CHAPTER 14

SNMP の設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上でサポートされています。ASA 8.3(*x*) では、サポートされていません。

この章では、SNMP および SNMP トラップを使用するためのセンサーの設定方法について説明します。次の事項について説明します。

SNMP について

注意 センサーに SNMP トラップを送信させるには、シグニチャの設定時にイベント アクションとして [Request SNMP Trap] も選択する必要があります。

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。SNMP を使用すると、ネットワーク管理者は、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、ネットワークの拡大に対する計画を策定できます。

SNMP は単純な要求/応答プロトコルです。ネットワーク管理システムが要求を発行し、管理デバイスが応答を返します。この動作は、Get、GetNext、Set、Trap という 4 種類のプロトコル処理のいずれかを使用して実装されます。

SNMP によってセンサーをモニタリング用に設定できます。SNMP は、ネットワーク管理ステーションがスイッチ、ルータ、センサーなどの多くのタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。

SNMP トラップを送信するようにセンサーを設定できます。SNMP トラップを使用すると、エージェントは非送信請求 SNMP メッセージを使用して管理ステーションに重要なイベントを通知できます。

トラップで指示される通知には次の利点があります。マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。ソリューションは、送信要求を行わずに、管理対象デバイス上のエージェントごとにマネージャに通知することです。イベントのトラップと呼ばれるメッセージを送信することで、この処理を行います。

イベントの受信後、マネージャはイベントを表示し、イベントに基づいてアクションを実行できます。たとえば、イベントをさらによく把握するために、マネージャから、エージェントに直接ポーリングがかけられたり、関連する他のデバイス エージェントにポーリングがかけられたりする場合があります。

（注）　トラップで指示される通知を使用して不要な SNMP 要求を除くことで、ネットワークとエージェントのリソースを大幅に節約できます。ただし、SNMP ポーリングを完全には排除できません。SNMP 要求は、検出とトポロジ変更に必要です。また、管理対象デバイス エージェントは、デバイスに致命的な停止が生じた場合にはトラップを送信できません。

詳細情報

センサーに SNMP トラップを送信させる手順については、「シグニチャへのアクションの割り当て」（P.7-18）を参照してください。

一般的な SNMP コンフィギュレーションの設定

（注）　SNMP を使用するようセンサーを設定するには、管理者である必要があります。

[General Configuration] ペインを使用して、SNMP を使用するようセンサーを設定します。

フィールド定義

[General Configuration] ペインには、次のようなフィールドがあります。

- [Enable SNMP Gets/Sets]：オンにすると、SNMP の Get と Set が許可されます。
- [SNMP Agent Parameters]：SNMP エージェントのパラメータを設定します。
  - [Read-Only Community String]：読み取り専用アクセス用のコミュニティ ストリングを指定します。
  - [Read-Write Community String]：読み取りおよび書き込みアクセス用のコミュニティ ストリングを指定します。
  - [Sensor Contact]：センサーの担当者か窓口（またはその両方）を指定します。
  - [Sensor Location]：センサーの場所を指定します。
  - [Sensor Agent Port]：センサーの IP ポートを指定します。デフォルトは 161 です。
  - [Sensor Agent Protocol]：センサーの IP プロトコルを指定します。

    デフォルトは UDP です。

SNMP 汎用パラメータの設定

汎用 SNMP パラメータを設定するには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [SNMP] > [General Configuration] と選択します。

ステップ 3　SNMP をイネーブルにして SNMP 管理ワークステーションにセンサー SNMP エージェントに要求を発行させるには、[Enable SNMP Gets/Sets] チェックボックスをオンにします。

ステップ 4　SNMP エージェント パラメータを設定します。

SNMP 管理ワークステーションがセンサー SNMP エージェントから要求可能ないくつかの値があります。

a. [Read-Only Community String] フィールドに、読み取り専用コミュニティ ストリングを入力します。読み取り専用コミュニティ ストリングは、センサー SNMP エージェントの識別に役立ちます。

b. [Read-Write Community String] フィールドに、読み取りおよび書き込みコミュニティ ストリングを入力します。読み取りおよび書き込み専用コミュニティ ストリングは、センサー SNMP エージェントの識別に役立ちます。

（注） 管理ワークステーションは、センサー上に存在するセンサー SNMP エージェントに SNMP 要求を送信します。管理ワークステーションが要求を発行したとき、コミュニティ ストリングがセンサー上のものと一致しないと、センサーはこれを拒否します。

c. [Sensor Contact] フィールドに、センサー担当者のユーザ ID を入力します。

d. [Sensor Location] フィールドに、センサーの場所を入力します。

e. [Sensor Agent Port] フィールドに、センサー SNMP エージェントのポートを入力します。デフォルトの SNMP ポート番号は 161 です。

f. [Sensor Agent Protocol] ドロップダウン リストから、センサー SNMP エージェントが使用するプロトコルを選択します。デフォルト プロトコルは UDP です。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 5　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

SNMP トラップの設定

この項では、SNMP トラップを設定する方法について説明します。次の項目を取り上げます。

[Traps Configuration] ペイン

（注）　センサー上の SNMP トラップを設定するには、管理者である必要があります。

[Traps Configuration] ペインを使用して、センサーに SNMP トラップとトラップ宛先を設定します。SNMP トラップは通知の一種です。「重大」、「エラー」、「警告」といったイベントの種類に応じてトラップを送信するよう、センサーを設定します。

[Traps Configuration] ペインのフィールド定義

[Traps Configuration] ペインには、次のようなフィールドがあります。

- [Enable SNMP Traps]：オンにすると、リモート サーバがプル型更新を使用することを示します。Bolt
- [SNMP Traps]：SNMP で通知するエラー イベントを選択します。
  - [Fatal]：重大なエラー イベントすべてにトラップを生成します。
  - [Error]：すべてのエラーのエラー イベントにトラップを生成します。
  - [Warning]：警告エラー イベントすべてにトラップを生成します。
- [Enable detailed traps for alerts]：オンにした場合、アラートの全文をトラップに含めます。オフにした場合、スパース モードが使用されます。スパース モードでは、アラートに 484 バイト未満のテキストが含められます。
- [Default Trap Community String]：トラップに特定のストリングが設定されていない場合に使用するコミュニティ ストリング。
- [SNMP Trap Destinations]：トラップの宛先を指定します。宛先について、次の情報を指定する必要があります。
  - [IP Address]：トラップ宛先の IP アドレス。
  - [UDP Port]：トラップ宛先の UDP ポート。
  - [Trap Community String]：トラップ コミュニティ ストリング。

[Add SNMP Trap Destination]/[Edit SNMP Trap Destination] ダイアログボックスのフィールド定義

[Add SNMP Trap Destination]/[Edit SNMP Trap Destination] ダイアログボックスには、次のフィールドがあります。

- [IP Address]：トラップ宛先の IP アドレス。
- [UDP Port]：トラップ宛先の UDP ポート。デフォルトはポート 162 です。
- [Trap Community String]：トラップ コミュニティ ストリング。

SNMP トラップの設定

SNMP トラップを設定するには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [SNMP] > [Traps Configuration] と選択します。

ステップ 3　SNMP トラップをイネーブルにするには、[Enable SNMP Traps] チェックボックスをオンにします。

ステップ 4　SNMP トラップのパラメータ設定：

a. SNMP トラップによる通知を受け取るエラー イベントのチェックをオンにします。「重大」、「エラー」、「警告」というイベントのいずれか、またはすべてを選択して、種類に応じて SNMP トラップを送信するようセンサーを設定できます。

b. 詳細な SNMP トラップを受信するには、[Enable detailed traps for alerts] チェックボックスをオンにします。

c. [Default Trap Community String] フィールドに、詳細なトラップに含まれるコミュニティ ストリングを入力します。

ステップ 5　発信先の管理ワークステーションをセンサーに知らせるため、SNMP トラップ宛先にパラメータを設定します。

a. [Add] をクリックします。

b. [IP Address] フィールドに SNMP 管理ステーションの IP アドレスを入力します。

c. [UDP Port] フィールドに SNMP 管理ステーションの UDP ポートを入力します。

d. [Trap Community String] フィールドにトラップ コミュニティ ストリングを入力します。

（注） コミュニティ ストリングはトラップ内に出現し、複数のエージェントから複数のタイプのトラップを受け取る場合に役立ちます。たとえば、ルータやセンサーがトラップを送信する場合に、コミュニティ ストリングに特定のルータやセンサーを判別する内容を含めておけば、コミュニティ ストリングに基づいてトラップをフィルタできます。

ヒント 変更を廃棄して [Add SNMP Trap Destination] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 6　[OK] をクリックします。新しい SNMP トラップ宛先が [Traps Configuration] ペインのリストに表示されます。

ステップ 7　SNMP トラップ宛先を編集するには、編集する宛先を選択して [Edit] をクリックします。

ステップ 8　必要に応じて、[UDP Port] と [Trap Community String] フィールドを編集します。

ヒント 変更を廃棄して [Edit SNMP Trap Destination] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。編集された SNMP トラップ宛先が [Traps Configuration] ペインのリストに表示されます。

ステップ 10　SNMP トラップ宛先を削除するには、編集する宛先を選択して [Delete] をクリックします。削除した SNMP トラップ宛先は [Traps Configuration] ペインのリストに表示されなくなります。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 11　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

サポートされている MIB

センサーでは、次のプライベート MIB をサポートしています。

- CISCO-CIDS-MIB
- CISCO-PROCESS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

（注） MIB II は、センサー上では使用可能ですが、サポートされていません。当社では、一部の要素（センシング インターフェイス上の IF MIB からのパケット カウントなど）が正しくないことを認識しています。MIB II からの要素を使用することはできますが、一部の情報については正確性が保証されません。リストされているその他の MIB はフル サポートされており、これらの出力は正確です。

これらのプライベート Cisco MIB は、次の URL の見出し [SNMP v2 MIBs] から取得できます。

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