簡易ネットワーク管理プロトコル

- 簡易ネットワーク管理プロトコル（SNMP）のサポート （1 ページ）
- SNMP 設定タスク フロー （27 ページ）
- SNMP トラップの設定 （45 ページ）
- SNMP トレースの設定 （48 ページ）
- SNMP のトラブルシューティング （49 ページ）

簡易ネットワーク管理プロトコル（SNMP）のサポート

アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

Serviceability GUI を使用して、V1、V2c、および V3 のコミュニティ ストリング、ユーザ、通知先など、SNMP 関連の設定を行います。ユーザが設定した SNMP 設定は、ローカル ノードに適用されます。ただし、システム構成でクラスタをサポートしている場合、SNMP の設定ウィンドウで、[すべてのノードに適用（Apply to All Nodes）]「」オプションを使用して、クラスタ内のすべてのサーバに設定を適用することもできます。

ヒント　Unified Communications Manager のみ：Cisco Unified CallManager または Unified Communications Manager 4.X で指定した SNMP 設定パラメータは、Unified Communications Manager 6.0 以降のアップグレード時に移行されません。Cisco Unified Serviceability で SNMP 設定手順を繰り返す必要があります。

SNMP は IPv4 と IPv6 をサポートし、CISCO-CCM-MIB には IPv4 と IPv6 の両方のアドレスやプリファレンスなどの列とストレージが含まれています。

SNMP の基礎

SNMP 管理のネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという 3 つの主要コンポーネントで構成されています。

- 管理対象デバイス：SNMP エージェントを含み、管理対象ネットワークに存在するネットワーク ノード。管理対象デバイスには管理情報が収集および格納され、その情報は SNMP を使用することによって利用可能になります。

  Unified Communications Manager および IM and Presence Service のみ：クラスタをサポートする設定では、クラスタ内の最初のノードが管理対象デバイスとして機能します。

- エージェント：管理対象デバイスに存在するネットワーク管理対象ソフトウェア モジュール。エージェントには、管理情報のローカルな知識が蓄積され、SNMP と互換性のある形式に変換されます。

  SNMP をサポートするため、マスターエージェントとサブエージェントのコンポーネントが使用されます。マスター エージェントはエージェント プロトコル エンジンとして機能し、SNMP 要求に関連する認証、許可、アクセス コントロール、およびプライバシーの機能を実行します。同様に、マスター エージェントには、MIB-II に関係するいくつかの管理情報ベース（MIB）変数が含まれています。また、マスターエージェントは、サブエージェントへの接続も行います。サブエージェントでの必要なタスクが完了すると、その接続を解除します。SNMP マスターエージェントはポート 161 で待ち受けし、ベンダー MIB の SNMP パケットを転送します。

  Unified Communications Manager サブ エージェントは、ローカルの Unified Communications Manager のみと通信します。Unified Communications Manager サブエージェントは SNMP マスター エージェントにトラップと情報メッセージを送信し、SNMP マスター エージェントは SNMP トラップ レシーバ（通知の宛先）と通信します。

  IM and Presence Service サブエージェントは、ローカルの IM and Presence Service とのみ対話します。IM and Presence Service サブエージェントは SNMP マスター エージェントにトラップと情報メッセージを送信し、SNMP マスターエージェントは SNMP トラップ レシーバ（通知の宛先）と通信します。

- ネットワーク管理システム（NMS）：SNMP 管理アプリケーション（および動作する PC）。ネットワーク管理に必要な処理リソースとメモリ リソースのほとんどを提供します。NMS では、管理対象デバイスをモニタおよび制御するアプリケーションが実行されます。次の NMS がサポートされます。

  - CiscoWorks LAN Management Solution
  - HP OpenView
  - SNMP および Unified Communications Manager SNMP インターフェイスをサポートするサードパーティ製アプリケーション

SNMP 管理情報ベース

SNMP では、階層的に編成された情報のコレクションである管理情報ベース（MIB）にアクセスできます。MIB は、オブジェクト ID で識別される管理対象オブジェクトで構成されます。MIB オブジェクトには、管理対象デバイスの特定の特性が格納され、1 つ以上のオブジェクトインスタンス（変数）で構成されます。

SNMP インターフェイスでは、次のシスコ標準 MIB が提供されます。

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

次の制限事項があります。

- Unified Communications Manager は、CISCO-UNITY-MIB をサポートしていません。
- Cisco Unity Connection では CISCO-CCM-MIB はサポートされません。
- IM and Presence Service では CISCO-CCM-MIB および CISCO-UNITY-MIB はサポートされません。

SNMP 拡張エージェントはサーバに常駐し、サーバが認識しているデバイスに関する詳細情報を提供する CISCO-CCM-MIB を公開します。クラスタ構成の場合、SNMP 拡張エージェントはクラスタ内の各サーバに常駐します。CISCO-CCM-MIB は、サーバ（クラスタでなく、クラスタをサポートする構成内のサーバ）にデバイスの登録状態、IP アドレス、説明、およびモデルタイプなどのデバイス情報を提供します。

SNMP インターフェイスでは、次の業界標準 MIB も提供されます。

- SYSAPPL-MIB
- MIB-II（RFC 1213）
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

Cisco Discovery Protocol MIB（CISCO-CDP-MIB）を読み取るには、CDP サブエージェントを使用します。この MIB を使用すると、SNMP 管理対象デバイスが自身をネットワーク上の他のシスコ デバイスにアドバタイズできるようになります。

CDP サブエージェントは CDP-MIB を実装します。CDP-MIB には、次のオブジェクトが含まれています。

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable

- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

（注） CISCO-CDP-MIB は、次の MIB の存在に依存しています。CISCO-SMI、CISCO-TC、CISCO-VTP-MIB。

SYSAPPL-MIB

インストールされているアプリケーション、アプリケーションコンポーネント、システム動作しているプロセスなど、SYSAPPL-MIB から情報を取得するには、System Application Agent を使用します。

System Application Agent は、SYSAPPL-MIB の次のオブジェクト グループをサポートしています。

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

表 *1 : SYSAPPL-MIB* のコマンド

コマンド	Description
デバイスに関連するクエリー	
sysApplInstallPkgVersion	ソフトウェアの製造元によってアプリケーション パッケージに割り当てられたバージョン番号を提供します。
sysApplElmPastRunUser	プロセス所有者のログイン名（root など）を提供します。

メモリ、ストレージ、CPU に関連するクエリー	
sysApplElmPastRunMemory	このプロセスが終了するまでに割り当てられた実システム メモリの合計（KB 単位）の最新の既知の値を提供します。
sysApplElmtPastRunCPU	このプロセスによって消費されたシステム CPU リソースの合計（1/100 秒単位）の最新の既知の値を提供します。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。
sysApplInstallElmtCurSizeLow	現在のファイル サイズ（modulo 2^32 バイト）を提供します。たとえば、合計サイズが 4,294,967,296 バイトのファイルの場合、この値は、0 になり、合計サイズが 4,294,967,295 バイトのファイルの場合、この値は、4,294,967,295 になります。
sysApplInstallElmtSizeLow	インストールされたファイル サイズ（modulo 2^32 バイト）を提供します。これは、インストール直後のディスク上のファイル サイズです。たとえば、合計サイズが 4,294,967,296 バイトのファイルの場合、この値は、0 になり、合計サイズが 4,294,967,295 バイトのファイルの場合、この値は、4,294,967,295 になります。
sysApplElmRunMemory	このプロセスに現在割り当てられている実システム メモリの合計値（KB 単位）を提供します。
sysApplElmRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値（1/100 秒単位）を提供します。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。

プロセスに関連するクエリー	
sysApplElmtRunState	実行中のプロセスの現在の状態を提供します。値は次のとおりです。実行中 (1)、 実行可能 (2)、実行可能であるが、CPU などのリソースを待機中 (3)、終了 (4)、その他 (5)。
sysApplElmtRunNumFiles	プロセスによって現在開かれている通常ファイルの数を提供します。この値の計算には、転送接続（ソケット）や、オペレーティング システム固有の特殊なファイル タイプは含まれません。
sysApplElmtRunTimeStarted	プロセスが開始された時刻を提供します。
sysApplElmtRunMemory	このプロセスに現在割り当てられている実システム メモリの合計値（KB 単位）を提供します。
sysApplElmtPastRunInstallID	インストール済み要素テーブルのインデックスを提供します。このオブジェクトの値は、このエントリが以前実行されたプロセスを表しているアプリケーション要素の sysApplInstallElmtIndex の値と同じです。
sysApplElmtPastRunUser	プロセス所有者のログイン名（root など）を提供します。
sysApplElmtPastRunTimeEnded	プロセスが終了した時刻を提供します。
sysApplElmtRunUser	プロセス所有者のログイン名（root など）を提供します。
sysApplRunStarted	アプリケーションが起動された日時を提供します。
sysApplElmtRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値（1/100 秒単位）を提供します。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。

ソフトウェア コンポーネントに関連するクエリー	
sysApplInstallPkgProductName	製造元によってソフトウェア アプリケーション パッケージに割り当てられた名前を提供します。
sysApplElmtRunParameters	プロセスの起動パラメータを提供します。
sysApplElmtRunName	プロセスのフル パスとファイル名を提供します。たとえば、実行パスが「opt/MYYpkg/bin/myyproc」のプロセス「myyproc」の場合は「/opt/MYYpkg/bin/myyproc」が返されます。
sysApplInstallElmtName	アプリケーションに含まれるこの要素の名前を提供します。
sysApplElmtRunUser	プロセス所有者のログイン名（root など）を提供します。
sysApplInstallElmtPath	この要素がインストールされているディレクトリのフル パスを提供します。たとえば、「/opt/EMPuma/bin」ディレクトリにインストールされている要素の場合、値は「/opt/EMPuma/bin」になります。ほとんどのアプリケーション パッケージには、パッケージ内の要素に関する情報が含まれています。また、要素は通常、パッケージのインストールディレクトリのサブディレクトリにインストールされます。パッケージの情報自体に要素のパス名が含まれていない場合、通常はサブディレクトリの簡易検索でパスを特定することができます。要素がその場所にインストールされておらず、エージェント実装のために別の情報も参照できない場合には、パスは不明となり、null が返されます。

sysApplMapInstallPkgIndex	このオブジェクトの値を提供し、このプロセスが含まれているアプリケーションのインストール済みソフトウェア パッケージを特定します。プロセスの親アプリケーションを特定できる場合、このオブジェクトの値は、このプロセスが含まれているインストール済みアプリケーションに対応する sysApplInstallPkgTable のエントリの sysApplInstallPkgIndex と同じになります。ただし、親アプリケーションを特定できない場合には（プロセスが特定のインストール済みアプリケーションに含まれない場合など）、このオブジェクトの値は「0」になります。これは、このプロセスをアプリケーションやインストール済みソフトウェアパッケージと関連付けることができないことを示します。
sysApplElmtRunInstallID	sysApplInstallElmtTable のインデックスを提供します。The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a running instance. このプロセスが、インストール済みの実行可能ファイルと関連付けられない場合、値は「0」になります。

sysApplRunCurrentState	実行中のアプリケーション インスタンスの現在の状態を提供します。値は次のとおりです。実行中 (1)、 実行可能 (2)、実行可能であるが、CPU などのリソースを待機中 (3)、終了 (4)、その他 (5)。この値は、このアプリケーション インスタンスの実行要素の評価（sysApplElmRunState を参照）および sysApplInstallElmtRole で定義されたロールに基づきます。エージェント実装は、その REQUIRED 要素の 1 つ以上がもはや実行されない場合アプリケーション インスタンスが終了のプロセスにある事を検出する可能性があります。エージェント実装のほとんどは、システム時刻を提供して REQUIRED 要素を開始するために、2 番目の内部ポーリングが完了するまで待機してからアプリケーション インスタンスを終了としてマークします。
sysApplInstallPkgDate	このソフトウェア アプリケーションがホストにインストールされた日時を提供します。
sysApplInstallPkgVersion	ソフトウェアの製造元によってアプリケーション パッケージに割り当てられたバージョン番号を提供します。
sysApplInstallElmtType	インストール済みアプリケーションに含まれている要素のタイプを提供します。
日付または時刻に関連するクエリー	
sysApplElmtRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値（1/100 秒単位）です。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。
sysApplInstallPkgDate	このソフトウェア アプリケーションがホストにインストールされた日時を提供します。

sysApplElmtPastRunTimeEnded	プロセスが終了した時刻を提供します。
sysApplRunStarted	アプリケーションが起動された日時を提供します。

MIB-II

MIB-II から情報を取得するには、MIB2 エージェントを使用します。MIB2 エージェントは、インターフェイスや IP など、RFC 1213 で定義されている変数へのアクセスを提供し、次のオブジェクト グループをサポートしています。

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

表 *2 : MIB-II* コマンド

コマンド	Description
デバイスに関連するクエリー	
sysName	この管理対象ノードに管理上割り当てられた名前を提供します。慣例として、この名前はノードの完全修飾ドメイン名になります。名前が不明な場合、この値は長さがゼロの文字列になります。
sysDescr	エンティティの説明テキストを提供します。この値には、システムのハードウェア タイプ、ソフトウェア オペレーティング システム、ネットワーク ソフトウェアの完全な名前とバージョン識別番号が含まれます。
SNMP 診断クエリー	
sysName	この管理対象ノードに管理上割り当てられた名前を提供します。慣例として、この名前はノードの完全修飾ドメイン名になります。名前が不明な場合、この値は長さがゼロの文字列になります。

sysUpTime	システムのネットワーク管理部分が最後に再初期化されてからの時間（1/100 秒単位）を提供します。
snmpInTotalReqVars	有効な SNMP Get-Request と Get-Next PDU を受信した結果として、SNMP プロトコルエンティティによって正常に取得された MIB オブジェクトの合計数を提供します。
snmpOutPkts	SNMP エンティティから転送サービスに渡された SNMP メッセージの合計数を提供します。
sysServices	このエンティティが提供する可能性があるサービスのセットを示す値を提供します。値は合計値です。この合計は最初は 0 の値を取りますが、このノードがトランザクションを実行する各レイヤ（L）について 1 ～ 7 の範囲を取り、この合計に（L - 1）の 2 乗が加算されます。たとえば、アプリケーションサービスを提供するホストであるノードの値が 4（2^（3-1））になる場合や、逆に、アプリケーションサービスを提供するホストであるノードの値が、72 (2^(4-1) + 2^(7-1)) になる場合があります。 （注） プロトコルのインターネットスイートの場合には、レイヤ 1 の物理（リピータなど）、レイヤ 2 のデータリンクまたはサブネットワーク（ブリッジなど）、レイヤ 3 のインターネット（IP をサポート）、レイヤ 4 のエンドツーエンド（TCP をサポート）、レイヤ 7 のアプリケーション（SMTP をサポート）を計算します。 OSI プロトコルを含むシステムでは、レイヤ 5 および 6 も計算できます。

snmpEnableAuthenTraps	SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。このオブジェクトの値は、すべての設定情報を上書きします。そのため、すべての authenticationFailure トラップを無効化できる手段が提供されます。 （注） シスコでは、このオブジェクトを不揮発性メモリに保存して、ネットワーク管理システムの再初期化後にも維持されるようにすることを強く推奨します。
Syslog に関連するクエリー	
snmpEnabledAuthenTraps	SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。このオブジェクトの値は、すべての設定情報を上書きします。そのため、すべての authenticationFailure トラップを無効化できる手段が提供されます。 （注） シスコでは、このオブジェクトを不揮発性メモリに保存して、ネットワーク管理システムの再初期化後にも維持されるようにすることを強く推奨します。
日付または時刻に関連するクエリー	
sysUpTime	システムのネットワーク管理部分が最後に再初期化されてからの時間（1/100 秒単位）を提供します。

HOST-RESOURCES MIB

HOST-RESOURCES-MIB から値を取得するには、Host Resources Agent を使用します。Host Resources Agent は、ストレージ リソース、プロセス テーブル、デバイス情報、およびインストールされたソフトウェア ベースなど、ホスト情報に対する SNMP アクセスを提供します。Host Resources Agent は次のオブジェクト グループをサポートしています。

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf

- hrSWInstalled

表 *3 : HOST-RESOURCES MIB* のコマンド

コマンド	Description
デバイスに関連するクエリー	
hrFSMountPoint	このファイル システムのルートのパス名を提供します。
hrDeviceDescr	デバイスの製造元やリビジョン、シリアル番号（オプション）など、このデバイスの説明テキストを提供します。
hrStorageDescr	ストレージのタイプおよびインスタンスの説明を提供します。
メモリ、ストレージ、CPU に関連するクエリー	
hrMemorySize	ホストに搭載されている物理的な読み取り/書き込みメイン メモリ（通常は RAM）の容量を提供します。
hrStorageSize	ストレージのサイズを hrStorageAllocationUnits の単位で提供します。このオブジェクトは書き込み可能であるため、操作が理に適っており、基盤となるシステムで実行可能な場合には、ストレージエリアのサイズのリモート設定が可能です。たとえば、バッファ プールに割り当てるメモリの量や、仮想メモリに割り当てるディスク容量を変更できます。
プロセスに関連するクエリー	
hrSWRunName	製造元、リビジョン、一般に知られている名前など、この実行中のソフトウェアの説明テキストを提供します。このソフトウェアがローカルにインストールされている場合は、対応する hrSWInstalledName で使用されているものと同じ文字列である必要があります。
hrSystemProcesses	このシステムに現在ロードされているか、実行中のプロセス コンテキストの数を提供します。
hrSWRunIndex	ホストで実行中の各ソフトウェアに固有の値を提供します。可能な限り、ネイティブかつ一意のシステム識別番号を使用します。
ソフトウェア コンポーネントに関連するクエリー	

hrSWInstalledName	製造元、リビジョン、一般に知られている名前、およびシリアル番号（オプション）など、このインストールされているソフトウェアの説明テキストを提供します。
hrSWRunPath	このソフトウェアのロード元である長期ストレージの場所（ディスク ドライブなど）の説明を提供します。
日付または時刻に関連するクエリー	
hrSystemDate	ホストのローカルの日時を提供します。
hrFSLastPartialBackupDate	このファイルシステムの一部が、バックアップのために別のストレージデバイスにコピーされた最後の日付を提供します。This information is useful for ensuring that backups are being performed regularly. この情報が不明な場合、この変数は 0000 年 1 月 1 日 00:00:00.0 に対応する値となり、「00 00 01 01 00 00 00 00」（16 進数）と符号化されます。

CISCO-SYSLOG-MIB

Syslog は、情報レベルから重大なものまでのすべてのシステムメッセージを追跡し、ログに記録します。この MIB を使用すると、ネットワーク管理アプリケーションでは Syslog メッセージを SNMP トラップとして受信できるようになります。

