Procedura di recupero della password per i Cisco IDS Sensor e IDS Services Module (IDSM-1, IDSM-2)

Sommario

Introduzione

In questo documento vengono illustrate le procedure per il ripristino dell'appliance Cisco Secure Intrusion Detection System (IDS) (in precedenza NetRanger) e dei moduli per tutte le versioni.

Prerequisiti

Requisiti

Se è necessario un server FTP, deve supportare la modalità passiva. È possibile ottenere i CD di ripristino utilizzando lo strumento di aggiornamento del prodotto (solo utenti registrati).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Appliance IDS versioni 3 e 4
- Appliance IPS versioni 5 e 6
- IDS Module (IDSM) versione 3 e IDSM-2 versione 4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Appliance IDS versione 3

Per l'accessorio versione 3 sono disponibili due opzioni. È possibile utilizzare la procedura di recupero della password o eseguire una nuova immagine che utilizzi il CD di ripristino versione 3. Si noti che tutte le informazioni vengono perse in una nuova immagine. La procedura di recupero della password è essenzialmente un recupero della password di Solaris. Utilizzare questa opzione solo se non si dispone di una stazione di gestione (Cisco Secure Policy Manager (CSPM), VPN/Security Management Solution (VMS), UNIX Director) da cui è possibile copiare la configurazione.

Con IDS Appliance versione 3 e precedenti, esistono due nomi utente denominati 'netrangr' e 'root'. La password predefinita per entrambi è 'attack'.

Recupero password dell'appliance IDS con versione 3

Questi file sono necessari per recuperare la password.

- Disco dell'Assistente alla configurazione del dispositivo di Solaris (disco di avvio). È possibile scaricare i file dal sito Web del supporto Sun .**Nota:** se il link non funziona, cercare il livello superiore del sito Web di assistenza Sun e cercare *Device Configuration Assistant Boot Diskette Solaris Driver Downloads* sotto Drivers. Cisco Systems, Inc. non gestisce il sito Web di supporto Sun e non ha alcun controllo sulla posizione dei contenuti.
- Solaris per CD-ROM Intel (x86).
- Accesso da console alla workstation.

Per recuperare la password, effettuare i seguenti passaggi.

1. Inserire il disco di avvio.
2. Inserire il CD nell'unità CD-ROM.

3. Spegnere la workstation, attendere dieci secondi e accenderla.Il sistema viene avviato dal disco di avvio. Una volta completata la configurazione, viene visualizzata la schermata iniziale di Configuration Assistant.
4. Premere **F3** per eseguire una scansione parziale del sistema per rilevare le periferiche di avvio.Al termine della scansione, viene visualizzato un elenco di dispositivi.
5. Verificare che la periferica CD-ROM sia presente nell'elenco delle periferiche, quindi premere **F2** per continuare.In una schermata viene visualizzato un elenco delle periferiche di avvio.
6. Selezionare l'unità **CD-ROM**, quindi premere la barra spaziatrice.Accanto al dispositivo CD-ROM è presente una X.
7. Premere **F2** per continuare.La workstation viene ora avviata dal CD-ROM.
8. Nella schermata utilizzata per selezionare un tipo di installazione, scegliere l'**opzione 2, Jumpstart**.Il sistema continua ad avviarsi.
9. Alla richiesta di selezione di una lingua, scegliere **l'opzione 0** per l'inglese.
10. Nella schermata successiva relativa alle lingue, scegliere nuovamente **l'opzione 0** per l'inglese ANSI.Il sistema continua ad avviarsi e viene visualizzata la schermata di installazione di Solaris.
11. Tenere premuto il tasto **Control** e digitare **C** per interrompere lo script di installazione e consentire l'accesso al prompt.
12. Digitare **mount -F ufs /dev/dsk/c0t0d0s0 /mnt.**La partizione '/' è ora montata nel punto di montaggio '/mnt'. Da qui è possibile modificare il file '/etc/shadow' e rimuovere la password root.
13. Digitare **cd /mnt/etc**.
14. Impostare l'ambiente della shell in modo da poter leggere correttamente i dati.Digitare **TERM=ansi**.Digitare **export TERM**.
15. Digitare **vi ombra**.A questo punto è possibile rimuovere la password dal file shadow. La voce deve essere:

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

    ":" è un separatore di campo e la password cifrata è il secondo campo.
16. Eliminare il secondo campo. Ad esempio,
    `root:gNyqp8ohdfxPI:10598::::::`
    viene modificato in

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

    In questo modo viene rimossa la password dell'utente root.
17. Digitare **:wq!** per scrivere e chiudere il file.
18. Rimuovere il disco e il CD-ROM dalle unità.
19. Digitare **init 6** per riavviare il sistema.
20. Digitare **root** al login: e premere **Invio**.
21. Premere **Invio** al prompt della password.A questo punto, è stato eseguito l'accesso al sensore Cisco Secure IDS.

Nuova immagine dell'appliance IDS con versione 3

Completare questa procedura per ricreare l'immagine dell'appliance IDS con versione 3.

Nota: assicurarsi che il mouse non sia collegato al sensore prima di procedere.

1. Inserire il CD di ripristino versione 3 nell'accessorio IDS e riavviarlo.
2. Seguire i prompt in base alla configurazione fino al completamento del ripristino.
3. Effettuare l'accesso utilizzando il nome utente e la password predefiniti 'root/attack'.
4. Eseguire il comando **sysconfig-sensor** per riconfigurare l'accessorio.

Appliance IDS versione 4

Procedura di ripristino se il nome utente/password dell'amministratore è noto

Se è nota una password per un account amministratore, è possibile utilizzare questo account utente per reimpostare altre password utente.

Ad esempio, sull'appliance IDS sono configurati due nomi utente denominati 'cisco' e 'adminuser'. È necessario reimpostare la password dell'utente 'cisco', quindi 'adminuser' esegue l'accesso e reimposta la password.

```
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#
```

Procedura di ripristino se il nome utente/password del servizio è noto

Se è nota una password per l'account del servizio, è possibile utilizzare questo account utente per reimpostare altre password utente.

Ad esempio, nell'appliance IDS sono configurati tre nomi utente denominati 'cisco', 'adminuser' e 'serviceuser'. È necessario reimpostare la password dell'utente 'cisco', quindi 'serviceuser' esegue l'accesso e reimposta la password.

```
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#
```

Nota: la password di root è uguale alla password dell'account del servizio.

Ricreare l'immagine dell'appliance IDS con versione 4

Completare questa procedura per ricreare l'immagine dell'accessorio IDS.

Nota: assicurarsi che il mouse non sia collegato al sensore prima di procedere.

1. Inserire il CD di ripristino versione 4 nell'accessorio IDS e riavviarlo.
2. Seguire i prompt in base alla configurazione fino al completamento del ripristino.
3. Effettua l'accesso con il nome utente/password predefiniti, ossia 'cisco/cisco'.
4. Eseguire il **programma** di **installazione** per riconfigurare l'accessorio.

Appliance IPS versione 5 e versione 6

Ricaricare, arrestare, ripristinare e ripristinare AIP-SSM

Utilizzare questi comandi per ricaricare, arrestare, reimpostare, recuperare la password e ripristinare il modulo AIP-SSM (Advanced Inspection and Prevention Security Services Module) direttamente da Adaptive Security Appliance:

Nota: è possibile immettere i comandi **hw-module** in modalità di esecuzione privilegiata o in modalità di configurazione globale. Potete immettere i comandi in modalità di instradamento singolo e in modalità di trasparenza singola. Per i dispositivi di sicurezza adattivi che funzionano in modalità multipla (instradata o trasparente), è possibile eseguire i comandi **hw-module** solo dal contesto del sistema (non dal contesto dell'amministratore o dell'utente).

- **hw-module module module *slot_number* reload**: questo comando ricarica il software sull'AIP-SSM senza eseguire un reset dell'hardware. È valido solo quando AIP-SSM è nello stato Attivo.
- **hw-module module module *slot_number* shutdown** - Questo comando chiude il software su AIP-SSM. È valido solo quando AIP-SSM è nello stato Attivo.
- **hw-module module module *slot_number* reset**: questo comando esegue un reset hardware di AIP-SSM. È applicabile quando la scheda si trova nello stato Attivo/Inattivo/Non risponde/Ripristino.
- **hw-module module *slot_number* password-reset**: questo comando recupera una password su un Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM) o su un AIP-SSM senza dover ricreare l'immagine del dispositivo.**Nota:** questo comando avvia il supporto da IPS 6.0 (versione ASA 7.2) e viene usato per ripristinare la password predefinita dell'account Cisco CLI su **cisco**.
- **modulo hw-module *slot_number* recover [avvio | stop | configure]** - Il comando **recovery** visualizza una serie di opzioni interattive per l'impostazione o la modifica dei parametri di ripristino. È possibile modificare il parametro o mantenere l'impostazione esistente quando si preme **Invio**.Per la procedura di ripristino di AIP-SSM, vedere Installazione dell'immagine del sistema AIP-SSM.**hw-module module module *slot_number* recover boot**: questo comando avvia il ripristino di AIP-SSM. È applicabile solo quando AIP-SSM è nello stato Attivo.**hw-module module module *slot_number* recover stop**: questo comando interrompe il ripristino di AIP-SSM. È applicabile solo quando AIP-SSM è in stato Recupero.**Nota:** se il ripristino AIP-SSM deve essere interrotto, usare il comando **recovery stop del modulo hw-1** entro 30-45 secondi dall'avvio del ripristino AIP-SSM. Se si aspetta ancora, possono verificarsi

conseguenze inaspettate. È ad esempio possibile che AIP-SSM sia impostato sullo stato Non risponde.**hw-module module module 1 recover configure**: utilizzare questo comando per configurare i parametri per il ripristino del modulo. I parametri essenziali sono l'indirizzo IP e la posizione dell'URL TFTP dell'immagine di ripristino.Esempio:

```
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]:
```

Ricreare l'immagine del sistema AIP-SSM

Per installare l'immagine del sistema AIP-SSM, completare i seguenti passaggi:

1. Accedere all'appliance ASA.
2. Accedere alla modalità di abilitazione:
   ```
   asa>enable
   ```
3. Configurare le impostazioni di ripristino per AIP-SSM:
   ```
   asa#hw-module module 1 recover configure
   ```

   Nota: se si verifica un errore nella configurazione di ripristino, usare il comando **hw-module 1 recovery stop** per interrompere la ricreazione dell'immagine del sistema e quindi correggere la configurazione.
4. Specificare l'URL TFTP per l'immagine del sistema:
   ```
   Image URL [tftp://0.0.0.0/]:
   ```
   Esempio:
   ```
   Image URL [tftp://0.0.0.0/]:
    tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img
   ```
5. Specificare l'interfaccia di comando e controllo di AIP-SSM:
   ```
   Port IP Address [0.0.0.0]:
   ```
   Esempio:
   ```
   Port IP Address [0.0.0.0]: 10.89.149.231
   ```
6. Lasciare l'ID VLAN su 0.
   ```
    VLAN ID [0]:
   ```
7. Specificare il gateway predefinito di AIP-SSM:
   ```
   Gateway IP Address [0.0.0.0] :
   ```
   Esempio:
   ```
   Gateway IP Address [0.0.0.0]:10.89.149.254
   ```
8. Eseguire il ripristino:
   ```
   asa#hw-module module 1 recover boot
   ```

9. Controllare periodicamente il ripristino fino al completamento:**Nota:** lo stato è guest@localhost.localdomain# durante il ripristino e guest@localhost.localdomain# al termine della creazione della nuova immagine.
   ```
   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#
```

Nota: per eseguire il debug di eventuali errori nel processo di ripristino, usare il comando **debug module-boot** per abilitare il debug del processo di ricreazione dell'immagine del sistema.

10. Sessione di AIP-SSM e inizializzazione di AIP-SSM con il comando **setup**.

IDSM

Non è possibile utilizzare alcun metodo per eseguire un recupero della password su IDSM mentre la configurazione viene mantenuta.

Nota: questa procedura richiede l'utilizzo della partizione di manutenzione. Se la password della partizione di manutenzione è stata modificata e non è possibile eseguire l'accesso, è necessario sostituire IDSM. In questo caso, contattare il supporto tecnico Cisco per assistenza.

Ricreare l'immagine di IDSM con uno switch con codice IOS (IOS integrato) nativo

Completare questa procedura per ricreare un'immagine dell'ISDM con uno switch con codice IOS nativo (Integrated IOS).

1. Avviare l'IDSM nella partizione di manutenzione usando il comando **hw-module module module *x* reset hdd:2** dove *x* sta per il numero di slot.

```
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. Verificare che IDSM sia in linea utilizzando il comando switch **show module** x.Assicurarsi che la versione del software IDSM sia contraddistinta dal numero 2 all'inizio, a indicare che il software della partizione di manutenzione è in esecuzione su IDSM e che lo stato sia 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. Connettersi alla partizione di manutenzione IDSM utilizzando il comando switch **session slot *x* processor 1**.Usare il nome utente/password di **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. Installare l'immagine memorizzata nella cache per ricreare l'immagine della partizione applicativa IDSM.Utilizzare il comando di diagnostica **ids-installer system /cache /show** per verificare che l'immagine memorizzata nella cache esista.

```
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)#
```

   Se non esiste alcuna immagine memorizzata nella cache o se la versione memorizzata nella cache non è quella che si desidera installare, andare al passaggio 5.Per ricreare l'immagine ISDM utilizzando l'immagine memorizzata nella cache, utilizzare il comando di diagnostica **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:\!
```

   Una volta completata la ricreazione dell'immagine, andare al punto 12.

5. Accertatevi che IDSM disponga di connettività IP. Eseguire il comando **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. Se IDSM dispone di connettività IP, procedere con il passaggio 11. Se non si dispone di connettività IP, procedere con i passaggi da 7 a 9.
7. Verificare che l'interfaccia di comando e controllo sia configurata correttamente sullo switch. Eseguire il comando **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. Verificare che i parametri di comunicazione siano configurati correttamente nella partizione di manutenzione IDSM. Eseguire il comando di diagnostica **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. Se nessuno dei parametri è impostato o se è necessario modificarne alcuni, utilizzare il comando di diagnostica **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. Controllare nuovamente la connettività IP dopo aver reimpostato l'IDSM per rendere effettive le modifiche. Se il problema persiste, risolvere il problema come per un normale problema di connettività IP, quindi procedere con il passaggio 11.
11. Ricreare l'immagine della partizione dell'applicazione IDSM. Scaricare l'immagine utilizzando il comando di diagnostica ids-installer system /nw /install /server=*indirizzo_ip /user=account* ***/save={****yes/no****} /dir=****percorso_ftp* ***/prefix=****prefisso_file* dove:*ip_address* è l'indirizzo IP del server FTP.*account* è il nome utente o account da utilizzare per accedere al server FTP.*salva* determina se salvare una copia dell'immagine scaricata come copia memorizzata nella cache. In caso affermativo, qualsiasi immagine memorizzata nella cache esistente viene sovrascritta. Se no, l'immagine scaricata viene installata nella partizione inattiva ma non viene salvata una copia memorizzata nella cache.*ftp_path* specifica la directory sul server FTP in cui si trovano i file immagine.*prefisso_file* è il nome del file .dat nell'immagine scaricata. L'immagine scaricata è costituita da un file con estensione .dat e da diversi file con estensione .cab. Il valore file_prefix deve essere il nome del file DAT, ma non il suffisso .dat.

```
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. Avviare IDSM nella partizione dell'applicazione utilizzando il comando switch **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!--- Output is suppressed.
```

Verificare inoltre che lo switch sia configurato per avviare IDSM nella partizione dell'applicazione. Per verificare questa condizione, usare il comando **show bootvar device module *x***.

```
SV9-1#show bootvar device module 6
```

```
[mod:6 ]:
SV9-1#
```

Per configurare la variabile del dispositivo di avvio per IDSM, usare il comando di configurazione dello switch **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. Verificare che IDSM sia in linea utilizzando il comando switch **show module** x.Verificare che la versione del software IDSM sia una versione della partizione dell'applicazione, ad esempio *3.0(1)S4*, e che lo stato sia 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. Connettersi a IDSM dopo l'avvio nella partizione dell'applicazione e configurarla in modo che possa comunicare con il director. Utilizzare il comando **setup**.Una volta stabilita la comunicazione con il director, è possibile scaricare la configurazione nell'IDSM.Per accedere, usare il nome utente/password **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: 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.
```

Nuova immagine di IDSM con switch con codice ibrido (CatOS)

Completare questa procedura per ricreare un'immagine ISDM con uno switch con codice ibrido (CatOS).

Nota: tutte le informazioni vengono perse nella partizione dell'applicazione. Non è possibile utilizzare alcun metodo per eseguire un recupero della password sull'IDSM mentre si mantiene la configurazione.

Nota: questa procedura richiede l'utilizzo della partizione di manutenzione. Se la password della partizione di manutenzione è stata modificata e non è possibile eseguire l'accesso, è necessario sostituire IDSM. In questo caso, contattare il supporto tecnico Cisco per assistenza.

1. Avviare IDSM nella partizione di manutenzione con il comando **reset** switch *x* ***hdd:2***.

```
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. Verificare che IDSM sia in linea con il comando switch **show module** x.Assicurarsi che la versione del software IDSM sia contraddistinta dal numero 2 all'inizio, a indicare che il software della partizione di manutenzione è in esecuzione su IDSM e che lo stato sia 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. Connettersi a IDSM dopo l'avvio nella partizione di manutenzione con il comando switch **session**x.Usare il nome utente/password di **ciscoids/attack**.

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

4. Installare l'immagine memorizzata nella cache per ricreare l'immagine della partizione applicativa IDSM.Verificare che l'immagine memorizzata nella cache esista usando il comando di diagnostica **ids-installer system /cache /show**.

```
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)#
```

Se non esiste alcuna immagine memorizzata nella cache o se la versione memorizzata nella cache non è quella che si desidera installare, andare al passaggio 5.Per ricreare un'immagine dell'ISDM che utilizza l'immagine memorizzata nella cache, utilizzare il comando di diagnostica **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:\!
```

Una volta completata la ricreazione dell'immagine, andare al punto 12.

5. Verificare che IDSM disponga di connettività IP con il comando **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. Se IDSM dispone di connettività IP, procedere con il passaggio 11. Se non si dispone di connettività IP, procedere con i passaggi da 7 a 9.
7. Verificare che l'interfaccia di comando e controllo sia configurata correttamente sullo switch con il comando **show port status *x*/2**.

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

8. Verificare che i parametri di comunicazione siano configurati correttamente nella partizione di manutenzione IDSM con il comando di diagnostica **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. Se nessuno dei parametri è impostato o se è necessario modificarne alcuni, utilizzare il comando di diagnostica **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. Controllare nuovamente la connettività IP dopo aver reimpostato l'IDSM per rendere effettive le modifiche.Se il problema persiste, risolvere il problema come per un normale problema di connettività IP, quindi procedere con il passaggio 11.
11. Ricreare l'immagine della partizione dell'applicazione IDSM. Scaricare l'immagine con il comando di diagnostica **ids-installer system /nw /install /server=*indirizzo_ip* /user=account /save={*yes/no*} /dir=*percorso_ftp* /prefix=*prefisso_file*** dove:*ip_address* è l'indirizzo IP del server FTP.*account* è il nome utente o account da utilizzare per accedere al server FTP.*salva* determina se salvare una copia dell'immagine scaricata come copia memorizzata nella cache. In caso affermativo, qualsiasi immagine memorizzata nella cache esistente viene sovrascritta. Se no, l'immagine scaricata viene installata nella partizione inattiva ma non viene salvata una copia memorizzata nella cache.*ftp_path* specifica la directory sul server FTP in cui si trovano i file immagine.*prefisso_file* è il nome del file .dat nell'immagine scaricata. L'immagine scaricata è costituita da un file con estensione .dat e da diversi file con estensione .cab. Il valore file_prefix deve essere il nome del file DAT, escluso il suffisso .dat.

```
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. Avviare IDSM nella partizione dell'applicazione con il comando **reset** switch *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.
```

Verificare inoltre che lo switch sia configurato per avviare IDSM nella partizione dell'applicazione. Per controllare questa condizione, usare il comando **show boot device *x***.

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

Per configurare la variabile del dispositivo di avvio per IDSM, usare il comando di configurazione dello switch **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. Verificare che IDSM sia in linea con il comando switch **show module *x***.Verificare che la versione del software IDSM sia una versione della partizione dell'applicazione, ad esempio *3.0(1)S4*, e che lo stato sia 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. Connettersi a IDSM dopo l'avvio nella partizione dell'applicazione e configurarla in modo che possa comunicare con il director. Utilizzare il comando **setup**.Eseguire il login con il nome utente/password di **ciscoids/attack**.

```
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

Procedura di ripristino se il nome utente/password dell'amministratore è noto

Se è nota una password per un account amministratore, è possibile utilizzare questo account utente per reimpostare altre password utente.

Ad esempio, in IDSM-2 sono configurati due nomi utente denominati 'cisco' e 'adminuser'. È necessario reimpostare la password dell'utente 'cisco', quindi 'adminuser' esegue l'accesso e reimposta la password.

```
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#
```

Procedura di ripristino se il nome utente/password del servizio è noto

Se è nota una password per l'account del servizio, è possibile utilizzare questo account utente per reimpostare altre password utente.

Ad esempio, in IDSM-2 sono configurati tre nomi utente denominati 'cisco', 'adminuser' e 'serviceuser'. È necessario reimpostare la password dell'utente 'cisco', quindi 'serviceuser' esegue l'accesso e reimposta la password.

```
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#
```

Nota: la password di root è la stessa dell'account del servizio.

Ricreare l'immagine di IDSM-2 con uno switch con codice IOS (IOS integrato) nativo

Completare questa procedura per ricreare l'immagine di ISDM-2 con uno switch con codice IOS nativo (Integrated IOS).

Nota: tutte le informazioni vengono perse nella partizione dell'applicazione. Non è possibile utilizzare alcun metodo per eseguire un recupero della password su IDSM-2 mentre la configurazione viene mantenuta.

1. Avviare IDSM-2 nella partizione di manutenzione con il comando **hw-module module module *x* reset cf:1** in cui *x* indica il numero di slot e cf indica 'compact flash'.**Nota:** se si verifica un problema utilizzando cf:1, provare a utilizzare hdd:2 come alternativa.

```
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. Verificare che IDSM-2 sia in linea con il comando switch **show module *x***.Accertarsi che alla fine della versione del software IDSM-2 sia presente l'indicazione 'm' e che lo stato sia 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. Connettersi a IDSM-2 dopo l'avvio nella partizione di manutenzione. Usare il comando switch **session slot xprocessor 1**.Utilizzare il nome utente/la password di **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. Assicurarsi che IDSM-2 disponga di connettività IP. Usare il comando **ping** *indirizzo_ip*.

```
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. Se IDSM-2 dispone di connettività IP, passare al punto 14.
6. Verificare che l'interfaccia di comando e controllo sia configurata correttamente sullo switch. Utilizzare il comando **show run | incl. rilevamento intrusioni**.

```
SV9-1#show run | inc intrusion-detection
intrusion-detection module 6 management-port access-vlan 210
```

7. Verificare che i parametri di comunicazione siano configurati correttamente nella partizione di manutenzione IDSM-2. Usare il comando **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. Se nessuno dei parametri è impostato o se è necessario modificarne alcuni, deselezionarli tutti. Usare il comando **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. Configurare l'indirizzo IP e le informazioni sulla maschera nella partizione di manutenzione IDSM-2. Usare il comando **ip address *ip_address netmask***.

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

10. Configurare il gateway predefinito nella partizione di manutenzione IDSM-2. Usare il comando **ip gateway *gateway-address***.

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

11. Configurare il nome host nella partizione di manutenzione IDSM-2. Usare il comando **ip host *hostname***.Anche se non è necessario, aiuta a identificare il dispositivo, in quanto imposta anche la richiesta.

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

12. Potrebbe essere necessario configurare l'indirizzo di broadcast in modo esplicito. Usare il comando **ip broadcast *address***.L'impostazione predefinita in genere è sufficiente.

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

13. Controllare nuovamente la connettività IP. Se il problema persiste, risolvere il problema come per un normale problema di connettività IP e procedere con il passaggio 14.
14. Ricreare l'immagine della partizione applicativa IDSM-2. Usare il comando **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. Avviare IDSM-2 nella partizione dell'applicazione. Usare il comando switch **hw-module 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.
```

In alternativa, è possibile utilizzare il comando **reset** su IDSM-2 se la variabile del dispositivo di avvio è impostata correttamente.Per controllare le impostazioni delle variabili del dispositivo di avvio per IDSM-2, usare il comando switch **show bootvar device module** x.

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

Per configurare la variabile del dispositivo di avvio per IDSM-2, usare il comando di configurazione dello switch **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
```

Per ripristinare IDSM-2 tramite la CLI delle informazioni di manutenzione, usare il comando **reset**.

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

16. Verificare che IDSM-2 sia in linea. Usare il comando switch **show module *x***.Accertarsi che la versione del software IDSM-2 sia una versione della partizione dell'applicazione, ad esempio *4.1(1)S47* e che lo stato sia 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. Connettersi a IDSM-2 dopo l'avvio nella partizione dell'applicazione. Usare il comando switch **session slot *x* processor 1**.Utilizzare il nome utente/password di **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. Configurare IDSM-2. Utilizzare il comando **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#
```

Nuova immagine per IDSM-2 con switch con codice ibrido (CatOS)

Completare questa procedura per ricreare un'immagine dell'ISDM-2 con uno switch con codice ibrido (CatOS).

1. Avviare IDSM-2 nella partizione di manutenzione. Usare il comando switch **reset *x* hdd:2**.**Nota:** se si verifica un problema utilizzando hdd:2, provare a utilizzare cf:1 come alternativa.

```
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. Verificare che IDSM-2 sia in linea. Usare il comando switch **show module *x***.Verificare che la versione del software IDSM-2 sia contrassegnata dalla lettera 'm' che indica che il software della partizione di manutenzione è in esecuzione e che lo stato sia 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. Connettersi a IDSM-2 dopo l'avvio nella partizione di manutenzione. Usare il comando switch **session *x*** .Utilizzare il nome utente/la password di **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. Assicurarsi che IDSM-2 disponga di connettività IP. Usare il comando **ping** *indirizzo_ip*.

```
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. Se IDSM-2 dispone di connettività IP, passare al punto 14.
6. Verificare che l'interfaccia di comando e controllo sia configurata correttamente sullo switch. Usare il comando **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. Verificare che i parametri di comunicazione siano configurati correttamente nella partizione di manutenzione IDSM-2. Usare il comando **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. Se nessuno dei parametri è impostato o se è necessario modificarne alcuni, cancellarli tutti con il comando **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
```

9. Configurare l'indirizzo IP e le informazioni sulla maschera nella partizione di manutenzione IDSM-2. Usare il comando **ip address** *ip_address netmask*.

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

10. Configurare il gateway predefinito nella partizione di manutenzione IDSM-2. Usare il comando **ip gateway** *gateway-address*.

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

11. Configurare il nome host nella partizione di manutenzione IDSM-2. Usare il comando **ip host** *hostname*.Anche se non è necessario, aiuta a identificare il dispositivo in quanto imposta anche il prompt.

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

12. Potrebbe essere necessario configurare l'indirizzo di broadcast in modo esplicito. Usare il comando **ip broadcast *address***.L'impostazione predefinita in genere è sufficiente.
```
guest@idsm2-sv-rack.localdomain#ip broadcast 10.66.79.223
```

13. Controllare nuovamente la connettività IP. Se il problema persiste, risolvere il problema seguendo la procedura descritta al punto 14.
14. Ricreare l'immagine della partizione applicativa IDSM-2. Usare il comando **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. Avviare IDSM-2 nella partizione dell'applicazione. Usare il comando switch **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.
```
In alternativa, è possibile utilizzare il comando **reset** su IDSM-2 se la variabile del dispositivo di avvio è impostata correttamente.Per controllare le impostazioni delle variabili del dispositivo di avvio per IDSM-2, usare il comando switch **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
```
Per configurare la variabile del dispositivo di avvio per IDSM-2, usare il comando di configurazione dello switch **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
```
Per ripristinare IDSM-2 tramite la CLI della partizione di manutenzione, usare il comando **reset**.
```
guest@idsm2-sv-rack.localdomain#reset
!--- Output is suppressed.
```
16. Verificare che IDSM-2 sia in linea. Usare il comando switch **show module *x***.Accertarsi che la versione del software IDSM-2 sia una versione della partizione dell'applicazione, ad esempio *4.1(1)S47,* e che lo stato sia 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. Connettersi a IDSM-2 dopo l'avvio nella partizione dell'applicazione. Usare il comando switch **session**x .Utilizzare il nome utente/password di **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. Configurare IDSM-2 con il comando **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
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#
```

Informazioni correlate

- Cisco IDS UNIX Director
- Catalyst serie 6500 Intrusion Detection System (IDSM-1) Services Module
- Catalyst serie 6500 Intrusion Detection System (IDSM-2) Services Module
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems