Kennwortwiederherstellung für die Cisco IDS-Sensor- und IDS-Dienstmodule (IDSM-1, IDSM-2)

Inhalt

Einführung

Dieses Dokument enthält Anweisungen zur Wiederherstellung Ihrer Cisco Secure Intrusion Detection System (IDS)-Appliance (ehemals NetRanger) und der Module für alle Versionen.

Voraussetzungen

Anforderungen

Wenn ein FTP-Server benötigt wird, muss er den passiven Modus unterstützen. Recovery-CDs können über das Product Upgrade Tool bezogen werden (nur registrierte Kunden).

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- IDS-Appliance Version 3 und 4
- IPS Appliance Versionen 5 und 6
- IDS-Modul (IDSM) Version 3 und IDSM-2 Version 4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

IDS-Appliance Version 3

Für die Appliance Version 3 stehen zwei Optionen zur Verfügung. Sie können den Kennwortwiederherstellungsvorgang verwenden oder ein Re-Image erstellen, das die Version 3 Recovery-CD verwendet. Beachten Sie, dass alle Informationen in einem Re-Image verloren gehen. Die Kennwortwiederherstellung erfolgt im Wesentlichen über eine Solaris-Kennwortwiederherstellung. Verwenden Sie diese Option nur, wenn Sie über keine Managementkonsole (Cisco Secure Policy Manager (CSPM), VPN/Security Management Solution (VMS), UNIX Director) verfügen, von der aus Sie die Konfiguration kopieren können.

Bei der IDS-Appliance Version 3 und früher existieren zwei Benutzernamen, die als 'netrangr' und 'root' bezeichnet werden. Das Standardkennwort für beide ist 'Attack'.

Kennwortwiederherstellung der IDS-Appliance, die Version 3 ausführt

Diese Dateien sind notwendig, um Ihr Kennwort wiederherzustellen.

- Solaris Device Configuration Assistant-Festplatte (Startdiskette) Sie können die Dateien von der Sun Support-Website herunterladen.**Hinweis:** Wenn dieser Link nicht funktioniert, versuchen Sie, zur obersten Ebene der Sun-Support-Website zu wechseln und unter Treiber nach *Device Configuration Assistant Boot Diskette Solaris Driver Downloads* zu suchen. Cisco Systems, Inc. verwaltet die Sun Support-Website nicht und hat keine Kontrolle darüber, wo sich die Inhalte befinden.
- Solaris für Intel (x86) CD-ROM.
- Konsolenzugriff auf die Workstation.

Führen Sie diese Schritte aus, um das Kennwort wiederherzustellen.

1. Legen Sie die Startdiskette ein.

2. Legen Sie die CD in das CD-ROM-Laufwerk ein.
3. Schalten Sie die Workstation aus, warten Sie zehn Sekunden, und schalten Sie sie ein.Das System startet von der Startdiskette. Nach der Konfiguration wird der erste Bildschirm des Configuration Assistant angezeigt.
4. Drücken Sie **F3**, um das System teilweise auf Startgeräte zu prüfen.Wenn die Prüfung abgeschlossen ist, wird eine Liste der Geräte angezeigt.
5. Stellen Sie sicher, dass das CD-ROM-Gerät in der Geräteliste angezeigt wird, und drücken Sie dann **F2**, um fortzufahren.Ein Bildschirm zeigt eine Liste der Startgeräte an.
6. Wählen Sie das **CD-ROM-**Laufwerk aus, und drücken Sie dann die Leertaste.Neben dem CD-ROM-Gerät befindet sich ein "X".
7. Drücken Sie **F2**, um fortzufahren.Die Workstation startet nun von der CD-ROM.
8. Wählen Sie auf dem Bildschirm zur Auswahl eines Installationstyps die **Option 2, Jumpstart aus**.Das System wird weiterhin gebootet.
9. Wählen Sie an der Eingabeaufforderung **Option 0** für Englisch aus.
10. Wählen Sie im nächsten Bildschirm für Sprachen erneut **Option 0** für Englisch ANSI aus.Das System wird weiterhin gestartet, und der Bildschirm Solaris Installation (Solaris-Installation) wird angezeigt.
11. Halten Sie die **Strg-**Taste gedrückt, und geben Sie **C ein**, um das Installationsskript zu beenden und den Zugriff auf die Eingabeaufforderung zu ermöglichen.
12. Geben Sie **mount -F ufs /dev/dsk/c0t0d0s0 /mnt ein.**Die Partition '/' wird nun am Mount-Punkt '/mnt' gemountet. Von hier aus können Sie die Datei '/etc/shatten' bearbeiten und das root-Passwort entfernen.
13. Geben Sie **cd /mnt/etc** ein.
14. Legen Sie die Shell-Umgebung so fest, dass Sie die Daten richtig lesen können.Geben Sie **TERM=ansi ein**.**TERM für Export eingeben**.
15. Geben Sie **vi-Schatten ein**.Sie befinden sich jetzt in der Schattendatei und können das Kennwort entfernen. Der Eintrag muss sein:

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

    Das ":" ist eine Feldtrennzeichen und das verschlüsselte Kennwort das zweite Feld.
16. Löscht das zweite Feld. Beispiel:
    `root:gNyqp8ohdfxPI:10598::::::`
    wird geändert in

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

    Dadurch wird das Kennwort für den Root-Benutzer entfernt.
17. Geben Sie **:wq!** um die Datei zu schreiben und zu beenden.
18. Entfernen Sie den Datenträger und die CD-ROM aus den Laufwerken.
19. Geben Sie **init 6 ein**, um das System neu zu starten.
20. Geben Sie **root** bei der Anmeldung ein: und drücken Sie dann die **Eingabetaste**.
21. Drücken Sie an der Kennworteingabeaufforderung **die Eingabetaste**.Sie sind jetzt beim Cisco Secure IDS Sensor angemeldet.

Image der IDS-Appliance, die Version 3 ausführt

Führen Sie diese Schritte aus, um ein neues Image der IDS-Appliance zu erstellen, die Version 3 ausführt.

Hinweis: Stellen Sie sicher, dass keine Maus an den Sensor angeschlossen ist, bevor Sie fortfahren.

1. Legen Sie die Version 3 Recovery-CD in die IDS-Appliance ein, und starten Sie sie neu.
2. Folgen Sie den Anweisungen auf Basis Ihrer Einrichtung, bis die Wiederherstellung erfolgreich war.
3. Melden Sie sich mit dem Standardbenutzernamen/-kennwort 'root/attack' an.
4. Führen Sie **sysconfig-sensor aus**, um die Appliance neu zu konfigurieren.

IDS-Appliance Version 4

Wiederherstellungsverfahren bei bekannter Benutzername/Kennwort des Administrators

Wenn ein Kennwort für ein Administratorkonto bekannt ist, kann dieses Benutzerkonto verwendet werden, um andere Benutzerkennwörter zurückzusetzen.

Beispielsweise werden auf der IDS-Appliance zwei Benutzernamen konfiguriert: "cisco" und "adminuser". Das Kennwort für den Benutzer "cisco" muss zurückgesetzt werden. 'adminuser' meldet sich an und setzt das Kennwort zurück.

```
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#
```

Wiederherstellungsverfahren, wenn Dienstbenutzername/Kennwort bekannt ist

Wenn ein Kennwort für das Dienstkonto bekannt ist, kann dieses Benutzerkonto verwendet werden, um andere Benutzerkennwörter zurückzusetzen.

Auf der IDS-Appliance werden beispielsweise drei Benutzernamen konfiguriert: "cisco", "adminuser" und "serviceuser". Das Kennwort für den Benutzer "cisco" muss zurückgesetzt werden. 'service user' meldet sich an und setzt das Kennwort zurück.

```
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#
```

Hinweis: Das Root-Kennwort entspricht dem Kennwort des Dienstkontos.

Image-IDS-Appliance, die Version 4 ausführt

Führen Sie diese Schritte aus, um ein Re-Image der IDS-Appliance zu erstellen.

Hinweis: Stellen Sie sicher, dass keine Maus an den Sensor angeschlossen ist, bevor Sie fortfahren.

1. Legen Sie die Version 4 Recovery-CD in die IDS-Appliance ein, und starten Sie sie neu.
2. Folgen Sie den Anweisungen auf Basis Ihrer Einrichtung, bis die Wiederherstellung erfolgreich war.
3. Melden Sie sich mit dem Standardbenutzernamen/-kennwort an, das 'cisco/cisco' lautet.
4. Führen Sie **Setup aus**, um die Einheit neu zu konfigurieren.

IPS Appliance Version 5 und Version 6

Laden Sie das AIP-SSM neu, fahren Sie es herunter, setzen Sie es zurück, und stellen Sie es wieder her.

Verwenden Sie die folgenden Befehle, um das Advanced Inspection and Prevention Security Services Module (AIP-SSM) direkt von der Adaptive Security Appliance neu zu laden, herunterzufahren, zurückzusetzen, das Kennwort wiederherzustellen:

Hinweis: Sie können die **hw-module-**Befehle im privilegierten EXEC-Modus oder im globalen Konfigurationsmodus eingeben. Sie können die Befehle im einzigen gerouteten Modus und im einzelnen transparenten Modus eingeben. Bei adaptiven Sicherheitsgeräten, die im Multi-Mode (geroutet oder transparent im Multi-Mode) betrieben werden, können Sie die **hw-module-**Befehle nur aus dem Systemkontext (nicht aus Administrator- oder Benutzerkontexten) ausführen.

- **hw-module module module module *slot_number* reload**: Dieser Befehl lädt die Software auf das AIP-SSM neu, ohne dass die Hardware zurückgesetzt wird. Sie ist nur dann wirksam, wenn sich das AIP-SSM im Up-Status befindet.
- **hw-module module module module *slot_number* shutdown** - Mit diesem Befehl wird die Software auf dem AIP-SSM heruntergefahren. Sie ist nur dann wirksam, wenn sich das AIP-SSM im Up-Status befindet.
- **hw-module module module module *slot_number* reset** - Dieser Befehl führt einen Hardware-Reset des AIP-SSM durch. Sie gilt, wenn sich die Karte im Status Nach oben/Nach unten/Nicht reagiert/Wiederherstellen befindet.
- **hw-module module module module module *slot_number* password-reset** - Mit diesem Befehl wird ein Kennwort für ein Cisco Content Security and Control Security Services Module (CSC-SSM) der Serie ASA 5500 oder das AIP-SSM wiederhergestellt, ohne dass ein neues Image des Geräts erforderlich ist.**Hinweis:** Dieser Befehl startet die Unterstützung von IPS 6.0 (ASA 7.2-Version) und wird verwendet, um das Cisco CLI-Kontenkennwort auf die Standard-**Cisco** wiederherzustellen.
- **hw-module module module module *slot_number* restore [boot | Stopp | configure]** - Der Befehl

restore zeigt eine Reihe interaktiver Optionen zum Einstellen oder Ändern der Wiederherstellungsparameter an. Sie können den Parameter ändern oder die bestehende Einstellung beibehalten, wenn Sie die **Eingabetaste** drücken.Informationen zum Wiederherstellen des AIP-SSM finden Sie unter Installieren des AIP-SSM-Systemabbilds.**hw-module module module module *slot_number* restore boot** - Dieser Befehl initiiert die Wiederherstellung des AIP-SSM. Sie ist nur anwendbar, wenn sich AIP-SSM im Betriebszustand befindet.**hw-module module module module *slot_number* restore stop** - Dieser Befehl beendet die Wiederherstellung des AIP-SSM. Sie ist nur anwendbar, wenn sich das AIP-SSM im Wiederherstellungszustand befindet.**Hinweis:** Wenn die AIP-SSM-Wiederherstellung gestoppt werden muss, müssen Sie den Befehl "**hw-module-Modul 1 restore stop**" innerhalb von 30 bis 45 Sekunden nach Start der AIP-SSM-Wiederherstellung ausführen. Wenn Sie länger warten, kann dies zu unerwarteten Konsequenzen führen. Das AIP-SSM kann beispielsweise im Status "Unreagierend" angezeigt werden.**hw-module module module 1 restore configure** - Verwenden Sie diesen Befehl, um Parameter für die Modulwiederherstellung zu konfigurieren. Die wichtigsten Parameter sind die IP-Adresse und der TFTP-URL-Speicherort des Wiederherstellungs-Image.Beispiel:

```
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]:
```

Erstellen Sie ein neues Image des AIP-SSM-Systemabbilds.

Gehen Sie wie folgt vor, um das AIP-SSM-Systemabbild zu installieren:

1. Melden Sie sich bei der ASA an.
2. Aktivieren Sie den Modus:
   ```
   asa>enable
   ```
3. Konfigurieren Sie die Wiederherstellungseinstellungen für das AIP-SSM:
   ```
   asa#hw-module module 1 recover configure
   ```

   Hinweis: Wenn Sie in der Wiederherstellungskonfiguration einen Fehler machen, verwenden Sie den Befehl **hw-module module module module 1 restore stop**, um die Systemneuerstellung zu beenden, und dann können Sie die Konfiguration korrigieren.
4. Geben Sie die TFTP-URL für das Systemabbild an:
   ```
   Image URL [tftp://0.0.0.0/]:
   ```
   Beispiel:
   ```
   Image URL [tftp://0.0.0.0/]:
    tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img
   ```
5. Geben Sie die Command-and-Control-Schnittstelle des AIP-SSM an:
   ```
   Port IP Address [0.0.0.0]:
   ```
   Beispiel:
   ```
   Port IP Address [0.0.0.0]: 10.89.149.231
   ```
6. Belassen Sie die VLAN-ID bei 0.
   ```
    VLAN ID [0]:
   ```
7. Geben Sie das Standard-Gateway des AIP-SSM an:
   ```
   Gateway IP Address [0.0.0.0] :
   ```
   Beispiel:
   ```
   Gateway IP Address [0.0.0.0]:10.89.149.254
   ```
8. Führen Sie die Wiederherstellung aus:
   ```
   asa#hw-module module 1 recover boot
   ```

9. Überprüfen Sie die Wiederherstellung regelmäßig, bis sie abgeschlossen ist:**Hinweis:** Der Status liest während der Wiederherstellung guest@localhost.localdomain# und liest guest@localhost.localdomain#, wenn die Neuerstellung abgeschlossen ist.

```
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#
```

Hinweis: Um Fehler zu debuggen, die im Wiederherstellungsvorgang auftreten können, verwenden Sie den Befehl **debug module-boot**, um das Debuggen des Systemwiederholungsprozesses zu aktivieren.

10. Sitzung zum AIP-SSM und Initialisierung des AIP-SSM mit dem **Setup-**Befehl.

IDSM

Sie können keine Methode verwenden, um eine Kennwortwiederherstellung im IDSM durchzuführen, während die Konfiguration erhalten bleibt.

Hinweis: Für dieses Verfahren muss die Wartungspartition verwendet werden. Wenn das Kennwort der Wartungspartition geändert wurde und Sie sich nicht anmelden können, muss das IDSM ersetzt werden. Wenden Sie sich in diesem Fall an den technischen Support von Cisco.

Re-Image-IDSM mit Switch, der nativen IOS-Code (Integrated IOS) ausführt

Führen Sie diese Schritte aus, um ein neues Image des ISDM mit einem Switch zu erstellen, auf dem Native IOS (Integrated IOS)-Code ausgeführt wird.

1. Starten Sie IDSM mithilfe des Switch-Befehls **hw-module module module *x* reset hdd:2**, wobei *x* für die Steckplatznummer steht.

```
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. Stellen Sie sicher, dass das IDSM mit dem Switch-Befehl **show module *x*** online gestellt wird.Stellen Sie sicher, dass sich zu Beginn die Version der IDSM-Software 2 befindet, die

anzeigt, dass die Wartungspartitionssoftware derzeit auf dem IDSM ausgeführt wird und dass der Status "OK" lautet.

```
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. Stellen Sie mithilfe des Switch-Befehls **Sitzungssteckplatz *x* Prozessor 1** eine Verbindung zur IDSM-Wartungspartition her.Verwenden Sie den Benutzernamen/das Kennwort von **Ciscoids/Attacke**.

```
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. Installieren Sie das zwischengespeicherte Bild, um die IDSM-Anwendungspartition erneut zu Image zu erstellen.Führen Sie den Diagnosebefehl **ids-installer system /cache /show aus,** um zu überprüfen, ob das zwischengespeicherte Image vorhanden ist.

```
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)#
```

   Wenn kein zwischengespeichertes Image vorhanden ist oder die Version nicht die Version ist, die Sie installieren möchten, fahren Sie mit Schritt 5 fort.Verwenden Sie den Diagnosebefehl **ids-installer system /cache /install**, um das ISDM mithilfe des zwischengespeicherten Images erneut abzuspielen.

```
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:\!
```

   Fahren Sie nach Abschluss des Re-Image mit Schritt 12 fort.

5. Stellen Sie sicher, dass das IDSM über IP-Verbindungen verfügt. Geben Sie den Befehl **ping *ip_address ein***.

```
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. Wenn das IDSM über IP-Verbindungen verfügt, fahren Sie mit Schritt 11 fort. Wenn Sie keine IP-Verbindung haben, fahren Sie mit den Schritten 7 bis 9 fort.

7. Stellen Sie sicher, dass die Command-and-Control-Schnittstelle ordnungsgemäß auf dem Switch konfiguriert ist. Geben Sie den Befehl **show run interface Gigx/2 ein**.

```
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. Stellen Sie sicher, dass die Kommunikationsparameter auf der IDSM-Wartungspartition korrekt konfiguriert sind. Führen Sie den Diagnosebefehl **ids-installer netconfig /view aus**.

```
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. Wenn keine der Parameter festgelegt sind oder einige geändert werden müssen, verwenden Sie den Diagnosebefehl **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. Überprüfen Sie die IP-Konnektivität erneut, nachdem Sie das IDSM zurückgesetzt haben, damit die Änderungen wirksam werden. Wenn die IP-Verbindung weiterhin ein Problem darstellt, beheben Sie das Problem gemäß einem normalen IP-Verbindungsproblem, und fahren Sie dann mit Schritt 11 fort.
11. Image der IDSM-Anwendungspartition erneut erstellen. Laden Sie das Image mit dem Diagnosebefehl **ids-installer system /nw /install /server=*ip_address* /user=*account* /save={*yes/no*} /dir=*ftp_path* /prefix=file_prefix, wobei:***ip_address*** ist die IP-Adresse des FTP-Servers.***Konto*** ist der Benutzer oder Kontoname, der bei der Anmeldung beim FTP-Server verwendet wird.***save*** bestimmt, ob eine Kopie des heruntergeladenen Bildes als zwischengespeicherte Kopie gespeichert werden soll. Wenn ja, wird jedes vorhandene zwischengespeicherte Bild überschrieben. Falls nein, wird das heruntergeladene Image auf der inaktiven Partition installiert, aber keine zwischengespeicherte Kopie wird gespeichert.***ftp_path*** gibt das Verzeichnis auf dem FTP-Server an, in dem sich die Bilddateien befinden.***file_prefix*** ist der Dateiname der .dat-Datei im heruntergeladenen Bild. Das heruntergeladene Bild besteht aus einer Datei mit der Erweiterung .dat und mehreren Dateien mit der Erweiterung .cab. Beim file_prefix-Wert muss es sich um den Namen der DAT-Datei handeln, wobei das Suffix .dat jedoch nicht enthalten sein muss.

```
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. Starten Sie IDSM mithilfe des Switch-Befehls **hw-module module x reset hdd:1 auf die** Anwendungspartition.

```
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.
```

Stellen Sie außerdem sicher, dass der Switch so konfiguriert ist, dass er das IDSM in die Anwendungspartition bootet. Um dies zu überprüfen, verwenden Sie den Befehl **show bootvar device module *x***.

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

Um die Boot-Device-Variable für IDSM zu konfigurieren, verwenden Sie den Switch-Konfigurationsbefehl **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. Stellen Sie sicher, dass das IDSM mit dem Switch-Befehl **show module *x*** online gestellt wird.Stellen Sie sicher, dass die IDSM-Softwareversion eine Anwendungspartitionsversion ist, z. B. *3.0(1)S4*, und dass der Status OK ist.

```
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. Stellen Sie jetzt eine Verbindung zum IDSM her, nachdem es in die Anwendungspartition hochgefahren ist, und konfigurieren Sie es so, dass es mit dem Director kommunizieren kann. Verwenden Sie den Befehl **setup**.Sobald die Kommunikation mit dem Director hergestellt ist, kann die Konfiguration auf das IDSM heruntergeladen werden.Verwenden Sie den Benutzernamen/das Kennwort von **Ciscoids/Attacke**, um sich anzumelden.

```
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.
```

Image-IDSM mit Switch, der Hybrid (CatOS)-Code ausführt

Führen Sie diese Schritte aus, um ein neues Image von ISDM mit einem Switch zu erstellen, der einen Hybrid-Code (CatOS) ausführt.

Hinweis: Alle Informationen auf der Anwendungspartition gehen verloren. Es gibt keine Methode, mit der Sie eine Kennwortwiederherstellung im IDSM durchführen können, während Sie die Konfiguration beibehalten.

Hinweis: Für dieses Verfahren muss die Wartungspartition verwendet werden. Wenn das Kennwort der Wartungspartition geändert wurde und Sie sich nicht anmelden können, muss das IDSM ersetzt werden. Wenden Sie sich in diesem Fall an den technischen Support von Cisco.

1. Starten Sie das IDSM mit dem Befehl **reset *x* hdd:2** auf die Maintenance-Partition.
```
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. Stellen Sie sicher, dass das IDSM mit dem Switch-Befehl **show module *x*** online ist.Stellen Sie sicher, dass sich zu Beginn die Version der IDSM-Software 2 befindet, die anzeigt, dass die Wartungspartitionssoftware derzeit auf dem IDSM ausgeführt wird und dass der Status "OK" lautet.
```
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. Stellen Sie jetzt eine Verbindung zum IDSM her, nachdem es mit der Switch-Befehlssitzung *x* in die Wartungspartition gestartet wurde.Verwenden Sie den Benutzernamen/das Kennwort von **Ciscoids/Attacke**.
```
ltd9-9> (enable)session 4
Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:
maintenance#
```
4. Installieren Sie das zwischengespeicherte Bild, um die IDSM-Anwendungspartition erneut zu Image zu erstellen.Stellen Sie sicher, dass das zwischengespeicherte Image mithilfe des Diagnosebefehls **ids-installer system /cache /show** vorhanden ist.
```
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)#
```

Wenn kein zwischengespeichertes Bild vorhanden ist oder die gecachte Version nicht die Version ist, die Sie installieren möchten, fahren Sie mit Schritt 5 fort.Um ein neues Image des ISDM zu erstellen, der das zwischengespeicherte Image verwendet, verwenden Sie den Diagnosebefehl **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:\!
```

Fahren Sie nach Abschluss des neuen Images mit Schritt 12 fort.

5. Stellen Sie sicher, dass das IDSM über IP-Verbindungen mit dem Befehl **ping *ip_address*** verfügt.

```
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. Wenn das IDSM über IP-Verbindungen verfügt, fahren Sie mit Schritt 11 fort. Wenn Sie keine IP-Verbindung haben, fahren Sie mit den Schritten 7 bis 9 fort.
7. Stellen Sie sicher, dass die Command-and-Control-Schnittstelle auf dem Switch mithilfe des Befehls **show port status *x*/2** korrekt konfiguriert ist.

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

8. Stellen Sie sicher, dass die Kommunikationsparameter auf der IDSM-Wartungspartition korrekt konfiguriert sind. Verwenden Sie hierzu den Diagnosebefehl **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. Wenn keine der Parameter festgelegt sind oder einige geändert werden müssen, verwenden Sie den Diagnosebefehl **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. Aktivieren Sie IP Connectivity erneut, nachdem Sie IDSM zurückgesetzt haben, damit die Änderungen wirksam werden.Wenn die IP-Verbindung weiterhin ein Problem darstellt, beheben Sie das Problem gemäß einem normalen IP-Verbindungsproblem, und fahren Sie dann mit Schritt 11 fort.
11. Image der IDSM-Anwendungspartition erneut erstellen. Laden Sie das Image mit dem Diagnosebefehl **ids-installer system /nw /install /server=*ip_address* /user=account /save={*yes/no*} /dir=*ftp_path* /prefix=*file_prefix* herunter, bei dem:***ip_address*** ist die IP-Adresse des FTP-Servers.***Konto*** ist der Benutzer oder Kontoname, der bei der Anmeldung beim FTP-Server verwendet wird.***save*** bestimmt, ob eine Kopie des heruntergeladenen Bildes als zwischengespeicherte Kopie gespeichert werden soll. Wenn ja, wird jedes vorhandene zwischengespeicherte Bild überschrieben. Falls nein, wird das heruntergeladene Image auf der inaktiven Partition installiert, aber keine zwischengespeicherte Kopie wird gespeichert.***ftp_path*** gibt das Verzeichnis auf dem FTP-Server an, in dem sich die Bilddateien befinden.***file_prefix*** ist der Dateiname der .dat-Datei im heruntergeladenen Bild. Das heruntergeladene Bild besteht aus einer Datei mit der Erweiterung .dat und mehreren Dateien mit der Erweiterung .cab. Beim file_prefix-Wert muss es sich um den Namen der DAT-Datei bis zum .dat-Suffix handeln.

```
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. Starten Sie IDSM mithilfe des Befehls **reset *x* hdd:1** auf der Anwendungspartition.

```
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.
```

Stellen Sie außerdem sicher, dass der Switch so konfiguriert ist, dass er das IDSM in die Anwendungspartition bootet. Verwenden Sie den Befehl **show boot device *x*, um dies** zu überprüfen.

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

Um die Boot-Device-Variable für IDSM zu konfigurieren, verwenden Sie den Switch-Konfigurationsbefehl **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. Stellen Sie sicher, dass das IDSM mit dem Befehl switch **show module *x*** online gestellt wird.Stellen Sie sicher, dass die IDSM-Softwareversion eine Anwendungspartitionsversion ist, z. B. *3.0(1)S4*, und dass der Status OK ist.

```
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. Stellen Sie jetzt eine Verbindung zum IDSM her, nachdem es in die Anwendungspartition hochgefahren ist, und konfigurieren Sie es so, dass es mit dem Director kommunizieren kann. Verwenden Sie den Befehl **setup**.Melden Sie sich mit dem Benutzernamen/Kennwort von **ciscoids/Attacke an**.

```
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

Wiederherstellungsverfahren bei bekannter Benutzername/Kennwort des Administrators

Wenn ein Kennwort für ein Administratorkonto bekannt ist, kann dieses Benutzerkonto verwendet werden, um andere Benutzerkennwörter zurückzusetzen.

Beispielsweise werden auf der IDSM-2 zwei Benutzernamen konfiguriert: "cisco" und "adminuser". Das Kennwort für den Benutzer "cisco" muss zurückgesetzt werden. 'adminuser' meldet sich an und setzt das Kennwort zurück.

```
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#
```

Wiederherstellungsverfahren, wenn Dienstbenutzername/Kennwort bekannt ist

Wenn ein Kennwort für das Dienstkonto bekannt ist, kann dieses Benutzerkonto verwendet

werden, um andere Benutzerkennwörter zurückzusetzen.

Auf der IDSM-2 werden beispielsweise drei Benutzernamen konfiguriert: "cisco", "adminuser" und "serviceuser". Das Kennwort für den Benutzer "cisco" muss zurückgesetzt werden. 'service user' meldet sich an und setzt das Kennwort zurück.

```
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#
```

Hinweis: Das Root-Kennwort entspricht dem Kennwort des Dienstkontos.

Image-IDSM-2 mit Switch, der einen IOS-Code (Integrated IOS) ausführt

Führen Sie diese Schritte aus, um ein neues Image von ISDM-2 mit einem Switch zu erstellen, auf dem Native IOS (Integrated IOS)-Code ausgeführt wird.

Hinweis: Alle Informationen auf der Anwendungspartition gehen verloren. Sie können keine Methode verwenden, um eine Kennwortwiederherstellung auf dem IDSM-2 durchzuführen, während die Konfiguration erhalten bleibt.

1. Starten Sie IDSM-2 mithilfe des Switch-Befehls **hw-module module module *x* reset cf:1**, wobei *x* für die Steckplatznummer steht und cf für "compact flash" steht.**Hinweis:** Wenn ein Problem mit cf:1 auftritt, verwenden Sie hdd:2 als Alternative.

```
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. Stellen Sie sicher, dass das IDSM-2 mit dem Befehl switch **show module *x*** online ist.Stellen Sie sicher, dass sich am Ende die Version der IDSM-2-Software "m" befindet und der Status "OK" lautet.

```
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. Stellen Sie jetzt eine Verbindung zum IDSM-2 her, nachdem es in die Wartungspartition gestartet wurde. Verwenden Sie den Switch-Befehl **Sitzungssteckplatz xprocessor 1**.Verwenden Sie den Benutzernamen/das Kennwort von **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. Stellen Sie sicher, dass die IDSM-2 über IP-Verbindungen verfügt. Verwenden Sie den Befehl **ping *ip_address***.

```
guest@idsm2-sv-rack.localdomain#ping 10.66.79.193
guest@idsm2-sv-rack.localdomain#ping 10.66.79.193
PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data.
64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=2.188 msec
64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.014 msec
64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=991 usec
64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.011 msec
64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.019 msec
--- 10.66.79.193 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.991/1.244/2.188/0.473 ms
guest@idsm2-sv-rack.localdomain#
```

5. Wenn das IDSM-2 über eine IP-Verbindung verfügt, fahren Sie mit Schritt 14 fort.
6. Stellen Sie sicher, dass die Command-and-Control-Schnittstelle ordnungsgemäß auf dem Switch konfiguriert ist. Verwenden des Befehls **show run | inc Intrusion Detection**.

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

7. Stellen Sie sicher, dass die Kommunikationsparameter auf der IDSM-2-Wartungspartition korrekt konfiguriert sind. Verwenden Sie den Befehl **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. Wenn keine Parameter festgelegt sind oder einige geändert werden müssen, löschen Sie alle Parameter. Verwenden Sie den Befehl **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. Konfigurieren Sie die IP-Adresse und die Maskeninformationen auf der IDSM-2-Maintenance-Partition. Verwenden Sie den Befehl **ip address *ip_address netmask***.

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

10. Konfigurieren Sie das Standardgateway auf der IDSM-2-Wartungspartition. Verwenden Sie den Befehl **ip gateway *gateway-address***.

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

11. Konfigurieren Sie den Hostnamen auf der IDSM-2-Wartungspartition. Verwenden Sie den Befehl **ip host *hostname***.Obwohl dies nicht notwendig ist, hilft es bei der Identifizierung des Geräts, da dies auch die Eingabeaufforderung festlegt.

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

12. Möglicherweise müssen Sie Ihre Broadcast-Adresse explizit konfigurieren. Verwenden Sie den Befehl **ip Broadcast *Address***.Die Standardeinstellung reicht in der Regel aus.

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

13. Überprüfen Sie erneut die IP-Verbindung. Wenn die IP-Verbindung weiterhin ein Problem darstellt, beheben Sie das Problem gemäß einem normalen IP-Verbindungsproblem, und fahren Sie mit Schritt 14 fort.
14. Image der IDSM-2-Anwendungspartition erneut erstellen. Verwenden Sie den Befehl **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. Starten Sie IDSM-2 von der Anwendungspartition. Verwenden Sie den Switch-Befehl **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.
```

Alternativ können Sie den Befehl **reset** auf dem IDSM-2 verwenden, solange die Boot-Device-Variable korrekt festgelegt ist.Um die Einstellung der Boot-Device-Variablen für IDSM-2 zu überprüfen, verwenden Sie den Befehl **show bootvar device module *x***.

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

Um die Boot-Device-Variable für IDSM-2 zu konfigurieren, verwenden Sie den Switch-Konfigurationsbefehl **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
```

Verwenden Sie den Befehl **reset**, um das IDSM-2 über die CLI Maintenance Partition (Maintenance Partition) zurückzusetzen.

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

16. Stellen Sie sicher, dass die IDSM-2 online ist. Verwenden Sie den Befehl switch **show module *x***.Stellen Sie sicher, dass die IDSM-2-Softwareversion eine Anwendungspartitionsversion ist, z. B. *4.1(1)S47* und dass der Status OK ist.

```
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. Stellen Sie jetzt eine Verbindung zum IDSM-2 her, nachdem es in die Anwendungspartition gestartet wurde. Verwenden Sie den Switch-Befehl **Sitzungssteckplatz *x* Prozessor 1**.Verwenden Sie den Benutzernamen/das Kennwort von **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. Konfigurieren Sie IDSM-2. Verwenden Sie den Befehl **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#
```

Re-Image für IDSM-2 mit Switch, der Hybrid (CatOS)-Code ausführt

Führen Sie diese Schritte aus, um ein neues Image des ISDM-2 mit einem Switch zu erstellen, der einen Hybrid-Code (CatOS) ausführt.

1. Starten Sie IDSM-2 in die Wartungspartition. Verwenden Sie den Befehl switch **reset *x* hdd:2**.**Hinweis:** Wenn ein Problem mit hdd:2 auftritt, versuchen Sie, cf:1 als Alternative zu verwenden.

```
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. Stellen Sie sicher, dass die IDSM-2 online ist. Verwenden Sie den Befehl switch **show module *x***.Stellen Sie sicher, dass sich am Ende der IDSM-2-Softwareversion "m" befindet, die anzeigt, dass die Software der Wartungspartition aktuell ausgeführt wird und dass der Status OK ist.

```
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. Stellen Sie jetzt eine Verbindung zum IDSM-2 her, nachdem es in die Wartungspartition gestartet wurde. Verwenden Sie den Switch-Befehl **session *x***.Verwenden Sie den Benutzernamen/das Kennwort von **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. Stellen Sie sicher, dass die IDSM-2 über IP-Verbindungen verfügt. Verwenden Sie den Befehl **ping *ip_address***.

```
guest@idsm2-sv-rack.localdomain#ping 10.66.79.193
PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data.
64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=1.035 msec
64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.041 msec
64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=1.066 msec
64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.074 msec
64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.026 msec
```

```
--- 10.66.79.193 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 1.026/1.048/1.074/0.034 ms
```

5. Wenn das IDSM-2 über eine IP-Verbindung verfügt, fahren Sie mit Schritt 14 fort.
6. Stellen Sie sicher, dass die Command-and-Control-Schnittstelle ordnungsgemäß auf dem Switch konfiguriert ist. Verwenden Sie den Befehl **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. Stellen Sie sicher, dass die Kommunikationsparameter auf der IDSM-2-Wartungspartition korrekt konfiguriert sind. Verwenden Sie den Befehl **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. Wenn keine der Parameter festgelegt sind oder einige geändert werden müssen, löschen Sie sie alle mithilfe des Befehls **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. Konfigurieren Sie die IP-Adresse und die Maskeninformationen auf der IDSM-2-Maintenance-Partition. Verwenden Sie den Befehl **ip address *ip_address netmask*.**

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

10. Konfigurieren Sie das Standardgateway auf der IDSM-2-Wartungspartition. Verwenden Sie den Befehl **ip gateway *gateway-address*.**

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

11. Konfigurieren Sie den Hostnamen auf der IDSM-2-Wartungspartition. Verwenden Sie den Befehl **ip host *hostname*.**Obwohl dies nicht notwendig ist, hilft es, das Gerät zu identifizieren, da dies auch die Eingabeaufforderung festlegt.

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

12. Möglicherweise müssen Sie Ihre Broadcast-Adresse explizit konfigurieren. Verwenden Sie den Befehl **ip Broadcast *Address*.**Die Standardeinstellung reicht in der Regel aus.

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

13. Überprüfen Sie erneut die IP-Verbindung. Wenn die IP-Verbindung weiterhin ein Problem darstellt, beheben Sie das Problem gemäß einem normalen IP-Verbindungsproblem, und fahren Sie mit Schritt 14 fort.
14. Image der IDSM-2-Anwendungspartition erneut erstellen. Verwenden Sie den Befehl **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. Starten Sie IDSM-2 von der Anwendungspartition. Verwenden Sie den Befehl 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.
```

Alternativ können Sie den Befehl **reset** auf dem IDSM-2 verwenden, solange die Boot-Device-Variable korrekt festgelegt ist.Verwenden Sie den Befehl **show boot device *x***, um die Einstellung der Boot-Device-Variablen für IDSM-2 zu überprüfen.

```
SV9-1> (enable)show boot device 6
Device BOOT variable = (null) (Default boot partition is hdd:1)
Memory-test set to PARTIAL
```

Um die Boot-Device-Variable für IDSM-2 zu konfigurieren, verwenden Sie den Switch configuration-Befehl **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
```

Um IDSM-2 über die CLI der Maintenance Partition zurückzusetzen, verwenden Sie den Befehl **reset**.

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

16. Stellen Sie sicher, dass die IDSM-2 online ist. Verwenden Sie den Befehl switch **show module *x***.Stellen Sie sicher, dass die IDSM-2-Softwareversion eine Anwendungspartitionsversion ist, z. B. *4.1(1)S47,* und dass der Status OK ist.

```
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. Stellen Sie jetzt eine Verbindung zum IDSM-2 her, nachdem es in die Anwendungspartition

gestartet wurde. Verwenden Sie den Switch-Befehl **session *x***.Verwenden Sie den Benutzernamen/das Kennwort von **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. Konfigurieren Sie IDSM-2 mithilfe des Befehls **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#
```

Zugehörige Informationen

- Cisco IDS UNIX Director
- Servicemodul: Catalyst Intrusion Detection System (IDSM-1) der Serie 6500
- Servicemodul: Catalyst Intrusion Detection System (IDSM-2) der Serie 6500
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation für Cisco Systeme