Cisco Syslog Agent では、次の MIB オブジェクトによるトラップ機能をサポートしています。

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

（注） CISCO-SYSLOG-MIB は、CISCO-SMI MIB の存在に依存します。

表 *4 : CISCO-SYSLOG-MIB* のコマンド

コマンド	Description
Syslog に関連するクエリー	

clogNotificationEnabled	デバイスが Syslog メッセージを生成するときに、clogMessageGenerated 通知が送信されるかどうかを示します。通知を無効化しても、syslog メッセージは、clogHistoryTable に追加されます。
clogMaxSeverity	syslog のどの重大度レベルを処理するかを示します。エージェントは、重大度がこの値より大きい Syslog メッセージを無視します。 （注） 重大度は数値が大きくなるほど低くなります。たとえば、エラー（4）は、デバッグ（8）より重大度が高いです。

CISCO-CCM-MIB および CISCO-CCM-CAPABILITY MIB

CISCO-CCM-MIB には、Unified Communications Manager と、Unified Communications Manager ノードで確認できる、電話やゲートウェイなどのそれに関連するデバイスについての動的な（リアルタイム）情報と設定された（静的）情報の両方が含まれています。簡易ネットワーク管理プロトコル（SNMP）テーブルには、IP アドレス、登録ステータス、およびモデルタイプなどの情報が格納されています。

SNMP は IPv4 と IPv6 をサポートし、CISCO-CCM-MIB には IPv4 と IPv6 の両方のアドレスやプリファレンスなどの列とストレージが含まれています。

（注） Unified Communications Manager は、Unified Communications Manager システム内のこの MIB をサポートしています。IM and Presence Service と Cisco Unity Connection はこの MIB をサポートしていません。

CISCO-CCM-MIB および MIB 定義のサポート リストを参照するには、次のリンクにアクセスしてください。

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

廃止オブジェクトを含め、Unified Communications Manage リリース全体での MIB の依存関係と MIB コンテンツを表示するには、次のリンクにアクセスしてください。 http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

動的テーブルは、Cisco CallManager サービスが起動され、実行中の場合のみ入力されます（またはUnified Communications Manage クラスタ設定の場合は、ローカルの Cisco CallManager サービス）。静的テーブルは、Cisco CallManager SNMP サービスが実行中の場合に入力されます。

表 *5 : Cisco-CCM-MIB* の動的テーブル

テーブル	コンテンツ
ccmTable	このテーブルには、ローカル Unified Communications Manager のバージョンおよびインストールIDが保存されます。また、このテーブルには、ローカルの Unified Communications Manager が認識するクラスタ内のすべての Unified Communications Manager についての情報も保存されますが、バージョンの詳細は、「「unknown」」と示されます。ローカルの Unified Communications Manager がダウンした場合、バージョンおよびインストールIDの値を除き、テーブルは空のままになります。
ccmPhoneFailed、ccmPhoneStatusUpdate、ccmPhoneExtn、ccmPhone、ccmPhoneExtension	Cisco Unified IP Phone の場合、ccmPhoneTable の登録済み電話機の数は、Unified Communications Manager/RegisteredHardware Phones perfmon カウンタと一致する必要があります。ccmPhoneTable には、登録済み、未登録、および拒否された Cisco Unified IP Phone ごとに 1 つのエントリがあります。ccmPhoneExtnTable では、インデックス ccmPhoneIndex と ccmPhoneExtnIndex を組み合わせて、ccmPhoneTable と ccmPhoneExtnTable のエントリが関連付けられます。
ccmCTIDevice、ccmCTIDeviceDirNum	ccmCTIDeviceTable には、各 CTI デバイスが 1 つのデバイスとして保存されます。CTI ルート ポイントまたは CTI ポートの登録ステータスに基づいて、Unified Communications Manager MIB 内の ccmRegisteredCTIDevices、ccmUnregisteredCTIDevices、ccmRejectedCTIDevices カウンタが更新されます。
ccmSIPDevice	CCMSIPDeviceTable には、各 SIP トランクが 1 つのデバイスとして保存されます。

テーブル	コンテンツ
ccmH323Device	ccmH323DeviceTable には、Unified Communications Manager（または、クラスタ設定の場合は、ローカルの Unified Communications Manager）に情報が含まれる H.323 デバイスのリストが含まれます。H.323 電話機または H.323 ゲートウェイの場合、ccmH.323DeviceTable には H.323 デバイスごとに 1 つのエントリが作成されます。(H.323 電話機およびゲートウェイは、Unified Communications Manager で登録されません。指定された H.323 電話機およびゲートウェイのコールを処理する準備ができると、Unified Communications Manager によって H.323Started アラームが生成されます。) システムにより、H.323 トランク情報の一部としてゲートキーパー情報が提供されます。
ccmVoiceMailDevice、ccmVoiceMailDirNum	Cisco uOne、ActiveVoice の場合、ccmVoiceMailDeviceTable には音声メッセージング デバイスごとに 1 つのエントリが作成されます。登録ステータスに基づいて、Cisc MIB 内の ccmRegisteredVoiceMailDevices、ccmUnregisteredVoiceMailDevices、ccmRejectedVoiceMailDevices カウンタが更新されます。

テーブル	コンテンツ
ccmGateway	ccmRegisteredGateways、ccmUnregisteredGateways、および ccmRejectedGateways は、それぞれ、登録されたゲートウェイ デバイスまたはポートの数、登録されていないゲートウェイ デバイスまたはポートの数、および拒否されたゲートウェイ デバイスまたはポートの数を追跡します。 Unified Communications Manager は、デバイスまたはポート レベルでアラームを生成します。ccmGatewayTable には、CallManager アラームに基づいて、デバイスレベルまたはポートレベルの情報が格納されます。登録済み、未登録、または拒否されたデバイスまたはポートごとに、1 つのエントリが ccmGatewayTable に存在します。2 つの FXS ポートと 1 つの T1 ポートを備えた VG200 の場合、ccmGatewayTable には 3 つのエントリが作成されます。ccmActiveGateway および ccmInActiveGateway のカウンタは、アクティブな（登録済みの）ゲートウェイ デバイスまたはポート、および接続されていない（未登録または拒否）ゲートウェイ デバイスまたはポートの数を追跡します。 登録ステータスに基づき、ccmRegisteredGateways、ccmUnregisteredGateways、ccmRejectedGateways の各カウンタが更新されます。
ccmMediaDeviceInfo	このテーブルには、少なくとも 1 回はローカルの Unified Communications Manager での登録を試みたすべてのメディア デバイスのリストが格納されます。
ccmGroup	このテーブルには、Unified Communications Manager クラスタ内の Unified Communications Manager グループが格納されます。
ccmGroupMapping	このテーブルは、クラスタ内のすべての Unified Communications Manager を Unified Communications Manager グループにマッピングします。ローカルの Unified Communications Manager ノードがダウンしても、このテーブルは空のままです。

表 *6 : CISCO-CCM-MIB* の静的テーブル

テーブル	コンテンツ
ccmProductType	このテーブルには、Unified Communications Manager（Unified Communications Manager クラスタ設定の場合はクラスタ）でサポートされる製品タイプのリストが格納されます。タイプには、電話機タイプ、ゲートウェイ タイプ、メディア デバイス タイプ、H.323 デバイス タイプ、CTI デバイス タイプ、音声メッセージング デバイス タイプ、SIP デバイス タイプなどがあります。
ccmRegion、ccmRegionPair	ccmRegionTable には、Cisco Communications Network（CCN）システムの地理的に離れた場所にあるすべてのリージョンのリストが格納されます。ccmRegionPairTable には、Unified Communications Manager クラスタの地理的リージョンペアのリストが含まれます。地理的リージョンペアは、接続元リージョンと接続先リージョンで定義されます。
ccmTimeZone	このテーブルには、Unified Communications Manager のクラスタ内のすべてのタイム ゾーン グループのリストが含まれます。
ccmDevicePool	このテーブルには、Unified Communications Manager のクラスタ内のすべてのデバイス プールのリストが含まれます。デバイスプールは、リージョン、日付/時刻グループ、および Unified Communications Manager グループによって定義されます。

（注） CISCO-CCM-MIB の 「ccmAlarmConfigInfo」 グループおよび 「ccmQualityReportAlarmConfigInfo」 グループでは、通知に関する設定パラメータを定義します。

CISCO-UNITY-MIB

CISCO-UNITY-MIB では、Cisco Unity Connection に関する情報を入手するために Connection SNMP エージェントを使用します。

CISCO-UNITY-MIB の定義を確認するには、次のリンクにアクセスして [SNMP v2 MIB（SNMP v2 MIBs）] をクリックしてください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml [英語]

（注） Cisco Unity Connection ではこの MIB をサポートしています。Unified Communications Manager と IM and Presence Service は、この MIB をサポートしていません。

Connection SNMP エージェントでは次のオブジェクトをサポートしています。

表 *7 : CISCO-UNITY-MIB* のオブジェクト

オブジェクト	説明
ciscoUnityTable	このテーブルには、ホスト名やバージョン番号など、Cisco Unity Connection サーバに関する一般的な情報が格納されます。
ciscoUnityPortTable	このテーブルには、Cisco Unity Connection のボイスメッセージングポートに関する一般的な情報が格納されます。
General Unity Usage Info オブジェクト	このグループには、Cisco Unity Connection のボイスメッセージングポートの容量と使用率に関する情報が格納されます。

SNMP の設定要件

システムにはデフォルトの SNMP 設定はありません。MIB 情報にアクセスするには、インストール後に SNMP の設定を行う必要があります。シスコでは、SNMP V1、V2c、および V3 バージョンをサポートしています。

