SNMP モニタリングの設定

ここでは、Simple Network Management Protocol（SNMP）トラップ、受信者、コミュニティ ストリング、グループの関連性、ユーザ セキュリティ モデル グループ、ユーザ アクセス権を設定する方法について説明します。

(注) この章では、ネットワークに存在する WAAS Central Manager と WAE を総称する用語として「Cisco WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（Cisco Network Modules-WAE ファミリのデバイス）、および WAAS を実行している Cisco Services Ready Engine サービス モジュール（SRE-SM）を指します。

この章の内容は、次のとおりです。

SNMP の概要

SNMP は、SNMP エージェントからの Cisco WAAS デバイスの外部モニタリングを可能にする、相互運用可能な標準ベースのプロトコルです。

SNMP-managed ネットワークは、次の主要コンポーネントで構成されます。

- 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上に存在しているネットワーク ノードです。管理対象デバイスには、ルータ、アクセス サーバ、スイッチ、ブリッジ、ハブ、コンピュータ ホスト、プリンタなどがあります。WAAS ソフトウェアを実行している WAAS デバイスごとに SNMP エージェントがあります。
- SNMP エージェント：管理対象デバイスに存在するソフトウェア モジュールです。エージェントにはローカルの管理情報が含まれ、その情報を SNMP と互換性のある形式に変換します。SNMP エージェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントは、トラップ、つまり特定イベントの通知を管理システムに送信することもできます。
- 管理ステーション：SNMP ホストと呼ぶこともあります。管理ステーションは、SNMP を使用して SNMP エージェントに SNMP Get 要求を送信して、WAAS デバイスから情報を取得します。管理対象デバイスは管理情報を収集して保存し、SNMP を使用してこの情報を管理ステーションで使用できるようにします。

事前に、SNMP 管理アプリケーションが管理ステーションで展開されていないと、この SNMP 情報にはアクセスできません。この SNMP 管理ステーションは、SNMP を使用して SNMP Get 要求をデバイス エージェントに送信して WAAS デバイスから情報を取得するため、SNMP ホストと呼ばれています。

ここでは、次の内容について説明します。

SNMP 通信プロセス

WAAS デバイス上の SNMP 管理ステーションと SNMP エージェントは、SNMP を使用して次のように通信を行います。

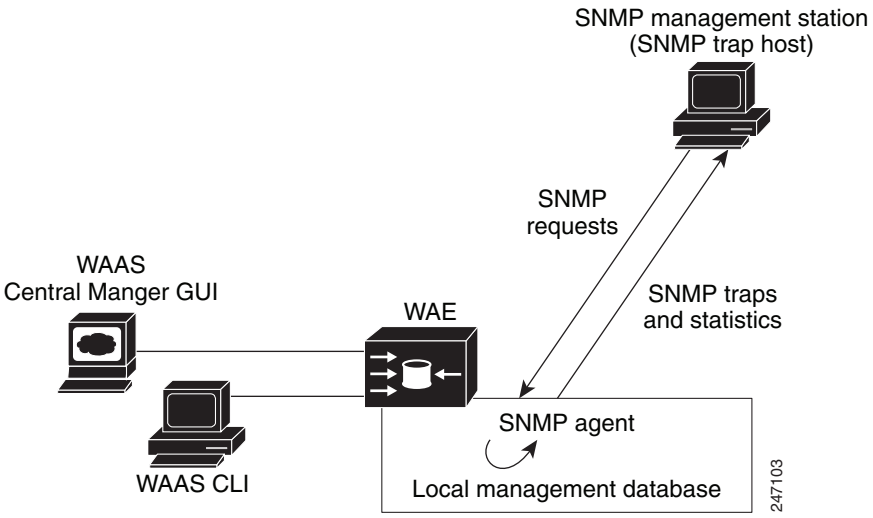
1. SNMP 管理ステーション（SNMP ホスト）は SNMP を使用して、WAAS デバイスの情報を要求します。
2. このような SNMP 要求を受信すると、WAAS デバイス上の SNMP エージェントは、各デバイスの情報が含まれるテーブルにアクセスします。このテーブル、またはデータベースが、MIB と呼ばれます。

（注）　WAAS デバイス上の SNMP エージェントは、異常状態にある SNMP ホストとの通信だけを開始します。そのホストに送信する必要があるトラップが発生すると、通信を開始します。このトピックの詳細については、SNMP トラップの有効化を参照してください。

3. MIB 内の特定の情報を検索した後、このエージェントは SNMP を使用して情報を SNMP 管理ステーションに送信します。

図 16-1 に、個々の WAAS デバイスに対するこれらの SNMP 動作を示します。

図 16-1　Cisco WAAS ネットワークの SNMP コンポーネント



サポートされている SNMP バージョン

WAAS ソフトウェアは、次の SNMP のバージョンをサポートします。

- バージョン 1（SNMPv1）：SNMP の初期の実装です。この機能の詳細については、RFC 1157 を参照してください。
- バージョン 2（SNMPv2c）：SNMP の 2 番めのリリースで、RFC 1902 に規定されています。データ タイプ、カウンタ サイズ、およびプロトコル動作に追加があります。
- バージョン 3（SNMPv3）：最新バージョンの SNMP で、RFC 2271 ～ RFC 2275 に規定されています。

WAAS ソフトウェアを実行する各シスコ デバイスには、SNMP プロトコルを使用してデバイスの設定とアクティビティに関する情報を通信するために必要なソフトウェアが含まれています。

SNMP セキュリティ モデルおよびセキュリティ レベル

SNMPv1 および SNMPv2c には、SNMP パケット トラフィックの機密性を保持するためのセキュリティ（つまり、認証またはプライバシー）機能がありません。その結果、ネットワークのパケットを検出することができ、SNMP コミュニティ ストリングが危険にさらされるリスクが軽減されます。

SNMPv1 および SNMPv2c のセキュリティ上の欠点を解決するために、SNMPv3 では、ネットワークを経由するパケットを認証および暗号化することで、WAAS デバイスへの安全なアクセスを実現しています。WAAS ソフトウェアの SNMP エージェントは、SNMPv3 はもちろん、SNMPv1 と SNMPv2c もサポートします。

SNMPv3 で提供されるセキュリティ機能は、次のとおりです。

- メッセージの完全性：伝送中にパケットが一切妨害されていないことを保証します。
- 認証：有効な送信元からのメッセージであるかどうかを判別します。
- 暗号化：パケットの内容をスクランブルして許可されていない送信元から見えないようにします。

SNMPv3 は、セキュリティ モデルだけでなく、セキュリティ レベルも備えています。セキュリティ モデルは、ユーザと、ユーザが所属するグループに対して設定される認証プロセスです。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットの処理時に使用されるセキュリティ プロセスが決まります。SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。

