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の詳細については、次の URL を参照してください。

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

- システム履歴ログ，1 ページ
- 監査ロギング，5 ページ
- netdump ユーティリティ，10 ページ

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。

関連トピック

システム履歴ログの機能，（1 ページ）

システム履歴ログのフィールド，（2 ページ）

CLI を使用したシステム履歴ログへのアクセス，（4 ページ）

システム履歴ログの機能

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（シスコ 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、またはリアルタイム監視ツール（RTMT）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含む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な日付と時刻が `mm/dd/yyyy hh:mm:ss` の形式で表示されます。
- 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

以下に、システム履歴ログの例を示します。

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
```

CLI を使用したシステム履歴ログへのアクセス

CLI を使用してシステム履歴ログにアクセスできます。

手順

システム履歴ログにアクセスするには、次の 2 つの **CLI file** コマンドのいずれかを使用します。

- `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。

関連トピック

RTMT を使用したシステム履歴ログへのアクセス，（5 ページ）

RTMT を使用したシステム履歴ログへのアクセス

RTMT を使用してシステム履歴ログにアクセスできます。

手順

[Trace & Log Central] タブから [インストールログの収集(Collect Install Logs)] をクリックします。RTMT の使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

関連トピック

CLI を使用したシステム履歴ログへのアクセス, （4 ページ）

監査ロギング

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。

- リアルタイム モニタリング ツール
- 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に書き込まれます。 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 コマンドライン インターフェイス（CLI）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。

すべての監査ログは、リアルタイム監視ツールの Trace & Log Central で収集、表示、および削除されます。 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)] と移動します。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。

関連トピック

監査ログの種類, （6 ページ）
監査ロギングのセットアップ, （9 ページ）

監査ログの種類

以下の種類の監査ログが RTMT に表示されます。

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、およびリアルタイム モニタリング ツール（RTMT）の設定変更についての情報を提供します。

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 では、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 ファイルが使用されます。最大ファイル サイズに達すると、そのファイルが閉じられ、新規アプリケーション監査ログ ファイルが作成されます。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 では設定されている数のファイルが保存されます。 ロギング イベントの一部は、RTMT Syslog Viewer 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の変更。
- SNMP 設定の変更。

RTMT は、監査イベント アラームで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 で監査が有効化されるまで、RTMT の vos フォルダは表示されません。

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。

監査ロギングのセットアップ

次の表に、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。

手順

ステップ 1 コマンド `utils auditd status` を実行して、オペレーティング システム監査ログを有効化します。status は enable または disable です。 RTMT からシステムの監査ログ ファイルを取得できます。

ステップ 2 コマンド `set auditlog status` を実行して、監査ロギングを有効化します。
status パラメータ（enable または disable）を入力するよう求めるプロンプトが表示されます。

RTMT からシステムの監査ログ ファイルを取得できます。

ステップ 3 コマンド `set auditlog purging` を実行して、ステータスの消去を設定します。
status パラメータ（enable または disable）を入力するよう求めるプロンプトが表示されます。

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、アクティブなパーティションにある監査ログに対して使用可能です。 非アクティブなパーティションに監査ログがある場合は、ディス

ク使用量が最高水準値を超えたときに、それらの監査ログは消去されます。 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。

ステップ 4 コマンド `set auditlogrotation` を実行して、ログ ローテーション ステータスを設定します。
status パラメータ（enable または disable）を入力するよう求めるプロンプトが表示されます。

（注） ログ 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。

システムは、このオプションを読み取り、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。

ステップ 5 コマンド `set auditlog maxfilesize` を実行して、ファイルの最大数を設定します。
size パラメータ（1 ～ 10）を入力するよう求めるプロンプトが表示されます。

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)] 設定の入力値は、 [ログ ローテーションで削除されるファイルの数(No. of Files Deleted on Log Rotation)] 設定 に入力する値よりも大きくなるようにしてください。

ステップ 6 コマンド `set auditlog maxnumfiles` を実行して、最大ファイル サイズを設定します。
filecount パラメータ（1 ～ 10000）を入力するよう求めるプロンプトが表示されます。

ステップ 7 コマンド `set auditlog remotesyslogseverity` を実行して、監査ログ リモート Syslog 重大度レベルを設定します。
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。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 コマンド `set auditlog remotesyslogserver` を実行して、リモート Syslog サーバ名を設定します。
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。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

Cisco Unified Communications Manager クラスタでは、netdump サーバとして少なくとも 2 つのノードを設定し、最初のノードと後続ノードの間でクラッシュ ダンプログを互いに送信できるようにする必要があります。

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。 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） シスコは、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。 netdump ユーティリティの設定をまだ行っていない場合は、Cisco Unified Communications Manager をサポート対象のアプライアンス リリースからアップグレードする前に行ってください。

netdump のサーバおよびクライアントを設定するには、Cisco Unified Communications オペレーティング システムで使用可能なコマンドライン インターフェイス（CLI）を使用します。

関連トピック

netdump サーバのセットアップ，（11 ページ）
netdump クライアントのセットアップ，（11 ページ）
netdump サーバ ファイル，（12 ページ）
netdump ステータスのモニタ，（12 ページ）

netdump サーバのセットアップ

netdump サーバとしてノードを設定するには、次の手順を使用します。

手順

ステップ 1 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。
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。

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 クライアントのセットアップ，（11 ページ）の説明に従って、netdump クライアントを設定します。

netdump クライアントのセットアップ

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

手順

ステップ 1 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。
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。

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` コマンドを実行します。
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 ファイル

netdump サーバからクラッシュ情報を表示するには、リアルタイム モニタリング ツールまたはコマンドライン インターフェイス（CLI）を使用します。 リアルタイム モニタリング ツールを使用して 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。 リアルタイム モニタリング ツールを使用してのファイル収集について詳しくは、『*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 ディレクトリのファイルに対して **file** CLI コマンドを使用します。 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 ステータスのモニタ

リアルタイム モニタリング ツールの SyslogSearchStringFound アラートを設定して、netdump ステータスをモニタできます。 以下の手順を使用して、適切なアラートを設定します。

手順

ステップ 1 リアルタイム モニタリング ツール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。

ステップ 5 [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 と入力し、[追加(Add)] 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 6 [次へ(Next)] をクリックします。

ステップ 7 [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。