SNMP エージェントは、コミュニティ名と認証トラップによるセキュリティを提供します。MIB 情報にアクセスするには、コミュニティ名を設定する必要があります。次の表に、必要な SNMP 構成時の設定を提供します。

表 *8 : SNMP* の設定要件

設定（**Configuration**）	**[Cisco Unified Serviceability]** ページ
V1/V2c コミュニティ ストリング	**SNMP** > **V1/V2c** > **コミュニティ ストリング**
V3 コミュニティ ストリング	**SNMP** > **V3** > **ユーザ**
MIB2 のシステムコンタクトおよびロケーション	**SNMP** > **SystemGroup** > **MIB2 システム グループ**
トラップ通知先（V1/V2c）	**SNMP** > **V1/V2c** > **Notification Destination**
トラップ通知先（V3）	**SNMP** > **V3** > **Notification Destination**

SNMP バージョン 1 のサポート

SNMP バージョン 1（SNMPv1）は、管理情報構造（SMI）の仕様の範囲内で機能する SNMP の初期実装で、User Datagram Protocol（UDP）や Internet Protocol（IP）などのプロトコル上で動作します。

SNMPv1 SMI では、高度な構造を持つテーブル（MIB）が定義されます。このテーブルは、表形式のオブジェクト（つまり、複数の変数を含むオブジェクト）のインスタンスのグループ化に使用されます。テーブルにはインデックスが付けられた 0 個以上の行が格納されるため、SNMP では、サポートされているコマンドを使用して、行全体を取得したり変更したりできます。

SNMPv1 では、NMS が要求を発行し、管理対象デバイスから応答が返されます。エージェントは、トラップ オペレーションを使用して、NMS に重要なイベントを非同期的に通知します。

Serviceability GUI では、SNMPv1 サポートを [V1/V2c の設定（V1/V2c Configuration）] ウィンドウで設定します。

SNMP バージョン 2c のサポート

SNMPv2c は、SNMPv1 と同様に、Structure of Management Information（SMI）の仕様の範囲内で機能します。MIB モジュールには、相互に関係のある管理対象オブジェクトの定義が格納されます。SNMPv1 で使用されるオペレーションと SNMPv2 で使用されるオペレーションは、ほぼ同じです。たとえば、SNMPv2 トラップ オペレーションは、SNMPv1 で使用する機能と同じですが、異なるメッセージ形式を使用する、SNMPv1 トラップに代わる機能です。

SNMPv2c のインフォーム オペレーションでは、ある NMS から別の NMS にトラップ情報を送信して、その NMS から応答を受信することができます。

Serviceability GUI では、SNMPv2c サポートを [V1/V2c の設定（V1/V2c Configuration）] ウィンドウで設定します。

SNMP バージョン 3 のサポート

SNMP バージョン 3 は、認証（要求が正規の送信元から送信されたものかどうかの確認）、プライバシー（データの暗号化）、認可（要求された操作がユーザに許可されているかどうかの確認）、およびアクセス コントロール（要求されたオブジェクトにユーザがアクセスできるかどうかの確認）などのセキュリティ機能を提供します。SNMP パケットがネットワーク上で公開されないように、SNMPv3 では暗号化を設定できます。

SNMPv3 では、SNMPv1 や SNMPv2 のようにコミュニティ ストリングを使用するのではなく、SNMP ユーザを使用します。

Serviceability GUI では、[V3の設定（V3 Configuration）] ウィンドウで SNMP v3 のサポートを設定します。

SNMP サービス

次の表のサービスでは、SNMP の操作をサポートしています。

（注） SNMP マスター エージェントは、MIB インターフェイスのプライマリ サービスとして機能します。Cisco CallManager SNMP サービスは手動でアクティブ化する必要があります。他のすべての SNMP サービスは、インストール後に実行する必要があります。

表 *9 : SNMP* サービス

MIB	サービス	ウィンドウ
CISCO-CCM-MIB	Cisco CallManager SNMP サービス	**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]**。サーバを選択した後、[パフォーマンスおよびモニタリング（Performance and Monitoring）] カテゴリを選択します。
SNMP エージェント	SNMP Master Agent	**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センター - ネットワーク サービス（Control Center - Network Services）]** サーバを選択した後、[Platform Services] カテゴリを選択します。 **[Cisco Unified IM and Presence Serviceability]** > **[ツール（Tools）]** > **[コントロール センター - ネットワーク サービス（Control Center - Network Services）]** サーバを選択した後、[Platform Services] カテゴリを選択します。
CISCO-CDP-MIB	Cisco CDP Agent	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
ハードウェア MIB	Native Agent Adaptor	
CISCO-UNITY-MIB	Connection SNMP Agent	**[Cisco Unity Connection Serviceability]** > **[ツール（Tools）]** > **[サービス管理（Service Management）]** サーバを選択した後、[Base Services] カテゴリを選択します。

⚠

注意 SNMP サービスを停止すると、ネットワーク管理システムが Unified Communications Manager または Cisco Unity Connection ネットワークをモニタしなくなるため、データが失われます。テクニカル サポート チームの指示がない限り、サービスを停止しないでください。

SNMP のコミュニティ ストリングとユーザ

SNMP コミュニティ ストリングでは、セキュリティは確保されませんが、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。SNMP コミュニティ ストリングは、SNMP v1 および v2c の場合にのみ設定します。

SNMPv3 では、コミュニティ ストリングを使用しません。バージョン 3 では、代わりに SNMP ユーザを使用します。SNMP ユーザを使用する目的はコミュニティ ストリングと同じですが、ユーザの暗号化や認証を設定できるため、セキュリティが確保されます。

Serviceability GUI では、デフォルトのコミュニティ ストリングやユーザは存在しません。

SNMP のトラップとインフォーム

SNMP エージェントは、重要なシステムイベントを識別するために、トラップ形式またはインフォーム形式で NMS に通知を送信します。トラップ形式の場合は宛先からの確認応答を受信しませんが、インフォーム形式の場合は確認応答を受信します。通知先を設定するには、Serviceability GUI の [SNMP 通知先設定（Notification Destination Configuration）] ウィンドウを使用します。

（注） Unified Communications Manager は、Unified Communications Manager および IM and Presence Service システムの SNMP トラップをサポートします。

SNMP 通知では、対応するトラップ フラグが有効な場合、トラップが即座に送信されます。Syslog エージェントの場合、アラームとシステム レベルのログ メッセージが Syslog デーモンに送信され、ログに記録されます。また、一部の標準的なサードパーティ製アプリケーションでもログ メッセージが syslog デーモンに送信され、ログに記録されます。これらのログ メッセージはローカルの syslog ファイルに記録され、SNMP トラップまたは通知への変換も行われます。

以下に、設定済みのトラップ通知先に送信される、Unified Communications Manager の SNMP のトラップおよびインフォーム メッセージの一覧を示します。

- Unified Communications Manager で障害が発生しました
- 電話機で障害が発生しました（Phone failed）
- 電話機ステータスの更新（Phones status update）
- ゲートウェイで障害が発生しました（Gateway failed）
- メディア リソース リストが使い果たされました（Media resource list exhausted）
- ルート リストが使い果たされました（Route list exhausted）
- ゲートウェイ レイヤ 2 の変更（Gateway layer 2 change）
- 品質レポート（Quality report）
- 悪質なコール（Malicious call）

- syslog メッセージが生成されました（Syslog message generated）

ヒント　通知先を設定する前に、必要なSNMPサービスがアクティブ化され、動作していることを確認します。また、コミュニティ ストリング/ユーザに対する特権が正しく設定されていることを確認します。

Serviceability GUI の **[SNMP]** > **[V1/V2]** > **[通知先（Notification Destination）]** または **[SNMP]** > **[V3]** > **[通知先（Notification Destination）]** を選択して SNMP トラップの宛先を設定します。

次の表では、ネットワーク管理システム（NMS）で設定するトラップとインフォームのパラメータについて説明します。この表の値を設定するには、その NMS をサポートする SNMP 製品のドキュメントの説明に従って、NMS 上で適切なコマンドを実行します。

（注）　この表に一覧されているパラメータは、最後の 2 つのパラメータを除き、すべて CISCO-CCM-MIB の一部です。最後の 2 つの clogNotificationsEnabled と clogMaxSeverity は、CISCO-SYSLOG-MIB の一部です。

IM and Presence Service の場合、NMS で clogNotificationsEnabled パラメータと clogMaxSeverity trap/inform パラメータのみを設定します。

表 *10 : Cisco Unified Communications Manager* のトラップおよびインフォーム設定パラメータ

パラメータ名	デフォルト値	生成されるトラップ	推奨設定
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	デフォルトの仕様を維持します。

パラメータ名	デフォルト値	生成されるトラップ	推奨設定
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Cisco Unified Communications Manager 管理では、Cisco ATA 186 デバイスを電話機として設定することができますが、Unified Communications Manager が SNMP トラップを Cisco ATA デバイスに送信する際には、ゲートウェイ タイプのトラップが送信されます（たとえば、ccmGatewayFailed など）。	なし。デフォルトではこのトラップは有効に設定されています。
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	ccmPhoneStatusUpdateAlarmInterval は 30 ～ 3600 の範囲の値に設定します。
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	ccmPhoneFailedAlarmInterval は 30 ～ 3600 の範囲の値に設定します。
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	なし。デフォルトではこのトラップは有効に設定されています。
ccmQualityReportAlarmEnable	True	このトラップは、Cisco Extended Functions サービスがサーバ上、または、クラスタ設定の場合には（Unified Communications Manager のみ）ローカル Unified Communications Manager サーバ上でアクティブ化されて実行されている場合にのみ生成されます。 ccmQualityReport	なし。デフォルトではこのトラップは有効に設定されています。
clogNotificationsEnabled	False	clogMessageGenerated	トラップ生成を有効にするには、clogNotificationsEnable を True に設定します。