表 16-1 に、セキュリティ モデルとセキュリティ レベルの組み合わせを示します。

表 16-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	プロセス
v1	noAuthNoPriv	コミュニティ ストリング	No	ユーザ認証の照合にコミュニティ ストリングを使用します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	ユーザ認証の照合にコミュニティ ストリングを使用します。
v3	noAuthNoPriv	Username	No	ユーザ認証の照合にユーザ名を使用します。
v3	AuthNoPriv	Message Digest 5（MD5）または Secure Hash Algorithm（SHA）	No	Hash-Based Message Authentication Code（HMAC）-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。
v3	AuthPriv	MD5 または SHA	Yes	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。暗号ブロック連鎖（CBC）- データ暗号規格 56 ビット（DES-56）に基づく、DES-56 暗号化（パケット認証）を提供します。

SNMPv3 エージェントは、次のモードで使用できます。

- noAuthNoPriv モード（パケットに対してオンになっているセキュリティ メカニズムはありません）
- AuthNoPriv モード（プライバシー アルゴリズム（DES-56）を使用して暗号化する必要がないパケット用）
- AuthPriv モード（暗号化する必要があるパケット用。プライバシーを保持するには、パケットに対して認証を実行する必要があります）

SNMPv3 を使用すれば、ユーザは、データが改ざんされるおそれを抱くことなく、SNMP エージェントから管理情報を安全に収集できます。また、コンテンツ エンジンの設定を変更する SNMP 設定パケットなどの機密情報を暗号化し、内容がネットワーク上に公開されるのを防ぐことができます。グループベースの管理モデルでは、さまざまなユーザが異なるアクセス特権で同じ SNMP エージェントにアクセスできます。

サポートされる MIB

この項では、WAAS がサポートしているシスコ固有の MIB について説明します。MIB は、アルファベット順に表示されます。

- CISCO-APPNAV-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONTENT-ENGINE-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-PROCESS-MIB
- CISCO-SMI
- CISCO-WAN-OPTIMIZATION-MIB
- ENTITY-MIB
- EVENT-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- MIB-II
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMPv2-MIB
- SNMP-VACM-MIB

CISCO-APPNAV-MIB

この MIB は、AppNav オブジェクトに関する情報を提供します。次のサービス コンテンツ オブジェクトは、WAAS デバイスが AppNav コントローラ モードの場合にサポートされます。

- cAppNavServContextIndex
- cAppNavServContextName
- cAppNavServContextCurrOpState
- cAppNavServContextLastOpState
- cAppNavServContextIRState
- cAppNavServContextJoinState

次の AppNav コントローラ のグループ オブジェクトがサポートされます。

- cAppNavACGIndex
- cAppNavACGName
- cAppNavACGServContextName

次の WAAS ノードのグループ オブジェクトがサポートされます。

- cAppNavSNGIndex
- cAppNavSNGName
- cAppNavSNGServContextName

次の AppNav コントローラ のオブジェクトがサポートされます。

- cAppNavACIndex
- cAppNavACIpAddrType
- cAppNavACIpAddr
- cAppNavACServContextName
- cAppNavACACGName
- cAppNavACCurrentCMState

次の WAAS ノードのオブジェクトがサポートされます。

- cAppNavSNIndex
- cAppNavSNIpAddrType
- cAppNavSNIpAddr
- cAppNavSNServContextName
- cAppNavSNSNGName
- cAppNavSNCurrentCMState

CISCO-CDP-MIB

この MIB は、ローカル インターフェイスの ifIndex 値を表示します。リピータ ポートに ifIndex 値が割り当てられていない 802.3 リピータでは、この値はポートの固有値であり、リピータでサポートされる ifIndex 値より大きくなります。この例では、特定のポートが cdpInterfaceGroup と cdpInterfacePort の対応する値によって示されています。この場合、これらの値は、RFC 1516 のグループ番号値とポート番号値に対応します。

CISCO-CONFIG-MAN-MIB

この MIB は、さまざまな位置に存在する設定データのモデルを表します。

- running：実行中のシステムによって使用中
- terminal：端末として接続されているハードウェアに保存
- local：NVRAM またはフラッシュ メモリにローカルに保存済み
- remote：ネットワーク上のサーバに保存済み

この MIB には、設定に明確に関連する操作のみが含まれています。ただし、一部のシステム機能は一般的なファイルの保存と転送に使用できます。

CISCO-CONTENT-ENGINE-MIB

これは、米国シスコの Cisco WAE デバイス用の MIB モジュールです。この MIB の次のオブジェクトがサポートされています。

- cceAlarmCriticalCount
- cceAlarmMajorCount

- cceAlarmMinorCount
- cceAlarmHistTable

CISCO-ENTITY-ASSET-MIB

この MIB は、entPhysicalTable-ENTITY-MIB（RFC 2037）の資産情報項目をモニタします。この MIB は、entPhysicalTable-ENTITY-MIB に表示される関連するエンティティの注文可能製品番号、シリアル番号、ハードウェア リビジョン、製造番号およびリビジョン、ファームウェア ID およびリビジョン（存在する場合）およびソフトウェア ID およびリビジョン（存在する場合）を表示します。

このデータが使用できないエンティティは、この MIB に表示されません。この MIB の表にはわずかな情報しか取り込まれません。したがって、特定の時点に特定のエンティティの変数が存在しない場合があります。たとえば、電源がオフのモジュールを表す行は、ソフトウェア ID（ceAssetSoftwareID）とリビジョン（ceAssetSoftwareRevision）の値を持たないことがあります。同様に、電源モジュールは、表にファームウェアやソフトウェア情報が表示されません。

データに他の項目がエンコードされている可能性がありますが（たとえば、シリアル番号に製造日）、すべてのデータ項目が単一のものと見なされます。項目を分解したり、項目を構文解析しないでください。文字列の等価および非等価演算だけを使用してください。

CISCO-PROCESS-MIB

CISCO-PROCESS-MIB は、デバイスのメモリおよび CPU 使用率を表示し、アクティブなシステム プロセスを示します。CPU 使用率は、システムがどのくらいビジーであるかに関するステータスを示します。数字は最長アイドル時間に対する現在のアイドル時間の割合です。（この情報はあくまでも推定値です）。この MIB の次のオブジェクトがサポートされます。

- cpmCPUTotal1minRev：過去 1 分間でシステムがどの程度ビジーだったかを示す全体的な CPU 使用率を表示します。
- cpmCPUTotal5minRev：過去 5 分間でシステムがどの程度ビジーだったかを示す全体的な CPU 使用率を表示します。

CISCO-SMI

これは管理情報構造（SMI）の MIB モジュールです。この MIB では何も照会できません。これは Cisco MIB の構造を説明しています。

CISCO-WAN-OPTIMIZATION-MIB

この MIB は、最適化およびアプリケーション アクセラレータに関連するステータスおよび統計に関する情報を提供します。

次の転送フローの最適化（TFO）統計オブジェクトがサポートされます。

- cwoTfoStatsTotalOptConn
- cwoTfoStatsActiveOptConn
- cwoTfoStatsMaxActiveConn
- cwoTfoStatsActiveOptTCPPlusConn
- cwoTfoStatsActiveOptTCPOnlyConn
- cwoTfoStatsActiveOptTCPPrepConn
- cwoTfoStatsActiveADConn

- cwoTfoStatsReservedConn
- cwoTfoStatsPendingConn
- cwoTfoStatsActivePTConn
- cwoTfoStatsTotalNormalClosedConn
- cwoTfoStatsResetConn
- cwoTfoStatsLoadStatus

