目次

概要

この資料にバージョン 4.1 から Cisco 侵入防御システム（IPS） 5.0 および それ以降へ Cisco 侵入検知センサ（IDS）ソフトウェアのためのイメージおよびシグニチャをアップグレードする方法を記述されています。

注バージョン 4.1 まで適当であるソフトウェア バージョン 5.x およびそれ以降から、Cisco IPS は Cisco IDS を取り替えます。

注 センサーは Cisco.com からソフトウェア アップデートをダウンロードできません。 Cisco.com から FTP サーバにソフトウェア アップデートをダウンロードして下さい次に FTP サーバからそれらをダウンロードするためにセンサーを設定します。

プロシージャのための[システムイメージをアップグレードし、ダウングレード、インストールすること](#)の [AIP-SSM System Image セクションをインストールすることを](#)参照して下さい。

バージョン 3.x および 4.x のための Cisco Secure IDS （以前の NetRanger）アプライアンスおよびモジュールを回復 する方法について詳細を学ぶために [Cisco IDS センサーおよび IDS サービス モジュール（IDSM-1、IDSM-2）におけるパスワード回復手順を](#)参照して下さい。

注ユーザトラフィックは ASA の**インラインおよび故障する開いた**設定のアップグレードの間に-AIP-SSM 影響を受けません。

注プロシージャに関する詳細については[コマンド ライン インターフェース 6.0 を使用して 5.1 から Cisco 侵入防御システム センサーの](#)バージョン 6.x に IPS 5.1 をアップグレードするために[設定](#)の [6.x](#) セクション[に Cisco アップグレード IPS ソフトウェアを](#)参照して下さい。

注センサーはオート更新のためのプロキシサーバをサポートしません。 プロキシ 設定はグローバル な相関機能だけのためです。

前提条件

要件

5.0 にアップグレードする必要がある最小必須 ソフトウェア バージョンは 4.1(1) です。

使用するコンポーネント

この文書に記載されている情報はソフトウェア バージョン 4.1 を実行する IDS ハードウェアに Cisco 4200 シリーズ基づいています（バージョン 5.0 にアップグレードされるため）。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『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。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

Cisco 4.1 からの 5.0 へのアップグレードは Cisco.com からのダウンロードとして利用できます。 Cisco.com の IPS ソフトウェアダウンロードにアクセスするのに使用するプロシージャのための Cisco IPS ソフトウェアを入手することを参照して下さい。

のアップグレードを行うためにここにリストされているメソッド使用できます:

- 5.0 アップグレード ファイルをダウンロードした後、**upgrade コマンド**で 5.0 アップグレード ファイルをインストールする方法のプロシージャのための Readme を参照して下さい。詳細については使用をこの資料の Upgrade コマンド セクション参照して下さい。
- センサーのためのオート アップデートを設定した場合、サーバのディレクトリに 5.0 アップグレード ファイルをその更新のためのセンサー ポーリング コピーして下さい。 詳細については使用をこの資料の自動アップグレード 指揮 班参照して下さい。
- リブートした後センサーでアップグレードをインストールすればおよびセンサーが使用不可能なら、センサーをイメージ変更して下さい。 以前のまたあらゆる Cisco IDS バージョンからのセンサーのアップグレードは 4.1 **回復** コマンドかリカバリ/アップグレード CD を使用するように要求します。 詳細についてはイメージ変更をこの資料のセンサー セクション参照して下さい。

センサーをアップグレードして下さい

これらのセクションはセンサーのソフトウェアをアップグレードする **upgrade コマンドを**使用する方法を説明します:

概要

拡張 .pkg があるこれらのファイルが付いているセンサーをアップグレードできます:

- シグニチャアップデート、たとえば、IPS-sig-S150-minreq-5.0-1.pkg
- シグニチャ エンジン更新、たとえば、IPS-engine-E2-req-6.0-1.pkg
- 主要な更新、たとえば、IPS-K9-maj-6.0-1-pkg
- マイナー な更新、たとえば、IPS-K9-min-5.1-1.pkg
- サービスパック更新、たとえば、IPS-K9-sp-5.0-2.pkg
- リカバリ パーティション更新、たとえば、IPS-K9-r-1.1-a-5.0-1.pkg
- パッチ リリース、たとえば、IPS-K9-patch-6.0-1p1-E1.pkg
- リカバリ パーティション更新、たとえば、IPS-K9-r-1.1-a-6.0-1.pkg

センサー アップグレードはセンサーのソフトウェア バージョンを変更します。

Upgrade コマンドおよびオプション

自動アップグレードを設定するためにサービス ホスト サブモードで自動アップグレード **オプション enabled コマンドを**使用して下さい。

これらのオプションによって、次の設定が割り当てられます。

- **デフォルト**か。システムデフォルト標準設定に値を設定し直します。
- **ディレクトリ**か。アップグレード ファイルがファイルサーバにあるディレクトリ。
- **ファイル COPY (ビット 0) プロトコル**か。ファイルサーバからファイルをダウンロードするのに使用されるファイルのコピー プロトコル。 有効値は **ftp** または **SCP** です。**注**SCP を使用する場合、SSH 既知ホスト リストにサーバを追加するのに **ssh ホストキー** コマンドを使用して下さい従ってセンサーは SSH によってそれと通信できます。 既知ホストへホストを追加することをリストしますプロシージャのために参照して下さい。
- **IP アドレス**か。ファイルサーバの IP アドレス。
- **パスワード**か。ファイルサーバの認証のためのユーザパスワード。
- **Schedule オプション**か。自動アップグレードが実行する場合のスケジュール。 カレンダー スケジューリングは特定の日の特定時にアップグレードを開始します。 定期的なスケジューリングは特定の定期的な間隔でアップグレードを開始します。**カレンダー スケジュール**か。自動アップグレードが実行された日の曜日および時を設定します。**日の週**か。自動アップグレードが実行された 曜日。 複数の日を選択できます。 土曜日までの日曜日は有効値です。**いいえ**か。エントリまたは選択設定を取除きます。**時間の日**か。自動アップグレードが始まる日の時。 複数回を選択できます。 有効値は hh です: mm[: ss]。**定期的スケジュール**か。最初の自動アップグレードが実行するはずである自動アップグレードの間で待つためにどの位設定しこと時間を。**間隔**か。自動アップグレードの間で待つ時間数。 有効値は 0 から 8760 です。**開始時刻**か。最初の自動アップグレードを開始する Time Of Day。 有効値は hh です: mm[: ss]。
- **ユーザ名**か。ファイルサーバの認証のためのユーザ名。

センサーをアップグレードする IDM 手順に関しては、センサーをアップデートすることを参照して下さい。

Upgrade コマンドを使用して下さい

IPS 6.0 へアップグレードする前に設定される**読み出し専用コミュニティ**および**読み書きコミュニティ** パラメータを持たない場合 SNMP エラーを受け取ります。 SNMP **セットを**使用していたりおよび/または機能を**得る**場合、IPS 6.0 にアップグレードする前に**読み出し専用コミュニティ**および**読み書きコミュニティ** パラメータを設定して下さい。 IPS 5.x では、**読み出し専用コミュニティはパブリック**にデフォルトで設定 され、**読み書きコミュニティは** private にデフォルトで設定 されました。 IPS 6.0 でこれら二つのオプションにデフォルト値がありません。 SNMP **gets を**使用しなかったし、IPS 5.x の**セットが**、たとえば、偽に設定 されたらイネーブル設定得れば、IPS 6.0 にアップグレードするべき問題がありません。 SNMP **gets を**使用し、IPS 5.x の**セットが**、たとえば、本当に設定 されたらイネーブル設定得れば、**読み出し専用コミュニティを**設定して下さい、特定の値または IPS 6.0 アップグレードへの**読み書きコミュニティ** パラメータは失敗します。

次のエラー メッセージが表示されます。

注IPS 6.0 拒否高いリスク イベント デフォルトで。 これは IPS 5.x からの変更です。 デフォルトを変更するために、拒否パケット インライン操作のための検知時のアクション 上書きするを作成し、それをディセーブルにされるために設定して下さい。 管理者が読み書きコミュニティに気づいていない場合それらはアップグレードするこのエラーメッセージを削除するために試みが試みられる前に SNMP を完全にディセーブルにすることを試みる必要があります。

センサーをアップグレードするためにこれらのステップを完了して下さい:

1. FTP、センサーからアクセス可能である HTTPS サーバに主要なアップデート ファイル（IPS-K9-maj-5.0-1-S149.rpm.pkg）をまたは SCP、HTTP、ダウンロードして下さい。 Cisco.com でソフトウェアを見つける方法のプロシージャのための Cisco IPS ソフトウェアを入手することを参照して下さい。**注**暗号特権のアカウントを使用して Cisco.com にログイン ファイルをダウンロードするためになります。 ファイル名は変更しないでください。 センサーがアップデートを受け入れることができるようにオリジナル ファイル名を維持して下さい。**注**ファイル名を変更しないで下さい。 センサーがアップデートを受け入れることができるようにオリジナル ファイル名を維持して下さい。
2. アドミニストレーター特権のアカウントを使用して CLI へのログイン。
3. 次の設定モードを入力します。`sensor#`**`configure terminal`**
4. センサーをアップグレードして下さい:`sensor(config)#`**`upgrade scp://<username>@<server IP>//upgrade/<file name>`****例：注**このコマンドは空間的な原因による 2 つの行にあります。`sensor(config)#`**`upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg`****注**FTP および HTTP/HTTPS サポートされたサーバのリストの FTP および HTTP/HTTPS サポートされたサーバを参照して下さい。 SSH 既知ホストへホストを追加することをリストします SSH 既知ホスト リストに SCP サーバを追加する方法に関する詳細については参照して下さい。
5. プロンプト表示された場合パスワードを入力して下さい:`sensor(config)#`**`upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg`**
6. アップグレードを完了するために**はい**入力して下さい。**注**主要な更新、マイナー な更新およびサービスパックは IPS プロセスの再始動を強制するまた更にインストールを完了するためにセンサーの再度ブートするを強制するかもしれません。 このように、少なくとも 2 分のサービスの割り込みがあります。 ただし、シグニチャアップデートはアップデートがされた後再度ブートするを必要としません。 最新の更新のためのダウンロード シグニチャアップデート（登録ユーザのみ）を参照して下さい。
7. センサ バージョンを確認して下さい:`sensor#`**`show version`**`Application Partition:Cisco`

```
Intrusion Prevention System, Version 5.0(1)S149.0OS Version 2.4.26-IDS-smp-bigphysPlatform:
ASA-SSM-20Serial Number: 021No license presentSensor up-time is 5 days.Using 490110976 out
of 1984704512 bytes of available memory (24% usage)system is using 17.3M out of 29.0M bytes
of available disk space (59% usage)application-data is using 37.7M out of 166.6M bytes of
available disk space (24 usage)boot is using 40.5M out of 68.5M bytes of available disk
space (62% usage)MainApp          2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600
RunningAnalysisEngine  2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  RunningCLI
2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600Upgrade History:  IDS-K9-maj-5.0-1-
14:16:00 UTC Thu Mar 04 2004Recovery Partition Version 1.1 - 5.0(1)S149sensor#
```

注 IPS 5.x に関しては、アップグレードは不明な型であることを示すメッセージを受け取ります。 このメッセージを無視できます。**注**オペレーティング システムはイメージ変更され、サービス アカウントによるセンサーに置かれたすべてのファイルは取除かれます。

センサーのアップグレードのための IDM プロシージャに関する詳細についてはセンサーをアップデートすることを参照して下さい。

自動アップグレードの設定

自動アップグレード

アップグレード ディレクトリの新しいアップグレード ファイルを自動的に探すためにセンサーを設定できます。 たとえば、複数のセンサーは異なるアップデート スケジュールの同じリモート FTP サーバ ディレクトリを、24 時間毎にのような、か 11:00 に月曜日、水曜日および金曜日指すことができます。

自動アップグレードをスケジュールするためにこの情報を規定 します:

- サーバ IP アドレス
- センサーがアップグレード ファイルがあるように確認するファイルサーバのディレクトリのパス
- ファイルのコピー プロトコル（ SCP か FTP ）
- ユーザ名 および パスワード
- アップグレード スケジュール

センサーが自動アップグレードのためにポーリングできる前に Cisco.com からソフトウェアアップグレードをダウンロードし、アップグレード ディレクトリにコピーして下さい。

注AIM-IPS と自動アップグレードをおよび他の IPS アプライアンスまたはモジュール使用する場合、ファイルがインストールされる自動的にダウンロードされ、必要がある AIM-IPS が正しく検出することができるように自動更新サーバに両方とも 6.0(1) アップグレード ファイル、IPS-K9-6.0-1-E1.pkg および AIM-IPS アップグレード ファイル、IPS-AIM-K9-6.0-4-E1.pkg、置くことを確かめて下さい。 自動更新サーバだけに 6.0(1) アップグレード ファイルを、IPS-K9-6.0-1-E1.pkg、置けば、AIM-IPS はダウンロードし、AIM-IPS のための不正確なファイルであるそれをインストールすることを試みます。

センサーをセンサーの自動アップグレードのための IDM プロシージャに関する詳細については自動的にアップデートすることを参照して下さい。

自動アップグレード コマンドを使用して下さい

自動アップデート コマンドについてはこの資料の Upgrade コマンドおよびオプション セクションを参照して下さい。

自動アップグレードをスケジュールするためにこれらのステップを完了して下さい:

1. アドミニストレーター特権があるアカウントの CLI へのログイン。
2. 自動的にアップグレード ディレクトリの新しいアップグレードを探すためにセンサーを設定して下さい。`sensor#`**`configure terminal`**`sensor(config)#`**`service host`**`sensor(config-hos)#`**`auto-upgrade-option enabled`**
3. スケジューリングを規定 して下さい:スケジュールするカレンダーに関しては特定の日の特定時にアップグレードを開始する:`sensor(config-hos-ena)#`**`schedule-option calendar-schedule`**`sensor(config-hos-ena-cal#`**`days-of-week sunday`**`sensor(config-hos-ena-cal#`**`times-of-day 12:00:00`**定期的なスケジューリングに関しては、特定の定期的な間隔でアップグレードを開始する:`sensor(config-hos-ena)#`**`schedule-option periodic-schedule`**`sensor(config-hos-ena-per)#`**`interval 24`**`sensor(config-hos-ena-per)#`**`start-time 13:00:00`**
4. ファイルサーバの IP アドレスを規定 して下さい:`sensor(config-hos-ena-per)#`**`exit`**`sensor(config-hos-ena)#`**`ip-address 10.1.1.1`**
5. アップグレード ファイルがファイルサーバにあるディレクトリを規定 して下さい :`sensor(config-hos-ena)#`**`directory /tftpboot/update/5.0_dummy_updates`**
6. ファイルサーバの認証のためのユーザ名を規定 して下さい:`sensor(config-hos-ena)#`**`user-name tester`**
7. ユーザのパスワードを規定 して下さい:`sensor(config-hos-ena)#`**`password`**`Enter password[]: `**`******`**`Re-enter password: `**`******`
8. ファイルサーバ プロトコルを規定 して下さい:`sensor(config-hos-ena)#`**`file-copy-protocol ftp`**注SCP を使用する場合、SSH 既知ホスト リストにサーバを追加するために **ssh ホスト キー** コマンドを使用して下さい従ってセンサーは SSH によってそれと通信できます。 既知ホストへホストを追加することをリストしますプロシージャのために参照して下さい。
9. 設定を確認して下さい:`sensor(config-hos-ena)#`**`show settings`**
```
    enabled   ------------------
------------------------------      schedule-option      ----------------------------------
-----------         periodic-schedule         ----------------------------------------------
--            start-time: 13:00:00            interval: 24 hours         ------------------
------------------------------     ------------------------------------------------      ip-
address: 10.1.1.1      directory: /tftpboot/update/5.0_dummy_updates      user-name: tester
password: <hidden>      file-copy-protocol: ftp default: scp   ---------------------------
------------------sensor(config-hos-ena)#
```
10. 自動アップグレード サブモードを終了して下さい:`sensor(config-hos-ena)#`**`exit`**`sensor(config-hos)#`**`exit`**`Apply Changes:?`**`[yes]:`**
11. 変更を加えるか、またはそれらを廃棄するために入力するために『Enter』 を押さない で下さい。

センサーをイメージ変更して下さい

これらの方法でセンサーをイメージ変更できます:

- CD-ROMドライブの IDS アプライアンスに関しては、リカバリ/アップグレード CD を使用して下さい。プロシージャのためにシステムイメージをアップグレードし、ダウングレード、インストールすることのリカバリ/アップグレード CD セクションを使用することを参照して下さい。
- すべてのセンサーに関しては、**回復** コマンドを使用して下さい。プロシージャのためのシステムイメージをアップグレードし、ダウングレード、インストールすることのアプリケーション パーティション セクションを回復 することを参照して下さい。
- IDS-4215 に関しては、IPS-4240 および IPS 4255 は、ROMMON をシステムイメージを復元するのに使用します。IDS-4215 システムイメージをインストールし、手順のためのシステムイメージをアップグレードし、ダウングレード、インストールすることの IPS-4240 および

IPS-4255 システムイメージ インストールすることをセクション参照して下さい。
- NM-CIDS に関しては、ブート・ローダを使用して下さい。プロシージャのためのシステムイメージをアップグレードし、ダウングレード、インストールすることの NM-CIDS System Image セクションをインストールすることを参照して下さい。
- IDSM-2 に関しては、メンテナンス パーティションからのアプリケーション パーティションをイメージ変更して下さい。インストールすることをダウングレード、プロシージャのためのシステムイメージをインストールするアップグレードの IDSM-2 System Image セクションを参照して下さい。
- AIP-SSM に関しては、**hw-module モジュール 1** を使用して ASA から**回復 します**イメージ変更して下さい**[設定して下さい | ブート]**コマンド。プロシージャのためのシステムイメージをアップグレードし、ダウングレード、インストールすることの AIP-SSM System Image セクションをインストールすることを参照して下さい。

関連情報

- **Cisco 侵入防御システムに関するサポート ページ**
- **、アップグレードし、および IPS 6.0 のためのシステムイメージをインストールすることダウングレード**
- **Cisco Catalyst 6500 シリーズ Intrusion Detection System （ IDSM-2 ） モジュール サポートページ**
- **Cisco IDS センサーおよび IDS サービス モジュール 1 におけるパスワード回復手順、IDSM-2 ）**
- **自動シグニチャ更新のトラブルシューティング**
- **テクニカルサポートとドキュメント - Cisco Systems**