CHAPTER 10

トラブルシューティング

この項では、Cisco Intercompany Media Engine サーバをトラブルシューティングする際に役立つツールについて説明します。Cisco Intercompany Media Engine 機能のトラブルシューティングに関する詳細については、以下の URL を参照してください。

http://docwiki.cisco.com/wiki/Cisco_Intercompany_Media_Engine

この項では、次のトピックについて取り上げます。

システム履歴ログ

このシステム履歴ログにより、初期システム インストール、システム アップグレード、Cisco オプション インストール、DRS バックアップと DRS 復元、バージョンの切り替え、リブート履歴などの情報が一元的に管理され、これらの概要をすばやく取得できます。

この項では、次のトピックについて取り上げます。

システム履歴ログの概要

システム履歴ログはシンプルな ASCII ファイル（**system-history.log**）で、データはデータベースでは管理されません。このログは過度にサイズが大きくなることがないため、システム履歴ファイルのローテーションは行われません。

システム履歴ログは、以下の機能を提供します。

- サーバ上の初期ソフトウェア インストールをログに記録します。
- すべてのソフトウェア アップグレード（Cisco オプション ファイルおよびパッチ）の成功、失敗、またはキャンセルをログに記録します。
- 実行されたすべての DRS のバックアップおよび復元をログに記録します。
- CLI または GUI によって発行されるバージョンの切り替えの呼び出しをすべてログに記録します。

- CLI または GUI によって発行される再起動とシャットダウンの呼び出しをすべてログに記録します。
- システムのすべてのブートをログに記録します。ブートは、再起動エントリまたはシャットダウン エントリと関連しない場合、手動によるリブート、電源の再投入、またはカーネル パニックの結果として生じます。
- 初期インストールから、または機能が使用可能になってからのシステム履歴を収めた単一ファイルを管理します。
- インストール フォルダに存在します。**file** コマンドを使用して CLI から、または Real Time Monitoring Tool（RTMT; リアルタイム監視ツール）からログにアクセスできます。

システム履歴ログのフィールド

ログには、製品名、製品バージョン、カーネル イメージなどの情報を格納する一般的なヘッダーが表示されます。以下に例を示します。

==========

Product Name - Cisco Intercompany Media Engine

Product Version - 8.0.0.30671-1

Kernel Image - 2.6.9-78.EL

==========

各システム履歴ログ エントリには、以下のフィールドが含まれます。

timestamp userid action description start/result

システム履歴ログ フィールドには、以下の値が含まれます。

- *timestamp*：サーバ上のローカル時刻と日付を *mm/dd/yyyy hh:mm:ss* という形式で表示します。
- *userid*：アクションを起動したユーザのユーザ名を表示します。
- *action*：以下のアクションのいずれか 1 つを表示します。
  - インストール
  - アップグレード
  - Cisco オプション インストール
  - バージョンの切り替え
  - システム再起動
  - シャットダウン
  - ブート
  - DRS バックアップ
  - DRS 復元
- *description*：以下のメッセージのいずれか 1 つを表示します。
  - *Version*：基本インストール アクションおよびアップグレード アクションに関する表示です。
  - *Cisco Option file name*：Cisco オプション インストール アクションに関する表示です。
  - *Timestamp*：DRS バックアップ アクションおよび DRS 復元アクションに関する表示です。
  - *Active version to inactive version*：バージョンの切り替えアクションに関する表示です。
  - *Active version*：システム再起動アクション、シャットダウン アクション、およびブート アクションに関する表示です。