次の一般アプリケーション アクセラレータ統計オブジェクトがサポートされます。

- cwoAoStatsName
- cwoAoStatsIsConfigured
- cwoAoStatsIsLicensed
- cwoAoStatsOperationalState
- cwoAoStatsStartUpTime
- cwoAoStatsLastResetTime
- cwoAoStatsTotalHandledConn
- cwoAoStatsTotalOptConn
- cwoAoStatsTotalHandedOffConn
- cwoAoStatsTotalDroppedConn
- cwoAoStatsActiveOptConn
- cwoAoStatsPendingConn
- cwoAoStatsMaxActiveOptConn
- cwoAoStatsLoadStatus
- cwoAoStatsBwOpt

次のサーバ メッセージ ブロック（SMB）アプリケーション アクセラレータ統計情報がサポートされます。

- cwoAoSmbxStatsBytesReadCache
- cwoAoSmbxStatsBytesWriteCache
- cwoAoSmbxStatsBytesReadServer
- cwoAoSmbxStatsBytesWriteServer
- cwoAoSmbxStatsBytesReadClient
- cwoAoSmbxStatsBytesWriteClient
- cwoAoSmbxStatsProcessedReqs
- cwoAoSmbxStatsActiveReqs
- cwoAoSmbxStatsTotalRemoteReqs
- cwoAoSmbxStatsTotalLocalReqs
- cwoAoSmbxStatsRemoteAvgTime
- cwoAoSmbxStatsLocalAvgTime
- cwoAoSmbxStatsMDCacheHitCount
- cwoAoSmbxStatsMDCacheHitRate

- cwoAoSmbxStatsMaxRACacheSize
- cwoAoSmbxStatsMaxMDCacheSize
- cwoAoSmbxStatsRAEvictedAge
- cwoAoSmbxStatsRTT
- cwoAoSmbxStatsTotalRespTimeSaving
- cwoAoSmbxStatsOpenFiles
- cwoAoSmbxStatsTotalFilesInRACache
- cwoAoSmbxStatsRdL4SignWANBytes
- cwoAoSmbxStatsWrL4SignWANBytes
- cwoAoSmbxStatsRdSignLANBytes
- cwoAoSmbxStatsWrSignLANBytes

次の HTTP アプリケーション アクセラレータ統計オブジェクトがサポートされます。

- cwoAoHttpxStatsTotalSavedTime
- cwoAoHttpxStatsTotalRTT
- cwoAoHttpxStatsTotalMDCMTime
- cwoAoHttpxStatsEstSavedTime
- cwoAoHttpxStatsTotalSPSessions
- cwoAoHttpxStatsTotalSPPFSessions
- cwoAoHttpxStatsTotalSPPFObjects
- cwoAoHttpxStatsTotalSPRTTSaved
- cwoAoHttpxStatsTotalSPPFMissTime

次の Message Application Programming Interface（MAPI）アプリケーション アクセラレータ統計オブジェクトがサポートされます。

- cwoAoMapixStatsUnEncrALRT
- cwoAoMapixStatsUnEncrARRT
- cwoAoMapixStatsTotalUnEncrLRs
- cwoAoMapixStatsTotalUnEncrRRs
- cwoAoMapixStatsUnEncrAvgRedTime
- cwoAoMapixStatsEncrALRT
- cwoAoMapixStatsEncrARRT
- cwoAoMapixStatsTotalEncrLRs
- cwoAoMapixStatsTotalEncrRRs
- cwoAoMapixStatsEncrAvgRedTime

次のネットワーク ファイル システム（NFS）アプリケーション アクセラレータ統計オブジェクトがサポートされます。

- cwoAoNfsxStatsALRT
- cwoAoNfsxStatsARRT
- cwoAoNfsxStatsTotalLRs

- cwoAoNfsxStatsTotalRRs
- cwoAoNfsxStatsEstTimeSaved

次のアプリケーション統計オブジェクトがサポートされます。

- cwoAppStatsAppName
- cwoAppStatsOriginalBytes
- cwoAppStatsOptimizedBytes
- cwoAppStatsPTBytes

次の最適化ポリシー マップ統計オブジェクトがサポートされます。

- cwoPmapStatsType
- cwoPmapStatsName
- cwoPmapStatsDescr
- cwoPmapStatsTotalConns
- cwoPmapStatsTotalBytes
- cwoPmapStatsTotalPTConns
- cwoPmapStatsTotalPTBytes

次の最適化クラス マップ統計オブジェクトがサポートされます。

- cwoCmapStatsType
- cwoCmapStatsName
- cwoCmapStatsDescr
- cwoCmapStatsTotalConns
- cwoCmapStatsTotalBytes
- cwoCmapStatsTotalPTConns
- cwoCmapStatsTotalPTBytes

次の最適化 DRE キャッシュ統計オブジェクトがサポートされます。

- cwoDreCacheStatsStatus
- cwoDreCacheStatsAge
- cwoDreCacheStatsTotal
- cwoDreCacheStatsUsed
- cwoDreCacheStatsDataUnitUsage
- cwoDreCacheStatsReplacedOneHrDataUnit
- cwoDreCacheStatsDataUnitAge
- cwoDreCacheStatsSigblockUsage
- cwoDreCacheStatsReplacedOneHrSigblock
- cwoDreCacheStatsSigblockAge

次の最適化 DRE パフォーマンス統計オブジェクトがサポートされます。

- cwoDrePerfStatsEncodeCompressionRatio
- cwoDrePerfStatsEncodeCompressionLatency
- cwoDrePerfStatsEncodeAvgMsgSize

- cwoDrePerfStatsDecodeCompressionRatio
- cwoDrePerfStatsDecodeCompressionLatency
- cwoDrePerfStatsDecodeAvgMsgSize

次の最適化 Akamai Connect パフォーマンス統計オブジェクトがサポートされます。

- cwoAoHttpxStatsAKC
- cwoAoHttpxStatsAKCBypassEntry
- cwoAoHttpxStatsAKCStdEntry
- cwoAoHttpxStatsAKCBasicEntry
- cwoAoHttpxStatsAKCAdvEntry
- cwoAoHttpxStatsAKCTotalEntry

ENTITY-MIB

これは、1 つの SNMP エージェントがサポートする複数の論理エンティティを表すための MIB モジュールです。この MIB は、RFC 2737 で文章化されています。この MIB の次のグループがサポートされています。

- entityPhysicalGroup
- entityLogicalGroup

entConfigChange 通知がサポートされています。

EVENT-MIB

この MIB は、ネットワーク管理目的でイベント トリガーと処理を定義します。MIB は RFC 2981 として公開されます。

HOST-RESOURCES-MIB

この MIB は、ホスト システムを管理します。「ホスト」という用語は、インターネットに接続されている他の類似したコンピュータと通信する、任意のコンピュータを意味します。HOST-RESOURCES-MIB は、主要な機能が通信サービスであるデバイス（ターミナル サーバ、ルータ、ブリッジ、モニタリング機器）に必ずしも適用されるとは限りません。この MIB は、すべてのインターネット ホスト（たとえば、UNIX のバリエーションを実行するパーソナル コンピュータやシステム）に共通する属性を提供します。この MIB の次のオブジェクトはサポートされていません。

