CHAPTER 10

センサーの保守

この章では、最新のソフトウェアによるセンサーの自動更新、即座の更新、工場出荷時のデフォルト設定の復元、センサーのシャットダウンなどの手段で、センサーを保守する方法について説明します。また、トラブルシューティングを目的として情報を生成しておき、TAC に問い合せるときに必要な場合にそれを使用することもできます。

この章は、次の項で構成されています。

センサーの自動更新

この項では、センサーの自動更新を設定する方法について説明します。取り上げる事項は次のとおりです。

概要

サービス パックとシグニチャの自動更新を設定し、これらのアップデートが中央の FTP または SCP サーバにロードされたときにダウンロードが行われ、センサーに適用されるようにすることができます。

自動更新は、DOS 形式のパスで設定された Windows FTP サーバでは動作しません。サーバの設定が DOS 形式のパスではなく、UNIX 形式のパス オプションに対応していることを確認してください。

（注） センサーは、サービス パックとシグニチャ アップデートを Cisco.com から自動的にダウンロードできません。サービス パックとシグニチャ アップデートは Cisco.com から FTP または SCP サーバにダウンロードし、この FTP または SCP サーバからセンサーがダウンロードするように設定する必要があります。

注意 Cisco.com から更新をダウンロードしたら、FTP または SCP サーバ上のダウンロード ファイルが完全な状態であることを保証できるように対策を講じる必要があります。

サポートされるユーザのロール

Auto Update パネルを表示したり、自動更新を設定したりするには、管理者である必要があります。

フィールド定義

Auto Update パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Enable Auto Update**：センサーはリモート サーバに保存されたアップデートをインストールします。

  Enable Auto Update が選択されていない場合は、すべてのフィールドがディセーブルになり値は消去されます。その他のすべての設定値を失わずに、このオン / オフを切り替えることはできません。
- **Remote Server Settings**：次のオプションを指定します。
  - **IP Address**：リモート サーバの IP アドレスを示します。
  - **File Copy Protocol**：FTP または SCP のどちらを使用するかを指定します。
  - **Directory**：リモート サーバ上のアップデートへのパスを示します。

- **Username**：リモート サーバ上のユーザ アカウントに対応するユーザ名を示します。
- **Password**：リモート サーバ上のユーザ アカウントのパスワードを示します。
- **Confirm Password**：リモート サーバのパスワードの再入力を要求してパスワードを確認します。

- **Schedule**：次のオプションを指定します。
  - **Start Time**：更新プロセスの開始時間を示します。

    これは、センサーがリモート サーバに接続し、使用可能なアップデートを検索する時点での時間です。
  - **Frequency**：更新を時間単位で実行するか、または週単位で実行するかを指定します。

    Hourly：*n* 時間ごとに更新を確認するように指定します。

    Daily：更新を実行する曜日を指定します。

ボタンの機能：

- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

自動更新の設定

自動更新を設定するには、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 IDM にログインします。

ステップ 2　**Configuration > Auto Update** をクリックします。

Auto Update パネルが表示されます。

ステップ 3　**Enable Auto Update** チェックボックスをオンにして、自動更新を使用可能にします。

ステップ 4　**IP Address** フィールドに、アップロードをダウンロードし保存するリモート サーバの IP アドレスを入力します。

ステップ 5　リモート サーバに接続するために使用するプロトコルを識別するため、File Copy Protocol リストから **FTP** または **SCP** のどちらかを選択します。

ステップ 6　**Directory** フィールドに、アップデートが配置されたリモート サーバのディレクトリへのパスを入力します。

パスの有効な値は 1 ～ 128 文字です。

ステップ 7　**Username** フィールドに、リモート サーバにログインするために使用するユーザ名を入力します。

ユーザ名の有効な値は 1 ～ 2047 文字です。

ステップ 8　**Password** フィールドに、リモート サーバのユーザ名パスワードを入力します。

パスワードの有効な値は 1 ～ 2047 文字です。

ステップ 9　**Confirm Password** フィールドにパスワードを再度入力します。

ステップ 10 更新を時間単位で指定するには、**Hourly** を選択し、次の手順を実行します。

a. **Start Time** フィールドに、アップデートを開始する時刻を入力します。

有効な値は hh:mm:ss です。

b. **Every_hours** フィールドに、各更新を実行する時間間隔を入力します。

有効な値は 1 ～ 8760 です。

たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新できるものがあれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーは、インストール可能な最新のアップデートを判別し、そのファイルをインストールします。

ステップ 11 更新を週単位で指定するには、**Daily** を選択し、次の手順を実行します。

a. **Start Time** フィールドに、アップデートを開始する時刻を入力します。

有効な値は hh:mm:ss です。

b. **Days** フィールドで、センサーが使用可能なアップデートを確認しダウンロードする曜日を選択します。

ヒント **Reset** をクリックして、変更を削除します。

ステップ 12 **Apply** をクリックし、変更を保存します。

デフォルト設定の復元

この項では、センサーに工場出荷時のデフォルト設定を復元する方法について説明します。取り上げる事項は次のとおりです。

概要

センサーはデフォルト設定に復元できます。

警告　**デフォルト設定を復元すると、現在のアプリケーションの設定が削除され、デフォルトの設定が復元されます。ネットワークの設定もデフォルトに戻り、センサーへの接続も即座に失われます。**

サポートされるユーザのロール

Restore Defaults パネルを表示したり、センサーのデフォルト設定を復元したりするには、管理者である必要があります。

フィールド定義

Restore Defaults パネルには次のフィールドとボタンがあります。

ボタンの機能：

- **Restore Defaults**：Restore Defaults ダイアログボックスを表示します。
  このダイアログボックスで、デフォルト設定の復元プロセスを開始できます。このプロセスは、センサーの設定をデフォルト設定に戻し、即座にセンサーへの接続を終了します。
- **OK**：デフォルト設定の復元プロセスを開始します。
- **Cancel**：Restore Defaults ダイアログボックスを閉じ、デフォルト設定の復元プロセスを実行せずに Restore Defaults パネルに戻ります。

デフォルト設定の復元

デフォルトの設定を復元するには、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 IDM にログインします。

ステップ 2　**Configuration > Restore Defaults** をクリックします。

Restore Defaults パネルが表示されます。

ステップ 3　**Restore Configuration Defaults** をクリックし、デフォルトの設定を復元します。

Restore Defaults ダイアログボックスが表示されます。

ステップ 4　**Yes** をクリックし、デフォルト設定の復元プロセスを開始します。

（注）　デフォルト設定を復元すると、IP アドレス、ネットマスク、デフォルト ゲートウェイ、およびアクセス リストはリセットされます。パスワードと時間はリセットされません。手動および自動ブロックも有効なままになります。

センサーのリブート

この項では、IDM からセンサーをリブートする方法について説明します。取り上げる事項は次のとおりです。

概要

Reboot Sensor パネルからセンサーをシャットダウンし再起動することができます。

サポートされるユーザのロール

Restore Sensor パネルを表示したり、センサーをリブートしたりするには、管理者である必要があります。

フィールド定義

Reboot Sensor パネルには次のボタンがあります。

ボタンの機能：

- **Reboot Sensor**：Reboot Sensor ダイアログボックスを表示します。
  このダイアログボックスで、センサーをシャットダウンし再起動するプロセスを開始できます。
- **OK**：センサーをシャットダウンし再起動します。これによって、即座にセンサーへの接続は失われます。センサーの再起動後にログインし直すことができます。
- **Cancel**：Reboot Sensor ダイアログボックスを閉じ、センサーをシャットダウンせずに Reboot Sensor パネルに戻ります。

センサーのリブート

センサーをリブートするには、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 IDM にログインします。

ステップ 2　**Configuration > Reboot Sensor** をクリックします。

Reboot Sensor パネルが表示されます。

ステップ 3　**Reboot Sensor** をクリックします。

Reboot Sensor ダイアログボックスが表示されます。

ステップ 4　**OK** をクリックして、センサーをシャットダウンし再起動します。

センサーのアプリケーションがシャットダウンし、その後、センサーがリブートします。リブート後に、ログインする必要があります。

（注）　CLI にログインしているユーザに対して、センサーがシャットダウンするという通知が表示されてから、30 秒後にシャットダウンされます。

センサーのシャットダウン

この項では、IDM からセンサーをシャットダウンする方法について説明します。取り上げる事項は次のとおりです。

概要

IPS アプリケーションをシャットダウンしてから、センサーを安全に電源を切断できる状態にします。

サポートされるユーザのロール

Shut Down Sensor パネルを表示したり、センサーをシャットダウンしたりするには、管理者である必要があります。

フィールド定義

Shut Down Sensor パネルには次のフィールドとボタンがあります。

ボタンの機能：

- **Shut Down Sensor**：Shut Down Sensor ダイアログボックスを表示します。
  このダイアログボックスで、センサーをシャットダウンするプロセスを開始できます。
- **OK**：センサーをシャットダウンし、開いているセンサーへの接続を即座に閉じます。
- **Cancel**：シャットダウン プロセスを開始せずに、Shut Down Sensor ダイアログボックスを閉じます。

センサーのシャットダウン

センサーをシャットダウンするには、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 IDM にログインします。

