Cisco UCS Manager GUI 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：2014 年 09 月 08 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 つ以上に責任を持ち、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	用途
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	用途
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}	必ずいずれか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、このドキュメント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　時間を節約する方法です。 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。 機器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、一般的な事故防止対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 マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手できる『*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。

その他のマニュアル リソース

B シリーズと C シリーズのすべてのドキュメントが格納された ISO ファイルは、http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821 で入手できます。 このページで、[Unified Computing System (UCS) Documentation Roadmap Bundle] をクリックします。

ISO ファイルは、ドキュメントのメジャー リリースの後に更新されます。

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、HTML ドキュメント内のフィードバック フォームよりご連絡ください mailto:ucs-docfeedback@cisco.com。 ご協力をよろしくお願いいたします。

第 I 部

システム モニタリング

第 1 章

トラフィックのモニタリング

この章は、次の内容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 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。
- SPAN トラフィックは Cisco UCS 6200 シリーズ ファブリック インターコネクトでは 1 Gbps に速度制限されます。

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

イーサネット トラフィック モニタリング セッションの作成

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。
3. [*Fabric_Interconnect_Name*] を右クリックし、[Create Traffic Monitoring Session] を選択します。
4. [Create Traffic Monitoring Session] ダイアログボックスで、次のフィールドに入力します。
5. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [*Fabric_Interconnect_Name*] を右クリックし、[Create Traffic Monitoring Session] を選択します。

ステップ 4 [Create Traffic Monitoring Session] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Name] フィールド	トラフィック モニタリング セッションの名前。 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で、この名前を変更することはできません。
[Admin State] フィールド	[Destination] フィールドで選択された物理ポートのトラフィックをモニタするかどうか。 次のいずれかになります。 • [Enabled]：ソース コンポーネントがセッションに追加されるとすぐに、Cisco UCS によって、ポート アクティビティのモニタリングが開始されます。 • [Disabled]：Cisco UCS によるポート アクティビティのモニタリングは実行されません。
[Destination] ドロップダウン リスト	その通信トラフィックをモニタする物理ポートをナビゲーション ツリーから選択します。

名前	説明
[Admin Speed] フィールド	モニタされるポート チャネルのデータ転送速度。 使用可能なデータ速度は、Cisco UCS ドメインにインストールされているファブリック インターコネクトによって異なります。

ステップ 5 [OK] をクリックします。

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。

既存のイーサネット トラフィック モニタリング セッションの宛先の設定

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Actions] 領域で、[Set Destination] をクリックします。
5. [Set Destination] ダイアログボックスで、次のフィールドに入力します。
6. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。

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

ステップ 4 [Actions] 領域で、[Set Destination] をクリックします。

ステップ 5 [Set Destination] ダイアログボックスで、次のフィールドに入力します。

例：

名前	説明
[Destination] フィールド	モニタされている物理ポート。
[Admin Speed] フィールド	モニタされるポート チャネルのデータ転送速度。 使用可能なデータ速度は、Cisco UCS ドメインにインストールされているファブリック インターコネクトによって異なります。

ステップ 6 [OK] をクリックします。

既存のイーサネット トラフィック モニタリング セッションの宛先のクリア

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Actions] 領域で、[Clear Destination] をクリックします。
5. Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。

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

ステップ 4 [Actions] 領域で、[Clear Destination] をクリックします。

ステップ 5 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ファイバ チャネル トラフィック モニタリング セッションの作成

手順の概要

1. [Navigation] ペインの [SAN] タブをクリックします。
2. [LAN] タブで、[SAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。
3. [*Fabric_Interconnect_Name*] を右クリックし、[Create Traffic Monitoring Session] を選択します。
4. [Create Traffic Monitoring Session] ダイアログボックスで、次のフィールドに入力します。
5. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [SAN] タブをクリックします。

ステップ 2 [LAN] タブで、[SAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [*Fabric_Interconnect_Name*] を右クリックし、[Create Traffic Monitoring Session] を選択します。

ステップ 4 [Create Traffic Monitoring Session] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Name] フィールド	トラフィック モニタリング セッションの名前。 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で、この名前を変更することはできません。
[Admin State] フィールド	[Destination] フィールドで選択された物理ポートのトラフィックをモニタするかどうか。 次のいずれかになります。 • [Enabled]：ソース コンポーネントがセッションに追加されるとすぐに、Cisco UCS によって、ポート アクティビティのモニタリングが開始されます。 • [Disabled]：Cisco UCS によるポート アクティビティのモニタリングは実行されません。
[Destination] ドロップダウン リスト	その通信トラフィックをモニタする物理ポートをナビゲーション ツリーから選択します。

名前	説明
[管理速度] ドロップダウン リスト	モニタされるポート チャネルのデータ転送速度。 次のいずれかになります。 • [1 Gbps] • [2 Gbps] • [4 Gbps] • [8 Gbps] • [Auto]：Cisco UCS がデータ転送速度を決定します。

ステップ 5 [OK] をクリックします。

次の作業

- 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。

既存のファイバ チャネル モニタリング セッションの宛先の設定

手順の概要

1. [Navigation] ペインの [SAN] タブをクリックします。
2. [SAN] タブで、[SAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Actions] 領域で、[Set Destination] をクリックします。
5. [Set Destination] ダイアログボックスで、次のフィールドに入力します。
6. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [SAN] タブをクリックします。

ステップ 2 [SAN] タブで、[SAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。

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

ステップ 4 [Actions] 領域で、[Set Destination] をクリックします。

ステップ 5 [Set Destination] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Destination] ドロップダウン リスト	その通信トラフィックをモニタする物理ポートをナビゲーション ツリーから選択します。
[管理速度] ドロップダウン リスト	モニタされるポート チャネルのデータ転送速度。 次のいずれかになります。 • [1 Gbps] • [2 Gbps] • [4 Gbps] • [8 Gbps] • [Auto]：Cisco UCS がデータ転送速度を決定します。

ステップ 6 [OK] をクリックします。

既存のファイバ チャネル トラフィック モニタリング セッションの宛先のクリア

手順の概要

1. [Navigation] ペインの [SAN] タブをクリックします。
2. [SAN] タブで、[SAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Actions] 領域で、[Clear Destination] をクリックします。
5. Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [SAN] タブをクリックします。

ステップ 2 [SAN] タブで、[SAN] > [Traffic Monitoring Sessions] > *[Fabric_Interconnect_Name]* > *[Monitor_Session_Name]* を展開します。

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

ステップ 4 [Actions] 領域で、[Clear Destination] をクリックします。

ステップ 5 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

モニタリング セッションへのトラフィック送信元の追加

トラフィック モニタリング セッションがモニタする複数の送信元タイプから複数の送信元を選択できます。 利用可能な送信元は、Cisco UCS ドメインに設定されたコンポーネントによって異なります。

（注） この手順では、イーサネット トラフィックのモニタリング セッションに対して送信元を追加する方法について説明します。 ファイバ チャネルのモニタリング セッションに送信元を追加する場合は、ステップ 2 の [LAN] タブの代わりに [SAN] タブを選択します。

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。

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。
3. [Fabric_Interconnect_Name] を展開し、設定するモニタ セッションをクリックします。
4. [Work] ペインの [General] タブをクリックします。
5. [Sources] 領域で、追加するトラフィック送信元のタイプのセクションを展開します。
6. モニタリングに使用できるコンポーネントを表示するには、テーブルの右端にある [+] ボタンをクリックして [Add Monitoring Session Source] ダイアログボックスを開きます。
7. 送信元のコンポーネントを選択し、[OK] をクリックします。
8. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [Fabric_Interconnect_Name] を展開し、設定するモニタ セッションをクリックします。

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

ステップ 5 [Sources] 領域で、追加するトラフィック送信元のタイプのセクションを展開します。

ステップ 6 モニタリングに使用できるコンポーネントを表示するには、テーブルの右端にある [+] ボタンをクリックして [Add Monitoring Session Source] ダイアログボックスを開きます。

ステップ 7 送信元のコンポーネントを選択し、[OK] をクリックします。
必要に応じて前述の 3 つのステップを繰り返し、複数の送信元のタイプから複数の送信元を追加します。

ステップ 8 [Save Changes] をクリックします。

次の作業

トラフィック モニタリング セッションをアクティブ化します。 セッションがすでにアクティブ化されている場合、トラフィックは送信元の追加時にモニタリングの宛先に転送されます。

トラフィック モニタリング セッションのアクティブ化

（注） この手順では、イーサネット トラフィックのモニタリング セッションをアクティブにする方法について説明します。 ファイバ チャネルのモニタリング セッションをアクティブにするには、ステップ 2 の [LAN] タブの代わりに [SAN] タブを選択します。

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。

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。
3. [Fabric_Interconnect_Name] を展開し、アクティブにするモニタ セッションをクリックします。
4. [Work] ペインの [General] タブをクリックします。
5. [Properties] 領域で、[Admin State] の [enabled] オプション ボタンをクリックします。
6. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。
ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。
ステップ 3 [Fabric_Interconnect_Name] を展開し、アクティブにするモニタ セッションをクリックします。
ステップ 4 [Work] ペインの [General] タブをクリックします。
ステップ 5 [Properties] 領域で、[Admin State] の [enabled] オプション ボタンをクリックします。
ステップ 6 [Save Changes] をクリックします。

トラフィック モニタの送信元が設定されている場合、トラフィック モニタリングの宛先ポートにトラフィックのフローが始まります。

トラフィック モニタリング セッションの削除

（注） この手順では、イーサネット トラフィックのモニタリング セッションを削除する方法について説明します。 ファイバ チャネルのモニタリング セッションを削除するには、ステップ 2 の [LAN] タブの代わりに [SAN] タブを選択します。

