侵入検知システム モジュールのアップグレード

目次

概要

この文書では、Cisco Intrusion Detection System Module (IDSM; 侵入検知システム モジュール) のアップグレードをアプリケーション パーティション、サービス パック、およびシグニチャの更新で行う方法について説明します。 IDS Sensor のアップグレードの詳細は、「Catalyst 6000 Intrusion Detection System Module」を参照してください。

前提条件

要件

設定を開始する前に、次の前提条件が満たされていることを確認してください。

- アップグレードする時点までアップ状態で、Director と通信を行っている IDS Sensor を使用します。
- アップグレードを行う前に、あらゆる種類のファイアウォールやパケット フィルタリング デバイスから干渉を受けずに、Sensor に対して ping、パッシブ FTP および Telnet を実行できることが必要です。

- パッシブ モードをサポートしている FTP サーバを使用できることを確認してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- IDSM Sensor モデル WS-X6381-IDS。ソフトウェア バージョン 2.5 を実行。
- Solaris バージョン 2.6、HP OpenView バージョン x5.01、IDS Director ソフトウェア バージョン 2.2.3 S9 を実行する IDS Director。
- Sensor および Director に対するパッシブ FTP と Telnet が可能な Solaris バージョン 2.8 を実行するワークステーション。
- ダウンロードからファイルをダウンロードして下さい（IDSk9-sig-3.0-2-S10.bin および nrdirUpdate-S10.bin はこの資料で、使用されます）。

注: この文書で使用されているものと完全に同じバージョンは、現在入手できない場合があります。

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

- IDS Director の名前は「dir1」で、IP アドレスは 192.168.1.3 です。
- IDSM Sensor の名前は「idsm」で、IP アドレスは 192.168.1.2 です。
- この例では、ホスト ID と IP アドレスの最後のオクテットが一致しています。
- 組織 ID は「1」として定義されています。
- FTP サーバの IP アドレスは 10.0.0.1 です。

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。

IDSM アプリケーション パーティションのアップグレード

以下の手順では、IDSM のアプリケーションのバージョンを 2.5(1)S2 から 3.0(1)S4 にアップグレードする方法について説明します。 IDSM のハードディスクはすべてフォーマットされ、設定はすべて失われてしまうため、アップグレード作業の前に IDSM の設定を保存しておいてください。

手順説明

下記に提供される手順に従って下さい。

1. IDSM にセッションを確立し、show configuration コマンドの出力を保存します。次に例を示します。`Console> (enable) **session 8** Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: **show configuration** Using 37584896 out of 267702272 bytes of available memory ! Using 439668736 out of 4211310592 bytes of available disk space ! Sensor version is : **2.5(1)S0** ! Sensor application status: nr.postofficed running nr.fileXferd running nr.loggerd running nr.packetd running nr.sapd running Configuration last modified Never Sensor: IP Address: 192.168.1.2 Netmask: 255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host ID: 2 Host Port: 45000 Organization Name: cisco Organization ID: 1 Director: IP Address: 192.168.1.3 Host Name: dir1 Host ID: 3 Host Port:`

```
45000 Heart Beat Interval (secs): 5 Organization Name: cisco Organization ID: 1 Direct
Telnet access to IDSM: disabled
```