パラメータ名	デフォルト値	生成されるトラップ	推奨設定
clogMaxSeverity	警告	clogMessageGenerated	clogMaxSeverity を warning に設定すると、アプリケーションが、重大度が警告以上の Syslog メッセージを生成したときに SNMP トラップが生成されます。

関連トピック

CISCO-CCM-MIB トラップ パラメータ （44 ページ）
CISCO-SYSLOG-MIB トラップ パラメータ （43 ページ）

SFTP サーバのサポート

内部テストでは、Cisco が提供し、Cisco TAC がサポートする Cisco Prime Collaboration Deployment（PCD）上で SFTP サーバを使用します。SFTP サーバ オプションの概要については、次の表を参照してください。

表 *11 : SFTP* サーバのサポート

SFTP サーバ	サポートの説明
Cisco Prime Collaboration Deployment	このサーバは Cisco が提供およびテストした SFTP サーバのみとなり、Cisco TAC がサポートします。 バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。バージョン（SFTP）または Unified Communications Manager をアップグレードする前に、『*Cisco Prime Collaboration Deployment Administration Guide*』を参照して、互換性のあるバージョンであることを確認してください。
テクノロジー パートナーの SFTP サーバ	これらのサーバはサード パーティが提供およびテストしたものです。バージョンの互換性は、サード パーティによるテストに依存します。テクノロジー パートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com

SFTP サーバ	サポートの説明
他のサードパーティの SFTP サーバ	これらのサーバはサード パーティが提供するものであり、シスコが行うテストは限られています。Cisco TAC はこれらのサーバを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベスト エフォートに基づきます。 （注） これらの製品がシスコでテストされていない場合、シスコはその機能を保証することができません。Cisco TAC は、これらの製品をサポートしていません。完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジー パートナーの SFTP サーバを利用してください。

SNMP 設定タスク フロー

簡易ネットワーク管理プロトコルの設定を行うには、以下のタスクを実行します。タスクが異なる場合があるため、どの SNMP バージョンを設定するかを必ず確認してください。SNMP V1、V2c、または V3 から選択することができます。

始める前に

SNMP ネットワーク管理システムをインストールして、設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	SNMP サービスの有効化 （28 ページ）	重要な SNMP サービスが稼働中であることを確認します。
ステップ 2	使用する SNMP のバージョンに応じて、以下のいずれかのタスクを実行します。 • SNMP コミュニティ ストリングの設定 （29 ページ） • SNMP ユーザの設定 （32 ページ）	SNMP V1 あるいは V2 の場合、SNMP コミュニティ ストリングを設定します。 SNMP V3 の場合は、SNMP ユーザを設定します。
ステップ 3	Remote SNMP Engine ID の取得 （36 ページ）	SNMP V3 の場合は、通知先の設定に必要なリモート SNMP エンジンのアドレスを取得します。

	コマンドまたはアクション	目的
		（注） Snmp V3 の場合は、この手順は必須ですが、SNMP V1 または V2c の場合は省略できます。
ステップ 4	SNMP 通知先の設定 （36 ページ）	すべての SNMP に、SNMP トラップおよび通知を送信する通知先を設定します。
ステップ 5	MIB2 システム グループの設定 （41 ページ）	MIB-II システム グループのシステム コンタクトおよびシステム ロケーションを設定します。
ステップ 6	CISCO-SYSLOG-MIB トラップ パラメータ （43 ページ）	CISCO-SYSLOG-MIB のトラップ設定を設定します。
ステップ 7	CISCO-CCM-MIB トラップ パラメータ （44 ページ）	Unified Communications Manager のみ：CISCO-CCM-MIB のトラップ設定を行います。
ステップ 8	SNMP Master Agent の再起動 （44 ページ）	SNMP の設定が完了したら、SNMP マスター エージェントを再起動します。
ステップ 9	SNMP ネットワークk管理システムで、Unified Communications Manager のトラップ パラメータを設定します。	

SNMP サービスの有効化

SNMP サービスが動作していることを確認するには、以下の手順を使用します。

手順

ステップ 1 [Cisco Unified Serviceability] にログインします。

ステップ 2 **Cisco SNMP Master Agent** ネットワーク サービスが実行中であることを確認します。サービスはデフォルトでオンになっています。

a) **[Tools（ツール）] > [Control Center - Network Services（コントロール センタのネットワーク サービス）]** を選択します。

b) パブリッシャ ノードを選択し、**移動**をクリックします。

c) **Cisco SNMP Master Agent** サービスが稼働していることを確認します。

ステップ 3 **Cisco Call Manager SNMP Service**を起動します。

a) **コントロール センター** > **サービスの有効化**を選択します。

b) **さーば** ドロップダウンから、パブリッシャ ノードを選択して、**移動**をクリックします。

c) **Cisco Call Manager SNMP サービス** が稼働していることを確認します。稼働していない場合は、対応するチェック ボックスをオンにして、**保存**をクリックします。

次のタスク

SNMP V1 または V2c を設定する場合は、SNMP コミュニティ ストリングの設定 （29 ページ）。

SNMP V3 を設定する場合は、SNMP ユーザの設定 （32 ページ）。

SNMP コミュニティ ストリングの設定

SNMP V1 または V2c を導入している場合は、以下の手順を使用して SNMP コミュニティ ストリングを設定します。

（注） この手順は、SNMP V1 または V2c の場合、必須となります。SNMP V3 では、コミュニティ ストリングではなく SNMP ユーザを設定します。

手順

ステップ 1 Cisco Unified Serviceabilityから、**SNMP** > **V1/V2c** > **コミュニティ ストリング**を選択します。

ステップ 2 **サーバ** を選択し、**検索** をクリックして、既存のコミュニティ ストリングを検索します。必要に応じて、検索パラメータを入力して特定のコミュニティ文字列を検索することができます。

ステップ 3 次のいずれかを実行します。

- 既存の SNMP コミュニティ ストリングを編集するには、そのストリングを選択します。
- 新しいコミュニティ ストリングを追加するには、[新規追加（Add New）] をクリックします。

（注） 既存のコミュニティ ストリングを削除するには、そのストリングを選択して、**選択したものを削除する** をクリックします。ユーザを削除したら、Cisco SNMP マスター エージェントを再起動します。

ステップ 4 **コミュニティ ストリング名**を入力します。

ステップ 5 **SNMP コミュニティ ストリングの設定** ウィンドウの各フィールドに入力します。フィールドおよびフィールドの設定の詳細は、コミュニティ ストリングの構成時の設定 （30 ページ）を参照してください。

ステップ 6 **アクセス権限** ドロップダウンで、そのコミュニティ ストリングの権限を設定します。

ステップ 7 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する**チェック ボックスをオンにします。

ステップ 8 **[保存（Save）]** をクリックします。

ステップ 9 **OK** をクリックして、SNMP マスター エージェントのサービスを再起動して、変更を反映させます。

次のタスク

SNMP 通知先の設定 （36 ページ）

コミュニティ ストリングの構成時の設定

次の表で、コミュニティ ストリングの構成時の設定について説明します。

表 *12*：コミュニティ ストリングの構成時の設定

フィールド	説明
サーバ	コミュニティ ストリングを検索する際に手順を実行してサーバの選択を指定しているため、[コミュニティ ストリング設定（Community String configuration）] ウィンドウの設定は読み取り専用として表示されます。 コミュニティ ストリングのサーバを変更するには、コミュニティ ストリングの検索手順を実行します。
コミュニティ ストリング（Community String）	コミュニティ ストリングの名前を入力します。この名前には、最長 32 文字を指定でき、英数字、ハイフン（-）、および下線文字（_）を任意に組み合わせることが可能です。 **ヒント** 部外者が推測しにくいコミュニティ ストリング名を選択してください。 コミュニティ ストリングを編集するとき、コミュニティ ストリングの名前は変更できません。
任意のホストからの SNMP パケットを受け入れる（Accept SNMP Packets from any host）	任意のホストから SNMP パケットを受け入れるには、このボタンをクリックします。

フィールド	説明
指定したホストからのSNMPパケットのみ受け入れる（Accept SNMP Packets only from these hosts）	特定のホストからのSNMPパケットを受け入れるには、このオプション ボタンをクリックします。 [ホスト名/IPv4/IPv6 アドレス（Hostname/IPv4/IPv6 Address）] フィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力し、[挿入（Insert）] をクリックします。 IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。 SNMPパケットを受け取るアドレスごとにこのプロセスを繰り返します。アドレスを削除するには、それを[ホストIPv4/IPv6アドレス（Host IPv4/IPv6 Addresses）] リスト ボックスから選択し、[削除（Remove）] をクリックします。