- HrPrinterEntry
- hrSWOSIndex
- hrSWInstalledGroup

IF-MIB

この MIB は、64 ビットのインターフェイス カウンタを含み、インターフェイス関連の統計情報のクエリーをサポートします。これらのカウンタにはデバイスのインターフェイスで送受信されたオクテット、ユニキャスト、マルチキャスト、およびブロードキャスト パケットが含まれます。ifCounterDiscontinuityTime を除き、ifXEntry のすべてのオブジェクトがサポートされています。この MIB は、RFC 2233 で文章化されています。

ループバック インターフェイスの情報は報告されません。

IP-MIB

この MIB モジュールは IP および ICMP の実装です（IP ルートの管理を除く）。

IP-FORWARD-MIB

MIB モジュールは CIDR マルチパス IP ルートの表示用です。

MIB-II

MIB-II はインターネット標準 MIB です。MIB-II は、RFC 1213 に規定され、TCP/IP に基づくインターネットのネットワーク管理プロトコル用です。この MIB は、ダウンロード サイトの v1 ディレクトリの RFC1213-MIB ファイルにあります（他の MIB は v2 ディレクトリにあります）。この MIB の次のオブジェクトはサポートされていません。

- ifInUnknownProtos
- ifOutNUcastPkts
- ipRouteAge
- TcpConnEntry group
- egpInMsgs
- egpInErrors
- egpOutMsgs
- egpOutErrors
- EgpNeighEntry group
- egpAs
- atTable、
- ipRouteTable

SNMP-FRAMEWORK-MIB

この MIB は、RFC 2571 で文章化されています。

SNMP-NOTIFICATION-MIB

この MIB は、RFC 3413 で文章化されています。

SNMP-TARGET-MIB

この MIB は、RFC 3413 で文章化されています。

SNMP-USM-MIB

この MIB は、RFC 2574 で文章化されています。

SNMPv2-MIB

この MIB は、RFC 1907 で文章化されています。WAAS では、この MIB の次の通知がサポートされています。

- coldStart
- linkUp

- linkDown
- authenticationFailure

SNMP-VACM-MIB

この MIB は、RFC 2575 で文章化されています。

MIB ファイルのダウンロード

WAAS ソフトウェアが稼働しているデバイスでサポートされるほとんどの MIB について、MIB ファイルを次の Cisco FTP サイトからダウンロードできます。

ftp://ftp.cisco.com/pub/mibs/v2

RFC1213-MIB ファイル（MIB-II 用）を次の Cisco FTP サイトからダウンロードできます。

ftp://ftp.cisco.com/pub/mibs/v1

それぞれの MIB で定義される MIB オブジェクトは、上記の FTP サイトの MIB ファイルで説明されており、明確です。

WAAS デバイスでの SNMP エージェントの有効化

デフォルトでは、WAAS デバイス上の SNMP エージェントが無効になっており、SNMP コミュニティ ストリングは定義されていません。SNMP コミュニティ ストリングは、WAAS デバイス上の SNMP エージェントへアクセスするときに、認証用のパスワードとして使用されます。認証されるには、WAAS デバイスに送信された SNMP メッセージの Community Name フィールドが、WAAS デバイスに定義された SNMP コミュニティ ストリングに一致している必要があります。

デバイスに SNMP コミュニティ ストリングを定義すると、WAAS デバイス上の SNMP エージェントが有効になります。WAAS Central Manager GUI を使用すると、デバイスまたはデバイス グループに SNMP コミュニティ ストリングを定義できます。

SNMP 要求に SNMPv3 プロトコルが使用されている場合は、次のステップで、SNMP ユーザ アカウントを定義します。このアカウントは、SNMP を使用して WAAS デバイスにアクセスするために使用できます。WAAS デバイスで SNMPv3 ユーザ アカウントを作成する方法の詳細については、SNMP ユーザの作成を参照してください。

SNMP を設定するためのチェックリスト

表 16-2 で、WAAS デバイスまたはデバイス グループで SNMP モニタリングを有効にするためのプロセスについて説明します。

表 16-2　　SNMP を設定するためのチェックリスト

タスク	追加情報と手順
1. SNMP モニタリングの準備をする。	詳細については、SNMP モニタリングの準備を参照してください。
2. 有効にしたい SNMP トラップを選択する。	WAAS Central Manager は、WAAS デバイスまたはデバイス グループで有効にできるさまざまなトラップを提供しています。 詳細については、SNMP トラップの有効化を参照してください。追加のトラップを定義するには、「ユーザ定義のトラップを生成するための SNMP トリガーの定義」セクション（ 16-17 ページ）を参照してください。

表 16-2　SNMP を設定するためのチェックリスト（続き）

タスク	追加情報と手順
3. SNMP トラップを受信する SNMP ホストを指定する。	WAAS デバイスまたはデバイス グループがトラップを送信する必要がある SNMP ホストを指定します。異なる WAAS デバイスが異なるホストへトラップを送信できるように、複数のホストを指定できます。 詳細については、SNMP ホストの指定を参照してください。
4. SNMP コミュニティ ストリングを指定する。	外部ユーザが MIB の読み取りまたは書き込みを実行できるように、SNMP コミュニティ ストリングを指定します。 詳細については、SNMP コミュニティ ストリングの指定を参照してください。
5. SNMP ビューを設定する。	SNMP グループを特定のビューに制限するには、グループに表示したい MIB サブツリーを指定するビューを作成する必要があります。 詳細については、SNMP ビューの作成を参照してください。
6. SNMP グループを作成する。	任意の SNMP ユーザを作成する、またはグループが特定の MIB サブツリーを表示するように制限したい場合は、SNMP グループを設定する必要があります。 詳細については、SNMP グループの作成を参照してください。
7. SNMP ユーザを作成する。	SNMP 要求に SNMPv3 プロトコルが使用されている場合は、SNMP を使用して WAAS デバイスにアクセスするために、少なくとも 1 つの SNMPv3 ユーザ アカウントを WAAS デバイスに定義する必要があります。 詳細については、SNMP ユーザの作成を参照してください。
8. SNMP 連絡先設定を構成する。	詳細については、SNMP 連絡先設定の構成を参照してください。

SNMP モニタリングの準備

WAAS ネットワークを SNMP モニタリング用に設定する前に、次の準備作業を完了します。

- WAAS デバイスが SNMP トラップを送信するために使用する SNMP ホスト（管理ステーション）を設定します。
- すべての WAAS デバイスがトラップを同じホストに送信するか、別のホストに送信するかを決定します。各 SNMP ホストの IP アドレスまたはホスト名を書き留めます。
- SNMP エージェントにアクセスするために使用するコミュニティ ストリングを入手します。
- グループ別にビューを制限できるように SNMP グループを作成するかどうかを決定します。
- 必要な追加の SNMP トラップを決定します。
- WAAS ネットワーク内のデバイス間でクロックを同期することが重要です。各 WAAS デバイス上で、クロックを同期するためにネットワーク タイム プロトコル（NTP）サーバが設定されていることを確認します。

