CHAPTER 7

Cisco IPICS ログの概要

この章では、Cisco IPICS で使用できるログの概要と、ログに記録された情報を取得して理解する方法について説明します。ログは、Cisco IPICS および PMC に関して発生する問題のトラブルシューティングに役立ちます。

この章は、次の項で構成されています。

Cisco IPICS ログ ファイルの概要と特定

Cisco IPICS ログ ファイルには、Cisco IPICS の使用状況の監査または追跡に使用できる情報が記録されます。また、ログ ファイルは、エラーの根本原因を特定するときに役立ちます。

表 7-1 に、Cisco IPICS ログを示します。

表 7-1　Cisco IPICS のログ ファイル

ログ名	説明
catalina.out	catalina.out ファイルには、Tomcat サービスなど、Cisco IPICS の Web ベースのプロセスに関する情報が記録されます。 catalina.out ファイルは、**/root/tomcat/current/logs** ディレクトリにあります。
Cisco IPICS Activity Log	Cisco IPICS アクティビティ ログには、チャネル、ユーザ、および VTG に関するアクティビティの情報が記録されます。 アクティビティ ログの情報を Microsoft Excel スプレッドシート形式でダウンロードして表示するには、IPICS ユーザとして Administration Console にログインし、**Administration > Activity Log Management > Logs** ウィンドウに移動して、**Download Activity Logs** をクリックします。Cisco IPICS がアクティビティ ログに保存する情報を変更するには、**Administration > Activity Log Options** に移動します。 アクティビティ ログの詳細については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Performing Cisco IPICS System Administrator Tasks」の章を参照してください。
csalog	このファイルには、CSA の起動とシャットダウンの履歴が記録されます。CSA のログ情報は、csalog ファイルと securitylog.txt ファイルに記録されます。 csalog ファイルは、**/var/log** ディレクトリにあります。

表 7-1　Cisco IPICS のログ ファイル（続き）

ログ名	説明
Cisco*nnn*MIVR*nnnn*.log	このログ ファイルには、ポリシー エンジンのコール シグナリングと Session Initiation Protocol（SIP）に関する情報が記録されます。 Cisco IPICS は、最初のファイルに Cisco001MIVR0001.log という名前を付けます。後続のファイルには、Cisco001MIVR0002.log、Cisco001MIVR0003.log というように名前が付けられます。 各 Cisco*nnn*MIVR*nnnn*.log ファイルのサイズ、Cisco IPICS が保持するファイルの総数、および Cisco IPICS がこれらのファイルに記録する情報を設定するには、Administration Console で **Policy Engine > Dial Engine > Control Center > Tracing** に移動し、Trace File Configuration 領域および Trace Settings 領域の情報を変更します。 Cisco001MIVR0001.log ファイルをダウンロードして表示するには、IPICS ユーザとして Administration Console にログインし、**Policy Engine > Dial Engine > Status** ウィンドウに移動して、**SIP Subsystem** または **Policy Engine Subsystem** をクリックします。次に、**Cisco001MIVR0001.log** をクリックします。後続のログ　ファイルをダウンロードして表示するには、SIP subsystem ウィンドウまたは Policy Engine Subsystem ウィンドウに移動し、表示する Cisco*nnn*MIVR*nnnn*.log ファイルをクリックします。 Cisco*nnn*MIVR*nnnn*.log ファイルは、**/opt/cisco/ippe/log/MIVR** ディレクトリにあります。

