Cisco IDS 传感器和 IDS 服务模块（IDSM-1、IDSM-2）的口令恢复过程

目录

简介

本文档提供了有关如何恢复 Cisco 安全入侵检测系统 (IDS)（之前称作 NetRanger）设备和所有版本的模块的过程。

先决条件

要求

如果需要 FTP 服务器，该服务器必须支持被动模式。使用产品升级工具（仅限注册用户）可以获得恢复 CD。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- IDS 设备版本 3 和 4
- IPS 设备版本 5 和 6
- IDS 模块 (IDSM) 版本 3 和 IDSM-2 版本 4

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。

IDS 设备版本 3

版本 3 设备有两个可用选项。可以使用口令恢复过程，也可以使用版本 3 恢复 CD 进行重新映像。请注意，重新映像将丢失所有信息。口令恢复过程本质上是 Solaris 口令恢复。只请使用此选项，如果没有一个管理站(Cisco Secure Policy Manager， VPN/安全管理解决方案(VM)， UNIX向导)您能复制配置。

使用 IDS 设备版本 3 和更低版本时，存在两个用户名“netrangr”和“root”。两个用户名的默认口令都是“attack”。

运行版本 3 的 IDS 设备的口令恢复

这些文件是恢复口令所必需的。

- Solaris 设备配置助手磁盘（引导盘）。可以从 Sun 支持网站下载文件 。**注意：** 如果此链路无法工作，可尝试转到 Sun 支持网站的顶层并在“驱动程序”下搜索*设备配置助手引导盘 Solaris 驱动程序下载*。Cisco Systems, Inc. 不负责维护 Sun 支持网站，也无权控制内容的位置。
- Solaris for Intel (x86) CD-ROM。
- 对工作站的控制台访问。

完成下列步骤以恢复口令。

1. 插入引导盘。
2. 将 CD 插入 CD-ROM 驱动器。
3. 关闭工作站，等待十秒钟，然后将其打开。系统从引导盘引导。完成一定的配置后，将显示初始“配置助手”屏幕。
4. 按 **F3** 对系统进行部分扫描以搜索引导设备。扫描完成时，将显示设备列表。
5. 确保 CD-ROM 设备显示在设备列表中，然后按 **F2** 继续操作。此时屏幕显示引导设备列表。
6. 选择 **CD-ROM drive**，然后按空格键。CD-ROM 设备旁边有一个“X”。
7. 按 **F2** 继续操作。此时工作站从 CD-ROM 进行引导。
8. 在用于选择安装类型的屏幕上，选择 **Option 2，Jumpstart**。系统继续引导。
9. 在系统提示选择语言时，选择 **Option 0**（英语）。
10. 在显示语言的下一个屏幕上，再次选择 **Option 0**（英语 ANSI）。系统继续引导，此时显示“Solaris Installation”屏幕。
11. 按住 **Control 键**并键入 C，以便停止安装脚本并允许您访问提示符。

12. 键入 **mount -F ufs /dev/dsk/c0t0d0s0 /mnt**。此时“/”分区已安装在“/mnt”装入点。在此处可以编辑“/etc/shadow”文件并删除根帐户口令。
13. 键入 **cd /mnt/etc**。
14. 设置 shell 环境以便正确读取数据。键入 **TERM=ansi**。键入 **export TERM**。
15. 键入 **vi Shadow**。此时已进入卷影文件，您可以删除口令。条目必须如下所示：**root:gNyqp8ohdfxPI:10598::::::** “：”是字段分隔符，加密口令是第二个字段。
16. 删除第二个字段。例如，root:gNyqp8ohdfxPI:10598::::::更改为 **root::10598::::::**. 此操作将删除根用户的口令。
17. 类型：**wq!**以写入并退出文件。
18. 从驱动器中取出磁盘和 CD-ROM。
19. 键入 **init 6** 以重新引导系统。
20. 在 login: 提示符处键入 **root**，然后按 **Enter**。
21. 在口令提示符处按 **Enter**。此时您已登录到 Cisco Secure IDS 传感器。

运行版本 3 的 IDS 设备的重新映像

完成下列步骤，对运行版本 3 的 IDS 设备进行重新映像。

注意： 在继续操作之前，请确保传感器未连接鼠标。

1. 将版本 3 恢复 CD 插入 IDS 设备并将其重新启动。
2. 根据设置按照提示操作，直到恢复成功。
3. 使用默认用户名/口令“root/attack”登录。
4. 运行 **sysconfig-sensor** 以便重新配置设备。

IDS 设备版本 4

已知管理员用户名/口令的恢复过程

如果已知管理员帐户的口令，则可以使用该用户帐户重置其他用户口令。

例如，IDS 设备上配置了两个用户名“cisco”和“adminuser”。用户“cisco”的口令需要重置，因此可使用“adminuser”登录并重置该口令。

```
sv8-4-ids4250 login: adminuserPassword:!--- Output is suppressed. idsm2-sv-rack#configure
terminal idsm2-sv-rack(config)#no username cisco idsm2-sv-rack(config)#username cisco priv admin
password 123cisco123 idsm2-sv-rack(config)#exit idsm2-sv-rack#exit sv8-4-ids4250 login: cisco
Password: !--- Output is suppressed. sv8-4-ids4250#
```

已知服务用户名/口令的恢复过程

如果已知服务帐户的口令，则可以使用该用户帐户重置其他用户口令。

例如，IDS 设备上配置了三个用户名“cisco”、“adminuser”和“serviceuser”。用户“cisco”的口令需要重置，因此可使用“serviceuser”登录并重置该口令。

```
sv8-4-ids4250 login: tacPassword:
!--- Output is suppressed. bash-2.05a$ su root Password: [root@sv8-4-ids4250 serviceuser]#passwd
cisco Changing password for user cisco. New password: Retype new password: passwd: all
authentication tokens updated successfully. [root@sv8-4-ids4250 serviceuser]#exit exit bash-
2.05a$ exit logout sv8-4-ids4250 login: cisco Password: !--- Output is suppressed. sv8-4-
```

```
ids4250#
```