- *result*：以下の結果を表示します。
  - 開始
  - 成功または失敗
  - キャンセル

例

例 1 にシステム履歴ログのサンプルを示します。

例 1　　システム履歴ログ

```
======================================
Product Name -    Cisco Intercompany Media Engine
Product Version - 8.0.0.30671-1
Kernel Image -    2.6.9-78.EL
======================================
08/28/2009 10:40:34 | root: Install 8.0.0.30671-1 Start
08/28/2009 10:58:03 | root: Boot 8.0.0.30671-1 Start
08/28/2009 11:02:47 | root: Install 8.0.0.30671-1 Success
08/28/2009 11:02:47 | root: Boot 8.0.0.30671-1 Start
08/28/2009 13:33:48 | root: Cisco Option Install ciscoime.proxy_commands.cop Start
08/28/2009 13:34:18 | root: Cisco Option Install ciscoime.proxy_commands.cop Success
09/07/2009 23:44:43 | root: Upgrade 8.0.0.30600-103 Start
09/07/2009 23:56:48 | root: Upgrade 8.0.0.30600-103 Success
09/07/2009 23:57:06 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103 Start
09/07/2009 23:57:52 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103 Success
09/07/2009 23:57:52 | root: Restart 8.0.0.30600-103 Start
09/08/2009 00:00:36 | root: Boot 8.0.0.30600-103 Start
09/17/2009 12:40:38 | root: Upgrade 8.0.0.96000-2 Start
09/17/2009 12:52:54 | root: Upgrade 8.0.0.96000-2 Success
09/17/2009 12:53:11 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2 Start
09/17/2009 12:53:55 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2 Success
09/17/2009 12:53:55 | root: Restart 8.0.0.96000-2 Start
09/17/2009 12:56:27 | root: Boot 8.0.0.96000-2 Start
09/17/2009 13:29:47 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103 Start
09/17/2009 13:30:34 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103 Success
09/17/2009 13:30:34 | root: Restart 8.0.0.30600-103 Start
09/17/2009 13:33:06 | root: Boot 8.0.0.30600-103 Start
09/17/2009 14:22:20 | root: Upgrade 8.0.0.30600-9003 Start
09/17/2009 14:33:30 | root: Upgrade 8.0.0.30600-9003 Success
09/17/2009 14:33:48 | root: Switch Version 8.0.0.30600-103 to 8.0.0.30600-9003 Start
09/17/2009 14:34:33 | root: Switch Version 8.0.0.30600-103 to 8.0.0.30600-9003 Success
09/17/2009 14:34:33 | root: Restart 8.0.0.30600-9003 Start
09/17/2009 14:37:03 | root: Boot 8.0.0.30600-9003 Start
```

システム履歴ログへのアクセス

CLI または RTMT のいずれかを使用して、システム履歴ログにアクセスできます。

CLI の使用

CLI **file** コマンドを使用して、システム履歴ログにアクセスできます。以下に例を示します。

- **file view install system-history.log**
- **file get install system-history.log**

CLI **file** コマンドの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

RTMT の使用

RTMT を使用して、システム履歴ログにアクセスできます。[Trace & Log Central] タブから [インストールログの収集 (Collect Install Logs)] を選択します。

RTMT の使用方法の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

監査ロギング

一元化された監査ロギングにより、Cisco Intercompany Media Engine システムへの設定変更を監査用の別のログ ファイルに記録できます。監査イベントとは、ログの記録が必要なすべてのイベントを表します。以下の Cisco Intercompany Media Engine システム コンポーネントは監査イベントを生成します。

- Real-Time Monitoring Tool
- Cisco Unified Communications オペレーティング システム
- コマンド ライン インターフェイス
- リモート サポート アカウント有効化（テクニカル サポート チームによって発行される CLI コマンド）

以下に、監査イベントの例を示します。

```
10:39:28.787| UserID:Administrator  ClientAddress:10.194.109.32  Severity:6  EventType:
CLICommand  ResourceAccessed: GenericCLI  EventStatus: Success  CompulsoryEvent: No
AuditCategory: AdministrativeEvent  ComponentID: CLI  AuditDetails: CLI Command-> utils
ime license file install IME20091020095547801_node32.lic App ID:Command Line Cluster ID:
Node ID: node32
```

監査イベントに関する情報が記録される監査ログは、共通パーティションで書き込まれます。Log Partition Monitor（LPM）を使用して、トレース ファイルと同様、必要に応じてこれらの監査ログの消去を管理します。デフォルトでは、LPM は監査ログを消去しますが、監査ユーザは Cisco Intercompany Media Engine Command Line Interface（CLI; コマンド ライン インターフェイス）からこの設定を変更できます。LPM は、共通パーティションのディスク使用量がしきい値を超えたときにアラートを送信します。ただし、このアラートには、監査ログまたはトレース ファイルのどちらのためにディスクがいっぱいになったかを示す情報は含まれていません。