表 7-1　Cisco IPICS のログ ファイル（続き）

ログ名	説明
Cisco*nnn*MVCD*nnnn*.log	このファイルには、ポリシー エンジンの Cluster View Daemon（CVD; クラスタ ビュー デーモン）コンポーネントのエラーとステータスに関する情報が記録されます。CVD は、ポリシー エンジンのノード マネージャで、Cisco IPICS ダイヤル エンジン サービスの起動プロセスの管理を担当します。 Cisco IPICS は、最初のファイルに Cisco001MVCD0001.log という名前を付けます。後続のファイルには、Cisco001MVCD0002.log、Cisco001MVCD0003.log というように名前が付けられます。 Cisco001MVCD0001.log ファイルをダウンロードして表示するには、IPICS ユーザとして Administration Console にログインし、**Policy Engine > Control Center > Status > Cluster View Daemon** ウィンドウに移動して、**Cisco001MVCD0001.log** をクリックします。後続のログ ファイルをダウンロードして表示するには、SIP subsystem ウィンドウまたは Policy Engine Subsystem ウィンドウに移動し、表示する Cisco*nnn*MVCD*nnnn*.log ファイルをクリックします。 Cisco*nnn*MVCD*nnnn*.log ファイルは、**/opt/cisco/ippe/log/MVCD** ディレクトリにあります。
db-maintenance.log	db-maintenance.log ファイルには、データベースのバックアップ操作および復元操作のレコードが記録されます。 db-maintenance.log ファイルをダウンロードして表示するには、IPICS ユーザとして Administration Console にログインし、**Administration > Database Management > Log** ウィンドウに移動して、**Download** をクリックします。 db-maintenance.log ファイルは、**/opt/cisco/ipics/database/logs** ディレクトリにあります。 db-maintenance.log ファイルの詳細については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Performing Cisco IPICS Database Backup and Restore Operations」の章を参照してください。

表 7-1　Cisco IPICS のログ ファイル（続き）

ログ名	説明
dbm_log_archive.log.gz	このファイルは、以前の db-maintenance.log 日次ログ ファイルからアーカイブされたデータが格納された圧縮ファイルです。 dbm_log_archive.log.gz ファイルをダウンロードして PC に保存するには、**Administration > Database Management > Log** ウィンドウで **Download** ボタンをクリックします。ファイルを PC にダウンロードすると、テキスト ファイルとして表示できます。 dbm_log_archive.log.gz ファイルは、**/opt/cisco/ipics/database/logs** ディレクトリにあります。 このアーカイブ ファイルの詳細については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Performing Cisco IPICS Database Backup and Restore Operations」の章を参照してください。
diagnostics.log	diagnostics.log ファイルには、データベース サブシステムに関連するメッセージが記録されます。このファイルは、**/opt/cisco/ipics/database/logs** ディレクトリにあります。
driverManager*n*.log	driverManager ログには、各コールに関連付けられたメディアのポリシー エンジン固有の情報が記録されます。 driverManager ログに取り込む詳細のレベルを設定するには、Administration Console で **Policy Engine > Control Center > Tracing** ウィンドウに移動し、LIB_MEDIA チェックボックスをオンまたはオフにします。 driverManager ファイルのサイズと総数は、Cisco IPICS によって設定されます。ユーザはこれらの設定を変更できません。 ログ ファイルが設定済みの最大サイズに達すると、Cisco IPICS はそのログ ファイルを閉じ、新しい空のログ ファイルを作成して、新しいログ ファイルの番号を 1 つインクリメントします。 driverManager*n*.log ファイルは、**/opt/cisco/ippe/log/MIVR** ディレクトリにあります。

表 7-1　Cisco IPICS のログ ファイル（続き）

ログ名	説明
install.log	install.log ファイルには、インストールされたパッケージや、インストール中に発生したエラーなど、Cisco IPICS オペレーティング システムのインストールに関する詳細が記録されます。 install.log ファイルは、**/root** ディレクトリにあります。
ipics.log	ipics.log ファイルには、Cisco IPICS サーバで発生するすべてのトランザクションに関するメッセージが記録されます。たとえば、Tomcat サービス、ポリシー エンジンのエントリ、または外部通知に関する情報がこのファイルに記録されます。このログ ファイルに記録される情報は、Cisco IPICS で問題が発生した場合のトラブルシューティングに役立ちます。 各メッセージは、シビラティ レベルでマークされます。また、TRACE から FATAL までの 7 つの重大度が規定されています。デフォルトでは、ipics.log ファイルには、INFO から FATAL レベルまでのロギングがすべて取り込まれます。 最新のシステム ログの表示は、Administration Console の **Serviceability > System Logs** ウィンドウで行うことができます。ipics.log の情報をダウンロードして表示するには、**Serviceability > System Logs** ウィンドウに移動し、**Download** をクリックします。 ipics.log ファイルにアクセスしてダウンロードする方法の詳細については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Understanding Cisco IPICS Serviceability and Diagnostic Information」の章を参照してください。 ipics.log ファイルは、**/root/tomcat/current/logs** ディレクトリにあります。
ipics_audit.log	ipics_audit.log ファイルには、ユーザ アクティビティが記録されます。このアクティビティには、ユーザがサーバへのログイン時に成功および失敗したアクションや、Cisco IPICS ユーザが Administration Console にログインしているときに実行したアクションなどがあります。 ipics_audit.log ファイルは、**/root/tomcat/current/logs** ディレクトリにあります。

表 7-1　Cisco IPICS のログ ファイル（続き）

ログ名	説明
ipics-install-log.txt	ipics-install-log.txt ファイルには、インストールされたパッケージ、作成されたユーザ名、インストール中に発生したエラーなど、Cisco IPICS サーバ ソフトウェアのインストールに関する詳細が記録されます。 install.log ファイルは、**/var/opt/CSCOipics/run/***yyyymmddhhmmss***/ipics-install-log.txt** ディレクトリにあります。 表示の意味は次のとおりです。 *yyyymmddhhmmss* は、サーバ ソフトウェアのインストールを実行した日付と時刻を表します。
ipics_pmc.log	このログ ファイルには、PMC ユーザの情報が収集されます。Cisco IPICS は、PMC ユーザのログイン時とログアウト時、またはユーザによる PMC の更新時にこのログ ファイルを更新します。 ipics_pmc.log ファイルは、**/root/tomcat/current/logs** ディレクトリにあります。 **（注）** ユーザの PMC データを追加で取得するには、PMC からサーバにログ情報をアップロードします。詳細については、P.7-10 の「PMC ログレベルの生成と変更」を参照してください。
ipics_rms.log	ipics_rms.log ファイルには、Cisco IPICS システムに属する RMS コンポーネントのログ データが収集されます。 ipics_rms.log ファイルは、**/root/tomcat/current/logs** ディレクトリにあります。

表 7-1　Cisco IPICS のログ ファイル（続き）

ログ名	説明
lmgrd.log	lmgrd.log ファイルには、Cisco IPICS のライセンスに関する情報と、ライセンスを管理するコンポーネントであるライセンス マネージャに関する情報が記録されます。Cisco IPICS は、ライセンス マネージャが実行するすべてのアクションを lmgrd.log ファイルに記録します。 lmgrd.log ファイルをダウンロードして表示するには、IPICS ユーザとして Administration Console にログインし、**Serviceability > Diagnostics** ウィンドウに移動して、**Download Diagnostic Results** をクリックします。zip 圧縮されたファイルを受信します。このファイルには、lmgrd.log ファイルと ipics.log ファイルのほか、Diagnostics ウィンドウに表示されている情報が含まれています。 lmgrd.log ファイルは、**/opt/cisco/ipics/license/versions/2.1/logs** ディレクトリにあります。
messages	messages ファイルには、次のイベントに関する情報が記録されます。 • CSA 処理に関連するメッセージ • SSH を使用して Cisco IPICS サーバにログインしたユーザ • 停止または起動したプロセス messages ファイルは、**/var/log** ディレクトリにあります。 7 日経過すると、CSA は新しいログを作成し、以前のログに番号の拡張子を付けてリネームします。その結果、ログには **messages.0**、**messages.1**、**messages.2** などの名前が付けられます。
ntpsetup.log	このファイルには、Network Time Protocol（NTP; ネットワーク タイム プロトコル）設定関連の情報が記録されます。 netsetup.log ファイルは、**/var/log** ディレクトリにあります。 **（注）** NTP を設定するには、**ntpsetup** コマンドを入力します。詳細については、P.6-7 の「ntpsetup ツールでの Cisco IPICS サーバの NTP の設定」を参照してください。

表 7-1　Cisco IPICS のログ ファイル（続き）

ログ名	説明
securitylog.txt	このファイルには、ルール違反などのセキュリティ関連のイベントのログが記録されます。このファイルは、CSA がセキュリティ イベントの記録に使用するプライマリ ファイルです。 securitylog.txt ファイルは、**/var/log** ディレクトリにあります。 securitylog.txt ファイルの詳細については、P.7-19 の「CLI コマンドを使用した CSA セキュリティ イベント ログの表示」を参照してください。
tacout	tacout ファイルには、Cisco IPICS の最新の診断情報の要約が記録されます。 tacout ファイルは、**/root/tomcat/current/logs** ディレクトリにあります。 ファイルのダウンロード方法など、tacout ファイルの詳細については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Understanding Cisco IPICS Serviceability and Diagnostic Information」の章を参照してください。

