障害およびログの表示

この章は、次の内容で構成されています。

障害サマリ

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 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Faults Summary] タブで、次の情報を確認します。

表 *1 : [Actions]* 領域

名前	説明
[Total]	[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	説明
[表示（Show）] ドロップダウン リスト	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。 • [簡易フィルタ（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いて障害エントリを表示するためのフィルタ オプション。マッチング ルールを使用して、[フィルタ（Filter）] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [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。

表 *2 : [*障害エントリ（*Fault Entries*）*]* 領域

名前	説明
[Time]	障害が発生した時刻。
シビラティ（重大度）（**Severity**）	次のいずれかになります。 • [クリア済み（Cleared）] : 障害または状態がクリアされました。 • **[Critical]** • **[Info]** • メジャー • マイナー • 警告
[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。
[Probable Cause]	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。
[Description]	障害についての詳細情報。 提案されるソリューションも含まれます。

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 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Faults History] タブで、次の情報を確認します。

表 *3 : [Actions]* 領域

名前	説明
[Total]	[Fault History] テーブルの合計行数を表示します。
[Column] ドロップダウン リスト	表示する列を選択できます。
[Show] ドロップダウン リスト	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。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づいてエントリを表示するフィルタ オプション。マッチング ルールを使用して、[Filter] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [Filter]アイコンを使用して、フィルタ フィールドの表示/非表示を切り替えることできます。

表 *4 : [Fault History]* エリア

名前	説明
[Time]	障害が発生した時刻。
シビラティ（重大度）（**Severity**）	次のいずれかになります。 • **[緊急（Emergency）]** • **[アラート（Alert）]** • **[Critical]** • **[エラー（Error）]** • 警告 • **[Notice]** • **[Informational]** • **デバッグ（Debug）**
[Source]	イベントをログに記録したソフトウェア モジュール。
[Probable Cause]	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。
[Description]	障害についての詳細情報。 提案されるソリューションも含まれます。

次のタスク

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 [Chassis] メニューで、[Faults and Logs] をクリックします。
ステップ 3 [Cisco IMC Log] タブで、次の情報を確認します。

表 *5 : [Actions]* 領域

名前	説明
[Clear Log] ボタン	すべてのログ ファイルをクリアします。 （注） このオプションは、ユーザ ID に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。
[Total]	[Cisco IMC Log] テーブルの合計行数を表示します。
[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	説明
[Show] ドロップダウン リスト	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。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づいてログ エントリを表示するフィルタ オプション。マッチング ルールを使用して、[Filter] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [Filter] アイコンを使用して、フィルタ フィールドの表示/非表示を切り替えることできます。

表 *6 : [Cisco IMC Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。

名前	説明
[Severity] カラム	イベントのシビラティ（重大度）。次のいずれかになります。 • **[緊急（Emergency）]** • **[アラート（Alert）]** • **[Critical]** • **[エラー（Error）]** • **警告** • **[Notice]** • **[Informational]** • **デバッグ（Debug）**
[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。
[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 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [System Event Log] タブで、次の情報を確認します。

表 *7 : [Actions]* 領域

名前	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。
[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 に **admin** または **user** ユーザ ロールが割り当てられている場合のみ使用できます。
[Chassis] ドロップダウン リスト	ログを表示する対象のシャーシまたはサーバを選択します。
[Total]	[System Event Log] テーブルの合計行数を表示します。
[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	説明
[Show] ドロップダウン リスト	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。 • [Quick Filter]：デフォルト ビュー。 • [Advanced Filter]：1 つ以上の条件に基づいてイベントを表示するためのフィルタ オプション。マッチング ルールを使用して、[Filter] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 [Go] をクリックすると、設定したフィルタ基準と一致するエントリが表示されます。 設定したフィルタ基準は、[Save] アイコンをクリックして保存することができます。保存されたフィルタ基準は、ユーザ定義のフィルタとして後で使用できます。 （注） ユーザ定義のフィルタは [Manage Preset Filters] ダイアログボックスに表示されます。 • [All]：すべてのエントリが表示されます。 • [Manage Preset Filters]：ユーザ定義のフィルタが表示されます。このダイアログボックスで、ユーザ定義のフィルタを編集したり削除したりできます。 • [List of pre-defined filters）]：システム定義のフィルタが表示されます。 （注） [フィルタ（Filter）]アイコンを使用して、フィルタ フィールドの表示/非表示を切り替えることできます。

