將映像和特徵碼IDS 4.1升級到IPS 5.0及更高版本(AIP-SSM、NM-IDS、IDSM-2)配置示例

目錄

簡介

本檔案介紹如何將思科入侵偵測感應器(IDS)軟體的映像和特徵碼從版本4.1升級為思科入侵防禦系統(IPS)5.0及更新版本。

注意：從軟體版本5.x及更高版本開始，Cisco IPS將取代Cisco IDS，後者在版本4.1之前一直適用。

附註： 感測器無法從Cisco.com下載軟體更新。您必須從Cisco.com將軟體更新下載到FTP伺服器，然後配置感測器以便從FTP伺服器下載這些更新。

有關過程，請參閱升級、降級和安裝系統映像的安裝AIP-SSM系統映像部分。

請參閱Cisco IDS感測器和IDS服務模組(IDSM-1、IDSM-2)的密碼恢復過程，以瞭解有關如何恢復Cisco Secure IDS（以前稱為NetRanger）裝置以及3.x版和4.x版模組的更多資訊。

注意：在ASA - AIP-SSM上的內聯和失效開放**設定**中，升級期間使用者流量不會受到影響。

註：有關將IPS 5.1升級到版本6.x過程的詳細資訊，請參閱使用命令列介面6.0配置Cisco入侵防禦系統感測器的將Cisco IPS軟體從5.1升級到6.x**部分。**

注意：感測器不支援代理伺服器進行自動更新。代理設定僅用於全域性關聯功能。

必要條件

需求

升級到5.0所需的最低軟體版本是4.1(1)。

採用元件

本檔案中的資訊是根據執行軟體版本4.1（升級到5.0版）的Cisco 4200系列IDS硬體。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

本節提供用於設定本文件中所述功能的資訊。

可從Cisco.com下載從Cisco 4.1升級到5.0。請參閱獲取Cisco IPS軟體，瞭解用於訪問Cisco.com上的IPS軟體下載的程式。

您可以使用下列任一方法執行升級：

- 下載5.0升級檔案後，請參閱自述檔案，瞭解如何使用**upgrade**命令安裝5.0升級檔案的過程。如需詳細資訊，請參閱本檔案的使用升級命令一節。
- 如果為感測器配置了自動更新，請將5.0升級檔案複製到感測器輪詢以獲取更新的伺服器上的目錄中。如需詳細資訊，請參閱本檔案的使用自動升級命令一節。
- 如果在感測器上安裝升級，並且感測器在重新啟動後不可用，則必須重新映像感測器。從低於4.1的任何Cisco IDS版本升級感測器還需要使用**recover**命令或恢復/升級CD。有關詳細資訊，請參閱本文檔的重新映像感測器部分。

升級感測器

以下各節說明如何使用**upgrade**命令升級感測器上的軟體：

- 概觀
- 升級命令和選項
- 使用Upgrade指令

概觀

您可以使用以下檔案升級感測器，所有這些檔案的副檔名為.pkg:

- 特徵碼更新，例如IPS-sig-S150-minreq-5.0-1.pkg

- 特徵碼引擎更新，例如IPS-engine-E2-req-6.0-1.pkg
- 主要更新，例如IPS-K9-maj-6.0-1-pkg
- 次要更新，例如IPS-K9-min-5.1-1.pkg
- Service Pack更新，例如IPS-K9-sp-5.0-2.pkg
- 恢復分割槽更新，例如IPS-K9-r-1.1-a-5.0-1.pkg
- 補丁版本，例如IPS-K9-patch-6.0-1p1-E1.pkg
- 恢復分割槽更新，例如IPS-K9-r-1.1-a-6.0-1.pkg

感測器升級會更改感測器的軟體版本。

升級命令和選項

在服務主機子模式下使用**auto-upgrade-option enabled**命令以配置自動升級。

這些選項適用：

- **default** — 將值設定回系統預設設定。
- **directory** — 升級檔案位於檔案伺服器上的目錄。
- **file-copy-protocol** — 用於從檔案伺服器下載檔案的檔案複製協定。有效值為**ftp**或**scp**。**注意：如果使用SCP，則必須使用ssh host-key命令將伺服器新增到SSH已知主機清單中，以便感測器可以通過SSH與其通訊。**有關過程，請參閱將主機新增到已知主機清單。
- **ip-address** — 檔案伺服器的IP地址。
- **password** — 用於檔案伺服器上的身份驗證的使用者密碼。
- **schedule-option** — 計畫自動升級時間。日曆排程在特定日期的特定時間啟動升級。定期計畫以特定的定期時間間隔啟動升級。**calendar-schedule** — 配置執行自動升級的一週中的日子和一天中的時間。**星期幾** — 執行自動升級的星期幾。可以選擇多天。星期日到星期六是有效值。**no** — 移除條目或選取設定。**times-of-day** — 自動升級開始的時間。可選取多次。有效值為hh:mm[:ss]。**periodic-schedule** — 配置應執行第一次自動升級的時間以及自動升級之間的等待時間。**interval** — 自動升級之間等待的小時數。有效值為0到8760。**start-time** — 一天中開始第一次自動升級的時間。有效值為hh:mm[:ss]。
- **user-name** — 文件伺服器上用於身份驗證的使用者名稱。

有關升級感測器的IDM過程，請參閱更新感測器。

使用Upgrade指令

如果在升級到IPS 6.0之前未配置只讀社群和讀寫社群參數，則會收到SNMP錯誤。如果您使用SNMP set和/或get功能，則必須在升級到IPS 6.0之前配置只讀社群和讀寫社群引數。在IPS 5.x中，預設情況下將只讀社群設定為public，預設情況下將**read-write-community**設定為private。在IPS 6.0中，這兩個選項沒有預設值。例如，如果您沒有在IPS 5.x中使用SNMP獲取和集,enable-set-get設定為false，則升級到IPS 6.0沒有問題。如果您在IPS 5.x中使用SNMP gets和**sets**，例如，enable-set-get設定為true，則必須將**read-only-community**和**read-write-community**引數配置為特定值，否則IPS 6.0升級失敗。

您收到以下錯誤消息：

```
Error: execUpgradeSoftware : Notification Application "enable-set-get" value set to true,
but "read-only-community" and/or "read-write-community" are set to null. Upgrade may not
continue with null values in these fields.
```

注意：IPS 6.0預設拒絕高風險事件。這與IPS 5.x有所不同。要更改預設值，請為deny packet inline操作建立一個事件操作覆蓋，並將其配置為禁用。如果管理員不知道讀寫社群，他們應該在嘗

試升級之前嘗試完全禁用SNMP，以刪除此錯誤消息。

完成以下步驟以升級感測器：

1. 將主更新檔案(IPS-K9-maj-5.0-1-S149.rpm.pkg)下載到可從感測器訪問的FTP、SCP、HTTP或HTTPS伺服器。有關如何在Cisco.com上查詢軟體的步驟，請參閱獲取Cisco IPS軟體。**注意：**您必須使用具有加密許可權的帳戶登入到Cisco.com才能下載該檔案。請勿更改檔名。您必須保留原始檔名，以便感測器接受更新。**注意：**請勿更改檔名。您必須保留原始檔名，以便感測器接受更新。
2. 使用具有管理員許可權的帳戶登入到CLI。
3. 進入配置模式：
   ```
   sensor#configure terminal
   ```
4. 升級感測器：
   ```
   sensor(config)#upgrade scp://
   ```

   範例：注意：由於空間原因，此命令位於兩行上。
   ```
   sensor(config)#upgrade scp://tester@10.1.1.1//upgrade/
   IPS-K9-maj-5.0-1-S149.rpm.pkg
   ```

   注意：有關支援的FTP和HTTP/HTTPS伺服器的清單，請參閱支援的FTP和HTTP/HTTPS伺服器。有關如何將SCP伺服器新增到SSH已知主機清單的詳細資訊，請參閱將主機新增到SSH已知主機清單。
5. 出現提示時輸入密碼：
   ```
   Enter password: ********
   Re-enter password: ********
   ```
6. 輸入**yes**完成升級。**注意：**主要更新、次要更新和服務包可能會強制重新啟動IPS進程，甚至會強制重新啟動感測器以完成安裝。因此，服務中斷至少兩分鐘。但是，簽名更新在完成更新後不需要重新啟動。請參閱下載特徵碼更新(僅限註冊客戶)以瞭解最新更新。
7. 驗證新感測器版本：
   ```
   sensor#show version

   Application Partition:


   Cisco Intrusion Prevention System, Version 5.0(1)S149.0


   OS Version 2.4.26-IDS-smp-bigphys

   Platform: ASA-SSM-20

   Serial Number: 021

   No license present

   Sensor 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  Running

AnalysisEngine  2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

CLI             2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600


Upgrade History:


  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004


Recovery Partition Version 1.1 - 5.0(1)S149


sensor#
```

附註： 對於IPS 5.x，您會收到一條消息，說明升級型別未知。您可以忽略此消息。**注意：**將重新映像作業系統，並刪除通過服務帳戶放置在感測器上的所有檔案。

有關升級感測器的IDM過程的詳細資訊，請參閱更新感測器。

配置自動升級

自動升級

可以將感測器配置為在升級目錄中自動查詢新的升級檔案。例如，多個感測器可以指向具有不同更新計畫的同一遠端FTP伺服器目錄，例如每24小時或星期一、星期三和星期五晚上11:00。

您可以指定以下資訊以安排自動升級：

- 伺服器IP地址
- 檔案伺服器上感測器檢查升級檔案的目錄的路徑
- 檔案複製協定（SCP或FTP）
- 使用者名稱和密碼
- 升級計畫

您必須從Cisco.com下載軟體升級並將其複製到升級目錄，感測器才能輪詢自動升級。

注意：如果將AIM-IPS和其他IPS裝置或模組使用自動升級，請確保將6.0(1)升級檔案IPS-K9-6.0-1-E1.pkg和AIM-IPS升級檔案IPS-AIM-K9-6.0-4-E1.pkg都放在自動更新伺服器上，以便AIM-IPS可以正確檢測需要自動下載和安裝的檔案。如果僅將6.0(1)升級檔案IPS-K9-6.0-1-E1.pkg放在自動更新伺服器上，則AIM-IPS將下載並嘗試安裝該檔案，對於AIM-IPS而言，該檔案不正確。

有關自動升級感測器的IDM過程的詳細資訊，請參閱自動更新感測器。

使用auto-upgrade指令

有關**auto-update**命令，請參閱本文檔的升級命令和選項部分。

完成以下步驟以安排自動升級：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 配置感測器，以便在升級目錄中自動查詢新的升級。
```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#auto-upgrade-option enabled
```

3. 指定計畫：對於日曆計畫（在特定日期的特定時間啟動升級）：
```
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
```

   對於定期計畫（以特定的定期時間間隔啟動升級）：
```
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. 指定檔案伺服器的IP地址：
```
sensor(config-hos-ena-per)#exit
sensor(config-hos-ena)#ip-address 10.1.1.1
```

5. 指定升級檔案位於檔案伺服器上的目錄：
```
sensor(config-hos-ena)#directory /tftpboot/update/5.0_dummy_updates
```

6. 指定檔案伺服器上的身份驗證使用者名稱：
```
sensor(config-hos-ena)#user-name tester
```

7. 指定使用者的密碼：
```
sensor(config-hos-ena)#password

Enter password[]: ******
Re-enter password: ******
```

8. 指定檔案伺服器協定：
```
sensor(config-hos-ena)#file-copy-protocol ftp
```

   注意：如果使用SCP，則必須使用**ssh host-key命令將伺服器新增到SSH已知主機清單中，以便感測器可以通過SSH與其通訊。**有關過程，請參閱[將主機新增到已知主機清單]。
9. 驗證設定：
```
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. 退出自動升級子模式：

```
sensor(config-hos-ena)#exit
sensor(config-hos)#exit

Apply Changes:?[yes]:
```

11. 按**Enter**以應用更改，或鍵入**no**以放棄更改。

重新映像感測器

您可以通過以下方式重新映像感測器：

- 對於帶有CD-ROM驅動器的IDS裝置，請使用恢復/升級光碟。有關過程，請參閱升級、降級和安裝系統映像的使用恢復/升級光碟部分。
- 對於所有感測器，請使用**recover**命令。有關過程，請參閱升級、降級和安裝系統映像的恢復應用程式分割槽部分。
- 對於IDS-4215、IPS-4240和IPS 4255，請使用ROMMON還原系統映像。有關過程，請參閱升級、降級和安裝系統映像的安裝IDS-4215系統映像和安裝IPS-4240和IPS-4255系統映像部分。
- 對於NM-CIDS，請使用引導載入程式。有關過程，請參閱升級、降級和安裝系統映像的安裝NM-CIDS系統映像部分。
- 對於IDSM-2，請從維護分割槽重新映像應用程式分割槽。有關過程，請參閱升級、降級和安裝系統映像的安裝IDSM-2系統映像部分。
- 對於AIP-SSM，使用**hw-module module 1 recover**從ASA重新映像[configure **| boot]命**令。有關過程，請參閱升級、降級和安裝系統映像的安裝AIP-SSM系統映像部分。

相關資訊

- **思科入侵防禦系統支援頁面**
- **升級、降級和安裝IPS 6.0的系統映像**
- **Cisco Catalyst 6500系列入侵偵測系統(IDSM-2)模組支援頁面**
- **Cisco IDS感測器和IDS服務模組1(IDSM-2)的密碼恢復過程**
- **自動簽名更新故障排除**
- **技術支援與文件 - Cisco Systems**