PMC ログレベルの生成と変更

PMC アプリケーションは、ユーザ アクティビティの分析に役立つログや、アプリケーションの使用時に発生する問題のトラブルシューティングに役立つログを生成します。PMC は、ログを PMC クライアント マシンのハードディスクに書き込みます。そのため、サーバへの通信が中断した場合でもアプリケーションはロギングを続行できます。

Cisco IPICS は、次のどちらかの条件が満たされた場合に、PMC からログを取得します。

- **User Management > Users >** *Username* **> PMC** タブで、**Get Logs from PMC** をクリックした場合

（注） サーバにおいて PMC ユーザからのログをアップロードできないようにするには、PMC アプリケーションで **Settings > Channels** に移動し、**Optimize for low bandwidth** チェックボックスをオンにします。PMC を低帯域幅で高遅延のネットワーク環境で使用している場合は、このボックスをオンにする必要があります。オンにしても、PMC は引き続きログを PMC クライアント マシンのハード ドライブに生成します。

- PMC ユーザがセッションのログインおよびログアウトを実行したときに自動的にログが Cisco IPICS サーバにアップロードされるように設定されている場合（このイベントはロールオーバーと呼ばれます）

  ロールオーバーの対象は Authentication、Channel Statistics、および User Interface ログで、Debug Log は対象ではありません。Debug Log の場合は、サーバがファイルのアップロードを要求するまで、ファイルにデータが継続的に蓄積されます。ロールオーバーの発生の詳細については、『*Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*』の「Using the PMC Application Logs」の章を参照してください。

ユーザは次の方法で PMC ログを変更できます。

- PMC ユーザが PMC アプリケーション内で設定を調整する。PMC アプリケーションで設定を調整する方法の詳細については、『*Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*』の「Using the PMC Application Logs」の章を参照してください。

- Cisco IPICS オペレータが Administration Console の **User Management > Users >** *Username* **> PMC** タブで、ログ設定を変更する。ログ設定の設定および変更方法の詳細については、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Performing Cisco IPICS Operator Tasks」の章を参照してください。

ログ ファイルのリストと説明については、『*Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*』の「Using the PMC Application Logs」の章を参照してください。

PMC ユーザのアクティビティ ログのダウンロードは、Administration Console の **Administration > Activity Log Management > Logs** タブで行うことができます。ダウンロードする情報には、チャネルと VTG に対するユーザの関連付け、チャネルのアクティブ化に関するアクティビティ、および会議への参加についての詳細が含まれています。**Administration > Activity Log Options** ウィンドウで、PMC 情報を取り込むようにアクティビティ ログを設定します。アクティビティ ログについては、『*Cisco IPICS Server Administration Guide, Release 2.1(1)*』の「Performing Cisco IPICS System Administrator Tasks」の章を参照してください。

この項では、次のトピックを扱います。

PMC Debug Log の情報の概要

Cisco IPICS の DebugLog.txt のデータ フィールドは、User Interface、Signaling、および Media の 3 つのカテゴリに分かれています。これらのデータ フィールドは、さらに 3 つのログレベルに分かれています。そのため、必要なデバッグ情報をより正確に取り込むことができます。Debug Log の各カテゴリには、次の情報が含まれます。

- User Interface：このカテゴリのフィールドは、PMC のユーザ インターフェイスの機能に関する情報を提供します。このカテゴリには、ボタンやボリューム コントロールなど、PMC アプリケーションに表示できる項目がすべて含まれています。また、User Interface カテゴリには、Cisco IPICS サーバに関する通信の問題をデバッグするための情報も含まれています。

