CSM 3.x:IDSセンサーとモジュールのインベントリへの追加

内容

はじめに

このドキュメントでは、Cisco Security Manager（CSM）に侵入検知システム（IDS）のセンサーとモジュール（Catalyst 6500 スイッチの IDSM、ルータの NM-CIDS、および ASA の AIP-SSM を含む）追加する方法について説明します。

注：CSM 3.2はIPS 6.2をサポートしていません。CSM 3.3 ではサポートされています。

前提条件

要件

このドキュメントでは、CSM デバイスと IDS デバイスが設置され、正しく機能することを前提としています。

使用するコンポーネント

このドキュメントの情報は、CSM 3.0.1 に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

Security Manager インベントリへのデバイスの追加

デバイスを Security Manager に追加するときには、DNS 名や IP アドレスなど、デバイスの一連の識別情報を指定します。追加したデバイスは、Security Manager デバイス インベントリに表示されます。インベントリに追加した後は、Security Manager でデバイスを管理できます。

デバイスを Security Manager インベントリに追加する方法を以下に挙げます。

- ネットワークからデバイスを追加する。
- ネットワーク上にまだ存在していない新しいデバイスを追加する。
- Device and Credentials Repository（DCR）から 1 つ以上のデバイスを追加する。
- 設定ファイルから 1 つ以上のデバイスを追加する。

注：このドキュメントでは、「ネットワークにまだ接続していない新しいデバイスを追加する」方法を中心に説明します。

IDS センサーとモジュールを追加するための手順

1 つのデバイスを Security Manager インベントリに追加するには、[Add New Device] オプションを使用します。このオプションは、事前プロビジョニングに使用できます。デバイスのハードウェアを受け取る前に、システムでデバイスを作成し、ポリシーをデバイスに割り当て、設定ファイルを生成できます。

デバイスのハードウェアを受け取ったら、Security Manager で管理するデバイスを準備する必要があります。詳細については、Security Manager で管理するデバイスの準備を参照してください。

この手順では、新しい IDS センサーとモジュールを追加する方法について説明します。

1. ツールバーの [Device View] ボタンをクリックします。

   [Devices] ページが表示されます。

2. デバイス セレクタで [Add] をクリックします。

   [New Device - Choose Method] ページが開き、4 つのオプションが表示されます。

3. [Add New Device] を選択し、[Next] をクリックします。

   [New Device - Device Information] ページが表示されます。

4. 該当するフィールドにデバイス情報を入力します。

   詳細については、「デバイス情報の指定：新しいデバイス」セクションを参照してください。

5. [Finish] をクリックします。

   システムが、次のようなデバイスの検証タスクを実行します。

   - データが正しくない場合は、システムがエラー メッセージを生成し、エラーが発生したページが表示され、対応する場所に赤のエラー アイコンが表示されます。
   - データが正しい場合は、デバイスがインベントリに追加され、デバイス セレクタに表示されます。

デバイス情報の指定：新しいデバイス

次のステップを実行します。

1. 新しいデバイスのデバイス タイプを選択します。

   a. サポートされているデバイス ファミリを表示するには、最上位のデバイス タイプのフォルダを選択します。

   b. サポートされているデバイス タイプを表示するには、デバイス ファミリのフォルダを選択します。

      a. [Cisco Interfaces and Modules] > [Cisco Network Modules] を選択して、[Cisco IDS Access Router Network Module] を追加します。同様に、[Cisco Interfaces and Modules] > [Cisco Services Modules] を選択して、AIP-SSM モジュールと IDSM モジュールを追加します（図を参照）。

      b. [Security and VPN]> [Cisco IPS 4200 Series Sensors] を選択して、[Cisco IDS 4210 Sensor] を CSM インベントリに追加します。

   c. デバイス タイプを選択します。

      注：デバイスを追加した後は、デバイスタイプを変更できません。

      [SysObjectId] フィールドに、そのデバイス タイプのシステム オブジェクト ID が表示されます。最初のシステム オブジェクト ID がデフォルトで選択されています。必要に応じて、別の ID を選択できます。

2. [IP Type]（[Static] または [Dynamic]）、[Host Name]、[Domain Name]、[IP Address]、[Display Name] など、デバイス識別情報を入力します。

3. [OS Type]、[Image Name]、[Target OS Version]、[Contexts]、[Operational Mode] など、デバイスのオペレーティング システムに関する情報を入力します。

4. 選択したデバイス タイプに応じて、[Auto Update] または [CNS-Configuration Engine] フィールドが表示されます。

   - [Auto Update]：PIX Firewall および ASA デバイスの場合に表示されます。
   - [CNS-Configuration Engine]：Cisco IOS® ルータの場合に表示されます。

注：このフィールドは、Catalyst 6500/7600およびFWSMデバイスではアクティブではありません。

5. 次のステップを実行します。

   - [Auto Update]：矢印をクリックすると、サーバのリストが表示されます。デバイスを管理するサーバを選択します。サーバがリストに表示されない場合は、次の手順を実行します。

     a. 矢印をクリックし、[+ Add Server...] を選択します。[Server Properties] ダイアログボックスが表示されます。

     b. 必須フィールドに情報を入力します。

     c. [OK] をクリックします。新しいサーバが、選択可能なサーバのリストに追加されます。

   - [CNS-Configuration Engine]：[IP Type] として [Static] と [Dynammic] のどちらを選択したかによって、異なる情報が表示されます。

     [Static]：矢印をクリックすると、構成エンジンのリストが表示されます。デバイスを管理する構成エンジンを選択します。リストに構成エンジンが表示されない場合は、次の手順を実行します。

     a. 矢印をクリックし、[+ Add Configuration Engine...] を選択します。[Configuration Engine Properties] ダイアログボックスが表示されます。

     b. 必須フィールドに情報を入力します。

     c. [OK] をクリックします。新しい構成エンジンが、選択可能な構成エンジンのリストに追加されます。

   - [Dynamic]：矢印をクリックすると、サーバのリストが表示されます。デバイスを管理するサーバを選択します。サーバがリストに表示されない場合は、次の手順を実行します。

     a. 矢印をクリックし、[+ Add Server...] を選択します。[Server Properties] ダイアログボックスが表示されます。

     b. 必須フィールドに情報を入力します。

     c. [OK] をクリックします。新しいサーバが、選択可能なサーバのリストに追加されます。

6. 次のステップを実行します。

   - Security Manager でデバイスを管理するには、[Manage in Cisco Security Manager] チェックボックスをオンにします。これはデフォルトです。

   - 追加しようとしているデバイスの唯一の機能が VPN エンド ポイントとしての機能性

である場合は、[Manage in Cisco Security Manager] チェックボックスをオフにします。

Security Manager は設定を管理せず、このデバイスの設定をアップロードもダウンロードもしません。

7. 親デバイス（PIX Firewall、ASA、または FWSM）が Security Manager によって管理されていないセキュリティ コンテキストを管理するには、[Security Context of Unmanaged Device] チェックボックスをオンにします。

   1 つの PIX ファイアウォール、ASA、または FWSM のパーティションを、セキュリティ コンテキストとも呼ばれる複数のセキュリティ ファイアウォールに分けることができます。各コンテキストは、それぞれに独自の設定およびポリシーを持つ独立したシステムです。このようなスタンドアロンのコンテキストは、親デバイス（PIX Firewall、ASA、または FWSM）が Security Manager の管理対象外であっても、Security Manager で管理できます。

   注：このフィールドは、デバイスセレクタで選択したデバイスが、セキュリティコンテキストをサポートするファイアウォールデバイス（PIXファイアウォール、ASA、FWSMなど）である場合にのみアクティブになります。

8. IPS Manager で Cisco IOS ルータを管理するには、[Manage in IPS Manager] チェックボックスをオンにします。

   このフィールドは、デバイス セレクタで Cisco IOS ルータを選択した場合にのみアクティブになります。

   注：IPS ManagerでIPS機能を管理できるのは、IPS機能を備えたCisco IOSルータ上だけです。詳細については、IPS の資料を参照してください。

   [Manage in IPS Manager] チェックボックスをオンにした場合は、[Manage in Cisco Security Manager] チェックボックスもオンにする必要があります。

   選択したデバイスが IDS である場合、このフィールドはアクティブになりません。ただし、IPS Manager は IDS センサーを管理するため、チェックボックスはオンになっています。

   選択したデバイスが PIX Firewall、ASA、または FWSM である場合は、IPS Manager がこれらのデバイス タイプを管理しないため、このフィールドはアクティブになりません。

9. [Finish] をクリックします。

   システムが、次のようなデバイスの検証タスクを実行します。

   - 入力したデータが正しくない場合は、システムがエラー メッセージを生成し、エラーが発生したページが表示されます。
   - 入力したデータが正しい場合は、デバイスがインベントリに追加され、デバイス セレクタに表示されます。

トラブルシュート

ここでは、設定に関するトラブルシューティングについて説明します。

エラー メッセージ

IPSをCSMに追加すると、「`Invalid device: Could not deduce the SysObjId for the platform type`」エラーメッセージが表示されます。

解決方法

このエラー メッセージを解決するには、次の手順を実行してください。

1. Windows で CSM Daemon サービスを停止し、[Program Files] > [CSCOpx] > [MDC] > [athena] > [config] > [Directory] を選択し、`VMS-SysObjID.xml` を見つけます。
2. CSMシステムで、デフォルトで`C:\Program Files\CSCOpx\MDC\athena\config\directory`にある元のVMS-SysObjID.xmlファイルを最新の`VMS-SysObjID.xml`ファイルに置き換えます。
3. CSM Daemon Manager サービス（CRMDmgtd）を再起動し、問題が発生していたデバイスの追加または検出を再試行します。

関連情報

- Cisco Security Manager のサポート ページ
- シスコ侵入検知システム サポート ページ
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。