

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[升级传感器](#)

[概述](#)

[Upgrade 命令和选项](#)

[使用 Upgrade 命令](#)

[配置自动升级](#)

[自动升级](#)

[使用 auto-upgrade 命令](#)

[重新映像传感器](#)

[相关信息](#)

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： 在软件版本 5.x 及更高版本中，Cisco IPS 替换了 Cisco IDS，Cisco IDS 适用于版本 4.1 及更低版本。

注意： 此传感器不能从 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。

要了解有关如何恢复版本 3.x 和 4.x 的 Cisco Secure IDS (以前称为 NetRanger) 设备和模块，请参阅[Cisco IDS 传感器和 IDS 服务模块 \(IDSM-1 和 IDSM-2\) 的口令恢复过程](#)。

注意： 在 ASA - AIP-SSM 上的 **inline and fail-open** 设置升级过程中，用户数据流不会受到影响。

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： 此传感器不支持代理服务器自动更新。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

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

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：

- 在您下载5.0升级文件后，参考步骤的README关于怎样安装5.0升级文件用**upgrade**命令。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：

- **默认**？送回值到系统默认默认设置。
- **目录**？升级文件在文件服务器查找的目录。
- **FILE复制协议**？用于的文件副本协议下载从文件服务器的文件。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地址**？文件服务器的IP地址。
- **密码**？验证的用户密码在文件服务器。
- **Schedule选项**？日程，当自动升级发生。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。**日程**？配置星期和每日定时自动升级被执行。**天周**？自动升级被执行的星期。您可以选择多天。有效值从星期日到星期六。**否**？取消条目或选择设置。**每日定时**？自动升级开始天的时期。您可以选择多个时间。有效值是 hh:分[:ss]。**日程**？多久配置第一自动升级应该发生的时间和等待在自动升级之间。**间隔**？等待的几小时数量在自动升级之间。有效值从 0 到 8760。**开始时间**？每日定时开始第一自动升级。有效值是 hh:分[:ss]。
- **用户名**？验证的用户名在文件服务器。

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：

注意：默认情况下，IPS 6.0 拒绝高风险事件。这是从 IPS 5.x 的一更改。为了更改默认，请创建拒绝数据包的一事件操作覆盖轴向操作并且配置将禁用的它。如果管理员不知道读/写社区那么他们应该设法禁用 SNMP 完全，在尝试升级做出为了删除此错误消息前。

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：**您必须使用具有加密权限的帐户登录到 Cisco.com 中才能下载文件。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。

2. 使用具有管理员权限的帐户登录 CLI。

3. 进入配置模式：`sensor#configure terminal`

4. 升级传感器：`sensor(config)#upgrade scp://<username>@<server IP>//upgrade/<file name>` **示例**
：**注意**：由于空间原因，该命令占两行。`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：`sensor(config)#upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg`

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 进程或者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：`sensor#show version`
Application Partition: Cisco Intrusion Prevention System, **Version 5.0(1)S149.00S** 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，您会收到一条指示升级属于未知类型的消息。您可以忽略此消息。**注意**：操作系统将被重新映像，通过服务帐户放在传感器上的所有文件都会被删除。

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：如果对 AIM-IPS 和其他 IPS 设备或模块使用自动升级，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哪一个文件。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。`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：`sensor(config-hos-ena)#schedule-option calendar-schedule``sensor(config-hos-ena-cal)#days-of-week sundays``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：`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：`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：`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：`sensor(config-hos-ena)#user-name tester`
7. 指定用户口令：`sensor(config-hos-ena)#password`Enter password[:] *****Re-enter password: *****
8. 指定文件服务器协议：`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：`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：`sensor(config-hos-ena)#exit``sensor(config-hos)#exit`Apply Changes:?[yes]:
11. 按回车为了应用更改或键入没有为了丢弃他们。

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]` 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](#)
- [排除故障自动签名更新](#)
- [技术支持和文档 - Cisco Systems](#)