  表 7-2 は、Cisco IPICS が収集する情報をログレベル別に説明しています。

表 7-2　User Interface のログレベル

ログ レベル	目的
Low	Cisco IPICS は、このログレベルでは、次の問題に関する情報を取得します。 • ユーザがログインできない • ユーザがチャネルをアクティブにするときに問題が発生する • ユーザが PMC を終了できない • PMC が不意にオフライン モードに移行する • サーバがエラーを報告する
Medium	Cisco IPICS は、サーバからの XML 通信を解釈するときに役立つ情報を報告します。
High	Cisco IPICS は、認証、GUI、および PMC サーバの更新機能に関する情報を収集します。

- Signaling : Signaling カテゴリには、音声チャネルの起動と停止に関する情報を提供するフィールドが含まれています。ユーザが PMC チャネルをアクティブまたは非アクティブにできない場合は、Signaling をオンにします。

  表 7-3 は、Cisco IPICS が Signaling のログレベルに従って報告する情報を説明しています。

表 7-3　Signaling のログレベル

ログ レベル	目的
Low および Medium	これらのログレベルのメッセージは、高レベルのステート マシンに関する問題を報告します。
High	このレベルのメッセージは、SIP メッセージングに関する問題を報告します。

- Media：このカテゴリのフィールドには、パケットや、エンドポイント間のデータを処理するコーデックなど、音声ストリームに関連する項目が含まれています。音声品質の問題を診断するには、Media 情報を使用します。

表 7-4 は、Media のログレベルに従って収集できる情報のタイプを説明しています。

表 7-4　Media のログレベル

ログ レベル	目的
Low	この情報には、受信（RX）および伝送（TX）ネットワーキング統計情報が含まれます。
Medium	この情報は、チャネルまたは VTG でオーディオ信号が混合する問題など、オーディオ混合の問題を診断するときに役立ちます。
High	この情報には、オーディオ コーデックを使用したオーディオ変換に関する情報が含まれます。

デバッグ ログレベルの使用方法

PMC ユーザのデバッグ情報のロギングを開始する場合は、情報カテゴリを 1 つ以上選択します。各カテゴリには、デバッグ フィールドのリストが含まれています。ログに取り込むフィールドに対応したカテゴリおよびログレベルを選択します。

表 7-5 は、各ログレベルに含まれるフィールドを示しています。

各カテゴリのログレベルは、累積型になっています。特定のカテゴリで Medium レベルを選択した場合、PMC は Low レベルと Medium レベルのログを DebugLog.txt ファイルに書き込みます。ロギングを High に設定した場合は、そのカテゴリのフィールドがすべて取り込まれます。

ヒント　デバッグを開始するときは、必ず、Low レベルのログ データを収集するようにしてください。Low レベルでも、必要なデータがすべて得られる場合があります。この設定を使用すると、数日間のログ アクティビティを収集しても、PMC クライアント マシンのハードディスクが満杯になることはありません。問題の原因を特定できなければ、次はロギングを Medium または High に設定します。

High レベルの使用は、短期間に限定してください。High レベルを使用する場合は、ユーザの PMC クライアント マシンのハード ドライブを注意深く監視して、

High レベルのログによってクライアントのハード ドライブが満杯になったり、PMC のパフォーマンスが低下したりすることがないようにする必要があります。

注意　すべてのデバッグ オプションを設定すると、システムで収集および生成される情報量が膨大になるため、デバッグ ロギングは、特定の問題を切り分ける場合に限って使用することをお勧めします。デバッグ作業が完了したら、必ず、デバッグ ログをクリアしてデバッグ ロギングをオフにしてください。

表 7-5 に、デバッグ カテゴリと、各カテゴリに関連付けられたフィールドおよびログレベルを示します。

表 7-5　Debug Log のフィールドとログレベル

カテゴリ	フィールド	ログレベル
User Interface	channel-activation-debug	Low
	error	
	exit-debug	
	sending-source-debug	
	sock-init-cleanup	
	xml-events	Medium
	xml-post	
	xml-vars	
	Auth	High
	critical-section-tune-debug	
	download-debug	
	gui-debug	
	server-task-debug	
	server-verbose	
	xml-deck	

表 7-5　Debug Log のフィールドとログレベル（続き）

カテゴリ	フィールド	ログレベル
Signaling	cc	Low
	fim	
	fsm	
	gsm	
	lsm	
	multicast-signaling-debug	
	sip-reg-state	
	sip-state	
	vcm	
	sip-task	Medium
	sip-trx	
	Auth	High
	cc-msg	
	sip-messages	

