Wachtwoordherstelprocedure voor Cisco IDS-sensor en IDS-servicesmodules (IDSM-1, IDSM-2)

Inhoud

Inleiding

Dit document bevat procedures voor het herstellen van uw Cisco Secure Inbraakdetectiesysteem (IDS) (voorheen NetRanger) en de modules voor alle versies.

Voorwaarden

Vereisten

Als een FTP-server nodig is, moet deze passieve modus ondersteunen. Cd's voor herstel kunnen worden verkregen met behulp van het product upgrade-programma (alleen geregistreerde klanten).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- IDS-applicatie versies 3 en 4
- IPS-applicaties versie 5 en 6
- IDS-module (IDSM) versie 3 en IDSM-2 versie 4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

IDS-applicatie versie 3

Er zijn twee opties beschikbaar voor het apparaat, versie 3. U kunt het wachtwoordherstelproces gebruiken of u kunt een nieuwe afbeelding maken op basis van de cd met versie 3. Merk op dat alle informatie op een herafbeelding verloren is. De wachtwoordherstelprocedure is in wezen een herstel van het wachtwoord door Solaris. Gebruik deze optie alleen als u geen beheerstation (Cisco Secure Policy Manager (CSPM), VPN/Security Management Solutions (VMS) en UNIX Director) hebt waaruit u de configuratie kunt kopiëren.

Bij IDS-applicatie versie 3 en hoger bestaan er twee gebruikersnamen, 'netwerk' en 'wortel' genaamd. Het defaultwachtwoord voor beide is 'aanval'.

Wachtwoordherstel van IDS-applicatie die versie 3 uitvoert

Deze bestanden zijn nodig om uw wachtwoord te kunnen herstellen.

- Solaris Devices Configuration Assistant-schijf (laarsschijf). U kunt de bestanden downloaden van de website voor ondersteuning van de zon .**Opmerking:** Als deze link niet werkt, probeer dan naar het bovenste niveau van de Sun-ondersteuningswebsite te gaan en zoek dan naar *Apparaatconfiguratie Assistant voor Opstarten Diskette Solaris driver Downloads* onder Drivers. Cisco Systems, Inc. behoudt de Sun Support website niet en heeft geen controle over de locatie van de inhoud.
- Solaris voor Intel (x86) CD-ROM.
- Console toegang tot het werkstation.

Voltooi deze stappen om het wachtwoord te herstellen.

1. Plaats de laarsschijf.
2. Plaats de CD in het CD-ROM station.
3. Schakel het werkstation uit, wacht tien seconden en schakel de functie in.Het systeem start

vanaf de laarsschijf. Na enige configuratie, toont het eerste scherm van Configuration Assistant.

4. Druk op **F3** om een partiële scan van het systeem te maken voor laars.Wanneer de scan is voltooid, wordt er een lijst met apparaten weergegeven.
5. Zorg ervoor dat het CD-ROM apparaat in de lijst met apparaten voorkomt en druk vervolgens op **F2** om verder te gaan.Een scherm toont een lijst van laars apparaten.
6. Selecteer het **CD-ROM** station en druk vervolgens op de spatiebalk.Er zit een 'X' naast het CD-ROM apparaat.
7. Druk op **F2** om verder te gaanHet werkstation start nu vanaf de CD-ROM.
8. Kies **optie 2, Jumpstart** op het scherm dat wordt gebruikt om een type installatie te selecteren.Het systeem blijft opstarten.
9. Kies **optie 0** voor het Engels als u een taal wilt selecteren.
10. Kies op het volgende scherm voor talen opnieuw **optie 0** voor Engels ANSI.Het systeem blijft opstarten en het installatiescherm van Solaris verschijnt.
11. Houd de **Control**-toets en type **C** ingedrukt om het installatiescript te stoppen en u toegang te geven tot de melding.
12. Type **montage -F ufs /dev/dsk/c0t0d0s0/mnt.**De '/' verdeling is nu gemonteerd op het '/ mnt' steunpunt. Hier kunt u het '/etc/schaduwbestand bewerken en het hoofdwachtwoord verwijderen.
13. Type **cd /mnt/enz**.
14. Stel de shell omgeving in zodat u de gegevens correct kunt lezen.Type **TERM=ansi**.Type **uitvoerTERM**.
15. Type **vi schaduw**.U bevindt zich nu in het schaduwbestand en kunt het wachtwoord verwijderen. De vermelding moet:

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

    ":" is een veldscheidingsteken en het gecodeerde wachtwoord is het tweede veld.
16. Verwijdert het tweede veld. Bijvoorbeeld:
    `root:gNyqp8ohdfxPI:10598::::::`
    wordt gewijzigd in

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

    Hiermee verwijdert u het wachtwoord voor de hoofdgebruiker.
17. Type **:wq!** om het bestand te schrijven en te stoppen.
18. Verwijder de schijf en de CD-ROM uit de schijf.
19. Type **init 6** om het systeem opnieuw te starten.
20. Typ bij inloggen wortel: en druk vervolgens op **ENTER**.
21. Druk op **ENTER** om het wachtwoord te vragen.U bent nu aangemeld bij de Cisco Secure IDS-sensor.

Herafbeelding van IDS-applicatie die versie 3 ondersteunt

Voltooi deze stappen om een ander beeld te geven van het IDS-applicatie waarin versie 3 is uitgevoerd.

N.B.: Zorg ervoor dat een muis niet op de sensor is aangesloten voordat u doorgaat.

1. Plaats de cd voor herstel van versie 3 in het IDS-apparaat en start het programma opnieuw op.
2. Volg de aanwijzingen op basis van uw instellingen totdat het herstel is geslaagd.
3. Aanmelden met behulp van de standaardgebruikersnaam/het wachtwoord van 'wortel/aanval'.
4. Draai **de** sysconfiguratie-**sensor** om het apparaat opnieuw in te stellen.

IDS-applicatie versie 4

Herstelprocedure als naam/wachtwoord van beheerder bekend is

Als er een wachtwoord voor een Administrator-account bekend is, kan deze gebruikersaccount worden gebruikt om andere gebruikerswachtwoorden te herstellen.

Zo worden bijvoorbeeld twee gebruikersnamen ingesteld op het IDS-applicatie 'cisco' en 'adminuser'. Het wachtwoord voor de gebruiker 'cisco' moet worden hersteld, zodat 'adminuser' zich inlogt en het wachtwoord opnieuw instelt.

```
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#
```

Herstelprocedure als de naam/het wachtwoord voor servicetoepassing bekend is

Als er een wachtwoord voor de servicerekening bekend is, kan deze gebruikersaccount worden gebruikt om andere wachtwoorden te resetten.

Zo worden er bijvoorbeeld drie gebruikersnamen ingesteld op het IDS-apparaat met de naam 'cisco', 'adminuser' en 'Service user'. Het wachtwoord voor de gebruiker 'cisco' moet worden hersteld, zodat de 'gebruiker van de service' zich inlogt en het wachtwoord opnieuw instelt.

```
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#
```

Opmerking: het hoofdwachtwoord is hetzelfde als het wachtwoord van de servicekening.

IDS-applicatie die werkt, versie 4

Voltooi deze stappen om een nieuwe afbeelding van het IDS-apparaat te maken.

N.B.: Zorg ervoor dat een muis niet op de sensor is aangesloten voordat u doorgaat.

1. Plaats de cd voor herstel van versie 4 in het IDS-apparaat en start het programma opnieuw op.
2. Volg de aanwijzingen op basis van uw instellingen totdat het herstel is geslaagd.
3. Aanmelden met behulp van de standaardgebruikersnaam/het wachtwoord voor Cisco/cisco.
4. Start **de installatie** om het apparaat opnieuw te configureren.

IPS-applicatie versie 5 en versie 6

Opnieuw laden, afsluiten, opnieuw instellen en herstellen van het AIP-SSM

Gebruik deze opdrachten om het wachtwoord te herladen, af te sluiten, te herstellen, en het wachtwoord voor geavanceerde inspectie en preventie security servicesmodule (AIP-SSM) direct te herstellen van de adaptieve security applicatie:

Opmerking: U kunt de **handmodule** opdrachten uit een bevoorrechte EXEC-modus of de globale configuratiemodus invoeren. U kunt de opdrachten in één routemodus en één transparante modus invoeren. Voor adaptieve security apparaten die in multi-mode (routed of Transparent multi-mode) werken, kunt u alleen de opdrachten **van de** hmodule vanuit de systeemcontext uitvoeren (niet vanuit een beheerder of een gebruikerscontext).

- **Hoe-module module** ***slot_number*** **herladen**-Deze opdracht herlaadt de software op het AIP-SSM zonder een hardware-reset te doen. Het is alleen effectief wanneer het AIP-SSM in de Up-status is.
- **Hoe-module module module** ***slot_number*** **shutdown**-Deze opdracht sluit de software op AIP-SSM af. Het is alleen effectief wanneer het AIP-SSM in de Up-status is.
- **Hoe-module module** ***slot_number*** **reset**-Deze opdracht voert een hardware-reset uit van AIP-SSM. Het is van toepassing wanneer de kaart zich in de Up/Down/Unresponsive/Recover staten bevindt.
- **Hoe-module module** ***slot_number*** **password-reset**-Deze opdracht herstelt een wachtwoord op een Cisco ASA 5500 Series Content Security and Control Services Module (CSC-SSM) of op AIP-SSM zonder dat u het apparaat opnieuw hoeft te image maken.**Opmerking:** deze opdracht start ondersteuning van IPS 6.0 (ASA 7.2 versie) en wordt gebruikt om het Cisco CLI-accountwachtwoord terug te zetten naar de standaard **cisco**.
- **Hoe-module module** ***sleuf_number*** **herstel [start | stop | configuratie]**—De **opdracht** herstellen geeft een aantal interactieve opties weer om de terugwinningsparameters in te stellen of te wijzigen. U kunt de parameter wijzigen of de bestaande instelling behouden wanneer u op **ENTER** drukt.Zie De afbeelding van het AIP-SSM installeren voor de procedure die u gebruikt om de AIP-SSM-software te herstellen.**Hoe-module module** ***sleuf_number*** **recovery start**-Deze opdracht initieert herstel van AIP-SSM. Het is alleen van toepassing wanneer AIP-SSM in de status Up staat is.**Hoe-module module** ***sleuf_number*** **herstellen stop**-Deze opdracht stopt met

de terugwinning van AIP-SSM. Het is alleen van toepassing wanneer het AIP-SSM zich in de herstelstaat bevindt.**Opmerking:** Als het herstel van AIP-SSM moet worden gestopt, moet u de opdracht **voor het** herstellen van **module 1** binnen 30 tot 45 seconden nadat u het herstel van AIP-SSM hebt gestart uitgeven. Als je langer wacht, kan dit onverwachte gevolgen hebben. Het AIP-SSM kan bijvoorbeeld ook optreden in de staat Unresponsief.**Hoe-module module 1 configuratie**-gebruik deze opdracht om parameters te configureren voor modulair herstel. De belangrijkste parameters zijn het IP-adres en de TFTP-URL-locatie van het herstelbeeld.Voorbeeld:

```
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]:
```

De AIP-SSM-systeemafbeelding opslaan

Voltooi deze stappen om de AIP-SSM-systeemafbeelding te installeren:

1. Meld u aan bij de ASA.
2. Geef de modus op:
   ```
   asa>enable
   ```
3. Configureer de herstelinstellingen voor de AIP-SSM:
   ```
   asa#hw-module module 1 recover configure
   ```

   Opmerking: Als u een fout maakt in de herstelconfiguratie, **gebruikt** u de opdracht **van de module 1 om de** systeemopnamen te stoppen en dan kunt u de configuratie corrigeren.
4. Specificeer de TFTP-URL voor de systeemafbeelding:
   ```
   Image URL [tftp://0.0.0.0/]:
   ```
   Voorbeeld:
   ```
   Image URL [tftp://0.0.0.0/]:
    tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img
   ```
5. Specificeer de opdracht en de besturingsinterface van AIP-SSM:
   ```
   Port IP Address [0.0.0.0]:
   ```
   Voorbeeld:
   ```
   Port IP Address [0.0.0.0]: 10.89.149.231
   ```
6. Laat de VLAN-id op 0 staan.
   ```
    VLAN ID [0]:
   ```
7. Specificeer de standaardgateway van AIP-SSM:
   ```
   Gateway IP Address [0.0.0.0] :
   ```
   Voorbeeld:
   ```
   Gateway IP Address [0.0.0.0]:10.89.149.254
   ```
8. Uitvoeren van de nuttige toepassing:
   ```
   asa#hw-module module 1 recover boot
   ```

9. Controleer de terugvordering af en toe totdat deze is voltooid:**Opmerking:** de status leest guest@localhost.localdomain# tijdens de recovery en leest guest@localhost.localdomain# wanneer de bewerking is voltooid.
   ```
   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#
```

Opmerking: Om fouten te debug die in het herstelproces kunnen optreden, gebruikt u de opdracht **Debug module-start** om het foutherstel van het systeem mogelijk te maken.

10. Sessie naar het AIP-SSM en initialiseer AIP-SSM met de **setup-**opdracht.

IDSM

Er is geen methode die u kunt gebruiken om een wachtwoord te herstellen op het IDSM terwijl de configuratie behouden blijft.

Opmerking: Deze procedure vereist het gebruik van de onderhoudsverdeling. Als het wachtwoord voor de onderhoudspartitie is gewijzigd en u niet kunt inloggen, moet IDSM worden vervangen. In dit geval neemt u contact op met Cisco Technical Support voor ondersteuning.

IDSM met een Switch opnieuw image maken dat Native IOS (Geïntegreerde IOS)-code uitvoert

Voltooi deze stappen om ISDM opnieuw te image te geven van een switch met een inheemse IOS (Geïntegreerde IOS)-code.

1. Start IDSM op de onderhoudspartitie met behulp van de opdracht **van de** switch**, hwmodule *x* reset hdd:2** waarbij *x* staat voor het nummer van de sleuf.

```
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. Controleer of IDSM online komt met behulp van de opdracht **switch**, **module *x*.**Zorg ervoor dat de IDSM-softwareversie 2 aan het begin heeft geplaatst die aangeeft dat de onderhoudsverdelingssoftware momenteel op IDSM draait en dat de status OK is.

```
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. Sluit aan op de IDSM-onderhoudspartitie door gebruik te maken van de switch **sessiesleuf *x* processor 1**.Gebruik de gebruikersnaam/het wachtwoord van **ciscoïden/aanvallen**.

```
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. Installeer de gecached afbeelding om de IDSM applicatie opnieuw te installeren.Geef het diagnostische commando **id-installatiesysteem/cache/show uit** om te controleren of het gecached beeld bestaat.

```
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)#
```

   Als er geen gecached afbeelding bestaat of de gecached versie is niet de afbeelding die u wilt installeren, gaat u naar stap 5.Gebruik het diagnostische commando **id-installatiesysteem /cachecache /-installeren** om de ISDM met behulp **van** de gecached afbeelding opnieuw te **image te** maken.

```
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:\!
```

   Ga verder naar stap 12 als de herafbeelding is voltooid.

5. Zorg ervoor dat IDSM IP connectiviteit heeft. Geef de opdracht uit **ping *ip_adres*.**

```
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. Als IDSM IP connectiviteit heeft, ga naar stap 11. Als u geen IP connectiviteit hebt, ga met stap 7 door 9 te werk.
7. Zorg ervoor dat de Opdracht en Control Interface goed op de switch is ingesteld. Geef de opdracht **show run interface Gigx/2 uit**.

```
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. Zorg ervoor dat de communicatieparameters goed zijn ingesteld op de onderhoudspartitie van IDSM. Geef de diagnostische opdracht **ids-installatieprogramma's/weergave uit**.

```
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. Als geen van de parameters wordt ingesteld, of als sommige ervan moeten worden gewijzigd, gebruik de diagnostische opdracht **ids-installatieprogramma/configuratie *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. Controleer IP-connectiviteit opnieuw nadat u de IDSM hebt hersteld om de wijzigingen in werking te stellen. Als IP-connectiviteit nog steeds een probleem is, is het oplossen van problemen zoals bij een normaal IP-aansluitingsprobleem, dan ga je met stap 11 verder.
11. Afbeelding van de IDSM-toepassingspartitie. Download het beeld met het diagnostische commando **ids-installatiesysteem /nw /install /server=*ip_address* /user=*account* /save={*yes/no*} /dir=*ftp_path* /prefix waar:***ip_adres*** is het IP adres van de FTP server.***De account*** is de gebruiker of de naam van de account die moet worden gebruikt bij het registreren in de FTP-server.***op te slaan*** bepaalt of u een kopie van de gedownload afbeelding als de gecached kopie wilt opslaan . Als ja, wordt een gecached afbeelding die bestaat overschreven. Als nee, de gedownload afbeelding is geïnstalleerd op de inactieve partitie, maar er wordt geen gecached kopie opgeslagen.***ftp_path*** specificeert de folder op de FTP server waar de beeldbestanden zich bevinden.***file_prefix*** is de bestandsnaam van het .dat bestand in de gedownload afbeelding. Het gedownload beeld bestaat uit één bestand met de .dat extensie en verschillende bestanden met de .cab extensie. De waarde file_prefix moet de naam van het DAT bestand zijn, tot maar niet het .dat suffix.

```
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. Start IDSM op de Application Partitie met behulp van de switch opdracht **hw-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.
```

Zorg er ook voor dat de switch is geconfigureerd om het IDSM op te starten in de toepassingsindeling. Om dit te controleren, gebruik de commando **show bootvar apparaatmodule *x*.**

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

Gebruik de **laarsapparaatmodule x hdd:1** om de variabele voor de IDSM-switch te configureren.

```
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. Controleer of IDSM online komt met behulp van de opdracht **switch**, **module *x*.**Zorg ervoor dat de IDSM-softwareversie een applicatie-versie is, bijvoorbeeld *3.0(1)S4*, en dat de status OK is.

```
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. Sluit aan op het IDSM nu het is opgestart in de applicatie en configureer het vervolgens zodat het naar de regisseur kan communiceren. Gebruik de **opdrachtinstellingen**.Zodra de communicatie met de regisseur tot stand is gebracht kan de configuratie worden gedownload naar het IDSM.Gebruik de gebruikersnaam/het wachtwoord van **ciscoïden/aanvallen** om in te loggen.

```
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.
```

IDSM opnieuw configureren met een Switch die Hybrid (CatOS) codering uitvoert

Voltooi deze stappen om ISDM opnieuw te starten met een switch met een hybride (CatOS) code.

Opmerking: alle informatie is verloren op de applicatie. Er is geen methode die u kunt gebruiken om een wachtwoord te herstellen op het IDSM terwijl u de configuratie behoudt.

Opmerking: Deze procedure vereist het gebruik van de onderhoudsverdeling. Als het wachtwoord voor de onderhoudspartitie is gewijzigd en u niet kunt inloggen, moet IDSM worden vervangen. In dit geval neemt u contact op met Cisco Technical Support voor ondersteuning.

1. Start IDSM op de onderhoudspartitie met de opdracht switch **reset *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. Controleer of IDSM online komt met de opdracht van de switch **module *x*.**Zorg ervoor dat de IDSM-softwareversie 2 aan het begin heeft geplaatst die aangeeft dat de onderhoudsverdelingssoftware momenteel op IDSM draait en dat de status OK is.

```
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. Sluit aan op het IDSM nu deze is opgestart in de onderhoudspartitie met de switch **sessie *x*.**Gebruik de gebruikersnaam/het wachtwoord van **ciscoïden/aanvallen**.

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

4. Installeer de gecached afbeelding om de IDSM applicatie opnieuw te installeren.Controleer dat het gecached beeld bestaat met het gebruik van de diagnostische opdracht **id-installateur systeem /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)#
```

Als er geen gecached afbeelding bestaat, of de gecached versie is niet de afbeelding die u wilt installeren, gaat u naar stap 5.Om de ISDM die het gecached beeld gebruikt opnieuw te image te maken, gebruikt u het diagnostische commando **id-installateur systeem /cache /installatie**.

```
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:\!
```

Nadat het beeld is voltooid, gaat u naar stap 12.

5. Zorg ervoor dat IDSM IP connectiviteit heeft met het gebruik van het bevel **pingelt *ip_adres*.**

```
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. Als IDSM IP connectiviteit heeft, ga naar stap 11. Als u geen IP connectiviteit hebt, ga met stap 7 door 9 te werk.
7. Zorg ervoor dat de Opdracht en Control Interface goed op de switch is geconfigureerd met behulp van de opdracht **poortstatus *x*/2 tonen**.

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

8. Zorg ervoor dat de communicatieparameters goed zijn geconfigureerd op de IDSM-onderhoudspartitie met het gebruik van de diagnostische opdracht **id-installateur netfig/weergave**.

```
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. Als geen van de parameters wordt ingesteld, of als sommige ervan moeten worden gewijzigd, gebruik de diagnostische opdracht **ids-installatieprogramma/configuratie *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. Controleer IP Connectivity opnieuw nadat u de IDSM opnieuw hebt ingesteld om de wijzigingen door te voeren.Als IP-connectiviteit nog steeds een probleem is, is het oplossen van problemen zoals bij een normaal IP-aansluitingsprobleem, dan ga je met stap 11 verder.
11. Afbeelding van de IDSM-toepassingspartitie. Download het beeld met het gebruik van het diagnostische commando **ids-installatiesysteem /nw /install/server=*ip_address* /user=account /save= {*yes/no*} /dir=*ftp_path* /prefix=*file_prefix* waar:***ip_adres*** is het IP adres van de FTP server.*De account* is de gebruiker of de naam van de account die moet worden gebruikt bij het registreren in de FTP-server.*op te slaan* bepaalt of u een kopie van de gedownload afbeelding als de gecached kopie wilt opslaan . Als ja, wordt een bestaande gecached afbeelding overschreven. Als nee, de gedownload afbeelding is geïnstalleerd op de inactieve partitie, maar er wordt geen gecached kopie opgeslagen.*ftp_path* specificeert de folder op de FTP server waar de beeldbestanden zich bevinden.*file_prefix* is de bestandsnaam van het .dat bestand in de gedownload afbeelding. Het gedownload beeld bestaat uit één bestand met de .dat extensie en verschillende bestanden met de .cab extensie. De waarde file_prefix zou de naam van het DAT bestand moeten zijn, tot maar

niet het .dat suffix.

```
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. Start IDSM op de Application Partition met behulp van de switch-opdracht **reset *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.
```

Zorg er ook voor dat de switch is geconfigureerd om het IDSM op te starten in de toepassingsindeling. IEgebruik de opdracht **om de laars *x* te tonen** om dit te controleren.

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

Om de variabele van het laarsapparaat voor IDSM te configureren gebruikt u de opdracht voor het configureren van de switch **om het laarsapparaat hdd:1 *x* in te stellen**.

```
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. Controleer of IDSM met het gebruik van de switch opdracht**module *x*** online komt.Zorg ervoor dat de IDSM-softwareversie een applicatie-versie is, bijvoorbeeld *3.0(1)S4*, en dat de status OK is.

```
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. Sluit aan op het IDSM nu het is opgestart in de applicatie en configureer het vervolgens zodat het naar de regisseur kan communiceren. Gebruik de **opdrachtinstellingen**.Aanmelden met de gebruikersnaam/het wachtwoord van **ciscoïden/aanvallen**.

```
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

Herstelprocedure als naam/wachtwoord van beheerder bekend is

Als er een wachtwoord voor een Administrator-account bekend is, kan deze gebruikersaccount worden gebruikt om andere gebruikerswachtwoorden te herstellen.

Bijvoorbeeld, twee gebruikersnamen worden gevormd op IDSM-2 genoemd "cisco" en "adminuser". Het wachtwoord voor de gebruiker 'cisco' moet worden hersteld, zodat 'adminuser' zich inlogt en het wachtwoord opnieuw instelt.

```
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#
```

Herstelprocedure als de naam/het wachtwoord voor servicetoepassing bekend is

Als er een wachtwoord voor de servicerekening bekend is, kan deze gebruikersaccount worden gebruikt om andere wachtwoorden te resetten.

Zo worden er bijvoorbeeld drie gebruikersnamen ingesteld op IDSM-2 met de naam 'cisco', 'adminuser' en 'Service user'. Het wachtwoord voor de gebruiker 'cisco' moet worden hersteld, zodat de 'gebruiker van de service' zich inlogt en het wachtwoord opnieuw instelt.

```
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#
```

Opmerking: het hoofdwachtwoord is hetzelfde als het wachtwoord van de servicerekening.

IDSM-2 opnieuw image maken van Switch die Native IOS (Geïntegreerde IOS)-code uitvoert

Voltooi deze stappen om ISDM-2 opnieuw te starten met een switch die Native IOS (Geïntegreerde IOS)-code draait.

Opmerking: alle informatie is verloren op de applicatie. Er is geen methode die u kunt gebruiken om een wachtwoord op IDSM-2 te herstellen terwijl de configuratie behouden blijft.

1. Start IDSM-2 op de onderhoudspartitie met behulp van de switch-opdracht **hw-module module *x* reset cf:1** waarbij *x* staat voor het nummer van de sleuf en cf staat voor 'compacte flitser'.**Opmerking:** Als er een probleem is dat u kunt tegenkomen met cf:1, probeer dan hdd:2 als alternatief te gebruiken.

```
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. Controleer of de IDSM-2 met het gebruik van de switch opdracht **show module *x*** online komt.Zorg ervoor dat de IDSM-2 softwareversie 'm' aan het eind heeft en dat de status OK is.

```
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. Sluit aan op de IDSM-2 nu deze is opgestart in de onderhoudspartitie. Gebruik de switch opdracht**sessiessleuf xprocessor 1**.Gebruik de gebruikersnaam/het wachtwoord van de

gast/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. Zorg ervoor dat IDSM-2 IP-connectiviteit heeft. Gebruik de opdracht ping *ip_adres*.

```
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. Als de IDSM-2 IP-connectiviteit heeft, ga dan naar stap 14.
6. Zorg ervoor dat de Opdracht en Control Interface goed op de switch is ingesteld. Gebruik de opdrachtregel tonen run | Inc-inbraakdetectie.

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

7. Zorg ervoor dat de communicatieparameters goed zijn geconfigureerd op de onderhoudspartitie van IDSM-2. Gebruik de opdracht om ip weer te geven.

```
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. Als geen van de parameters is ingesteld of als een aantal ervan moet worden gewijzigd, moet u alle parameters wissen. Gebruik de opdracht op 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. Configureer het IP-adres en maskerinformatie over de IDSM-2 onderhoudspartitie. Gebruik het commando ip adres *ip_address netmask*.

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

10. Configureer de standaardgateway op de IDSM-2 onderhoudspartitie. Gebruik het commando ip *gateway-adres*.

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

11. Configureer de hostname op de IDSM-2 onderhoudspartitie. Gebruik de opdracht ip host *hostname*.Alhoewel dit niet nodig is, helpt het het apparaat te identificeren aangezien dit ook de prompt bepaalt.

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

12. Mogelijk moet u uw omroepadres expliciet configureren. Gebruik het commando **ip *uitzending-adres***.De standaardinstelling is meestal voldoende.
```
guest@idsm2-sv-rack.localdomain#ip broadcast 10.66.79.223
```

13. Controleer de IP-connectiviteit opnieuw. Als IP-connectiviteit nog steeds een probleem is, kan u problemen oplossen zoals bij een normaal IP-aansluitingsprobleem en gaat u met stap 14 verder.
14. Herafbeelding van de IDSM-2 applicatie. Gebruik de **opdrachtupgrade *ftp-url* —installeer**.
```
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. Start de IDSM-2 op de applicatie. Gebruik de opdracht switch **hoe 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 plaats hiervan kunt u de opdracht **reset** gebruiken op de IDSM-2 zolang de variabele op het beginapparaat correct is ingesteld.Om de instelling van de variabele voor de laarsmachine voor de IDSM-2 te controleren, gebruikt u de opdracht switch **om bootvar apparaatmodule *x* te tonen**.
```
SV9-1#show bootvar device module 6
[mod:6 ]:
SV9-1#
```
Gebruik de **laarsmachine-module *x* hdd:1** om de variabele voor de IDSM-2 **te** configureren.
```
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
```
Gebruik de opdracht **resetten** om IDSM-2 te resetten via de onderhoudspartitie CLI.
```
guest@idsm2-sv-rack.localdomain#reset
!--- Output is suppressed.
```

16. Controleer of de IDSM-2 online komt. Gebruik de opdracht switch **tonen module *x*.**Zorg ervoor dat de IDSM-2-softwareversie een applicatie-versie is, bijvoorbeeld *4.1(1)S47* en dat de status OK is.

```
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. Sluit aan op de IDSM-2 nu deze is opgestart in de toepassingsverdeling. Gebruik de switch opdracht **sessie sleuf *x* processor 1**.Gebruik de gebruikersnaam/het wachtwoord van **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. Configureer de IDSM-2. Gebruik de **opdrachtinstellingen**.

```
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#
```

Herafbeelding voor IDSM-2 met Switch met Hybrid (CatOS)-code

Voltooi deze stappen om ISDM-2 een andere afbeelding te geven met een switch met de hybride (CatOS) code.

1. Start de IDSM-2 in de onderhoudspartitie. Gebruik de opdracht switch **reset *x* hdd:2**.**Opmerking:** Als er een probleem is dat u kunt oplossen met hdd:2, probeer dan cf:1 als alternatief te gebruiken.

```
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. Controleer of de IDSM-2 online komt. Gebruik de opdracht switch **tonen module *x***.Zorg ervoor dat de IDSM-2 softwareversie 'm' op het einde heeft geplaatst dat aangeeft dat de software voor de onderhoudspartitie momenteel draait en dat de status OK is.

```
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. Sluit aan op de IDSM-2 nu deze is opgestart in de onderhoudspartitie. Gebruik de opdrachtsessie van de switch *x*.Gebruik de gebruikersnaam/het wachtwoord van de **gast/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. Zorg ervoor dat IDSM-2 IP-connectiviteit heeft. Gebruik de opdracht **ping *ip_adres*.**

```
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. Als de IDSM-2 IP-connectiviteit heeft, ga dan naar stap 14.
6. Zorg ervoor dat de Opdracht en Control Interface goed op de switch is ingesteld. Gebruik de opdracht **om poortstatus *x*/2 weer te geven**.

```
SV9-1> (enable)show port status 6/2
Port  Name                 Status     Vlan       Duplex Speed Type
----- -------------------- ---------- ---------- ------ ----- ------------
 6/2                       connected  210          full  1000 Intrusion De
```

7. Zorg ervoor dat de communicatieparameters goed zijn geconfigureerd op de onderhoudspartitie van IDSM-2. Gebruik de opdracht **om ip weer te geven**.

```
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. Als geen van de parameters wordt ingesteld of als sommige ervan moeten worden gewijzigd, wis ze allemaal met behulp van de opdracht **helder 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. Configureer het IP-adres en maskerinformatie over de IDSM-2 onderhoudspartitie. Gebruik het commando **ip adres *ip_address netmask*.**

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

10. Configureer de standaardgateway op de IDSM-2 onderhoudspartitie. Gebruik de commando **ip *gateway-adres***.
```
guest@localhost.localdomain#ip gateway 10.66.79.193
guest@localhost.localdomain#
```
11. Configureer de hostname op de IDSM-2 onderhoudspartitie. Gebruik de opdracht **ip host *hostname***.Alhoewel dit niet nodig is, helpt het het apparaat te identificeren aangezien dit ook de prompt instelt.
```
guest@localhost.localdomain#ip host idsm2-sv-rack
guest@idsm2-sv-rack.localdomain#
```
12. Mogelijk moet u uw omroepadres expliciet configureren. Gebruik het commando **ip *uitzending-adres***.De standaardinstelling is meestal voldoende.
```
guest@idsm2-sv-rack.localdomain#ip broadcast 10.66.79.223
```

13. Controleer IP-connectiviteit opnieuw. Als IP-connectiviteit nog steeds een probleem is, is het oplossen van problemen zoals per een normaal IP-aansluitingsprobleem dan met stap 14 te werk gaan.
14. Herafbeelding van de IDSM-2 applicatie. Gebruik de **opdrachtupgrade *ftp-url* —installeer**.
```
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. Start de IDSM-2 op de applicatie. Gebruik de opdracht 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 plaats hiervan kunt u ook de opdracht **reset** op de IDSM-2 gebruiken zolang de variabele op het beginapparaat correct is ingesteld.Om de instelling van de variabele voor de laarsmachine voor de IDSM-2 te controleren, gebruikt u de opdracht switch **om het laarsapparaat *x* weer te geven**.
```
SV9-1> (enable)show boot device 6
Device BOOT variable = (null) (Default boot partition is hdd:1)
Memory-test set to PARTIAL
```
Om de variabele van het laarsapparaat voor IDSM-2 te configureren gebruikt u de opdracht voor het configureren van de switch **om het laarsapparaat hdd:1 *x* in te stellen**.
```
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
```

Gebruik de opdracht **resetten** om IDSM-2 te resetten via de onderhoudspartitie CLI.

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

16. Controleer of de IDSM-2 online komt. Gebruik de opdracht switch **tonen module *x*.**Zorg ervoor dat de IDSM-2-softwareversie een applicatie-versie is, bijvoorbeeld *4.1(1)S47,* en dat de status OK is.

```
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. Sluit aan op de IDSM-2 nu deze is opgestart in de toepassingsverdeling. Gebruik de switch commandosessie *x.*Gebruik de gebruikersnaam/het wachtwoord van **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. Configuratie IDSM-2 met het gebruik van de **bevelopstelling**.

```
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#
```

Gerelateerde informatie

- Cisco IDS UNIX-directeur
- Catalyst 6500 Series servicesmodule voor inbraakdetectiesysteem (IDSM-1)
- Catalyst 6500 Series servicesmodule voor inbraakdetectiesysteem (IDSM-2)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems