CHAPTER 11

SNMP の設定

この章では、SNMP の設定方法について説明します。

（注） センサーに SNMP トラップを送信させるには、シグニチャを設定する際に **request-snmp-trap** をイベント アクションとして選択します。詳細については、P.7-13 の「シグニチャへのアクションの割り当て」を参照してください。

この章は、次の項で構成されています。

SNMP の概要

SNMP は、ネットワーク デバイス間の管理情報の交換を促進するアプリケーション レイヤ 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 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、ネットワーク成長の計画を立てることができます。

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、管理対象デバイスが応答を返します。この動作は、Get、GetNext、Set、および Trap の 4 つのプロトコル操作のいずれかを使用することによって実装されます。

SNMP によるモニタリングのためにセンサーを設定することができます。SNMP は、ネットワーク管理ステーションが、スイッチ、ルータ、センサーなどさまざまな種類のデバイスの健全性とステータスを監視する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することができます。SNMP トラップを使用すると、エージェントが割り込み SNMP メッセージによって管理ステーションに重大なイベントを通知することができます。

トラップで指示された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に責任を負っていて、各デバイスに多数のオブジェクトがある場合、すべてのデバイス上のすべてのオブジェクトからの情報をポーリングまたは要求するのは実際的ではありません。解決法は、管理対象デバイス上の各エージェントが送信要求なしでマネージャに通知することです。これは、イベントのトラップとして知られているメッセージを送信することによって実行されます。

イベントの受信後、マネージャはそれを表示し、イベントに基づいてアクションを実行することができます。たとえば、マネージャはエージェントを直接ポーリングすることもできますし、イベントをよりよく理解するためにその他の関連するデバイス エージェントをポーリングすることもできます。

（注）　トラップで指示された通知は、重要でない SNMP 要求を排除することによって、ネットワークおよびエージェントのリソースを実質的に節約できます。ただし、SNMP ポーリングを完全に排除することはできません。SNMP 要求は、ディスカバリとトポロジの変更に必要です。さらに、深刻な停止の場合、管理対象デバイス エージェントはトラップを送信できません。

SNMP の設定

SNMP の汎用パラメータをサービス通知サブモードで設定します。

（注）　センサーに SNMP トラップを送信させるには、シグニチャを設定する際に **request-snmp-trap** をイベント アクションとして選択します。詳細については、P.7-13 の「シグニチャへのアクションの割り当て」を参照してください。

次のオプションが適用されます。

- **default**：値をシステム デフォルト設定に戻します。
- **enable-set-get [true | false]**：Object Identifier（OID; オブジェクト ID）の取得および設定をイネーブルにします。
- **no**：エントリまたは選択設定を削除します。
- **read-only-community**：SNMP エージェントの読み取り専用コミュニティ名。
  デフォルトは public です。
- **read-write-community**：SNMP エージェントの読み取り / 書き込みコミュニティ名。
  デフォルトは private です。
- **snmp-agent-port**：SNMP エージェントが受信するポート。
  デフォルト SNMP ポート番号は 161 です。
- **snmp-agent-protocol**：SNMP エージェントが通信に使用するプロトコル。
  デフォルト プロトコルは UDP です。
- **system-contact**：このセンサーの接続情報。
  system-contact オプションでは、SNMPv2-MIB::sysContact.0 値が変更されます。
- **system-location**：センサーの場所。
  system-location オプションでは、SNMPv2-MIB::sysLocation.0 値が変更されます。

SNMP の汎用パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　通知サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service notification
sensor(config-not)#
```

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がセンサー SNMP エージェントに要求を発行できるようにします。

```
sensor(config-not)# enable-set-get true
```

ステップ 4　SNMP エージェント パラメータを設定します。

次の値で、センサー SNMP エージェントにコミュニティ名を設定します。コミュニティ名はプレーンテキストのパスワード メカニズムで、SNMP クエリーの weak 認証を行うのに使用されます。

a. 読み取り専用コミュニティ ストリングを割り当てます。

```
sensor(config-not)# read-only-community PUBLIC1
```

読み取り専用コミュニティ名で、SNMP エージェントに対するクエリーのパスワードを指定します。

b. 読み取り / 書き込みコミュニティ ストリングを割り当てます。

```
sensor(config-not)# read-write-community PRIVATE1
```

読み取り / 書き込みコミュニティ名で、SNMP エージェントに対するセットのパスワードを指定します。

（注） 管理ワークステーションは SNMP 要求を、センサーに常駐するセンサー SNMP エージェントに送信します。管理ワークステーションから発行された要求において、コミュニティ ストリングがセンサー上の内容と一致しない場合、センサーによって要求が拒否されます。

c. センサー接続ユーザ ID を割り当てます。