SNMP トラップの有効化

WAAS デバイスが SNMP トラップを送信できるようにするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [General Settings] を選択します。[SNMP General Settings] ウィンドウが表示されます（図 16-2 を参照）。表 16-3 に、このウィンドウ内のフィールドについて説明します。

図 16-2　[SNMP General Settings] ウィンドウ

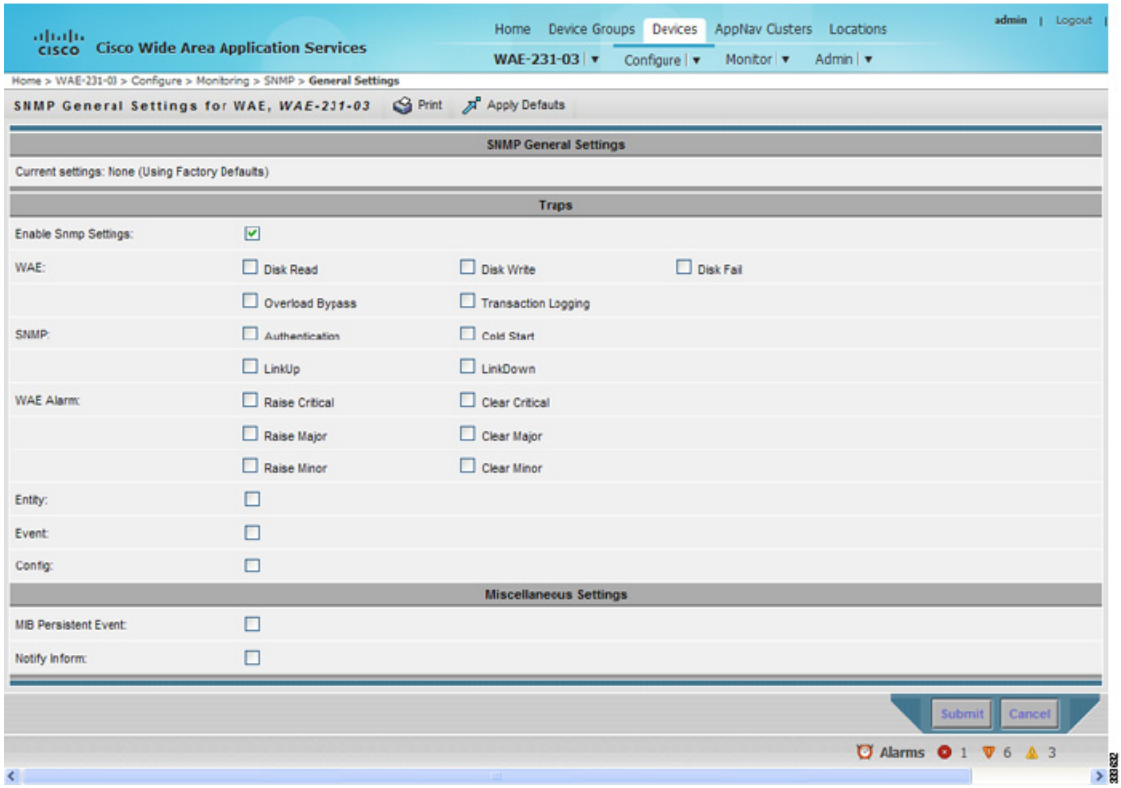


表 16-3　SNMP 一般設定

GUI パラメータ	機能
トラップ	
Enable Snmp Settings	SNMP トラップを有効にします。
WAE	SNMP WAE トラップを有効にします。 • [Disk Read]：ディスク読み取りエラー トラップを有効にします。 • [Disk Write]：ディスク書き込みエラー トラップを有効にします。 • [Disk Fail]：ディスク障害エラー トラップを有効にします。 • [Overload Bypass]：WCCP 過負荷迂回エラー トラップを有効にします。 • [Transaction Logging]：トランザクション ログ書き込みエラー トラップを有効にします。

表 16-3　　SNMP 一般設定 （続き）

GUI パラメータ	機能
SNMP	SNMP 固有トラップを有効にします。 • [Authentication]：認証トラップを有効にします。 • [Cold Start]：コールド スタート トラップを有効にします。 • [LinkUp]：リンク アップ トラップ。 • [LinkDown]：リンク ダウン トラップ。
WAE Alarm	SNMP アラーム トラップを有効にします。 • [Raise Critical]：クリティカル アラーム設定トラップを有効にします。 • [Clear Critical]：クリティカル アラーム消去トラップを有効にします。 • [Raise Major]：メジャー アラーム設定トラップを有効にします。 • [Clear Major]：メジャー アラーム消去トラップを有効にします。 • [Raise Minor]：マイナー アラーム設定トラップを有効にします。 • [Clear Minor]：マイナー アラーム消去トラップを有効にします。
Entity	SNMP エンティティ トラップを有効にします。
Event	イベント MIB を有効にします。
Config	CiscoConfigManEvent エラー トラップを有効にします。
その他の設定	
MIB Persistent Event	SNMP Event MIB の永続性を有効にします（このチェックボックスは、選択されているデバイスが Central Manager の場合には表示されません）。
Notify Inform	SNMP notify inform 要求を有効にします。inform 要求は、トラップより信頼性に優れていますが、ルータとネットワークのリソース使用量が増えます。 受信者がトラップを受信したときに受信確認を送信しないため、トラップの信頼性は低くなります。送信側は、トラップが受信されたかどうかを判断できません。ただし、inform 要求を受信する SNMP マネージャは、SNMP 応答でメッセージの受信を確認します。送信側が応答を受信しない場合、インフォーム要求を再び送信できます。したがって、情報が目的の宛先に到達する可能性が高まります。

ステップ 3　SNMP トラップを有効にするには、該当するチェックボックスを選択します。

ステップ 4　[Submit] をクリックします。

デフォルト設定またはデバイス グループ設定の適用後に保存されていない変更がある場合は、[Current Settings] の横に「Click Submit to Save」メッセージが赤で表示されます。また、[Reset] をクリックすると、すでに設定したウィンドウ設定に戻すことができます。[Reset] ボタンは、デフォルトまたはデバイス グループ設定を適用して現在のデバイス設定を変更し、まだ設定を送信していない場合だけ表示されます。

CLI から SNMP トラップを有効にするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用できます。

外部 SNMP サーバによる SNMP へのアクセスを制御するには、**snmp-server access-list** グローバル コンフィギュレーション コマンドを使用して SNMP ACL を適用します。

(注)　SNMP サーバ ACL を使用している場合は、ループバック インターフェイスを許可する必要があります。

(注)　[SNMP General Settings] ウィンドウからデバイス グループ設定を上書きする場合、Central Manager は SNMP コミュニティ、SNMP グループ、SNMP ユーザ、SNMP ビュー、および SNMP ホスト設定を削除します。この動作の確認が要求されます。

特別な設定に関連した他の MIB オブジェクトの追加 SNMP トラップを定義するには、ユーザ定義のトラップを生成するための SNMP トリガーの定義を参照してください。

