Cisco UCS Manager CLI システム モニタリング ガイド リリース 2.2

初版：2013 年 12 月 11 日

最終更新：2016 年 07 月 27 日

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

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

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

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

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

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。

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

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

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

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。

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。

警告

安全上の重要事項

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

これらの注意事項を保管しておいてください。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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

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

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

その他のマニュアル リソース

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

マニュアルに関するフィードバック

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

第 1 章

トラフィックのモニタリング

この章は、次の項で構成されています。

トラフィック モニタリング

トラフィック モニタリングは、1 つ以上のソース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。

重要 入力トラフィックのみに対しポート チャネルの SPAN をモニタまたは使用できます。

セッションのタイプ

トラフィックモニタリングセッションを作成すると、トラフィックを受信する宛先ポートをイーサネットとファイバ チャネルのいずれかから選択できます。宛先ポートのタイプは、セッションのタイプを決定し、次に使用可能なトラフィックの送信元を決定します。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。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。

トラフィックの送信元

イーサネットのトラフィック 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のいずれかをモニタできます。

- アップリンク イーサネット ポート
- イーサネット ポート チャネル
- VLAN
- サービス プロファイル vNIC
- サービス プロファイル vHBA
- FCoE ポート
- ポート チャネル
- ユニファイド アップリンク ポート

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のいずれかをモニタできます。

- アップリンク ファイバ チャネル ポート
- SAN ポート チャネル
- VSAN
- サービス プロファイル vHBA
- ファイバ チャネル ストレージ ポート

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、次のガイドラインを考慮します。

- 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なるのは 2 つだけです。
- 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、セッションをアクティブにする必要があります。
- トラフィック モニタリング セッションは、Cisco UCS ポッド内のファブリック インターコネクトで一意的である必要があります。そのため、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 セッションを作成する必要があります。
- 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 トラフィック モニタリング セッションでモニタされ、イーサネット宛先ポートを持つ場合、宛先トラフィックは FCoE になります。
- 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 2 つのセッションを作成し、2 台のアナライザを接続する必要があります。両方のセッションのトラフィック送信元として vNIC を追加します。
- 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 ポートを個別にソース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。
- 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。
- 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 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。
- 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。
- 6200 シリーズ ファブリック インターコネクトでは、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。

（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。

イーサネット トラフィック モニタリング セッションの作成

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

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

手順

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

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

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

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

次の作業

- トラフィック モニタリング セッションにトラフィック ソースを追加します。
- トラフィック モニタリング セッションをアクティブ化します。

ファイバ チャネル トラフィック モニタリング セッションの作成

手順

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

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

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

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

次の作業

- 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。

モニタリングセッションへのトラフィック送信元の追加

モニタリング セッションへのアップリンク ソース ポートの追加

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

はじめる前に

トラフィック モニタリング セッションが作成されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク コマンド モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのアップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope interface***slot-numport-num*	指定されたアップリンク ポートのインターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/interface # **create mon-src***session-name*	指定されたモニタリング セッションのソースとしてアップリンク ポートを追加します。
ステップ 5	UCS-A /eth-uplink/fabric/interface/mon-src # **set direction** {**both** | **receive** | **transmit**}	（任意） モニタするトラフィックの方向を指定します。 （注） 方向を選択しない場合、デフォルトの方向は Rx です。
ステップ 6	UCS-A /eth-uplink/fabric/interface/mon-src # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
```

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

次の作業

トラフィック モニタリング セッションにはさらにソースを追加できます。

モニタリング セッションへの vNIC または vHBA 発信元の追加

（注） この手順では、トラフィック モニタリング セッションのソースとして vNIC を追加する方法について説明します。ソースとして vHBA を追加するには、ステップ 2 で **scope vnic** コマンドの代わりに **scope vhba** コマンドを入力します。

はじめる前に

トラフィック モニタリング セッションが作成されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Switch-A# **scope system**	システム モードを開始します。
ステップ 2	Switch-A /system # **scope vm-mgmt**	VM 管理モードを開始します。
ステップ 3	Switch-A /system/vm-mgmt # **show virtual-machine**	（任意） 実行中の仮想マシンを表示します。
ステップ 4	Switch-A /system/vm-mgmt # **scope virtual-machine** *uuid*	ダイナミック vNIC を含む仮想マシンのコマンドモードを開始します。
ステップ 5	Switch-A /system/vm-mgmt/virtual-machine # **show expand**	（任意） vNIC の MAC アドレスを含む仮想マシンの詳細が表示されます。
ステップ 6	Switch-A /system/vm-mgmt/virtual-machine # **scope vnic***mac-address*	指定した MAC アドレスの vNIC コマンド モードを開始します。
ステップ 7	Switch-A /system/vm-mgmt/virtual-machine/vnic # **create mon-src** *session-name*	指定されたモニタリングセッションのソースとして vNIC を追加します。

	コマンドまたはアクション	目的
ステップ 8	Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **set direction** {**both** | **receive** | **transmit**}	（任意） モニタするトラフィックの方向を指定します。
ステップ 9	Switch-A /system/vm-mgmt/virtual-machine/vnic/mon-src # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例では、モニタ セッションのソースとしてダイナミック vNIC 上の入力トラフィックを追加し、トランザクションをコミットします。

```
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 #
```

次の作業

トラフィック モニタリング セッションにはさらにソースを追加できます。

モニタリング セッションへの VLAN または VSAN 発信元の追加

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

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

はじめる前に

トラフィック モニタリング セッションが作成されている必要があります。

手順

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

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

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

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

次の作業

トラフィック モニタリング セッションにはさらにソースを追加できます。

モニタリング セッションへのストレージ ポート送信元の追加

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

はじめる前に

トラフィック モニタリング セッションが作成されている必要があります。

手順

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

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

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

次の作業

トラフィック モニタリング セッションにはさらにソースを追加できます。

トラフィック モニタリング セッションのアクティブ化

（注） この手順では、イーサネット トラフィックのモニタリング セッションをアクティブ化する方法について説明します。ファイバ チャネル トラフィックのモニタリング セッションをアクティブにするには、次の変更が必要になります。

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

はじめる前に

トラフィック モニタリング セッションを設定する。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-traffic-mon**	イーサネット トラフィック モニタリング コマンド モードを開始します。
ステップ 2	UCS-A /eth-traffic-mon # **scope fabric** {**a** | **b**}	指定したファブリックで、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。
ステップ 3	UCS-A /eth-traffic-mon/fabric # **scope eth-mon-session***session-name*	指定した名前のトラフィック モニタリング セッションのコマンド モードを開始します。
ステップ 4	UCS-A /eth-traffic-mon/fabric/eth-mon-session # **disable** | **enable**	トラフィックのモニタリング セッションをイネーブルまたはディセーブルにします。
ステップ 5	UCS-A /eth-traffic-mon/fabric/eth-mon-session # **commit-buffer**	トランザクションをシステムの設定にコミットします。

アクティブ化すると、トラフィックモニタリングセッションは、トラフィックの送信元が設定されるとすぐに宛先へのトラフィックの転送を開始します。

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

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

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

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

トラフィック モニタリング セッションの削除

（注） この手順では、イーサネット トラフィックのモニタリング セッションを削除する方法について説明します。ファイバ チャネル トラフィックのモニタリング セッションを削除するには、次の変更が必要です。

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

手順

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

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

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

第 2 章

ハードウェアのモニタリング

この章は、次の項で構成されています。

ファン モジュールのモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis***chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **show environment fan**	シャーシ内のすべてのファンの環境ステータスを表示します。 これには次の情報が含まれます。 • 全体のステータス • 運用性 • 電源の状態 • 温度ステータス

	コマンドまたはアクション	目的
		• しきい値ステータス • 電圧ステータス
ステップ 3	UCS-A /chassis # **scope fan-module** *tray-num module-num*	指定したファン モジュールでモジュール シャーシ モードを開始します。 （注） 各シャーシには、1つのトレイが含まれるため、このコマンドのトレイ番号は常に 1 です。
ステップ 4	UCS-A /chassis/fan-module # **show** [**detail** | **expand**]	指定したファン モジュールの環境ステータスを表示します。

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

```
UCS-A# scope chassis 1
UCS-A /chassis # show environment fan
Chassis 1:
    Overall Status: Power Problem
    Operability: Operable
    Power State: Redundancy Failed
    Thermal Status: Upper Non Recoverable

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

        Fan Module Stats:
             Ambient Temp (C): 25.000000

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

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

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

        Fan Module Stats:
             Ambient Temp (C): 24.000000
```

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

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

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

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

管理インターフェイスのモニタリング

管理インターフェイス モニタリング ポリシー

このポリシーは、ファブリック インターコネクトの mgmt0 イーサネット インターフェイスのモニタ方法を定義します。Cisco UCS 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。

影響を受ける管理インターフェイスが管理インスタンスであるファブリック インターコネクトに属する場合、Cisco UCS は従属のファブリック インターコネクトのステータスがアップであること、それに対する現在のエラーのレポートが存在しないことを確認し、それからエンドポイントへ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現在ハイアベイラビリティ設定のプライマリ内部の場合、管理プレーンのフェールオーバーがトリガーされます。データ プレーンは、フェールオーバーの影響を受けません。

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をモニタする間隔。
- 管理が使用できないと判断し障害メッセージを生成する前にシステムの失敗を許容するモニタリングの最大試行回数。

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

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

管理インターフェイス モニタリング ポリシーの設定

手順

ステップ 1 モニタリング モードを開始します。
UCS-A# **scope monitoring**

ステップ 2 管理インターフェイス モニタリング ポリシーをイネーブルにするか、ディセーブルにします。
UCS-A /monitoring # **set mgmt-if-mon-policy admin-state {enabled | disabled}**

ステップ 3 システムがデータの記録の間で待機する秒数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy poll-interval**

90 ～ 300 の整数を入力します。

ステップ 4 管理インターフェイスが使用できないと判断し障害メッセージを生成する前にシステムの失敗を許容するモニタリングの最大試行回数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy max-fail-reports** *num-mon-attempts*

2 ～ 5 の整数を入力します。

ステップ 5 システムが使用するモニタリング メカニズムを指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy monitor-mechanism {mii-status | ping-arp-targets | ping-gateway**

- **mii-status**：システムはメディア独立型インターフェイス（MII）のアベイラビリティをモニタします。
- **ping-arp-targets**：システムは Address Resolution Protocol（ARP）を使用して指定されたターゲットに ping を送信します。

- **ping-gateway**：システムは管理インターフェイスでこの Cisco UCS ドメインに指定されたデフォルト ゲートウェイ アドレスに ping を送信します。

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

a) 前回の試行が失敗したとき、もう一度MIIからの応答を要求する前にシステムが待機する秒数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy mii-retry-interval** *num-seconds*

3 ～ 10 の範囲の整数を入力します。

b) インターフェイスが使用不能であるとシステムが判断するまでにシステムがMIIをポーリングする回数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy mii-retry-count** *num-retries*

1 ～ 3 の整数を入力します。

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

a) システムが ping する最初の IPv4 または IPv6 アドレスを指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp-target1*|*ndisc-target1*} {*ipv4-addr*|*ipv6-addr*}

IPv4 アドレスに 0.0.0.0 と入力すると、ARP ターゲットが削除されます。または IPv6 アドレスの場合は N-disc ターゲットが削除されます。

b) システムが ping する第 2 の IPv4 または IPv6 アドレスを指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp-target2*|*ndisc-target2*} {*ipv4-addr*|*ipv6-addr*}

IPv4 アドレスに 0.0.0.0 と入力すると、ARP ターゲットが削除されます。または IPv6 アドレスの場合は N-disc ターゲットが削除されます。

c) システムが ping する第 3 の IPv4 または IPv6 アドレスを指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy** {*arp-target3*|*ndisc-target3*} {*ipv4-addr*|*ipv6-addr*}

IPv4 アドレスに 0.0.0.0 と入力すると、ARP ターゲットが削除されます。または IPv6 アドレスの場合は N-disc ターゲットが削除されます。

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

d) ターゲット IP アドレスに送信する ARP 要求の数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy arp-requests** *num-requests*

1 ～ 5 の整数を入力します。

e) 使用不能と見なす前にシステムが ARP ターゲットからの応答を待機する秒数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy arp-deadline** *num-seconds*

5 ～ 15 の範囲内の数を入力してください。

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

a) システムがゲートウェイに ping を実行する必要がある回数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy ping-requests**

1 ～ 5 の整数を入力します。

b) アドレスが使用不能であるとシステムが判断するまでゲートウェイからの応答を待機する秒数を指定します。
UCS-A /monitoring # **set mgmt-if-mon-policy ping-deadline**

5 ～ 15 の整数を入力します。

ステップ 9 UCS-A /monitoring # **commit-buffer**
トランザクションをシステムの設定にコミットします。

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

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

ローカル ストレージのモニタリング

Cisco UCS でのローカル ストレージのモニタリングでは、ブレードまたはラック サーバに物理的に接続されているローカル ストレージに関するステータス情報を提供します。これには、RAID コントローラ、物理ドライブおよびドライブ グループ、仮想ドライブ、RAID コントローラ バッテリ（BBU）、Transportable Flash Module（TFM）および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（OOB）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 C460 M2 ラック サーバ
- Cisco UCS C420 M3 ラック サーバ
- Cisco UCS C260 M2 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

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

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

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

- Cisco UCS B200 M1/M2 ブレード サーバ
- Cisco UCS B250 M1/M2 ブレード サーバ

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

ローカル ストレージ モニタリングの前提条件

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

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

レガシー ディスク ドライブのモニタリング

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

Cisco UCS のレガシー ディスク ドライブ モニタリングにより、Cisco UCS ドメイン内のサポート対象ブレードサーバについて、ブレードに搭載されているディスク ドライブのステータスが Cisco UCS Manager に提供されます。ディスク ドライブ モニタリングは、LSI ファームウェアから Cisco UCS Manager への単方向の障害信号により、ステータス情報を提供します。

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

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

フラッシュ ライフ ウェア レベル モニタリング

フラッシュ ライフ ウェア レベル モニタリングによって、ソリッド ステート ドライブの寿命をモニタできます。フラッシュ ライフ残量の割合とフラッシュ ライフの状態の両方を表示できます。ウェア レベル モニタリングは次の Cisco UCS ブレード サーバのフュージョン IO メザニン カードでサポートされます。

- Cisco UCS B22 M3 ブレード サーバ
- Cisco UCS B200 M3 ブレード サーバ
- Cisco UCS B420 M3 ブレード サーバ
- Cisco UCS 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

（注） ウェア レベル モニタリングの必須事項は次のとおりです。

- Cisco UCS Manager がリリース 2.2(2a) 以降である。
- フュージョン IO メザニン カードのファームウェアのバージョンが 7.1.15 以降である。

Flash 寿命ステータスの表示

手順

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

次に、サーバ 3 の Flash 寿命ステータスを表示する例を示します。

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

RAID Controller:
    ID: 1
    Type: FLASH
    PCI Addr: 131:00.0
    Vendor: Cisco Systems Inc
    Model: UCSC-F-FIO-1205M
    Serial: 1315D2B52
    HW Rev: FLASH
    Raid Support: No
    OOB Interface Supported: No
    Rebuild Rate: N/A
    Controller Status: Unknown

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

UCS-A /chassis/server #
```

ローカル ストレージ コンポーネントのステータスの表示

手順

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

次に、サーバ 2 のローカル ディスク ステータスを表示する例を示します。

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

        RAID Controller 1:
            Type: SAS
            Vendor: LSI Logic   Symbios Logic
            Model: LSI MegaRAID SAS 2004 ROMB
            Serial: LSIROMB-0
            HW Revision: B2
            PCI Addr: 01:00.0
            Raid Support: RAID0, RAID1
            OOB Interface Supported: Yes
            Rebuild Rate: 31
            Controller Status: Optimal

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

            Local Disk 2:
                Product Name: 600G AL12SE SAS Hard Disk Drive
                PID: A03-D600GA2
                VID: V01
                Vendor: TOSHIBA
                Model: MBF2600RC
                Vendor Description: Toshiba Corporation
                Serial: EA00PB109T4A
                HW Rev: 0
                Block Size: 512
                Blocks: 1169920000
                Operability: Operable
                Oper Qualifier Reason: N/A
                Presence: Equipped
```

```
                Size (MB): 571250
                Drive State: Online
                Power State: Active
                Link Speed: 6 Gbps
                Device Type: HDD

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

            Virtual Drive 0:
                Type: RAID 1 Mirrored
                Block Size: 512
                Blocks: 285155328
                Operability: Operable
                Presence: Equipped
                Size (MB): 139236
                Lifecycle: Allocated
                Drive State: Optimal
                Strip Size (KB): 64
                Access Policy: Read Write
                Read Policy: Normal
                Configured Write Cache Policy: Write Through
                Actual Write Cache Policy: Write Through
                IO Policy: Direct
                Drive Cache: No Change
                Bootable: False

UCS-A /chassis/server #
```

ディスク ドライブのステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope 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。
ステップ 2	UCS-A /chassis # **scope server** *server-num*	サーバ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}	RAID コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/raid-controller # **show local-disk** [*local-disk-id* | **detail** | **expand**]	

次の例は、ディスク ドライブのステータスを示しています。

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

Local Disk:
    ID: 1
    Block Size: 512
    Blocks: 60545024
```

```
    Size (MB): 29563
    Operability: Operable
    Presence: Equipped
```

RAID コントローラ動作の表示

手順

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

次に、サーバ 3 の RAID コントローラ動作を表示する例を示します。

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

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

UCS-A /chassis/server #
```

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 カードや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

（注） 特定の NVIDIA グラフィックス処理ユニット（GPU）では、エラー訂正コード（ECC）と vGPU は同時にサポートされません。それぞれの GPU について NVIDIA から公開されているリリース ノートを参照して、ECC と vGPU が同時にサポートされるかどうかを確認することをお勧めします。

グラフィックス カードのプロパティの表示

手順

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

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

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

Graphics Card:
ID  Slot Id    Is Supported Firmware Version
--- ---------- ------------ ----------------
1   5          Yes          80.07.6D.00.13|2401.0502.00.02

UCS-A /server # show graphics-card detail

Graphics Card:
ID: 1
Slot Id: 5
Is Supported: Yes
Vendor: nVidia Corporation
Model: Nvidia GRID K1 P2401-502
Serial: NA
Firmware Version: 80.07.6D.00.13|2401.0502.00.02

UCS-A /server #
```

グラフィックス コントローラのプロパティの表示

手順

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

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

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

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

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 Release 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

RAID バッテリ ステータスのモニタリング

この手順は、RAID 設定および TFM をサポートする Cisco UCS サーバにのみ該当します。BBU に障害が発生した場合、または障害が予測される場合には、そのユニットをできるだけ早く交換する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope chassis***chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis #**scope server***server-num*	サーバ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server # **scope raid-controller***raid-contr-id* {**flash** | **sas** | **sata** | **sd** | **unknown**}	RAID コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/raid-controller # **show raid-battery expand**	RAID バッテリ ステータスを表示します。

この例では、サーバのバッテリ バックアップ ユニットに関する情報を表示する方法を示します。

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

    Transportable Flash Module:
        Presence: Equipped
        Vendor: Cisco Systems Inc
```

```
Model: UCSB-RAID-1GBFM
Serial: FCH164279W6
```

TPM モニタリング

トラステッド プラットフォーム モジュール（TPM）は、すべての Cisco UCS M3 ブレード サーバとラックマウント サーバに搭載されています。オペレーティング システムでの暗号化に TPM を使用することができます。たとえば、Microsoft の BitLocker ドライブ暗号化は Cisco UCS サーバ上で TPM を使用して暗号キーを保存します。

Cisco UCS Manager では、TPM が存在しているか、有効またはアクティブになっているかどうかを含めた TPM のモニタリングが可能です。

TPM のプロパティの表示

手順

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

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

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

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

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

第 3 章

統計関連ポリシーの設定

この章は、次の項で構成されています。

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。報告インターバル中に複数の統計データ ポイントが収集できるように、報告インターバルは収集インターバルよりも長くなります。これにより、最小値、最大値、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：アダプタ関連統計情報
- シャーシ：シャーシ関連統計情報
- 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す
- 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：サーバ関連統計情報

（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 でデルタ カウンタに表示される値は、収集間隔での最後の 2 つのサンプル間の差異として算出された値です。さらに、Cisco UCS Manager には、収集間隔のサンプルの平均、最小、最大の各デルタ値が表示されます。

統計情報収集ポリシーの変更

手順

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

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

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

統計情報しきい値ポリシーの設定

統計情報しきい値ポリシー

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

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

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

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

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

サーバおよびサーバコンポーネントの統計情報しきい値ポリシー設定

サーバおよびサーバ コンポーネントの統計情報しきい値ポリシーの設定

手順

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

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create stats-threshold-policy***policy-name*	指定された統計情報しきい値ポリシーを作成し、組織統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCS-A /org/stats-threshold-policy # **set descr***description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、ServStatsPolicy という名前のサーバおよびサーバ コンポーネントの統計情報しきい値ポリシーを作成し、ポリシーに説明を加え、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # set descr "Server stats threshold policy."
UCS-A /org/stats-threshold-policy* # commit-buffer
UCS-A /org/stats-threshold-policy #
```

次の作業

統計情報しきい値ポリシーに 1 つ以上のポリシー クラスを設定します。詳細については、「サーバおよびサーバ コンポーネントの統計情報しきい値ポリシー クラスの設定, （37 ページ）」を参照してください。

