



障害およびログの表示

この章の内容は、次のとおりです。

- ・ 障害サマリー, 1 ページ
- ・ 障害履歴, 4 ページ
- ・ Cisco IMC ログ, 7 ページ
- ・ システムイベントログ, 9 ページ
- ・ ロギング制御, 12 ページ

障害サマリー

障害サマリーの表示

手順

ステップ1 [ナビゲーション (Navigation)] ペインの [シャーシ (Chassis)] メニューをクリックします。

ステップ2 [シャーシ (Chassis)] メニューの [障害およびログ (Faults and Logs)] をクリックします。

ステップ3 [障害サマリー (Faults Summary)] タブで、次の情報を確認します。

表 1 : [アクション (Actions)] 領域

[名前 (Name)]	説明
[合計 (Total)]	[障害エントリ (Fault Entries)] テーブルの合計行数を表示します。
[列 (Column)] ドロップダウンリスト	表示する列を選択できます。

[名前 (Name)]	説明
[表示 (Show)] ドロップダウンリスト	<p>フィルタを使用して障害のエントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。</p> <ul style="list-style-type: none"> • [クイック フィルタ (Quick Filter)] : デフォルト ビュー。 • [高度なフィルタ (Advanced Filter)] : 1つ以上の条件に基づき障害エントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは[フィルタ (Filter)] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 <p>設定したフィルタ条件に一致するエントリを表示するには、[移動 (Go)] をクリックします。</p> <p>設定したフィルタ条件を保存するには、[保存 (Save)] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。</p> <p>(注) ユーザ定義のフィルタは、[プリセット フィルタの管理 (Manage Preset Filters)] ダイアログボックスに表示されます。</p> <ul style="list-style-type: none"> • [すべて (All)] : すべてのエントリを表示します。 • [プリセット フィルタの管理 (Manage Preset Filters)] : ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義 フィルタのリスト (List of pre-defined filters)] : システム定義のフィルタを表示します。 <p>(注) [フィルタ (Filter)] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。</p>

表 2 : [障害エントリ (Fault Entries)] 領域

[名前 (Name)]	説明
時刻 (Time)	障害が発生した時刻。
重大度 (Severity)	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> ・[クリア済み (Cleared)] : ある障害または状態が解消されました。 ・クリティカル (Critical) ・情報 (Info) ・[メジャー (Major)] ・[マイナー (Minor)] ・警告
コード (Code)	障害に割り当てられた固有識別情報。
[DN]	識別名 (DN) は、サーバ上でのデバイスのエンドポイントおよびそのインスタンスの階層表現です。
考えられる原因	障害の原因となったイベントに関連付けられた固有識別情報。
説明	障害についての詳細情報。 提案される解決策も含まれます。

障害履歴

障害履歴の表示

手順

-
- ステップ1** [ナビゲーション (Navigation)] ペインの [シャーシ (Chassis)] メニューをクリックします。
 - ステップ2** [シャーシ (Chassis)] メニューの [障害およびログ (Faults and Logs)] をクリックします。
 - ステップ3** [障害履歴 (Faults History)] タブで、次の情報を確認します。

表 3 : [アクション (Actions)] 領域

[名前 (Name)]	説明
[合計 (Total)]	[障害履歴 (Fault History)] テーブルの合計行数を表示します。
[列 (Column)] ドロップダウンリスト	表示する列を選択できます。

[名前 (Name)]	説明
<p>[表示 (Show)] ドロップダウンリスト</p>	<p>フィルタを使用して障害履歴エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。</p> <ul style="list-style-type: none"> • [クイック フィルタ (Quick Filter)] : デフォルト ビュー。 • [高度なフィルタ (Advanced Filter)] : 1つ以上の条件に基づきエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは[フィルタ (Filter)] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 <p>設定したフィルタ条件に一致するエントリを表示するには、[移動 (Go)] をクリックします。</p> <p>設定したフィルタ条件を保存するには、[保存 (Save)] アイコンをクリックします。これはユーザ定義のフィルタになります。</p> <p>(注) ユーザ定義のフィルタは、[プリセット フィルタの管理 (Manage Preset Filters)] ダイアログボックスに表示されます。</p> <ul style="list-style-type: none"> • [すべて (All)] : すべてのエントリを表示します。 • [プリセット フィルタの管理 (Manage Preset Filters)] : ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義 フィルタのリスト (List of pre-defined filters)] : システム定義のフィルタを表示します。 <p>(注) [フィルタ (Filter)] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。</p>

表 4 : [障害履歴 (Faults History)] 領域

[名前 (Name)]	説明
時刻 (Time)	障害が発生した時刻。
重大度 (Severity)	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> • 緊急 (Emergency) • アラート (Alert) • クリティカル (Critical) • エラー (Error) • 警告 • 通知 (Notice) • 情報 (Informational) • デバッグ (Debug)
ソース (Source)	イベントをログに記録したソフトウェア モジュール。
考えられる原因	障害の原因となったイベントに関連付けられた固有識別情報。
説明	障害についての詳細情報。 提案される解決策も含まれます。

次の作業

Cisco IMC ログ

Cisco IMC ログの表示

手順

ステップ1 [ナビゲーション (Navigation)] ペインの [シャーシ (Chassis)] メニューをクリックします。

ステップ2 [シャーシ (Chassis)] メニューの [障害およびログ (Faults and Logs)] をクリックします。

ステップ3 [Cisco IMC ログ (Cisco IMC Log)] タブで、次の情報を確認します。

表 5 : [アクション (Actions)] 領域

[名前 (Name)]	説明
[ログの消去 (Clear Log)] ボタン	すべてのログファイルを消去します。 (注) このオプションは、ユーザ ID が [admin] または [user] ユーザ ロールに割り当てられている場合にのみ使用できます。
[合計 (Total)]	[Cisco IMC ログ (Cisco IMC Log)] テーブルの合計行数を表示します。
[列 (Column)] ドロップダウンリスト	表示する列を選択できます。

[名前 (Name)]	説明
[表示 (Show)] ドロップダウンリスト	<p>フィルタを使用して Cisco IMC ログエントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。</p> <ul style="list-style-type: none"> ・[クイック フィルタ (Quick Filter)] : デフォルト ビュー。 ・[高度なフィルタ (Advanced Filter)] : 1つ以上の条件に基づきログエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは[フィルタ (Filter)] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 <p>設定したフィルタ条件に一致するエントリを表示するには、[移動 (Go)] をクリックします。</p> <p>設定したフィルタ条件を保存するには、[保存 (Save)] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。</p> <p>(注) ユーザ定義のフィルタは、[プリセット フィルタの管理 (Manage Preset Filters)] ダイアログボックスに表示されます。</p> <ul style="list-style-type: none"> ・[すべて (All)] : すべてのエントリを表示します。 ・[プリセット フィルタの管理 (Manage Preset Filters)] : ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 ・[事前定義 フィルタのリスト (List of pre-defined filters)] : システム定義のフィルタを表示します。 <p>(注) [フィルタ (Filter)] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。</p>

表 6 : [Cisco IMC ログ (Cisco IMC Log)] テーブル

[名前 (Name)]	説明
[時刻 (Time)] カラム	イベントが発生した日時。
[重大度 (Severity)] カラム	イベントの重大度。次のいずれかになります。 <ul style="list-style-type: none"> • 緊急 (Emergency) • アラート (Alert) • クリティカル (Critical) • エラー (Error) • 警告 • 通知 (Notice) • 情報 (Informational) • デバッグ (Debug)
[ソース (Source)] カラム	イベントをログに記録したソフトウェア モジュール。
[説明 (Description)] カラム	イベントの説明。

システムイベントログ

システムイベントログの表示

[システムイベントログ (System Event Log)] タブには、シスコシステムイベントログ (Cisco SEL) の内部に保存される総容量である 131068 エントリに対して、最新の 3008 システムイベントのみが表示されます。Cisco SEL の最大容量 (131068 レコード) に達すると、最も古いエントリが最新のエントリで上書きされます。

手順

- ステップ 1 [ナビゲーション (Navigation)] ペインの [シャーシ (Chassis)] メニューをクリックします。
- ステップ 2 [シャーシ (Chassis)] メニューの [障害およびログ (Faults and Logs)] をクリックします。
- ステップ 3 [システムイベントログ (System Event Log)] タブで、次の情報を確認します。

表 7: [アクション (Actions)] 領域

名称	説明
SEL フルネス インジケータ	[システムイベントログ (System Event Log)] タブの使用済み領域にパーセントで表示されます。この割合は 3008 エントリを基準として計算されます ([システムイベントログ (System Event Log)] タブには、常に最新の 3008 システムイベントのみが表示されます)。たとえば、[システムイベントログ (System Event Log)] タブに 1504 エントリがある場合、50 パーセントとして表示されます。 最初に 3008 エントリのセットに達した後は、SEL がクリアされるまで、状態は常に 100% として表示されます。
[ログの消去 (Clear Log)] ボタン	ログファイルからすべてのイベントをクリアします。 (注) このオプションは、ユーザ ID が [admin] または [user] ユーザ ロールに割り当てられている場合にのみ使用できます。
[シャーシ (Chassis)] ドロップダウンリスト	ログを表示するシャーシまたはサーバを選択します。
[合計 (Total)]	[システムイベントログ (System Event Log)] テーブルの合計行数を表示します。
[列 (Column)] ドロップダウンリスト	表示する列を選択できます。

名称	説明
[表示 (Show)] ドロップダウンリスト	<p>フィルタを使用してイベントを表示する方法をカスタマイズします。これらの内容は次のとおりです。</p> <ul style="list-style-type: none"> • [クイック フィルタ (Quick Filter)] : デフォルト ビュー。 • [高度なフィルタ (Advanced Filter)] : 1つ以上の条件に基づきイベントを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは[フィルタ (Filter)] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 <p>設定したフィルタ条件に一致するエントリを表示するには、[移動 (Go)] をクリックします。</p> <p>設定したフィルタ条件を保存するには、[保存 (Save)] アイコンをクリックします。これはユーザ定義のフィルタになります。</p> <p>(注) ユーザ定義のフィルタは、[プリセット フィルタの管理 (Manage Preset Filters)] ダイアログボックスに表示されます。</p> <ul style="list-style-type: none"> • [すべて (All)] : すべてのエントリを表示します。 • [プリセット フィルタの管理 (Manage Preset Filters)] : ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義 フィルタのリスト (List of pre-defined filters)] : システム定義のフィルタを表示します。 <p>(注) [フィルタ (Filter)] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。</p>

表 8 : [システムイベントログ (System Event Log)] テーブル

名称	説明
[時刻 (Time)] カラム	イベントが発生した日時。
[重大度 (Severity)] カラム	重大度フィールドには、テキストと色分けされたアイコンの両方が含まれます。アイコンについては、緑色は通常動作、黄色は情報を示し、警告、クリティカルおよび回復不能なエラーは赤色で表示されます。
[説明 (Description)] カラム	イベントの説明。

ロギング制御

ロギング制御の表示

手順

ステップ 1 [ナビゲーション (Navigation)] ペインの [シャーシ (Chassis)] メニューをクリックします。

ステップ 2 [シャーシ (Chassis)] メニューの [障害およびログ (Faults and Logs)] をクリックします。

ステップ 3 [ロギング制御 (Logging Controls)] タブで、次の情報を確認します。
リモートロギング

[名前 (Name)]	説明
[有効化 (Enable)] チェックボックス	オンにすると、Cisco IMC は [IP アドレス (IP Address)] フィールドで指定された Syslog サーバにログメッセージを送信します。
[ホスト名/IP アドレス (Host Name/IP Address)] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモートシステムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[ポート (Port)] フィールド	1 ~ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

[名前 (Name)]	説明
[プロトコル (Protocol)] フィールド	syslog メッセージ送信用のトランスポート層プロトコル。次のいずれかを選択できます。 <ul style="list-style-type: none"> • [TCP] • UDP
[リポートするための最小重大度 (Minimum Severity to Report)] フィールド	リモートログに含まれるメッセージの最低レベルを指定します。次のいずれかを選択できます。 <ul style="list-style-type: none"> • 緊急 (Emergency) • アラート (Alert) • クリティカル (Critical) • エラー (Error) • 警告 • 通知 (Notice) • 情報 (Informational) • デバッグ (Debug)

(注) Cisco IMC では、選択した重大度よりも低い重大度のメッセージはリモートでログに記録されません。たとえば、[エラー (Error)] を選択した場合、Cisco IMC リモートログには重大度が [緊急 (Emergency)]、[アラート (Alert)]、[クリティカル (Critical)]、または [エラー (Error)] のすべてのメッセージが含まれます。[警告 (Warning)]、[通知 (Notice)]、[情報 (Informational)]、または [デバッグ (Debug)] のメッセージは表示されません。

ローカル ロギング (Local Logging)

この領域には、上記の表に示すように [リポートするための最小重大度 (Minimum Severity to Report)] ドロップダウンリストのみが表示されます。ローカルログに含めるメッセージの最低レベルを指定できます。

次の作業

リモートサーバへの Cisco IMC ログの送信

Cisco IMC ログエントリを受信するように 1 台または 2 台のリモート syslog サーバのプロファイルを設定できます。

はじめる前に

- リモート syslog サーバが、リモートホストからのログを受信するよう設定されている必要があります。
- リモート syslog サーバが、authentication-related ログなどのすべてのタイプのログを受信するよう設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達することを許可するよう設定されている必要があります。

手順

ステップ1 [ナビゲーション (Navigation)] ペインの [シャーシ (Chassis)] メニューをクリックします。

ステップ2 [シャーシ (Chassis)] メニューの [障害およびログ (Faults and Logs)] をクリックします。

ステップ3 [リモート Syslog サーバ (Remote Syslog Server)] 領域のいずれかで、次のフィールドに値を入力します。

[名前 (Name)]	説明
[有効化 (Enable)] チェックボックス	オンにすると、Cisco IMC は [IP アドレス (IP Address)] フィールドで指定された Syslog サーバにログメッセージを送信します。
[ホスト名/IP アドレス (Host Name/IP Address)] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモートシステムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[ポート (Port)] フィールド	1 ~ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

ステップ4 (任意) [リポートするための最小重大度 (Minimum Severity to Report)] ドロップダウンリストで、リモートログに含まれるメッセージの最低レベルを指定します。次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- 緊急 (Emergency)
- アラート (Alert)
- クリティカル (Critical)
- エラー (Error)
- 警告
- 通知 (Notice)
- 情報 (Informational)

- デバッグ (Debug)

(注) Cisco IMC では、選択した重大度よりも低い重大度のメッセージは、リモートでログに記録されません。たとえば、[エラー (Error)]を選択した場合、Cisco IMC リモートログには重大度が[緊急 (Emergency)]、[アラート (Alert)]、[クリティカル (Critical)]、または[エラー (Error)]のすべてのメッセージが含まれます。[警告 (Warning)]、[通知 (Notice)]、[情報 (Informational)]、または[デバッグ (Debug)]のメッセージは表示されません。

ステップ5 [変更の保存 (Save Changes)] をクリックします。

Cisco IMC ログしきい値の設定

はじめる前に

手順

- ステップ1 [ナビゲーション (Navigation)]ペインの[シャーシ (Chassis)]メニューをクリックします。
ステップ2 [シャーシ (Chassis)]メニューの[障害およびログ (Faults and Logs)]をクリックします。
ステップ3 [ローカルロギング (Local Logging)]領域で、[リポートするための最小重大度 (Minimum Severity to Report)]ドロップダウンリストを使用して、Cisco IMC ログに含まれるメッセージの最低レベルを指定します。
次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- 緊急 (Emergency)
- アラート (Alert)
- クリティカル (Critical)
- エラー (Error)
- 警告
- 通知 (Notice)
- 情報 (Informational)
- デバッグ (Debug)

(注) Cisco IMC では、選択した重大度よりも低い重大度のメッセージはログに記録されません。たとえば、[エラー (Error)]を選択した場合、Cisco IMC ログには重大度が[緊急 (Emergency)]、[アラート (Alert)]、[クリティカル (Critical)]、または[エラー (Error)]のすべてのメッセージが含まれます。[警告 (Warning)]、[通知 (Notice)]、[情報 (Informational)]、または[デバッグ (Debug)]のメッセージは表示されません。

リモートサーバへのテスト Cisco IMC ログの送信

はじめる前に

- リモート syslog サーバが、リモートホストからのログを受信するよう設定されている必要があります。
- リモート syslog サーバが、authentication-related ログなどのすべてのタイプのログを受信するよう設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達することを許可するよう設定されている必要があります。

手順

ステップ1 [ナビゲーション (Navigation)] ペインの [シャーシ (Chassis)] メニューをクリックします。

ステップ2 [シャーシ (Chassis)] メニューの [障害およびログ (Faults and Logs)] をクリックします。

ステップ3 [障害およびログ (Faults and Logs)] ペインの [ロギング制御 (Logging Controls)] タブをクリックします。

ステップ4 [アクション (Action)] 領域の [テスト Syslog の送信 (Send Test Syslog)] をクリックします。設定されているリモートサーバにテスト Cisco IMC ログが送信されます。