Cisco IDS感應器和IDS服務模組(IDSM-1、IDSM-2)的密碼復原程式

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[IDS裝置版本3](#)
[運行版本3的IDS裝置的密碼恢復](#)
[運行版本3的IDS裝置的重新映像](#)
[IDS裝置版本4](#)
[已知管理員使用者名稱/密碼的恢復過程](#)
[服務使用者名稱/密碼為已知時的恢復過程](#)
[重新映像運行版本4的IDS裝置](#)
[IPS裝置版本5和版本6](#)
[重新載入、關閉、重置和恢復AIP-SSM](#)
[重新映像AIP-SSM系統映像](#)
[IDSM](#)
[使用運行本地IOS（整合IOS）代碼的交換機重新映像IDSM](#)
[使用執行混合(CatOS)代碼的交換機重新映像IDSM](#)
[ISDM-2](#)
[已知管理員使用者名稱/密碼的恢復過程](#)
[服務使用者名稱/密碼為已知時的恢復過程](#)
[使用運行本地IOS（整合IOS）代碼的交換機重新映像IDSM-2](#)
[使用執行混合(CatOS)代碼的交換機重新映像IDSM-2](#)
[相關資訊](#)

簡介

本文提供如何恢復思科安全入侵偵測系統(IDS)（前身為NetRanger）裝置和所有版本的模組的步驟。

必要條件

需求

如果需要FTP伺服器，它必須支援被動模式。恢復光碟可以使用產品升級工具獲取(僅限註冊客戶)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- IDS裝置版本3和4
- IPS裝置版本5和6
- IDS Module(IDSM)版本3和IDSM-2版本4

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

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

IDS裝置版本3

版本3裝置有兩個可用選項。您可以使用密碼復原程式，也可以使用版本3復原CD進行重新映像。請注意，重新映像時會丟失所有資訊。口令恢復過程實質上是Solaris口令恢復。僅當沒有可從其複製配置的管理站(思科安全策略管理器(CSPM)、VPN/安全管理解決方案(VMS)和UNIX導向器)時，才使用此選項。

對於IDS裝置版本3及更低版本，存在兩個名為「netrangr」和「root」的使用者名稱。 兩者的預設密碼為「attack」。

運行版本3的IDS裝置的密碼恢復

這些檔案是恢復密碼所必需的。

- Solaris Device Configuration Assistant磁碟（引導磁碟）。 您可以從Sun支援網站下載檔案。**注意：如**果此連結不起作用，請嘗試轉到Sun支援網站的頂級，然後在「驅動程式」下搜尋「*Device Configuration Assistant Boot Diskette Solaris Driver Downloads*」。Cisco Systems，Inc.不維護Sun支援網站 ，無法控制內容所在的位置。
- Solaris for Intel(x86)光碟。
- 通過控制檯訪問工作站。

完成以下步驟即可復原密碼。

1. 插入啟動盤。
2. 將CD插入CD-ROM驅動器。
3. 關閉工作站，等待10秒，然後將其開啟。系統從啟動盤啟動。進行某些配置後，將顯示初始Configuration Assistant螢幕。
4. 按**F3**可對系統進行引導裝置的部分掃描。掃描完成後，將顯示裝置清單。
5. 確保CD-ROM裝置出現在裝置清單中，然後按**F2**繼續。螢幕顯示啟動裝置清單。
6. 選擇**CD-ROM**驅動器，然後按空格鍵。CD-ROM裝置旁邊有一個「X」。
7. 按**F2**繼續。工作站現在從CD-ROM啟動。
8. 在用於選擇安裝型別的螢幕上，選擇**選項2, Jumpstart**。系統繼續啟動。
9. 在提示選擇語言時，選擇**選項0**選擇英語。
10. 在語言的下一個螢幕中，再次為英語ANSI選擇**Option 0**。系統繼續引導並顯示「Solaris安裝」螢幕。

11. 按住**Control**鍵並鍵入**C**可停止安裝指令碼並允許訪問提示。
12. 鍵入**mount -F ufs /dev/dsk/c0t0d0s0 /mnt。**「/」分割槽現在裝載在「/mnt」裝載點。您可以在此處編輯「/etc/shadow」檔案並刪除根密碼。
13. 鍵入**cd /mnt/etc**。
14. 設定shell環境以便可以正確讀取資料。鍵入**TERM=ansi**。鍵入**export TERM**。
15. 鍵入**vi shadow**。您現在位於卷影檔案中，可以刪除密碼。條目必須是：