2. ダウンロードから適切なファイルをダウンロードして下さい。IDS Sensor と readme ファイルは、「Cisco IDS Appliance Sensor 3DES」のセクションにあります。 IDS Director と readme ファイルは、「Cisco IDS Director 3DES」のセクションにあります。 この文書では、次のファイルを使用していますが、実際にはその時点での最新ファイルを使用してください。
```
IDSMk9-a-3.0-1-S4.readme
IDSMk9-a-3.0-1-S4-1.cab
IDSMk9-a-3.0-1-S4-2.cab
IDSMk9-a-3.0-1-S4-3.cab
IDSMk9-a-3.0-1-S4-4.cab
IDSMk9-a-3.0-1-S4-5.cab
IDSMk9-a-3.0-1-S4.dat
```
3. これらのファイルを FTP サーバの適切なディレクトリに置きます。この例では、ルート ディレクトリにファイルを置いています。 次に示す出力例は、FTP クライアントから FTP サーバにアクセスしたときのものです。
```
user@solariswkstn% ftp user@solariswkstn Connected to solariswkstn.cisco.com. 220 solariswkstn FTP server (SunOS 5.8) ready. Name (solariswkstn:username): user 331 Password required for user. Password: 230 User user logged in. Remote system type is UNIX. Using binary mode to transfer files. ftp> pwd 250 CWD command successful. 257 "/" is current directory. ftp> ls 227 Entering Passive Mode (10,0,0,1,169,229) 150 ASCII data connection for /bin/Ls (10.0.0.1,43494) (0 bytes). total 110878 -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:34 IDSMk9-a-3.0-1-S4-1.cab -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:22 IDSMk9-a-3.0-1-S4-2.cab -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:24 IDSMk9-a-3.0-1-S4-3.cab -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:24 IDSMk9-a-3.0-1-S4-4.cab -rw-r--r-- 1 jlimbo cisco 1126530 May 11 15:23 IDSMk9-a-3.0-1-S4-5.cab -rw-r--r-- 1 jlimbo cisco 600 May 11 15:20 IDSMk9-a-3.0-1-S4.dat 226 ASCII Transfer complete. ftp> exit 221 Goodbye. user@solariswkstn%
```
4. メンテナンス パーティションをアクティブ パーティションとして設定 し、そして IDSM にメンテナンス パーティションに (アプリケーションはデフォルト設定です) コンソール接続を行い、IDSM のネットワークコンフィギュレーション パラメータを設定 して下さい。以下の例では、IDSM は Catalyst 6509 シャーシのスロット 8 にあります。
```
Console> (enable) set boot device hdd:2 Console> (enable) reset 8 This command will reset module 8. Unsaved configuration on module 8 will be lost Do you want to continue (y/n) [n]? y Module 8 shut down in progress, please don't remove module until shutdown completed. Console> (enable) Module 8 shutdown completed. Module resetting... Console> (enable) session 8 Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: maintenance# maintenance# diag maintenance(diag)#ids-installer netconfig /configure /ip=192.168.1.2 /subnet=255.255.255.0 /gw=192.168.1.1 STATUS: Network parameters for the config port have been configured!
```
注: モジュールをリセットして、変更が反映されるようにします。
5. IDSM のリブートが終了したら、再度 IDSM にセッションを確立し、ids-installer コマンドを発行して非アクティブなアプリケーション パーティションをインストールします。次に例を示します。
```
Console> (enable) session 8 Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: maintenance# diag maintenance(diag)# ids-installer system /nw /install /server=10.0.0.1 /user=user /save=yes /dir='//' /prefix=IDSMk9-a-3.0-1-S4 Please enter login password: ********* Downloading the image.. File 05 of 05 FTP STATUS: Installation files have been downloaded successfully! Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is E893-5968 Extracting the image... ########################## ----snip----- STATUS: Image has been successfully installed on drive C:\! maintenance(diag)# exit
```

アプリケーション パーティションのアップグレードの検証

特定の **show** コマンドは、Output Interpreter Tool (登録ユーザ専用) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

IDSM をリブートしてアプリケーション パーティションに戻り、イメージが正しくアップグレードされていることを確認してください。次に例を示します。

```
Console> (enable) set boot device hdd:1 Console> (enable) reset 8 This command will reset module 8. Unsaved configuration on module 8 will be lost Do you want to continue (y/n) [n]? y Module 8 shut down in progress, please don't remove module until shutdown completed. Console> (enable) Module 8 shutdown completed. Module resetting... Console> (enable) session 8 Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: idsm# show configuration Using 48259072 out of 267702272 bytes of available memory ! Using 504688640 out of 4211310592 bytes of available disk space ! Sensor version is : 3.0(1)S4 ! Sensor application status: nr.postofficed running nr.fileXferd running nr.loggerd running nr.packetd running nr.sapd running Configuration last modified Wed May 01 01:03:56 2002 Sensor: IP Address: 192.168.1.2 Netmask: 255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host ID: 2 Host Port: 45000 Organization Name: cisco Organization ID: 1 Director: IP Address: 192.168.1.3 Host Name: dir1 Host ID: 3 Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: cisco Organization ID: 1
```

IDSM サービス パックのアップグレード

IDSN サービスパックをアップデートするのに次のプロシージャを使用して下さい。

1. **セッション#**コマンドの発行による IDSM へのセッションは次の例に示すように (#モジュール番号があるかところで) 、および **configure terminal コマンドを**、発行します。`idsm# idsm#configure terminal`
2. apply ftp://<username@server/dir/filename> コマンドを発行して FTP 接続し、サービス パックを適用します。次に例を示します。`idsm(config)#apply ftp://user@10.0.0.1//IDSMk9-sp-3.0-3-S10.exe WARNING: Installing Service Pack will temporarily disable IDS. Continue with IDS Service Pack install?: y Enter the FTP user password: ********* Connecting to site... Receiving file. Installing as 3.0(3)S10 Installing files from Service Pack 3.0(2) Installing files from Signature Update 10 Starting NetRanger Signatures Merging Utility... Checking file: C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf... Adding signature: SigOfGeneral 993 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3111 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3112 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3114 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3160 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3162 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3454 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3455 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 4060 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 4101 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 4601 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5158 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5159 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5160 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5161 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5162 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5163 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5164 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5165 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5166 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5167 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5168 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5169 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5170 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5171 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5172 to C:\Program Files\ Cisco`

```
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5173 to C:\Program
Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5174 to
C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
5175 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 5176 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 6197 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6901 to C:\Program Files\ Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 6902 to C:\Program
Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 6903 to
C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
6910 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 6920 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Installing
files from Service Pack 3.0(3) The Install for IDSM Service Pack file IDSMk9-sp-3.0-3-
S10.exe was successful 2002 May 13 18:29:34 %PAGP-5-PORTFROMSTP:Port 8/1 left bridge port
8/1 2002 May 13 18:29:34 %DTP-5-NONTRUNKPORTON:Port 8/1 has become non-trunk Systems needs
to be restarted. Rebooting... Module 8 shut down in progress, please don't remove module
until shutdown completed. idsm(config)# Console> (enable) Module 8 shutdown completed.
Module resetting...
```

サービス パックのアップグレードの検証

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

session # コマンド（# はモジュール番号）を発行して IDSM へのセッションを確立し、show configuration コマンドを発行します。次に例を示します。

```
idsm#show configuration Using 46059520 out of 267702272 bytes of available memory ! Using
466886656 out of 4211310592 bytes of available disk space ! Sensor version is : 3.0(3)S10 !
Sensor application status: nr.postofficed running nr.fileXferd running nr.loggerd running
nr.packetd running nr.sapd running Configuration last modified Fri May 10 23:02:57 2002 Sensor:
IP Address: 192.168.1.2 Netmask: 255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host
ID: 2 Host Port: 45000 Organization Name: cisco Organization ID: 1 Director: IP Address:
192.168.1.3 Host Name: dir1 Host ID: 3 Host Port: 45000 Heart Beat Interval (secs): 5
Organization Name: cisco Organization ID: 1 Direct Telnet access to IDSM: enabled Current access
list entries: [1] 192.168.1.0 0.0.0.255 idsm#
```

IDSM シグニチャのアップグレード

ISDM シグニチャをアップグレードするのに次のプロシージャを使用して下さい。

1. **セッション#**コマンドの発行による IDSM へのセッションは次の例に示すように（#モジュール番号があるかところで）、および **configure terminal コマンドを**、発行します。`idsm#` `idsm#configure terminal`
2. apply ftp://<username@server/dir/filename> コマンドを発行して FTP 接続し、IDSM シグニチャを適用します。次に例を示します。`idsm(config)#apply ftp://user@10.0.0.1//IDSMk9-sig-3.0-3-S13.exe` WARNING: Installing Signature Update will temporally disable IDS. Continue with IDS Signature Update install?: % Please answer 'yes' or 'no'. Continue with IDS Signature Update install?: yes Enter the FTP user password: ********* Connecting to site... Receiving file. WARNING!!! Installation of this IDSM Signature Update will now prevent unistalling of the current IDSM Service Pack 3.0(3). WARNING!!! To uninstall IDSM Service Pack 3.0(3) you will need to first uninstall this IDSM Signature Update. Starting NetRanger Signatures Merging Utility... Checking file: C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf... Adding signature: SigOfGeneral 1107 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3116 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3117 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3118 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3119 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.

```
Adding signature: SigOfGeneral 3120 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3163 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3403 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
3456 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 3501 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 3651 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 4507 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5178 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5179 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
5180 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 5181 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 5182 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5183 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5184 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5188 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
5191 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 5194 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 5195 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5196 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5197 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5199 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
5200 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. The Install for IDSM
Signature Update file IDSMk9-sig-3.0-3-S13.exe was successful Systems needs to be
restarted. Rebooting... Module 8 shut down in progress, please don't remove module until
shutdown completed. idsm(config)# Console> (enable) Module 8 shutdown completed. Module
resetting... 2002 May 13 18:58:08 %SYS-3-SUP_OSBOOTSTATUS:Starting IDSM Diagnostics 2002
May 13 18:58:50 %SYS-3-SUP_OSBOOTSTATUS:IDSM diagnostics completed successfully. 2002 May
13 18:58:56 %SYS-5-MOD_OK:Module 8 is online 2002 May 13 18:58:56 %PAGP-5-PORTFROMSTP:Port
8/1 left bridge port 8/1 2002 May 13 18:58:56 %DTP-5-TRUNKPORTON:Port 8/1 has become dot1q
trunk 2002 May 13 18:58:56 %PAGP-5-PORTTOSTP:Port 8/2 joined bridge port 8/2 2002 May 13
18:58:57 %SYS-3-MOD_PORTINTFINSYNC:Port Interface in sync for Module 8 2002 May 13 18:58:57
%PAGP-5-PORTTOSTP:Port 8/1 joined bridge port 8/1 Console> (enable) Console> (enable)
session 8 Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids
Password:
```

シグニチャ アップグレードの検証

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

session # コマンド（# はモジュール番号）を発行して IDSM へのセッションを確立し、show configuration コマンドを発行します。次に例を示します。

```
idsm#show configuration Using 46014464 out of 267702272 bytes of available memory ! Using
470089728 out of 4211310592 bytes of available disk space ! Sensor version is : 3.0(3)S13 !
Sensor application status: nr.postofficed running nr.fileXferd running nr.loggerd running
nr.packetd running nr.sapd running Configuration last modified Fri May 10 23:02:57 2002 Sensor:
IP Address: 192.168.1.2 Netmask: 255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host
ID: 2 Host Port: 45000 Organization Name: cisco Organization ID: 1 Director: IP Address:
192.168.1.3 Host Name: dir1 Host ID: 3 Host Port: 45000 Heart Beat Interval (secs): 5
Organization Name: cisco Organization ID: 1 Direct Telnet access to IDSM: enabled Current access
list entries: [1] 192.168.1.0 0.0.0.255 idsm#
```

IDSM2 のアップグレード手順

以降のセクションは ISDM2 のアップグレードで情報を提供します。

メンテナンス パーティションのアップグレード手順

メンテナンス パーティションを 1.3.1 から 1.3.2 へアップグレードするために、スイッチで次のコマンドの発行によってアプリケーション パーティションで IDSM2 ブレードを起動して下さい。

```
reset <mod> hdd:1

Console> (enable) reset 5 hdd:1
```

```
idsm-2#show version Application Partition: Cisco Systems Intrusion Detection Sensor, Version
4.0(1)S41 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDS2-XL Sensor up-time is 43 min. Using
748920832 out of 1979682816 bytes of available memory (37% usage) Using 997M out of 17G bytes of
available disk space (6% usage) MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running Logger
2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running NetworkAccess 2003_Jan_23_02.00
(Release) 2003-01-23T02:00:25-0600 Running TransactionSource 2003_Jan_23_02.00 (Release) 2003-
01-23T02:00:25-0600 Running WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600 Upgrade History: No upgrades
installed Maintenance Partition Version 1.3(1) idsm-2(config)#upgrade ftp://user@10.1.1.1/mp.1-
3-2.bin.gz Password: ******** Warning: Executing this command will re-image the maintenance
partition. The system may be rebooted to complete the upgrade. Continue with upgrade? : yes
```

イメージ変更が完了したおよびシステムがリブートしたら、**show version** はアップグレードが正常だったことを確認することを可能にします。

```
idsm-2#show version Application Partition: Cisco Systems Intrusion Detection Sensor, Version
4.0(1)S41 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDS2-XL Using 762945536 out of 1979682816
bytes of available memory (38% usage) Using 1007M out of 17G bytes of available disk space (7%
usage) MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running AnalysisEngine
2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running Authentication 2003_Jan_23_02.00
(Release) 2003-01-23T02:00:25-0600 Running Logger 2003_Jan_23_02.00 (Release) 2003-01-
23T02:00:25-0600 Running NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running WebServer
2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running CLI 2003_Jan_17_18.33 (Release)
2003-01-17T18:33:18-0600 Upgrade History: No upgrades installed Maintenance Partition Version
1.3(2)
```

メンテナンス パーティションからのアプリケーション パーティションのイメージ変更

注意： IDS モジュールをイメージ変更した後、**setup コマンド**を使用して IDS モジュールを初期化して下さい。 このプロセスはすべてのセンサー設定を取除き、アプリケーション パーティションをイメージ変更します。 このプロセスはアプリケーション パーティションが破損しているまたは得難いときだけ使用する必要があります。 アプリケーション パーティションがアクセス可能である場合、現在のコンフィギュレーションが無効になることを避けるためにアプリケーション パーティション自体からアップグレードするのにマイナー な イメージアップグレードを使用して下さい。

1. スイッチの次のコマンドの発行によってメンテナンス パーティションに（起動後）入って下さい。`reset <mod> cf:1`

   ```
   Console> (enable)reset 5 cf:1 This command will reset module 5. Unsaved configuration on
   module 5 will be lost Do you want to continue (y/n) [n]? y SendShutDownMsg: shut down
   module 5 no responce, reset module... Module 5 experienced problems during shutdown. It may
   take several minutes to come online. Console> (enable) 2003 Sep 02 14:01:55 %SYS-3-
   SUP_OSBOOTSTATUS:MP OS Boot Status: f inished booting Console> (enable) Console> (enable)
   ```

sess 5 Trying IDS-5... Connected to IDS-5. Escape character is '^]'. Cisco Maintenance image

2. 次のユーザ名 および パスワードの入力によって IDS モジュールにログイン して下さい。
login: **guest** Password: **cisco** Maintenance image version: 1.3(2)
guest@localhost.localdomain#ip address 172.16.171.22 255.255.255.192
guest@localhost.localdomain#ip gateway 172.16.171.1
3. **configure terminal コマンド**を使用して設定ターミナル モードを開始して下さい。
4. **アップグレード ftp:// <user>@< FTP サーバ IP>/<directory path>/<image file>** コマンドを使用してイメージ変更を行って下さい。FTP サーバ パスワードを入力するためにプロンプト表示されます (必要であれば) 。 またインストールを続行するためにプロンプト表示されます。 続くために **y を**入力して下さい。guest@localhost.localdomain#**upgrade ftp://user@10.1.1.1/ WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz** ftp://user@10.1.1.1//home/user/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz (unknown size) /tmp/upgrade.gz [-] 65259K 66825226 bytes transferred in 13.38 sec (4878.70k/sec) Upgrade file ftp://user@10.1.1.1//home/user/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz is downloaded. Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing it [y|N]: y Proceeding with upgrade. Please do not interrupt. If the upgrade is interrupted or fails, boot into Maintenance image again and restart upgrade. Creating IDS application image file... Initializing the hard disk... Applying the image, this process may take several minutes... Performing post install, please wait... Application image upgrade complete. You can boot the image now.
guest@localhost.localdomain#**exit** logout
5. **リセット <module number> hdd:1** コマンドの入力によってアプリケーション パーティションに IDS モジュールをリブートして下さい。Console> (enable)**reset 5 hdd:1** This command will reset module 5. Unsaved configuration on module 5 will be lost Do you want to continue (y/n) [n]? **y** Module 5 shut down in progress, please don't remove module until shutdown completed. Console> (enable) Module 5 shutdown completed. Module resetting...
6. IDS モジュールがリブートしたら、ソフトウェア バージョンをチェックして下さい。**注: これはまた確認するために使用することができます。**Console> (enable)
Console> (enable)**sess 5** Trying IDS-5... Connected to IDS-5. Escape character is '^]'.
login: **cisco** Password: You are required to change your password immediately (password aged)
Changing password for cisco (current) UNIX password: New password: Retype new password:
NOTICE This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto If you require further assistance please contact us by sending email to export@cisco.com. sensor# sensor#**show version** Application Partition: Cisco Systems Intrusion Detection Sensor, Version 4.1(1)S47 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDSM2-BUN Sensor up-time is 4 min. Using 701689856 out of 1979682816 bytes of available memory (35% usage) Using 527M out of 17G bytes of available disk space (4% usage) MainApp 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running AnalysisEngine 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running Authentication 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running Logger 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running NetworkAccess 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running TransactionSource 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running WebServer 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running CLI 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Upgrade History: No upgrades installed Maintenance Partition Version 1.3(2)
7. アプリケーション パーティション CLI への**ログインは setup コマンド**を使用して IDS モジュールを、初期化し。