注意： 根口令与服务帐户的口令相同。

对运行版本 4 的 IDS 设备进行重新映像

完成下列步骤，对 IDS 设备进行重新映像。

注意： 在继续操作之前，请确保传感器未连接鼠标。

1. 将版本 4 恢复 CD 插入 IDS 设备并将其重新启动。
2. 根据设置按照提示操作，直到恢复成功。
3. 使用默认用户名/口令“cisco/cisco”登录。
4. 运行 **setup** 以便重新配置设备。

IPS 设备版本 5 和版本 6

AIP-SSM 的重新加载、关闭、重置和恢复

下列命令可用于重新加载、关闭、重置、恢复口令，以及直接从自适应安全设备恢复高级检查和防御安全服务模块 (AIP-SSM)：

注意： 可以在特权 EXEC 模式或全局配置模式下输入 **hw-module** 命令。可以在单一路由模式和单一透明模式下输入这些命令。对于在多模式（路由或透明多模式）下运行的自适应安全设备，只能通过系统上下文执行 **hw-module** 命令（而不是从管理员或用户上下文执行）。

- **hw-module module slot_number reload** — 此命令在 AIP-SSM 上重新加载软件，而无需进行硬件重置。只有 AIP-SSM 处于 UP 状态时，此命令才有效。
- **hw-module module slot_number shutdown** — 此命令关闭 AIP-SSM 上的软件。只有 AIP-SSM 处于 UP 状态时，此命令才有效。
- **hw-module module slot_number reset** — 此命令执行 AIP-SSM 的硬件重置。当卡处于 Up/Down/Unresponsive/Recover 状态时，此命令才可用。
- **hw-module module slot_number** password-reset — 此命令 恢复 Cisco ASA 5500 系列内容安全和控制安全服务模块 (CSC-SSM) 或 AIP-SSM 上的口令，而无需重新映像设备。**注意：** 此命令从 IPS 6.0（ASA 7.2 版）开始提供支持，用于将 Cisco CLI 帐户口令恢复为默认口令 **cisco**。
- **hw-module module slot_number recover [boot|终止|configure]** — recover 命令显示一组用于设置或更改恢复参数的交互选项。按下 **Enter** 时，可以更改参数或保持现有设置。有关用于恢复 AIP-SSM 的过程，请参阅安装 AIP-SSM 系统映像。**hw-module module slot_number recover boot** — 此命令开始 AIP-SSM 的恢复。只有 AIP-SSM 处于 Up 状态时，此命令才可用。**hw-module module slot_number recover stop** — 此命令停止 AIP-SSM 的恢复。只有 AIP-SSM 处于 Recover 状态时，此命令才可用。**注意：** 如果需要停止 AIP-SSM 恢复，则必须在开始 AIP-SSM 恢复后 30 到 45 秒内发出 **hw-module module 1 recover stop** 命令。如果超过此等待时间，则可能导致意外的后果。例如，AIP-SSM 可能会以 Unresponsive 状态出现。**hw-module module 1 recover configure** — 使用此命令配置用于模块恢复的参数。基本参数是 IP 地址和恢复映像 TFTP 的 URL 位置。**示例：**
```
aip-ssm#hardware-module module 1 recover configure Image URL [tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-1.img]: Port IP Address [10.89.149.226]: VLAN ID [0]: Gateway IP Address [10.89.149.254]:
```

对 AIP-SSM 系统映像进行重新映像

完成下列步骤以安装 AIP-SSM 系统映像：

1. 登录到 ASA。
2. 进入启用模式：asa>enable
3. 配置 AIP-SSM 的恢复设置：asa#**hw-module module 1 recover configure** **注意：** 如果恢复配置出错，请使用 **hw-module module 1 recover stop** 命令停止系统重新映像，随后可更正配置。
4. 为系统映像指定 TFTP URL：Image URL [tftp://0.0.0.0/]: **示例：Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img**
5. 指定 AIP-SSM 的命令和控制接口：Port IP Address [0.0.0.0]:**示例：Port IP Address [0.0.0.0]: 10.89.149.231**
6. 将 VLAN ID 保留为 0。 VLAN ID [0]:
7. 指定 AIP-SSM 的默认网关：Gateway IP Address [0.0.0.0] :**示例：Gateway IP Address [0.0.0.0]:10.89.149.254**
8. 执行恢复：asa#**hw-module module 1 recover boot**
9. 定期检查恢复，直到其完成：**注意：** 在恢复过程中，状态显示为 guest@localhost.localdomain#，当重新映像完成时，状态显示为 guest@localhost.localdomain#。asa#**show module 1** Mod Card Type Model Serial No. --- ------ ------------------------------------ ------------------ ----------- 0 ASA 5540 Adaptive Security Appliance ASA5540 P2B00000019 1 ASA 5500 Series Security Services Module-20 ASA-SSM-20 P1D000004F4 Mod MAC Address Range Hw Version Fw Version Sw Version --- ------------ ------------------- ------------ ------------ --------------- 0 000b.fcf8.7b1c to 000b.fcf8.7b20 0.2 1.0(7)2 7.0(0)82 1 000b.fcf8.011e to 000b.fcf8.011e 0.1 1.0(7)2 5.0(0.22)S129.0 Mod Status --- ------------------ 0 Up Sys 1 Up asa# **注意：** 要调试恢复进程中可能发生的任何错误，请使用 **debug module-boot** 命令启用系统重新映像进程的调试。
10. 向 AIP-SSM 发起会话并使用 **setup** 命令初始化 AIP-SSM。

IDSM

保留配置时，无法对 IDSM 执行口令恢复。

注意： 此过程要求使用维护分区。如果已更改维护分区口令，而您无法登录，则需要更换 IDSM。在这种情况下，请与 Cisco 技术支持联系以获得帮助。

使用运行本地 IOS（集成 IOS）代码的交换机对 IDSM 进行重新映像

完成下列步骤，使用运行本地 IOS（集成 IOS）代码的交换机对 ISDM 进行重新映像。

1. 启动IDSM到维护分区使用*x*代表插槽编号的switch命令**hw-module模块*x*重置的hdd:2**。SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- -------------------------- ---------- ------------------ ----------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------------------------------- ------ ------------ ------------ ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok SV9-1#**hw-module module 6 reset hdd:2** Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y % reset issued for module 6 *!--- Output suppressed.*
2. 使用交换机命令 **show module x** 检查 IDSM 是否进入在线状态。确保 IDSM 软件版本的开头为 2（表示维护分区软件当前正在 IDSM 上运行），并且状态为 OK。SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- -------------------------------------- --------- --------- ----------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------------------------------- ------ ------------ ------ ------ ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 2.5(0) Ok
3. 使用交换机命令 **session slot x processor 1** 连接到 IDSM 维护分区。使用用户名/口令

ciscoids/attack。SV9-1#**session slot 6 proc 1** The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: ciscoidsPassword: maintenance#

4. 安装缓存映像以便对 IDSM 应用程序分区进行重新映像。发出诊断命令 **ids-installer system /cache /show** 以验证缓存映像是否存在。maintenance#**diag** maintenance(diag)#**ids-installer system /cache /show** Details of the cached image: Package Name : IDSMk9-a-3.0-1-S4 Release Info : 3.0-1-S4 Total CAB Files in the package : 5 CAB Files present : 5 CAB Files missing : 0 List of CAB Files missing ---------- maintenance(diag)# 如果缓存映像不存在或缓存版本不是您要安装的版本，请继续执行步骤 5。要对使用缓存映像的 ISDM 进行重新映像，请使用诊断命令 **ids-installer system /cache /install**。maintenance(diag)#**ids-installer system /cache /install** 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 E41E-3608 Extracting the image... *!--- Output is suppressed.* STATUS: Image has been successfully installed on drive C:\! 重新映像完成后，继续执行步骤 12。
5. 确保 IDSM 具有 IP 连接。发出命令 **ping ip_address** 。maintenance#**diag** maintenance(diag)#**ping 10.66.84.1** Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
6. 如果 IDSM 具有 IP 连接，请继续执行步骤 11。如果没有 IP 连接，请继续执行步骤 7 至步骤 9。
7. 确保在交换机上正确配置命令和控制接口。发出命令 **show run interface Gigx/2**。SV9-1#**show run interface Gig6/2** Building configuration... Current configuration : 115 bytes ! interface GigabitEthernet6/2 no ip address switchport switchport access vlan 210 switchport mode access end SV9-1#
8. 确保在 IDSM 维护分区上正确配置通信参数。发出诊断命令 **ids-installer netconfig /view**。maintenance#**diag** maintenance(diag)#**ids-installer netconfig /view** IP Configuration for Control Port: IP Address : 10.66.84.124 Subnet Mask : 255.255.255.128 Default Gateway : 10.66.84.1 Domain Name Server : 1.1.1.1 Domain Name : cisco Host Name : idsm-sv-rack
9. 如果未设置任何参数或需要更改其中某些参数，请使用诊断命令 **ids-installer netconfig /configure parameters** 。maintenance(diag)#**ids-installer netconfig /configure / ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 / dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack** STATUS: Network parameters for the config port have been configured ! NOTE: Reset the module for the changes to take effect!
10. 在您重置IDSM使更改生效后，再请检查IP连通性。如果 IP 连接仍然有问题，请按普通 IP 连接问题进行故障排除，然后继续执行步骤 11。
11. 对 IDSM 应用程序分区进行重新映像。使用诊断命令 **ids-installer system /nw /install /server=ip_address /user=account /save={yes/no} /dir=ftp_path /prefix=file_prefix** 下载映像，其中：*ip_address* 是 FTP 服务器的 IP 地址。*account* 是登录到 FTP 服务器时要使用的用户名或帐户名。*save* 用于确定是否将下载映像的副本保存为缓存副本。如果为 yes，则会覆盖所有存在的缓存映像。如果为 no，则会将下载的映像安装在非活动分区中，而不保存缓存副本。*ftp_path* 指定 FTP 服务器上映像文件所在的目录。*file_prefix* 是下载的映像中 .dat 文件的文件名。下载的映像包括一个扩展名为 .dat 的文件和若干扩展名为 .cab 的文件。file_prefix 值必须是 DAT 文件的名称，但不包含 .dat 后缀。maintenance#**diag** maintenance(diag)#**ids-installer system /nw /install /server=10.66.64.10 /user=cisco /save=yes /dir='/tftpboot/georgia' /** 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 2407-F686 Extracting the image... *!--- Output is suppressed.* STATUS: Image has been successfully installed on drive C:\!
12. 使用switch命令**hw-module模块x重置的hdd:1，**启动IDSM到应用程序分区。SV9-1#**hw-module module 6 reset hdd:1** Device BOOT variable for reset = Warning: Device list is not

verified. Proceed with reload of module? [confirm]y *!--- Output is suppressed.* 另外，确保交换机配置为将 IDSM 引导至应用程序分区。要检查此配置，请使用命令 **show bootvar device module x** 。SV9-1#**show bootvar device module 6** [mod:6]: SV9-1# 为了配置IDSM的引导程序设备变量，请使用switch configuration命令**引导程序设备模块x hdd:1**。SV9-1#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. SV9-1(config)#**boot device module 6 hdd:1** Device BOOT variable = hdd:1 Warning: Device list is not verified. SV9-1(config)#endSV9-1#**show bootvar device module 6** [mod:6]: hdd:1 SV9-1#

13. 使用交换机命令 **show module x** 检查 IDSM 是否进入在线状态。确保 IDSM 软件版本是应用程序分区版本（例如 *3.0(1)S4* ），并且状态为 OK。SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- ------------------------------------ ------------------ ----------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- --------------------------------- ------ ------------ ------------ ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok
14. 既然 IDSM 已引导至应用程序分区，则连接到 IDSM 并对其进行配置，使其可以与控制器通信。使用命令 **setup**。与控制器建立通信后，便可以将配置下载到 IDSM。使用用户名/口令 **ciscoids/attack** 登录。SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: ciscoids
Password:#**setup** --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration diaglog at any prompt. Default settings are in square brackets '[]'. Current Configuration: Configuration last modified Never Sensor: IP Address: 10.0.0.1 Netmask: 255.0.0.0 Default Gateway:Host Name: Not Set Host ID: Not Set Host Port: 45000 Organization Name: Not Set Organization ID: Not Set Director: IP Address: Not Set Host Name: Not Set Host ID: Not Set Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: Not Set Organization ID: Not Set Direct Telnet access to IDSM: disabled Continue with configuration dialog? [yes]: Enter virtual terminal password[]: Enter sensor IP address[10.0.0.1]: 10.66.84.124 Enter sensor netmask [255.0.0.0]: 255.255.255.128 Enter sensor default gateway []: 10.66.84.1 Enter sensor host name []: idsm-sv-rack Enter sensor host id []: 124 Enter sensor host post office port [45000]: Enter sensor organization name []: cisco Enter sensor organization id []: 100 Enter director IP address[]: 10.66.79.249 Enter director host name []: vms1 Enter director host id []: 249 Enter director host post office port [45000]: Enter director heart beat interval [5]: Enter director organization name []: cisco Enter director organization id []: 100 Enable direct Telnet access to IDSM? [no]: The following configuration was entered: Configuration last modified Never Sensor:IP Address: 10.66.84.124 Netmask: 255.255.255.128 Default Gateway: 10.66.84.1 Host Name: idsm-sv-rack Host ID: 124 Host Port: 45000 Organization Name: cisco Organization ID: 100 Director: IP Address: 10.66.79.249 Host Name: vms1 Host ID: 249 Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: cisco Organization ID: 100 Direct Telnet access to IDSM: disabled WARNING: Applying this configuration will cause all configuration files to be initialized and the card to be rebooted. Apply this configuation?: yes Configuration Saved. Resetting... *!--- Output is suppressed.*

使用运行混合 (CatOS) 代码的交换机对 IDSM 进行重新映像

完成下列步骤，使用运行混合 (CatOS) 代码的交换机对 ISDM 进行重新映像。

注意： 应用程序分区中的所有信息将丢失。保留配置时，无法对 IDSM 执行口令恢复。

注意： 此过程要求使用维护分区。如果已更改维护分区口令，而您无法登录，则需要更换 IDSM。在这种情况下，请与 Cisco 技术支持联系以获得帮助。

1. 启动IDSM到有switch命令**重置的*x* hdd:2**维护分区。ltd9-9> (enable) **show module 4** Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ -------------- ---- --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ------------------- ----------- 4 SAD063000CE Mod MAC-Address(es) Hw Fw Sw

--- ------------------------------------ ------ ---------- ---------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 3.0(5)S23 ltd9-9> (enable)**reset 4 hdd:2** This command will reset module 4. Unsaved configuration on module 4 will be lost Do you want to continue (y/n) [n]? y Module 4 shut down in progress, please don't remove module until shutdown completed. *!--- Output is suppressed.*

2. 使用交换机命令 **show module x** 检查 IDSM 是否进入在线状态。确保 IDSM 软件版本的开头为 2（表示维护分区软件当前正在 IDSM 上运行），并且状态为 OK。ltd9-9> (enable) **show module 4** Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ---------- -- ---------- --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ---------- ---------- 4 SAD 063000CEMod MAC-Address(es) Hw Fw Sw --- ------ ---------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 2.5(0)
3. 既然 IDSM 已引导至维护分区，则使用交换机命令 **session x** 连接到 IDSM。使用用户名/口令 **ciscoids/attack**。ltd9-9> (enable)**session 4** Trying IDS-4... Connected to IDS-4. Escape character is '^]'. login: ciscoids Password: maintenance#
4. 安装缓存映像以便对 IDSM 应用程序分区进行重新映像。使用诊断命令 **ids-installer system /cache /show** 验证缓存映像是否存在。maintenance#**diag** maintenance(diag)#**ids-installer system /cache /show** Details of the cached image: Package Name : IDSMk9-a-3.0-1-S4 Release Info : 3.0-1-S4 Total CAB Files in the package : 5 CAB Files present : 5 CAB Files missing : 0 List of CAB Files missing ---------- maintenance(diag)# 如果缓存映像不存在或缓存版本不是您要安装的版本，请继续执行步骤 5。要对使用缓存映像的 ISDM 进行重新映像，请使用诊断命令 **ids-installer system /cache /install**。maintenance(diag)#**ids-installer system /cache /install** 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 E41E-3608 Extracting the image... *!--- Output is suppressed.* STATUS: Image has been successfully installed on drive C:\! 重新映像完成后，继续执行步骤 12。
5. 使用命令 **ping ip_address** 确保 IDSM 具有 IP 连接。maintenance#**diag** maintenance(diag)#**ping 10.66.84.1** Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255
6. 如果 IDSM 具有 IP 连接，请继续执行步骤 11。如果没有 IP 连接，请继续执行步骤 7 至步骤 9。
7. 使用命令 **show port status x/2** 确保在交换机上正确配置命令和控制接口。ltd9-9> (enable)**show port status 4/2** Port Name Status Vlan Duplex Speed Type ----- ---------- ---- ---------- ---------- ------ ----- ------------ 4/2 connected 1 full 1000 Intrusion De
8. 使用诊断命令 **ids-installer netconfig /view** 确保在 IDSM 维护分区上正确配置通信参数。maintenance#**diag** maintenance(diag)#**ids-installer netconfig /view** IP Configuration for Control Port: IP Address : 10.66.84.124 Subnet Mask : 255.255.255.128 Default Gateway : 10.66.84.1 Domain Name Server : 1.1.1.1 Domain Name : cisco Host Name : idsm-sv-rack
9. 如果未设置任何参数或需要更改其中某些参数，请使用诊断命令 **ids-installer netconfig /configure parameters** 。maintenance(diag)# **ids-installer netconfig /configure / ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 / dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack**
10. 重置 IDSM 使更改生效后，再次检查 IP 连接。如果 IP 连接仍然有问题，请按普通 IP 连接问题进行故障排除，然后继续执行步骤 11。
11. 对 IDSM 应用程序分区进行重新映像。使用诊断命令 **ids-installer system /nw /install /server=ip_address /user=account /save={yes/no} /dir=ftp_path /prefix=file_prefix** 下载映像，其中：*ip_address* 是 FTP 服务器的 IP 地址。*account* 是登录到 FTP 服务器时要使用的用户名或帐户名。*save* 用于确定是否将下载映像的副本保存为缓存副本。如果为 yes，则会覆盖所有现有的缓存映像。如果为 no，则会将下载的映像安装在非活动分区中，而不保存缓存副本。*ftp_path* 指定 FTP 服务器上映像文件所在的目录。*file_prefix* 是下载的映像中 .dat 文件的文件名。下载的映像包括一个扩展名为 .dat 的文件和若干扩展名为 .cab 的文件。file_prefix 值应为 DAT 文件的名称，但不包含 .dat 后缀。maintenance#**diag** maintenance(diag)#**ids-installer system /nw /install /server=10.66.64.10 /user=cisco**

/save=yes /dir='/tftpboot/georgia' /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 2407-F686 Extracting the image... *!--- Output is suppressed.* STATUS: Image has been successfully installed on drive C:\!

12. 启动IDSM到有使用的应用程序分区switch命令**重置*x* hdd:1**。ltd9-9> (enable)**reset 4 hdd:1** This command will reset module 4. Unsaved configuration on module 4 will be lost Do you want to continue (y/n) [n]? y *!--- Output is suppressed.* 另外，确保交换机配置为将 IDSM 引导至应用程序分区。使用命令 **show boot devicex** 检查此配置。ltd9-9> (enable)**show boot device 4** Device BOOT variable = 为了配置IDSM的引导程序设备变量，请使用switch configuration命令**set boot设备hdd:1** *X*。ltd9-9> (enable)**set boot device hdd:1 4** Device BOOT variable = hdd:1 Warning: Device list is not verified but still set in the boot string. ltd9-9> (enable)**show boot device 4** Device BOOT variable = hdd:1
13. 使用交换机命令 **show module x** 检查 IDSM 是否进入在线状态。确保 IDSM 软件版本是应用程序分区版本（例如 *3.0(1)S4*），并且状态为 OK。ltd9-9> (enable)**show module 4** Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ ------------ ----- --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ------------------- ----------- 4 SAD063000CE Mod MAC-Address(es) Hw Fw Sw --- ---------------------------------- ------ ---------- ---------------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 3.0(1)S4
14. 既然 IDSM 已引导至应用程序分区，则连接到 IDSM 并对其进行配置，使其可以与控制器通信。使用命令 **setup**。使用用户名/口令 **ciscoids/attack** 登录。ltd9-9> (enable)session 4 Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:#**setup** --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration diaglog at any prompt. Default settings are in square brackets '[]'. Current Configuration: Configuration last modified Never Sensor: IP Address: 10.0.0.1 Netmask: 255.0.0.0 Default Gateway: Host Name: Not Set Host ID: Not Set Host Port: 45000 Organization Name: Not Set Organization ID: Not Set Director: IP Address: Not Set Host Name: Not Set Host ID: Not Set Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: Not Set Organization ID: Not Set Direct Telnet access to IDSM: disabled Continue with configuration dialog? [yes]: Enter virtual terminal password[]: Enter sensor IP address[10.0.0.1]: 10.66.84.124 Enter sensor netmask [255.0.0.0]: 255.255.255.128 Enter sensor default gateway []: 10.66.84.1 Enter sensor host name []: idsm-sv-rack Enter sensor host id []: 124 Enter sensor host post office port [45000]: Enter sensor organization name []: cisco Enter sensor organization id []: 100 Enter director IP address[]: 10.66.79.249 Enter director host name []: vms1 Enter director host id []: 249 Enter director host post office port [45000]: Enter director heart beat interval [5]: Enter director organization name []: cisco Enter director organization id []: 100 Enable direct Telnet access to IDSM? [no]: The following configuration was entered: Configuration last modified Never Sensor: IP Address: 10.66.84.124 Netmask: 255.255.255.128 Default Gateway: 10.66.84.1 Host Name: idsm-sv-rack Host ID: 124 Host Port: 45000 Organization Name: cisco Organization ID: 100 Director:IP Address: 10.66.79.249 Host Name: vms1 Host ID: 249 Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: cisco Organization ID: 100 Direct Telnet access to IDSM: disabled WARNING: Applying this configuration will cause all configuration files to be initialized and the card to be rebooted. Apply this configuation?: yes Configuration Saved. Resetting... *!--- Output is suppressed.*

ISDM-2

已知管理员用户名/口令的恢复过程

如果已知管理员帐户的口令，则可以使用该用户帐户重置其他用户口令。

例如，IDSM-2 上配置了两个用户名“cisco”和“adminuser”。用户“cisco”的口令需要重置，因此可使用“adminuser”登录并重置该口令。

```
SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type
'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: adminuser
Password: !--- Output is suppressed. idsm2-sv-rack#configure terminal idsm2-sv-rack(config)#no
username cisco idsm2-sv-rack(config)#username cisco priv admin password 123cisco123 idsm2-sv-
rack(config)#exit idsm2-sv-rack#exit [Connection to 127.0.0.61 closed by foreign host] SV9-
1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit'
at the remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: !---
Output is suppressed. idsm2-sv-rack#
```

已知服务用户名/口令的恢复过程

如果已知服务帐户的口令，则可以使用该用户帐户重置其他用户口令。

例如，IDSM-2 上配置了三个用户名“cisco”、“adminuser”和“serviceuser”。用户“cisco”的口令需要重置，因此可使用“serviceuser”登录并重置该口令。

```
SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type
'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: serviceuser
Password: !--- Output is suppressed. bash-2.05a$ su root Password: [root@idsm2-sv-rack
serviceuser]#passwd cisco Changing password for user cisco. New password: Retype new password:
passwd: all authentication tokens updated successfully. [root@idsm2-sv-rack serviceuser]# exit
exit bash-2.05a$ exit logout [Connection to 127.0.0.61 closed by foreign host] SV9-1#session
slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit' at the
remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: !--- Output
is suppressed. idsm2-sv-rack#
```

注意： 根口令与服务帐户的口令相同。

使用运行本地 IOS（集成 IOS）代码的交换机对 IDSM-2 进行重新映像

完成下列步骤，使用运行本地 IOS（集成 IOS）代码的交换机对 ISDM-2 进行重新映像。

注意： 应用程序分区中的所有信息将丢失。保留配置时，无法对 IDSM-2 执行口令恢复。

1. 启动IDSM-2到有*x*代表插槽编号的使用的维护分区switch命令**hw-module模块*x*重置的cf:1，**并且锎代表‘微型闪存’。**注意：** 使用cf:1，如果问题遇到，请设法使用hdd:2作为替代方案。
   ```
   SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- --------------------------
   --------- ------------------ ----------- 6 8 Intrusion Detection System WS-SVC-IDSM2
   SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ---------------------------------- ------
   ------------ ------------ ------- 6 0030.f271.e3fd to 0030.f271.e404 0.102 7.2(1) 4.1(1)S47
   Ok Mod Sub-Module Model Serial Hw Status --- --------------------------- -------------- --
   ------------ ------- ------- 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 Ok Mod
   Online Diag Status --- ------------------- 6 Pass SV9-1#hw-module module 6 reset cf:1
   Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload
   of module? [confirm]y % reset issued for module 6 !--- Output is suppressed.
   ```
2. 使用交换机命令 **show module x** 检查 IDSM-2 是否进入在线状态。确保 IDSM-2 软件版本的末尾为“m”，并且状态为 OK。
   ```
   SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ---
   -- ------------------------------------ ------------------ ----------- 6 8 Intrusion
   Detection System (MP) WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ------
   --------------------------- ------ ------------ ------------ ------- 6 0030.f271.e3fd to
   0030.f271.e404 0.102 7.2(1) 1.3(2)m Ok Mod Sub-Module Model Serial Hw Status --- ----------
   ---------------- -------------- -------------- ------- ------- 6 IDS 2 accelerator board
   WS-SVC-IDSUPG 0347FDB6B8 2.0 Ok Mod Online Diag Status --- ------------------- 6 Pass
   ```
3. 既然 IDSM-2 已引导至维护分区，则连接到 IDSM-2。使用交换机命令 **session slot xprocessor 1**。使用用户名/口令 **guest/cisco**。
   ```
   SV9-1#session slot 6 processor 1 The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end
   ```

the session Trying 127.0.0.61 ... Open Cisco Maintenance image login: guest Password: Maintenance image version: 1.3(2) guest@idsm2-sv-rack.localdomain#

4. 确保 IDSM-2 具有 IP 连接。使用命令 **ping ip_address**。guest@idsm2-sv-rack.localdomain#**ping 10.66.79.193** guest@idsm2-sv-rack.localdomain#**ping 10.66.79.193** PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data. 64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=2.188 msec 64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.014 msec 64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=991 usec 64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.011 msec 64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.019 msec --- 10.66.79.193 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max/mdev = 0.991/1.244/2.188/0.473 ms guest@idsm2-sv-rack.localdomain#
5. 如果 IDSM-2 具有 IP 连接，请继续执行步骤 14。
6. 确保在交换机上正确配置命令和控制接口。使用命令 **show run|inc intrusion-detection**。SV9-1#**show run | inc intrusion-detection** intrusion-detection module 6 management-port access-vlan 210
7. 确保在 IDSM-2 维护分区上正确配置通信参数。使用命令 **show ip**。guest@idsm2-sv-rack.localdomain#**show ip** IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP Broadcast : 10.66.79.223 DNS Name : idsm2-sv-rack.localdomain Default Gateway : 10.66.79.193Nameserver(s) :
8. 如果未设置任何参数或需要更改其中某些参数，请将其全部清除。使用命令 clear **ip**。guest@idsm2-sv-rack.localdomain#**clear ip** guest@localhost.localdomain#**show ip** IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0 Nameserver(s) :
9. 配置 IDSM-2 维护分区上的 IP 地址和掩码信息。使用命令 **ip address ip_address netmask**。guest@localhost.localdomain#**ip address 10.66.79.210 255.255.255.224**
10. 配置 IDSM-2 维护分区上的默认网关。使用命令 **ip gateway gateway-address**。guest@localhost.localdomain#**ip gateway 10.66.79.193**
11. 配置 IDSM-2 维护分区上的主机名。使用命令 **ip host hostname**。尽管此操作不是必要的，但由于同时设置提示符，因此可帮助标识设备。guest@localhost.localdomain#**ip host idsm2-sv-rack** guest@idsm2-sv-rack.localdomain#
12. 您可能需要明确配置广播地址。使用命令 **ip broadcast broadcast-address**。默认设置通常可满足需要。guest@idsm2-sv-rack.localdomain#**ip broadcast 10.66.79.223**
13. 再次检查 IP 连接。如果 IP 连接仍然有问题，请按普通 IP 连接问题进行故障排除，然后继续执行步骤 14。
14. 对 IDSM-2 应用程序分区进行重新映像。使用命令 **upgrade ftp-url--安装**。guest@idsm2-sv-rack.localdomain#**upgrade ftp://cisco@10.66.64.10// tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz --install** Downloading the image. This may take several minutes... Password for cisco@10.66.64.10: 500 'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not understood. ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz (unknown size)/tmp/upgrade.gz [|] 65259K 66825226 bytes transferred in 71.40 sec (913.99k/sec) Upgrade file ftp://cisco@10.66.64.10//tftpboot/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.
15. 将 IDSM-2 引导至应用程序分区。请使用switch命令**hw-module模块*x*重置的hdd:1**。SV9-1#**hw-module module 6 reset hdd:1** Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y % reset issued for module 6 *!--- Output is suppressed.* 或者，也可以在 IDSM-2 上使用 **reset** 命令，前提是引导设备变量设置正确。要检查 IDSM-2 的引导设备变量设置，请使用交换机命令 **show bootvar device module x**。SV9-1#**show bootvar device module 6** [mod:6]: SV9-1# 为了配置IDSM-2的引导程序设备变量，请使用switch configuration命令**引导程序设备模块*x* hdd:1**。SV9-1#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. SV9-1(config)#boot device module 6 hdd:1 Device BOOT variable = hdd:1 Warning: Device list is not verified. SV9-1(config)#exitSV9-1#**show bootvar device module 6** [mod:6]: hdd:1 要通过维护分区 CLI

重置 IDSM-2，请使用命令 **reset**。`guest@idsm2-sv-rack.localdomain#reset !--- Output is suppressed.`

16. 检查 IDSM-2 是否进入在线状态。使用交换机命令 **show module x**。确保 IDSM-2 软件版本是应用程序分区版本（例如 *4.1(1)S47*），并且状态为 OK。`SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- ------------------------------------ ---------- ---- ----------- 6 8 Intrusion Detection System WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ---------------------------------- ------ ---------- ---------- ------ 6 0030.f271.e3fd to 0030.f271.e404 0.102 7.2(1) 4.1(1)S47 Ok Mod Sub-Module Model Serial Hw Status --- ------------------------- -------------- -------------- ------- ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 Ok Mod Online Diag Status --- ------------------ 6 Pass`
17. 既然 IDSM-2 已引导至应用程序分区，则连接到 IDSM-2。使用交换机命令 **session slot x processor 1**。使用用户名/口令 **cisco/cisco**。`SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open 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: !--- Output is suppressed.`
18. 配置 IDSM-2。使用命令 **setup**。`sensor#setup --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration:networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway 10.1.9.1 hostname sensor telnet Option disabled accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit Current time: Sat Sep 20 23:34:53 2003 Setup Configuration last modified: Sat Sep 20 23:32:38 2003 Continue with configuration dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]: 10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The following configuration was entered. networkParams ipAddress 10.66.79.210 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit [0] Go to the command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration and exit setup.Enter your selection [2]:Configuration Saved. sensor#`

使用运行混合 (CatOS) 代码的交换机对 IDSM-2 进行重新映像

完成下列步骤，使用运行混合 (CatOS) 代码的交换机对 ISDM-2 进行重新映像。

1. 将 IDSM-2 引导至维护分区。请使用switch命令**重置*x* hdd:2**。**注意：** 使用hdd:2，如果问题遇到，请设法使用cf:1作为替代方案。`SV9-1> (enable)show module 6 Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ ------------------ --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- -------- ----------- ----------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ------------------ ------------------ ------ ---------- ---------------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47 Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ---------- ------------ ------------------ ----------- ------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 SV9-1> (enable)reset 6 hdd:2 This command will reset module 6. Unsaved configuration on module 6 will be lost Do you want to continue (y/n) [n]? y Module 6 shut down in progress, please don't remove module until shutdown completed. !--- Output is suppressed.`
2. 检查 IDSM-2 是否进入在线状态。使用交换机命令 **show module x**。确保 IDSM-2 软件版本的末尾为“m”（表示维护分区软件当前正在运行），并且状态为 OK。`SV9-1> (enable)show module 6 Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ ---------- --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- ------------------ ----------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ---------- ---------- ------ 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 1.3(2)m Mod Sub-Type Sub-`

```
Model Sub-Serial Sub-Hw Sub-Sw --- ---------------------- ------------------ ----------
------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0
```

3. 既然 IDSM-2 已引导至维护分区，则连接到 IDSM-2。使用交换机命令 **session x**。使用用户名/口令 **guest/cisco**。`SV9-1> (enable)`**`session 6`** `Trying IDS-6... Connected to IDS-6. Escape character is '^]'. Cisco Maintenance image login: guest Password: Maintenance image version: 1.3(2) guest@idsm2-sv-rack.localdomain#`
4. 确保 IDSM-2 具有 IP 连接。使用命令 **ping ip_address**。`guest@idsm2-sv-rack.localdomain#`**`ping 10.66.79.193`** `PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data. 64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=1.035 msec 64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.041 msec 64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=1.066 msec 64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.074 msec 64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.026 msec --- 10.66.79.193 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max/mdev = 1.026/1.048/1.074/0.034 ms`
5. 如果 IDSM-2 具有 IP 连接，请继续执行步骤 14。
6. 确保在交换机上正确配置命令和控制接口。使用命令 **show port status x/2**。`SV9-1> (enable)`**`show port status 6/2`** `Port Name Status Vlan Duplex Speed Type ----- ---------- ---- ---------- ---------- ------ ----- ------------ 6/2 connected 210 full 1000 Intrusion De`
7. 确保在 IDSM-2 维护分区上正确配置通信参数。使用命令 **show ip**。`guest@idsm2-sv-rack.localdomain#`**`show ip`** `IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP Broadcast : 10.255.255.255 DNS Name : idsm2-sv-rack.localdomain Default Gateway : 10.66.79.193 Nameserver(s) :`
8. 如果未设置任何参数或需要更改其中某些参数，请使用命令 clear **ip** 将其全部清除。`guest@idsm2-sv-rack.localdomain#`**`clear ip`** `guest@localhost.localdomain#`**`show ip`** `IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0`
9. 配置 IDSM-2 维护分区上的 IP 地址和掩码信息。使用命令 **ip address ip_address netmask**。`guest@localhost.localdomain#`**`ip address 10.66.79.210 255.255.255.224`** `guest@localhost.localdomain#`
10. 配置 IDSM-2 维护分区上的默认网关。使用命令 **ip gateway gateway-address**。`guest@localhost.localdomain#`**`ip gateway 10.66.79.193`** `guest@localhost.localdomain#`
11. 配置 IDSM-2 维护分区上的主机名。使用命令 **ip host hostname**。尽管此操作不是必要的，但由于同时设置提示符，因此可帮助标识设备。`guest@localhost.localdomain#`**`ip host idsm2-sv-rack`** `guest@idsm2-sv-rack.localdomain#`
12. 您可能需要明确配置广播地址。使用命令 **ip broadcast broadcast-address**。默认设置通常可满足需要。`guest@idsm2-sv-rack.localdomain#`**`ip broadcast 10.66.79.223`**
13. 再次检查 IP 连接。如果 IP 连接仍然有问题，请按普通 IP 连接问题进行故障排除，然后继续执行步骤 14。
14. 对 IDSM-2 应用程序分区进行重新映像。使用命令 **upgrade ftp-url--安装**。`guest@idsm2-sv-rack.localdomain#`**`upgrade ftp://cisco@10.66.64.10// tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz --install`** `Downloading the image. This may take several minutes... Password for cisco@10.66.64.10:500 'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not understood.ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin. gz (unknown size)/tmp/upgrade.gz [|] 65259K 66825226 bytes transferred in 71.37 sec (914.35k/sec) Upgrade file ftp://cisco@10.66.64.10//tftpboot/ 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.`
15. 将 IDSM-2 引导至应用程序分区。请使用switch命令**重置*x* hdd:1**。`SV9-1> (enable)`**`reset 6 hdd:1`** `This command will reset module 6. Unsaved configuration on module 6 will be lost Do you want to continue (y/n) [n]? y Module 6 shut down in progress, please don't remove module until shutdown completed.` *`!--- Output is suppressed.`* 或者，也可以在 IDSM-2 上使用 **reset** 命令，前提是引导设备变量设置正确。要检查 IDSM-2 的引导设备变量设置，请使

用交换机命令 **show boot device x**。`SV9-1> (enable)`**`show boot device 6`** `Device BOOT variable = (null) (Default boot partition is hdd:1) Memory-test set to PARTIAL` 为了配置IDSM-2的引导程序设备变量，请使用switch configuration命令**set boot设备hdd:1** *X*。`SV9-1> (enable)`**`set boot device hdd:1 6`** `Device BOOT variable = hdd:1 Memory-test set to PARTIAL Warning: Device list is not verified but still set in the boot string. SV9-1> (enable)` **`show boot device 6`** `Device BOOT variable = hdd:1 Memory-test set to PARTIAL` 要通过维护分区 CLI 重置 IDSM-2，请使用命令 **reset**。`guest@idsm2-sv-rack.localdomain#`**`reset`** *`!--- Output is suppressed.`*

16. 检查 IDSM-2 是否进入在线状态。使用交换机命令 **show module x**。确保 IDSM-2 软件版本是应用程序分区版本（例如 *4.1(1)S47*），并且状态为 OK。`SV9-1> (enable)`**`show module 6`** `Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ ----- ------------- --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- ------------------- ----------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ------------------------------------ ------ ---------- -------- --------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47 Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ---------------------- ------------------ ------- ---- ------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0`
17. 既然 IDSM-2 已引导至应用程序分区，则连接到 IDSM-2。使用交换机命令 **session x**。使用用户名/口令 **cisco/cisco**。`SV9-1> (enable)`**`session 6`** `Trying IDS-6... Connected to IDS-6. 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:` *`!--- Output is suppressed.`*
18. 使用命令 **setup** 配置 IDSM-2。`sensor#`**`setup`** `--- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway 10.1.9.1 hostname sensor telnetOption disabled accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit Current time: Sat Sep 20 21:39:29 2003 Setup Configuration last modified: Sat Sep 20 21:36:30 2003 Continue with configuration dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]: 10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The following configuration was entered. networkParams ipAddress 10.66.79.210 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit [0] Go to the command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration and exit setup. Enter your selection[2]: Configuration Saved. sensor#`

相关信息

- Cisco IDS UNIX Director
- Catalyst 6500 系列入侵检测系统 (IDSM-1) 服务模块
- Catalyst 6500 系列入侵检测系统 (IDSM-2) 服务模块
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems