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

本文檔介紹如何將思科入侵檢測感測器(IDS)軟體的映像和特徵碼從版本4.1升級到思科入侵防禦系統(IPS) 5.0及更高版本。

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。

注意：感測器無法從Cisco.com下載軟體更新。您必須從Cisco.com將軟體更新下載到您的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、下載和安裝系統映像的安裝AIP-SSM系統映像部分。

要詳細瞭解如何恢復Cisco Secure IDS（前身為NetRanger）裝置以及3.x和4.x版模組，請參閱Cisco IDS感測器和IDS服務模組(IDSM-1、IDSM-2)的口令恢復過程。

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

注意：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，瞭解將IPS 5.1升級到版本6.x的過程的詳細資訊。

注意：感測器不支援代理伺服器進行自動更新。代理設定僅用於全局關聯功能。

必要條件

需求

您需要的最低軟體版本是4.1(1)，才能升級到5.0。

採用元件

本文檔中的資訊基於運行軟體版本4.1（將升級到版本5.0）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。

從Cisco 4.1升級到5.0可從Cisco.com下載。有關用來訪問Cisco.com上的IPS軟體下載的過程，請參閱獲取Cisco IPS軟體。

您可以使用此處列出的任何方法來執行升級：

- 下載5.0升級檔案後，請參閱自述檔案以瞭解有關如何使用upgrade命令安裝5.0升級檔案的過程。有關詳細資訊，請參閱本文檔的使用Upgrade命令部分。
- 如果為感測器配置了Auto Update（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。有關詳細資訊，請參閱本文檔的使用auto-upgrade命令部分。
- 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。從任何早於4.1的Cisco IDS版本升級感測器時也需要使用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

以下部分說明如何使用upgrade命令升級感測器上的軟體：

- 概觀
- Upgrade命令和選項
- 使用Upgrade指令

概觀

可以使用以下檔案升級感測器，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
- 簽名引擎更新，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
- 服務包更新，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
- 修補版本，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。

Upgrade命令和選項

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

這些選項適用：

- default -將值設定回系統預設設定。
- directory -檔案伺服器上升級檔案所在的目錄。
- 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 命令以將伺服器增加到SSH已知主機清單中，以使感測器可以透過SSH與之通訊。有關過程，請參閱向已知主機清單中增加主機。
- ip-address -檔案伺服器的IP地址。
- password -檔案伺服器上用於進行身份驗證的使用者口令。
- schedule-option -排程自動升級發生的時間。日曆排程在特定日期的特定時間啟動升級。定期排程以特定的定期間隔啟動升級。
  - calendar-schedule -配置執行自動升級的每週天數和每天時間。
    - days-of-week -執行自動升級的每週天數。您可以選擇多天。星期日到星期六是有效值。
    - no -刪除條目或選擇設定。
    - times-of-day -開始自動升級的一天中的時間。您可以選取多次。有效值為hh：mm[：ss]。

    - periodic-schedule -配置首次自動升級應當發生的時間以及兩次自動升級之間的等待時間。
        - interval -兩次自動升級之間等待的小時數。有效值為0到8760。
        - start-time -啟動首次自動升級的一天中的時間。有效值為hh：mm[：ss]。
- user-name -檔案伺服器上用於身份驗證的使用者名稱。

有關用於升級感測器的IDM過程，請參閱升級感測器。

使用Upgrade指令

如果未在升級到IPS 6.0之前配置read-only-community和read-write-community引數，則會收到SNMP錯誤。如果正在使用SNMP set和/或get功能，則必須在升級到IPS 6.0之前配置read-only-community和read-write-community引數。在IPS 5.x中，預設情況下已將read-only-community設定為public，並將read-write-community設定為private。在IPS 6.0中，這兩個選項沒有預設值。如果未在IPS 5.x中使用SNMP get 和set，例如，將enable-set-get設定為false，則升級到IPS 6.0不會出現任何問題。如果在IPS 5.x中使用了SNMP get和set，例如，將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升級將失敗。

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：預設情況下，IPS 6.0拒絕高風險事件。這與IPS 5.x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，並將其配置為停用。如果管理員不知道讀寫社群，則他們應該在嘗試升級之前嘗試完全停用SNMP，以移除此錯誤訊息。

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上查詢軟體的過程，請參閱獲取Cisco IPS軟體。

   注意：您必須使用具有密碼編譯許可權的帳戶登入Cisco.com，才能下載檔案。請勿變更檔案名稱。您必須保留原始檔名，感測器才能接受更新。

   注意：請勿更改檔名。您必須保留原始檔名，感測器才能接受更新。

2. 使用具有管理員許可權的帳戶登入到CLI。
3. 進入組態設定模式：

<#root>

sensor#

configure terminal

4. 升級感測器：

<#root>

sensor(config)#

upgrade scp://

@

//upgrade/

範例：

注意：由於空間原因，此命令使用兩行。

<#root>

sensor(config)#

upgrade scp://tester@10.1.1.1//upgrade/
IPS-K9-maj-5.0-1-S149.rpm.pkg

注意：請參閱支援的FTP和HTTP/HTTPS伺服器，瞭解支援的FTP和HTTP/HTTPS伺服器清單。有關如何將SCP伺服器增加到SSH已知主機清單的詳細資訊，請參閱向SSH已知主機清單中增加主機。

5. 出現提示時輸入密碼：

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

6. 鍵入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，服務中斷至少持續兩分鐘。但是，完成更新後，簽名更新不需要重新啟動。有關最新更新，請參閱下載簽名更新(僅限註冊客戶)。

7. 驗證新的感測器版本：

```
<#root>

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#
```

注意：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。

註：作業系統將重新映像，透過服務帳戶放置在感測器上的所有檔案將被刪除。

有關用於升級感測器的IDM過程的詳細資訊，請參閱升級感測器。

配置自動升級

自動升級

您可以將感測器配置為自動在升級目錄中查詢新的升級檔案。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位址
- 檔案伺服器上感測器檢查升級檔案的目錄路徑
- 檔案複製協定（SCP或FTP）
- 使用者名稱和密碼
- 升級排程

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自動升級和其他IPS裝置或模組一起使用，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。

有關用於自動升級感測器的IDM過程的詳細資訊，請參閱自動升級感測器。

使用auto-upgrade指令

請參閱本文檔的Upgrade命令和選項部分以瞭解auto-update 命令。

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。

```
<#root>
sensor#
configure terminal
sensor(config)#
service host
sensor(config-hos)#
auto-upgrade-option enabled
```

3. 指定排程：
   - 對於行事曆排程（在特定日期的特定時間開始升級）：

```
<#root>
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，它以特定的定期間隔啟動升級：

```
<#root>
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：

```
<#root>
sensor(config-hos-ena-per)#
exit
sensor(config-hos-ena)#
ip-address 10.1.1.1
```

5. 指定升級檔案在檔案伺服器上的目錄：

```
<#root>
sensor(config-hos-ena)#
directory /tftpboot/update/5.0_dummy_updates
```

6. 指定檔案伺服器上用於驗證的使用者名稱：

```
<#root>
sensor(config-hos-ena)#
user-name tester
```

7. 指定使用者的密碼：

```
<#root>
sensor(config-hos-ena)#
password

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

8. 指定檔案伺服器通訊協定：

```
<#root>
sensor(config-hos-ena)#
file-copy-protocol ftp
```

注意：如果使用SCP，則必須使用ssh host-key 命令以將伺服器增加到SSH已知主機清單中，以使感測器可以透過SSH與之通訊。有關過程，請參閱向已知主機清單中增加主機。

9. 驗證設定：

```
<#root>
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：

```
<#root>
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

您可以透過下列方式重新映像感應器：

- 對於帶有CD-ROM驅動器的IDS裝置，請使用恢復/升級CD。

  有關過程，請參閱升級、下載和安裝系統映像的使用恢復/升級CD部分。

- 對於所有感測器，請使用recover命令。

  有關過程，請參閱升級、下載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，使用ROMMON恢復系統映像。

  有關過程，請參閱升級、下載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、下載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、下載和安裝系統映像的安裝IDSM-2系統映像部分。

- 對於AIP-SSM，請使用hw-module module 1 recover [configure | boot]命令從ASA重新映像。

  有關過程，請參閱升級、下載和安裝系統映像的安裝AIP-SSM系統映像部分。

相關資訊

- Cisco入侵防禦系統支援頁
- 升級、下載和安裝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和IDSM-2的口令恢復過程
- 自動簽名更新故障排除
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。