表 7-5　Debug Log のフィールドとログレベル（続き）

カテゴリ	フィールド	ログレベル
Media	AMuteTrans	Low
	AudioSink	
	AudioSource	
	MediaStream	
	OpenALAudioSink	
	RTPAudioSink	
	RTPAudioSockets	
	RTPAudioSource	
	RTPAudioStream	
	RTPJitterBuf	
	sock-init-Cleanup	
	WaveAudioSource	
	WaveFileSource	
	RxStats	
	TxStats	
Media	ACMTrans	Medium
	ASL	
	AudioBufferAndPlayback	
	dsp	
	FilePlay	
	PCMMixer	
	PCMVolTrans	
	PCMVolumeMax	
	RTPAudioStreamMgr	
	RxDetailStats	
	VAD	

表 7-5　Debug Log のフィールドとログレベル（続き）

カテゴリ	フィールド	ログレベル
Media	AudioDump	High
	AudioSamp	
	AudioSampLost	
	AudioSampMgr	
	AudioTrans	
	AutomaticGainControl	
	dtmf	
	FIRTrans	
	FSAudioBuf	
	G7112PCMTrans	
	G7232PCMTrans	
	G729A2PCMTrans	
	Limiter	
	PCM2G711Trans	
	PCM2G723Trans	
	PCM2G729ATrans	
	RTCPPacket	
	TimeSample	
	TimeRxSample	
	TimeTxSample	

CSA ログの確認

CSA がシステム アクションを拒否した場合、プロセスによってメッセージが生成されます。このメッセージには、次のいずれかの方法でアクセスできます。

- CSA Utility を開き、Message ペインにメッセージを表示する。
- セキュリティ イベント ログを表示する。このログには、システムで発生したセキュリティ イベントがすべて記録されています。
- **/var/log** ディレクトリに移動し、現在の CSA ログとアーカイブされた CSA ログを表示する。

この項では、次のトピックを扱います。

CSA Utility での CSA メッセージの表示

CSA Utility でステータス メッセージを表示するには、次の手順を実行します。

手順

ステップ 1　CSA トレイ アイコン（赤色の旗）をダブルクリックして、CSA Utility を開きます。

CSA Utility が表示されます。

ステップ 2　セキュリティ ログにアクセスするには、**Messages** をクリックします。

Messages ペインにステータス メッセージが表示されます。

ステップ 3　CSA ログにアクセスするには、**View Log** をクリックします。

現在のセキュリティ イベント ログが、テキスト ビューア ウィンドウに表示されます。

CLI コマンドを使用した CSA セキュリティ イベント ログの表示

Cisco IPICS サーバの **/var/log** ディレクトリには、現在の CSA ログとアーカイブされた CSA ログが含まれています。

セキュリティ イベントが記録されるログのファイル名は **securitylog.txt** です。securitylog.txt ファイルのサイズが 100 MB に達すると、CSA は新しいログを作成し、以前のログ ファイルをアーカイブして名前変更します。アーカイブされたログ ファイルには、**securitylog-***yyyymmdd-hhmm***.txt** という名前が付けられます。

表示の意味は次のとおりです。

yyyymmdd-hhmm は、CSA がログ ファイルをアーカイブした日付です。

CLI コマンドを使用して securitylog.txt ファイルを表示するには、次の手順を実行します。

手順

ステップ 1　ルート ユーザ ID を使用して Cisco IPICS サーバにログインします。

ステップ 2　**/var/log** ディレクトリに移動するには、次のコマンドを入力します。

[root] #**cd /var/log**

ステップ 3　ディレクトリ内のセキュリティ イベント ログ ファイルを表示するには、次のコマンドを入力します。

[root] #**ls -al securitylog***

名前が securitylog で始まるファイルが表示されます。

ステップ 4　ログ ファイルの内容を表示するには、次のコマンドを入力します。

[root] #**cat securitylog**[**-***yyyymmdd-hhmm*]**.txt**

表示の意味は次のとおりです。

yyyymmdd-hhmm は、アーカイブされたログ ファイルの日付です。

CSA ログに表示されるメッセージについては、次の URL で CSA のマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html