ユーザ定義のトラップを生成するための SNMP トリガーの定義

特別な設定に関連した他の MIB オブジェクトの追加 SNMP トラップを定義するには、次の手順に従って、追加の SNMP トリガーを作成してください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [Trigger] を選択します。[SNMP Trigger List Entries] ウィンドウが表示されます。このウィンドウの列は、表 16-4 で示すパラメータと同じです。

ステップ 3　タスクバーで、[Create New SNMP Trigger List Entry] アイコンをクリックします。[Creating New SNMP Trigger] ウィンドウが表示されます。表 16-4 に、このウィンドウ内のフィールドについて説明します。

表 16-4　新しい SNMP トリガー設定の作成

GUI パラメータ	機能
Trigger Name	モニタする通知トリガーのカスタム定義名。
MIB Name	モニタするオブジェクトの MIB 変数名。
Wild Card	（任意）[MIB Name] 値がワイルドカードの場合、このチェックボックスを選択します。SNMP トリガーを編集するときは、このチェックボックスは無効になります。
Frequency	トリガー サンプルの間で待機する秒数（60 ～ 600）

表 16-4　新しいSNMP トリガー設定の作成 （続き）

GUI パラメータ	機能
Test	SNMP トラップを開始するのに使用するテスト。次のいずれかのテストを選択します。 • [absent]：最後のサンプリングで存在した指定の MIB オブジェクトが、現在のサンプリングでは存在しない。 • [equal]：指定された MIB オブジェクトの値が指定されたしきい値と等しい。 • [greater-than]：指定された MIB オブジェクトの値が、指定されたしきい値より高い。 • [less-than]：指定された MIB オブジェクトの値が、指定されたしきい値より低い。 • [on-change]：最後のサンプリング以降、指定された MIB オブジェクトの値が変更された。 • [present]：以前のサンプリングでは存在しなかった指定の MIB オブジェクトが、現在のサンプリングで存在する。 • [threshold]：MIB オブジェクトの最大しきい値と最小しきい値を設定する。
Sample Type	（任意）サンプル タイプ。次のとおりです。 • [absolute]：0 ～ 2147483647 の範囲内の固定整数値に対して、テストが評価されます。 • [delta]：現在のサンプリングと以前のサンプリングの間における MIB オブジェクトの値の変動に対して、テストが評価されます。
Threshold Value	MIB オブジェクトのしきい値。[Test] ドロップダウン リストで [absent]、[on-change]、または [present] が選択されると、このフィールドは使用されません。
MIB Var1 MIB Var2 MIB Var3	（任意）通知に追加する最大 3 つの代替 MIB 変数の名前。これらの名前の検証はサポートされないので、必ず正しい名前を入力してください。
Comments	トラップの説明

ステップ 4　上記のフィールドには、MIB 名、周期、テスト、サンプル タイプ、しきい値、および説明を入力します。

（注）　読み取り/書き込みの MIB オブジェクトと読み取り専用の MIB オブジェクトにのみ有効なトリガーを作成できます。読み取りと作成 MIB オブジェクトにトリガーを作成する場合は、1 データ フィードのポーリング サイクル後に Central Manager 設定から削除されます。

ステップ 5　[Submit] をクリックします。

新しい SNMP トリガーが [SNMP Trigger List] ウィンドウに表示されます。

[SNMP Trigger List Entries] ウィンドウの MIB 名の横にある [Edit] アイコンをクリックすると、SNMP トリガーを編集できます。

MIB 名の横にある Edit アイコンをクリックしてから、[Delete] タスクバー アイコンをクリックすると、SNMP トリガーを削除できます。

(注)　デフォルト SNMP トリガのいずれかを削除した場合、それはリロード後に復元されます。

(注)　WAE を以前のバージョンから 6.0 のバージョンにアップグレードすると、すべてのトリガーが削除されます。

Central Manager を 6.0 にアップグレードすると、すべてのデバイス グループ トリガーが、前のソフトウェア バージョンを実行する WAE（存在する場合）にコピーされ、その後すべてのデバイス グループ トリガーが削除されます。また、（バージョン 6.0 を実行する）Central Manager によって管理されている、（6.0 より前のバージョンを実行する）すべての WAE について、[Trigger Aggregate Settings] が False に設定されます。これにより、DG トリガーは、6.0 よりも前のバージョンを実行するどのデバイスにも適用されなくなります。

(注)　WAE を 6.0 からそれ以前のリリースにダウングレードする場合、すべての IPv6 の設定が削除されます。すべてのトリガーおよびモニタ ユーザ設定が削除されます。

CLI から SNMP トラップを定義するには、**snmp trigger** グローバル コンフィギュレーション コマンドを使用できます。

外部 SNMP サーバによる SNMP へのアクセスを制御するには、**snmp-server access-list** グローバル コンフィギュレーション コマンドを使用して SNMP ACL を適用します。

(注)　SNMP サーバ ACL を使用している場合は、ループバック インターフェイスを許可する必要があります。

SNMP トリガーの集約

個々の WAE デバイスは、カスタム SNMP トリガーを定義できます。また、他のカスタム SNMP トリガーが定義されているデバイス グループに所属することもできます。

[SNMP Trigger List Entries] ウィンドウ内の [Aggregate Settings] オプション ボタンは、個々のデバイスでの SNMP トリガーの集約方法を次のように制御します。

- デバイスの設定にそのデバイスとそれが所属するデバイス グループに定義されたすべてのカスタム SNMP トリガーを使用する場合は、[Yes] を選択します。
- デバイス自身に定義されたカスタム SNMP トリガーだけに制限する場合は、[No] を選択します。

設定を変更すると次のメッセージが表示されます。「This option will take effect immediately and will affect the device configuration.Do you wish to continue?」[OK] をクリックして作業を続行します。

SNMP ホストの指定

ホストは、作成順に表示されます。作成できる SNMP ホストの最大数は 4 です。

SNMP ホストを指定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [Host] を選択します。[SNMP Hosts] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Create New SNMP Host] アイコンをクリックします。[Creating New SNMP Host] ウィンドウが表示されます。表 16-5 に、このウィンドウ内のフィールドについて説明します。

表 16-5　SNMP ホスト設定

GUI パラメータ	機能
Trap Host	WAE から SNMP トラップ メッセージで送信される SNMP トラップ ホストのホスト名または IP アドレス。これは必須フィールドで、現在は IPv6 アドレスをサポートしています。
Community/User	WAE から SNMP トラップ メッセージで送信される SNMP コミュニティまたはユーザの名前（最大 64 文字）。これは必須フィールドです。
Authentication	SNMP トラップ動作の受信者へ通知を送信するために使用するセキュリティ モデル。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [No-auth]：セキュリティ メカニズムなしで通知を送信します。 • [v2c]：バージョン 2c セキュリティを使用して通知を送信します。 • [v3-auth]：SNMP バージョン 3 AuthNoPriv を使用して通知を送信します。 • [v3-noauth]：SNMP バージョン 3 NoAuthNoPriv を使用して通知を送信します。 • [v3-priv]：SNMP バージョン 3 AuthPriv を使用して通知を送信します。
Retry	inform 要求に許される再試行回数（1 ～ 10）。デフォルトは、2 回です。
Timeout	inform 要求のタイムアウト（1 ～ 1000 秒）。デフォルトは 15 秒です。