マイナー な イメージアップグレード

このアップデートはアプリケーション パーティションがまだアクセス可能であるが、このアプリ

ケーションの一部だけ壊れている状況で使用することができます。 アプリケーション パーティションをイメージ変更するのに完全なイメージの使用と比べてマイナー な イメージはセンサー コンフィギュレーションを保ちます。

マイナー な アップデートをインストールするために、次の手順に従って下さい:

1. アドミニストレーター特権のアカウントを使用して CLI にログイン して下さい。
2. **configure terminal コマンドの**発行によってコンフィギュレーションモードを開始して下さい。
3. センサーをアップグレードするために**アップグレード[URL]/<filename>** コマンドを入力して下さい。**[URL]**指す Uniform Resource Locator はシグニチャアップデート パッケージがどこにを見つけられるかあります。 たとえば、FTP によってアップデートを取得するために、次を入力して下さい:
   upgrade ftp://<username>@<ip-address>//<directory>/<filename> 利用可能 な 転送する メソッドは SCP、FTP、HTTP、または HTTPS です。
4. プロンプト表示された場合適切なパスワードを入力して下さい。
5. プロンプト表示された場合アップグレードを完了するために、**はい**入力して下さい。

IDSM2 サービスパックかシグニチャのアップグレード手順

ISDM2 サービス袋かシグニチャをアップグレードするのに次のプロシージャを使用して下さい。

1. サービスパックまたはシグニチャが付いているセンサーをアップグレードするために、アプリケーション パーティションで起動して下さい。sensor24#**show version** Application Partition: Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S41 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDS2-XL Sensor up-time is 16:45. Using 377667584 out of 1979682816 bytes of available memory (19% usage) Using 765M out of 17G bytes of available disk space (5% usage) MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 NotRunning Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running Logger 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600 Upgrade History: No upgrades installed Maintenance Partition Version 1.3(2)
2. IDS モジュール CLI にログイン して下さい。
3. **configure terminal コマンド**を使用して configure terminal モードを開始して下さい。
4. プロンプト表示された場合サービスパックをインストールするために**アップグレード ftp://<user>@< FTP サーバ IP>/<directory path>/<service パック file>** コマンドを入力し、インストールを確認するために **y を**入力して下さい。モジュールはインストールが完了するとリブートします。sensor24#**configure terminal** sensor24(config)#**upgrade ftp://user@10.1.1.1/IDS-K9-min-4.1-1-S47.rpm.pkg** Password: ******** Warning: Executing this command will apply a minor version upgrade to the application partition. The system may be rebooted to complete the upgrade. Continue with upgrade? : yes Broadcast message from root (Sat Sep 20 17:59:09 2003): Applying update IDS-K9-min-4.1-1-S47. Shutting down all CIDS processes. All connections will be terminated. The system will be rebooted upon completion of the update. Console> Module 5 shut down in progress, please don't remove module until shutdown completed. Console> Module 5 shutdown completed. Module resetting...
5. モジュールがリブートした後、スイッチ CLI に入り、バージョンをチェックして下さい。**注**:これはまた確認するために使用することができます。sensor24#**show version** Application Partition: Cisco Systems Intrusion Detection Sensor, Version 4.1(1)S47 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDSM2-BUN Sensor up-time is 6 min. Using 401248256 out of 1979682816 bytes of available memory (20% usage) Using 872M out of 17G bytes of available

```
disk space (6% usage) MainApp 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
AnalysisEngine 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running Authentication
2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running Logger 2003_Jun_20_06.00
(Release) 2003-06-20T05:53:31-0500 Running NetworkAccess 2003_Jun_20_06.00 (Release) 2003-
06-20T05:53:31-0500 Running TransactionSource 2003_Jun_20_06.00 (Release) 2003-06-
20T05:53:31-0500 Running WebServer 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500
Running CLI 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Upgrade History: * IDS-
maj-4.0-1-S41 12:41:04 UTC Tue Apr 29 2003 IDS-K9-min-4.1-1-S47.rpm.pkg 17:59:06 UTC Sat
Sep 20 2003 Maintenance Partition Version 1.3(2) sensor24#
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Secure Intrusion Detection のサポートページ
- Cisco IDS アクティブ アップデート通知への加入
- Netranger に関する文書
- テクニカルサポート - Cisco Systems