ステップ 2　**Configuration > Shut Down Sensor** をクリックします。

Shut Down Sensor パネルが表示されます。

ステップ 3　**Shut Down Sensor** をクリックします。

Shut Down Sensor ダイアログボックスが表示されます。

ステップ 4　**OK** をクリックして、センサーをシャットダウンします。

センサーのアプリケーションがシャットダウンし、開いているセンサーへの接続は閉じられます。

（注）　CLI にログインしているユーザに対して、センサーがシャットダウンするという通知が表示されてから、30 秒後にシャットダウンされます。

センサーの更新

この項では、最新のソフトウェアでセンサーを更新する方法について説明します。取り上げる事項は次のとおりです。

概要

Update Sensor パネルから、即座にサービス パックとシグニチャ アップデートを適用できます。

（注）　センサーは、サービス パックとシグニチャ アップデートを Cisco.com からダウンロードできません。サービス パックとシグニチャ アップデートは Cisco.com から FTP サーバにダウンロードし、この FTP サーバからセンサーがダウンロードするように設定する必要があります。

サポートされるユーザのロール

Update Sensor パネルを表示したり、サービス パックやシグニチャ アップデートでセンサーを更新したりするには、管理者である必要があります。

フィールド定義

Update Sensor パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Update is located on a remote server and is accessible by the sensor**：次のオプションを指定します。
  - **URL**：アップデートが配置されているサーバのタイプを示します。FTP、HTTP/S、または SCP のどれを使用するかを指定します。
  - **://**：リモート サーバ上のアップデートへのパスを示します。
  - **Username**：リモート サーバ上のユーザ アカウントに対応するユーザ名を示します。
  - **Password**：リモート サーバ上のユーザ アカウントのパスワードを示します。
- **Update is located on this client**：次のオプションを指定します。
  - **Local File Path**：このローカル クライアント上のアップデート ファイルへのパスを示します。
  - **Browse Local**：このローカル クライアント上のファイル システムの Browse ダイアログボックスを表示します。このダイアログボックスで、アップデート ファイルにナビゲートできます。

ボタンの機能：

- **Update Sensor**：Update Sensor ダイアログボックスを表示します。このダイアログボックスで、インスタント アップデートを開始できます。
- **OK**：Update Sensor パネルに設定されたパラメータに従って、即座にセンサーを更新します。
- **Cancel**：更新を実行せずに Update Sensor ダイアログボックスを閉じます。

センサーの更新

サービス パックとシグニチャ アップデートをすぐに適用するには、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 IDM にログインします。

ステップ 2　**Configuration > Update Sensor** をクリックします。

Update Sensor パネルが表示されます。

ステップ 3　アップデートをリモート サーバからプルダウンしてセンサーにインストールするには、次の手順を実行します。

a. **Update is located on a remote server and is accessible by the sensor** を選択します。

b. **URL** フィールドにアップデートを検索できる URL を入力します。

サポートされる URL タイプは、次のとおりです。

- FTP：FTP ネットワーク サーバの発信元 URL。

  このプレフィクスの構文は、次のとおりです。

  `ftp://location/relative_directory/filename`

  または

  `ftp://location//absolute_directory/filename`

- HTTPS：Web サーバの発信元 URL

  このプレフィクスの構文は、次のとおりです。

  `https://location/directory/filename`

  （注） HTTPS プロトコルを使用する前に、**tls trusted-host** コマンドを使用して TLS 信頼ホストを設定します。

- SCP：SCP ネットワーク サーバの発信元 URL。

  このプレフィクスの構文は、次のとおりです。

  `scp://location/relative_directory/filename`

  または

  `scp://location/absolute_directory/filename`

- HTTP：Web サーバの発信元 URL

  このプレフィクスの構文は、次のとおりです。

  `http://location/directory/filename`

次の例は、FTP プロトコルを示しています。

```
ftp://user@ip_address/UPDATES/file_name.rpm.pkg
```

（注）　アップデートをあらかじめ Cisco.com からダウンロードし、FTP サーバに保存しておく必要があります。

c. **Username** フィールドに、リモート サーバ上のアカウントのユーザ名を入力します。

d. **Password** フィールドに、リモート サーバ上のこのアカウントに関連付けられたパスワードを入力します。

ステップ 4　ローカル　クライアントからセンサーにプッシュしてインストールするには、次の手順を実行します。

a. **Update is located on this client** を選択します。

b. ローカル クライアント上のアップデート ファイルへのパスを指定するか、または **Browse Local** をクリックしてローカル クライアント上のファイルをナビゲートします。

ステップ 5　**Update Sensor** をクリックします。

Update Sensor ダイアログボックスに、更新するとセンサーへの接続が失われ再度ログインする必要が生じることを示すメッセージが表示されます。

ステップ 6　**OK** をクリックして、センサーを更新します。

ヒント　変更を元に戻してダイアログボックスを閉じるには、**Cancel** をクリックします。

（注）　サービス パック、マイナー アップデート、メジャー アップデート、エンジニアリング パッチによる更新時には、IDM および CLI の接続は失われます。これらのアップデートのいずれかを適用すると、インストーラが自動的に IPS アプリケーションを再起動します。センサーをリブートできます。シグニチャ アップデートを適用する場合は、接続が失われないため、システムをリブートする必要はありません。

診断レポートの生成

この項では、診断レポートを生成する方法について説明します。取り上げる事項は次のとおりです。

概要

トラブルシューティング用に、センサーの診断情報を取得できます。診断レポートには、TAC がセンサーのトラブルシューティングに使用することを目的として、ログ、ステータス、設定などの内部システムの情報が含まれています。

（注）　診断レポートの生成には数分かかることがあります。

Diagnostics Report パネルでレポートを表示できます。また、**Save** をクリックして、それをハードディスク ドライブに保存することもできます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

診断を実行するには、管理者である必要があります。

フィールド定義

Diagnostics Report パネルには次のボタンがあります。

ボタンの機能：

- **Save**：**Save As** ダイアログボックスが表示されます。ここで、診断レポートのコピーをハードディスク ドライブに保存できます。
- **Generate Report**：診断プロセスを開始します。

  このプロセスが完了するまでに数分かかることがあります。プロセスが完了すると、レポートが生成され、更新されたレポートで表示がリフレッシュされます。

診断レポートの生成

診断を実行するには、次の手順を実行します。

注意　診断プロセスが開始したら、IDM 内のその他のオプションをクリックしたり、Diagnostics パネルを終了したりしないでください。このプロセスが完了するまで、センサーのその他のタスクは一切実行できません。

ステップ 1　管理者特権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　**Monitoring > Support Information > Diagnostics Report** をクリックします。

Diagnostics パネルが表示されます。

ステップ 3　**Generate New Report** をクリックします。

（注）　診断プロセスが完了するまでに数分かかることがあります。プロセスの実行が完了すると、更新された結果で表示がリフレッシュされます。

（注）　このレポートをファイルとして保存するには、**Save** をクリックします。**Save As** ダイアログボックスが表示され、レポートをハードディスク ドライブに保存できます。

統計情報の表示

この項では、センサーの統計情報を表示する方法について説明します。取り上げる事項は次のとおりです。

概要

Statistics パネルには、次のカテゴリの統計情報が表示されます。

- 分析エンジン
- イベント サーバ
- イベント ストア
- ホスト
- インターフェイスのコンフィギュレーション
- ロガー
- Attack Response Controller（以前は Network Access Controller と呼ばれていました）
- 通知
- トランザクション サーバ
- トランザクション ソース
- 仮想センサー
- Web サーバ

サポートされるユーザのロール

管理者、オペレータ、およびビューアがシステムの統計情報を表示できます。

フィールド定義

Statistics パネルには次のボタンがあります。

ボタンの機能：

- **Refresh**：Web サーバ、トランザクション ソース、トランザクション サーバ、Network Access Controller（IPS 5.1 では Attack Response Controller と呼ばれていますが、統計情報では引き続き Network Access Controller として示されています。）、Logger、ホスト、イベント ストア、イベント サーバ、分析エンジン、インターフェイスのコンフィギュレーション、および認証を含め、センサー アプリケーションに関する最新の情報を表示します。

統計情報の表示

センサーの統計情報を表示するには、次の手順を実行します。

ステップ 1　**Monitoring > Support Information > Statistics** の順に選択します。

Statistics ページが表示されます。

ステップ 2　統計情報が変化した場合にそれらを更新するには、**Refresh** をクリックします。

システム情報の表示

この項では、システム情報を表示する方法について説明します。取り上げる事項は次のとおりです。

概要

System Information ページには、次の情報が表示されます。

- TAC 接続情報
- センサーの稼働時間
- センサーのタイプ
- ソフトウェア バージョン
- アプリケーションの状態
- インストールされているアップグレード
- PEP 情報
- メモリの使用状況
- ディスクの使用状況

サポートされるユーザのロール

システム情報を表示するには、管理者またはオペレータである必要があります。ビューアは、センサーの稼働時間とディスクの使用状況を除くすべてのシステム情報を表示できます。

フィールド定義

System Information パネルには次のボタンがあります。

ボタンの機能：

- **Refresh**：ソフトウェア バージョンや PEP 情報を含む、センサーに関する最新の情報を表示します。

システム情報の表示

システム情報を表示するには、次の手順を実行します。

ステップ 1　**Monitoring > Support Information > System Information** をクリックします。

System Information パネルに、システムに関する情報が表示されます。

ステップ 2　**Refresh** をクリックします。

パネルがリフレッシュされ、新しい情報が表示されます。