ヒント　Cisco Audit Event Service は、監査ロギングをサポートしています。監査ログが記録されていない場合、CLI（utils service stop **Cisco Audit Event Service** および utils service start **Cisco Audit Event Service**）を使用してこのサービスを停止および開始します。

Real-Time Monitoring Tool の [Trace & Log Central] から、すべての監査ログの収集、表示、および削除が行えます。RTMT の [Trace & Log Central] で監査ログにアクセスします。[システム (System)] > [リアルタイムトレース (Real Time trace)] > [監査ログ (Audit Logs)] > [ノード (Nodes)] と進みます。ノードを選択した後、別ウィンドウが表示されたら、[システム (System)] > [Cisco 監査ログ (Cisco Audit Logs)] を選択します。

以下のタイプの監査ログが RTMT に表示されます。

- 「アプリケーション ログ」（P.10-5）
- 「オペレーティング システム ログ」（P.10-5）
- 「リモート サポート アカウント有効化のログ」（P.10-6）

アプリケーション ログ

RTMT の AuditApp フォルダに表示されるアプリケーション監査ログは、Cisco Unified Communications Manager の管理、Cisco Unified サービスアビリティ、CLI、および Real-Time Monitoring Tool（RTMT; リアルタイム監視ツール）の設定変更を行います。

デフォルトでは、アプリケーション ログは有効ですが、CLI **set auditlog status** コマンドを使用して監査ロギングを無効にできます。監査ログが無効になると、監査ログ ファイルは新規で作成されなくなります。

Cisco Unified Communications Manager は、設定された最大ファイル サイズに達するまで、1 つのアプリケーション監査ログ ファイルを使用します。最大ファイル サイズに達すると、そのファイルを閉じ、新規アプリケーション監査ログ ファイルを作成します。システムでログ ファイルのローテーションが指定されている場合、Cisco Unified Communications Manager は設定されている数のファイルを保存します。ロギング イベントの一部は、RTMT SyslogViewer を使用して表示できます。

以下の Cisco Unified サービスアビリティのイベントは、ログに記録されます。

- [サービスアビリティ (Serviceability)] ウィンドウからのサービスのアクティブ化、非アクティブ化、開始、または停止。
- トレース設定およびアラーム設定での変更。
- SNMP 設定での変更。

RTMT は、監査イベント アラームを使用する以下のイベントをログに記録します。

- アラート設定。
- アラート一時停止。
- 電子メール設定。
- ノード アラート ステータスの設定。
- アラート追加。
- アラート アクションの追加。
- アラートのクリア。
- アラートの有効化。
- アラート アクションの削除。
- アラートの削除。

（注） 監査ログは、コマンドの実行が許可されていない場合でも、CLI コマンドを正常にログに記録します。たとえば、次の操作は、ブートストラップ サーバでのみ許可されています。

```
admin:set ime dht global storagequota 1
```

上記のコマンドが他のサーバで実行されると、ユーザは「このコマンドの実行はブートストラップサーバでのみ許可されています(This command is only allowed to be run on a bootstrap server)」というメッセージを受け取りますが、監査ログは CLI コマンドを status=Success でログに記録します。

オペレーティング システム ログ

RTMT の vos フォルダに表示されるオペレーティング システム監査ログは、オペレーティング システムによってトリガーされるイベントを記録します。デフォルトでは、有効ではありません。**utils auditd** CLI コマンドによって、このイベントに関するステータスの有効化、無効化、または付与が行われます。

CLI で監査が有効になるまで、RTMT の vos フォルダには表示されません。

リモート サポート アカウント有効化のログ

RTMT の vos フォルダに表示されるリモート サポート アカウント有効化の監査ログは、テクニカル サポート チームによって発行される CLI コマンドを記録します。ユーザはこのログを設定できません。このログは、テクニカル サポート チームによってリモート サポート アカウントが有効なときのみ、作成されます。