フィールド	説明
アクセス権限（Access Privileges）	ドロップダウン リスト ボックスで、適切なアクセス レベルを次のリストの中から選択します。 **ReadOnly** コミュニティ ストリングは、MIB オブジェクトの値の読み取りのみが可能です。 **ReadWrite** コミュニティ ストリングは、MIB オブジェクトの値を読み書きできます。 **ReadWriteNotify** コミュニティ ストリングは、MIB オブジェクト値の読み取りおよび書き込みと、トラップおよびインフォーム メッセージでの MIB オブジェクト値の送信が可能です。 **NotifyOnly** コミュニティ ストリングは、トラップおよびインフォーム メッセージでの MIB オブジェクト値の送信のみ可能です。 **ReadNotifyOnly** コミュニティ ストリングは、MIB オブジェクト値の読み取りと、トラップおよびインフォーム メッセージでの値の送信が可能です。 なし コミュニティ ストリングはトラップ情報の読み取り、書き込み、送信を行えません。 ヒント　トラップ設定パラメータを変更するには、NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 権限でコミュニティ ストリングを設定します。 IM and Presence Service は ReadNoticyOnly をサポートしていません。
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードにコミュニティ ストリングを適用する場合は、このチェックボックスをオンにします。 このフィールドは、Unified Communications Manager および IM and Presence Service のクラスタにのみ適用されます。

SNMP ユーザの設定

SNMP V3 を導入している場合は、以下の手順を使用して SNMP ユーザを設定します。

（注） この手順は、SNMP V3 の場合にのみ必要です。SNMP V1 または V2c の場合は、コミュニティストリングを設定します。

手順

ステップ 1 Cisco Unified Serviceability で、**SNMP** > **V3** > **ユーザ**を選択します。

ステップ 2 **サーバ**を選択して、**検索** をクリックして、既存の SNMP ユーザを検索します。必要に応じて、検索パラメータを入力して特定のユーザを検索することができます。

ステップ 3 次のいずれかを実行します。

- 既存の SNMP ユーザを編集するには、ユーザを選択します。
- 新しい SNMP ユーザを追加するには、**新規追加** をクリックします。

（注） 既存のユーザを削除するには、ユーザを選択して **選択したものを削除する**をクリックします。ユーザを削除したら、Cisco SNMP マスター エージェントを再起動します。

ステップ 4 [SNMP User Name] を入力します。

ステップ 5 SNMP ユーザの設定を入力します。フィールドおよびフィールドの設定の詳細は、SNMP V3 のユーザ構成時の設定 （34 ページ）を参照してください。

ヒント 設定を保存する前であれば、[すべてクリア（Clear All）] ボタンをクリックしてウィンドウ内の設定に入力した情報をすべて消去することができます。

ステップ 6 **アクセス権限** ドロップダウンで、このユーザに割り当てるアクセス権限を設定します。

ステップ 7 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する** チェック ボックスをオンにします。

ステップ 8 **[保存（Save）]** をクリックします。

ステップ 9 **OK** をクリックして、SNMP マスター エージェントを再起動します。

（注） 設定したユーザが存在するこのサーバにアクセスするには必ず NMS で適切な認証およびプライバシー設定を使用して、このユーザを設定します。

次のタスク

Remote SNMP Engine ID の取得 （36 ページ）

SNMP V3 のユーザ構成時の設定

次の表に、SNMP V3 のユーザ構成時の設定について説明します。

表 *13 : SNMP V3* のユーザ構成時の設定

フィールド	説明
サーバ	通知先の検索の手順を実行したときにサーバを指定済みのため、この設定は読み取り専用として表示されます。 アクセスを提供するサーバを変更するには、SNMPユーザの検索手順を実行します。
ユーザ名（User Name）	このフィールドには、アクセスを提供するユーザの名前を入力します。この名前には、最長32文字を指定でき、英数字、ハイフン（-）、および下線文字（_）を任意に組み合わせることが可能です。 ヒント　ネットワーク管理システム（NMS）に設定済みのユーザを入力します。 既存の SNMP ユーザの場合、この設定は読み取り専用として表示されます。
認証を要求（Authentication Required）	認証を義務付けるには、このチェックボックスをオンにして、[パスワード（Password）] フィールドと [パスワードを再入力（Reenter Password）] フィールドにパスワードを入力し、適切なプロトコルを選択します。パスワードには 8 文字以上が必要です。 （注）　FIPS モードまたは拡張セキュリティ モードが有効になっている場合は、プロトコルとして [SHA] を選択します。
プライバシーを要求（Privacy Required）	[認証を要求（Authentication Required）] チェックボックスをオンにした場合は、プライバシー情報を指定できます。プライバシーを義務付けるには、このチェックボックスをオンにして、[パスワード（Password）] フィールドと [パスワードを再入力（Reenter Password）] フィールドにパスワードを入力し、プロトコルのチェックボックスをオンにします。パスワードには 8 文字以上が必要です。 （注）　FIPS モードまたは拡張セキュリティ モードが有効になっている場合は、プロトコルとして [AES128] を選択します。
任意のホストからの SNMP パケットを受け入れる（Accept SNMP Packets from any host）	任意のホストからのSNMPパケットを受け入れるには、このオプション ボタンをクリックします。

フィールド	説明
指定したホストからの SNMP パケットのみ受け入れる（Accept SNMP Packets only from these hosts）	特定のホストからの SNMP パケットを受け入れるには、このオプション ボタンをクリックします。 [ホスト名/IPv4/IPv6 アドレス（Hostname/IPv4/IPv6 Address）] フィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力し、[挿入（Insert）] をクリックします。 IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。 SNMP パケットを受け取るアドレスごとにこのプロセスを繰り返します。アドレスを削除するには、それを [ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Addresses）] リスト ボックスから選択し、[削除（Remove）] をクリックします。
アクセス権限（Access Privileges）	ドロップダウン リスト ボックスから、アクセス レベルとして次のいずれかのオプションを選択します。 **ReadOnly** MIB オブジェクトの値の読み取りのみが可能です。 **ReadWrite** MIB オブジェクトの値の読み取りおよび書き込みが可能です。 **ReadWriteNotify** MIB オブジェクトの値の読み取りおよび書き込みと、トラップおよびインフォーム メッセージの MIB オブジェクト値の送信が可能です。 **NotifyOnly** トラップおよびインフォーム メッセージの MIB オブジェクト値の送信のみ可能です。 **ReadNotifyOnly** MIB オブジェクトの値の読み取りと、トラップおよびインフォーム メッセージの値の送信も可能です。 なし トラップ情報の読み取り、書き込み、送信を行えません。 ヒント　トラップ設定パラメータを変更するには、NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 権限でユーザを設定します。

フィールド	説明
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードにユーザ設定を適用する場合は、このチェックボックスをオンにします。 これは、Unified Communications Manager と IM and Presence Service クラスタにのみ適用されます。

Remote SNMP Engine ID の取得

SNMP V3 を導入している場合は、次の手順を使用して、通知先の設定に必要なリモート SNMP エンジン ID を取得します。

（注） Snmp V3 の場合は、この手順は必須ですが、SNMP V1 または 2C の場合は省略できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 `utils snmp walk 1` CLI コマンドを実行します。

ステップ 3 設定されているコミュニティ文字列 (SNMP V1/V2) または設定されたユーザ (SNMP V3) を入力します。

ステップ 4 サーバの IP アドレスを入力します。たとえば、localhost の場合は `127.0.0.1` を入力します。

ステップ 5 オブジェクト ID (OID) として `1.3.6.1.6.3.10.2.1.1.0` を入力します。

ステップ 6 ファイルの場合は、`file` を入力します。

ステップ 7 `y` と入力します。
システム出力である 16 進数文字列は、リモート SNMP エンジン ID を表します。

ステップ 8 SNMP が実行されている各ノードでこの手順を繰り返します。

次のタスク

SNMP 通知先の設定 （36 ページ）

SNMP 通知先の設定

この手順を使用して、SNMP トラップおよび通知を送信する通知先を設定します。この手順は、SNMP V1、V2c、または V3 のいずれかでも使用することができます。

始める前に

SNMP コミュニティ ストリングあるいは SNMP ユーザが未設定の場合、以下のいずれかのタスクを実行します。

- SNMP V1/V2 については、以下を参照してください。 SNMP コミュニティ ストリングの設定 （29 ページ）
- SNMP V3 については、以下を参照してください。 SNMP ユーザの設定 （32 ページ）

手順

ステップ 1 Cisco Unifeid Serviceability で、以下のいずれかを選択します。

- SNMP V1 または V2の場合、**SNMP** > **V1 または V2** > **通知先**を選択します
- SNMP V3 の場合、**SNMP** > **V3** > **通知先**を選択します

ステップ 2 **サーバ**を選択して、**検索** をクリックして、既存の SNMP 通知先を検索します。必要に応じて、検索パラメータを入力して特定の通知先を検索することができます。

ステップ 3 次のいずれかを実行します。

- 既存の SNMP 通知先を編集するには、通知先を選択します。
- 新しい SNMP 通知先を追加するには、[新規追加（Add New）] をクリックします。

（注） 既存の SNMP 通知先を削除するには、通知先を選択して、**選択したものを削除する**をクリックします。ユーザを削除した後、**Cisco SNMP マスターエージェント**を再起動します。

ステップ 4 **ホスト IP アドレス** ドロップダウンで、既存のアドレスを選択するか、**新規追加** をクリックして、新しいホスト IP アドレスを入力します。

ステップ 5 SNMP V1、V2 のみ。SNMP V1 あるいは V2c を設定する場合、いずれかに応じて、**SNMP バージョン** フィールドで、V1 あるいは V2C オプション ボタンをオンにします。

ステップ 6 SNMP V1 または V2 の場合は、以下の手順を実行します。

a) SNMP V2 のみ。**通知タイプ** ドロップダウンで、**通知** あるいは **トラップ**を選択します。
b) 設定した**コミュニティ ストリング** を選択します。

ステップ 7 SNMP V3 の場合は、以下の手順を実行します。

a) **通知タイプ** ドロップダウンで、**通知** あるいは **トラップ**を選択します。
b) **リモート SNMP エンジン ID** ドロップダウンで、既存のエンジン ID を選択するか、**新規追加** を選択して、新しい ID を入力します。
c) **セキュリティ レベル** ドロップダウンで、適切なセキュリティ レベルを割り当てます。

ステップ 8 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する**チェック ボックスをオンにします。

ステップ 9 [挿入（Insert）] をクリックします。

ステップ 10 **OK** をクリックして、SNMP マスター エージェントを再起動します。

例

（注） [通知先の設定] ウィンドウのフィールドの説明については、以下のトピックのいずれかを参照してください。

- SNMP V1 および V2c の通知先の設定 （38 ページ）
- SNMP V3 の通知先の設定 （40 ページ）

次のタスク

MIB2 システム グループの設定 （41 ページ）

SNMP V1 および V2c の通知先の設定

次の表では、SNMP V1/V2c の通知先の構成時の設定について説明します。

表 *14 : SNMP V1/V2c* の通知先の構成時の設定

フィールド	説明
サーバ	通知先を検索するための操作ですでにサーバを指定済みのため、この設定は読み取り専用として表示されます。 通知先のサーバを変更するには、コミュニティ ストリングを検索するための手順を実行します。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Addresses）	ドロップダウン リスト ボックスから、トラップ宛先のホストの IPv4/IPv6 アドレスを選択するか、[新規追加（Add New）] をクリックします。[新規追加（Add New）] をクリックした場合は、[ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）] フィールドにトラップ宛先の IPv4/IPv6 アドレスを入力します。 既存の通知先の場合、ホストの IP アドレスの設定は変更できません。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）	このフィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力します。 IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。

フィールド	説明
部品番号	フィールドに、SNMP パケットを受信する宛先サーバ上の通知を受け取るポート番号を入力します。
V1 または V2c	[SNMPバージョン情報（SNMP Version Information）] ペインで、適切な SNMP バージョンのオプション ボタン（[V1] または [V2c]）をクリックします。これは使用している SNMP のバージョンによります。 • [V1] を選択した場合は、コミュニティ ストリングを設定します。 • [V2c] を選択した場合は、通知タイプを設定してからコミュニティ ストリングを設定します。
コミュニティ ストリング（Community String）	ドロップダウン リスト ボックスから、このホストで生成される通知メッセージに使用するコミュニティ ストリング名を選択します。 最小限の通知権限（ReadWriteNotify または Notify Only）を持つコミュニティ ストリングのみが表示されます。これらの権限を持つコミュニティ ストリングを設定していない場合、ドロップダウン リスト ボックスに選択肢が表示されません。必要に応じて、[新規コミュニティ ストリングの作成（Create New uiCommunity String）] をクリックしてコミュニティ ストリングを作成します。 IM and Presence のみ：最小限の通知権限（ReadWriteNotify、ReadNotifyOnly、または Notify Only）を持つコミュニティ ストリングのみが表示されます。これらの権限を持つコミュニティ ストリングを設定していない場合、ドロップダウン リスト ボックスに選択肢が表示されません。必要に応じて、[新規コミュニティ ストリングの作成（Create New Community String）] をクリックしてコミュニティ ストリングを作成します。
通知の種類（Notification Type）	ドロップダウン リスト ボックスから適切な通知タイプを選択します。
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードに通知先の設定を適用する場合は、このチェックボックスをオンにします。 これは、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。

SNMP V3 の通知先の設定

次の表では、SNMP V3 の通知先の構成時の設定について説明します。

表 *15 : SNMP V3* の通知先の構成時の設定

フィールド	説明
サーバ	SNMP V3 の通知先を検索するための操作ですでにサーバを指定済みのため、この設定は読み取り専用として表示されます。 通知先のサーバを変更するには、SNMP V3 の通知先を検索するための手順を実行し、別のサーバを選択します。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Addresses）	ドロップダウン リスト ボックスから、トラップ宛先のホストの IPv4/IPv6 アドレスを選択するか、[新規追加（Add New）] をクリックします。[新規追加（Add New）] をクリックした場合は、[ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）] フィールドにトラップ宛先の IPv4/IPv6 アドレスを入力します。 既存の通知先の場合、ホストの IP アドレスの設定は変更できません。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）	このフィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力します。 IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。
部品番号	フィールドに、宛先サーバ上の通知を受け取るポート番号を入力します。
通知の種類（Notification Type）	ドロップダウン リスト ボックスから [インフォーム（Inform）] または [トラップ（Trap）] を選択します。 **ヒント** [インフォーム（Inform）] オプションを選択することを推奨します。通知機能では、受信確認されるまでメッセージが再送されるため、トラップよりも信頼性が高くなります。
リモート SNMP エンジン ID（Remote SNMP Engine Id）	この設定は、[通知の種類（Notification Type）] ドロップダウン リスト ボックスから [インフォーム（Inform）] を選択した場合に表示されます。 ドロップダウン リスト ボックスからエンジン ID を選択するか、[新規追加（Add New）] を選択します。[新規追加（Add New）] を選択した場合は、[リモート SNMP エンジン ID（Remote SNMP Engine Id）] フィールドに 16 進数値で ID を入力します。

フィールド	説明
セキュリティ レベル（Security Level）	ドロップダウン リスト ボックスからユーザに対する適切なセキュリティ レベルを選択します。 **noAuthNoPriv** 認証もプライバシーも設定しません。 **authNoPriv** 認証を設定しますが、プライバシーは設定しません。 **authPriv** 認証とプライバシーを設定します。
[ユーザ情報（User Information）] ペイン	ペインから、次のいずれかのタスクを実行し、通信先とユーザの間の関連付けを設定または解除します。 **1.** 新しいユーザを作成するには、[新規ユーザの作成（Create New User）] をクリックします。 **2.** 既存のユーザを変更するには、ユーザのオプション ボタンをクリックしてから、**[選択したユーザの更新（Update Selected User）]** をクリックします。 **3.** ユーザを削除するには、ユーザのオプションボタンをクリックしてから、**[選択したユーザの削除（Delete Selected User）]** をクリックします。 表示されるユーザは、通知先に設定したセキュリティ レベルに応じて変化します。
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードに通知先の設定を適用する場合は、このチェックボックスをオンにします。 これは、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。

MIB2 システム グループの設定

以下の手順で、MIB-II システム グループのシステム コンタクトおよびシステム ロケーションを設定します。たとえば、システムの連絡先として「管理者、555-121-6633」と入力し、システム ロケーションとして「San Jose, Bldg 23, 2nd floor」と入力することができます。この手順は、SNMP V1、V2、および V3 に対して使用できます。

手順

ステップ 1 Cisco Unified Serviceabilityで、**SNMP** > **SystemGroup** > **MIB2 システム グループ**を選択します。

ステップ 2 **サーバ** ドロップダウンで、ノードを 1 つ選択して、**移動**をクリックします。

ステップ 3 **システムの連絡先** および **システム ロケーション** フィールドの設定を完了します。

ステップ 4 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する** チェック ボックスをオンにします。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 **OK** をクリックして、SNMP マスター エージェント サービスを再起動します。

例

（注） フィールドの説明のヘルプは、以下を参照してください MIB2 システム グループの設定 （42 ページ）

（注） フィールドをクリアするには、**すべてクリア** をクリックします。**すべてクリア** をクリックした後、**保存**をクリックすると、該当の記録が削除されます。

MIB2 システム グループの設定

次の表で、MIB2 システム グループの構成時の設定について説明します。

表 *16 : MIB2* システム グループの構成時の設定

フィールド	説明
サーバ	ドロップダウン リスト ボックスからコンタクトを設定するサーバを選択し、[移動（Go）] をクリックします。
システム管理者（System Contact）	問題が発生したときに知らせる人を入力します。
システムの場所（System Location）	システム コンタクトとして識別される人の場所を入力します。
すべてのノードに適用（Apply to All Nodes）	システム設定をクラスタ内のすべてのノードに適用するには、このチェック ボックスをオンにします。 これは、Unified Communications Manager と IM and Presence Service クラスタにのみ適用されます。

CISCO-SYSLOG-MIB トラップ パラメータ

システムの CISCO-SYSLOG-MIB トラップ設定を行う場合は次のガイドラインを使用してください。

- SNMP Set 操作を使用して、clogsNotificationEnabled（1.3.6.1.4.1.9.9.41.1.1.2）を True に設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID を True に設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

- SNMP Set 操作を使用して clogMaxSeverity（1.3.6.1.4.1.9.9.41.1.1.3）値を設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID 値を設定します。

```
snmpset-c public-v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i
<value>
```

  <value> には重大度の数値を入力します。値が大きくなるほど、重大度は低くなります。値 1（緊急）は最も高い重大度を表し、値 8（デバッグ）は最も低い重大度を表します。Syslog Agent では、指定した値よりも大きいメッセージは無視されます。たとえば、すべての Syslog メッセージをトラップする場合は値 8 を使用します。

  重大度の値は次のとおりです。

  - 1: Emergency
  - 2：警報
  - 3：重大
  - 4：エラー
  - 5：警告
  - 6：通知
  - 7：情報
  - 8：デバッグ

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

（注） 指定されている Syslog バッファ サイズよりも大きいトラップ メッセージ データは、ロギング前に Syslog によって切り捨てられます。Syslog トラップ メッセージの長さの制限は 255 バイトです。

CISCO-CCM-MIB トラップ パラメータ

- SNMP Set 操作を使用して、ccmPhoneFailedAlarmInterval（1.3.6.1.4.1.9.9.156.1.9.2）を 30 ～ 3600 の範囲の値に設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID 値を設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

- SNMP Set 操作を使用して、ccmPhoneStatusUpdateAlarmInterval（1.3.6.1.4.1.9.9.156.1.9.4）を 30 ～ 3600 の範囲の値に設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID 値を設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
```

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

CISCO-UNITY-MIB トラップ パラメータ

Cisco Unity Connection のみ：Cisco Unity Connection SNMP エージェントはトラップ通知を有効化しませんが、トラップは Cisco Unity Connection アラームによってトリガーできます。Cisco Unity Connection のアラーム定義は、Cisco Unity Connection Serviceability の **[アラーム（Alarm）]** > **[定義（Definitions）]** 画面で確認できます。

CISCO-SYSLOG-MIB を使用してトラップ パラメータを設定できます。

関連トピック

CISCO-SYSLOG-MIB トラップ パラメータ （43 ページ）

SNMP Master Agent の再起動

すべての SNMP 設定を完了したら、SNMP Master Agent サービスを再起動します。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[コントロールセンター-ネットワークサービス（Control Center - Network Services）]** の順に選択します。

ステップ 2 **サーバ** を選択して、**移動**をクリックします。

ステップ 3 **SNMP Master Agent** を選択します。

ステップ 4 **[Restart（再起動）]** をクリックします。

SNMP トラップの設定

設定可能な SNMP トラップ設定を行うには、CLI コマンドを使用します。SNMP トラップの設定パラメータと推奨される設定のヒントは、CISCO-SYSLOG-MIB、CISCO-CCM-MIB、および CISCO-UNITY-MIB で提供されています。

SNMP トラップの設定

SNMP トラップを設定するには、以下の手順を実行します。

始める前に

SNMP 用のシステム設定詳細については、SNMP 設定タスク フロー （27 ページ）を参照してください。

SNMP コミュニティ ストリング（SNMP V1 または V2 の場合）あるいは SNMP ユーザ（SNMP V3 の場合）の **アクセス権限** が以下のいずれかに設定されていることを確認します。**ReadWriteNotify**、**ReadNotify**、**NotifyOnly**。

手順

ステップ 1 CLI にログインし、`utils snmp test` CLI コマンドを実行して、SNMP が実行されていることを確認します。

ステップ 2 SNMP トラップの生成 （45 ページ） に従って、SNMP トラップ を生成します（たとえば、ccmPhoneFailed または MediaResourceListExhausted トラップなど）。

ステップ 3 トラップが生成されない場合は、次の手順を実行します。

- Cisco Unified Serviceability で、**[アラーム（Alarm）] > [設定（Configuration）]** を選択し、[CM サービス（CM Services）] および [Cisco CallManager] を選択します。
- [すべてのノードに適用（Apply to All Nodes）] チェックボックスをオンにします。
- [ローカル Syslog（Local Syslogs）] で、[アラーム イベント レベル（Alarm Event Level）] ドロップダウン リスト ボックスを [情報（Informational）] に設定します。

ステップ 4 トラップを再現し、対応するアラームが CiscoSyslog ファイルに記録されるかどうかを確認します。

SNMP トラップの生成

ここでは、特定のタイプの SNMP トラップを生成するためのプロセスについて説明します。個別のトラップを生成するために、SNMP をサーバ上でセットアップし、実行する必要があります。SNMP トラップを生成するためのシステムのセットアップ方法については、SNMP トラップの設定 （45 ページ） の指示に従ってください。

（注） 個々のSNMPトラップの処理時間は、生成しようとしているトラップによって異なります。一部の SNMP トラップは、生成するために最大で数分がかかる場合があります。

表 *17 : SNMP* トラップの生成

SNMP トラップ	プロセス
ccmPhoneStatusUpdate	ccmPhoneStatusUpdate トラップをトリガーするには： **1.** ccmAlarmConfig Info mib テーブルで、ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 以上に設定します。 **2.** Cisco Unified Communications Manager Administration にログインします。 **3.** Unified Communications Manager に登録され、稼働中の電話機の場合は、電話機をリセットします。 電話の登録が解除されるので、再登録すると ccmPhoneStatusUpdate トラップが生成されます。
ccmPhoneFailed	ccmPhoneFailed トラップをトリガーするには： **1.** ccmAlarmConfigInfo mib テーブルで、ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) =30 以上に設定します。 **2.** Cisco Unified Communications Manager Administration で、電話の MAC アドレスを無効な値に変更します。 **3.** Cisco Unified Communications Manager Administration で、電話機の再登録を行います。 **4.** TFTP サーバ A を指すように電話を設定し、別のサーバに電話を差し込みます。
ccmGatewayFailed	ccmGatewayFailed SNMP トラップをトリガーするには： **1.** ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) が true に設定されていることを確認します。 **2.** Cisco Unified Communications Manager Administration で、ゲートウェイの MAC アドレスを無効な値に変更します。 **3.** ゲートウェイをリブートします。

SNMP トラップ	プロセス
ccmGatewayLayer2Change	レイヤ2がモニタされている動作中のゲートウェイ（MGCPバックホール ロードなど）で ccmGatewayLayer2Change トラップをトリガーするには： **1.** ccmAlarmConfig Info mib テーブルで、ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true に設定します。 **2.** Cisco Unified Communications Manager Administration で、ゲートウェイの MAC アドレスを無効な値に変更します。 **3.** ゲートウェイをリセットします。
MediaResourceListExhausted	MediaResourceListExhausted トラップをトリガーするには： **1.** Cisco Unified Communications Manager Administration で、標準会議ブリッジ リソース（CFB-2）のいずれかを含むメディア リソース グループを作成します。 **2.** 作成したメディア リソース グループを含むメディア リソース グループ リストを作成します。 **3.** [電話の設定] ウィンドウで、作成したメディア リソース グループ リストを、メディア リソース グループ リストに設定します。 **4.** IP Voice Media Streaming サービスを停止します。このアクションにより、ConferenceBridge リソース（CFB-2）が動作を停止します。 **5.** メディア リソース グループ リストを使用する電話で電話会議を行います。「使用可能な会議ブリッジがありません（No Conference Bridge available）」 というメッセージが電話画面に表示されます。
RouteListExhausted	RouteListExhausted トラップをトリガーするには： **1.** ゲートウェイを 1 つ含むルート グループを作成します。 **2.** 作成したルート グループを含むルート グループ リストを作成します。 **3.** ルート グループ リストを使用してコールをルーティングする固有のルート パターンを作成します。 **4.** ゲートウェイの登録を解除します。 **5.** いずれかの電話から、ルート パターンに一致する番号に電話をかけます。

SNMP トラップ	プロセス
MaliciousCallFailed	MaliciousCallFailed トラップをトリガーするには： **1.** すべての使用可能な「MaliciousCall」ソフトキーを含むソフトキー テンプレートを作成します。 **2.** 新しいソフトキーテンプレートをネットワークの電話に割り当てて、電話をリセットします。 **3.** 電話間で電話をかけます。 **4.** コール中に、「MaliciousCall」ソフトキーを選択します。
ccmCallManagerFailed	CallManager 障害アラームは、内部エラーが発生すると生成されます。内部エラーには、CPU の不足による内部スレッドの終了、16 秒を超える CallManager サーバの停止、タイマーの問題などがあります。このアラームを手動で生成することはできません。 （注） ccmCallManagerFailed アラームまたはトラップを生成して CallManager サービスをシャット ダウンし、コア ファイルを生成します。混乱を避けるために、コア ファイルはすぐに削除することを推奨します。
トラップとしての syslog メッセージ	特定の重大度を超える syslog メッセージをトラップとして受信するには、clogBasic テーブルで次の 2 つの MIB オブジェクトを設定します。 **1.** clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2) を true（1）に設定します。デフォルト値は false（2）です。例：snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 **2.** clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) を、トラップを生成するレベルよりも大きいレベルに設定します。デフォルト値は警告（5）です。 設定された重大度レベル以下のアラーム重大度を持つすべての syslog メッセージがトラップとして送信されます。例：snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

SNMP トレースの設定

Unified Communications Manager の場合、Cisco CallManager SNMP エージェントのトレースを設定するには、Cisco Unified Serviceability の [トレース設定] ウィンドウで、[パフォーマンスおよびモニタリング サービス] サービス グループの [Cisco CallManager SNMP サービス] を選択しま

す。デフォルトの設定は、すべてのエージェントに対して存在します。Cisco CDP Agent および Cisco Syslog Agent の場合、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』に従って、CLI を使用してトレース設定を変更します。

Cisco Unity Connection の場合、Cisco Unity Connection SNMP エージェントのトレースを設定するには、Cisco Unity Connection Serviceability の [トレース設定（Trace Configuration）] ウィンドウで Connection SNMP エージェントのコンポーネントを選択します。

SNMP のトラブルシューティング

トラブルシューティングのヒントについては、この項を参照してください。すべての機能サービスとネットワーク サービスが動作していることを確認してください。

問題

システムから MIB をポーリングできない

この状態は、コミュニティ ストリングまたは SNMP ユーザがシステム上に設定されていないか、システム上に設定されているものと一致しないことを意味します。デフォルトでは、コミュニティ ストリングまたはユーザはシステムに設定されていません。

解決方法

SNMP の設定ウィンドウを使用して、コミュニティ ストリングまたは SNMP ユーザがシステム上に適切に設定されているかどうかを確認します。

問題

システムから通知を受信できない。

この状態は、通知の宛先がシステム上に正しく設定されていないことを意味します。

解決方法

[通知先（Notification Destination）]（V1/V2c または V3）設定ウィンドウで、通知の宛先を正しく設定したことを確認します。