    ```
    root:gNyqp8ohdfxPI:10598::::::
    ```

    「：」是欄位分隔符，加密的密碼是第二個欄位。
16. 刪除第二個欄位。例如，
    ```
    root:gNyqp8ohdfxPI:10598::::::
    ```
    更改為

    ```
    root::10598::::::.
    ```

    這將刪除root使用者的密碼。
17. 輸入**:wq!**以便寫入和退出檔案。
18. 從驅動器中取出磁碟和CD-ROM。
19. 鍵入**init 6**以重新啟動系統。
20. 在登入時輸入**root**:提示，然後按**Enter**鍵。
21. 出現密碼提示時按**Enter**。您現在已登入到Cisco Secure IDS感測器。

運行版本3的IDS裝置的重新映像

完成以下步驟，重新映像運行版本3的IDS裝置。

注意：繼續操作之前，請確保滑鼠未連線到感測器。

1. 將版本3恢復光碟插入IDS裝置並重新啟動它。
2. 根據您的設定按照提示操作，直到恢復成功。
3. 使用預設使用者名稱/密碼「root/attack」登入。
4. 運行**sysconfig-sensor**以重新配置裝置。

IDS裝置版本4

已知管理員使用者名稱/密碼的恢復過程

如果知道管理員帳戶的密碼，則可以使用該使用者帳戶重置其他使用者密碼。

例如，在IDS裝置上配置兩個名為「cisco」和「adminuser」的使用者名稱。 使用者「cisco」的密碼需要重置，因此「adminuser」登入並重置密碼。

```
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#
```

服務使用者名稱/密碼為已知時的恢復過程

如果知道服務帳戶的密碼，則可以使用此使用者帳戶重置其他使用者密碼。

例如，在IDS裝置上配置三個使用者名稱，分別名為「cisco」、「adminuser」和「serviceuser」。 使用者「cisco」的密碼需要重置，因此「serviceuser」登入並重置密碼。

```
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：根密碼與服務帳戶的密碼相同。

重新映像運行版本4的IDS裝置

完成以下步驟即可重新映像IDS裝置。

注意：繼續操作之前，請確保滑鼠未連線到感測器。

1. 將版本4恢復光碟插入IDS裝置並重新啟動它。
2. 根據您的設定按照提示操作，直到恢復成功。
3. 使用預設使用者名稱/密碼「cisco/cisco」登入。
4. 運行**setup**以重新配置裝置。

IPS裝置版本5和版本6

重新載入、關閉、重置和恢復AIP-SSM

使用以下命令直接從自適應安全裝置重新載入、關閉、重置、恢復密碼以及恢復高級檢測和防禦安全服務模組(AIP-SSM):

註：您可以在特權EXEC**模式或**全域性配置模式下輸入hw-module命令。您可以在單路由模式和單透明模式下輸入命令。對於在多模式（路由或透明多模式）下運行的自適應安全裝置，您只能從系統上下文（而不是從管理員或使用者上下文）執行**hw-module**命令。

- hw-module module *slot_number* ***reload*** — 此命令在不執行硬體重置的情況下重新載入AIP-SSM上的軟體。僅當AIP-SSM處於Up狀態時才有效。
- hw-module module *slot_number* ***shutdown*** — 此命令關閉AIP-SSM上的軟體。僅當AIP-SSM處

於Up狀態時才有效。

- hw-module module *slot_number* ***reset*** — 此命令執行AIP-SSM的硬體重置。當卡處於Up/Down/Unresponse/Recover狀態時適用。
- hw-module module *slot_number* ***password-reset — 此命令可恢復Cisco ASA 5500系列內容安全與控制安全服務模組(CSC-SSM)或AIP-SSM上的密碼，而無需重新映像裝置。*** **注意**：此命令從IPS 6.0（ASA 7.2版本）開始支援，用於將Cisco CLI帳戶密碼還原為預設**cisco**。
- **hw-module module *slot_number* recover [boot |停止 | configure] - recover命令顯示一組用於設定或更改恢復引數的互動式選項。**按**Enter**鍵時，可以更改引數或保留現有設定。有關用於恢復AIP-SSM的過程，請參閱安裝AIP-SSM系統映像。hw-module module *slot_number* ***recover boot*** — 此命令啟動AIP-SSM的恢復。僅當AIP-SSM處於Up狀態時才適用。**hw-module module *slot_number* recover stop** — 此命令停止AIP-SSM的恢復。僅當AIP-SSM處於「恢復」狀態時才適用。**注意：**如果需要停止AIP-SSM恢復，則必須在啟動AIP-SSM恢復後30到45秒內發出**hw-module module 1 recover** stop命令。如果你再等下去，可能會導致意想不到的後果。例如，AIP-SSM可能會進入無響應狀態。**hw-module module 1 recover configure** — 使用此命令配置模組恢復引數。基本引數是IP地址和恢復映像TFTP URL位置。範例：

```
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]:
```

重新映像AIP-SSM系統映像

完成以下步驟，安裝AIP-SSM系統映像：

1. 登入到ASA。
2. 進入啟用模式：
   ```
   asa>enable
   ```
3. 配置AIP-SSM的恢復設定：
   ```
   asa#hw-module module 1 recover configure
   ```

   注意：如果恢復配置出錯，請使用**hw-module module 1 recover stop命令停止系統重新映**像，然後您可以更正配置。
4. 指定系統映像的TFTP URL:
   ```
   Image URL [tftp://0.0.0.0/]:
   ```
   範例：
   ```
   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的命令和控制介面：
   ```
   Port IP Address [0.0.0.0]:
   ```
   範例：
   ```
   Port IP Address [0.0.0.0]: 10.89.149.231
   ```
6. 將VLAN ID保留為0。
   ```
    VLAN ID [0]:
   ```
7. 指定AIP-SSM的預設網關：
   ```
   Gateway IP Address [0.0.0.0] :
   ```
   範例：
   ```
   Gateway IP Address [0.0.0.0]:10.89.149.254
   ```
8. 執行恢復：
   ```
   asa#hw-module module 1 recover boot
   ```

9. 定期檢查恢復，直到恢復完成：**注意：**在恢復過程中，狀態將讀取

guest@localhost.localdomain#，而在重新映像完成時，狀態將讀取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#
```

註：為了調試恢復過程中可能發生的錯誤，請使用**debug module-boot**命令啟用系統重新映像進程的調試。

10. 會話到AIP-SSM，並使用**setup**命令初始化AIP-SSM。

IDSM

保留配置時，沒有方法可用於在IDSM上執行密碼恢復。

注意：此過程需要使用維護分割槽。如果已更改維護分割槽密碼，並且您無法登入，則需要更換IDSM。在這種情況下，請聯絡思科技術支援以獲得幫助。

使用運行本地IOS（整合IOS）代碼的交換機重新映像IDSM

完成這些步驟，使用執行原生IOS（整合IOS）代碼的交換機重新映像ISDM。

1. 使用交換機命令**hw-module module *x* reset hdd:2**(其中*x*代表插槽編號)將IDSM引導至維護分割槽。

```
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. 使用交換機命令**show module *x***檢查IDSM是否聯機。確保IDSM軟體版本在開頭有2個，表示維護分割槽軟體當前在IDSM上運行，並且狀態為正常。

```
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. 使用交換機命令**session slot *x* processor 1**連線到IDSM維護分割槽。使用**ciscoids/attack**的使用者名稱/密碼。

```
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. 安裝快取的映像以重新映像IDSM應用程式分割槽。發出diagnostics命令**ids-installer system /cache /show**以驗證快取的映像是否存在。

```
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)#
```

如果不存在快取的映像或快取的版本不是要安裝的版本，請繼續執行步驟5。要使用快取的映像重新映像ISDM，請使用診斷命令**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:\!
```

重新映像完成後，請繼續執行步驟12。

5. 確保IDSM具有IP連線。發出命令**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連線，請繼續執行步驟11。如果沒有IP連線，請繼續執行步驟7到9。
7. 確保在交換機上正確配置命令和控制介面。發出**show run interface Gigx/2**指令。

```
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. 確保在IDSM維護分割槽上正確配置了通訊引數。發出診斷命令**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. 如果未設定任何引數，或者需要更改某些引數，請使用診斷命令**ids-installer netconfig /configure** 引數。

```
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. 重置IDSM後再次檢查IP連線，以使更改生效。如果IP連線仍然有問題，請根據正常IP連線問題排除故障，然後繼續執行步驟11。
11. 重新映像IDSM應用程式分割槽。使用診斷命令ids-installer system /nw /install /server=*ip_address* /user=*account* **/save={***yes/no***} /dir=***ftp_path* **/prefix=***file_prefix*下載映像，其中：*ip_address*是FTP伺服器的IP地址。*account*是在登入到FTP伺服器時使用的使用者或帳戶名稱。*save*確定是否將下載映像的副本儲存為快取副本。如果是，則會覆蓋存在的任何快取映像。如果不是，則下載的映像將安裝在非活動分割槽上，但快取的副本不會儲存。*ftp_path*指定映像檔案所在的FTP伺服器上的目錄。*file_prefix*是下載映像中.dat檔案的檔案名稱。已下載的映像由一個副檔名為.dat的檔案和幾個副檔名為.cab的檔案組成。file_prefix值需要是DAT檔案的名稱，最多但不包括.dat字尾。

```
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. 使用交換機命令**hw-module module x reset hdd:1**將IDSM引導至應用程式分割槽。

```
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.
```

此外，請確保交換機配置為將IDSM引導至應用程式分割槽。若要檢查這一點，請使用**show bootvar device module *x*** 指令。

```
SV9-1#show bootvar device module 6
[mod:6 ]:
SV9-1#
```

要配置IDSM的引導裝置變數，請使用交換機配置命令**boot device module 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. 使用交換機命令**show module *x***檢查IDSM是否聯機。確保IDSM軟體版本是應用程式分割槽版本，例如*3.0(1)S4*，並且狀態為正常。

```
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. 現在連線到IDSM已引導到應用程式分割槽，並對其進行配置，以便與控制器通訊。使用命令**setup**。與控制器建立通訊後，配置即可下載到IDSM。使用**ciscoids/attack**的使用者名稱/密碼登入。

```
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.
```

使用執行混合(CatOS)代碼的交換機重新映像IDSM

完成這些步驟，使用執行混合(CatOS)代碼的交換機重新映像ISDM。

注意：應用程式分割槽中的所有資訊都將丟失。保留配置時，沒有方法可用於在IDSM上執行密碼恢復。

注意：此過程需要使用維護分割槽。如果已更改維護分割槽密碼，並且您無法登入，則需要更換IDSM。在這種情況下，請聯絡思科技術支援以獲得幫助。

1. 使用交換機命令**reset *x* hdd:2**將IDSM引導至維護分割槽。

```
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. 使用交換機命令**show module *x***檢查IDSM是否聯機。確保IDSM軟體版本在開頭有2個，表示維護分割槽軟體當前在IDSM上運行，並且狀態為正常。

```
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. 使用**switch command session** x 命令引導至維護分割槽後，請連線到IDSM。使用**ciscoids/attack**的使用者名稱/密碼。

```
ltd9-9> (enable)session 4
Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:
maintenance#
```

4. 安裝快取的映像以重新映像IDSM應用程式分割槽。使用diagnostics命令**ids-installer system /cache /show**驗證快取的映像是否存在。

```
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)#
```

如果不存在快取的映像，或者快取的版本不是要安裝的版本，請繼續執行步驟5。若要重新映像使用快取映像的ISDM，請使用診斷命令**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:\!
```

重新映像完成後，請繼續執行步驟12。

5. 使用命令**ping** ***ip_address*** 確保IDSM具有IP連線。

```
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連線，請繼續執行步驟11。如果沒有IP連線，請繼續執行步驟7到9。
7. 使用命令**show port status** ***x***/2，確認交換器上的命令和控制介面已正**確設定。**

```
ltd9-9> (enable)show port status 4/2
Port  Name                 Status     Vlan       Duplex Speed Type
----- -------------------- ---------- ---------- ------ ----- ------------
 4/2                       connected  1            full  1000 Intrusion De
```

8. 使用診斷命令**ids-installer netconfig /view**，確保在IDSM維護分割槽上正確配置通訊引數。

```
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. 如果未設定任何引數，或者需要更改某些引數，請使用診斷命令**ids-installer netconfig /configure** 引數。

```
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後再次檢查IP連線，以使更改生效。如果IP連線仍然有問題，請根據正常IP連線問題排除故障，然後繼續執行步驟11。
11. 重新映像IDSM應用程式分割槽。使用診斷命令**ids-installer system /nw /install /server=*ip_address* /user=account /save={*yes/no*}** /dir=*ftp_path* **/*prefix*=***file_prefix***下載映像，其中：*ip_address*是FTP伺服器的IP地址。*account*是在登入到FTP伺服器時使用的使用者或帳戶名稱。*save*確定是否將下載映像的副本儲存為快取副本。如果是，則覆蓋任何現有的快取映像。如果不是，則下載的映像將安裝在非活動分割槽上，但快取的副本不會儲存。*ftp_path*指定映像檔案所在的FTP伺服器上的目錄。*file_prefix*是下載映像中.dat檔案的檔案名稱。已下載的映像由一個副檔名為.dat的檔案和幾個副檔名為.cab的檔案組成。file_prefix值應該是DAT檔案的名稱，最多但不包括.dat字尾。

```
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**reset *x* hdd:**將IDSM引導至應用程式分割槽。

```
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.
```

此外，請確保配置了交換機，以便將IDSM引導到應用程式分割槽。使用**show boot device** x指令檢查此情況。

```
ltd9-9> (enable)show boot device 4
Device BOOT variable =
```

要配置IDSM的引導裝置變數，請使用交換機配置命令**set boot device 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. 使用交換機命令**show module *x***檢查IDSM是否聯機。確保IDSM軟體版本是應用程式分割槽版本，例如*3.0(1)S4*，並且狀態為正常。

```
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. 現在連線到IDSM已引導到應用程式分割槽，並對其進行配置，以便與控制器通訊。使用命令**setup**。使用使用者名稱/密碼**ciscoids/attack**登入。

```
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

已知管理員使用者名稱/密碼的恢復過程

如果知道管理員帳戶的密碼，則可以使用該使用者帳戶重置其他使用者密碼。

例如，在IDSM-2上配置兩個名為「cisco」和「adminuser」的使用者名稱。 使用者「cisco」的密碼需要重置，因此「adminuser」登入並重置密碼。

```
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#
```

服務使用者名稱/密碼為已知時的恢復過程

如果知道服務帳戶的密碼，則可以使用此使用者帳戶重置其他使用者密碼。

例如，在IDSM-2上配置了三個名為「cisco」、「adminuser」和「serviceuser」的使用者名稱。 使用者「cisco」的密碼需要重置，因此「serviceuser」登入並重置密碼。

```
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：根密碼與服務帳戶的密碼相同。

使用運行本地IOS（整合IOS）代碼的交換機重新映像IDSM-2

完成以下步驟，使用執行原生IOS（整合IOS）代碼的交換機重新映像ISDM-2。

注意：應用程式分割槽中的所有資訊都將丟失。保留配置時，沒有方法可用於在IDSM-2上執行密碼恢復。

1. 使用switch命令**hw-module module *x* reset cf:1**(其中*x*代表插槽編號，cf代表「compact flash」)將IDSM-2引導至維護分割槽。**注意**：如果使用cf:1時出現問題，請嘗試使用hdd:2作為備用選項。

```
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. 使用交換機命令**show module *x***檢查IDSM-2是否聯機。確保IDSM-2軟體版本末尾有「m」，並且狀態為正常。

```
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. 現在連線到IDSM-2，因為它已引導到維護分割槽。使用交換機命令**session slot xprocessor 1**。使用使用者名稱/密碼**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. 確保IDSM-2具有IP連線。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連線，請繼續執行步驟14。
6. 確保在交換機上正確配置命令和控制介面。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. 確保在IDSM-2維護分割槽上正確配置了通訊引數。使用命令**show ip**。

```
guest@idsm2-sv-rack.local
domain#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. 如果未設定任何引數，或者需要更改某些引數，請清除所有引數。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. 在IDSM-2維護分割槽上配置IP地址和掩碼資訊。使用命令**ip address *ip_address netmask*** 。

```
guest@localhost.localdomain#ip address 10.66.79.210 255.255.255.224
```

10. 在IDSM-2維護分割槽上配置預設網關。使用命令**ip gateway *gateway-address*** 。

```
guest@localhost.localdomain#ip gateway 10.66.79.193
```

11. 在IDSM-2維護分割槽上配置主機名。使用命令**ip host *hostname*** 。雖然這不是必需的，但有助於識別裝置，因為這樣也會設定提示。

```
guest@localhost.localdomain#ip host idsm2-sv-rack
```

```
guest@idsm2-sv-rack.localdomain#
```

12. 您可能需要顯式配置廣播地址。使用命令**ip broadcast *broadcast-address***。預設設定通常足夠。

```
guest@idsm2-sv-rack.localdomain#ip broadcast 10.66.79.223
```

13. 再次檢查IP連線。如果IP連線仍然有問題，請根據正常IP連線問題排除故障，並繼續步驟14。
14. 重新映像IDSM-2應用程式分割槽。使用命令**upgrade *ftp-url*** —install。

```
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. 將IDSM-2引導到應用程式分割槽。使用交換機命令**hw-module module *x* reset 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，只要引導裝置變數設定正確，您就可以在IDSM-2上使用**reset**命令。要檢查IDSM-2的引導裝置變數設定，請使用交換機命令**show bootvar device module *x***。

```
SV9-1#show bootvar device module 6
[mod:6 ]:
SV9-1#
```

要配置IDSM-2的引導裝置變數，請使用交換機配置命令**boot device module *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
```

要通過維護分割槽CLI重置IDSM-2，請使用命令**reset**。

```
guest@idsm2-sv-rack.localdomain#reset
!--- Output is suppressed.
```

16. 檢查IDSM-2是否聯機。使用switch指令**show module *x***。確保IDSM-2軟體版本是應用程式分割槽版本，例如*4.1(1)S47*，並且狀態為正常。

```
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. 現在連線到IDSM-2，因為它已引導到應用程式分割槽。使用交換機命令**session slot *x* processor 1**。使用使用者名稱/密碼**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#
```

使用執行混合(CatOS)代碼的交換機重新映像IDSM-2

完成這些步驟，使用執行混合(CatOS)代碼的交換機重新映像ISDM-2。

1. 將IDSM-2引導到維護分割槽。使用交換機命令**reset *x* hdd:2**。**注意**：如果使用hdd:2時出現問題，請嘗試使用cf:1作為替代方法。

```
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. 檢查IDSM-2是否聯機。使用switch指令**show module *x***。確保IDSM-2軟體版本在末尾有「m」，表示維護分割槽軟體當前正在運行，並且狀態為正常。

```
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. 現在連線到IDSM-2，因為它已引導到維護分割槽。使用交換機命令 **session *x***。使用使用者名稱/密碼**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. 確保IDSM-2具有IP連線。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連線，請繼續執行步驟14。
6. 確保在交換機上正確配置命令和控制介面。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. 確保在IDSM-2維護分割槽上正確配置了通訊引數。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. 如果沒有設定任何引數或需要更改某些引數，請使用命令clear ip清除這些引數。

```
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. 在IDSM-2維護分割槽上配置IP地址和掩碼資訊。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. 在IDSM-2維護分割槽上配置預設網關。使用命令ip gateway *gateway-address* 。

```
guest@localhost.localdomain#ip gateway 10.66.79.193
guest@localhost.localdomain#
```

11. 在IDSM-2維護分割槽上配置主機名。使用命令ip host *hostname* 。雖然這不是必需的，但它有助於識別裝置，因為這樣也會設定提示。

```
guest@localhost.localdomain#ip host idsm2-sv-rack
guest@idsm2-sv-rack.localdomain#
```

12. 您可能需要顯式配置廣播地址。使用命令ip broadcast *broadcast-address* 。預設設定通常足夠。

```
guest@idsm2-sv-rack.localdomain#ip broadcast 10.66.79.223
```

13. 再次檢查IP連線。如果IP連線仍是一個問題，請根據正常IP連線問題進行故障排除，然後繼續執行步驟14。
14. 重新映像IDSM-2應用程式分割槽。使用命令upgrade *ftp-url* —install。

```
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. 將IDSM-2引導到應用程式分割槽。使用交換機命令**reset *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，只要引導裝置變數設定正確，您就可以在IDSM-2上使用**reset**命令。要檢查IDSM-2的引導裝置變數設定，請使用交換機命令**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
```

要為IDSM-2配置引導裝置變數，請使用交換機配置命令**set boot device 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
```

要通過維護分割槽CLI重置IDSM-2，請使用命令**reset**。

```
guest@idsm2-sv-rack.localdomain#reset
!--- Output is suppressed.
```

16. 檢查IDSM-2是否聯機。使用switch指令**show module *x***。確保IDSM-2軟體版本是應用程式分割槽版本，例如*4.1(1)S47*，並且狀態為正常。

```
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. 現在連線到IDSM-2，因為它已引導到應用程式分割槽。使用交換機命令**session *x***。使用使用者名稱/密碼**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#
```

相關資訊

- Cisco IDS UNIX Director
- Catalyst 6500系列入侵偵測系統(IDSM-1)服務模組
- Catalyst 6500系列入侵偵測系統(IDSM-2)服務模組
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems