Cisco IDS 센서 및 IDS 서비스 모듈의 비밀번호 복구 절차(IDSM-1, IDSM-2)

목차

소개

이 문서에서는 Cisco IDS(Secure Intrusion Detection System)(이전의 NetRanger) 어플라이언스와 모든 버전의 모듈을 복구하는 방법에 대한 절차를 제공합니다.

사전 요구 사항

요구 사항

FTP 서버가 필요한 경우 수동 모드를 지원해야 합니다. 복구 CD는 제품 업그레이드 툴을 사용하여 얻을 수 있습니다(등록된 고객만 해당).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IDS Appliance 버전 3 및 4
- IPS Appliance 버전 5 및 6
- IDSM(IDS Module) 버전 3 및 IDSM-2 버전 4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

IDS Appliance 버전 3

버전 3 어플라이언스에 대해 두 가지 옵션을 사용할 수 있습니다. 비밀번호 복구 프로세스를 사용하거나 버전 3 복구 CD를 사용하는 이미지를 재생성할 수 있습니다. 재이미지에서는 모든 정보가 손실됩니다. 비밀번호 복구 절차는 기본적으로 Solaris 비밀번호 복구입니다. 컨피그레이션을 복사할 수 있는 관리 스테이션(Cisco CSPM(Secure Policy Manager), VPN/VMS(Security Management Solution), UNIX Director)이 없는 경우에만 이 옵션을 사용합니다.

IDS Appliance 버전 3 이하에서는 'netrangr' 및 'root'라는 두 개의 사용자 이름이 있습니다. 둘 다의 기본 비밀번호는 'attack'입니다.

버전 3을 실행하는 IDS 어플라이언스의 비밀번호 복구

이러한 파일은 비밀번호를 복구하기 위해 필요합니다.

- Solaris Device Configuration Assistant 디스크(부트 디스크). Sun 지원 웹 사이트에서 파일을 다운로드할 수 있습니다 .**참고:** 이 링크가 작동하지 않으면 Sun 지원 웹 사이트의 최상위 레벨로 이동하여 Drivers(드라이버) 아래에서 Device Configuration Assistant Boot Diskette Solaris Driver Downloads(*디바이스 컨피그레이션 보조자 부팅 디스켓 Solaris 드라이버 다운로드)를* 검색해 보십시오. Cisco Systems, Inc.는 Sun 지원 웹 사이트 를 유지하지 않으며 콘텐츠의 위치를 제어할 수 없습니다.
- Solaris for Intel (x86) CD-ROM.
- 워크스테이션에 대한 콘솔 액세스

비밀번호를 복구하려면 다음 단계를 완료하십시오.

1. 부팅 디스크를 삽입합니다.
2. CD-ROM 드라이브에 CD를 넣습니다.
3. 워크스테이션을 끄고 10초 동안 기다린 다음 켜십시오.시스템이 부팅 디스크에서 부팅됩니다. 일부 컨피그레이션 후 초기 Configuration Assistant 화면이 표시됩니다.
4. 시스템에서 부팅 디바이스를 부분 스캔하려면 **F3**을 누릅니다.검사가 완료되면 디바이스 목록이 표시됩니다.
5. CD-ROM 디바이스가 디바이스 목록에 나타나는지 확인한 다음 **F2**를 눌러 계속합니다.부팅 디바이스 목록이 화면에 표시됩니다.

6. **CD-ROM** 드라이브를 선택한 다음 스페이스 바를 누릅니다.CD-ROM 디바이스 옆에 'X'가 있습니다.
7. 계속하려면 **F2**를 누릅니다.이제 워크스테이션이 CD-ROM에서 부팅됩니다.
8. 설치 유형을 선택하는 데 사용되는 화면에서 **옵션 2, Jumpstart를** 선택합니다.시스템이 계속 부팅됩니다.
9. 언어를 선택하라는 메시지가 표시되면 **Option 0** for English를 선택합니다.
10. 언어의 다음 화면에서 영어 ANSI의 **옵션 0을** 다시 선택합니다.시스템이 계속 부팅되고 Solaris Installation 화면이 나타납니다.
11. 설치 스크립트를 중지하고 프롬프트에 액세스할 수 있도록 **Control** 키를 길게 누르고 **C**를 입력합니다.
12. mount **-F ufs /dev/dsk/c0t0d0s0 /mnt 를 입력합니다.**'/' 파티션이 이제 '/mnt' 마운트 지점에 마운트됩니다. 여기에서 '/etc/shadow' 파일을 편집하고 루트 암호를 제거할 수 있습니다.
13. cd **/mnt/etc 를 입력합니다**.
14. 데이터를 올바르게 읽을 수 있도록 셸 환경을 설정합니다.TERM**=ansi를 입력합니다**.export **TERM을 입력합니다**.
15. vi **shadow를 입력합니다**.이제 섀도 파일에 있으며 암호를 제거할 수 있습니다. 항목은 다음과 같아야 합니다.

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

    ":"은 필드 구분 기호로, 암호화된 암호는 두 번째 필드입니다.
16. 두 번째 필드를 삭제합니다. 예를 들어
    ```
    root:gNyqp8ohdfxPI:10598::::::
    ```
    다음으로 변경

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

    루트 사용자의 비밀번호가 제거됩니다.
17. 유형**:wq!** 파일을 작성하고 종료합니다.
18. 드라이브에서 디스크와 CD-ROM을 제거합니다.
19. 시스템을 재부팅하려면 **init 6**을 입력합니다.
20. 로그인에 root를 입력합니다. 프롬프트를 표시한 다음 Enter를 **누릅니다**.
21. 비밀번호 프롬프트에서 Enter를 누릅니다.이제 Cisco Secure IDS Sensor에 로그인합니다.

버전 3을 실행하는 IDS 어플라이언스의 이미지 재지정

버전 3을 실행하는 IDS 어플라이언스를 다시 이미징하려면 다음 단계를 완료하십시오.

참고: 계속하기 전에 마우스가 센서에 연결되어 있지 않은지 확인하십시오.

1. 버전 3 복구 CD를 IDS 어플라이언스에 넣고 재부팅합니다.
2. 복구에 성공할 때까지 설정에 따라 프롬프트를 따릅니다.
3. 'root/attack'의 기본 사용자 이름/비밀번호를 사용하여 로그인합니다.
4. 어플라이언스**를** 재구성하려면 sysconfig-sensor를 실행합니다.

IDS Appliance 버전 4

관리자 사용자 이름/비밀번호를 알고 있는 경우 복구 절차

관리자 계정의 암호를 알고 있는 경우 이 사용자 계정을 사용하여 다른 사용자 암호를 재설정할 수 있습니다.

예를 들어, 두 개의 사용자 이름이 'cisco' 및 'adminuser'라는 IDS 어플라이언스에 구성됩니다. 'cisco' 사용자의 비밀번호를 재설정해야 하므로 'adminuser'가 로그인하고 비밀번호를 재설정합니다.

```
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#
```

서비스 사용자 이름/비밀번호를 알고 있는 경우 복구 절차

서비스 계정의 암호를 알고 있는 경우 이 사용자 계정을 사용하여 다른 사용자 암호를 재설정할 수 있습니다.

예를 들어, IDS Appliance에 'cisco', 'adminuser' 및 'serviceuser'라는 세 개의 사용자 이름이 구성됩니다. 'cisco' 사용자의 비밀번호를 재설정해야 하므로 'serviceuser'가 로그인하고 비밀번호를 재설정합니다.

```
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#
```

참고: 루트 비밀번호는 서비스 계정의 비밀번호와 동일합니다.

버전 4를 실행하는 IDS 어플라이언스 이미지 재지정

IDS 어플라이언스를 다시 이미징하려면 다음 단계를 완료하십시오.

참고: 계속하기 전에 마우스가 센서에 연결되어 있지 않은지 확인하십시오.

1. 버전 4 복구 CD를 IDS 어플라이언스에 넣고 재부팅합니다.
2. 복구에 성공할 때까지 설정에 따라 프롬프트를 따릅니다.
3. 'cisco/cisco'의 기본 사용자 이름/비밀번호를 사용하여 로그인합니다.
4. 어플라이언스를 재구성하려면 setup을 실행합니다.

IPS Appliance 버전 5 및 버전 6

AIP-SSM 다시 로드, 종료, 재설정 및 복구

다음 명령을 사용하여 Adaptive Security Appliance에서 직접 AIP-SSM(Advanced Inspection and Prevention Security Services Module)을 다시 로드, 종료, 재설정, 복구하고 복구할 수 있습니다.

참고: 특별 권한 EXEC 모드 또는 전역 컨피그레이션 모드에서 **hw-module** 명령을 입력할 수 있습니다. 단일 라우팅 모드 및 단일 투명 모드에서 명령을 입력할 수 있습니다. 다중 모드(라우팅 또는 투명 다중 모드)에서 작동하는 적응형 보안 디바이스의 경우 시스템 컨텍스트(관리자 또는 사용자 컨텍스트가 아닌)에서 **hw-module** 명령만 실행할 수 있습니다.

- **hw-module module *slot_number* reload**—이 명령은 하드웨어 재설정을 수행하지 않고 AIP-SSM에서 소프트웨어를 다시 로드합니다. AIP-SSM이 작동 상태인 경우에만 유효합니다.
- **hw-module module *slot_number* shutdown** - 이 명령은 AIP-SSM에서 소프트웨어를 종료합니다. AIP-SSM이 작동 상태인 경우에만 유효합니다.
- **hw-module module *slot_number* reset** - 이 명령은 AIP-SSM의 하드웨어 재설정을 수행합니다. 카드가 Up/Down/Unresponsive/Recover 상태일 때 적용됩니다.
- **hw-module module *slot_number* password-reset**—이 명령은 디바이스를 다시 이미지화할 필요 없이 Cisco ASA 5500 Series CSC-SSM(Content Security and Control Security Services Module) 또는 AIP-SSM에서 비밀번호를 복구합니다.**참고:** 이 명령은 IPS 6.0(ASA 7.2 버전)에서 지원을 시작하고 Cisco CLI 계정 비밀번호를 기본 **cisco**로 복원하는 데 사용됩니다.
- **hw-module module *slot_number* recover [boot] | 중지 | configure]**—**recover** 명령은 복구 매개변수를 설정하거나 변경하기 위한 대화형 옵션 집합을 표시합니다. Enter 키를 누르면 매개변수를 변경하거나 기존 설정을 유지할 수 **있습니다**.AIP-SSM을 복구하는 데 사용하는 절차는 AIP-SSM 시스템 이미지 설치를 참조하십시오.**hw-module module *slot_number* recover boot**—이 명령은 AIP-SSM의 복구를 시작합니다. AIP-SSM이 작동 상태인 경우에만 적용됩니다.**hw-module module *slot_number* recover stop**—이 명령은 AIP-SSM의 복구를 중지합니다. AIP-SSM이 복구 상태인 경우에만 적용됩니다.**참고:** AIP-SSM 복구를 중지해야 하는 경우 AIP-SSM 복구를 시작한 후 30~45초 이내에 **hw-module module 1 recover stop** 명령을 실행해야 합니다. 조금만 더 기다리면 예기치 않은 결과를 초래할 수 있습니다. 예를 들어 AIP-SSM이 Unresponsive(응답하지 않음) 상태가 될 수 있습니다.**hw-module module 1 recover configure** - 모듈 복구를 위한 매개변수를 구성하려면 이 명령을 사용합니다. 필수 매개변수는 IP 주소 및 복구 이미지 TFTP URL 위치입니다.예:

```
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]:
```

AIP-SSM 시스템 이미지 재이미지

AIP-SSM 시스템 이미지를 설치하려면 다음 단계를 완료하십시오.

1. ASA에 로그인합니다.
2. 활성화 모드를 입력합니다.
   ```
   asa>enable
   ```
3. AIP-SSM에 대한 복구 설정을 구성합니다.
   ```
   asa#hw-module module 1 recover configure
   ```

참고: 복구 컨피그레이션에서 오류가 발생하면 hw-**module module 1 recover stop** 명령을 사용하여 시스템 재이미지화를 중지한 다음 컨피그레이션을 수정할 수 있습니다.

4. 시스템 이미지의 TFTP URL을 지정합니다.
   ```
   Image URL [tftp://0.0.0.0/]:
   ```
   예:
   ```
   Image URL [tftp://0.0.0.0/]:
    tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img
   ```
5. AIP-SSM의 명령 및 제어 인터페이스를 지정합니다.
   ```
   Port IP Address [0.0.0.0]:
   ```
   예:
   ```
   Port IP Address [0.0.0.0]: 10.89.149.231
   ```
6. VLAN ID를 0으로 둡니다.
   ```
    VLAN ID [0]:
   ```
7. AIP-SSM의 기본 게이트웨이를 지정합니다.
   ```
   Gateway IP Address [0.0.0.0] :
   ```
   예:
   ```
   Gateway IP Address [0.0.0.0]:10.89.149.254
   ```
8. 복구를 실행합니다.
   ```
   asa#hw-module module 1 recover boot
   ```
9. 복구가 완료될 때까지 주기적으로 복구를 확인합니다.**참고:** 상태는 복구 중 guest@localhost.localdomain#을 읽고 이미지로 다시 설치할 때 guest@localhost.localdomain#을 읽습니다.
   ```
   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#
   ```
   참고: 복구 프로세스에서 발생할 수 있는 오류를 디버깅하려면 debug **module-boot** 명령을 사용하여 시스템 재이미지화 프로세스의 디버깅을 활성화합니다.
10. AIP-SSM에 대한 세션을 시작하고 **setup** 명령으로 AIP-SSM을 초기화합니다.

IDSM

컨피그레이션이 유지되는 동안 IDSM에서 비밀번호 복구를 수행하는 데 사용할 수 있는 방법은 없습니다.

참고: 이 절차에서는 유지 관리 파티션을 사용해야 합니다. 유지 보수 파티션 암호가 변경되었고 로그인할 수 없는 경우 IDSM을 교체해야 합니다. 이 경우 Cisco 기술 지원에 문의하십시오.

네이티브 IOS(Integrated IOS) 코드를 실행하는 스위치와 함께 IDSM 이미지 재생성

Native IOS(Integrated IOS) 코드를 실행하는 스위치로 ISDM을 다시 이미징하려면 다음 단계를 완료합니다.

1. switch 명령 hw-**module module module *x* reset hdd**를 사용하여 IDSM을 Maintenance Partition(유지 관리 파티션)으로 부팅합니다. 여기서 *x*는 슬롯 번호를 나타냅니다.

```
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. switch 명령 **show module *x***를 사용하여 IDSM이 온라인 상태로 **제공되는지 *확인합니다*.**IDSM 소프트웨어 버전이 시작 부분에 2가 있는지 확인합니다. 이는 유지 관리 파티션 소프트웨어가 현재 IDSM에서 실행되고 있으며 상태가 OK임을 나타냅니다.

```
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. switch 명령 **세션 슬롯 *x* 프로세서 1**을 사용하여 IDSM 유지 관리 파티션*에 **연결합니다*** .ciscoids/**attack**의 사용자 이름/비밀번호**를 사용합니다**.

```
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. IDSM 애플리케이션 파티션을 다시 이미징하려면 캐시된 이미지를 설치합니다.캐시된 이미지가 **있는지** 확인하기 위해 diagnostics 명령 **ids-installer system /cache /show**를 실행합니다.

```
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)#
```

캐시된 이미지가 없거나 캐시된 버전이 설치하려는 이미지가 아닌 경우 5단계로 진행합니다 .캐시된 이미지를 사용하여 ISDM을 다시 이미징하려면 diagnostics 명령 ids-installer **system /cache /install을** 사용합니다.

```
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:\!
```

재이미지가 완료되면 12단계로 진행합니다.

5. IDSM에 IP 연결이 있는지 확인합니다. ping ip_*address* 명령을 *실행합니다.*

```
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. IDSM에 IP 연결이 있는 경우 11단계로 진행합니다. IP 연결이 없는 경우 7단계부터 9단계까지 진행합니다.
7. Command and Control Interface(명령 및 제어 인터페이스)가 스위치에 올바르게 구성되어 있는지 확인합니다. **show run interface Gix/2 명령을 실행합니다**.

```
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. 통신 매개변수가 IDSM 유지 관리 파티션에 올바르게 구성되어 있는지 확인합니다. diagnostics 명령 ids**-installer netconfig /view를 실행합니다**.

```
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. 설정된 매개 변수가 없거나 매개 변수 중 일부를 변경해야 하는 경우 diagnostics 명령 ids**-installer netconfig /configure *매개 변수*를** 사용합니다**.**

```
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. IDSM을 재설정한 후 IP 연결을 다시 확인하여 변경 사항을 적용합니다. IP 연결이 여전히 문제인 경우 일반적인 IP 연결 문제에 따라 문제를 해결한 다음 11단계를 진행합니다.
11. IDSM 애플리케이션 파티션을 다시 이미징합니다. 진단 명령 ids**-installer 시스템 /nw /install /server=*ip_address* /**user=*account /save={yes/no}* /**dir=*ftp_path* **/prefix=file_prefix***ip_address*는 FTP 서버의 IP 주소입니다.*account*는 FTP 서버에 로그인할 때 사용할 사용자 또는 계정 이름입니다.*저장*은 다운로드한 이미지의 복사본을 캐시된 복사본으로 저장할지 여부를 결정합니다. "예"를 선택하면 존재하는 캐시된 이미지를 덮어씁니다. no인 경우 다운로드한 이미지가 비활성 파티션에 설치되지만 캐시된 복사본은 저장되지 않습니다.*ftp_path*는 이미지 파일이 있는 FTP 서버의 디렉토리를 지정합니다.*file_prefix*는 다운로드한 이미지에 있는 .dat 파일의 파일 이름입니다. 다운로드한 이미지는 확장명이 .dat인 파일 하나와 확장명이 .cab인 파일 여러 개로 구성됩니다. file_prefix 값은 .dat 접미사를 포함하지 않는 DAT 파일의 이름이어야 합니다.

```
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. switch 명령 hw-**module module x reset hdd:1**을 사용하여 IDSM을 애플리케이션 파티션**으로 부팅합니다**.

```
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.
```

또한 스위치가 IDSM을 애플리케이션 파티션으로 부팅하도록 구성되어 있는지 확인합니다. 이를 확인하려면 show bootvar **device module *x*** 명령을 사용합니다.

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

IDSM에 대한 부팅 디바이스 변수를 구성하려면 switch configuration 명령 **boot device module x hdd:1을** 사용합니다.

```
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. switch 명령 **show module *x***를 사용하여 IDSM이 온라인 상태로 **제공되는지 *확인합니다*** .IDSM 소프트웨어 버전이 애플리케이션 파티션 버전(예: *3.0(1)S4)*이고 상태가 OK인지 확인합니다.

```
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. 애플리케이션 파티션으로 부팅되었으므로 IDSM에 연결하고 디렉터와 통신할 수 있도록 구성합니다. 명령 **설정**을 **사용합니다**.디렉터와의 통신이 설정되면 구성을 IDSM에 다운로드할 수 있습니다.로그인하려면 ciscoids**/attack**의 사용자 이름/비밀번호를 사용합니다.

```
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.
```

하이브리드(CatOS) 코드를 실행하는 스위치와 함께 IDSM 이미지 재작성

하이브리드(CatOS) 코드를 실행하는 스위치로 ISDM을 다시 이미징하려면 다음 단계를 완료하십시오.

참고: 애플리케이션 파티션에서 모든 정보가 손실됩니다. 컨피그레이션을 유지하는 동안 IDSM에서 비밀번호 복구를 수행하는 데 사용할 수 있는 방법은 없습니다.

참고: 이 절차에서는 유지 관리 파티션을 사용해야 합니다. 유지 보수 파티션 암호가 변경되었고 로그인할 수 없는 경우 IDSM을 교체해야 합니다. 이 경우 Cisco 기술 지원에 문의하십시오.

1. switch 명령을 사용하여 IDSM을 Maintenance Partition(유지 관리 파티션)으로 부팅합니다. **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. IDSM이 switch 명령 **show module *x***와 함께 온라인 상태로 제공되는지 *확인합니다*.IDSM 소프트웨어 버전이 시작 부분에 2가 있는지 확인합니다. 이 버전은 유지 관리 파티션 소프트웨어가 현재 IDSM에서 실행되고 있으며 상태가 OK임을 나타냅니다.
```
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. 스위치 명령 **세션 *x***를 사용하여 유지 관리 파티션으로 부팅되었으므로 IDSM에 *연결합니다* .ciscoids/**attack**의 사용자 이름/비밀번호**를 사용합니다**.
```
ltd9-9> (enable)session 4
Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:
maintenance#
```
4. IDSM 애플리케이션 파티션을 다시 이미징하려면 캐시된 이미지를 설치합니다.diagnostics 명령 ids-installer **system /cache /show**를 사용하여 캐시된 이미지가 있는지 **확인합니다**.
```
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)#
```

캐시된 이미지가 없거나 캐시된 버전이 설치하려는 이미지가 아닌 경우 5단계로 진행합니다 .캐시된 이미지를 사용하는 ISDM을 다시 이미징하려면 diagnostics 명령 ids-installer **system /cache /install**을 사용합니다.

```
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:\!
```

리이미지가 완료되면 12단계로 진행합니다.

5. IDSM에 ping ip_*address* 명령 사용과 함께 IP 연결**이 *있는지 확인합니다*.**

```
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. IDSM에 IP 연결이 있는 경우 11단계로 진행합니다. IP 연결이 없는 경우 7단계부터 9단계까지 진행합니다.
7. **show port status *x*/2** 명령을 사용하여 Command and Control Interface가 스위치**에서** 제대로 구성되었는지 확인합니다.

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

8. diagnostics 명령 ids-installer netconfig **/view**를 사용하여 IDSM 유지 관리 파티션에서 통신 매개 변수**가** 올바르게 **구성되었는지 확인합니다**.

```
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. 설정된 매개 변수가 없거나 매개 변수 중 일부를 변경해야 하는 경우 diagnostics 명령 ids-installer netconfig /configure ***매개 변수를*** 사용합니다.

```
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. IDSM을 재설정한 후 IP Connectivity(IP 연결)를 다시 확인하여 변경 사항을 적용합니다.IP 연결이 여전히 문제인 경우 일반적인 IP 연결 문제에 따라 문제를 해결한 다음 11단계를 진행합니다.
11. IDSM 애플리케이션 파티션을 다시 이미징합니다. 진단 명령 ids-installer **시스템 /nw /install /server=*ip_address* /user=account /save={*yes/no*} /dir=*ftp_path* /prefix=*file_prefix*를** 사용하여 이미지를 다운로드합니다.*ip_address*는 FTP 서버의 IP 주소입니다.*account*는 FTP 서버에 로그인할 때 사용할 사용자 또는 계정 이름입니다.*저장*은 다운로드한 이미지의 복사본을

캐시된 복사본으로 저장할지 여부를 결정합니다. 예인 경우 기존의 캐시된 이미지를 덮어씁니다. no인 경우 다운로드한 이미지가 비활성 파티션에 설치되지만 캐시된 복사본은 저장되지 않습니다.*ftp_path*는 이미지 파일이 있는 FTP 서버의 디렉토리를 지정합니다.*file_prefix*는 다운로드한 이미지에 있는 .dat 파일의 파일 이름입니다. 다운로드한 이미지는 확장명이 .dat인 파일 하나와 확장명이 .cab인 파일 여러 개로 구성됩니다. file_prefix 값은 .dat 접미사를 포함하지 않는 DAT 파일의 이름이어야 합니다.

```
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. switch 명령을 사용하여 IDSM을 Application Partition(애플리케이션 파티션)으로 부팅합니다. **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.
```

또한 IDSM을 애플리케이션 파티션으로 부팅하기 위해 스위치가 구성되어 있는지 확인합니다. IU이 **확인을 하려면 show boot device *x*** 명령을 사용합니다.

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

IDSM에 대한 부팅 디바이스 변수를 구성하려면 switch configuration 명령 set boot device hdd:**1 *x*를** 사용합니다**.**

```
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. IDSM이 switch 명령 **show module *x***를 사용하여 온라인 상태로 제공되는지 *확인합니다*.IDSM 소프트웨어 버전이 애플리케이션 파티션 버전(예: *3.0(1)S4)*이고 상태가 OK인지 확인합니다.

```
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. 애플리케이션 파티션으로 부팅되었으므로 IDSM에 연결하고 디렉터와 통신할 수 있도록 구성합니다. 명령 **설정을 사용합니다**.ciscoids/attack의 사용자 이름/비밀번호**로 로그인합니다**.

```
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

관리자 사용자 이름/비밀번호를 알고 있는 경우 복구 절차

관리자 계정의 암호를 알고 있는 경우 이 사용자 계정을 사용하여 다른 사용자 암호를 재설정할 수 있습니다.

예를 들어, 이름이 'cisco'와 'adminuser'인 IDSM-2에 두 개의 사용자 이름이 구성됩니다. 'cisco' 사용자의 비밀번호를 재설정해야 하므로 'adminuser'가 로그인하고 비밀번호를 재설정합니다.

```
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#
```

서비스 사용자 이름/비밀번호를 알고 있는 경우 복구 절차

서비스 계정의 암호를 알고 있는 경우 이 사용자 계정을 사용하여 다른 사용자 암호를 재설정할 수 있습니다.

예를 들어, 이름이 'cisco', 'adminuser' 및 'serviceuser'인 IDSM-2에 세 개의 사용자 이름이 구성됩니다. 'cisco' 사용자의 비밀번호를 재설정해야 하므로 'serviceuser'가 로그인하고 비밀번호를 재설정합니다.

```
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#
```

참고: 루트 비밀번호는 서비스 계정의 비밀번호와 동일합니다.

네이티브 IOS(Integrated IOS) 코드를 실행하는 스위치와 함께 IDSM-2 이미지 조정

네이티브 IOS(Integrated IOS) 코드를 실행하는 스위치로 ISDM-2를 다시 이미징하려면 다음 단계를 완료하십시오.

참고: 애플리케이션 파티션에서 모든 정보가 손실됩니다. 컨피그레이션이 유지되는 동안 IDSM-2에서 비밀번호 복구를 수행하기 위해 사용할 수 있는 방법은 없습니다.

1. switch 명령 hw-module module *x* ***reset cf:1***을 사용하여 IDSM-2를 Maintenance Partition으로 부팅합니다. 여기서 *x*는 슬롯 번호를, cf는 'compact flash'를 나타냅니다.**참고:** cf:1을 사용하여 문제가 발생한 경우 hdd:2를 대안으로 사용하십시오.

```
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. IDSM-2가 switch 명령 **show module *x***를 사용하여 온라인 상태로 제공되는지 *확인합니다*.IDSM-2 소프트웨어 버전이 끝에 'm'이 있고 상태가 OK인지 확인하십시오.

```
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. 유지 관리 파티션으로 부팅되었으므로 IDSM-2에 연결합니다. switch 명령 **세션 슬롯 xprocessor 1을 사용합니다**.guest/cisco의 사용자 이름/비밀번호**를 사용합니다**.

```
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. IDSM-2에 IP 연결이 있는지 확인합니다. ping ip_*address* 명령을 *사용합니다.*

```
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. IDSM-2에 IP 연결이 있는 경우 14단계로 진행합니다.
6. Command and Control Interface(명령 및 제어 인터페이스)가 스위치에 올바르게 구성되어 있는지 확인합니다. **show run** 명령 사용 **| 침입 탐지**.

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

7. 통신 매개변수가 IDSM-2 Maintenance Partition에 올바르게 구성되어 있는지 확인합니다. show ip 명령을 **사용합니다**.

```
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. 설정된 매개변수가 없거나 일부 매개변수를 변경해야 하는 경우 모두 지웁니다. 명령 clear ip를 **사용합니다**.

```
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. IDSM-2 유지 관리 파티션에 IP 주소 및 마스크 정보를 구성합니다. ip **address** ip_*address 넷 마스크* 명령*을 사용합니다.*

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

10. IDSM-2 유지 관리 파티션에서 기본 게이트웨이를 구성합니다. **ip gateway** *gateway-address* 명령을 사용합니다.

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

11. IDSM-2 유지 관리 파티션에서 호스트 이름을 구성합니다. 명령 **ip 호스트** ***호스트 이름을 사용합니다.***이 작업은 필요하지 않지만, 이렇게 하면 프롬프트가 설정되므로 디바이스를 식별

하는 데 도움이 됩니다.

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

12. 브로드캐스트 주소를 명시적으로 구성해야 할 수도 있습니다. ip broadcast *broadcast-address* 명령*을 사용합니다.*기본 설정은 일반적으로 충분합니다.

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

13. IP 연결을 다시 확인합니다. IP 연결이 여전히 문제인 경우 일반적인 IP 연결 문제에 따라 문제를 해결하고 14단계를 계속 진행합니다.
14. IDSM-2 애플리케이션 파티션을 다시 이미징합니다. upgrade ftp-*url* ***—install*** 명령을 **사용합니다**.

```
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. IDSM-2를 애플리케이션 파티션으로 부팅합니다. switch 명령 hw-**module module module *x reset hdd*:1을 사용합니다**.

```
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.
```

또는 부팅 디바이스 변수가 올바르게 설정된 경우 IDSM-2에서 reset 명령을 사용할 수 있습니다.IDSM-2에 대한 부팅 디바이스 변수 설정을 확인하려면 switch 명령 **show bootvar device module *x*를** 사용합니다.

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

IDSM-2에 대한 부팅 디바이스 변수를 구성하려면 switch configuration 명령 **boot device module *x* hdd:1을** 사용합니다.

```
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
```

Maintenance Partition CLI를 통해 IDSM-2를 재설정하려면 명령 **reset**을 사용합니다.

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

16. IDSM-2가 온라인 상태인지 확인합니다. switch 명령 **show module *x*를 *사용합니다*.**IDSM-2

소프트웨어 버전이 응용 프로그램 파티션 버전인지(예: *4.1(1)S47)* 및 상태가 OK인지 확인합니다.

```
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. 애플리케이션 파티션으로 부팅되었으므로 IDSM-2에 연결합니다. switch 명령 **세션 슬롯 *x* 프로세서 1*을* 사용합니다.**cisco/cisco의 사용자 이름/비밀번호**를 사용합니다**.

```
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. IDSM-2를 구성합니다. 명령 **설정**을 사용합니다.

```
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#
```

CatOS(Hybrid) 코드를 실행하는 스위치가 있는 IDSM-2의 이미지 재작성

하이브리드(CatOS) 코드를 실행하는 스위치로 ISDM-2를 다시 이미징하려면 다음 단계를 완료하십시오.

1. IDSM-2를 Maintenance Partition(유지 관리 파티션)으로 부팅합니다. switch 명령을 사용하여 **reset *x* hdd:2를 사용합니다.참고: hdd**:2를 사용하여 문제가 발생하면 cf:1을 대안으로 사용하십시오.

```
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. IDSM-2가 온라인 상태인지 확인합니다. switch 명령 **show module *x*를 사용합니다.**IDSM-2 소프트웨어 버전이 끝에 'm'이 있는지 확인하고, 이는 유지 관리 파티션 소프트웨어가 현재 실행되고 있으며 상태가 OK임을 나타냅니다.

```
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. 유지 관리 파티션으로 부팅되었으므로 IDSM-2에 연결합니다. switch 명령 **세션 *x*를 사용합니다.**guest/cisco의 사용자 이름/비밀번호**를 사용합니다**.

```
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. IDSM-2에 IP 연결이 있는지 확인합니다. ping ip_*address* 명령을 *사용합니다.*

```
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. IDSM-2에 IP 연결이 있는 경우 14단계로 진행합니다.
6. Command and Control Interface(명령 및 제어 인터페이스)가 스위치에 올바르게 구성되어 있는지 확인합니다. **show port status *x*/2** 명령을 사용합니다.

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

7. 통신 매개변수가 IDSM-2 Maintenance Partition에 올바르게 구성되어 있는지 확인합니다. show ip 명령을 **사용합니다**.

```
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. 설정된 매개 변수가 없거나 매개 변수 중 일부를 변경해야 하는 경우 clear ip 명령을 사용하여 모든 매개 변수를 **지웁니다**.

```
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. IDSM-2 유지 관리 파티션에 IP 주소 및 마스크 정보를 구성합니다. 명령 **ip address *ip_address 넷마스크를 사용합니다.***

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

```
guest@localhost.localdomain#
```

10. IDSM-2 유지 관리 파티션에서 기본 게이트웨이를 구성합니다. **ip gateway** ***gateway-address*** 명령을 사용합니다.

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

11. IDSM-2 유지 관리 파티션에서 호스트 이름을 구성합니다. 명령 **ip 호스트** ***호스트 이름을 사용합니다.***이 작업은 필요하지 않지만, 이렇게 하면 프롬프트가 설정되므로 디바이스를 식별하는 데 도움이 됩니다.

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

12. 브로드캐스트 주소를 명시적으로 구성해야 할 수도 있습니다. ip broadcast *broadcast-address* 명령*을 사용합니다.*기본 설정은 일반적으로 충분합니다.

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

13. IP 연결을 다시 확인하십시오. IP 연결이 여전히 문제인 경우 일반적인 IP 연결 문제에 따라 문제를 해결한 다음 14단계를 진행합니다.
14. IDSM-2 애플리케이션 파티션을 다시 이미징합니다. upgrade ftp-*url* ***—install*** 명령을 **사용합니다**.

```
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. IDSM-2를 애플리케이션 파티션으로 부팅합니다. switch 명령을 사용하여 **reset** ***x*** **hdd:1을 사용합니다**.

```
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.
```

또는 부팅 디바이스 변수가 올바르게 설정된 경우 IDSM-2에서 reset 명령을 사용할 수 있습니다.IDSM-2에 대한 부팅 디바이스 변수 설정을 확인하려면 switch 명령 **show boot device** ***x를*** 사용합니다.

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

IDSM-2에 대한 부팅 디바이스 변수를 구성하려면 switch configuration 명령 set boot device hdd:**1** ***x를*** 사용합니다.

```
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
```

유지 관리 파티션 CLI를 통해 IDSM-2를 재설정하려면 명령 **reset**을 사용합니다.

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

16. IDSM-2가 온라인 상태인지 확인합니다. switch 명령 **show module *x*를 사용합니다.**IDSM-2 소프트웨어 버전이 애플리케이션 파티션 버전(예: *4.1(1)S47)*이고 상태가 OK인지 확인합니다.

```
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. 애플리케이션 파티션으로 부팅되었으므로 IDSM-2에 연결합니다. switch 명령 **세션 *x*를 사용합니다.**cisco/cisco의 사용자 이름/비밀번호**를 사용합니다**.

```
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. 명령 **설정**을 사용하여 IDSM-2를 **구성합니다**.

```
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#
```

관련 정보

- Cisco IDS UNIX Director
- Catalyst 6500 Series IDSM-1(Intrusion Detection System) Services Module
- Catalyst 6500 Series IDSM-2(Intrusion Detection System) Services Module
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems