目次

概要

このドキュメントでは、以前 NetRanger と呼ばれていた Cisco Secure Intrusion Detection System（IDS）バージョン 3.1 以前に関する FAQ を記載しています。

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。

一般

Q. どこで Cisco Secure IDS のその他の情報を見つけることができますか。

A. Cisco Secure IDS の詳細については製品マニュアルのフルセットを参照して下さい。

Q. IDS システム全体（IDS センサ + IDS 管理用ソフト）のためのシグニチャをアップデートする方法

A. センサーおよび管理プラットフォーム シグニチャを別々にアップグレードしなければなりません。 管理用ソフトがセンサーからのシグニチャを学べない従って同様にアップデートする必要がありますことに注目して下さい。 Cisco Secure ダウンロード（登録ユーザのみ）から各アプリケーションのための最新のシグニチャ アップデート ファイルをダウンロードして下さい。 同じ位置で利用可能 な README ファイルはアップグレード手順のための手順が含まれています。

Q. どこでシグニチャの完全なリストを見つけることができますか。

A. IDS シグニチャのリストは Cisco Secure 百科事典（登録ユーザのみ）を通して利用できます。

Q. UNIX IDS およびスタンドアロン センサのユーザ向けのデフォルトパスワードとは何か。

A. UNIX IDS スタンドアロン センサおよび IDS 管理用ソフトで、デフォルトパスワードはユーザ **netrangr** および**ルート**のための「攻撃」です。 ルート ユーザになる **su コマンドを**発行するときデフォルトパスワードはです「攻撃」。 Intrusion Detection System Module（IDSM）ブレードで、デフォルトパスワードはユーザ名 **ciscoids** のための「攻撃」です。

Q. コンフィギュレーションをダンプするために Intrusion Detection System Module

（IDSM）ブレードを得る方法

A. ローカル FTP サーバを必要とします従ってコンフィギュレーションをアップロードできます。

1. ブレードの diag モードからこのコマンドを入力して下さい。 **report systemstatus site** <ftp_target_ip_address> **user** <ftpusername> **dir** <directoryname>
2. 「システム レポートを生成する Continue に尋ねられた場合か」。続くために **y を**入力して下さい。
3. プロンプト表示されるとき指定 ユーザの FTP パスワードを入力して下さい。 プロセスが完了するとき、プロセスは失敗したかどうかまたはファイルが送信 されたら示すメッセージを受け取ります。

Q. インストールしたり/とき IDS を、ログファイルはどこで置かれますアンインストールしますか。

A. インストール/アップデート ログはこれらの場所で見つけることができます:

- ディレクター インストール ログは /var/adm/nrInstall.log にあります。
- センサー サービスパック アップデート ログは /usr/nr/sp-update/ にあります。
- シグニチャアップデート ログは /usr/nr/sig-update/ にあります。

Q. どんなシグニチャが IDS に PIX で利用できますか。

A. IDS は PIX 6.0 およびそれ以降にだけ利用できます。 シグニチャは syslog メッセージ 400000 ～ 400051 で、Cisco Secure IDS シグニチャ メッセージとして参照されて含まれています。 各シグニチャに関する詳細については PIX システムログメッセージ ドキュメントを参照して下さい。

Q. シグニチャアップデートがリリースされるとき知らせることができますか。

A. Cisco Secure IDS に関するプロダクトニュースのための E メール アラートを受け取るために Cisco IDS アクティブなアップデート通知に申し込んで下さい。

Q. IDS センサを管理するのにどのアプリケーションを使用する必要があり違いは何その間のありますか。

A. バージョン 3.1 前に、管理オプションは Cisco Secure Policy Manager（CSPM）か UNIX ディレクタを使用することです。 2 間の主な違いは UNIX ディレクタは UNIX Solarisサーバの HP OpenView の上を動作するが CSPM が Windows サーバの独立 した アプリケーションとして動作することです。 IDS 3.1 を使うと、バージョン 3.1 センサーの一部である PC でインストールされるか、または IDS Device Manager を使用するセンサーは IDS Event Viewer（IEV）またによって管理することができます。 デバイスマネージャは Secure Socket Layer（SSL）を使用してセンサーを設定した後デフォルトで有効に なります。

Q. どこで Software Development Kit（SDK）ソフトウェアを入手できますか。

A. SDK ソフトウェアはパブリックに利用できません。

IDS センサ

Q. センサ バージョン 3.x および 4.x 間の相違点とは何か。

A. バージョン 4.0 は複数の新しい 機能を提供します。 最も顕著な新しい 機能は Cisco IOS® と同じような Command Line Interface （ CLI ）です。

Q. どのように IDS でインターフェイス速度をコードすること困難な I か。

A. ハードな設定は 3.x および 4.0 コードの速度/デュプレックス サポートされないし、Feature 要求（ Cisco バグ ID CSCdy43054 （ 登録ユーザのみ ））に対して不具合があります。 機能はインターフェイスの設定で現在利用可能の 5.0 コードで利用できます。

Q. バージョン 3.0 から 3.1 へセンサソフトウェアをアップグレードする方法

A. 顧客は Cisco Secure ダウンロード（ 登録ユーザのみ ）からバージョン 3.1 のためのアップデート ファイルをダウンロードできます。

Q. バージョン 2.5 から 3.0 へセンサソフトウェアをアップグレードする方法

A. 顧客は Cisco Secure ダウンロード（ 登録ユーザのみ ）からバージョン 3.0 のためのアップデート ファイルをダウンロードできます。 サービスパックおよびシグニチャアップデートがバージョン 2.5 にインストールされているソフトウェア アップデートを同じようにインストールして下さい。 プロシージャは Cisco IDS センサー設定に関する注記 バージョン 3.0 に詳しく説明があります。

Q. バージョン 2.2 から 3.0 へセンサソフトウェアをアップグレードする方法

A. 3.0 アップグレード ファイルは Cisco Secure ダウンロード（ 登録ユーザのみ ）からダウンロードすることができますがこのファイルは 2.5 の前に更新バージョンにできません。 Product Upgrade Tool （ 登録ユーザのみ ）を通して利用可能 な ソフトウェア バージョンから 2.2 に 3.0 をアップグレードするのにアップグレード/リカバリ CD を使用して下さい。 この CD のための部品番号は IDS-SW-U です。

注アップグレード/リカバリ CD を発注する有効なサポート 契約を持たなければなりません。

Q. キーボードを接続し、がセンサーに監視します、きちんと起動しません。 どうすればよいのですか。

A. サポートされたキーボードを使用している確認し、監視して下さいことを。 いくつかのブランドおよびモデルは Cisco Secure IDS と互換性がないし、IDS センサがきちんと起動することを防ぎます。 特定のブランド詳細については Cisco Secure IDS 機器 起動障害を参照して下さい。

Q. Cisco Secure ダウンロードの IDS セクションで、アップデート ファイルの 2 つの型が表示されます（ サービスパックおよびシグニチャ ）。 これらのファイル間の違いとは何か。

A. これらのファイルのそれぞれはここに説明される命名規則によって示されるようにソフトウェ

ア アップデートか付加の、設定 される仕様が含まれています。

- IDS Sensor アプライアンス ソフトウェアのためのサービスパック アップデートは IDS センサ コア アプリケーション アプリケーション・ ソフトウェア、またバグ修正に機能強化が含まれています。 たとえば、**IDSk9-sp-3.0-5-S17.bin** と名付けられるファイルはソフトウェア バージョン 3.0(5) プラス シグニチャー定第 17 にアップデートが含まれています。
- シグニチャ アップデート ファイルはシグニチャ（攻撃フィンガープリント）の更新だけ含まれています。 たとえば、**IDSk9-sig-3.0-5-S18.bin** と名付けられるファイルは 3.0(5) センサソフトウェアのためのシグニチャー定第 18 が含まれています。

顧客は Cisco Secure ダウンロード（登録ユーザのみ）サイトからこれらのファイルをダウンロードできます。

Q. どのようにセンサーが正しくルータを排除するために設定されるかどうか言うことができますか。

A. ユーザ **netrangr** としてセンサーへのログインはこのコマンドを実行し、:

nrgetbulk *<appID> <sensorHostID> <sensorOrgID> <priority> <token>*
それ示します不正侵入をブロックするのに使用されるシャニング デバイスの IP アドレスを「*<IP_address>* アクティブと」同じような応答を受け取る必要があります。 この出力はコマンド構文および予想される 応答の例を示したものです:

```
netrangr@sensor:/usr/nr>nrgetbulk 10003 38 1000 1 NetDeviceStatus10.48.66.68 ActiveSuccess
```

ルータにログイン センサーがログオンされるかどうか見る **who コマンドを**発行するためにまたでき。

Q. nrconns コマンドを発行するとき"value not set"を示すエラーメッセージが表示されています。 問題を解決するには、どうすればよいですか

A. このエラーメッセージはセンサーの /usr/nr/etc/routes や /usr/nr/etc/hosts ファイルにおける潜在的な問題を示唆します。 … /routes ファイルはセンサーとディレクター間の postofficed 通信を定義します。 … /hosts ファイルはセンサーおよびディレクターの名前および IP アドレスを定義します。

ユーザルートとしてログインまたでき、**sysconfig-sensor コマンドを**実行し、IDS コミュニケーション インフラストラクチャ 情報を再度入力します。

Q. それらをどこかに保存するためにセンサーからログファイルをコピーするのに FTP を使用する方法

A. このプロシージャに関する詳細については表示されるべきコピー IP ログファイルを参照して下さい。

Q. センサソフトウェア バージョン 2.5 および 3.1 の configd デーモンに何が起こりましたか。

A. 2.2.x コード ベースの UNIX ディレクタ、またセンサー両方のすべてのコマンドを処理する Configd はデーモンです。 2.5 および 3.0 コード ベースでは、この機能性はもはや存在 する他のデーモンおよび configd デーモンに吸収されませんでした。

Q. センサーのシグニチャをアップデートするとき、表示されます: `NetRanger` 。というエラー メッセージが表示されます。 何をこれについてする必要がありますか。

A. nr.packetd がデーモン リストにあるようにするためにセンサーの /usr/nr/etc/daemons ファイルを編集して下さい。 それからサービスを停止し、開始して下さい。

Q. 制御 インタフェースである探知インターフェイスであり、IDS 4210、か。

A. 上の制御 インタフェースは **iprb1** です: 、下部のの探知インターフェイスは **iprb0** であり:。

Q. センサーの `ifconfig - a` 発行するときだけ 1 つのインターフェイスを参照する理由

A. **ifconfig コマンドは**制御 インタフェースだけ示す必要があります。 他はインターフェイスまだセンサー、ユーザによって（探知インターフェイス）ではないですそれを見られますはず使用されますが。 このインターフェイスを、ログイン ルートとして参照し、インターフェイス名を判別する **ifconfig - a コマンドを**発行する必要があれば。 特定のインターフェイスのステータスをチェックするために **ifconfig** *<interface>* **錘**コマンドを発行して下さい。

Q. どのようにセンサーのインターフェイス速度をハードコードできますか。

A. センサーのインターフェイス速度をハードコードすることは必要ではないはずであるし、テクニカル サポートによってサポートされません。 スイッチが自動ネゴシエーションのために設定される場合、インターフェイスは接続されるスイッチと速度をネゴシエートします。 ネットワークからのセンサーへのトラフィックは単方向です（すなわち、センサーは受け取ります）。 従って、それは 100 半二重はネゴシエートされたことをスイッチが示す場合一般に適切です（想定はスイッチポートが 100 M）であることです。

UNIX Director

Q. ディレクターの 2.2.x バージョンと新しい 3.0 センサーを使用できますか。

A. はい、しかしあなたバージョン 2.2.3 または それ 以降にディレクター ソフトウェアをアップグレードするべきです。 登録 ユーザは Cisco Secure ダウンロード（登録ユーザのみ）からこれらのファイルをダウンロードできます。

Q. どのようにディレクター デーモンのどんなバージョンを使用しているか述べることができますか。

A. **cat /usr/nr/VERSION** コマンドを発行し、出力は含まれているバージョン番号がチェックして下さい。

注ディレクターの **nrvers コマンド**の出力はデーモンのバージョン実行する、ディレクター ソフトウェアのバージョン自体を告げないがディレクターで告げます。

Q. 設定をダンプするためにディレクターを得る方法

A. ユーザ **netrangr** としてログインは /usr/nr/var/tmp/Report_For_Director.html と名付けられるファイルに構成情報を送信 するためにスクリプト /usr/nr/bin/director/nrCollectInfo を実行し。

Q. HP OpenView ディスプレイの多くのエラーが（ 可能性としては以上 1,000 ）あります。 それらを削除しますが、もどって来続けます。 これは、なぜですか。

A. IDS ディレクターがエラーでいっぱいになり、それらをすべて表示することができない場合それはファイルにバッファリングし始めます。 IDS デーモンを停止し、ファイルを取り払う開いたがある OpenView マップを終了して下さい。 ファイル **/usr/nr/var/nrDirmap.buffer.default を**削除し、そして IDS デーモンおよび OpenView マップを再起動して下さい。

Q. HP OpenView マップにアラームを得る問題があっています。 /usr/nr/var/errors.nrdirmap でエラーが表示され続けます。 どうすればよいのですか。

A. 2.2.2 以前の IDS バージョンでは、するべき最も容易な事柄は OpenView データベースを一掃することです。 /var/opt/OV/share/databases/openview のデータベース ライフ。 OpenView データベースを削除するためにこれらのステップを完了して下さい。

1. すべてを **ovstop コマンド**で OpenView 開いたマップ閉じ、そして **nrstop コマンド**で IDS サービスを停止して下さい。
2. ユーザルートおよび問題 **/usr/nr/bin/director/nrDeleteOVwDb** として**ログイン。**
3. /usr/nr/var ディレクトリのすべての「error.*」ファイルを取除いて下さい（ たとえば、errors.configd ）。
4. **nrstart コマンド**でサービスを再開し、そして **ovstart コマンド**で OpenView を再起動して下さい。 **注**ディレクター バージョン 2.2.2 では、全体のデータベースの代りに OpenView データベースの IDS 部品だけ取除くことができます。 このプロシージャは IDS ディレクター コンフィギュレーション ガイドに説明があります。

Q. OpenView マップのアラームを得ることができません。 ディレクターの /usr/nr/var/errors.postofficed ファイルは nrdirmap はこのマシンで動作するために認可されないことを言うメッセージが含まれています。 これはどのように解決すればよいですか。

A. このコマンドを実行して下さい。

```
cp /usr/nr/etc/.lt/license-all.lic /usr/nr/etc/licenses
```

ユーザ **netrangr が**ファイルを所有するように、そして再開します IDS サービスをして下さい。

Q. nrConfigure ユーティリティを実行し、ディレクターをダブルクリックするとき、このメッセージが表示されます: 「*<director_name>* のためのセンサーの種類があることが不可能。 ポストオフィスおよび packetd が」動作していることを確認して下さい。 どうすればよいのですか。

A. 問題は nrConfigure が（ によってべきな ）の packetd プロセスをディレクターのデーモン ファイル見るので発生します。 それがセンサーだったように nrConfigure がバージョンのためにディレクターを問い合わせるとき、ディレクターはセンサ バージョンと応答できません。

この問題を解決するためにこれらのステップを完了して下さい。

1. これらのプロセスがセンサーでしか動作する必要がないので、nr.packetd、nr.sensord および nr.managed のための /usr/nr/etc/daemons ファイルおよび Remove エントリを編集して下さい。
2. **nrstop コマンド**でサービスを停止し、そして **nrstart コマンド**でサービスを再開して下さい。
3. nrConfigure がシャットダウンされたことを確認して下さい。
4. **ovw コマンド**で OpenView を開始して下さい。
5. 破損した nrConfigure データベースを削除するために Security > Advanced > nrConfigure DB > Delete の順に選択 して下さい。
6. 続行することを頼まれた場合**はい**入力して下さい。
7. ディレクターおよび OpenView 主要なウィンドウのセンサーすべてを強調表示して下さい。
8. マシンからの現在のコンフィギュレーション バージョンで新しい nrConfigure データベースを作成するために Security > Advanced > nrConfigure DB > Create の順に選択 して下さい。

Q. OpenView マップでデフォルトで有効に なることから nrdirmap アプリケーションを守る方法

A. UNIX ディレクタの IDS アプリケーションを実行するユーザはまた OpenView の他のアプリケーションを実行できます。 これは助言されません、場合によっては避けることができません。 問題は他のアプリケーションが OpenView で動作するとき好ましくない nrdirmap が OpenView 各マップのためにデフォルトで有効に なることです。

マップにそれらで有効に なる nrdirmap がある選択できるようにデフォルトを変更するために UNIX ディレクタのこれらのステップを完了して下さい。

1. ユーザ **netrangr** としてログイン。
2. 型 **cd $OV_REGISTRATION/C.**（ OV_REGISTRATION は環境変数の一部です。 通常パスは /etc/opt/OV/share/registration/C です。 ）
3. 型 **SU ルート**。
4. この出力が示すように nrdirmap ファイルを編集し、「コマンド」行を変更して下さい:
   ```
   Command -Shared -Initial "nrdirmap"; !--- Changes to:Command -Shared -Initial "nrdirmap -d";
   ```
5. nrdirmap ファイルを保存して下さい。
6. OpenView をリサイクルして下さい。 マップが **ovw コマンド**で始動する時この場合、**ps -ef をタイプします | グレップ dirmap は**ここに示されているそれと同じような出力をもたらす必要があります。 `- d` スイッチの `nrdirmap` 注意して下さい。 `>ps -ef | grep dirmap`netrangr 7175 6820 0 09:50:47 pts/2 0:00 grep dirmapnetrangr 7158 7152 0 09:50:21 ? 0:00 nrdirmap -d

OpenView で作成される新しいマップに今デフォルトで有効に なる nrdirmap がありません。 インストールされる nrdirmap でマップを作成したいと思う場合このプロシージャが説明するので OpenView GUI からそれをして下さい。

1. OpenView 主要なメニューから、新しいマップの名前を Map > New の順に選択 し、入力して下さい。
2. 設定可能なアプリケーションの下で、NetRanger/ディレクターを見るはずです。 **NetRanger/ディレクターを**選択し、『Configure For this Map』 をクリック して下さい。
3. 「言うオプションに関しては nrdirmap はこのマップのために有効に する必要がありますか。」、nrdirmap を有効に したいと思う場合『True』 を選択 して下さい。

4. 『Verify』 を選択 し、『OK』 をクリック して下さい。

Q. 以前のバージョンでそうする可能性があるのに、ディレクター バージョン 2.2.3 にアップグレードし、非常により 5 今水平のにイベントの重大度を設定できません。 なぜでしょうか。

A. 重大度はディレクターのバージョン 2.2.3 で範囲だけ 1 ～ 5.サポートするために変更されました。

IDS Cisco Secure Policy Manager (CSPM)

Q. IDS センサを管理するのに CSPM のどのバージョンを使用する必要がありますか。

A. 現在 CSPM のバージョン 2.3i は CSPM 3.0 ができない一方 IDS センサを管理できるものです。 センサーおよび他の Cisco Secure デバイスを管理すればのに CSPM を (PIX、ルータのような) 使用すれば、2 つの個々のウィンドウ サーバで 2 CSPM バージョンを (2.3i および 3.x) インストールして下さい。 対応するデバイスを管理するのにサーバのそれぞれを使用できます: センサーのための CSPM 2.3i および PIX のための CSPM 3.x、ルータ、等。

Q. IDS センサを管理し、通信作業を確かめるために CSPM を設定する方法

A. CSPM を IDS センサを管理するために通信作業を確認するために設定する方法に関する詳細については CSPM での Cisco Secure IDS センサーの設定を参照して下さい。

Q. CSPM のアプライアンスのためのシグニチャを調整できますか。

A. 調整はシグニチャが (スイープするのホストの数のような) 奪取 し、設定操作および重大度をように意味しないものを変更することを始動させることができる含みます。

CSPM は (あらゆるバージョンで) アプライアンスのためのシグニチャを調整ことをできません。 それはシグニチャの操作および重大度しか設定なできます。 すなわち、重大度 シグニチャに関連付ける操作がそのシグニチャを始動させるものが設定できないし、が、CSPM は設定できます。 センサーの SigWizMenu がセンサーを調整するのに使用されなければなりません。 設定の異なる部分に影響を与えるので SigWizMenu および CSPM は同じセンサーを設定するのに使用することができます。

注UNIX ディレクタ バージョン 2.2.3 または それ 以降を使用する場合、nrConfigure ユーティリティは SigWizMenu が設定するすべてを設定できます。 2.2.3 にアップグレードした後、SigWizMenu の代りにシグニチャを調整するのに nrConfigure を使用する必要があります。

関連情報

- Cisco 侵入防御システム 製品サポート
- Cisco Secure Intrusion Detection System に関する文書
- Cisco Secure Intrusion Detection System のための Field Notice
- テクニカルサポートとドキュメント - Cisco Systems