サーバおよびサーバ コンポーネントの統計情報しきい値ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。 ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **delete stats-threshold-policy** *policy-name*	指定された統計情報しきい値ポリシーを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、ServStatsPolicy という名前のサーバおよびサーバ コンポーネント統計情報しきい値ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # delete stats-threshold-policy ServStatsPolicy
UCS-A /org* # commit-buffer
UCS-A /org #
```

サーバおよびサーバ コンポーネントの統計情報しきい値ポリシー クラスの設定

はじめる前に

ポリシー クラスを含むことになるサーバおよびサーバ コンポーネントの統計情報しきい値ポリシーの設定や識別を実行します。詳細については、「サーバおよびサーバ コンポーネントの統計情報しきい値ポリシーの設定, （35 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope stats-threshold-policy** *policy-name*	組織統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCS-A /org/stats-threshold-policy # **create class** *class-name*	指定された統計情報しきい値ポリシー クラスを作成し、組織統計情報しきい値ポリシー クラス モードを開始します。*class-name* 引数は、設定されている特定の統計情報しきい値ポリシーに使用できるクラス名キーワードのいずれかになります。使用可能なクラス名キーワードのリストを表示するには、**create class ?** コマンドを組織統計情報しきい値ポリシー モードで入力します。 （注） 統計情報しきい値ポリシーには複数のクラスを設定できます。
ステップ 4	UCS-A /org/stats-threshold-policy /class # **create property** *property-name*	指定された統計情報しきい値ポリシー クラス プロパティを作成し、組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。*property-name* 引数は、設定されている特定の統

	コマンドまたはアクション	目的
		計情報しきい値ポリシー クラスに使用できるプロパティ名キーワードのいずれかになります。使用可能なプロパティ名キーワードのリストを表示するには、**create property ?** コマンドを組織統計情報しきい値ポリシー クラス モードで入力します。 （注） ポリシー クラスには複数のプロパティを設定できます。
ステップ 5	UCS-A /org/stats-threshold-policy/class/property # **set normal-value** *value*	クラス プロパティに通常値を指定します。*value* の形式は、設定しているクラスプロパティによって異なる場合があります。必要な形式を確認するには、**set normal-value ?** コマンドを組織統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 6	UCS-A /org/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**} {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	クラス プロパティに、指定したしきい値を作成し、組織統計情報しきい値ポリシー クラス プロパティしきい値モードを開始します。 （注） クラスプロパティに対して複数のしきい値を設定できます。
ステップ 7	UCS-A /org/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	降格または昇格のクラス プロパティしきい値を指定します。*value* の形式は、設定されているクラス プロパティしきい値によって異なる場合があります。必要な形式を確認するには、**set deescalating ?** または **set escalating ?** コマンドを組織統計情報しきい値ポリシークラスプロパティしきい値モードで入力します。 （注） 降格と昇格の両方のクラスプロパティしきい値を指定できます。
ステップ 8	UCS-A /org/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、CPU 統計情報のサーバおよびサーバ コンポーネント統計情報しきい値ポリシー クラスを作成し、CPU 温度プロパティを作成し、通常の CPU 温度を摂氏 48.5 度に指定し、通常超えの警告しきい値摂氏 50 度を作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # create class cpu-stats
UCS-A /org/stats-threshold-policy/class* # create property cpu-temp
UCS-A /org/stats-threshold-policy/class/property* # set normal-value 48.5
UCS-A /org/stats-threshold-policy/class/property* # create threshold-value above-normal
```

```
warning
UCS-A /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
UCS-A /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /org/stats-threshold-policy/class/property/threshold-value #
```

サーバおよびサーバ コンポーネントの統計情報しきい値ポリシー クラスの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope stats-threshold-policy** *policy-name*	指定された統計情報しきい値ポリシーを入力します。
ステップ 3	UCS-A /org/stats-threshold-policy # **delete class** *class-name*	指定した統計情報しきい値ポリシー クラスをポリシーから削除します。
ステップ 4	UCS-A /org/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、CPU 統計情報のサーバおよびサーバ コンポーネント統計情報しきい値ポリシー クラスを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # delete class cpu-stats
UCS-A /org/stats-threshold-policy* # commit-buffer
UCS-A /org/stats-threshold-policy #
```

アップリンク イーサネット ポートの統計情報しきい値ポリシー設定

アップリンク イーサネット ポートの統計情報しきい値ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope stats-threshold-policy default**	イーサネット アップリンク統計情報しきい値ポリシー モードを開始します。

	コマンドまたはアクション	目的
		（注） アップリンク イーサネット ポート統計情報しきい値ポリシーの作成（または削除）は実行できません。既存のデフォルト ポリシーに入る（スコープを設定する）ことだけが可能です。
ステップ 3	UCS-A /eth-uplink/stats-threshold-policy # **set descr** *description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /eth-uplink/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、デフォルト アップリンク イーサネット ポートしきい値ポリシーに入り、ポリシーの説明を記入し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink* # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy* # set descr "Uplink Ethernet port stats threshold
 policy."
UCS-A /eth-uplink/stats-threshold-policy* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy #
```

次の作業

統計情報しきい値ポリシーに 1 つ以上のポリシー クラスを設定します。詳細については、「アップリンク イーサネット ポートの統計情報しきい値ポリシー クラスの設定, （40 ページ）」を参照してください。

アップリンク イーサネット ポートの統計情報しきい値ポリシー クラスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope stats-threshold-policy default**	イーサネット アップリンク統計情報しきい値ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/stats-threshold-policy # **create class** *class-name*	指定された統計情報しきい値ポリシー クラスを作成し、イーサネット アップリンク統計情報しきい値ポリシー クラス モードを開始します。*class-name* 引数は、設定されている特定の統計情報しきい値ポリシーに使用できるクラス名キーワードのいずれかになります。使用可能なクラス名キーワードのリストを表示するには、**create class ?** コマンドをイーサネット アップリンク統計情報しきい値ポリシー モードで入力します。 （注） 統計情報しきい値ポリシーには複数のクラスを設定できます。
ステップ 4	UCS-A /eth-uplink/stats-threshold-policy /class # **create property** *property-name*	指定された統計情報しきい値ポリシー クラス プロパティを作成し、イーサネット アップリンク統計情報しきい値ポリシー クラス プロパティ モードを開始します。*property-name* 引数は、設定されている特定の統計情報しきい値ポリシー クラスに使用できるプロパティ名キーワードのいずれかになります。使用可能なプロパティ名キーワードのリストを表示するには、**create property ?** コマンドをイーサネット アップリンク統計情報しきい値ポリシー クラス モードで入力します。 （注） ポリシー クラスには複数のプロパティを設定できます。
ステップ 5	UCS-A /eth-uplink/stats-threshold-policy /class/property # **set normal-value** *value*	クラス プロパティに通常値を指定します。*value* の形式は、設定しているクラス プロパティによって異なる場合があります。必要な形式を確認するには、**set normal-value ?** コマンドをイーサネット アップリンク統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 6	UCS-A /eth-uplink/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**} {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	クラス プロパティに、指定したしきい値を作成し、イーサネット アップリンク統計情報しきい値ポリシー クラス プロパティしきい値モードを開始します。 （注） クラス プロパティに対して複数のしきい値を設定できます。
ステップ 7	UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	降格または昇格のクラス プロパティしきい値を指定します。*value* の形式は、設定されているクラス プロパティしきい値によって異なる場合があります。必要な形式を確認するには、**set deescalating ?** または **set escalating ?** コマンドをイーサネット アップリンク統計情報しきい値ポリシー クラス プロパティしきい値モードで入力します。

	コマンドまたはアクション	目的
		（注） 降格と昇格の両方のクラス プロパティしきい値を指定できます。
ステップ 8	UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、イーサネット エラー統計情報のアップリンク イーサネット ポート統計情報しきい値ポリシー クラスを作成し、巡回冗長検査（CRC）エラー カウント プロパティを作成し、各ポーリング間隔の通常の CRC エラー カウントを 1000 に指定し、通常超えの警告しきい値 1250 を作成し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink* # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy* # create class ether-error-stats
UCS-A /eth-uplink/stats-threshold-policy/class* # create property crc-delta
UCS-A /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
UCS-A /eth-uplink/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
1250
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

アップリンク イーサネット ポートの統計情報しきい値ポリシー クラスの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope stats-threshold-policy default**	イーサネット アップリンク統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCS-A /eth-uplink/stats-threshold-policy # **delete class** *class-name*	指定した統計情報しきい値ポリシー クラスをポリシーから削除します。
ステップ 4	UCS-A /eth-uplink/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次に、イーサネット エラー統計情報のアップリンク イーサネット ポート統計情報しきい値ポリシー クラスを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope stats-threshold-policy default
```

```
UCS-A /eth-uplink/stats-threshold-policy # delete class ether-error-stats
UCS-A /eth-uplink/stats-threshold-policy* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy #
```

サーバ ポート、シャーシ、およびファブリック インターコネクトの統計情報しきい値ポリシー設定

サーバポート、シャーシ、およびファブリックインターコネクトの統計情報しきい値ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope stats-threshold-policy default**	イーサネット サーバ統計情報しきい値ポリシー モードを開始します。 （注） サーバ ポート、シャーシ、およびファブリック インターコネクトの統計情報しきい値ポリシーの作成（または削除）はできません。既存のデフォルト ポリシーに入る（スコープを設定する）ことだけが可能です。
ステップ 3	UCS-A /eth-server/stats-threshold-policy # **set descr** *description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /eth-server/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、デフォルトのサーバポート、シャーシ、およびファブリックインターコネクト統計情報しきい値ポリシーに入り、ポリシーの説明を記入し、トランザクションをコミットします。

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # set descr "Server port, chassis, and fabric
interconnect stats threshold policy."
UCS-A /eth-server/stats-threshold-policy* # commit-buffer
UCS-A /eth-server/stats-threshold-policy #
```

次の作業

統計情報しきい値ポリシーに 1 つ以上のポリシー クラスを設定します。詳細については、「サーバ ポート、シャーシ、およびファブリック インターコネクトの統計情報しきい値ポリシー クラスの設定, （44 ページ）」を参照してください。

サーバポート、シャーシ、およびファブリックインターコネクトの統計情報しきい値ポリシー クラスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope stats-threshold-policy default**	イーサネット サーバ統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCS-A /eth-server/stats-threshold-policy # **create class** *class-name*	指定された統計情報しきい値ポリシー クラスを作成し、イーサネット サーバ統計情報しきい値ポリシー クラス モードを開始します。*class-name* 引数は、設定されている特定の統計情報しきい値ポリシーに使用できるクラス名キーワードのいずれかになります。使用可能なクラス名キーワードのリストを表示するには、**create class ?** コマンドをイーサネット サーバ統計情報しきい値ポリシー モードで入力します。 （注） 統計情報しきい値ポリシーには複数のクラスを設定できます。
ステップ 4	UCS-A /eth-server/stats-threshold-policy /class # **create property** *property-name*	指定された統計情報しきい値ポリシー クラス プロパティを作成し、サーバ アップリンク統計情報しきい値ポリシー クラス プロパティ モードを開始します。*property-name* 引数は、設定されている特定の統計情報しきい値ポリシー クラスに使用できるプロパティ名キーワードのいずれかになります。使用可能なプロパティ名キーワードのリストを表示するには、**create property ?** コマンドをイーサネット サーバ統計情報しきい値ポリシー クラス モードで入力します。 （注） ポリシークラスには複数のプロパティを設定できます。
ステップ 5	UCS-A /eth-server/stats-threshold-policy /class/property # **set normal-value** *value*	クラス プロパティに通常値を指定します。*value* の形式は、設定しているクラス プロパティによって異なる場合があります。必要な形式を確認するには、**set normal-value ?** コマンドをイーサネット サーバ統計情

	コマンドまたはアクション	目的
		報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 6	UCS-A /eth-server/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**} {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	クラス プロパティに、指定したしきい値を作成し、イーサネット サーバ統計情報しきい値ポリシークラスプロパティしきい値モードを開始します。 （注） クラスプロパティに対して複数のしきい値を設定できます。
ステップ 7	UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	降格または昇格のクラス プロパティしきい値を指定します。*value* の形式は、設定されているクラス プロパティしきい値によって異なる場合があります。必要な形式を確認するには、**set deescalating ?** または **set escalating ?** コマンドをイーサネット サーバ統計情報しきい値ポリシークラスプロパティしきい値モードで入力します。 （注） 降格と昇格の両方のクラスプロパティしきい値を指定できます。
ステップ 8	UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、シャーシ統計情報にサーバポート、シャーシ、ファブリックインターコネクト統計情報しきい値ポリシー クラスを作成し、入力電力（W）プロパティを作成し、通常電力を 8 kW に指定し、通常超えの警告しきい値 11 kW を作成し、トランザクションをコミットします。

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # create class chassis-stats
UCS-A /eth-server/stats-threshold-policy/class* # create property input-power
UCS-A /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
UCS-A /eth-server/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
11000.0
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value #
```

サーバポート、シャーシ、およびファブリックインターコネクトの統計情報しきい値ポリシー クラスの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope stats-threshold-policy default**	イーサネット サーバ統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCS-A /eth-server/stats-threshold-policy # **delete class** *class-name*	指定した統計情報しきい値ポリシー クラスをポリシーから削除します。
ステップ 4	UCS-A /eth-server/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、シャーシ統計情報のファブリック インターコネクト統計情報しきい値ポリシー クラス、シャーシ、サーバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # delete class chassis-stats
UCS-A /eth-server/stats-threshold-policy* # commit-buffer
UCS-A /eth-server/stats-threshold-policy #
```

ファイバ チャネル ポートの統計情報しきい値ポリシー設定

ファイバ チャネル ポートの統計情報しきい値ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope stats-threshold-policy default**	ファイバチャネルアップリンク統計情報しきい値ポリシー モードを開始します。

	コマンドまたはアクション	目的
		（注） アップリンク ファイバ チャネル ポート統計情報しきい値ポリシーの作成（または削除）は実行できません。既存のデフォルトポリシーに入る（スコープを設定する）ことだけが可能です。
ステップ 3	UCS-A /fc-uplink/stats-threshold-policy # **set descr** *description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /fc-uplink/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、デフォルトアップリンク ファイバチャネル ポート統計情報しきい値ポリシーに入り、ポリシーの説明を記入し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy* # set descr "Uplink Fibre Channel stats threshold
 policy."
UCS-A /fc-uplink/stats-threshold-policy* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy #
```

次の作業

統計情報しきい値ポリシーに 1 つ以上のポリシー クラスを設定します。詳細については、「ファイバ チャネル ポートの統計情報しきい値ポリシー クラスの設定, （47 ページ）」を参照してください。

ファイバ チャネル ポートの統計情報しきい値ポリシー クラスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope stats-threshold-policy default**	ファイバ チャネル アップリンク統計情報しきい値ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fc-uplink/stats-threshold-policy # **create class** *class-name*	指定された統計情報しきい値ポリシークラスを作成し、ファイバ チャネル アップリンク統計情報しきい値ポリシー クラス モードを開始します。*class-name* 引数は、設定されている特定の統計情報しきい値ポリシーに使用できるクラス名キーワードのいずれかになります。使用可能なクラス名キーワードのリストを表示するには、**create class ?** コマンドをファイバ チャネル アップリンク統計情報しきい値ポリシー モードで入力します。 （注） 統計情報しきい値ポリシーには複数のクラスを設定できます。
ステップ 4	UCS-A /fc-uplink/stats-threshold-policy /class # **create property** *property-name*	指定された統計情報しきい値ポリシークラスプロパティを作成し、ファイバ チャネル アップリンク統計情報しきい値ポリシー クラス プロパティ モードを開始します。*property-name* 引数は、設定されている特定の統計情報しきい値ポリシー クラスに使用できるプロパティ名キーワードのいずれかになります。使用可能なプロパティ名キーワードのリストを表示するには、**create property ?** コマンドをファイバ チャネル アップリンク統計情報しきい値ポリシークラスモードで入力します。 （注） ポリシー クラスには複数のプロパティを設定できます。
ステップ 5	UCS-A /fc-uplink/stats-threshold-policy /class/property # **set normal-value** *value*	クラス プロパティに通常値を指定します。*value* の形式は、設定しているクラス プロパティによって異なる場合があります。必要な形式を確認するには、**set normal-value ?** コマンドをファイバ チャネル アップリンク統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 6	UCS-A /fc-uplink/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**} {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	クラスプロパティに、指定したしきい値を作成し、ファイバ チャネル アップリンク統計情報しきい値ポリシー クラス プロパティしきい値モードを開始します。 （注） クラスプロパティに対して複数のしきい値を設定できます。
ステップ 7	UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	降格または昇格のクラス プロパティしきい値を指定します。*value* の形式は、設定されているクラス プロパティしきい値によって異なる場合があります。必要な形式を確認するには、**set deescalating ?** または **set escalating ?** コマンドをファイバ チャネル アップリンク統計情報

	コマンドまたはアクション	目的
		しきい値ポリシー クラス プロパティしきい値モードで入力します。 （注） 降格と昇格の両方のクラスプロパティしきい値を指定できます。
ステップ 8	UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例は、ファイバ チャネル統計情報にアップリンク ファイバ チャネル ポート統計情報しきい値ポリシークラスを作成し、平均受信バイトプロパティを作成し、通常の各ポーリング間隔の平均受信バイト数を 150 MB に指定し、通常超えの警告しきい値 200 MB を作成し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy* # create class fc-stats
UCS-A /fc-uplink/stats-threshold-policy/class* # create property bytes-rx-avg
UCS-A /fc-uplink/stats-threshold-policy/class/property* # set normal-value 150000000
UCS-A /fc-uplink/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
200000000
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value #
```

アップリンク ファイバ チャネル ポートの統計情報しきい値ポリシー クラスの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope stats-threshold-policy default**	ファイバ チャネル アップリンク統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCS-A /fc-uplink/stats-threshold-policy # **delete class** *class-name*	指定した統計情報しきい値ポリシー クラスをポリシーから削除します。
ステップ 4	UCS-A /fc-uplink/stats-threshold-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次に、ファイバ チャネル統計情報のアップリンク ファイバ チャネル ポート統計情報しきい値ポリシー クラスを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy # delete class fc-stats
UCS-A /fc-uplink/stats-threshold-policy* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy #
```

第 4 章

Call Home の設定

この章は、次の項で構成されています。

Call Home

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 は CLI の適切な **show** コマンドを実行し、そのコマンドの出力をメッセージに添付します。

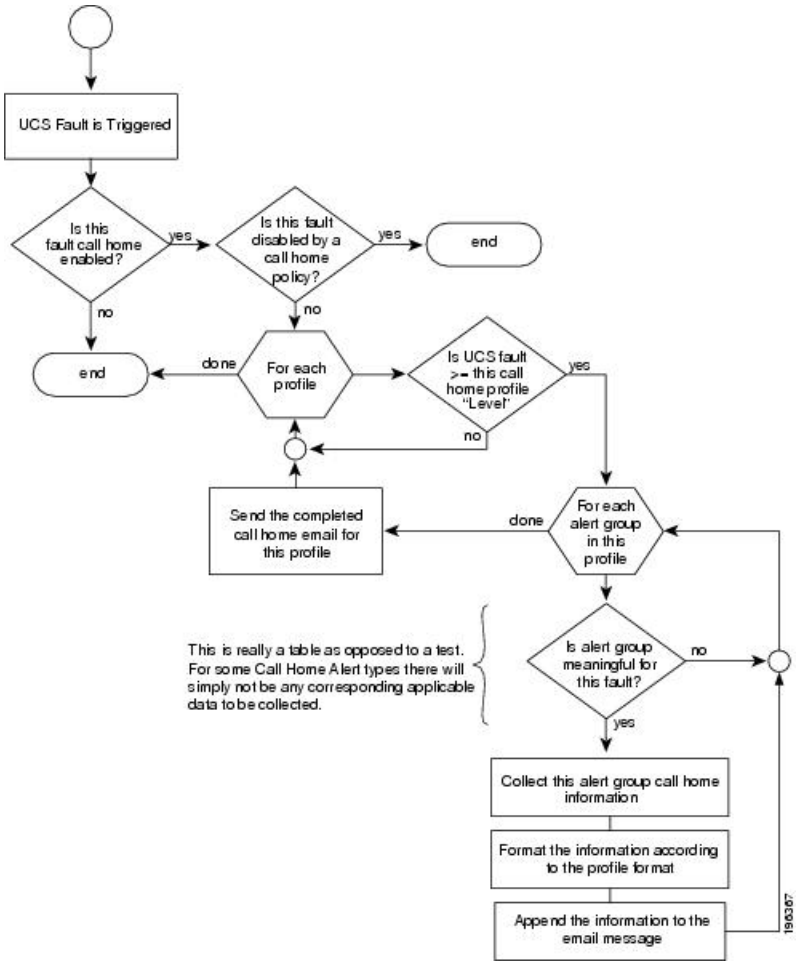
Cisco UCS では、Call Home メッセージが次のフォーマットで配信されます。

- 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 アラートをトリガー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 *1*：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 により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。

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開発されています。 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 *1*：障害と *Call Home* の重大度のマッピング

Call Home の重大度	Cisco UCS Fault	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。

Call Home の重大度	Cisco UCS Fault	Call Home での意味
(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	警告（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。

（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 CCO 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、シスコからダウンロードできます。

Smart Call Home を設定するには、次の手順を実行する必要があります。

- 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。
- Cisco UCS ドメイン ドメインの Call Home Customer ID として使用する予定の CCO 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、CCO の Profile Manager の Additional Access の下にあるアカウント プロパティ内で更新できます。

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。

Call Home の設定

手順

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

	コマンドまたはアクション	目的
ステップ 5	UCS-A /monitoring/callhome # **set email** *email-addr*	主要 Call Home 連絡先の電子メールアドレスを指定します。 （注） 電子メール アドレスに #（ハッシュ記号）、スペース、&（アンパサンド）などの特殊文字が含まれていると、電子メールサーバが電子メールメッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メールアドレスを使用することをお勧めします。
ステップ 6	UCS-A /monitoring/callhome # **set phone-contact** *phone-num*	主要 Call Home 連絡先の電話番号を指定します。+（プラス記号）と国番号から始まる国際形式の番号を入力する必要があります。
ステップ 7	UCS-A /monitoring/callhome # **set street-address** *street-addr*	主要 Call Home 連絡先の住所を指定します。 255 文字以下の ASCII 文字で入力します。
ステップ 8	UCS-A /monitoring/callhome # **set customer-id** *id-num*	ライセンス上のサポート契約の契約番号を含む CCO ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 9	UCS-A /monitoring/callhome # **set contract-id** *id-num*	サービス契約の契約 ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 10	UCS-A /monitoring/callhome # **set site-id** *id-num*	サービス契約のサイト ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 11	UCS-A /monitoring/callhome # **set from-email** *email-addr*	Call Home メッセージの [From] フィールドで使用する電子メール アドレスを指定します。
ステップ 12	UCS-A /monitoring/callhome # **set reply-to-email** *email-addr*	Call Home メッセージの [Reply To] フィールドで使用する電子メール アドレスを指定します。
ステップ 13	UCS-A /monitoring/callhome # **set hostname** {*hostname* | *ip-addr*|*ip6-addr*}	電子メール メッセージを送信するために Call Home が使用する SMTP サーバのホスト名、IPv4 または IPv6アドレスを指定します。
ステップ 14	UCS-A /monitoring/callhome # **set port** *port-num*	電子メール メッセージを送信するために Call Home が使用する SMTP サーバ ポートを指定します。有効なポート番号は 1 ～ 65535 です。
ステップ 15	UCS-A /monitoring/callhome # **set throttling** {**off** | **on**}	Call Home スロットリングをイネーブルまたはディセーブルにします。イネーブルにされると、スロッ

	コマンドまたはアクション	目的
		トリングはあまりにも多くのCall Home電子メールメッセージが同じイベントに対して送信されるのを防ぎます。デフォルトでは、スロットリングはイネーブルです。
ステップ 16	UCS-A /monitoring/callhome # **set urgency {alerts | critical | debugging | emergencies | errors | information | notifications | warnings}**	Call Home電子メール メッセージの緊急性レベルを指定します。ファブリック インターコネクトのペアが複数存在する大規模な UCS 配置のコンテキストでは、緊急性レベルによってある特定の Cisco UCS ドメインからの Call Home メッセージに別のものより高い重要性を付与することが可能になります。2 つのファブリック インターコネクトだけを含む小さい UCS 配置のコンテキストでは、緊急性レベルはほとんど意味を持ちません。
ステップ 17	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

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

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

```
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Call Home のディセーブル化

手順

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

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

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

Call Home のイネーブル化

手順

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

次に、Call Home をイネーブルにし、トランザクションをコミットする例を示します。

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

システム インベントリ メッセージの設定

システム インベントリ メッセージの設定

手順

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

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

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

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

システム インベントリ メッセージの送信

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

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

手順

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

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

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

Call Home プロファイルの設定

Call Home プロファイル

Call Home プロファイルは、指定した受信者に送信されるアラートを決定します。プロファイルを設定して、必要な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のチームがある場合があります。このハードウェアのチームは、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。ただし、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 グループ機能を使用すると、定義済みまたは Call Home プロファイルに送信する一連の Call Home アラートを選択できます。 は、Call Home アラートが宛先プロファイルにアソシエートされたいずれかのアラート グループに属する場合、およびアラートで、Call Home メッセージ重大度が宛先プロファイルに設定されているメッセージ重大度と同じか、それ以上である場合のみ、Call Home アラートを宛先プロファイルの電子メールの宛先に送信します。

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。
診断	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。
Environmental	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。

Call Home プロファイルの設定

デフォルトでは、Cisco TAC-1 プロファイルを設定する必要があります。ただし、指定したレベルでイベントが発生したときに、指定された 1 つ以上のグループに電子メール アラートを送信するために、追加プロファイルを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **create profile** *profile-name*	モニタリング Call Home プロファイル モードを開始します。
ステップ 4	UCS-A /monitoring/callhome/profile # **set level** {**critical** | **debug** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}	プロファイルのイベント レベルを指定します。各プロファイル固有のイベント レベルを設定できます。 そのイベント レベル以上の Cisco UCS 障害が、このプロファイルをトリガーします。
ステップ 5	UCS-A /monitoring/callhome/profile # **set alertgroups** *group-name* • **ciscotac** • **diagnostic** • **environmental** • インベントリ • **license** • **lifecycle** • **linecard** • **supervisor** • **syslogport** • **system** • **test**	プロファイルに基づいてアラートを受け取る 1 つ以上のグループを指定します。*group-name* 引数には、同一コマンドラインで入力される、次のキーワードを 1 つ以上設定できます。
ステップ 6	UCS-A /monitoring/callhome/profile # **add alertgroups** *group-names*	（任意） Call Home プロファイルに基づいて警告を受け取るグループの既存のリストに 1 つ以上のグループを追加します。

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

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

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

Call Home プロファイルの削除

手順

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

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

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

テスト Call Home アラートの送信

はじめる前に

Call Home と Call Home プロファイルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **send-test-alert** {[**alert-group** {**diagnostic** | **environmental**}] [**alert-level** {**critical** | **debug** | **fatal** | **major** | **minor** | **normal** | **notify** |	テスト Call Home アラートを送信します。テスト Call Home アラートは、すべての **alert-*** パラメータを指定する必要があり、そうしなければ Cisco UCS Manager はテスト メッセージを生成

	コマンドまたはアクション	目的
	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*]}	できません。**alert-*** パラメータには以下が含まれています。 • **alert-description**：アラート説明 • **alert-group**：アラート グループ • **alert-level**：イベントの重大度 • **alert-message-type**：メッセージ タイプ • **alert-message-subtype**：メッセージ サブタイプ Call Home テスト アラートを送信されると、Call Home は他のアラートと同様に応答し、設定された宛先電子メール アドレスにこれを転送します。

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

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

Call Home ポリシーの設定

Call Home ポリシー

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

ある種類の障害またはイベントに対してアラートをディセーブルするには、その種類に対して Call Home ポリシーを作成する必要があります。まず最初にその種類に対してポリシーを作成し、次にポリシーをディセーブルにします。

Call Home ポリシー

ヒント　デフォルトでは、重要なシステム イベントすべてについて、アラートが電子メールで送信されます。しかし、必要に応じて、Call Home ポリシーで、その他の重要なシステム イベントに対するアラート メールの送信をイネーブルにするか、ディセーブルにするかを設定することができます。

手順

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

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

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

Call Home ポリシーのディセーブル化

手順

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

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

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

Call Home ポリシーのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **scope policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}	指定したポリシーでモニタリング Call Home ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /monitoring/callhome/policy # **enable**	指定したポリシーをイネーブルにします。
ステップ 5	UCS-A /monitoring/callhome/policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

Call Home ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリングモードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **delete policy** {**equipment-inoperable** | **fru-problem** | **identity-unestablishable** | **thermal-problem** | **voltage-problem**}	指定されたポリシーを削除します
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

Anonymous Reporting の設定

Anonymous Reporting のイネーブル化

Call Home サーバで Anonymous Reporting をイネーブルにできます。

手順

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

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

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

Anonymous Reporting のディセーブル化

Call Home サーバで Anonymous Reporting をディセーブルにできます。

手順

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

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

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

Anonymous レポートの表示

Call Home サーバから Anonymous レポートを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A/monitoring # **scope callhome**	モニタリング Call Home モードを開始します。

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

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

```
UCS-A # scope monitoring
UCS-A/monitoring # scope callhome
UCS-A/monitoring/callhome # scope anonymous-reporting
UCS-A/monitoring/callhome/anonymous-reporting # show detail
UCS-A/monitoring/callhome/anonymous-reporting # show inventory
UCS-A/monitoring/callhome/anonymous-reporting # show content
<anonymousData>
<discreteData
smartCallHomeContract="false"
ethernetMode="EndHost"
fcMode="EndHost"
disjointL2Used="false"
fabricFailoverUsed="false"
numVnicAdaptTempl="3"
numServiceProfiles="7"
updatingSPtemplUsed="false"
initialSPtemplUsed="true"
lanConnPolicyUsed="true"
sanConnPolicyUsed="false"
updatingAdaptTemplUsed="false"
initialAdaptTemplUsed="true"
numMsoftVMnets="10"
numOfVMs="3"
discreteFEX="false"
ucsCentralConnected="false"/>
<bladeUnit
chassisId="1"
slotId="4"
…..
```

例：Smart Call Home 用の Call Home の設定

Smart Call Home の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **enable**	Call Home をイネーブルにします。
ステップ 4	UCS-A /monitoring/callhome # **set contact***name*	Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。
ステップ 5	UCS-A /monitoring/callhome # **set email***email-addr*	主要 Call Home 連絡先の電子メールアドレスを指定します。 Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。
ステップ 6	UCS-A /monitoring/callhome # **set phone-contact***phone-num*	主要 Call Home 連絡先の電話番号を指定します。+（プラス記号）と国番号から始まる国際形式の番号を入力する必要があります。
ステップ 7	UCS-A /monitoring/callhome # **set street-address***street-addr*	主要 Call Home 連絡先の住所を指定します。
ステップ 8	UCS-A /monitoring/callhome # **set customer-id***id-num*	ライセンス上のサポート契約の契約番号を含む CCO ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 9	UCS-A /monitoring/callhome # **set contract-id***id-num*	サービス契約の契約 ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 10	UCS-A /monitoring/callhome # **set site-id***id-num*	サービス契約のサイト ID 番号を指定します。番号は、最大 255 文字の自由なフォーマットの英数字です。
ステップ 11	UCS-A /monitoring/callhome # **set from-email***email-addr*	Call Home メッセージの [From] フィールドで使用する電子メール アドレスを指定します。

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

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

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

次の作業

Smart Call Home を使用するよう Call Home プロファイルを設定するには、「デフォルトの Cisco TAC-1 プロファイルの設定, （75 ページ）」へ進みます。

デフォルトの Cisco TAC-1 プロファイルの設定

CiscoTAC-1 プロファイルのデフォルト設定は次のとおりです。

- 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

はじめる前に

「Smart Call Home の設定, （73 ページ）」セクションを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /monitoring/callhome # **scope profile CiscoTac-1**	デフォルト Cisco TAC-1 プロファイルのモニタリング Call Home プロファイル モードを開始します。
ステップ 2	UCS-A /monitoring/callhome/profile # **set level normal**	プロファイルのイベント レベルに **normal** を指定します。
ステップ 3	UCS-A /monitoring/callhome/profile # **set alertgroups ciscotac**	プロファイルに **ciscotac** アラート グループを指定します。
ステップ 4	UCS-A /monitoring/callhome/profile # **set format xml**	電子メール メッセージのフォーマットを **xml** に指定します。
ステップ 5	UCS-A /monitoring/callhome/profile # **set maxsize 5000000**	電子メール メッセージに最大サイズ **5000000** を指定します。
ステップ 6	UCS-A /monitoring/callhome/profile # **create destination callhome@cisco.com**	電子メール受信者を **callhome@cisco.com** に指定します。
ステップ 7	UCS-A /monitoring/callhome/profile/destination # **exit**	モニタリング Call Home プロファイル モードを終了します。
ステップ 8	UCS-A /monitoring/callhome/profile # **exit**	モニタリング Call Home モードを終了します。

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

```
UCS-A /monitoring/callhome* # scope profile CiscoTac-1
```

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

次の作業

「Smart Call Home 用のシステム インベントリ メッセージの設定, （76 ページ）」に進んで、Smart Call Home で使用するシステム インベントリ メッセージを設定します。

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

はじめる前に

「デフォルトの Cisco TAC-1 プロファイルの設定, （75 ページ）」セクションを完了します。

手順

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

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

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

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

次の作業

Smart Call Home 登録プロセスを開始するインベントリ メッセージを送信するには、「Smart Call Home の登録, （77 ページ）」に進みます。

Smart Call Home の登録

はじめる前に

「Smart Call Home 用のシステム インベントリ メッセージの設定, （76 ページ）」セクションを完了します。

手順

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

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

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

次の作業

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

1. 電子メール内のリンクをクリックします。

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

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

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

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

第 5 章

システム イベント ログの管理

この章は、次の項で構成されています。

システム イベント ログ

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

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

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

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

サーバのシステム イベント ログの表示

各サーバのシステム イベント ログの表示

手順

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

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

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

     c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Deasserted
    d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber | Deasserted

     e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
 Asserted
     f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
    10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted
```

シャーシ内の全サーバのシステム イベント ログの表示

手順

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

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

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

     c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Deasserted
    d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber | Deasserted

     e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
 Asserted
     f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
    10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted
```

SEL ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope ep-log-policy sel**	組織エンドポイント ログ ポリシー モードを開始し、SEL ポリシーにスコープします。
ステップ 3	UCS-A /org/ep-log-policy # **set description***description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**]	バックアップ操作をトリガーするアクションを指定します。
ステップ 5	UCS-A /org/ep-log-policy # **set backup clear-on-backup** {**no** | **yes**}	バックアップ操作の発生後にシステム イベント ログをクリアするかどうかを指定します。
ステップ 6	UCS-A /org/ep-log-policy # **set backup destination** *URL*	バックアップ操作のプロトコル、ユーザ、パスワード、リモート ホスト名、リモート パスを指定します。使用するプロトコルに応じ、次の構文のいずれかを指定して URL を指定します。 • **ftp:**//*username*@*hostname*/*path* • **scp:**//*username*@*hostname*/*path* • **sftp:**//*username*@*hostname*/*path* • **tftp:**//*hostname*:*port-num*/*path* （注） バックアップ先は、**set backup hostname**、**set backup password**、**set backup protocol**、**set backup remote-path**、**set backup user**、または **set backup destination** コマンドを使用して指定することもできます。いずれかの方法を使用してバックアップ先を指定します。
ステップ 7	UCS-A /org/ep-log-policy # **set backup format** {*ascii* | *binary*}	バックアップ ファイルの形式を指定します。
ステップ 8	UCS-A /org/ep-log-policy # **set backup hostname** {*hostname* | *ip-addr*}	リモート サーバのホスト名または IP アドレスを指定します。
ステップ 9	UCS-A /org/ep-log-policy # **set backup interval** {**1-hour** | **2-hours** | **4-hours** | **8-hours** | **24-hours** | **never**}	自動バックアップ操作の間隔を指定します。**never** キーワードを指定すると、自動バックアップは実行されません。
ステップ 10	UCS-A /org/ep-log-policy # **set backup password***password*	ユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 11	UCS-A /org/ep-log-policy # **set backup protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモート サーバとの通信時に使用するプロトコルを指定します。

	コマンドまたはアクション	目的
ステップ 12	UCS-A /org/ep-log-policy # **set backup remote-path***path*	バックアップ ファイルが保存されるリモート サーバのパスを指定します。
ステップ 13	UCS-A /org/ep-log-policy # **set backup user** *username*	システムがリモート サーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 14	UCS-A /org/ep-log-policy # **commit-buffer**	トランザクションをコミットします。

次の例は、システム イベント ログ（ASCII 型式）を 24 時間ごとまたはログがいっぱいになったときにバックアップするよう、またバックアップ操作発生後にシステムイベントログをクリアするよう SEL ポリシーを設定し、トランザクションをコミットします。

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

サーバのシステム イベント ログのバックアップ

個々のサーバのシステム イベント ログのバックアップ

はじめる前に

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

手順

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

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

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

シャーシ内の全サーバのシステム イベント ログのバックアップ

はじめる前に

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

手順

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

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

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

サーバのシステム イベント ログのクリア

個々のサーバのシステム イベント ログのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **clear sel** *chassis-id*/*blade-id*	システム イベント ログをクリアします。

	コマンドまたはアクション	目的
ステップ 2	UCS-A# **commit-buffer**	トランザクションをコミットします。

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

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

シャーシ内の全サーバのシステム イベント ログのクリア

手順

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

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

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

第 6 章

障害、イベント、およびログの設定

この章は、次の項で構成されています。

障害収集ポリシーの設定

グローバル障害ポリシー

グローバル障害ポリシーは、障害がクリアされた日時、フラッピング間隔（障害発生とクリア状態の間の時間）、および保持間隔（システムで障害が発生していた時間）など、Cisco UCS ドメイン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 は障害を生成します。これはアクティブな状態です。
2. 障害が軽減されると、フラッピングまたはフラッピングを防ぐことを目的としたソーキング間隔になります。障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。フラッピング間隔のうち、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。

障害収集ポリシーの設定

手順

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

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

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

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

障害抑制の設定

フォールト抑制

フォールト抑制を使用すると、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。 フォールト抑制タスクを作成し、一時的な障害がレイズ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ユーザによって手動で停止されるまで抑制されたままになります。 障害抑制が終了すると、Cisco UCS Manager はクリアされなかった未処理の抑制された障害に関する通知を送信します。

障害抑制では以下を使用します。

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。
- スケジュールを使用すると、1 回のみの実行にも、定期的なスケジュールの設定にも使用でき、保存および再利用が可能です。

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 によって定義されます。

- **default-chassis-all-maint**：シャーシ内のすべてのブレード サーバ、電源、ファン モジュール、および IOM の障害を抑制します。

  このポリシーは、シャーシ レベルでのみ選択できます。

- **default-chassis-phys-maint**：シャーシ内のすべてのファン モジュールおよび I/O モジュールの障害を抑制します。

  このポリシーは、シャーシ レベルでのみ選択できます。

- **default-fex-all-maint**：FEX 内のすべてのラックマウント サーバ、電源、ファン モジュール、および IOM の障害を抑制します。

  このポリシーは、FEX レベルでのみ選択できます。

- **default-fex-phys-maint**：FEX 内のすべてのファン モジュールおよび I/O モジュールの障害を抑制します。

このポリシーは、FEX レベルでのみ選択できます。

- **default-server-maint**：すべてのブレードサーバおよびラックマウントサーバの障害を抑制します。

  このポリシーは、シャーシ、FEX、組織、およびサービスプロファイルレベルで選択できます。

- **default-iom-maint**：シャーシまたは FEX 内のすべての 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 レベルで選択できます。

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 と の両方で編集できるようになります。 ただし、変更できるのは固定時間間隔を使用するか でスケジュールを使用するかの切り替えのみです。

シャーシに対する障害抑制の設定

固定時間間隔を使用したシャーシに対する障害抑制タスクの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
ステップ 2	UCS-A/chassis # **create fault-suppress-task** *name*	シャーシで障害抑制タスクを作成し、障害抑制タスクモードを開始します。 This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

	コマンドまたはアクション	目的
ステップ 3	UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*	適用する障害抑制ポリシーを指定します。次のいずれかになります。 • default-chassis-all-maint—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs. • default-chassis-phys-maint—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis. • default-server-maint—Suppresses faults for servers. （注） When applied to a chassis, only servers are affected. • default-iom-maint—Suppresses faults for IOMs in a chassis or FEX.
ステップ 4	UCS-A/chassis/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケジュール モードを開始します。
ステップ 5	UCS-A/chassis/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 6	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 7	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 8	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

スケジュールを使用したシャーシに対する障害抑制タスクの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
ステップ 2	UCS-A/chassis # **create fault-suppress-task** *name*	シャーシで障害抑制タスクを作成し、障害抑制タスク モードを開始します。 This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
ステップ 3	UCS-A/chassis/fault-suppress-task # **set schedule** *name*	使用するスケジュールを指定します。 （注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。
ステップ 4	UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*	適用する障害抑制ポリシーを選択します。次のいずれかになります。 • default-chassis-all-maint—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs. • default-chassis-phys-maint—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis. • default-server-maint—Suppresses faults for servers. （注） When applied to a chassis, only servers are affected. • default-iom-maint—Suppresses faults for IOMs in a chassis or FEX.

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

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

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

シャーシに対する障害抑制タスクの削除

手順

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

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

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

シャーシに対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.

	コマンドまたはアクション	目的
ステップ 2	UCS-A/chassis # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します
ステップ 3	UCS-A/chassis/fault-suppress-task # **set fault-suppress-policy** *policy-name*	障害抑制ポリシーを変更します。次のいずれかになります。 • default-chassis-all-maint—Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs. • default-chassis-phys-maint—Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis. • default-server-maint—Suppresses faults for servers. • default-iom-maint—Suppresses faults for IOMs in a chassis or FEX. （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 4 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/chassis/fault-suppress-task # **set schedule** *name*	使用するスケジュールを適用します。 （注） 一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。 スケジュールから一定時間間隔に変更すると、スケジュールへの参照がコミットするときにクリアされます。
ステップ 5	UCS-A/chassis/fault-suppress-task # **scope local-schedule**	ローカルスケジュールモードを開始します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A/chassis/fault-suppress-task/local-schedule # **scope occurrence single-one-time**	single-one-time モードを開始します。
ステップ 7	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 8	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。
ステップ 9	UCS-A/chassis/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

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

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

シャーシに対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis***chassis-num*	指定したシャーシでシャーシモードを開始します。
ステップ 2	UCS-A/chassis # **show fault suppressed**	シャーシに対する抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。

	コマンドまたはアクション	目的
ステップ 3	UCS-A/chassis # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 4	UCS-A/chassis/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

次に、シャーシに対する抑制された障害を表示する例を示します。

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

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

UCS-A/chassis #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

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

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

I/O モジュールに対する障害抑制の設定

固定時間間隔を使用した IOM に対する障害抑制タスクの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom***iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。

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

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

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

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

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

スケジュールを使用した IOM に対する障害抑制タスクの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis***chassis-num* | **fex***fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom***iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **create fault-suppress-task***name*	IOM で障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
ステップ 4	UCS-A/chassis|fex/iom/fault-suppress-task # **set schedule***name*	使用するスケジュールを指定します。

	コマンドまたはアクション	目的
		（注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。
ステップ 5	UCS-A/chassis|fex/iom/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

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

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

IOM に対する障害抑制タスクの削除

手順

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

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

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

```
UCS-A/chassis/iom* # commit-buffer
```

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

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

IOM に対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom***iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 4 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/chassis|fex/iom/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。

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

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

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

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

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

IOM に対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** [**chassis** *chassis-num* | **fex** *fex-num*]	指定したシャーシ または FEX でシャーシ モードを開始します。
ステップ 2	UCS-A /chassis|fex # **scope iom***iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A/chassis|fex/iom # **show fault suppressed**	IOM の抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 4	UCS-A/chassis|fex/iom # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 5	UCS-A/chassis|fex/iom/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

次に、シャーシ上の IOM の抑制された障害を表示する例を示します。

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

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

```
UCS-A/chassis/iom #
```

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

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

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

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

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

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

FEX に対する障害抑制の設定

固定時間間隔を使用したシャーシに対する障害抑制タスクの設定

手順

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

	コマンドまたはアクション	目的
ステップ 3	UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*	適用する障害抑制ポリシーを指定します。次のいずれかになります。 • default-chassis-all-maint シャーシとそのシャーシにインストールされたすべてのコンポーネントの障害を抑制します。コンポーネントには、すべてのサーバ、電源、ファンモジュール、IOM などが含まれます。 • default-chassis-phys-maint シャーシとそのシャーシにインストールされたすべてのファンモジュールと電源の障害を抑制します。 • default-server-maint サーバの障害を抑制します。 （注） シャーシに適用された場合、サーバのみが影響を受けます。 • default-iom-maintシャーシまたは FEX 内の IOM の障害を抑制します。
ステップ 4	UCS-A/fex/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカルスケジュールモードを開始します
ステップ 5	UCS-A/fex/fault-suppress-task/local-schedule # **create occurrence single-one-time**	ワンタイム オカレンスを作成し、single-one-time モードを開始します。
ステップ 6	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set date** *month day-of-month year hour minute seconds*	このオカレンスを実行する日時を指定します。
ステップ 7	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このタスクを実行できる時間の最大長を指定します。タスクを手動で停止するまで実行するには、none または omit this step と入力します。

	コマンドまたはアクション	目的
ステップ 8	UCS-A/fex/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

スケジュールを使用した FEX に対する障害抑制タスクの設定

手順

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

	コマンドまたはアクション	目的
		• default-fex-phys-maint：FEX とその FEX 内のすべてのファン モジュールと電源の障害を抑制します。 • default-iom-maint：シャーシまたは FEX 内の IOM の障害を抑制します。
ステップ 5	UCS-A/fex/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

FEX に対する障害抑制タスクの削除

手順

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

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

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

FEX に対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fex** *fex-num*	指定された FEX の fex モードを開始します。
ステップ 2	UCS-A/fex # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。
ステップ 3	UCS-A/fex/fault-suppress-task # **set fault-suppress-policy** *policy-name*	障害抑制ポリシーを変更します。次のいずれかになります。 • default-fex-all-maint—Suppresses faults for the FEX and all power supplies, fan modules, and IOMs in the FEX. • default-fex-phys-maint—Suppresses faults for the FEX and all fan modules and power supplies in the FEX. • default-iom-maint—Suppresses faults for IOMs in a chassis or FEX. （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 4 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/fex/fault-suppress-task # **set schedule** *name*	一定時間間隔からスケジュールに変更すると、一定時間間隔はコミットするときに消去されます。

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

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

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

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

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

FEX に対する抑制された障害と障害抑制タスクの表示

手順

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

次に、FEX に対する抑制された障害を表示する例を示します。

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

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

UCS-A/fex #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

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

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

サーバに対する障害抑制の設定

固定時間間隔を使用したサーバに対する障害抑制タスクの設定

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

手順

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

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

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

スケジュールを使用したサーバに対する障害抑制タスクの設定

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

手順

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

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

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

サーバに対する障害抑制タスクの削除

手順

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

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

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

サーバに対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバモードを開始します。
ステップ 2	UCS-A/server # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 3 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 4 に進みます。
ステップ 3	UCS-A/server/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。

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

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

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

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

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

サーバに対する抑制された障害と障害抑制タスクの表示

手順

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

次に、サーバに対する抑制された障害を表示する例を示します。

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

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

UCS-A/server #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

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

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

サービス プロファイルに対する障害抑制の設定

固定時間間隔を使用したサービス プロファイルに対する障害抑制タスクの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org***org-name*	指定した組織の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、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create fault-suppress-task** *name*	シャーシで障害抑制タスクを作成し、障害抑制タスク モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
ステップ 4	UCS-A/org/service-profile/fault-suppress-task # **create local-schedule**	ローカル スケジュールを作成し、ローカル スケ

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

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

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

スケジュールを使用したサービス プロファイルに対する障害抑制タスクの設定

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

手順

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

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

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

サービス プロファイルに対する障害抑制タスクの削除

手順

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

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

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

サービス プロファイルに対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org***org-name*	指定した組織の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、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A/org/service-profile # **scope fault-suppress-task** *name*	障害抑制タスクモードを開始します。

	コマンドまたはアクション	目的
		（注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 4 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 5 に進みます。
ステップ 4	UCS-A/org/service-profile/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。

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

	コマンドまたはアクション	目的
ステップ 9	UCS-A/org/service-profile/fault-suppress-task/local-schedule/single-one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

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

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

サービス プロファイルに対する抑制された障害と障害抑制タスクの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org***org-name*	指定した組織の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、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A/org/service-profile # **show fault suppressed**	サーバに対する抑制された障害を表示します。 （注） 選択したコンポーネント内の障害のみが表示されます。
ステップ 4	UCS-A/org/service-profile # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A/org/service-profile/fault-suppress-task # **show detail expand**	タスクのスケジュールまたは固定時間間隔を表示します。

次に、サービス プロファイルに対する抑制された障害を表示する例を示します。

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

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

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

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

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

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

組織に対する障害抑制の設定

固定時間間隔を使用した組織に対する障害抑制タスクの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org***org-name*	指定した組織の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、*/* を *org-name* として入力します。
ステップ 2	UCS-A/org # **create fault-suppress-task** *name*	組織の障害抑制タスクを作成し、障害抑制タスク モードを開始します。

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

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

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

スケジュールを使用した組織に対する障害抑制タスクの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org***org-name*	指定した組織の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、*/* を *org-name* として入力します。
ステップ 2	UCS-A/org # **create fault-suppress-task***name*	組織の障害抑制タスクを作成し、障害抑制タスクモードを開始します。 この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
ステップ 3	UCS-A/org/fault-suppress-task # **set schedule***name*	使用するスケジュールを指定します。 （注） すでにあるスケジュールを障害抑制タスクで使用する必要があります。
ステップ 4	UCS-A/org/fault-suppress-task # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

組織に対する障害抑制タスクの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org***org-name*	指定した組織の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、*/* を *org-name* として入力します。
ステップ 2	UCS-A/org # **delete fault-suppress-task** *name*	指定された障害抑制タスクを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A/org # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例では、task1 と呼ばれる障害抑制タスクを削除する方法を示します。

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

組織に対する障害抑制タスクの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org***org-name*	指定した組織の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、*/* を *org-name* として入力します。
ステップ 2	UCS-A/org # **scope fault-suppress-task** *name*	障害抑制タスク モードを開始します。 （注） 障害抑制タスクに別のスケジュールを適用するには、ステップ 3 に進みます。障害抑制タスクの一定時間間隔を変更するには、ステップ 4 に進みます。
ステップ 3	UCS-A/org/fault-suppress-task # **set schedule** *name*	別のスケジュールを適用します。

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

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

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

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

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

組織に対する抑制された障害と障害抑制タスクの表示

手順

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

次に、組織に対する抑制された障害を表示する例を示します。

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

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

UCS-A/org #
```

次に、task1 と呼ばれる障害抑制タスクを表示する例を示します。

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

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

Core File Exporter の設定

Core File Exporter

コア ファイルが発生すると、Cisco UCSによりただちに Core File Exporter が使用され、それらのファイルが TFTP を介してネットワーク上の指定の場所にエクスポートされます。この機能を使用することにより、tar ファイルをコア 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 の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope sysdebug**	モニタリング システム デバッグ モードを開始します。
ステップ 3	UCS-A /monitoring/sysdebug # **enable core-export-target**	Core File Exporter のイネーブル化Core File Exporter がイネーブルな状態でエラーによりサーバがコア ダンプを実行する場合、システムはコア ファイルを TFTP 経由で指定されたリモート サーバへエクスポートします。
ステップ 4	UCS-A /monitoring/sysdebug # **set core-export-target path** *path*	コア ファイルをリモート サーバにエクスポートするときに使用するパスを指定します。
ステップ 5	UCS-A /monitoring/sysdebug # **set core-export-target port***port-num*	TFTP を介してコア ダンプ ファイルをエクスポートするときに使用するポート番号を指定します。有効な値の範囲は 1 ～ 65,535 です。
ステップ 6	UCS-A /monitoring/sysdebug # **set core-export-target server-description** *description*	コア ファイルを保存するために使用するリモート サーバの説明を加えます。
ステップ 7	UCS-A /monitoring/sysdebug # **set core-export-target server-name***hostname*	TFTP を介して接続するリモート サーバのホスト名を指定します。
ステップ 8	UCS-A /monitoring/sysdebug # **commit-buffer**	トランザクションをコミットします。

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

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

Core File Exporter のディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope sysdebug**	モニタリング システム デバッグ モードを開始します。
ステップ 3	UCS-A /monitoring/sysdebug # **disable core-export-target**	Core File Exporter をディセーブルにします。Core File Exporter がディセーブルの場合、コア ファイルは自動的にエクスポートされません。
ステップ 4	UCS-A /monitoring/sysdebug # **commit-buffer**	トランザクションをコミットします。

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

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

Syslog の設定

手順

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

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring # {**enable** | **disable**} **syslog console**	コンソールへの Syslog の送信をイネーブルまたはディセーブルにします。
ステップ 3	UCS-A /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}	（任意） 表示するメッセージの最低レベルを選択します。syslog がイネーブルの場合、システムはそのレベル以上のメッセージをコンソールに表示します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
ステップ 4	UCS-A /monitoring # {**enable** | **disable**} **syslog monitor**	オペレーティング システムによる syslog 情報のモニタリングをイネーブルまたはディセーブルにします。
ステップ 5	UCS-A /monitoring # **set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	（任意） 表示するメッセージの最低レベルを選択します。モニタの状態がイネーブルの場合、システムはそのレベル以上のメッセージを表示します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。 （注） Critical より下のレベルのメッセージは、**terminal monitor** コマンドを入力した場合にのみ端末モニタに表示されます。
ステップ 6	UCS-A /monitoring # {**enable** | **disable**} **syslog file**	syslog ファイルへの syslog 情報の書き込みをイネーブルまたはディセーブルにします。
ステップ 7	UCS-A /monitoring # **set syslog file name***filename*	メッセージが記録されるファイルの名前。ファイル名は 16 文字まで入力できます。
ステップ 8	UCS-A /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	（任意） ファイルに保存するメッセージの最低レベルを選択します。ファイルの状態がイネーブルの場合、システムはそのレベル以上のメッセージを syslog ファイルに保存します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
ステップ 9	UCS-A /monitoring # **set syslog file size***filesize*	（任意） 最新のメッセージで最も古いものを上書きし始める前の、最大ファイル サイズ（バイト単位）。有効な範囲は 4096 ～ 4194304 バイトです。

	コマンドまたはアクション	目的
ステップ 10	UCS-A /monitoring # {**enable** | **disable**} **syslog remote-destination** {**server-1** | **server-2** | **server-3**}	最大 3 台の外部 syslog サーバへの syslog メッセージの送信をイネーブルまたはディセーブルにします。
ステップ 11	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **level**{**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}	（任意） 外部ログに保存するメッセージの最低レベルを選択します。remote-destination がイネーブルにされると、システムはそのレベル以上を外部サーバに送信します。レベル オプションは緊急性の降順で一覧表示されます。デフォルトのレベルは Critical です。
ステップ 12	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **hostname***hostname*	指定されたリモート Syslog サーバのホスト名または IP アドレス。ホスト名は 256 文字まで入力できます。
ステップ 13	UCS-A /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**}	（任意） 指定されたリモート syslog サーバに送信される syslog メッセージに含まれるファシリティ レベル。
ステップ 14	UCS-A /monitoring # {**enable** | **disable**} **syslog source** {**audits** | **events** | **faults**}	次のいずれかになります。 • audits：すべての監査ログ イベントのロギングを有効化またはディセーブルにします。 • events：すべてのシステム イベントのロギングを有効化またはディセーブルにします。 • faults：すべてのシステム障害のロギングを有効化またはディセーブルにします。
ステップ 15	UCS-A /monitoring # **commit-buffer**	トランザクションをコミットします。

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

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

監査ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティモードを開始します。
ステップ 2	UCS-A /security # **show audit-logs**	監査ログを表示します。

次の例では、監査ログを表示します。

```
UCS-A# scope security
UCS-A /security # show audit-logs
Audit trail logs:
    Creation Time        User       ID       Action           Description

    -------------------- ---------- -------- ---------------- -----------

    2013-01-04T19:05:36.027
                         internal    1055936 Creation         Fabric A:
local us
er admin logge
    2013-01-03T23:08:37.459
                         admin       1025416 Creation         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:08:37.459
                         admin       1025417 Deletion         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:08:02.387
                         admin       1025299 Creation         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:08:02.387
                         admin       1025300 Deletion         Uplink FC
VSAN mem
ber port A/1/3
    2013-01-03T23:03:23.926
                         admin       1025096 Creation         Uplink FC
VSAN mem
ber port A/1/3
UCS-A /security #
```

ログ ファイル エクスポータの設定

ログ ファイル エクスポータ

Cisco UCS Manager は、実行ごとにログ ファイルを生成します。 ログ ファイルのサイズは最大 20 MB で、最大 5 つのバックアップがサーバに保存できます。 ログ ファイル エクスポータにより、ログ ファイルを削除する前にリモート サーバにエクスポートすることができます。 ログ ファイル名には次の情報が含まれます。

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

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

注意事項と制約事項

- ログのエクスポートには、tftp またはパスワードなしの scp または sftp を使用することを推奨します。 標準の scp または sftp が使用される場合、ユーザ パスワードは暗号化された形式でコンフィギュレーション ファイルに保存されます。
- HA セットアップでは、各側からのログ ファイルは別々にエクスポートされます。 一方のログ エクスポートが失敗しても、もう一方が補うことはありません。

リモート サーバへのログ ファイルのエクスポート

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope sysdebug**	モニタリング システム デバッグ モードを開始します。
ステップ 3	UCS-A /monitoring/sysdebug # **scope log-export-policy**	ログ ファイルのエクスポート モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /monitoring/sysdebug/log-export-policy # **set admin-state** {**disabled** | **enabled**}	ログ ファイルのエクスポートが有効かどうか。
ステップ 5	UCS-A /monitoring/sysdebug/log-export-policy # **set desc***description*	（任意） ログのエクスポート ポリシーの説明を入力します。
ステップ 6	UCS-A /monitoring/sysdebug/log-export-policy # **set hostname***hostname*	リモート サーバのホスト名を指定します。
ステップ 7	UCS-A /monitoring/sysdebug/log-export-policy # **set passwd**	Enter キーを押すと、パスワードを入力するように促されます。 リモート サーバのユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 8	UCS-A /monitoring/sysdebug/log-export-policy # **set passwordless-ssh** {**no** | **yes**}	パスワードなしの SSH ログインを有効にします。
ステップ 9	UCS-A /monitoring/sysdebug/log-export-policy # **set proto** {**scp** | **ftp** | **sftp** | **tftp**}	リモート サーバとの通信時に使用するプロトコルを指定します。
ステップ 10	UCS-A /monitoring/sysdebug/log-export-policy # **set path***path*	ログ ファイルが保存されるリモート サーバのパスを指定します。
ステップ 11	UCS-A /monitoring/sysdebug/log-export-policy # **set user***username*	システムがリモート サーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 12	UCS-A /monitoring/sysdebug/log-export-policy # **commit-buffer**	トランザクションをコミットします。

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

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # scope log-export-policy
UCS-A /monitoring/sysdebug/log-export-policy # set admin-state enable
UCS-A /monitoring/sysdebug/log-export-policy* # set hostname 10.10.1.1
UCS-A /monitoring/sysdebug/log-export-policy* # set path /
UCS-A /monitoring/sysdebug/log-export-policy* # set user testuser
UCS-A /monitoring/sysdebug/log-export-policy* # set proto scp
```

```
UCS-A /monitoring/sysdebug/log-export-policy* # set passwd
password:
UCS-A /monitoring/sysdebug/log-export-policy* # set passwordless-ssh yes
UCS-A /monitoring/sysdebug/log-export-policy* # commit-buffer
UCS-A /monitoring/sysdebug/log-export-policy #
```

第 7 章

NetFlow モニタリング

この章は、次の項で構成されています。

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、および Cisco UCS VIC 1225）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。

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すべての情報で構成され、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特性は、フローのすべてのパケットに含まれるバイト数や合計パケット数などの、測定可能な値です。

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。次のタイプのフロー レコード定義を使用できます。

- [System-defined]：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、ネットワーキングのプロパティはプロファイルに含まれるエクスポータ 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 モニタと出力方向の 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 6100 シリーズ Fabric Interconnect ではサポートされません。
- NetFlow モニタリングは、 Cisco UCS1200 および 1300 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 VIC アダプタでは、NetFlow を FCoE トラフィックに対して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。

フロー レコード定義の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-record***flow-record-name*	指定されたフロー レコードのフロー レコード モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-record # **set keytype** {**ipv4keys** | **ipv6keys** | **l2keys**}	キー タイプを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-record # **set ipv4keys** {**dest-port** | **ip-protocol** | **ip-tos** | **ipv4-dest-address** | **ipv4-src-address** | **src-port**}	ステップ 3 で選択したキー タイプの属性を指定します。 （注） ステップ 3 で **ipv4keys** を選択した場合にのみ、このコマンドを使用します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /eth-flow-mon/flow-record # **set ipv6keys** {**dest-port** | **ip-protocol** | **ipv6-dest-address** | **ipv6-src-address** | **src-port**}	ステップ 3 で選択したキー タイプの属性を指定します。 （注） ステップ 3 で **ipv6keys** を選択した場合にのみ、このコマンドを使用します。
ステップ 6	UCS-A /eth-flow-mon/flow-record # **set l2keys** {**dest-mac-address** | **ethertype** | **src-mac-address**}	ステップ 3 で選択したキー タイプの属性を指定します。 （注） ステップ 3 で **l2keys** を選択した場合にのみ、このコマンドを使用します。
ステップ 7	UCS-A /eth-flow-mon/flow-record # **set nonkeys** {**counter-bytes-long** | **counter-packets-long** | **sys-uptime-first** | **sys-uptime-last**}	非キー属性を指定します。
ステップ 8	UCS-A /eth-flow-mon/flow-record # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

エクスポータ プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フローモニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **scope flow-profile***profile-name*	指定されたプロファイルのフロー プロファイル モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-profile # **show config**	フロー プロファイルの設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-flow-mon/flow-profile # **enter vlan***vlan-name*	エクスポータ プロファイルに関連付けられた VLAN を指定します。PVLAN とローカル VLAN はサポートされません。すべての VLAN は公開されており、両方のファブリック インターコネクトに共通である必要があります。
ステップ 5	UCS-A /eth-flow-mon/flow-profile/vlan # **enter fabric** {**a** | **b**}	指定されたファブリックのフロー プロファイル モードを開始します。
ステップ 6	UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **set addr***ip-addr***subnet***ip-addr*	ファブリックのエクスポータ プロファイルの送信元 IP アドレスおよびサブネット マスクを指定します。 **重要** 指定した IP アドレスが、Cisco UCS ドメイン内で一意であるかを確認します。Cisco UCS Manager ですでに使用されている IP アドレスを指定した場合、IP アドレスの競合が発生する可能性があります。
ステップ 7	UCS-A /eth-flow-mon/flow-profile/vlan/fabric/ # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

NetFlow コレクタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-collector***flow-collector-name*	指定されたフロー コレクタのフロー コレクタ モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-collector # **set dest-port***port_number*	フロー コレクタの宛て先ポートを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-collector # **set vlan***vlan_id*	フロー コレクタの VLAN ID を指定します。
ステップ 5	UCS-A /eth-flow-mon/flow-collector # **enter ip-if**	IPv4 コンフィギュレーション モードを開始します。
ステップ 6	UCS-A /eth-flow-mon/flow-collector/ip-if # **set addr***ip-address*	エクスポータ IP アドレスを指定します。
ステップ 7	UCS-A /eth-flow-mon/flow-collector/ip-if # **set exporter-gw***gw-address*	エクスポータ ゲートウェイ アドレスを指定します。
ステップ 8	UCS-A /eth-flow-mon/flow-collector/ip-if # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

フロー エクスポータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-exporter***flow-exporter-name*	指定されたフローエクスポータのフローエクスポータ モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-exporter # **set dscp***dscp_number*	DiffServ コード ポイントを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-exporter # **set flow-collector***flow-collector_name*	フロー コレクタを指定します。
ステップ 5	UCS-A /eth-flow-mon/flow-exporter # **set exporter-stats-timeout***timeout_number*	NetFlow フローエクスポータ データを再送信する場合のタイムアウト期間を指定します。
ステップ 6	UCS-A /eth-flow-mon/flow-exporter # **set interface-table-timeout***timeout_number*	NetFlow フロー エクスポータ インターフェイステーブルの再送信の時間を指定します。
ステップ 7	UCS-A /eth-flow-mon/flow-exporter # **set template-data-timeout***timeout_number*	NetFlow テンプレート データを再送信する場合のタイムアウト期間を指定します。
ステップ 8	UCS-A /eth-flow-mon/flow-exporter # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

フロー モニタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。
ステップ 2	UCS-A /eth-flow-mon # **enter flow-monitor***flow-monitor-name*	指定されたフロー モニタのフロー モニタ モードを開始します。
ステップ 3	UCS-A /eth-flow-mon/flow-monitor # **set flow-record***flow-record-name*	フロー レコードを指定します。
ステップ 4	UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter***flow-exporter-name*	□番目のフローエクスポータを指定します。
ステップ 5	UCS-A /eth-flow-mon/flow-monitor # **create flow-exporter***flow-exporter-name*	2 番目のフローエクスポータを指定します。
ステップ 6	UCS-A /eth-flow-mon/flow-monitor # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次に、フロー モニタを作成し、トランザクションをコミットする例を示します。

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

フロー モニタ セッションの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-flow-mon**	イーサネット フロー モニタ モードを開始します。

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

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

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

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

手順

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

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

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

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

vNIC へのフロー モニタ セッションの関連付け

手順

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

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

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