監査ロギングの設定

表 10-1 に、Cisco Intercompany Media Engine サーバで SNMP ユーザを操作するために必要なコマンドを示します。

表 10-1　監査ロギング設定チェックリスト

設定手順		関連する手順と項目
ステップ 1	オペレーティング システム監査ログを有効にします。RTMT からシステムの監査ログ ファイルを取得できます。 **ヒント** オペレーティング システム監査ログのステータスを確認するには、**utils auditd status** CLI コマンドを入力します。	utils auditd *status* ここで、 *status* は enable または disable です。
ステップ 2	監査ロギングを有効にします。RTMT からシステムの監査ログ ファイルを取得できます。 **ヒント** 監査ログのステータスを確認するには、**show auditlog** CLI コマンドを入力します。	set auditlog status *status* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *status* は enable または disable です。
ステップ 3	ステータスの消去を設定します。 Log Partition Monitor（LPM）は、[消去の有効化 (Enable Purging)] オプションを確認し、監査ログを消去するかどうかを識別します。消去が有効な場合、共通パーティションのディスク使用量が最高水準値を超えると、LPM は RTMT 内のすべての監査ログ ファイルを消去します。ただし、チェックボックスをオフにすることで、消去を無効にできます。 消去が無効な場合、ディスクがいっぱいになるまで、監査ログの数は増加します。このアクションは、システムに障害が発生する原因になる可能性があります。 この消去オプションは、監査ログがあるパーティションがアクティブかどうかに応じて指定できます。監査ログが非アクティブなパーティションにある場合、ディスク使用量が最高水準値を超えたときに、それらの監査ログを消去します。 RTMT の [Trace & Log Central] > [監査ログ (Audit Logs)] を選択して、監査ログにアクセスできます。	set auditlog purging *status* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *status* は enable または disable です。

表 10-1　監査ロギング設定チェックリスト （続き）

設定手順		関連する手順と項目
ステップ 4	ログ ローテーション ステータスを設定します。 システムは、このオプションを読み込み、監査ログ ファイルをローテーションする必要があるか、または新規ファイルを作成し続ける必要があるかを識別します。ファイルの最大数は、5000 を超えて指定できません。[ローテーションの有効化 (Enable Rotation)] オプションが有効な場合、ファイルの最大数に達すると、システムは最も古い監査ログ ファイルから上書きを開始します。 **ヒント** ローテーションが無効な場合、監査ログは [ファイルの最大数 (Maximum No. of Files)] 設定 を無視します。	set auditlogrotation *status* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *status* は enable または disable です。
ステップ 5	ファイルの最大数を設定します。 ログに含めるファイルの最大数を入力します。[ファイルの最大数 (Maximum No. of Files)] 設定に入力した値が、[ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)] 設定に入力した値より 大きいことを確認してください。	set auditlog maxnumfiles *filecount* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *filecount* は 1 ～ 10000 の範囲です。
ステップ 6	最大ファイル サイズを設定します。	set auditlog maxfilesize *size* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *size* は 1 ～ 10 の範囲です。
ステップ 7	監査ログ リモート Syslog 重大度レベルを設定します。	set auditlog remotesyslogseverity *severity* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *severity* は 「緊急 (Emergency)」、「アラート (Alert)」、「重要 (Critical)」、「エラー (Error)」、「警告 (Warning)」、「通知 (Notice)」、「情報 (Informational)」、または「デバッグ (Debug)」 のいずれかです。
ステップ 8	リモート Syslog サーバ名を入力します。	set auditlog remotesyslogserver *servername* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *servername* は、リモート Syslog サーバの有効なホスト名です。

netdump ユーティリティ

netdump ユーティリティを使用して、データおよびメモリ クラッシュ ダンプ ログをネットワーク上の 1 台のサーバから別のサーバに送信できます。netdump クライアントとして設定されたサーバは、クラッシュ ログを netdump サーバとして設定されたサーバに送信します。ログ ファイルは、netdump サーバのクラッシュ ディレクトリに送信されます。

Cisco Unified Communications Manager クラスタでは、少なくとも 2 つのノードを netdump サーバとして設定する必要があります。そうすることで、最初のノードも後続のノードも、相互にクラッシュ ダンプ ログを送信できます。

たとえば、クラスタに 3 台のサーバ（1 台のプライマリ（最初の）ノードと 2 台の後続ノード）がある場合、最初のノードと後続ノード #1 を netdump サーバとして設定できます。また、最初のノードを後続ノード #1 の netdump クライアントとして設定し、後続のすべてのノードを最初のノードの netdump クライアントとして設定できます。最初のノードがクラッシュした場合、最初のノードは netdump を後続ノード #1 に送信します。後続ノードのいずれかがクラッシュした場合、そのノードは netdump を最初のノードに送信します。

Cisco Unified Communications Manager サーバを netdump サーバとして設定する代わりに、外部の netdump サーバを使用することもできます。外部 netdump サーバの設定の詳細については、TAC にお問い合わせください。

（注） Cisco は、Cisco Unified Communications Manager をインストールした後に netdump ユーティリティを設定して、トラブルシューティングに役立てることをお勧めします。設定をまだ行っていない場合、サポートされているアプライアンス リリースから Cisco Unified Communications Manager をアップグレードする前に、この netdump ユーティリティを設定してください。

netdump のサーバおよびクライアントを設定するには、次のセクションで説明されるように、Cisco Unified Communications オペレーティング システムを使用可能にする Command Line Interface（CLI; コマンド ライン インターフェイス）を使用します。

- 「netdump サーバの設定」（P.10-9）
- 「netdump クライアントの設定」（P.10-10）
- 「netdump サーバが収集するファイルでの作業」（P.10-10）
- 「netdump ステータスの監視」（P.10-10）

netdump サーバの設定

netdump サーバとしてノードを設定するには、以下の手順を使用します。

手順

ステップ 1　『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』で説明されているように、netdump サーバとして設定するノード上で、CLI セッションを開始します。

ステップ 2　**utils netdump server start** コマンドを実行します。

ステップ 3　netdump サーバのステータスを表示するには、**utils netdump server status** コマンドを実行します。

ステップ 4　「netdump クライアントの設定」（P.10-10）で説明されるように、netdump クライアントを設定します。

netdump クライアントの設定

netdump クライアントとしてノードを設定するには、以下の手順を使用します。

手順

ステップ 1　『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』で説明されているように、netdump クライアントとして設定するノード上で、CLI セッションを開始します。

ステップ 2　**utils netdump client start** *ip-address-of-netdump-server* コマンドを実行します。

ステップ 3　**utils netdump server add-client** *ip-address-of-netdump-client* を実行します。netdump クライアントとして設定する各ノードに対して、このコマンドを繰り返し実行します。

（注）　正しい IP アドレスが入力されているか確認してください。CLI は IP アドレスを検証しません。

ステップ 4　netdump クライアントのステータスを表示するには、**utils netdump client status** コマンドを実行します。

netdump サーバが収集するファイルでの作業

netdump サーバからクラッシュ情報を表示するには、Real-Time Monitoring Tool または Command Line Interface（CLI; コマンド ライン インターフェイス）を使用します。Real-Time Monitoring Tool を使用して netdump ログを収集するには、[Trace & Log Central] で [ファイルの収集 (Collect Files)] オプションを選択します。[システムサービス / アプリケーションの選択 (Select System Services/Applications)] タブで、[Netdump ログ (Netdump logs)] チェックボックスを選択します。Real-Time Monitoring Tool を使用するファイルの収集の詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

CLI を使用して netdump ログを収集するには、クラッシュ ディレクトリにあるファイルに「file」CLI コマンドを実行します。ログのファイル名は、netdump クライアントの IP アドレスで始まり、末尾にファイルの作成日が付きます。file コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

netdump ステータスの監視

Real-Time Monitoring Tool の SyslogSearchStringFound アラートを設定して、netdump ステータスを監視できます。以下の手順を使用して、適切なアラートを設定してください。

手順

ステップ 1　Real-Time Monitoring Tool のクイック起動チャネルから、[ツール (Tools)] > [Alert Central] を選択します。

ステップ 2　[SyslogStringMatchFound] アラートを右クリックし、[アラート / プロパティの設定 (Set Alert/Properties)] を選択します。

ステップ 3　[次へ (Next)] を 3 回クリックします。

ステップ 4　[SysLogアラート(SysLog Alert)] ウィンドウで、[追加(Add)] ボタンをクリックします。[検索文字列の追加(Add Search String)] ダイアログボックスが表示されたら、「**netdump: failed**」を入力し、[追加(Add)] をクリックします。次に、[次へ(Next)] をクリックします。

（注）　大文字/小文字および構文が完全に一致していることを確認してください。

ステップ 5　[電子メール通知(Email Notification)] ウィンドウで、適切なトリガー アラート アクションを選択して、任意のユーザ定義の電子メール テキストを入力し、[保存(Save)] をクリックします。