Cisco Unified MeetingPlace SNMP

この付録では、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップと、SNMP トラップでサポートされる Cisco Unified MeetingPlace 例外について説明します。

次の項を参照してください。

Cisco Unified MeetingPlace SNMP について

Cisco Unified MeetingPlace SNMP 機能を使用すると、ネットワーク上の他のデバイスの管理と同じ方法で Cisco Unified MeetingPlace を監視できます。SNMP 管理ツールを使用し、適切に設定することによって、ネットワーク ステータス情報を取得し、システムにアクセスできます。

SNMP 機能は、すべての標準「MIB II」クエリと Cisco Unified MeetingPlace MIB トラップのセットをサポートします。MIB II クエリには、Cisco Unified MeetingPlace のサーバ名、場所、連絡先名などの情報と、ネットワーク インターフェイスに関するさまざまな統計情報が含まれます。

表 D-1 で、Cisco Unified MeetingPlace MIB トラップが生成される条件を説明します。

表 D-1　Cisco Unified MeetingPlace SNMP

アラーム	生成される条件
T1 ステータス	T1 回線がダウンしたとき。
Gateway System Integrity Manager（SIM）	Gateway SIM がアラームを登録したとき。
サーバ起動	サーバが再起動またはクラッシュ（コールド スタート）したとき。
メジャー ハードウェア アラーム	メジャー ハードウェア障害が発生したとき。
メジャー ソフトウェア アラーム	メジャー ソフトウェア障害が発生したとき。
マイナー ハードウェア アラーム	マイナー ハードウェア障害が発生したとき。
マイナー ソフトウェア アラーム	マイナー ソフトウェア障害が発生したとき。

各メジャーおよびマイナーのハードウェアやソフトウェアの通知には、アラームをレポートしたソフトウェア モジュールおよびサーバを示す整数のアラーム コードが含まれます。ハードウェア アラームの場合、4 つの追加コードによって、デバイス タイプ、デバイス、アドレス、スロット番号、およびポート番号が識別されます。これらのフィールドは、MIB で定義されます。

lattraps.mib という MIB ファイル（SNMP バージョン 1 形式）には、すべての MIB アラームが含まれています。この MIB ファイルを監視システムにロードし、トラップ メッセージを正しく表示できるように設定する必要があります。lattraps.mib をダウンロードするには、http://www.cisco.com/cgi-bin/tablebuild.pl/meetingplace-serv にアクセスします。

メジャー アラームとマイナー アラームのリストについては、http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_tech_notes_list.html にある『*MeetingPlace Server Alarm Reference*』マニュアルを参照してください。

次の点に留意してください。

- 通常、各アラーム インスタンスは、別々の通知を生成します。ただし、1 つの特定のインシデントが、複数の種類のアラームをトリガーすることもあります。
- *MeetingPlaceConfs* MIB は、将来の使用のために予約されています。この MIB はクエリに応答しますが、Cisco Unified MeetingPlace サーバの会議に関する情報を含んでいません。

連絡先および場所の情報の設定

Cisco Unified MeetingPlace SNMP オプションをインストールすると、特別な設定情報なしで Cisco Unified MeetingPlace サーバを任意の SNMP 管理ステーションから参照できます。ただし、SNMP モジュールへのアクセスを制御し、SNMP データ交換を設定するには、システム管理者が Configure タブの Network Management Information トピックと Network Management Communities トピックに情報を入力する必要があります。

Network Management Information は、SNMP モジュールへの高レベル アクセスを制御し、Cisco Unified MeetingPlace がネットワーク上の他のデバイスと SNMP データを交換できるようにします。Cisco Unified MeetingPlace システムに関する問題について SNMP システム管理者が適切な担当者に連絡できるように、System contact フィールドと System location フィールドにデータを入力してください。

ヒント　Cisco Unified MeetingPlace システムの連絡先と場所は、SNMP 管理ステーションから設定することもできます。

連絡先および場所の情報を設定する

ステップ 1　MeetingTime で、**Configure** タブを選択します。

ステップ 2　**Network Management Info** トピックを選択し、次のパラメータを設定します。

パラメータ	設定
IP Port Number	Cisco Unified MeetingPlace が、着信 SNMP メッセージを検索できるポート。通常、ポート 161 を使用します。
System Contact	Cisco Unified MeetingPlace システム管理者の名前。
System Location	Cisco Unified MeetingPlace システムの物理的な場所。
Disable SNMP Queries	すべての SNMP クエリをオフにできます。

コミュニティ情報の設定

Configure タブの Network Management Communities トピックを使用して、Cisco Unified MeetingPlace への SNMP 経由のアクセスを制御する SNMP コミュニティを定義できます。また、Network Management Communities トピックは、SNMP モジュールから利用できるネットワーク情報を表示します。

次の 2 種類のネットワーク管理コミュニティを設定できます。

- トラップ コミュニティ : Cisco Unified MeetingPlace による標準 MIB II トラップの送信先ホストを定義します。
- 非トラップ コミュニティ : SNMP メッセージへの応答で提供されるアクセスの種類を制御します（読み取りと書き込み、読み取り専用、アクセス不可）。

問題がある場合は、ホスティング管理者に連絡してください。

注意　SNMP エージェントは、トラップ コミュニティでクエリを受け付けません。そのため、たとえばパブリック コミュニティを使用するクエリを作成する場合は、*public* をトラップ コミュニティに指定しないでください。

コミュニティ情報を設定する

ステップ 1　MeetingTime で、**Configure** タブを選択します。

ステップ 2　**Network Mgmt Info** トピックを選択します。

次の属性を設定します（この手順で説明します）。

属性	設定
Name	ネットワーク管理コミュニティの名前。標準の「パブリック」および「プライベート」のコミュニティが事前定義されています。これらは、*MeetingPlace-public* および *MeetingPlace-private* と呼ばれます。これらの値を使用することも、独自の値に置き換えることもできます。
IP Address	トラップ コミュニティへのトラップを送信する先の IP アドレス。このパラメータは、非トラップ コミュニティでは無視されます。
Read-Write	*Yes* に設定した場合、このコミュニティの SNMP メッセージは格納されている SNMP データを変更できます（トラップ コミュニティでは無視されます）。通常、管理者は、パブリック コミュニティでは読み取り専用を選択し、プライベート コミュニティには読み取りと書き込みアクセスを使用します。
Is It a Trap	SNMP エージェントは、「トラップ」を通じて予防的に管理者に通知できます（「I am restarting」など）。SNMP モジュールは、システムが再起動したとき、ネットワーク リンクの状態が変わったとき、認証に失敗した SNMP メッセージを受信したときに、トラップをアクティブにできます。

ステップ 3　次の表で示すように、プライベート コミュニティを削除し、パブリック コミュニティとトラップ コミュニティの名前を変更します。

作業内容	操作
プライベート コミュニティの削除	**Query** ボタンをクリックしてから **<** または **>** ボタンをクリックし、プライベート コミュニティを検索します。**Delete** をクリックし、**Save Changes** をクリックします。
パブリック コミュニティの名前の変更	**Query** ボタンをクリックしてから **<** または **>** ボタンをクリックし、パブリック コミュニティを検索します。次の名前を示されているとおりに正確に入力します（大文字と小文字は区別されます）。 **rwcHP1** 次に、**Save Changes** をクリックします。 **（注）** この値は、すべてのサーバで同じで、変わりません。
トラップ コミュニティの名前の変更	IP アドレスを現在のサーバの値に設定します。次に、**Save Changes** をクリックします。

ステップ 4　Cisco Unified MeetingPlace 8106 または 8112 を再起動して、これらの変更を有効にします。

トラップがトラップ コードと共に、SNMP 管理ツールにイベントとして表示されます。ほとんどの SNMP 管理ツールで、イベント メッセージとアラームの重大度の両方を設定できます。したがって、システム管理者が簡単に発見し、理解できるように、T1 および Gateway SIM のトラップを設定することをお勧めします。一般的なコードのリストについては、P.D-5 の「SNMP トラップについて」を参照してください。

SNMP トラップについて

次の表で、Cisco Unified MeetingPlace SNMP サービスがサポートする SNMP トラップを説明します。

Cisco Unified MeetingPlace サーバがアラーム条件を生成すると、アラーム条件はハードウェアまたはソフトウェア、メジャーまたはマイナーに分類されます。次に、そのアラームに適したトラップが生成されます。このトラップには、ペイロードとして、実際のアラーム コードなどの追加情報が含まれます。

メジャーおよびマイナーのハードウェアやソフトウェアのトラップの形式については、http://www.cisco.com/cgi-bin/tablebuild.pl/meetingplace-serv にある *lattraps.mib* を参照してください。

これらのトラップは T1 または GWSIM トラップのほかに生成されるため、結果として同じ条件から複数のトラップが生成されることがあります。

（注）　*MeetingPlaceConfs* MIB は、将来の使用のために予約されています。この MIB はクエリに応答しますが、Cisco Unified MeetingPlace サーバの会議に関する情報を含んでいません。

表 D-2 で、各トラップ タイプとその値について説明します。

表 D-2　SNMP トラップ

トラップ タイプ	トラップの値	説明
coldStart	SNMP_TRAP_COLDSTART (0) OID=1.3.6.1.6.3.1.1.5, trap type 0	すべてのデバイスの汎用トラップ。送信側のプロトコル エンティティが再初期化され、エージェントの設定またはプロトコル エンティティの実装が変更された可能性があることを示します。 通常、会議サーバを再起動したときに発生します。
T1	OID-1.3.6.1.4.1.7185.3.1.3.0, trap type 1	送信側のプロトコル エンティティが、イベントの発生を認識したことを示します。 このトラップの値は、Gateway 例外（P.D-6 の「SNMP トラップがサポートする Cisco Unified MeetingPlace 例外」を参照）が Cisco Unified MeetingPlace システムから検出されたことを示します。このトラップを受信した場合は、例外ログをチェックし、何が発生したかを調べてください。
Major hardware	OID=1.3.6.1.4.1.7185.3.1.3.0, trap type 3	詳細については *lattraps.mib* を参照してください。
Minor hardware	OID=1.3.6.1.4.1.7185.3.1.3.0, trap type 4	詳細については *lattraps.mib* を参照してください。
Major software	OID=1.3.6.1.4.1.7185.3.1.3.0, trap type 5	詳細については *lattraps.mib* を参照してください。
Minor software	OID=1.3.6.1.4.1.7185.3.1.3.0, trap type 6	詳細については *lattraps.mib* を参照してください。

SNMP トラップがサポートする Cisco Unified MeetingPlace 例外

次の例外が Cisco Unified MeetingPlace Gateway SIM から生成され、SNMP サーバで受信されます。次に、SNMP サーバはトラップを SNMP クライアントに送信します。例外は、代替ログ ファイル *cm_alt.log* で説明されます。

表 D-3 で、各例外コードとその値について説明します。

表 D-3　SNMP トラップがサポートする例外

例外コード	数値	イベントの説明
EX_SPAN_RED_ALARM	EX_TV_BASE+120 （Ex_TV_BASE　0xB000）	Red Alarm detected on this T1 span ([%d], card %d, [%d], span %d)
EX_MPDATASVC_STATUSNOTRESP	EX_GWERR_BASE+258 （EX_GWERR_BASE 0x120000）	WebPub Data Service (Unit %d) Not Responding
EX_MPAGENT_STATUSNOTRESP	EX_GWERR_BASE+322	WebPub Agent (Unit %d) Not Responding
EX_MPAUDIO_STATUSNOTRESP	EX_GWERR_BASE+386	WebPub Audio Service (Unit %d) Not Responding
EX_SMTP_STATUSNOTRESP	EX_GWERR_BASE+514	SMTP Gateway (Unit %d) Not Responding
EX_OUTLOOK_STATUSNOTRESP	EX_GWERR_BASE+1026	Outlook Gateway (Unit %d) Not Responding
EX_NOTES_STATUSNOTRESP	EX_GWERR_BASE+1282	Notes Gateway (Unit %d) Not Responding
EX_MPNOTIFY_STATUSNOTRESP	EX_GWERR_BASE+1346	MPNotify Service (Unit %d) Not Responding
EX_DATACONF_STATUSNOTRESP	EX_GWERR_BASE+1538	DataConf Gateway (Unit %d) Not Responding
EX_DATACONFGCC_STATUSNOTRESP	EX_GWERR_BASE+1602	DataConf GCC Service (Unit %d) Not Responding
EX_DATACONFMCS_STATUSNOTRESP	EX_GWERR_BASE+1666	DataConf MCS Service (Unit %d) Not Responding
EX_DATACONFSAMETIME_STATUSNOTRESP	EX_GWERR_BASE+1730	DataConf Sametime Service (Unit %d) Not Responding
EX_VOIPMPSTREAM_STATUSNOTRESP	EX_GWERR_BASE+1858	VoIP MPStream Service (Unit %d) Not Responding
EX_DCDIR_STATUSNOTRESP	EX_GWERR_BASE+2050	MP Directory Service (Unit %d) Not Responding
EX_GWSIMAGENT_STATUSNOTRESP	EX_GWERR_BASE+3842	Gateway SIM Agent (Unit %d) Not Responding
EX_UNITFAULT	EX_SI_BASE+129	Communication lost with unit %d アクティブ ユニットがダウンしていました。
EX_CRASH	EX_SI_BASE+73	System crashed: power fail, reset, or watchdog timer これは Gateway SIM 関連の例外ではありません。サーバがクラッシュし、リブートした後、クラッシュしたことを認識すると発生します。