表 *8 : [System Event Log]* テーブル

名前	説明
[Time] カラム	イベントが発生した日時。
[Severity] カラム	シビラティ（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。
[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 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [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	説明
[有効（Enabled）] チェックボックス	オンにすると、Cisco IMC は [IP Address] フィールドで指定された Syslog サーバーにログ メッセージを送信します。
セキュアリモートsyslogの有効化	オンにすると、Cisco IMC は、ロギング用の安全な接続をサポートするリモート Syslog サーバへの安全な暗号化されたアウトバウンド接続を確立します。 （注） このチェックボックスをオンにすると、デフォルトで **[プロトコル（Protocol）]** フィールドが無効になります。
[Host Name/IP Address] フィールド	Cisco IMC ログを保存する 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。

名前	説明
[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 ポート番号は、514 です。
[Protocol] フィールド	syslog メッセージの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。 • TCP • UDP
[握手状態（Handshake Status）]	セキュアなリモート Syslog が有効になっている場合、Cisco IMC は SSL ハンドシェイクを実行して、証明書が指定された IP アドレス用であるかどうかを確認します。
[リポートするための最小シビラティ（重大度）（Minimum Severity to Report）] フィールド	リモート ログに含めるメッセージの最初レベルを指定します。次のいずれかを選択できます。 • **[緊急（Emergency）]** • **[アラート（Alert）]** • **[Critical]** • **[エラー（Error）]** • **警告** • **[Notice]** • **[Informational]** • **デバッグ（Debug）**

（注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（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、[Error] を選択した場合、Cisco IMC リモート ログにはシビラティ（重大度）が [Emergency]、[Alert]、[Critical]、または [Error] のすべてのメッセージが含まれます。[Warning]、[Notice]、[Informational]、または [Debug] のメッセージは表示されません。

Local Logging

このエリアには、上記の表に示す [Minimum Severity to Report] ドロップダウン リストだけが表示されます。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。

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 サーバーのプロファイルを設定できます。

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように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 サーバに到達するように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 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [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	説明
[有効（Enabled）] チェックボックス	オンにすると、Cisco IMC は [IP アドレス（IP Address）] フィールドに指定された Syslog サーバにログ メッセージを送信します。
[**Host Name/IP Address**] フィールド	Cisco IMC ログを保存する 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 ポート番号は、514 です。

ステップ 4 （任意） **[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。シビラティ（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）]**
- **[Critical]**
- **[エラー（Error）]**
- 警告
- **[Notice]**
- **[Informational]**
- デバッグ（**Debug**）

（注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（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、[**Error**] を選択した場合、Cisco IMC リモート ログにはシビラティ（重大度）が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

ステップ 5 **[Save Changes]**をクリックします。

Cisco IMC ログしきい値の設定

始める前に

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 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 必須: [**Local Logging**] 領域で、[**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。シビラティ（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）]**
- **[Critical]**
- **[エラー（Error）]**
- 警告
- **[Notice]**
- **[Informational]**
- デバッグ（**Debug**）

（注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（重大度）のメッセージはログに記録されません。たとえば、[**Error**] を選択した場合、Cisco IMC ログにはシビラティ（重大度）が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

リモート サーバーへのテスト Cisco IMC ログの送信

始める前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように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 サーバに到達するように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 [Chassis] メニューで、[Faults and Logs] をクリックします。

ステップ 3 [Faults and Logs] ペインの [Logging Controls] タブをクリックします。

ステップ 4 [**Action**] 領域の [**Send Test Syslog**] をクリックします。

設定されているリモート サーバーにテスト Cisco IMC ログが送信されます。

リモート Syslog 証明書の管理

リリース 4.2 (2a) 以降、リモート Syslog 証明書を Cisco UCS C シリーズ サーバーにアップロードできます。証明書を 1 つまたは 2 つの Cisco UCS C シリーズ サーバーにアップロードできます。

リモート Syslog 証明書のアップロード

リモート サーバーの場所またはローカルの場所からリモート Syslog 証明書をアップロードできます。

始める前に

- admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer

- .pem

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）]** メニューで、**[障害とログ（Faults and Logs）]** を選択します。

ステップ 3 **[障害とログ（Faults and Logs）]**ペインの **[ロギング制御（Logging Controls）]**を選択します。

ステップ 4 リモート Syslog 証明書をアップロードするには、**[リモート Syslog 証明書のアップロード（Upload Remote Syslog Certificate）]** ボタンをクリックします。

[リモート Syslog 証明書のアップロード（Upload Remote Syslog Certificate）] ダイアログボックスが表示されます。

ステップ 5 **[サーバーの選択:（Select Server:）]** ドロップダウン リストから、リモート Syslog 証明書をアップロードするサーバーを選択します。

ステップ 6 次のいずれかの方法を使用して、証明書をアップロードできます。

- リモートロケーションからアップロード
- ブラウザクライアント経由のアップロード
- **[リモート Syslog 証明書の貼り付け（Paste Remote Syslog Certificate）]** テキスト ボックスに証明書の内容を直接貼り付けます。
- **[リモートの場所からアップロード (Upload from remote location)]**: リモートの場所からリモート syslog 証明書をアップロードするには、このオプションボタンを選択します。

名前	説明
[リモートの場所からアップロード (Upload from remote location)] フィールド	次のいずれかのプロトコルを選択します。 • TFTP • FTP • SCP • SFTP • HTTP （注） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。
[サーバ IP/ホスト名 (Server IP/Hostname)] ボタン	リモート サーバのホスト名または IP アドレスを入力します。
パスおよびファイル名	リモート syslog 証明書をアップロードするリモート サーバ上のファイルパスとファイル名を入力します。

名前	説明
Username	リモート サーバのユーザ名を入力します。
Password	リモート サーバのパスワードです。

- **[ブラウザ クライアントでアップロード (Upload by Browser client)]**: ブラウザ クライアントを使用してリモート syslog 証明書をアップロードするには、このオプション ボタンを選択します。

  [参照 (Browse)] をクリックして、リモート syslog 証明書をアップロードする場所に移動します。

- **[リモート Syslog 証明書の内容をペースト (Paste リモート Syslog Certificate Content)]**: このオプション ボタンを選択すると、外部証明書の詳細がテキスト ボックスに直接貼り付けられます。

リモート Syslog 証明書の削除

サーバーからリモート Syslog 証明書を削除できます。

始める前に

admin 権限を持つユーザとしてログインする必要があります。

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）]** メニューで、**[障害とログ（Faults and Logs）]** を選択します。

ステップ 3 **[障害とログ（Faults and Logs）]**ペインの **[ロギング制御（Logging Controls）]**を選択します。

ステップ 4 リモート Syslog 証明書を削除するには、**[リモート Syslog 証明書の削除（Delete Remote Syslog Certificate）]** ボタンをクリックします。

[リモート Syslog 証明書の削除（Delete Remote Syslog Certificate）] ダイアログボックスが表示されます。

ステップ 5 リモート Syslog 証明書を削除するサーバーのそれぞれのチェック ボックスを選択します。

ステップ 6 [削除（Delete）] をクリックします。

ポップアップ ウィンドウに削除の確認メッセージが表示されます。

ステップ 7 [OK] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。