scope eth-flow-mon**
2. UCS-A /eth-flow-mon # **enter flow-collector** *flow-collector-name*
3. UCS-A /eth-flow-mon/flow-collector # **set dest-port** *port_number*
4. UCS-A /eth-flow-mon/flow-collector # **set vlan** *vlan_id*
5. UCS-A /eth-flow-mon/flow-collector # **enter ip-if**
6. UCS-A /eth-flow-mon/flow-collector/ip-if # **set addr** *ip-address*
7. UCS-A /eth-flow-mon/flow-collector/ip-if # **set exporter-gw** *gw-address*
8. UCS-A /eth-flow-mon/flow-collector/ip-if # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-collector** *flow-collector-name* | Enters the flow collector mode for the specified flow collector. |
| **Step 3** | UCS-A /eth-flow-mon/flow-collector # **set dest-port** *port_number* | Specifies the destination port for the flow collector. |
| **Step 4** | UCS-A /eth-flow-mon/flow-collector # **set vlan** *vlan_id* | Specifies the VLAN ID for the flow collector. |
| **Step 5** | UCS-A /eth-flow-mon/flow-collector # **enter ip-if** | Enters IPv4 configuration mode. |
| **Step 6** | UCS-A /eth-flow-mon/flow-collector/ip-if # **set addr** *ip-address* | Specifies the exporter IP address. |
| **Step 7** | UCS-A /eth-flow-mon/flow-collector/ip-if # **set exporter-gw** *gw-address* | Specifies the exporter gateway address. |
| **Step 8** | UCS-A /eth-flow-mon/flow-collector/ip-if # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to configure a NetFlow collector, set the exporter IP and gateway address, and commit the transaction:

```
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 #
```

# Configuring a Flow Exporter

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-exporter** *flow-exporter-name* | Enters the flow exporter mode for the specified flow exporter. |
| **Step 3** | UCS-A /eth-flow-mon/flow-exporter # **set dscp** *dscp_number* | Specifies the differentiated services code point. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | UCS-A /eth-flow-mon/flow-exporter # **set flow-collector** *flow-collector_name* | Specifies the flow collector. |
| **Step 5** | UCS-A /eth-flow-mon/flow-exporter # **set exporter-stats-timeout** *timeout_number* | Specifies the timeout period for resending NetFlow flow exporter data. |
| **Step 6** | UCS-A /eth-flow-mon/flow-exporter # **set interface-table-timeout** *timeout_number* | Specifies the time period for resending the NetFlow flow exporter interface table. |
| **Step 7** | UCS-A /eth-flow-mon/flow-exporter # **set template-data-timeout** *timeout_number* | Specifies the timeout period for resending NetFlow template data. |
| **Step 8** | UCS-A /eth-flow-mon/flow-exporter # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to configure a flow exporter, set the timeout values, and commit the transaction:

```
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 #
```

# Configuring a Flow Monitor

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-monitor** *flow-monitor-name* | Enters the flow monitor mode for the specified flow monitor. |
| **Step 3** | UCS-A /eth-flow-mon/flow-monitor # **set flow-record** *flow-record-name* | Specifies the flow record. |
| **Step 4** | UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter** *flow-exporter-name* | Specifies the first flow exporter. |
| **Step 5** | UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter** *flow-exporter-name* | Specifies the second flow exporter. |
| **Step 6** | UCS-A /eth-flow-mon/flow-monitor # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a flow monitor and commit the transaction:

```
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 #
```

# Configuring a Flow Monitor Session

### SUMMARY STEPS

1. UCS-A# **scope eth-flow-mon**
2. UCS-A /eth-flow-mon # **enter flow-mon-session** *flow-monitor-session-name*
3. UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-1*
4. UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-2*
5. UCS-A /eth-flow-mon/flow-mon-session # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **enter flow-mon-session** *flow-monitor-session-name* | Enters the flow monitor session mode for the specified flow monitor session. |
| **Step 3** | UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-1* | Specifies the first flow monitor. |
| **Step 4** | UCS-A /eth-flow-mon/flow-mon-session # **create flow-monitor** *flow-monitor-2* | Specifies the second flow monitor. |
| **Step 5** | UCS-A /eth-flow-mon/flow-mon-session # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to create a flow monitor session with two flow monitors:

```
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 #
```

# Configuring a NetFlow Cache Active and Inactive Timeout

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope eth-flow-mon** | Enters the ethernet flow monitor mode. |
| **Step 2** | UCS-A /eth-flow-mon # **scope flow-timeout** *timeout-name* | Enters the flow timeout mode for the specified flow timeout. |
| **Step 3** | UCS-A /eth-flow-mon/flow-timeout # **set cache-timeout-active** *timeout-value* | Specifies the active timeout value. This value can be between 60 and 4092 seconds. The default value is 120 seconds. |
| **Step 4** | UCS-A /eth-flow-mon/flow-timeout # **set cache-timeout-inactive** *timeout-value* | Specifies the inactive timeout value. This value can be between 15 and 4092 seconds. The default value is 15 seconds. |
| **Step 5** | UCS-A /eth-flow-mon/flow-timeout # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to change the NetFlow timeout values and commit the transaction:

```
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 #
```

# Associating a Flow Monitor Session to a vNIC

### SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *profile-name*
3. UCS-A /org/service-profile # **scope vnic** *vnic-name*
4. UCS-A /org/service-profile/vnic # **enter flow-mon-src** *flow-monitor-session-name*
5. UCS-A /org/service-profile/vnic # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope org** *org-name* | 指定した組織の設定モードに入ります。ルート組織モードを開始するには、*org-name* に **/** を入力します。 |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | UCS-A /org # **scope service-profile** *profile-name* | Enters the organization service profile mode for the specified service profile. |
| **Step 3** | UCS-A /org/service-profile # **scope vnic** *vnic-name* | Enters the organization service profile mode for the specified vNIC. |
| **Step 4** | UCS-A /org/service-profile/vnic # **enter flow-mon-src** *flow-monitor-session-name* | Associates the flow monitor session to the vNIC. |
| **Step 5** | UCS-A /org/service-profile/vnic # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example shows how to associate the flow monitor session s1 to the vNIC eth5:

```
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

トラフィック モニタリングでは、1つまたは複数の送信元ポートからのトラフィックをコピーし、コピーされたトラフィックを分析用の専用宛先ポートに送信してネットワーク アナライザに分析させます。この機能は、Switched Port Analyzer（SPAN）としても知られています。

### トラフィック モニタリング セッションの種類

モニタリング セッションが 2 種類あります。

- イーサネット
- ファイバ チャネル

宛先ポートの種類により、どのようなモニタリング セッションを必要とするかが決まります。イーサネットのトラフィック モニタリング セッションの場合、宛先ポートは未設定の物理ポートであることが必要です。Cisco UCS 6400 シリーズ ファブリック インターコネクトs 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、および 6454 ファブリック インターコネクトについては、ファイバチャネル宛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 | 宛先ポート |
|---|---|
| • アップリンク イーサネット ポート<br>• イーサネット ポート チャネル<br>• VLAN<br>• サービス プロファイル vNIC<br>• サービス プロファイル vHBA<br>• FCoE ポート<br>• ポート チャネル<br>• ユニファイド アップリンク ポート<br>• VSAN | 未設定のイーサネット ポート |

（注） すべてのトラフィックの送信元は宛先ポートと同じスイッチ内にある必要があります。宛先ポートとして設定されたポートを送信元ポートとしても設定することはできません。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 ポートは、非仮想化ラック サーバ アダプタへのポートの場合にのみ送信元にすることができます。

### Cisco UCS 6400 シリーズ ファブリック インターコネクトのトラフィック モニタリング

- Cisco UCS 6400 シリーズ ファブリック インターコネクトは、宛先ポートとしてのファイバ チャネル ポートをサポートしません。したがって、イーサネット ポートは、このファブリック インターコネクトでトラフィック モニタリング セッションを設定するための唯一のオプションです。

- Cisco UCS 6400 シリーズ ファブリック インターコネクトでは、ファブリック インターコネクトごとに 2 つ以上の送信元に対する送信方向のトラフィックのモニタリングをサポートします。
- 送信方向と受信方向のトラフィックについて、ポート チャネル送信元で SPAN をモニタまたは使用できます。
- 1 つのモニタ セッションの宛先ポートとしてポートを設定できます。
- 送信方向の送信元としてポート チャネルをモニタできます。
- 送信方向の送信元として vEth をモニタすることはできません。

### Cisco UCS 6300 ファブリック インターコネクトのトラフィック モニタリング

- Cisco UCS 6300 ファブリック インターコネクトはポートベースのミラーリングをサポートしています。
- Cisco UCS 6300 ファブリック インターコネクトは、VLAN SPAN を受信方向でのみサポートします。
- イーサネット SPAN は Cisco UCS 6300 ファブリック インターコネクトに基づいたポートです。

### Cisco UCS 6200 ファブリック インターコネクトのトラフィック モニタリング

- Cisco UCS 6200 および 6324 ファブリック インターコネクトでは、ファブリック インターコネクトごとに最大 2 つの送信元で「送信」方向のモニタリング トラフィックがサポートされています。
- Cisco UCS 6200 では、SPAN トラフィックは SPAN 宛先ポートの速度によりレート制限されています。これは 1 Gbps または 10 Gbps のいずれかです。

**重要** (6200 および 6324 ファブリック インターコネクトの場合) 入力トラフィック専用ポート チャネル上で SPAN の使用またはモニタができます。

### ファイバ チャネル全体のトラフィック モニタリング

ファイバ チャネル トラフィック アナライザまたはイーサネット トラフィック アナライザを使用して、ファイバ チャネル トラフィックをモニタできます。ファイバ チャネル トラフィックが、イーサネット宛先ポートでイーサネット トラフィック モニタリング セッションでモニタされる場合、宛先トラフィックは FCoE になります。Cisco UCS 6300 ファブリック インターコネクトは、FC SPAN を、入力側でのみサポートします。Cisco UCS 6248 ファブリック インターコネクトのファイバ チャネル ポートは送信元ポートとして設定できません。

ファイバ チャネル トラフィック モニタリング セッションでは、次のトラフィックの送信元ポートおよび宛先ポートのいずれかをモニタできます。

| 送信元ポート | 宛先ポート |
|---|---|
| • FC ポート<br>• FC ポート チャネル<br>• アップリンク ファイバ チャネル ポート<br>• SAN ポート チャネル<br>• VSAN<br>• サービス プロファイル vHBA<br>• ファイバ チャネル ストレージ ポート | • ファイバ チャネル アップリンク ポート<br>• 未設定のイーサネット ポート（Cisco UCS 64108、6454、6332、および6332-16UP ファブリック インターコネクト） |

# トラフィックモニタリングに関するガイドラインと推奨事項

トラフィック モニタリングを設定するか、アクティブにする場合は、次のガイドラインを考慮してください。

### トラフィック モニタリング セッション

トラフィックモニタリングセッションは作成時にはデフォルトでディセーブルです。トラフィックモニタリングを開始するには、まずセッションをアクティブにします。トラフィックモニタリング セッションは、 Cisco UCSポッド内のどのファブリック インターコネクトでも固有である必要があります。一意の名前と一意のVLANソースを使用して各モニタリングセッションを作成します。サーバからのトラフィックを監視するには、サーバに対応するサービス プロファイルからすべての vNIC を追加します。

### ファブリックインターコネクトごとにサポートされるアクティブトラフィックモニタリングセッションの最大数

トラフィック モニタリング セッションは最大 16 まで作成し保存できますが、同時にアクティブにできるのは 4 つだけです。各 Cisco UCS 6400 シリーズ ファブリック インターコネクトおよび 6300 ファブリック インターコネクトについては、最大 4 個のトラフィック方向のみをモニタ出来ます。受信および送信方向は、それぞれ 1 モニタリング セッションとしてカウントされます。一方、双方向モニタリングセッションは、2 モニタリング セッションとしてカウントされます。次に例を示します。

- 4 つのアクティブ セッション：各セッションが 1 方向だけでトラフィックをモニタするように設定されている場合。
- 2 つのアクティブ セッション—：各セッションでトラフィックを双方向にモニタするように設定されている場合。

• 3 つのアクティブ セッション：1 つ目のセッションが単方向で、2 つ目のセッションが双方向の場合。

（注） トラフィックモニタリングは、システムリソースにかなりの負荷をかけることがあります。負荷を最小限にするには、不必要なトラフィックができるだけ少ない送信元を選択し、不必要なときにはトラフィック モニタリングをディセーブルにします。

### vNIC

トラフィック モニタリングの宛先は単一の物理ポートであるため、トラフィック モニタリング セッションは 1 つのファブリックだけを監視できます。ファブリック フェールオーバーにわたって中断されない vNIC トラフィックをモニタリングするには、ファブリックごとに 1 つ、合計 2 つのセッションを作成し、2 台のアナライザを接続します。両方のセッションでまったく同じ名前を使用して、トラフィックの送信元として vNIC を追加します。仮想コンピュータのポート プロファイルを変更すると、送信元ポートとして使用されている、関連付けられた vNIC はモニタリングから削除され、モニタリング セッションを再設定する必要があります。トラフィック モニタリング セッションが Cisco UCS Manager リリース 2.0 より前のリリースのもとでダイナミック vNIC で設定された場合、アップグレード後にトラフィック モニタリング セッションを再設定する必要があります。Cisco UCS 6200 は、送信方向での vNIC からのトラフィック モニタリングをサポートします。ただし、Cisco UCS 6400 シリーズ ファブリック インターコネクトは、送信方向で vNIC からのトラフィック モニタリング トラフィックをサポートしていません。

### vHBA

vHBA はイーサネットまたはファイバ チャネルのどちらのモニタリング セッションの送信元としても設定できますが、同時に両方の送信元とすることはできません。VHBA が SPAN 送信元として設定されている場合、 SPAN 宛先は、VN タグが付いたフレームのみを受信します。これは、直接 FC フレームを受信しません。Cisco UCS 6200 では、送信方向 vHBA からのトラフィック モニタリングをサポートします。ただし、Cisco UCS 6400 シリーズ ファブリック インターコネクトは、送信方向で vHBA からのトラフィック モニタリング トラフィックをサポートしていません。

# Creating an Ethernet Traffic Monitoring Session

**Note** This procedure describes creating an Ethernet traffic monitoring session. To create a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **create fc-mon-session** command instead of the **create eth-mon-session** command in Step 3.

### SUMMARY STEPS

1. UCS-A# **scope eth-traffic-mon**
2. UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}
3. UCS-A /eth-traffic-mon/fabric # **create eth-mon-session** *session-name*
4. UCS-A /eth-traffic-mon/fabric/eth-mon-session # **create dest-interface** *slot-num port-num*
5. UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **set speed***admin-speed*
6. UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A /eth-traffic-mon # **scope fabric** {**a** \| **b**} | 指定したファブリックで、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。 |
| **Step 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。 |
| **Step 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。 |
| **Step 5** | UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **set speed***admin-speed* | Sets the モニタされるポート チャネルのデータ転送速度. This can be:<br>• 1gbps—1 Gbps<br>• 10gbps—10 Gbps<br>• 20gbps—20 Gbps<br>• 40gbps—40 Gbps |
| **Step 6** | UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example creates an Ethernet traffic monitoring session to copy and forward traffic to the destination port at slot 2, port 12, sets the admin speed to 20 Gbps, and commits the transaction:

```
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 #
```

### What to do next

- 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。

# Creating a Fibre Channel Traffic Monitoring Session

### SUMMARY STEPS

1. UCS-A# **scope fc-traffic-mon**
2. UCS-A /fc-traffic-mon # **scope fabric** {**a** | **b**}
3. UCS-A /fc-traffic-mon/fabric # **create fc-mon-session** *session-name*
4. UCS-A /fc-traffic-mon/fabric/fc-mon-session # **create dest-interface** *slot-num port-num*
5. UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **set speed***admin-speed*
6. UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A /fc-traffic-mon # **scope fabric** {**a** \| **b**} | 指定したファブリックで、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。 |
| **Step 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。 |
| **Step 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。 |
| **Step 5** | UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **set speed***admin-speed* | Sets the モニタされるポート チャネルのデータ転送速度. This can be:<br>• 1gbps—1 Gbps<br>• 2gbps—2 Gbps<br>• 4gbps—4 Gbps<br>• 8gbps—8 Gbps<br>• auto—Cisco UCSがデータ転送速度を決定します。 |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | UCS-A /fc-traffic-mon/fabric/fc-mon-session/dest-interface # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example creates a Fibre channel traffic monitoring session to copy and forward traffic to the destination port at slot 1, port 10, sets the admin speed to 8 Gbps, and commits the transaction:

```
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 #
```

### What to do next

- 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。

# Adding Traffic Sources to a Monitoring Session

## Adding an Uplink Source Port to a Monitoring Session

**Note** This procedure describes adding an Ethernet uplink port as a source for a traffic monitoring session. To add a Fibre Channel uplink port as a source, enter the **scope fc-uplink** command instead of the **scope eth-uplink** command in Step 1.

### Before you begin

A traffic monitoring session must be created.

### SUMMARY STEPS

1. UCS-A# **scope eth-uplink**
2. UCS-A /eth-uplink # **scope fabric** {**a** | **b**}
3. UCS-A /eth-uplink/fabric # **scope interface** *slot-num port-num*
4. UCS-A /eth-uplink/fabric/interface # **create mon-src** *session-name*
5. (Optional) UCS-A /eth-uplink/fabric/interface/mon-src # **set direction** {**both** | **receive** | **transmit**}
6. UCS-A /eth-uplink/fabric/interface/mon-src # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A /eth-uplink # **scope fabric** {**a** \| **b**} | Enters uplink fabric mode for the specified fabric. |
| **Step 3** | UCS-A /eth-uplink/fabric # **scope interface** *slot-num port-num* | Enters the interface command mode for the specified uplink port. |
| **Step 4** | UCS-A /eth-uplink/fabric/interface # **create mon-src** *session-name* | Adds the uplink port as a source to the specified monitoring session. |
| **Step 5** | (Optional) UCS-A /eth-uplink/fabric/interface/mon-src # **set direction** {**both** \| **receive** \| **transmit**} | Specifies the traffic direction to be monitored.<br>**Note** If you do not select any direction, the default direction is Rx. |
| **Step 6** | UCS-A /eth-uplink/fabric/interface/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example adds the ingress traffic on Ethernet uplink port 3 on slot 2 of fabric A as a source for a monitoring session and commits the transaction:

```
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 #
```

### What to do next

You can add additional sources to the traffic monitoring session.

# Adding a vNIC or vHBA Source to a Monitoring Session

**Note** This procedure describes adding a vNIC as a source for a traffic monitoring session. To add a vHBA as a source, enter the **scope vhba** command instead of the **scope vnic** command in Step 2.

### Before you begin

A traffic monitoring session must be created.

### SUMMARY STEPS

1. Switch-A# **scope system**
2. Switch-A /system # **scope vm-mgmt**
3. (Optional) Switch-A /system/vm-mgmt # **show virtual-machine**
4. Switch-A /system/vm-mgmt # **scope virtual-machine** *uuid*
5. (Optional) Switch-A /system/vm-mgmt/virtual-machine # **show expand**
6. Switch-A /system/vm-mgmt/virtual-machine # **scope vnic** *mac-address*
7. Switch-A /system/vm-mgmt/virtual-machine/vnic # **create mon-src** *session-name*
8. (Optional) Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **set direction** {**both** | **receive** | **transmit**}
9. Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Switch-A# **scope system** | Enters system mode. |
| **Step 2** | Switch-A /system # **scope vm-mgmt** | Enters VM management mode. |
| **Step 3** | (Optional) Switch-A /system/vm-mgmt # **show virtual-machine** | Displays the running virtual machines. |
| **Step 4** | Switch-A /system/vm-mgmt # **scope virtual-machine** *uuid* | Enters command mode for the virtual machine that contains the dynamic vNIC. |
| **Step 5** | (Optional) Switch-A /system/vm-mgmt/virtual-machine # **show expand** | Displays the virtual machine details, including the vNIC MAC address. |
| **Step 6** | Switch-A /system/vm-mgmt/virtual-machine # **scope vnic** *mac-address* | Enters the command mode for the vNIC at the specified MAC address. |
| **Step 7** | Switch-A /system/vm-mgmt/virtual-machine/vnic # **create mon-src** *session-name* | Adds the vNIC as a source to the specified monitoring session. |
| **Step 8** | (Optional) Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **set direction** {**both** | **receive** | **transmit**} | Specifies the traffic direction to be monitored. |
| **Step 9** | Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example adds the ingress traffic on a dynamic vNIC as a source for a monitoring session and commits the transaction:

```
Switch-A# scope system
Switch-A /system # scope vm-mgmt
Switch-A /system/vm-mgmt # show virtual-machine
Virtual Machine:
    UUID: 42327c42-e00c-886f-e3f7-e615906f51e9
    Service Profile: org-root/ls-dsw-bld1-esx
```

```
    Server: sys/chassis-1/blade-1
    Status: Online
.
.
.
Switch-A /system/vm-mgmt # scope virtual-machine 42327c42-e00c-886f-e3f7-e615906f51e9
Switch-A /system/vm-mgmt/virtual-machine # show expand
Virtual Machine:
    UUID: 42327c42-e00c-886f-e3f7-e615906f51e9
    Service Profile: org-root/ls-dsw-bld1-esx
    Server: sys/chassis-1/blade-1
    Status: Online

    vNIC:
        Name:
        Status: Online
        MAC Address: 00:50:56:B2:00:00

        VIF:
            Vif Id: 32772
            Status: Online
            Phys Fabric ID: B
            Virtual Fabric:
Switch-A /system/vm-mgmt/virtual-machine # scope vnic 00:50:56:B2:00:00
Switch-A /system/vm-mgmt/virtual-machine/vnic # create mon-src Monitor23
Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src* # set direction receive
Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src* # commit-buffer

Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src #
```

### What to do next

You can add additional sources to the traffic monitoring session.

# Adding a VLAN or VSAN Source to a Monitoring Session

**Note** This procedure describes adding a VLAN as a source for a traffic monitoring session. To add a VSAN as a source, the following changes are required:

- Enter the **scope fc-uplink** command instead of the **scope eth-uplink** command in Step 1.
- Enter the **create vsan** command instead of the **create vlan** command in Step 3.

### Before you begin

A traffic monitoring session must be created.

## SUMMARY STEPS

1. UCS-A# **scope eth-uplink**
2. UCS-A /eth-uplink # **scope fabric** {**a** | **b**}
3. UCS-A /eth-uplink/fabric # **create vlan** *vlan-name* *vlan-id*
4. UCS-A /eth-uplink/fabric/vlan # **create mon-src** *session-name*

5. UCS-A /eth-uplink/fabric/vlan/mon-src # **commit-buffer**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A /eth-uplink # **scope fabric** {**a** \| **b**} | Enters uplink fabric mode for the specified fabric.<br>**Note** This step is required when adding a local VLAN as a source. To add a global VLAN as a source, omit this step. |
| **Step 3** | UCS-A /eth-uplink/fabric # **create vlan** *vlan-name vlan-id* | Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters uplink VLAN mode. |
| **Step 4** | UCS-A /eth-uplink/fabric/vlan # **create mon-src** *session-name* | Adds the VLAN as a source to the specified monitoring session. |
| **Step 5** | UCS-A /eth-uplink/fabric/vlan/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

### Example

The following example adds a local VLAN as a source for an Ethernet monitoring session and commits the transaction:

```
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 #
```

### What to do next

You can add additional sources to the traffic monitoring session.

# Adding a Storage Port Source to a Monitoring Session

**Note** This procedure describes adding a Fibre Channel storage port as a source for a Fibre Channel traffic monitoring session. To add an FCoE storage port as a source for an Ethernet traffic monitoring session, enter the **create interface fcoe** command instead of the **create interface fc** command in Step 3.

### Before you begin

A traffic monitoring session must be created.

### SUMMARY STEPS

1. UCS-A# **scope fc-storage**
2. UCS-A /fc-storage # **scope fabric** {**a** | **b**}
3. UCS-A /fc-storage/fabric # **create interface fc** *slot-num port-num*
4. UCS-A /fc-storage/fabric/fc # **create mon-src** *session-name*
5. UCS-A /fc-storage/fabric/fc/mon-src # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | UCS-A# **scope fc-storage** | Enters Fibre Channel storage port command mode. |
| **Step 2** | UCS-A /fc-storage # **scope fabric** {**a** \| **b**} | Enters Fibre Channel storage port fabric mode for the specified fabric. |
| **Step 3** | UCS-A /fc-storage/fabric # **create interface fc** *slot-num port-num* | Creates a Fibre Channel storage port interface and enters the interface command mode. |
| **Step 4** | UCS-A /fc-storage/fabric/fc # **create mon-src** *session-name* | Adds the storage port as a source to the specified monitoring session. |
| **Step 5** | UCS-A /fc-storage/fabric/fc/mon-src # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example adds a Fibre Channel storage port on port 3 of slot 2 as a source for a Fibre Channel monitoring session and commits the transaction:

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric # create 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 #
```

#### What to do next

You can add additional sources to the traffic monitoring session.

# Activating a Traffic Monitoring Session

**Note** This procedure describes activating an Ethernet traffic monitoring session. To activate a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **scope fc-mon-session** command instead of the **scope eth-mon-session** command in Step 3.

### Before you begin

Configure a traffic monitoring session.

## SUMMARY STEPS

1. UCS-A# **scope eth-traffic-mon**
2. UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}
3. UCS-A /eth-traffic-mon/fabric # **scope eth-mon-session** *session-name*
4. UCS-A /eth-traffic-mon/fabric/eth-mon-session # **disable** | **enable**
5. UCS-A /eth-traffic-mon/fabric/eth-mon-session # **commit-buffer**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A /eth-traffic-mon # **scope fabric** {**a** \| **b**} | 指定したファブリックで、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。 |
| **Step 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。 |
| **Step 4** | UCS-A /eth-traffic-mon/fabric/eth-mon-session # **disable** \| **enable** | Disables or enables the traffic monitoring session. |
| **Step 5** | UCS-A /eth-traffic-mon/fabric/eth-mon-session # **commit-buffer** | Commits the transaction to the system configuration. |

When activated, the traffic monitoring session begins forwarding traffic to the destination when a traffic source is configured.

### Example

The following example activates an Ethernet traffic monitoring session and commits the transaction:

```
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 #
```

# Deleting a Traffic Monitoring Session

**Note** This procedure describes deleting an Ethernet traffic monitoring session. To delete a Fibre Channel traffic monitoring session, the following changes are required:

- Enter the **scope fc-traffic-mon** command instead of the **scope eth-traffic-mon** command in Step 1.
- Enter the **delete fc-mon-session** command instead of the **delete eth-mon-session** command in Step 3.

### SUMMARY STEPS

1. UCS-A# **scope eth-traffic-mon**
2. UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}
3. UCS-A /eth-traffic-mon/fabric # **delete eth-mon-session** *session-name*
4. UCS-A /eth-traffic-mon/fabric # **commit-buffer**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 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。 |
| **Step 2** | UCS-A /eth-traffic-mon # **scope fabric** {**a** \| **b**} | 指定したファブリックで、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。 |
| **Step 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。 |
| **Step 4** | UCS-A /eth-traffic-mon/fabric # **commit-buffer** | Commits the transaction to the system configuration. |

#### Example

The following example deletes an Ethernet traffic monitoring session and commits the transaction:

```
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 #
```

# SPAN Restrictions for the Cisco UCS Mini

Consider the following guidelines and restrictions when configuring the SPAN feature on Cisco UCS Mini

- FC port as SPAN destination is not supported.
- VSAN as SPAN source is not supported.
- FC uplink ports as SPAN source is not supported.