升级镜像和签名IDS 4.1到IPS 5.0及以上版本(AIP-SSM、NM-IDS， IDSM-2)配置示例

目录

简介

本文档描述如何将 Cisco 入侵检测传感器 (IDS) 软件的映像和签名从版本 4.1 升级到 Cisco 入侵防御系统 (IPS) 5.0 及更高版本。

注意：从软件版本5.x及更高版本开始，Cisco IPS将取代Cisco IDS，后者在版本4.1之前一直适用。

注意：传感器无法从Cisco.com下载软件更新。您必须从 Cisco.com 将软件更新下载到您的 FTP 服务器，然后配置传感器以从您的 FTP 服务器上下载它们。

有关过程，请参阅升级、下载和安装系统映像的安装 AIP-SSM 系统映像部分。

要详细了解如何恢复Cisco Secure IDS（以前称为NetRanger）设备和版本3.x和4.x的模块，请参阅Cisco IDS传感器和IDS服务模块(IDSM-1、IDSM-2)的口令恢复过程。

注意：在ASA - AIP-SSM上的内联和失效开放设置升级过程中，用户流量不会受到影响。

注意：有关将IPS 5.1升级到版本6.x的过程的详细信息，请参阅使用命令行界面6.0配置Cisco入侵防御系统传感器的将Cisco IPS软件从5.1升级到6.x部分。

注意：传感器不支持代理服务器进行自动更新。代理设置只用于全局相关功能。

先决条件

要求

要升级到 5.0，至少需要软件版本 4.1(1)。

使用的组件

此文档中的信息基于运行软件版本 4.1（要升级到版本 5.0）的 Cisco 4200 系列 IDS 硬件。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

本部分提供有关如何配置本文档所述功能的信息。

从 Cisco 4.1 到 5.0 的升级程序可从 Cisco.com 下载。有关用来访问 Cisco.com 上的 IPS 软件下载的过程，请参阅获取 Cisco IPS 软件。

您可以使用下列任何方法来执行升级：

- 下载5.0升级文件后，请参阅自述文件以了解有关如何使用upgrade命令安装5.0升级文件的过程。有关详细信息，请参阅本文档的使用 Upgrade 命令部分。
- 如果您为传感器配置了自动更新，请将 5.0 升级文件复制到您的传感器轮询更新的服务器上的目录中。有关详细信息，参阅本文档的使用 auto-upgrade 命令部分。
- 如果在您的传感器上安装升级程序，并且传感器在重新启动后无法使用，则必须重新映像您的传感器。从任何早于 4.1 的 Cisco IDS 版本升级传感器时也需要使用 recover 命令或恢复/升级 CD。有关详细信息，请参阅本文档的重新映像传感器部分。

升级传感器

以下部分说明如何使用 upgrade 命令升级传感器上的软件：

- 概述
- Upgrade 命令和选项
- 使用 Upgrade 命令

概述

您可以使用以下文件（它们都具有扩展名 .pkg）升级传感器：

- 签名更新，例如，IPS-sig-S150-minreq-5.0-1.pkg
- 签名引擎更新，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
- Service Pack 更新，例如，IPS-K9-sp-5.0-2.pkg
- 恢复分区更新，例如，IPS-K9-r-1.1-a-5.0-1.pkg
- 补丁程序版本，例如，IPS-K9-patch-6.0-1p1-E1.pkg
- 恢复分区更新，例如，IPS-K9-r-1.1-a-6.0-1.pkg

传感器升级会更改该传感器的软件版本。

Upgrade 命令和选项

在服务主机子模式下使用 auto-upgrade-option enabled 命令来配置自动升级。

这些选项适用：

- default -将值设置回系统默认设置。
- directory -文件服务器上升级文件所在的目录。
- file-copy-protocol -用于从文件服务器下载文件的文件复制协议。有效值包括 ftp 或 scp。

  注意：如果使用SCP，则必须使用ssh host-key命令以将服务器添加到SSH已知主机列表中，以使传感器可以通过SSH与之通信。有关过程，请参阅向已知主机列表中添加主机。
- ip-address -文件服务器的IP地址。
- password —文件服务器上用于进行身份验证的用户口令。
- schedule-option - 调度自动升级发生的时间。日历调度在特定日期的特定时间启动升级。定期调度按特定的定期时间间隔启动升级。
  - calendar-schedule -配置执行自动升级的每周天数和每天时间。
    - days-of-week -执行自动升级的每周天数。您可以选择多天。有效值从星期日到星期六。
    - no -删除条目或选择设置。
    - times-of-day -开始自动升级的一天中的时间。您可以选择多个时间。有效值为hh：mm[：ss]。

    - periodic-schedule -配置首次自动升级应当发生的时间以及两次自动升级之间的等待时间。
        - interval -两次自动升级之间等待的小时数。有效值从 0 到 8760。
        - start-time - 启动首次自动升级的一天中的时间。有效值为hh：mm[：ss]。
- user-name — 文件服务器上用于身份验证的用户名。

有关用于升级传感器的 IDM 过程，请参阅升级传感器。

使用 Upgrade 命令

如果未在升级到 IPS 6.0 之前配置 read-only-community 和 read-write-community 参数，则会收到 SNMP 错误。如果正在使用 SNMP set 和/或 get 功能，则必须在升级到 IPS 6.0 之前配置 read-only-community 和 read-write-community 参数。在 IPS 5.x 中，默认情况下已将 read-only-community 设置为 public，并将 read-write-community 设置为 private。在 IPS 6.0 中，这两个选项没有默认值。如果未在 IPS 5.x 中使用 SNMP get 和 set 功能，例如，将 enable-set-get 设置为 false，则升级到 IPS 6.0 不会出现任何问题。如果在 IPS 5.x 中使用了 SNMP get 和 set 功能，例如，将 enable-set-get 设置为 true，则必须将 read-only-community 和 read-write-community 参数配置为特定值，否则 IPS 6.0 升级将失败。

您将收到以下错误消息：

```
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：默认情况下，IPS 6.0拒绝高风险事件。这与IPS 5.x不同。要更改默认值，请为deny数据包内联操作创建事件操作覆盖，并将其配置为禁用。如果管理员不知道读写社区，则他们应尝试完全禁用SNMP，然后尝试进行升级，以删除此错误消息。

要升级传感器，请完成以下步骤：

1. 将主要更新文件 (IPS-K9-maj-5.0-1-S149.rpm.pkg) 下载到可从您的传感器访问的 FTP、SCP、HTTP 或 HTTPS 服务器。

   有关如何在 Cisco.com 上查找软件的过程，请参阅获取 Cisco IPS 软件。

   注意：必须使用具有加密权限的帐户登录到Cisco.com以下载文件。请不要更改文件名。您必须保留原始文件名以使传感器接受更新。

   注意：请勿更改文件名。您必须保留原始文件名以使传感器接受更新。

2. 使用具有管理员权限的帐户登录 CLI。
3. 进入配置模式：

<#root>

sensor#

configure terminal

4. 升级传感器：

<#root>

sensor(config)#

upgrade scp://

@

//upgrade/

示例：

注意：由于空间原因，此命令分为两行。

<#root>

sensor(config)#

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

注意：有关所支持的FTP和HTTP/HTTPS服务器的列表，请参阅支持的FTP和HTTP/HTTPS服务器。有关如何将 SCP 服务器添加到 SSH 已知主机列表的详细信息，请参阅向 SSH 已知主机列表中添加主机。

5. 出现提示时输入口令：

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

6. 键入 yes 完成升级。

注意：主要更新、次要更新和Service Pack可能会强制重新启动IPS进程，甚至强制重新启动传感器以完成安装。因此，至少存在两分钟的服务中断。然而，签名更新在完成更新后不需要重新启动。有关最近的更新，请参阅下载签名更新（仅限注册用户）。

7. 验证新传感器版本：

```
<#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：对于IPS 5.x，您会收到一条消息，表明升级类型未知。您可以忽略此消息。

注意：操作系统将重新映像，通过服务帐户放在传感器上的所有文件都将删除。

有关用于升级传感器的 IDM 过程的详细信息，请参阅升级传感器。

配置自动升级

自动升级

您可以将传感器配置为在您的升级目录中自动查找新的升级文件。例如，几个传感器可以使用不同的更新调度（例如每 24 小时或星期一、星期三和星期五的下午 11:00）指向同一远程 FTP 服务器目录。

请指定以下信息以调度自动升级：

- 服务器 IP 地址
- 文件服务器上传感器在其中检查升级文件的目录路径
- 文件复制协议（SCP 或 FTP）
- 用户名和密码
- 升级调度

您必须从 Cisco.com 下载软件升级程序并将它复制到升级目录中，然后传感器才能轮询自动升级程序。

注意：如果将AIM-IPS自动升级与其他IPS设备或模块一起使用，请确保将6.0(1)升级文件IPS-K9-6.0-1-E1.pkg和AIM-IPS升级文件IPS-AIM-K9-6.0-4-E1.pkg都放置在自动更新服务器上，以便AIM-

IPS可以正确检测需要自动下载和安装的文件。如果您只将 6.0(1) 升级文件 (IPS-K9-6.0-1-E1.pkg) 放在自动更新服务器上，AIM-IPS 将下载并试图安装它，但它对 AIM-IPS 来说是不正确的文件。

有关用于自动升级传感器的 IDM 过程的详细信息，请参阅自动升级传感器。

使用 auto-upgrade 命令

请参阅本文档的 Upgrade 命令和选项部分以了解 auto-update 命令。

要调度自动升级，请完成以下步骤：

1. 使用具有管理员权限的帐户登录 CLI。
2. 配置传感器以在您的升级目录中自动查找新的升级程序。

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

3. 指定调度：
   - 对于日历调度，它将在特定日期的特定时间启动升级：

```
<#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
```

   - 对于定期调度，它将按特定的周期时间间隔启动升级：

```
<#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. 指定文件服务器的 IP 地址：

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

5. 指定文件服务器上升级文件所在的目录：

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

6. 指定文件服务器上用于身份验证的用户名：

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

7. 指定用户口令：

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

Enter password[]:
******
```

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

8. 指定文件服务器协议：

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

注意：如果使用SCP，则必须使用ssh host-key命令以将服务器添加到SSH已知主机列表中，以使传感器可以通过SSH与之通信。有关过程，请参阅向已知主机列表中添加主机。

9. 验证设置：

```
<#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. 退出自动升级子模式：

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

Apply Changes:?
[yes]:
```

11. 按Enter 以应用更改或键入no 以放弃更改。

重新映像传感器

您可以通过以下方法重新映像您的传感器：

- 对于具有 CD-ROM 驱动器的 IDS 设备，请使用恢复/升级 CD。

  有关过程，请参阅升级、下载和安装系统映像的使用恢复/升级 CD 部分。

- 对于所有传感器，请使用 recover 命令。

  有关过程，请参阅升级、下载和安装系统映像的恢复应用程序分区部分。

- 对于 IDS-4215、IPS-4240 和 IPS 4255，请使用 ROMMON 还原系统映像。

  有关过程，请参阅升级、下载和安装系统映像的安装 IDS-4215 系统映像和安装 IPS-4240 和 IPS-4255 系统映像部分。

- 对于 NM-CIDS，请使用引导加载程序。

  有关过程，请参阅升级、下载和安装系统映像的安装 NM-CIDS 系统映像部分。

- 对于 IDSM-2，请从维护分区重新映像应用程序分区。

  有关过程，请参阅升级、下载和安装系统映像的安装 IDSM-2 系统映像部分。

- 对于 AIP-SSM，请使用 hw-module module 1 recover [configure | boot] 命令从 ASA 重新映像。

有关过程，请参阅升级、下载和安装系统映像的安装 AIP-SSM 系统映像部分。

相关信息

- Cisco 入侵防御系统支持页
- 升级、下载和安装 IPS 6.0 的系统映像
- Cisco Catalyst 6500 系列入侵检测系统 (IDSM-2) 模块支持页
- Cisco IDS 传感器和 IDS 服务模块 1 和 IDSM-2 的口令恢复过程
- 自动签名更新故障排除
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。