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。
3. [Fabric_Interconnect_Name] を展開し、削除するモニタ セッションをクリックします。
4. [Work] ペインの [General] タブをクリックします。
5. [Actions] 領域で、[Delete] アイコンをクリックします。
6. Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。
ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。
ステップ 3 [Fabric_Interconnect_Name] を展開し、削除するモニタ セッションをクリックします。
ステップ 4 [Work] ペインの [General] タブをクリックします。
ステップ 5 [Actions] 領域で、[Delete] アイコンをクリックします。
ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

第 2 章

ハードウェアのモニタリング

この章は、次の内容で構成されています。

ファブリック インターコネクトのモニタリング

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。
3. モニタするファブリック インターコネクトのノードをクリックします。
4. [Work] ペインで次のタブのいずれかをクリックして、ファブリック インターコネクトのステータスを表示します。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

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

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

オプション	説明
[General] タブ	障害の概要、ファブリックインターコネクトプロパティの概要、ファブリック インターコネクトとそのコンポーネントの物理表示など、ファブリック インターコネクトのステータスの概要が示されます。
[Physical Ports] タブ	ファブリックインターコネクトのすべてのポートのステータスが表示されます。 このタブには次のサブタブが含まれます。 • [Uplink Ports] タブ • [Server Ports] タブ • [Fibre Channel Ports] タブ • [Unconfigured Ports] タブ
[Fans] タブ	ファブリック インターコネクトのすべてのファン モジュールのステータスが表示されます。
[PSUs] タブ	ファブリックインターコネクトのすべての電源モジュールのステータスが表示されます。
[Physical Display] タブ	ファブリックインターコネクトとすべてのポートおよびその他のコンポーネントがグラフィック表示されます。 コンポーネントに障害がある場合、そのコンポーネントの横に障害アイコンが表示されます。
[Faults] タブ	ファブリック インターコネクトで発生した障害の詳細が表示されます。
[Events] タブ	ファブリックインターコネクトで発生したイベントの詳細が表示されます。
[Statistics] タブ	ファブリックインターコネクトとそのコンポーネントに関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。

シャーシのモニタリング

ヒント　シャーシ内の個々のコンポーネントをモニタするには、そのコンポーネントのノードを展開します。

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Chassis] を展開します。
3. モニタするシャーシをクリックします。
4. 次のタブのいずれかをクリックして、シャーシのステータスを表示します。

手順の詳細

ステップ 1　[Navigation] ペインの [Equipment] タブをクリックします。

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

ステップ 3　モニタするシャーシをクリックします。

ステップ 4　次のタブのいずれかをクリックして、シャーシのステータスを表示します。

オプション	説明
[General] タブ	障害の概要、シャーシプロパティの概要、シャーシとそのコンポーネントの物理表示など、シャーシのステータスの概要が示されます。
[Servers] タブ	シャーシ内の全サーバのステータスと選択されたプロパティが表示されます。
[Service Profiles] タブ	シャーシ内のサーバに関連付けられたサービスプロファイルのステータスが表示されます。
[IO Modules] タブ	シャーシ内のすべてのIOモジュールのステータスと選択されたプロパティが表示されます。
[Fans] タブ	シャーシ内のすべてのファン モジュールのステータスが表示されます。
[PSUs]	シャーシ内のすべての電源モジュールのステータスが表示されます。

オプション	説明
[Hybrid Display] タブ	シャーシとファブリック インターコネクト間の接続に関する詳細情報が表示されます。 この表示には、次のコンポーネントを表すアイコンがあります。 • システムの各ファブリック インターコネクト。 • 選択したコンポーネントでの I/O モジュール（IOM）。これは、接続パスを見やすくするために独立したユニットとして表示されます。 • サーバと PSU を示す選択したシャーシ、または選択したラック サーバ。
[Slots] タブ	シャーシ内のすべてのスロットのステータスが表示されます。
[Installed Firmware] タブ	シャーシ内のIOモジュールおよびサーバの現在のファームウェア バージョンが表示されます。 このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。
[SEL Logs] タブ	シャーシ内のサーバに対するシステム イベント ログが表示され、そのログにアクセスできます。
[Power Control Monitor] タブ	電源グループ、シャーシ、およびサーバの詳細が表示されます。
[Connectivity Policy] タブ	ファブリックに対するシャーシ ID、ファブリック ID、および接続タイプの詳細が表示されます。
[Faults] タブ	シャーシで発生した障害の詳細が表示されます。
[Events] タブ	シャーシで発生したイベントの詳細が表示されます。
[FSM] タブ	シャーシに関連するFSMタスクの詳細およびステータスが表示されます。 この情報を使用して、これらのタスクにおけるエラーを診断できます。
[Statistics] タブ	シャーシとそのコンポーネントに関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Temperatures] タブ	シャーシのコンポーネントの温度に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Power] タブ	シャーシのコンポーネントの電力に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。

ブレード サーバのモニタリング

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。
3. モニタするサーバをクリックします。
4. [Work] ペインで次のタブのいずれかをクリックして、サーバのステータスを表示します。
5. [Navigation] ペインで、 *[Server_ID]* > [Adapters] > *[Adapter_ID]* を展開します。
6. [Work] ペインで、アダプタの次のコンポーネントを 1 つ以上右クリックしてナビゲータを開き、コンポーネントのステータスを表示します。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

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

ステップ 3 モニタするサーバをクリックします。

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

オプション	説明
[General] タブ	障害の概要、サーバ プロパティの概要、サーバとそのコンポーネントの物理表示など、サーバのステータスの概要が示されます。

オプション	説明
[Inventory] タブ	サーバのコンポーネントのプロパティとステータスに関する詳細情報が次のサブタブに表示されます。 • [Motherboard]：マザーボードとサーバ BIOS 設定に関する情報。 このサブタブから、破損した BIOS ファームウェアを復旧させることもできます。 • [CIMC]：CIMC とそのファームウェアに関する情報。サーバの SEL にもアクセスできます。 また、このサブタブから、静的またはプールされた管理 IP アドレスの割り当て、CIMC ファームウェアの更新、アクティブ化を行うこともできます。 • [CPUs]：サーバの各 CPU に関する情報。 • [Memory]：サーバの各メモリ スロットと、スロットの DIMM に関する情報。 • [Adapters] ：サーバに取り付けられた各アダプタに関する情報。 • [HBAs]：各 HBA のプロパティと、サーバに関連付けられたサービス プロファイルでの HBA の設定。 • [NICs]：各 NIC のプロパティと、サーバに関連付けられたサービス プロファイルでの NIC の設定。 各行を展開すると、関連する VIF および vNIC に関する情報を表示できます。 • [iSCSI vNICs]：各 iSCSI vNIC のプロパティと、サーバに関連付けられたサービス プロファイルでのその vNIC の設定。 • [Storage]：ストレージ コントローラのプロパティ、サーバに関連付けられたサービス プロファイルでのローカル ディスク設定ポリシー、サーバの各ハード ディスクに関する情報。 **ヒント** ハード ディスク ドライブやソリッド ステート ドライブなどの SATA デバイスがサーバに 1 台以上搭載されている場合、Cisco UCS Manager GUI はその SATA デバイスのベンダー名を [Vendor] フィールドに表示します。 ただし、Cisco UCS Manager CLI は [Vendor] フィールドに ATA を表示し、ベンダー名などのベンダー情報は [Vendor Description] フィールドに表示されます。 この 2 番目のフィールドは Cisco UCS Manager GUI にはありません。
[Virtual Machines] タブ	サーバでホストされている仮想マシンの詳細情報が表示されます。
[Installed Firmware] タブ	CIMC、アダプタ、その他のサーバ コンポーネントのファームウェア バージョンが表示されます。 このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。

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

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

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

- アダプタ
- DCE インターフェイス
- HBA
- NIC

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

ラックマウント サーバのモニタリング

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。
3. モニタするサーバをクリックします。
4. [Work] ペインで次のタブのいずれかをクリックして、サーバのステータスを表示します。
5. [Navigation] ペインで、 *[Server_ID]* > [Adapters] > *[Adapter_ID]* を展開します。
6. [Work] ペインで、アダプタの次のコンポーネントを 1 つ以上右クリックしてナビゲータを開き、コンポーネントのステータスを表示します。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 モニタするサーバをクリックします。

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

オプション	説明
[General] タブ	障害の概要、サーバ プロパティの概要、サーバとそのコンポーネントの物理表示など、サーバのステータスの概要が示されます。

オプション	説明
[Inventory] タブ	サーバのコンポーネントのプロパティとステータスに関する詳細情報が次のサブタブに表示されます。 • [Motherboard]：マザーボードとサーバ BIOS 設定に関する情報。 このサブタブから、破損した BIOS ファームウェアを復旧させることもできます。 • [CIMC]：CIMC とそのファームウェアに関する情報。サーバの SEL にもアクセスできます。 また、このサブタブから、静的またはプールされた管理 IP アドレスの割り当て、CIMC ファームウェアの更新、アクティブ化を行うこともできます。 • [CPU]：サーバの各 CPU に関する情報。 • [Memory]：サーバの各メモリ スロットと、スロットの DIMM に関する情報。 • [Adapters] ：サーバに取り付けられた各アダプタに関する情報。 • [HBAs]：各 HBA のプロパティと、サーバに関連付けられたサービス プロファイルでの HBA の設定。 • [NICs]：各 NIC のプロパティと、サーバに関連付けられたサービス プロファイルでの NIC の設定。 各行を展開すると、関連する VIF および vNIC に関する情報を表示できます。 • [iSCSI vNICs]：各 iSCSI vNIC のプロパティと、サーバに関連付けられたサービス プロファイルでのその vNIC の設定。 • [Storage]：ストレージ コントローラのプロパティ、サーバに関連付けられたサービスプロファイルでのローカルディスク設定ポリシー、サーバの各ハード ディスクに関する情報。 **ヒント** ハード ディスク ドライブやソリッド ステート ドライブなどの SATA デバイスがサーバに 1 台以上搭載されている場合、Cisco UCS Manager GUI はその SATA デバイスのベンダー名を [Vendor] フィールドに表示します。 ただし、Cisco UCS Manager CLI は [Vendor] フィールドに ATA を表示し、ベンダー名などのベンダー情報は [Vendor Description] フィールドに表示されます。 この 2 番目のフィールドは Cisco UCS Manager GUI にはありません。
[Virtual Machines] タブ	サーバでホストされている仮想マシンの詳細情報が表示されます。
[Installed Firmware] タブ	CIMC、アダプタ、その他のサーバ コンポーネントのファームウェア バージョンが表示されます。 このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。

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

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

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

- アダプタ
- DCE インターフェイス
- HBA
- NIC

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

I/O モジュールのモニタリング

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Chassis] > [Chassis Number] > [FI-IO Modules] を展開します。
3. モニタするモジュールをクリックします。
4. 次のいずれかのタブをクリックして、モジュールのステータスを表示します。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [Chassis Number] > [FI-IO Modules] を展開します。

ステップ 3 モニタするモジュールをクリックします。

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

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

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 ポリシーはディセーブルです。

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

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] を展開します。
3. [Management Interfaces] をクリックします。
4. [Work] ペインで、[Management Interfaces Monitoring Policy] タブをクリックします。
5. 次のフィールドに入力します。
6. モニタリング メカニズムに を選択する場合、 領域 の次のフィールドに入力します。
7. モニタリング メカニズムに を選択する場合、 領域 の該当するタブのフィールドに入力します。
8. モニタリング メカニズムに を選択する場合、 領域 の次のフィールドに入力します。
9. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] を展開します。

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

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

ステップ 5 次のフィールドに入力します。

名前	説明
[Admin Status] フィールド	モニタリング ポリシーを、管理インターフェイスに対してイネーブルまたはディセーブルにするかどうか。
[Poll Interval] フィールド	データ記録の間に Cisco UCS が待機する秒数。 90 ～ 300 の整数を入力します。
[Max Report Fail Count] フィールド	Cisco UCS が管理インターフェイスを使用できないと判断し、障害メッセージを生成するまでのモニタリングの最大失敗回数。 2 ～ 5 の整数を入力します。

名前	説明
[Monitoring Mechanism] フィールド	Cisco UCS で使用するモニタリングのタイプ。 次のいずれかになります。 • [Mii Status]：Cisco UCS はメディア独立型インターフェイス（MII）のアベイラビリティをモニタします。 このオプションを選択すると、Cisco UCS Manager GUI は [Media Independent Interface Monitoring] 領域を表示します。 • [Ping Arp Targets]：Cisco UCS は指定されたターゲットを Address Resolution Protocol（ARP）を使用して ping します。 このオプションを選択すると、Cisco UCS Manager GUI は [ARP Target Monitoring] 領域を表示します。 • [Ping Gateway]：Cisco UCS は、[Management Interfaces] タブでこの Cisco UCS ドメインに指定されたデフォルト ゲートウェイ アドレスを ping します。 このオプションを選択すると、Cisco UCS Manager GUI は [Gateway Ping Monitoring] 領域を表示します。

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

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

ステップ 7 モニタリング メカニズムに を選択する場合、 領域 の該当するタブのフィールドに入力します。
IPv4 アドレスを使用している場合は、[IPv4] サブタブの次のフィールドに入力します。

名前	説明
[Target IP 1] フィールド	Cisco UCS が ping する最初の IPv4 アドレス。
[Target IP 2] フィールド	Cisco UCS が ping する 2 番目の IPv4 アドレス。
[Target IP 3] フィールド	Cisco UCS が ping する 3 番目の IPv4 アドレス。

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

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

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

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

ステップ 8 モニタリング メカニズムに　を選択する場合、 領域 の次のフィールドに入力します。

名前	説明
[Number of ping Requests] フィールド	Cisco UCS がゲートウェイを ping する回数。 1 ～ 5 の整数を入力します。
[Max Deadline Timeout] フィールド	Cisco UCS がアドレスを使用できないと判断するまでに、Cisco UCS がゲートウェイからの応答を待機する秒数。 5 ～ 15 の整数を入力します。

ステップ 9 [Save Changes] をクリックします。

ローカル ストレージのモニタリング

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

- 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 ストレージのモニタリングやレガシー ディスク ドライブのモニタリングの際に満たす必要があります。

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

レガシー ディスク ドライブのモニタリング

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

Cisco UCS Manager 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 ドメイン 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。

Flash 寿命消耗レベルのモニタリング

Flash 寿命消耗レベルのモニタリングにより、ソリッド ステート ドライブの耐用期間をモニタすることができます。 残りの Flash 寿命の割合および Flash 寿命のステータスをどちらも表示できます。 消耗レベルのモニタリングは、Fusion IO メザニン カードを搭載した次の Cisco UCS ブレード サーバ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） 消耗レベルのモニタリングには次が必要です。

- Cisco UCS Manager は Release 2.2(2a) 以降であること。
- Fusion IO メザニン カードのファームウェア バージョンは 7.1.15 以降であること。

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

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。
3. ローカル ストレージ コンポーネントのステータスを表示するサーバをクリックします。
4. [Work] ペインの [Inventory] タブをクリックします。
5. [Storage] サブタブをクリックして、RAID コントローラと FlexFlash コントローラのステータスを表示します。
6. 下矢印をクリックして、[Local Disk Configuration Policy]、[Actual Disk Configurations]、[Disks]、および [Firmware] バーを展開し、その他のステータス情報を表示します。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

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

ステップ 3 ローカル ストレージ コンポーネントのステータスを表示するサーバをクリックします。

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

ステップ 5 [Storage] サブタブをクリックして、RAID コントローラと FlexFlash コントローラのステータスを表示します。

ステップ 6 下矢印をクリックして、[Local Disk Configuration Policy]、[Actual Disk Configurations]、[Disks]、および [Firmware] バーを展開し、その他のステータス情報を表示します。

（注） [Local Disk Configuration Policy] および [Actual Disk Configurations] 領域には、Cisco UCS B460 ブレード サーバのマスター ノードのデータのみが表示されます。 スレーブ ノードのフィールドは表示されません。

グラフィックス カード モニタリング

グラフィックス カードのモニタリング

Cisco UCS Manager では、特定のグラフィック カードおよび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ます。

- Cisco UCS C240 M3 ラック サーバ
- Cisco UCS C460 M4 ラック サーバ

グラフィックス カードのプロパティの表示

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 グラフィックス カード設定を表示するサーバを選択します。

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

ステップ 5 [GPU] サブタブをクリックします。

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 では、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）のステータスを判断できます。 BBU の動作ステータス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 が見つからないか、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ています。

TFM およびスーパーキャパシタの機能は、Cisco UCS Manager Release 2.1（2）以降でサポートされています。

TFM およびスーパーキャパシタの注意事項と制限事項

TFM およびスーパーキャパシタの制限事項

- Cisco UCS B420 M3 ブレード サーバでは、TFM およびスーパーキャパシタ用の CIMC センサーは Cisco UCS Manager で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 サーバにインストールされていない場合、またはインストール後に削除されている場合、障害は生成されません。
- TFM が Cisco UCS B420 M3 ブレード サーバにインストールされておらず、スーパーキャパシタがインストールされている場合、Cisco UCS Manager は BBU システム全体が検出されないと報告します。 TFM およびスーパーキャパシタの両方がブレード サーバ上に物理的に存在することを確認してください。

TFM およびスーパーキャパシタをサポートする 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 サーバにのみ適用されます。 BBU が故障した場合、または故障すると予測される場合には、そのユニットをできるだけ早く交換する必要があります。

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
ステップ 2 [Equipment] ペインで、[Chassis] > *[Chassis Number]* > [Servers] > *[Server Number]* を展開します。
ステップ 3 [Work] ペインの [Inventory] タブをクリックします。
ステップ 4 [Storage] サブタブをクリックして、[RAID Battery (BBU)] 領域を表示します。

RAID バッテリ障害の表示

（注） これは、RAID 設定および TFM をサポートする Cisco UCS サーバにのみ適用されます。

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] ペインで、[Chassis] > *[Chassis Number]* > [Servers] > *[Server Number]* を展開します。
3. [Work] ペインで、[Faults] タブをクリックします。
4. 状況の詳細を確認するバッテリを選択します。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。
ステップ 2 [Equipment] ペインで、[Chassis] > *[Chassis Number]* > [Servers] > *[Server Number]* を展開します。
ステップ 3 [Work] ペインで、[Faults] タブをクリックします。
ステップ 4 状況の詳細を確認するバッテリを選択します。

TPM モニタリング

トラステッド プラットフォーム モジュール（TPM）は、すべてのCisco UCS M3 ブレード サーバやラックマウント サーバに搭載されています。 オペレーティング システムでの暗号化に TPM を

使用することができます。 たとえば、Microsoft の BitLocker ドライブ暗号化は Cisco UCS サーバ上で TPM を使用して暗号キーを保存します。

Cisco UCS Manager では、TPM が存在しているか、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

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

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

ステップ 3 TPM 設定を表示するサーバを選択します。

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

ステップ 5 [Motherboard] サブタブをクリックします。

第 3 章

統計関連ポリシーの設定

この章は、次の内容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：ブレード 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。

統計情報収集ポリシーの変更

（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。

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Stats Management] > [Stats] を展開します。
3. 変更するポリシーを右クリックし、[Modify Collection Policy] を選択します。
4. [Modify Collection Policy] ダイアログボックスで、次のフィールドに値を入力します。
5. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Stats Management] > [Stats] を展開します。

ステップ 3 変更するポリシーを右クリックし、[Modify Collection Policy] を選択します。

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

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

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

ステップ 5 [OK] をクリックします。

統計情報しきい値ポリシーの設定

統計情報しきい値ポリシー

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

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

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

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

（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 コンポーネントのしきい値ポリシーの作成

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

手順の概要

1. [Navigation] ペインの [Servers] タブをクリックします。
2. [Servers] タブで、[Servers] > [Policies] を展開します。
3. ポリシーを作成する組織のノードを展開します。
4. [Threshold Policies] を右クリックし、[Create Threshold Policy] を選択します。
5. [Create Threshold Policy] ウィザードの [Define Name and Description] ページで、次の手順を実行します。
6. [Create Threshold Policy] ウィザードの [Threshold Classes] ページで、次の手順を実行します。
7. [Threshold Definitions] ページで、次の手順を実行します。
8. [Create Threshold Policy] ウィザードの [Threshold Classes] ページで、次の手順を実行します。
   - ポリシーの別のしきい値クラスを設定するには、ステップ 6 および 7 を繰り返します。
   - ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。
9. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

a) 次のフィールドに入力します。

名前	説明
[名前] フィールド	ポリシーの名前。 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で、この名前を変更することはできません。

名前	説明
[説明] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Owner] フィールド	次のいずれかになります。 • [ローカル]：このポリシーは、Cisco UCS ドメイン内のサービスプロファイルとサービスプロファイルテンプレートでのみ使用できます。 • [グローバル移行中]：このポリシーの制御は、Cisco UCS Central に移行中です。 移行が完了すると、このポリシーは Cisco UCS Central に登録されているすべての Cisco UCS ドメインで使用可能になります。 • [グローバル]：このポリシーは、Cisco UCS Central で管理されます。 このポリシーを変更する場合は、必ず Cisco UCS Central を使用して変更してください。

b) [Next] をクリックします。

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

a) [Add] をクリックします。

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

c) [Next] をクリックします。

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

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。

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

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

d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つ以上をオンにします。

- Critical
- Major
- Minor

- Warning
- Condition
- Info

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

- Info
- Condition
- Warning
- Minor
- Major
- Critical

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

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

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

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

ステップ 9 [OK] をクリックします。

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

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

手順の概要

1. [Navigation] ペインの [Servers] タブをクリックします。
2. [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。
3. [Threshold Policies] ノードを展開します。
4. しきい値クラスを追加するポリシーを右クリックして、[Create Threshold Class] を選択します。
5. [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。
6. [Threshold Definitions] ページで、次の手順を実行します。
7. [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次のいずれかの手順を実行します。
   - ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
   - ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。
8. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。

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

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

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

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

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

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。
b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。
c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。
d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - Critical
   - Major
   - Minor
   - Warning
   - Condition

- Info

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - Info
   - Condition
   - Warning
   - Minor
   - Major
   - Critical
g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。
   - クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
   - クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

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

ステップ 8 [OK] をクリックします。

サーバおよびサーバ コンポーネントのしきい値ポリシーの削除

手順の概要

1. [Navigation] ペインの [Servers] タブをクリックします。
2. [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。
3. [Threshold Policies] ノードを展開します。
4. 削除するポリシーを右クリックし、[Delete] を選択します。
5. Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。
ステップ 2 [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。
ステップ 3 [Threshold Policies] ノードを展開します。
ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。
ステップ 5 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

アップリンク イーサネット ポートしきい値ポリシーへのしきい値クラスの追加

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

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [LAN Cloud] を展開します。
3. [Threshold Policies] ノードを展開します。
4. [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。
5. [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。
6. [Threshold Definitions] ページで、次の手順を実行します。
7. [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。
   - ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
   - ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。
ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] を展開します。
ステップ 3 [Threshold Policies] ノードを展開します。
ステップ 4 [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。
ステップ 5 [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。
a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。

b) [Next] をクリックします。

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

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。

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

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

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

- Critical
- Major
- Minor
- Warning
- Condition
- Info

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

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

- Info
- Condition
- Warning
- Minor
- Major
- Critical

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

h) [Finish Stage] をクリックします。

i) 次のいずれかを実行します。

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

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

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

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

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

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

手順の概要

1. [Navigation] ペインの [LAN] タブをクリックします。
2. [LAN] タブで、[LAN] > [Internal LAN] を展開します。
3. [Threshold Policies] ノードを展開します。
4. [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。
5. [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。
6. [Threshold Definitions] ページで、次の手順を実行します。
7. [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。
   - ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
   - ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

手順の詳細

ステップ 1　[Navigation] ペインの [LAN] タブをクリックします。

ステップ 2　[LAN] タブで、[LAN] > [Internal LAN] を展開します。

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

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

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

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

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

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。

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

- Critical
- Major
- Minor
- Warning
- Condition
- Info

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

- Info
- Condition
- Warning
- Minor
- Major
- Critical

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

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

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

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

ファイバ チャネル ポートしきい値ポリシーへのしきい値クラスの追加

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

手順の概要

1. [Navigation] ペインの [SAN] タブをクリックします。
2. [SAN] タブで、[SAN] > [SAN Cloud] を展開します。
3. [Threshold Policies] ノードを展開します。
4. [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。
5. [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。
6. [Threshold Definitions] ページで、次の手順を実行します。
7. [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。
   - ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
   - ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [SAN] タブをクリックします。

ステップ 2 [SAN] タブで、[SAN] > [SAN Cloud] を展開します。

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

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

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

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

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

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。
b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。
c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。
d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - Critical
   - Major
   - Minor

- Warning
- Condition
- Info

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

- Info
- Condition
- Warning
- Minor
- Major
- Critical

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

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

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

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

第 4 章

Call Home の設定

この章は、次の内容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。

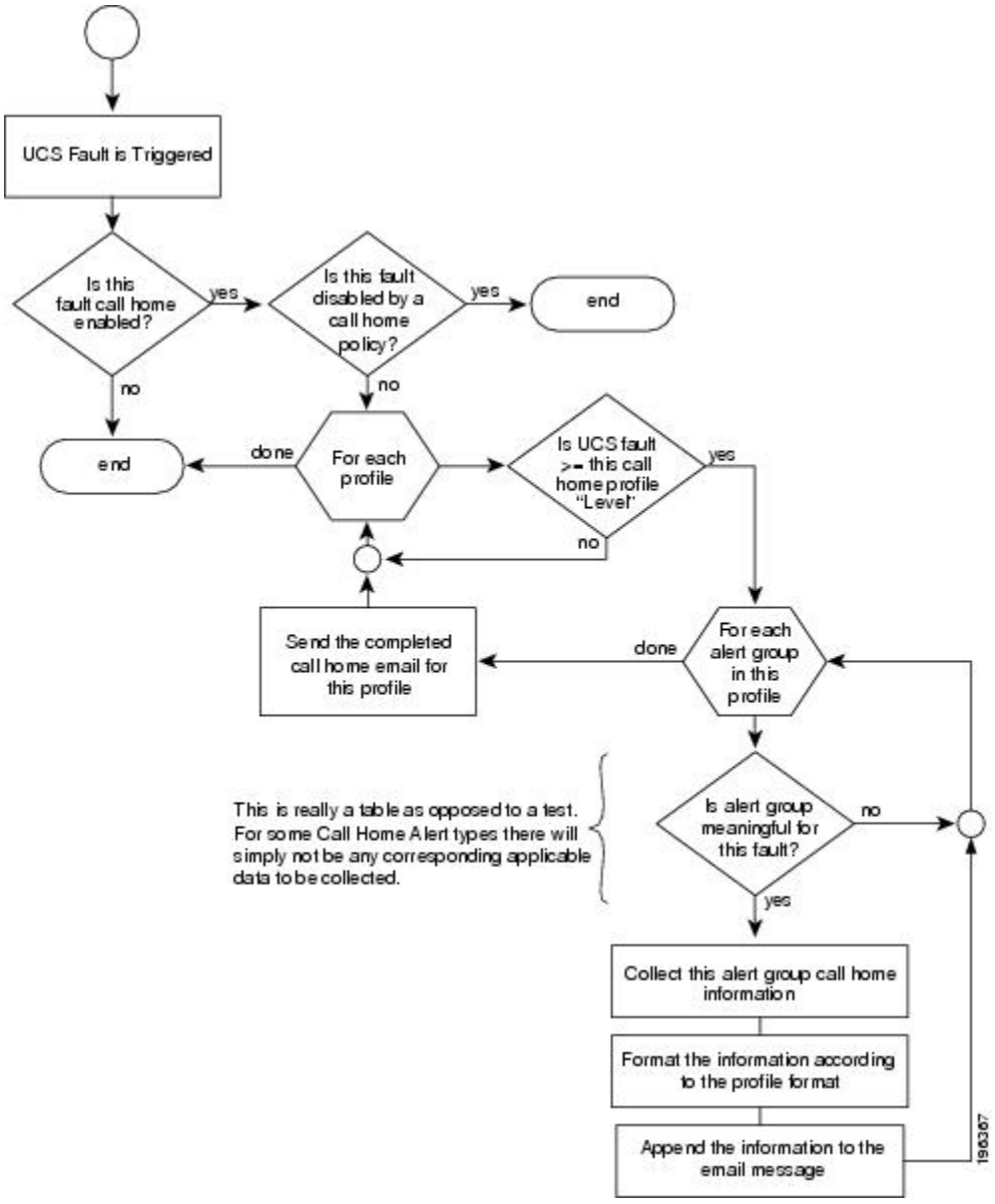
Cisco UCS では、Call Home メッセージが次のフォーマットで配信されます。

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

Cisco Smart Call Home

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

（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、レポートは電子メールとして送信されます。

Call Home の設定

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Admin] 領域で、次のフィールドに入力して [Call Home] をイネーブルにします。
5. [Contact Information] 領域で、次のフィールドに必要な連絡先情報を入力します。
6. [Ids] 領域で、Call Home が使用する ID 情報を次のフィールドに入力します。
7. [Email Addresses] 領域で、Call Home アラート メッセージの電子メール情報を次のフィールドに入力します。
8. [SMTP Server] 領域で、Call Home が電子メール メッセージを送信する SMTP サーバに関する情報を次のフィールドに入力します。
9. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

名前	説明
[State] フィールド	次のいずれかになります。 • [Off]：この Cisco UCS ドメインでは Call Home は使用されません。 • [On]：Cisco UCS では、システムで定義されている Call Home ポリシーおよびプロファイルに基づいて Call Home アラートが生成されます。 （注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。

名前	説明
[Switch Priority] ドロップダウン リスト	次のいずれかになります。 • Alerts • Critical • Debugging • Emergencies • Errors • Information • Notifications • Warnings
[Throttling] フィールド	同じイベントについて受信する重複メッセージの数を制限するかどうかを指定します。 次のいずれかになります。 • [On]：送信される重複メッセージの数が 2 時間以内に 30 件を超えると、そのアラート タイプに関するそれ以降のメッセージは破棄されます。 • [Off]：検出された数に関係なく、すべての重複メッセージが送信されます。

a) [State] フィールドで、[on] をクリックします。
（注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。

b) [Switch Priority] ドロップダウン リスト から、次のいずれかのレベルを選択します。
- Alerts
- Critical
- Debugging
- Emergencies
- Errors
- Information
- Notifications
- Warnings

ファブリック インターコネクトの複数のペアがある大規模な Cisco UCS の展開の場合は、メッセージの受信者がメッセージの優先度を判断できるように、このフィールドを使用して特定の 1 つの Cisco

UCS ドメインからのメッセージに重大度を割り当てることができます。 このフィールドは、小規模な Cisco UCS の展開（単一の Cisco UCS ドメインなど）には有用でないことがあります。

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

名前	説明
[Contact] フィールド	主要 Call Home 連絡先。 255 文字以下の ASCII 文字で入力します。
[Phone] フィールド	主要連絡先の電話番号。 +（プラス記号）と国番号から始まる国際形式の番号を入力します。ハイフンは使用できますが、カッコは使用できません。
[Email] フィールド	主要連絡先の電子メール アドレス。 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。 （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。
[Address] フィールド	主要連絡先の住所。 255 文字以下の ASCII 文字で入力します。

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

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

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

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

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

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

名前	説明
[Host (IP Address or Hostname)] フィールド	SMTP サーバの IPv4 または IPv6 アドレスまたはホスト名。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、Cisco UCS Manager で DNS サーバを設定する必要があります。
[Port] フィールド	SMTP サーバとの通信に使用されるポート番号。 1 ～ 65535 の整数を入力します。 デフォルトは 25 です。

ステップ 9 [Save Changes] をクリックします。

Call Home のディセーブル化

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Admin] 領域の [State] フィールドで、[off] をクリックします。
5. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4 [Admin] 領域の [State] フィールドで、[off] をクリックします。

（注） このフィールドが [off] に設定されている場合、Cisco UCS Manager ではこのタブの残りのフィールドが表示されません。

ステップ 5 [Save Changes] をクリックします。

Call Home のイネーブル化

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Admin] 領域の [State] フィールドで、[on] をクリックします。
5. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4 [Admin] 領域の [State] フィールドで、[on] をクリックします。

（注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。

ステップ 5 [Save Changes] をクリックします。

次の作業

Call Home が完全に設定されていることを確認します。

システム インベントリ メッセージの設定

システム インベントリ メッセージの設定

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインで [System Inventory] タブをクリックします。
4. [Properties] 領域で、次のフィールドに値を入力します。
5. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

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

ステップ 5 [Save Changes] をクリックします。

システム インベントリ メッセージの送信

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

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

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインで [System Inventory] タブをクリックします。
4. [Actions] 領域で [Send System Inventory Now] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4 [Actions] 領域で [Send System Inventory Now] をクリックします。
Cisco UCS Manager は、Call Home 用に設定された受信者にシステム インベントリ メッセージをただちに送信します。

Call Home プロファイルの設定

Call Home プロファイル

Call Home プロファイルは、指定した受信者に送信されるアラートを決定します。 プロファイルを設定して、必要な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。 Cisco UCS 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。

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

アラート グループ	説明
Cisco TAC	Smart Call Home 宛ての、他のアラート グループからのすべてのクリティカル アラート。
Diagnostic	サーバの POST の完了など診断によって生成されたイベント。
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 プロファイルの作成

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

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインで、[Profiles] タブをクリックします。
4. テーブルの右側のアイコン バーの [+] をクリックします。
5. [Create Call Home Profile] ダイアログボックスで、次の情報フィールドに値を入力します。
6. [Email Configuration] 領域で、次のフィールドに値を入力して電子メール アラートを設定します。
7. [Recipients] 領域で次の手順を実行して電子メール アラートの 1 つ以上の電子メール受信者を追加します。
8. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create Call Home Profile] ダイアログボックスで、次の情報フィールドに値を入力します。

名前	説明
[Name] フィールド	このプロファイルのユーザ定義名。 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で、この名前を変更することはできません。

名前	説明
[Level] フィールド	Cisco UCS の障害がこのレベル以上の場合は、プロファイルがトリガーされます。 次のいずれかになります。 • Critical • Debug • Disaster • Fatal • Major • Minor • Normal • Notification • Warning
[Alert Groups] フィールド	この Call Home プロファイルに基づいて警告されるグループ。 これは次のいずれか、または複数の値になります。 • [Cisco Tac]：Cisco TAC の受信者 • [Diagnostic]：POST 完了サーバ障害通知の受信者 • [Environmental]：PSU やファンなどの問題に関する通知の受信者

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

名前	説明
[Format] フィールド	次のいずれかになります。 • [Xml]：Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用するマシンが読み取り可能な形式。 この形式により、Cisco Systems Technical Assistance Center との通信が可能になります。 • [Full Txt]：人間が判読するのに適している完全にフォーマットされたメッセージ（詳細な情報付き）。 • [Short Txt]：ポケットベルまたは印刷されたレポートに適している 1 ～ 2 行の障害の説明。

名前	説明
[Max Message Size] フィールド	指定された Call Home 受信者に送信される最大メッセージ サイズ。 1 ～ 5000000 の整数を入力します。 デフォルトは 5000000 です。 フルテキスト メッセージおよび XML メッセージの推奨最大サイズは 5000000 です。 ショートテキスト メッセージの推奨最大サイズは 100000 です。 Cisco TAC アラート グループの場合、最大メッセージ サイズは 5000000 である必要があります。

ステップ 7 [Recipients] 領域で次の手順を実行して電子メール アラートの 1 つ以上の電子メール受信者を追加します。

a) テーブルの右側のアイコン バーの [+] をクリックします。

b) [Add Email Recipients] ダイアログボックスで、[Email] フィールド に Call Home アラートの送信先の電子メール アドレスを入力します。
保存した電子メール アドレスは削除できますが、変更はできません。

c) [OK] をクリックします。

ステップ 8 [OK] をクリックします。

Call Home プロファイルの削除

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインで、[Profiles] タブをクリックします。
4. 削除するプロファイルを右クリックし、[Delete] を選択します。
5. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

ステップ 5 [Save Changes] をクリックします。

Call Home ポリシーの設定

Call Home ポリシー

Call Home ポリシーは、特定の種類の障害またはシステム イベントに対して Call Home アラートを送信するかどうかを決定します。デフォルトでは、特定の種類の障害およびシステムイベントに対してアラートを送信するよう Call Home がイネーブルになります。 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、すべての Call Home ポリシーが有効になっており、重要なシステム イベントすべてについてアラートが電子メールで送信されます。

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [Policies] タブをクリックします。
4. テーブルの右側のアイコン バーの [+] をクリックします。
5. [Create Call Home Policy] ダイアログボックスで、次のフィールドに値を入力します。
6. [OK] をクリックします。
7. 異なる種類の障害またはイベントに Call Home ポリシーを設定する場合は、ステップ 6 および 7 を繰り返します。

手順の詳細

ステップ 1　[Navigation] ペインの [Admin] タブをクリックします。

ステップ 2　[Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4　テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[状態] フィールド	このフィールドが [有効] の場合、関連付けられた原因と一致するエラーが発生した際にシステムはこのポリシーを使用します。 それ以外の場合、一致するエラーが発生しても、システムはこのポリシーを無視します。 デフォルトでは、すべてのポリシーが有効になります。
[原因] フィールド	このアラートをトリガーするイベント。 各ポリシーは、アラートがいずれかのタイプのイベントに送信されるかどうかを定義します。

ステップ 6 [OK] をクリックします。

ステップ 7 異なる種類の障害またはイベントに Call Home ポリシーを設定する場合は、ステップ 6 および 7 を繰り返します。

Call Home ポリシーのディセーブル化

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [Policies] タブをクリックします。
4. ディセーブルにするポリシーを右クリックし、[Show Navigator] を選択します。
5. [State] フィールドで、[Disabled] をクリックします。
6. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

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

ステップ 6 [OK] をクリックします。

Call Home ポリシーのイネーブル化

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [Policies] タブをクリックします。
4. イネーブルにするポリシーを右クリックし、[Show Navigator] を選択します。
5. [State] フィールドで、[Enabled] をクリックします。
6. [OK] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
ステップ 3 [Work] ペインの [Policies] タブをクリックします。
ステップ 4 イネーブルにするポリシーを右クリックし、[Show Navigator] を選択します。
ステップ 5 [State] フィールドで、[Enabled] をクリックします。
ステップ 6 [OK] をクリックします。

Call Home ポリシーの削除

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [Policies] タブをクリックします。
4. ディセーブルにするポリシーを右クリックし、[Delete] を選択します。
5. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

ステップ 5 [Save Changes] をクリックします。

Anonymous Reporting のイネーブル化

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

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call home] を展開します。

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

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

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

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

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

- [Host (IP Address or Hostname)]：SMTP サーバの IPv4 または IPv6 アドレス、あるいはホスト名。
- [Port]：システムが SMTP サーバとの通信で使用するポート番号。
  1 ～ 65535 の整数を入力します。 デフォルトは 25 です。

ステップ 7 [Save Changes] をクリックします。

例：Smart Call Home 用の Call Home の設定

Smart Call Home の設定

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインの [General] タブをクリックします。
4. [Admin] 領域で次の作業を行い、Call Home をイネーブルにします。
5. [Contact Information] 領域で、次のフィールドに必要な連絡先情報を入力します。
6. [Ids] 領域で、次のフィールドに Smart Call Home ID 情報を入力します。
7. [Email Addresses] 領域で、次のフィールドに Smart Call Home アラート メッセージの電子メール情報を入力します。
8. [SMTP Server] 領域で、次のフィールドに Call Home が電子メール メッセージを送信するために使用する SMTP サーバに関する情報を入力します。
9. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

a) [State] フィールドで、[on] をクリックします。

（注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。

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

- Alerts
- Critical
- Debugging
- Emergencies
- Errors
- Information
- Notifications
- Warnings

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

名前	説明
[Contact] フィールド	主要 Call Home 連絡先。 255 文字以下の ASCII 文字で入力します。
[Phone] フィールド	主要連絡先の電話番号。 +（プラス記号）と国番号から始まる国際形式の番号を入力します。ハイフンは使用できますが、カッコは使用できません。
[Email] フィールド	主要連絡先の電子メール アドレス。 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。 （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。
[Address] フィールド	主要連絡先の住所。 255 文字以下の ASCII 文字で入力します。

ステップ 6 [Ids] 領域で、次のフィールドに Smart Call Home ID 情報を入力します。

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

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

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

ステップ 8 [SMTP Server] 領域で、次のフィールドに Call Home が電子メール メッセージを送信するために使用する SMTP サーバに関する情報を入力します。

名前	説明
[Host (IP Address or Hostname)] フィールド	SMTP サーバの IPv4 または IPv6 アドレスまたはホスト名。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、Cisco UCS Manager で DNS サーバを設定する必要があります。
[Port] フィールド	SMTP サーバとの通信に使用されるポート番号。 1 ～ 65535 の整数を入力します。 デフォルトは 25 です。

ステップ 9 [Save Changes] をクリックします。

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

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインで、[Profiles] タブをクリックします。
4. Cisco TAC-1 プロファイルを右クリックし、[Recipient] を選択します。
5. [Add Email Recipients] ダイアログボックスで、次の手順を実行します。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

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

a) [Email] フィールド で、Call Home アラートの送信先の電子メール アドレスを入力します。
たとえば、「callhome@cisco.com」と入力します。

保存した電子メール アドレスは削除できますが、変更はできません。

b) [OK] をクリックします。

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

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインで [System Inventory] タブをクリックします。
4. [Properties] 領域で、次のフィールドに値を入力して、システム インベントリ メッセージを Smart Call Home に送信する方法を指定します。
5. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

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

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

ステップ 5 [Save Changes] をクリックします。

Smart Call Home の登録

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。
3. [Work] ペインで [System Inventory] タブをクリックします。
4. [Actions] 領域で [Send System Inventory Now] をクリックし、登録プロセスを開始します。
5. シスコから登録電子メールを受信したら、Smart Call Home の登録を完了するために、次の手順を実行します。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4 [Actions] 領域で [Send System Inventory Now] をクリックし、登録プロセスを開始します。
シスコがシステム インベントリを受信すると、Smart Call Home の登録電子メールが、[General] タブの [Contact Information] 領域で設定した電子メール アドレスに送信されます。

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

a) 電子メール内のリンクをクリックします。
リンクにより Web ブラウザで Cisco Smart Call Home ポータルが開きます。

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

c) Cisco Smart Call Home によって示される手順に従います。
条項および条件に同意したら、Cisco UCS ドメインの Cisco Smart Call Home 登録は完了です。

第 5 章

システム イベント ログの管理

この章は、次の内容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。

各サーバのシステム イベント ログの表示

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。
3. システム イベント ログを表示するサーバをクリックします。
4. [Work] ペインの [SEL Logs] タブをクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

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

ステップ 3 システム イベント ログを表示するサーバをクリックします。

ステップ 4 [Work] ペインの [SEL Logs] タブをクリックします。
Cisco UCS Manager によってサーバのシステム イベント ログが取得され、イベントのリストが表示されます。

シャーシ内のサーバのシステム イベント ログの表示

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] > [Chassis] > *[Chassis_Name]* を展開します。
3. [Work] ペインの [SEL Logs] タブをクリックします。
4. [Server] テーブルで、システム イベント ログを表示するサーバを選択します。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

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

ステップ 3 [Work] ペインの [SEL Logs] タブをクリックします。
Cisco UCS Manager によってサーバのシステム イベント ログが取得され、イベントのリストが表示されます。

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

Cisco UCS Manager によってサーバのシステム イベント ログが取得され、イベントのリストが表示されます。

SEL ポリシーの設定

手順の概要

1. [Navigation] ペインの [Equipment] タブをクリックします。
2. [Equipment] タブで、[Equipment] ノードを展開します。
3. [Work] ペインの [Policies] タブをクリックします。
4. [SEL Policy] サブタブをクリックします。
5. （任意） [General] 領域で、[Description] フィールドにポリシーの説明を入力します。
6. [Backup Configuration] 領域で、次のフィールドに値を入力します。
7. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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

ステップ 4 [SEL Policy] サブタブをクリックします。

ステップ 5 （任意） [General] 領域で、[Description] フィールドにポリシーの説明を入力します。
この領域の他のフィールドは読み取り専用です。

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

名前	説明
[プロトコル] フィールド	リモート サーバとの通信時に使用するプロトコル。 次のいずれかになります。 • [FTP] • [TFTP] • [SCP] • [SFTP]

名前	説明
[Hostname] フィールド	バックアップ設定が存在する場所のサーバのホスト名または IP アドレス。 IPv4 または IPv6 アドレスではなくホスト名を使用する場合、Cisco UCS Manager で DNS サーバを設定する必要があります。 （注） バックアップ ファイルの名前は、Cisco UCS によって生成されます。 名前は次の形式になります。 `sel-system-name-chchassis-id-servblade-id-blade-serial-timestamp`
[Remote Path] フィールド	必要に応じて、リモート サーバ上のファイルの絶対パスを指定します。 SCP を使用する場合、絶対パスは常に必要です。 他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロード フォルダにあれば、リモート パスを指定する必要はありません。 ファイル サーバの設定方法の詳細については、システム管理者に問い合わせてください。
[Backup Interval] ドロップダウン リスト	自動バックアップ間の待機時間。 次のいずれかになります。 • [Never]：自動 SEL データ バックアップを実行しません。 • [1 Hour] • [2 Hours] • [4 Hours] • [8 Hours] • [24 Hours] • [1 Week] • [1 Month] （注） システムによって自動バックアップを作成する場合は、[Action] オプション ボックス内の [Timer] チェックボックスがオンになっていることを確認してください。
[Format] フィールド	バックアップ ファイルに使用する形式。 次のいずれかになります。 • Ascii • 2 進数
[Clear on Backup] チェックボックス	オンにすると、Cisco UCS はバックアップ後にすべてのシステム イベント ログをクリアします。

名前	説明
[ユーザ] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。 このフィールドは、プロトコルが TFTP の場合は適用されません。
[パスワード] フィールド	リモート サーバのユーザ名のパスワード。 このフィールドは、プロトコルが TFTP の場合は適用されません。
[Action] オプション ボックス	オンにした各チェックボックスのイベントが発生したとき、システムによって SEL バックアップが作成されます。 • [Log Full]：ログが許容される最大サイズに到達。 • [On Change of Association]：サーバとそのサービス プロファイルの間のアソシエーションが変化。 • [On Clear]：システム イベント ログがユーザによって手動でクリア。 • [Timer]：[Backup Interval] ドロップダウン リストで指定された時間間隔に到達。
[Reset Configuration] ボタン	バックグラウンドの設定情報をリセットするには、このボタンをクリックします。

ステップ 7 [Save Changes] をクリックします。

サーバのシステム イベント ログの管理

システム イベント ログの 1 つ以上のエントリのコピー

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

手順の概要

1. Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、マウスを使用してシステム イベント ログからコピーするエントリを強調表示します。
2. Copy をクリックして、強調表示されたテキストをクリップボードにコピーします。
3. 強調表示されたテキストをテキスト エディタまたは他のドキュメントに貼り付けます。

手順の詳細

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

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

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

システム イベント ログの印刷

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

手順の概要

1. Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、[Print] をクリックします。
2. [Print] ダイアログボックス で、次の手順を実行します。

手順の詳細

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

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

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

b) [Print] をクリックします。

システム イベント ログのリフレッシュ

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

手順の概要

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

手順の詳細

Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、[Refresh] をクリックします。
Cisco UCS Manager はサーバのシステム イベント ログを取得し、アップデートされたイベントのリストを表示します。

システム イベント ログの手動バックアップ

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

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。

手順の概要

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

手順の詳細

Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、[Backup] をクリックします。
Cisco UCS Manager は、SEL ポリシーで指定された場所にシステム イベント ログをバックアップします。

システム イベント ログの手動クリア

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

手順の概要

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

手順の詳細

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

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

第 6 章

障害、イベント、およびログの設定

この章は、次の内容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 保持期間にその状態が再発すると、障害はアクティブな状態を返します。 この状況が再発生しない場合は、障害が削除されます。

グローバル障害ポリシーの設定

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。
3. [Settings] をクリックします。
4. [Work] ペインで [Global Fault Policy] タブをクリックします。
5. [Global Fault Policy] タブで、次のフィールドに入力します。
6. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Settings] をクリックします。

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

ステップ 5 [Global Fault Policy] タブで、次のフィールドに入力します。

名前	説明
[Flapping Interval] フィールド	障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 これを防止するため、Cisco UCS Manager では、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。 フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。 その時点で何が発生するかは、[Clear Action] フィールドの設定によって異なります。 5 ～ 3,600 の範囲の整数を入力します。 デフォルトは 10 です。
[Initial Severity] フィールド	次のいずれかになります。 • Info • Condition • Warning

名前	説明
[Action on Acknowledgment] フィールド	ログがクリアされると、確認されたアクションは常に削除されます。このオプションは変更できません。
[Clear Action] フィールド	障害がクリアされるときに Cisco UCS Manager が実行するアクション。 次のいずれかになります。 • [Retain]：Cisco UCS Manager GUI は [Length of time to retain cleared faults] セクションを表示します。 • [Delete]：障害メッセージにクリアのマークが付いた時点で、Cisco UCS Manager はこれらのメッセージをすべて削除します。
[Clear Interval] フィールド	特定の時間が経過した後に、Cisco UCS Manager が障害を自動的にクリアするかどうか。 次のいずれかになります。 • [Never]：Cisco UCS Manager はどの障害も自動的にクリアしません。 • [other]：Cisco UCS Manager GUI は [dd:hh:mm:ss] フィールドを表示します。
[dd:hh:mm:ss] フィールド	Cisco UCS Manager が障害にクリア済みのマークを自動的に付けるまでの経過時間（日、時、分、および秒）。 その時点で何が発生するかは、[Clear Action] フィールドの設定によって異なります。
[Length of Time to Retain Cleared Faults] セクション	
[Retention Interval] フィールド	[Clear Action] フィールドが [Retain] に設定されている場合、これは、クリア済みのマークが付けられた後に Cisco UCS Manager が障害を保持する時間です。 次のいずれかになります。 • [Forever]：システムに存在している期間に関係なく、Cisco UCS Manager はクリア済み障害メッセージをファブリック インターコネクトにすべて残します。 • [other]：Cisco UCS Manager GUI は [dd:hh:mm:ss] フィールドを表示します。
[dd:hh:mm:ss] フィールド	Cisco UCS Manager がクリア済み障害メッセージを削除するまでの経過時間（日、時、分、および秒）。

ステップ 6 [Save Changes] をクリックします。

Core File Exporter の設定

Core File Exporter

Cisco UCS コア ファイルが発生すると、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

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。
3. [Settings] をクリックします。
4. [Work] ペインで [TFTP Core Exporter] タブをクリックします。
5. [TFTP Core Exporter] タブで、次のフィールドに入力します。
6. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Settings] をクリックします。

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

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

名前	説明
[Admin State] フィールド	次のいずれかになります。 • [Enabled]：エラーによってサーバがコア ダンプを生成した場合、Cisco UCS は FTP を介して所定の場所にコア ダンプ ファイルを送信します。 このオプションを選択すると、Cisco UCS Manager GUI はこの領域にその他のフィールドを表示し、FTP エクスポート オプションを指定できるようになります。 • [Disabled]：コア ダンプ ファイルは自動的にエクスポートされません。

名前	説明
[Description] フィールド	コア ファイルのユーザ定義による説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Port] フィールド	TFTP を介してコア ダンプ ファイルをエクスポートするときに使用されるポート番号。
[Hostname] フィールド	TFTP を介して接続されるホスト名か IPv4 アドレスまたは IPv6 アドレス。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、Cisco UCS Manager で DNS サーバを設定する必要があります。
[Path] フィールド	リモート システムにコア ダンプ ファイルを保存するときに使用するパス。

ステップ 6 [Save Changes] をクリックします。

Core File Exporter のディセーブル化

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。
3. [Settings] をクリックします。
4. [Work] ペインで [Settings] タブをクリックします。
5. [TFTP Core Exporter] 領域で、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。
6. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。
ステップ 3 [Settings] をクリックします。
ステップ 4 [Work] ペインで [Settings] タブをクリックします。
ステップ 5 [TFTP Core Exporter] 領域で、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。
ステップ 6 [Save Changes] をクリックします。

Syslog の設定

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。
3. [Syslog] をクリックします。
4. [Work] ペインで [Syslog] タブをクリックします。
5. [Local Destinations] 領域で、次のフィールドに値を入力します。
6. [Remote Destinations] 領域で、次のフィールドに情報を入力し、Cisco UCSコンポーネントにより生成されたメッセージを保存できる最大 3 つの外部ログを設定します。
7. [Local Sources] 領域で、次のフィールドに入力します。
8. [Save Changes] をクリックします。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。
ステップ 3 [Syslog] をクリックします。
ステップ 4 [Work] ペインで [Syslog] タブをクリックします。
ステップ 5 [Local Destinations] 領域で、次のフィールドに値を入力します。

名前	説明
[Console] セクション	

名前	説明
[管理状態] フィールド	Cisco UCS でコンソールに Syslog メッセージが表示されるかどうか。次のいずれかになります。 • [Enabled]：Syslog メッセージはコンソールに表示され、ログに追加されます。 • [Disabled]：Syslog メッセージはログに追加されますが、コンソールには表示されません。
[Level] フィールド	このオプションが [enabled] である場合、表示する最も低いメッセージ レベルを選択します。 Cisco UCS にはそのレベル以上のメッセージが表示されます。 次のいずれかになります。 • Emergencies • Alerts • Critical
[Monitor] セクション	
[管理状態] フィールド	Cisco UCS でモニタに Syslog メッセージが表示されるかどうか。 次のいずれかになります。 • [Enabled]：Syslog メッセージはモニタに表示され、ログに追加されます。 • [Disabled]：Syslog メッセージはログに追加されますが、モニタには表示されません。 [管理状態] が有効の場合は、Cisco UCS Manager GUI に、このセクションの残りのフィールドが表示されます。

名前	説明
[Level] ドロップダウン リスト	このオプションが [enabled] である場合、表示する最も低いメッセージ レベルを選択します。 モニタにはそのレベル以上のメッセージが表示されます。 次のいずれかになります。 • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information • Debugging
[File] セクション	
[管理状態] フィールド	Cisco UCS がファブリック インターコネクトでシステム ログ ファイルにメッセージを保存するかどうか。 次のいずれかになります。 • [Enabled]：メッセージはログ ファイルに保存されます。 • [Disabled]：メッセージは保存されません。 [管理状態] が有効の場合は、Cisco UCS Manager GUI に、このセクションの残りのフィールドが表示されます。
[Level] ドロップダウン リスト	システムに保存するメッセージの最も低いレベルを選択します。Cisco UCS は、ファブリック インターコネクトのファイル内に、そのレベル以上のメッセージを保存します。 次のいずれかになります。 • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information • Debugging

名前	説明
[Name] フィールド	メッセージが記録されるファイルの名前。 名前には 16 文字以内の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）が使用できます。 デフォルトは messages です。
[Size] フィールド	ファイルの可能最大サイズ（バイト単位）。ファイルがこのサイズを超えると、Cisco UCS Manager によって最も古いメッセージから最新メッセージへの上書きが開始されます。 4096 ～ 4194304 の整数を入力します。

ステップ 6 [Remote Destinations] 領域で、次のフィールドに情報を入力し、Cisco UCSコンポーネントにより生成されたメッセージを保存できる最大 3 つの外部ログを設定します。

名前	説明
[管理状態] フィールド	次のいずれかになります。 • [有効化] • [無効化] [管理状態] が有効の場合は、Cisco UCS Manager GUI に、このセクションの残りのフィールドが表示されます。
[Level] ドロップダウン リスト	システムに保存するメッセージの最も低いレベルを選択します。 リモート ファイルにそのレベル以上のメッセージが保存されます。 次のいずれかになります。 • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information • Debugging

名前	説明
[Hostname] フィールド	リモート ログ ファイルが存在するホスト名または IP アドレス。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、Cisco UCS Manager で DNS サーバを設定する必要があります。
[Facility] ドロップダウン リスト	次のいずれかになります。 • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7

ステップ 7 [Local Sources] 領域で、次のフィールドに入力します。

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

ステップ 8 [Save Changes] をクリックします。

監査ログの表示

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

手順の概要

1. [Navigation] ペインの [Admin] タブをクリックします。
2. [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。
3. [Audit Logs] をクリックします。
4. [Work] ペインに監査ログが表示されます。

手順の詳細

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Audit Logs] をクリックします。

ステップ 4 [Work] ペインに監査ログが表示されます。

第 7 章

NetFlow モニタリング

この章は、次の内容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て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 は、IPv4、IPv6、およびレイヤ 2 キーをサポートします。 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 レコードの定義は、フローキーとフロー値の固有の組み合わせです。 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いて、フロー コネクタにフローを転送します。 フロー エクスポータ プロファイルには、NetFlow パケットをエクスポートする際に使用されるネットワーキング プロパティが含まれます。 ネットワーキング プロパティには、各ファブリック インターコネクトの VLAN、送信元 IP アドレス、およびサブネット マスクが含まれます。

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

フロー コレクタは、フロー エクスポータからフローを受信します。 各フロー コレクタには、フローの送信先を定義する IP アドレス、ポート、外部ゲートウェイ IP、および 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、およびタイムアウト 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、収集するフロー情報やその収集元を指定できます。 各フロー モニタは、出力方向または入力方向に対して動作します。

フロー モニタ セッションには、入力方向と出力方向にそれぞれ最大 2 つずつ、合計 4 つのフローモニタが含まれます。 フロー モニタ セッションは、vNIC に関連付けることもできます。

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 UCS VIC 1240、Cisco UCS VIC 1280、および Cisco UCS VIC 1225 アダプタでのみサポートされます。 第一世代のアダプタまたはシスコ製以外の VIC アダプタはサポートされません。

  リリース 2.2(3a) 以降では、NetFlow モニタリングは、Cisco UCS VIC 1340、Cisco UCS VIC 1380、および Cisco UCS VIC 1227 アダプタでもサポートされます。
- 最大 64 のフロー レコードの定義、フロー エクスポータ、およびフロー モニタを設定できます。
- 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 をフロー コレクタと併用できるようにするには、エクスポータ インターフェイスとして定義しておく必要があります。
- 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 レコード定義の作成

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Netflow Monitoring] を展開します。

ステップ 3 [Flow Record Definitions] を右クリックし、[Create Flow Record Definition] を選択します。

ステップ 4 [Create Flow Record Definition] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
Name	フロー レコード定義の名前。 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で、この名前を変更することはできません。

フィールド	説明
Description	フロー レコード定義のユーザ定義による説明。
Keys	使用するキーのオプション ボタンを選択します。 次のいずれかになります。 • [IPv4]：IPv4 キーで選択ウィンドウに入力します。 • [IPv6]：IPv6 キーで選択ウィンドウに入力します。 • [Layer 2 Switched]：レイヤ 2 キーで選択ウィンドウに入力します。 フローの対象とするプロパティのチェックボックスをオンにします。
Measured Properties	フローの対象とする非キー フィールドのチェックボックスをオンにします。 これは次のいずれか、または複数の値になります。 • Counter Bytes Long • Counter Packets Long • Sys Uptime First • Sys Uptime Last

ステップ 5 [OK] をクリックします。

フロー レコード定義の表示

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Netflow Monitoring] を展開します。

ステップ 3 [Flow Record Definitions] を選択して、すべてのフロー定義のリストを表示します。

ステップ 4 フロー定義の名前をダブルクリックして、選択したフロー定義のプロパティを表示します。
[Properties] ウィンドウで、フローに使用するキーおよび非キーを変更できます。

エクスポータ プロファイルの定義

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Netflow Monitoring] > [Flow Exporters] > [Flow Exporter Profiles] を展開します。

ステップ 3 [Flow Exporter Profile default] をクリックします。

ステップ 4 [Properties] 領域で、[Exporter Interface(s)] テーブルの横にある [Add] をクリックします。

ステップ 5 [Create Exporter Interface] ダイアログボックスで、次のフィールドに入力します。

名前	説明
VLAN	エクスポータ インターフェイスと関連付ける VLAN を選択するか、[Create VLANs] をクリックして新しい VLAN を作成します。 PVLAN およびローカル 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。
Fabric A Source IP	ファブリック A のエクスポータ インターフェイスの送信元 IP。
Fabric A Subnet Mask	ファブリック A のエクスポータ インターフェイスのサブネット マスク。
Fabric B Source IP	ファブリック B のエクスポータ インターフェイスの送信元 IP。
Fabric B Subnet Mask	ファブリック B のエクスポータ インターフェイスのサブネット マスク。

ステップ 6 [OK] をクリックします。

フロー コレクタの作成

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] を展開します。

ステップ 3 [Netflow Monitoring] をクリックします。

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

ステップ 5 [Flow Collectors] テーブルの横にある [Add] をクリックします。

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

名前	説明
Name	フロー コレクタの名前。 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で、この名前を変更することはできません。
Description	フロー コレクタのユーザ定義による説明。
Collector IP	フロー コレクタの IP アドレス。
Port	フロー コレクタのポート。 1 ～ 65535 の値を入力します。
Exporter Gateway IP	フロー コレクタの外部ゲートウェイ IP。
VLAN	フロー コレクタに関連付けられている VLAN。 VLANをフローコレクタで使用できるようにするには、[Create Exporter Interface] ダイアログボックスで定義しておく必要があります。

ステップ 7 [OK] をクリックします。

フロー エクスポータの作成

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Netflow Monitoring] を展開します。

ステップ 3 [Flow Exporters] を右クリックし、[Create Flow Exporter] を選択します。

ステップ 4 [Create Flow Exporter] ダイアログボックスで、次のフィールドに入力します。

名前	説明
Name	フロー エクスポータの名前。 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で、この名前を変更することはできません。
Description	フロー エクスポータのユーザ定義による説明。
DSCP	DiffServ コード ポイント（DSCP）値。 値の範囲は、0 ～ 63 です。
Version	エクスポータのバージョン。 デフォルトでは、バージョン 9 です。
Exporter Profile	フロー エクスポータに関連付けるエクスポータ プロファイル。
Flow Collector	フロー エクスポータと関連付けるフロー コレクタを選択するか、[Create Flow Exporter] をクリックして新しいフロー エクスポータを作成します。
Template Data Timeout	NetFlow テンプレート データ再送信のタイムアウト期間。 1 ～ 86400 の値を入力します。
Option Exporter Stats Timeout	NetFlow フロー エクスポータ データ再送信のタイムアウト期間。 1 ～ 86400 の値を入力します。
Option Interface Table Timeout	NetFlow フロー エクスポータ インターフェイス テーブル再送信のタイムアウト期間。 1 ～ 86400 の値を入力します。

ステップ 5 [OK] をクリックします。

フロー モニタの作成

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Netflow Monitoring] を展開します。

ステップ 3 [Flow Monitors] を右クリックし、[Create Flow Monitor] を選択します。

ステップ 4 [Create Flow Monitor] ダイアログボックスで、次のフィールドに入力します。

名前	説明
Name	フロー モニタの名前。 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で、この名前を変更することはできません。
Description	フロー モニタのユーザ定義による説明。
Flow Definition	使用するフロー定義を値のリストから選択するか、[Create Flow Record Definition] をクリックして新しいフロー定義を作成します。
Flow Exporter 1	使用するフロー エクスポータを値のリストから選択するか、[Create Flow Exporter] をクリックして新しいフロー エクスポータを作成します。
Flow Exporter 2	使用するフロー エクスポータを値のリストから選択するか、[Create Flow Exporter] をクリックして新しいフロー エクスポータを作成します。
Timeout Policy	使用するタイムアウト ポリシーを値のリストから選択します。

ステップ 5 [OK] をクリックします。

フロー モニタ セッションの作成

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Netflow Monitoring] を展開します。

ステップ 3 [Flow Monitor Sessions] を右クリックし、[Create Flow Monitor Session] を選択します。

ステップ 4 [Create Flow Monitor Session] ダイアログボックスで、次のフィールドに入力します。

名前	説明
Name	フロー モニタ セッションの名前。 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で、この名前を変更することはできません。
Description	フロー モニタ セッションのユーザ定義による説明。
Flow Definition	使用するフロー モニタを値のリストから選択するか、[Create Flow Monitor] をクリックして新しいフロー モニタを作成します。
Host Receive Direction Monitor 1	使用するフロー モニタを値のリストから選択するか、[Create Flow Monitor] をクリックして新しいフロー モニタを作成します。
Host Receive Direction Monitor 2	使用するフロー モニタを値のリストから選択するか、[Create Flow Monitor] をクリックして新しいフロー モニタを作成します。
Host Transmit Direction Monitor 1	使用するフロー モニタを値のリストから選択するか、[Create Flow Monitor] をクリックして新しいフロー モニタを作成します。
Host Transmit Direction Monitor 2	使用するフロー モニタを値のリストから選択するか、[Create Flow Monitor] をクリックして新しいフロー モニタを作成します。

ステップ 5 [OK] をクリックします。

vNIC へのフロー モニタ セッションの関連付け

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Netflow Monitoring] > [Flow Monitor Sessions] を展開します。

ステップ 3 関連付けるフロー モニタ セッションをクリックします。

ステップ 4 [Flow Exporter Profile default] をクリックします。

ステップ 5 [Properties] 領域で、[vNICs] を展開します。

ステップ 6 テーブルの横にある [Add] をクリックします。

ステップ 7 [Add Monitoring Session Source] ダイアログボックスで、フロー モニタ セッションと関連付ける vNIC を選択します。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 9 [Save] をクリックして、ダイアログボックスを閉じます。