ステップ 4　SNMP トラップ ホストのホスト名または IP アドレス、SNMP コミュニティまたはユーザ名、通知を送信するためのセキュリティ モデル、および inform 要求の再試行回数とタイムアウトを入力します。

ステップ 5　[Submit] をクリックします。

CLI から SNMP ホストを指定するには、**snmp-server host** グローバル コンフィギュレーション コマンドを使用できます。

SNMP コミュニティ ストリングの指定

SNMP コミュニティ ストリングは、WAAS デバイスに存在する SNMP エージェントにアクセスするために使用するパスワードです。コミュニティ ストリングは、group と read-write の 2 種類あります。コミュニティ ストリングは、SNMP メッセージのセキュリティを強化します。

コミュニティ ストリングは、作成順に表示されます。作成できる SNMP コミュニティの最大数は 10 です。デフォルトでは、SNMP エージェントは無効で、コミュニティ ストリングは設定されていません。コミュニティ ストリングを設定すると、デフォルトですべてのエージェントへの読み取り専用アクセスが許可されます。

SNMP エージェントを有効にし、SNMP エージェントにアクセスできるコミュニティ ストリングを設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [Community] を選択します。[SNMP Community Strings] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Create New SNMP Community String] アイコンをクリックします。[Creating New SNMP Community String] ウィンドウが表示されます。表 16-6 に、このウィンドウ内のフィールドについて説明します。

表 16-6　SNMP コミュニティ設定

GUI パラメータ	機能
Community	WAE の SNMP エージェントにアクセスするときに認証用のパスワードとして使用するコミュニティ ストリング。認証されるには、WAE に送信された SNMP メッセージの「Community Name」フィールドが、ここで定義した SNMP コミュニティ ストリングに一致している必要があります。コミュニティ ストリングを入力すると、WAE 上の SNMP エージェントが有効になります。このフィールドには、最大 64 文字を入力できます。 これは必須フィールドです。
Group name/rw	コミュニティ ストリングが属するグループ。[Read/Write] オプションを使用すると、このコミュニティ ストリングに read または write グループを関連付けることができます。[Read/Write] オプションは、MIB サブツリーの一部へのアクセスだけを許可します。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [None]：コミュニティ ストリングに関連付けるグループ名を指定したくない場合は、このオプションを選択します。このオプションを選択すると、[Group Name] フィールドは無効のままになります。 • [Group]：グループ名を指定したい場合は、このオプションを選択します。 • [Read/Write]：コミュニティ ストリングに関連付けられたグループへの読み取り / 書き込みアクセスを許可したい場合は、このオプションを選択します。このオプションを選択すると、[Group Name] フィールドは無効のままになります。 これは必須フィールドです。

表 16-6　SNMP コミュニティ設定（続き）

GUI パラメータ	機能
Group Name	コミュニティ ストリングが属するグループの名前。このフィールドには、最大 64 文字を入力できます。このフィールドは、前のフィールドで [Group] オプションを選択した場合にだけ使用できます。

ステップ 4　適切なフィールドに、コミュニティ ストリングを入力し、グループへの読み取り/書き込みアクセスを許可するかどうかを選択し、グループ名を入力します。

ステップ 5　[Submit] をクリックします。

CLI からコミュニティ ストリングを設定するには、**snmp-server community** グローバル コンフィギュレーション コマンドを使用できます。

SNMP ビューの作成

ユーザのグループを特定の MIB ツリーを表示するように制限するには、WAAS Central Manager GUI を使用して SNMP ビューを作成する必要があります。ビューを作成したら、後続の項の説明に従って、このグループに属する SNMP グループと SNMP ユーザを作成する必要があります。

ビューは、作成順に表示されます。作成できるビューの最大数は 10 です。

バージョン 2 SNMP（SNMPv2）MIB ビューを作成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [View] を選択します。[SNMP Views] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Create New View] アイコンをクリックします。[Creating New SNMP View] ウィンドウが表示されます。表 16-7 に、このウィンドウ内のフィールドについて説明します。

表 16-7　SNMPv2 ビュー設定

GUI パラメータ	機能
Name	このビュー サブツリーのファミリ名を表す文字列（最大 64 文字）。ファミリ名は、ENTITY-MIB のような有効な MIB 名である必要があります。これは必須フィールドです。
Family	MIB のサブツリーを識別するオブジェクト ID（最大 64 文字）。これは必須フィールドです。
View Type	ビューから MIB ファミリを包含するか、除外するかを決定するビュー オプション。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [Included]：MIB ファミリをビューに入れます。 • [Excluded]：MIB ファミリをビューから除外します。

ステップ 4　適切なフィールドに、ビュー名、ファミリ名、およびビューの種類を入力します。

ステップ 5　[Submit] をクリックします。

ステップ 6　あとの項の説明に従って、このビューに割り当てる SNMP グループを作成します。

CLI から SNMP ビューを作成するには、**snmp-server view** グローバル コンフィギュレーション コマンドを使用できます。

SNMP グループの作成

任意の SNMP ユーザを作成する、またはユーザのグループが特定の MIB サブツリーを表示するように制限したい場合は、SNMP グループを設定する必要があります。

グループは、作成順に表示されます。作成できる SNMP グループの最大数は 10 です。

ユーザ セキュリティ モデル グループを定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [Group] を選択します。[SNMP Group Strings for WAE] ウィンドウが表示されます。

ステップ 3　タスクバーで、[Create New SNMP Group String] アイコンをクリックします。[Creating New SNMP Group String for WAE] ウィンドウが表示されます。表 16-8 に、このウィンドウ内のフィールドについて説明します。

表 16-8　SNMP グループ設定

GUI パラメータ	機能
Name	SNMP グループの名前。最大 64 文字を入力できます。これは必須フィールドです。
Sec Model	グループ用のセキュリティ モデル。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [v1]：バージョン 1 セキュリティ モデル（SNMP バージョン 1 [noAuthNoPriv]） • [v2c]：バージョン 2c セキュリティ モデル（SNMP バージョン 2 [noAuthNoPriv]） • [v3-auth]：ユーザ セキュリティ レベル SNMP バージョン 3 AuthNoPriv • [v3-noauth]：ユーザ セキュリティ レベル SNMP バージョン 3 noAuthNoPriv • [v3-priv]：ユーザ セキュリティ レベル SNMP バージョン 3 AuthPriv **（注）** SNMPv1 または SNMPv2c セキュリティ モデルに従って定義されたグループは、SNMP ユーザには関連付けないでください。それらは、コミュニティ ストリングだけに関連付ける必要があります。

表 16-8　SNMP グループ設定（続き）

GUI パラメータ	機能
Read View	エージェントの内容を表示できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。グループのユーザに読み取りアクセスを提供するには、ビューを指定する必要があります。 SNMP ビューを作成する方法については、SNMP ビューの作成を参照してください。
Write View	データを入力し、エージェントの内容を設定できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。 SNMP ビューを作成する方法については、SNMP ビューの作成を参照してください。
Notify View	notify、inform、または trap を指定できるビューの名前（最大 64 文字）。デフォルトで、ビューは定義されません。 SNMP ビューを作成する方法については、SNMP ビューの作成を参照してください。

