升级入侵检测系统模块

目录

简介

本文解释如何执行在应用程序分区、服务包和签名更新的Cisco入侵检测系统模块(IDSM)升级。欲了解更详细的信息在升级IDS传感器，参考Catalyst 6000入侵检测系统模块。

先决条件

要求

尝试此配置之前，请确保满足下列前提条件：

- 从和仍然通信与直到升级的时期的导向器的IDS传感器开始。
- 您应该能顺利地使用ping、无源FTP和Telnet达到传感器，不用干扰从所有类防火墙或信息包过滤设备在升级前。
- 确保您有FTP服务器该支持被动模式。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本2.5的IDSM传感器式样WS-X6381-IDS。
- IDS控制器运行Solaris版本2.6， HP OpenView版本x5.01， IDS控制器软件版本2.2.3 S9。
- 有无源FTP和Telnet访问的Solaris版本2.8工作站对传感器和导向器。
- 下载从下载的文件(IDSk9-sig-3.0-2-S10.bin和nrdirUpdate-S10.bin，用于本文)。

注意： 用于本文的确切的版本可能不是现在可以得到的。

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

- IDS控制器被命名"dir1,"，并且IP地址是192.168.1.3。
- IDSM传感器被命名“idsm”，并且IP地址是192.168.1.2。
- 主机ID匹配IP地址的最后一个八位位组在示例的。
- 组织ID定义作为"1."
- FTP服务器IP地址是10.0.0.1。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

升级 IDSM 应用程序部分

以下步骤显示您如何升级从应用程序版本2.5(1)S2的IDSM到3.0(1)S4。请保存IDSM配置，在升级，作为整个IDSM硬盘将被格式化前，并且所有配置将丢失。

逐步指导

遵从下面提供的说明。

1. 如以下示例所显示，会话到IDSM里和保存输出**show configuration命令**。`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. 下载从下载的适当的文件。IDS传感器和README文件查找在*Cisco IDS设备传感器3DES*部分下。IDS控制器和README文件查找在*Cisco IDS Director 3DES*部分下。在本文中，使用以下文件，然而您应该使用任何文件是多数当前：`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. 安置文件在FTP服务器的适当的目录。在本例中，文件在根目录安置。下列是从FTP客户端的输出示例:到FTP服务器。`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. 设置维护分区作为活动分区，然后控制到IDSM到维护分区(应用程序是默认设置)并且设置IDSM的网络配置参数。在以下示例中， IDSM在Catalyst 6509机箱的slot 8。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! **注意：** 重置模块使更改生效。
5. 一旦IDSM完成重新启动，如以下示例所显示，回到IDSM的会话和通过发出**ids-installer命令**安装非激活应用程序分区。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

验证应用分区升级

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

重新启动IDSM回到应用程序分区并且验证镜像顺利地升级，如以下示例所显示。

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

升级 IDSM 服务包

使用以下步骤更新IDSN服务包。

1. 会话到IDSM里通过发出**session -命令**(其中#是模块号)如以下示例所显示，和发出**configure terminal命令**。idsm#

idsm#**configure terminal**

2. 如以下示例所显示，发出**应用ftp:// < username@server /dir/filename>**命令通过FTP连接，并且运用服务包。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...

验证服务包升级

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

会话到IDSM里通过发出**session -命令**(其中#是模块号)如以下示例所显示，和发出**show configuration命令**。

```
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#
```

升级 IDSM 签名

使用以下步骤升级ISDM签名。

1. 会话到IDSM里通过发出**session -命令**(其中#是模块号)如以下示例所显示，和发出**configure terminal命令**。`idsm#`
   `idsm#configure terminal`
2. 如以下示例所显示，发出**应用ftp:// < *username@server /dir/filename*>**命令通过FTP连接，并且应用IDSM签名， ：`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:

验证签名升级

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

会话到IDSM里通过发出**session -命令**(其中#是模块号)如以下示例所显示，和发出**show configuration命令**。

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#

升级IDSM2

以下部分在升级提供信息ISDM2。

升级维护分区

要升级从1.3.1的维护分区到1.3.2，请通过发出以下at命令启动在应用程序分区的IDSM2刀片交换机。

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

一旦重新镜像完成，并且系统重新启动， **show version将**允许您确认升级是成功的。

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)

再镜像从维护分区的应用程序分区

警告： 使用**setup命令，**在再镜像IDS模块以后，您必须初始化IDS模块。此进程删除所有传感器配置并且再镜像应用程序分区。此进程，只有当应用程序分区是损坏或不可访问的，应该使用。如果应用程序分区可访问，避免丢失当前配置，请使用较小镜像升级从应用程序分区升级。

1. 启动到维护分区通过发出以下on命令交换机。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. 通过输入以下用户名和密码登录IDS模块。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. 使用**configure terminal命令，**输入配置终端模式。
4. 使用**升级ftp:// <user>@< FTP服务器IP>/<directory path>/<image file>**命令，执行重新镜像。将提示您输入FTP服务器密码(如果必须)。也将提示您继续进行安装。继续的回车**y**。
   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. 重新启动IDS模块到应用程序分区通过输入**reset <module number> hdd:1命令。**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. 当IDS模块重新启动时，请检查软件版本。**注意：** 可能也使用这验证目的。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. 使用**setup命令**，登陆对应用程序分区CLI并且初始化IDS模块。

较小镜像升级

此更新可以用于应用程序分区可访问的情况，但是仅一部分的此应用程序是残破的。与使用全双工镜像比较再镜像应用程序分区，较小镜像保留传感器配置。

要安装较小更新，请遵从这些步骤：

1. 使用与管理员权限的一个帐户登录CLI。
2. 通过发出**configure terminal命令**输入配置模式。
3. 键入**upgrade [URL]/<filename>命令**升级传感器。**[URL]**是指向的统一资源定位器签名更新包查找的地方。例如，通过FTP获取更新，请输入以下：
   upgrade ftp://<username>@<ip-address>//<directory>/<filename> 可用的传输方法是SCP、FTP、HTTP或者HTTPS。
4. 输入适当的密码，当提示。
5. 要完成升级，请键入**是**，当提示。

升级IDSM2服务包或签名

使用以下步骤升级ISDM2服务大袋或签名。

1. 要升级有服务包或签名的传感器，启动在应用程序分区。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. 登录IDS模块CLI。
3. 使用**configure terminal命令**，输入configure terminal模式。
4. 输入**升级ftp:// <user>@< FTP服务器IP>/<directory path>/<service装箱file>**命令安装服务包和，当提示，键入**y**确认安装。当安装完成，模块重新启动。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. 在模块重新启动后，请输入交换机CLI并且检查版本。**注意：** 可能也使用这验证目的。

```
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#
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco安全入侵检测支持页
- 订阅对Cisco IDS活动更新通知
- Netranger的文档
- 技术支持 - Cisco Systems