```
sensor(config-not)# system-contact BUSINESS
```

d. センサーの場所を入力します。

```
sensor(config-not)# system-location AUSTIN
```

e. センサー SNMP エージェントのポートを入力します。

```
sensor(config-not)# snmp-agent-port 161
```

（注） ポートまたはプロトコルを変更する場合はセンサーをリブートする必要があります。

f. 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。

```
sensor(config-not)# snmp-agent-protocol udp
```

（注） ポートまたはプロトコルを変更する場合はセンサーをリブートする必要があります。

ステップ 5　設定を確認します。

```
sensor(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   error-filter: error|fatal <defaulted>
   enable-detail-traps: false <defaulted>
   enable-notifications: false <defaulted>
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: public <defaulted>
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
sensor(config-not)#
```

ステップ 6　通知サブモードを終了します。

```
sensor(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 7　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

SNMP トラップの設定

SNMP トラップをサービス通知サブモードで設定します。

（注）　センサーに SNMP トラップを送信させるには、シグニチャを設定する際に **request-snmp-trap** をイベント アクションとして選択します。詳細については、P.7-13 の「シグニチャへのアクションの割り当て」を参照してください。

次のオプションが適用されます。

- **enable-detail-traps [true | false]**：詳細トラップの送信をサイズ制限なしでイネーブルにします。このオプションを設定しない場合、トラップは希薄モード（484 バイト未満）で送信されます。
- **enable-notifications [true | false]**：イベント通知をイネーブルにします。
- **error-filter [warning | error | fatal]**：SNMP トラップを生成するエラーを決定します。SNMP トラップは、フィルタに一致する evError イベントすべてに対して生成されます。デフォルトは、error および fatal です。
- **trap-community-name**：トラップの宛先を定義したときに名前が指定されていなかった場合に、トラップ送信に際して使用されるコミュニティ名。
- **trap-destinations**：シグニチャ アクションで生成されたエラー イベントおよびアラート イベントを送信する宛先を定義します。
  - **trap-community-name**：トラップを送信するときに使用されるコミュニティ名。コミュニティ名が指定されていない場合、汎用トラップ コミュニティ名が使用されます。
  - **trap-port**：SNMP トラップの送信先ポート番号。

SNMP トラップを設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　通知サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service notification
sensor(config-not)#
```

ステップ 3　SNMP トラップをイネーブルにします。

```
sensor(config-not)# enable-notifications true
```

ステップ 4　SNMP トラップのパラメータを設定します。

a.　SNMP トラップを使用して通知するエラー イベントを選択します。

```
sensor(config-not)# error-filter [error | warning | fatal]
```

（注）　**error-filter [error | warning | fatal]** コマンドには、エラー トラップ、警告トラップ、および重大トラップがあります。重大度に基づいて、トラップをフィルタリングして組み込みます（フィルタリングして排除ではない）。

b. 詳細 SNMP トラップが必要であるかどうかを選択します。

```
sensor(config-not)# enable-detail-traps true
```

c. 詳細トラップに組み込むコミュニティ ストリングを入力します。

```
sensor(config-not)# trap-community-name TRAP1
```

ステップ 5　どの管理ワークステーションに送信するかをセンサーに知らせるため、SNMP トラップ宛先のパラメータを設定します。

a. SNMP 管理ステーションの IP アドレスを入力します。

```
sensor(config-not)# trap-destinations 10.1.1.1
```

b. SNMP 管理ステーションの UDP ポートを入力します。

```
sensor(config-not-tra)# trap-port 162
```

デフォルトは 162 です。

c. トラップ コミュニティ ストリングを入力します。

```
sensor(config-not-tra)# trap-community-name AUSTIN_PUBLI
```

（注） コミュニティ ストリングがトラップに表示されます。これは、複数のエージェントから複数のタイプのトラップを受信する場合に役立ちます。たとえば、ルータまたはセンサーがトラップを送信する場合に、具体的にルータまたはセンサーを識別する何かをコミュニティ ストリングに入力すると、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リングすることができます。

ステップ 6　設定を確認します。

```
sensor(config-not-tra)# exit
sensor(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 1)
   -----------------------------------------------
      ip-address: 10.1.1.1
      -----------------------------------------------
         trap-community-name: AUSTIN_PUBLIC default:
         trap-port: 161 default: 162
      -----------------------------------------------
   -----------------------------------------------
   error-filter: warning|error|fatal default: error|fatal
   enable-detail-traps: true default: false
   enable-notifications: true default: false
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: PUBLIC1 default: public
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
sensor(config-not)#
```

ステップ 7　通知サブモードを終了します。

```
sensor(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 8　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

サポートされている MIB

次のプライベート MIB がセンサーでサポートされています。

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

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

センサーでサポートされている管理 MIB は、rfc1213 (mib-2) です。

この mib-2 は、たとえば http://rfc.net/rfc1213.html のようなパブリック ドメインから取得できます。