ステップ 4　適切なフィールドに、SNMP グループ設定名、セキュリティ モデル、および読み取り、書き込み、および通知ビューの名前を入力します。

ステップ 5　[Submit] をクリックします。

ステップ 6　あとの項の説明に従って、この新しいグループに属する SNMP ユーザを作成します。

CLI から SNMP グループを作成するには、**snmp-server group** グローバル コンフィギュレーション コマンドを使用できます。

SNMP ユーザの作成

ユーザは、作成順に表示されます。作成できるユーザの最大数は 10 です。

SNMP エンジンにアクセスできるユーザを定義するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [User] を選択します。デバイスまたはデバイス グループ用の SNMP ユーザのリストが表示されます。

ステップ 3　タスクバーで、[Create New SNMP User] アイコンをクリックします。[Creating New SNMP User] ウィンドウが表示されます。表 16-9 に、このウィンドウ内のフィールドについて説明します。

表 16-9　SNMP ユーザ設定

GUI パラメータ	機能
Name	デバイスまたはデバイス グループにアクセスできるユーザの名前を表す文字列（最大 32 文字）。これは必須フィールドです。
Group	ユーザが属するグループの名前（最大 64 文字）。これは必須フィールドです。

表 16-9　SNMP ユーザ設定 （続き）

GUI パラメータ	機能
Remote SNMP ID	リモート SNMP エンティティのグローバル一意名識別子（10 ～ 64 文字）。SNMPv3 メッセージを WAE へ送信するには、WAE にリモート SNMP ID を持つ少なくとも 1 人のユーザを設定する必要があります。SNMP ID は、オクテット文字列形式で入力する必要があります。このフィールドに入力できるのは、16 進数文字とコロン（:）だけです。入力した文字列に何らかの色がついた場合、それはページの送信後に削除されます。
Authentication Algorithm	送信中の SNMP パケットの完全性を保証する認証アルゴリズム。ドロップダウン リストから、次のいずれかのオプションを選択します。 • [No-auth]：SNMP パケット用にセキュリティ メカニズムをオンにする必要がありません。 • [MD5]：ハッシュに基づくメッセージ認証コード MD5（HMAC-MD5）アルゴリズムに基づく認証を提供します。 • [SHA]：ハッシュに基づくメッセージ認証コード安全なハッシュ（HMAC-SHA）アルゴリズムに基づく認証を提供します。
Authentication Password	ユーザ認証（HMAC-MD5 または HMAC-SHA）パスワードを設定する文字列（最大 256 文字）。表示制限を超える場合、文字数が表示領域に合わせて調整されます。特殊文字のスペース、左一重引用符（`）、一重引用符（'）、二重引用符（"）、パイプ（|）、疑問符（?）は使用できません。 認証アルゴリズム用に [no-auth] オプションを選択した場合、このフィールドはオプションです。そうでない場合は、このフィールドに値を入力する必要があります。
Confirmation Password	確認用の認証パスワード。再入力するパスワードは、前のフィールドに入力したパスワードと同じである必要があります。
Private Password	SNMP エージェントが SNMP ホストからパケットを受信できるようにする認証（HMAC-MD5 または HMAC-SHA）パラメータを設定する文字列（最大 256 文字の英数字）。表示制限を超える場合、文字数が表示領域に合わせて調整されます。スペース、左一重引用符（`）、二重引用符（"）、パイプ（|）、疑問符（?）の特殊文字は使用できません。 **（注）** WAAS ソフトウェア バージョン 6.x 以降を使用する SNMPv3 ユーザの場合、プライベート パスワードは最小 8 文字、最大 256 文字の英数字である必要があります。
Confirmation Password	確認用のプライベート パスワード。再入力するパスワードは、前のフィールドに入力したパスワードと同じである必要があります。

ステップ 4　適切なフィールドに、ユーザ名、ユーザが属するグループ、ユーザが属するリモート エンティティのエンジン ID、SNMP トラフィックの改ざんから保護するために使用する認証アルゴリズム、ユーザ認証パラメータ、およびパケット用の認証パラメータを入力します。

ステップ 5　[Submit] をクリックします。

CLI から SNMP ユーザを作成するには、**snmp-server user** グローバル コンフィギュレーション コマンドを使用できます。

さらに、設定されたトリガーをモニタするためにモニタ ユーザを設定する場合、そのモニタ ユーザを [Monitor User Settings] ドロップダウン ボックスから選択します。

どの SNMP V3 ユーザでもモニタ ユーザとして設定できます。v3-private 以外の V3 認証を持つグループで作成されたすべての SNMP ユーザは、モニタ ユーザになる資格があります。モニタ ユーザは、その役割でいる間は削除できません。同様に、モニタ ユーザが対応するモニタ ユーザ グループで設定されている場合、そのグループも削除できません。

CLI からモニタ ユーザを作成するには、**snmp-server monitor user** グローバル コンフィギュレーション コマンドを使用できます。

SNMP 資産タグ設定の構成

CISCO-ENTITY-ASSET-MIB に値を作成する SNMP 資産タグ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [Asset Tag] を選択します。[SNMP Asset Tag Settings] ウィンドウが表示されます。

ステップ 3　[Asset Tag Name] フィールドに、資産タグの名前を入力します。

ステップ 4　[Submit] をクリックします。

CLI から SNMP 資産タグ設定を構成するには、**asset tag** グローバル コンフィギュレーション コマンドを使用できます。

SNMP 連絡先設定の構成

SNMP 連絡先設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [Contact Information] を選択します。[SNMP Contact Settings] ウィンドウが表示されます。

ステップ 3　提供されるフィールドに、連絡先の氏名と住所を入力します。

ステップ 4　[Submit] をクリックします。

CLI から SNMP 連絡先設定を構成するには、**snmp-server contact** グローバル コンフィギュレーション コマンドを使用できます。

SNMP トラップ ソース設定値の設定

SNMP トラップの送信元になるソース インターフェイスを設定するには、次の手順を実行します。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*] を選択します。（この設定は、デバイス グループではサポートされていません）。

ステップ 2　[Configure] > [Monitoring] > [SNMP] > [Trap Source] を選択します。[SNMP Trap Source Settings] ウィンドウが表示されます。

ステップ 3　[Trap Source] ドロップダウン リストから、トラップ ソースとして使用されるインターフェイスを選択します。使用可能な物理、スタンバイ、およびポート チャネル インターフェイスから、IP アドレスを持つものだけがリストに表示されます。vWAAS デバイスでは、IP アドレスが割り当てられた仮想インターフェイスがリストに表示されます。

（注）　トラップ ソースとして割り当てられたインターフェイスは、トラップ ソースとしての割り当てを解除するまでは削除できません。

ステップ 4　[Submit] をクリックします。

CLI から SNMP トラップ ソースの設定値を設定するには、**snmp-server trap-source** グローバル コンフィギュレーション コマンドを使用できます。