CHAPTER 15

SNMP の設定

この章では、SNMP の設定方法について説明します。内容は次のとおりです。

SNMP について

注意 センサーが SNMP トラップを送信するようにするには、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は要求を発行し、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 つのプロトコル処理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用にセンサーを設定できます。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によって、重要でない SNMP 要求がなくなり、ネットワークとエージェントのリソースが大幅に節約されます。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。

SNMP の設定

サービス通知サブモードで、一般的な SNMP パラメータを設定します。

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}**：オブジェクト ID（OID）の **gets** と **sets** 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 read-only 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 read-write コミュニティ名。デフォルトは、private です。
- **snmp-agent-port**：SNMP エージェントがリッスンするポート。デフォルトの SNMP ポート番号は 161 です。
- **snmp-agent-protocol**：SNMP エージェントが通信するプロトコル。デフォルト プロトコルは UDP です。
- **system-contact**：このセンサーに関する連絡先情報。system-contact オプションによって、SNMPv2-MIB::sysContact.0 値が変更されます。
- **system-location**：センサーの場所。system-location オプションによって、SNMPv2-MIB::sysLocation.0 値が変更されます。

SNMP の一般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 CLI にログインします。

ステップ 2　通知サブモードを開始します。

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

ステップ 3　SNMP をイネーブルにし、SNMP 管理ワークステーションが、センサーの 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 パラメータを指定します。

これらの値によって、センサーの SNMP エージェントでコミュニティ名が設定されます。コミュニティ名は、SNMP クエリの簡易的な認証に使用されるプレーン テキストのパスワード メカニズムです。

a.　読み取り専用のコミュニティ ストリングを割り当てます。

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

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

b. 読み書き可能なコミュニティ ストリングを割り当てます。

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

読み書き可能なコミュニティ名では、SNMP エージェントに対する **set** にパスワードを指定します。

（注） 管理ワークステーションは、センサーに常駐しているセンサーの SNMP エージェントに対して、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、コミュニティ ストリングがセンサーのコミュニティ ストリングと一致しなかった場合、センサーによってその要求が拒否されます。

c. センサーの連絡先ユーザ 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. センサーの 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した場合は、センサーをリブートする必要があります。

f. センサーの SNMP エージェントが使用するプロトコルを指定します。

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

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

ステップ 5　設定を確認できます。

```
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　Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

SNMP トラップの設定

注意　センサーが SNMP トラップを送信するようにするには、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。

サービス通知サブモードで SNMP トラップを設定します。

次のオプションが適用されます。

- **enable-detail-traps {true | false}**：サイズ制限のない詳細なトラップの送信をイネーブルにします。このオプションを指定しない場合、トラップはスパース 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 トラップが生成され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すべての evError イベント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するときに名前が指定されていない場合、トラップの送信時に使用するコミュニティ名。
- **trap-destinations**：シグニチャ アクションから生成されたエラー イベントとアラート イベントを送信する宛先を定義します。
  - **trap-community-name**：トラップの送信時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は、一般的なトラップ コミュニティ名が使用されます。
  - **trap-port**：SNMP トラップの送信先のポート番号。

SNMP トラップを設定するには、次の手順に従ってください。

ステップ 1　管理者権限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　通知サブモードを開始します。

```
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指定します。

a.　SNMP トラップを通じて通知を受ける error イベントを指定します。

```
sensor(config-not)# error-filter {error | warning | fatal}
```

（注）　**error-filter {error | warning | fatal}** コマンドには、error、warning、および fatal のトラップが含まれます。これは、重大度に基づいてトラップをフィルタリングし、トラップを（排除するのではなく）抽出します。

b. 詳細な SNMP トラップが必要かどうかを指定します。

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

c. 詳細なトラップに含めるコミュニティ ストリングを入力します。

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

ステップ 5　センサーがトラップの送信先管理ワークステーションを認識するように、SNMP トラップ宛先のパラメータを指定します。

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 ストリングは、トラップ内に表示され、複数のエージェントからさまざまな種類のトラップを受信してい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している可能性があり、そのルータまたはセンサーを明示的に特定する文字をコミュニティ ストリングに含めた場合は、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できます。

ステップ 6　設定を確認できます。

```
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　Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

詳細情報

シグニチャにアクションを割り当てる手順については、「シグニチャへのアクションの割り当て」（P.8-15）を参照してください。

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

（注）　MIB II はセンサーで使用できますが、サポート対象外です。一部の要素が正しくないことが確認されています（センシング インターフェイスの IF MIB からのパケット数など）。MIB II からの要素を使用できますが、すべての要素が正しい情報を提供していることは保証されません。上記の他の MIB はすべてサポートされ、それぞれの出力は正確です。

次の URL の「SNMP v2 MIBs」で、これらのプライベート Cisco MIB を入手できます。

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