Procedimiento de recuperación de contraseña para el sensor IDS y los Módulos de servicios IDS (IDSM-1, IDSM-2) de Cisco.

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Artefacto IDS versión 3
Recuperación de contraseña del ids appliance que funciona con la versión 3
Re-imagen del ids appliance que funciona con la versión 3
Artefacto IDS versión 4
Procedimiento de recuperación si se sabe el nombre de usuario del administrador/la contraseña
Procedimiento de recuperación si se sabe el nombre de usuario/la contraseña del servicio
Ids appliance de la re-imagen que funciona con la versión 4
Versión 5 y versión 6 del dispositivo IPS
La recarga, apaga, reajustó, y recupera el AIP-SSM
Nueva imagen la imagen del sistema AIP-SSM
IDSM
Re-imagen IDSM con el Switch que funciona con el código del Native IOS (IOS integrado)
Rehaga la imagen el IDSM con el Switch que funciona con el código híbrido (de CatOS)
ISDM-2
Procedimiento de recuperación si se sabe el nombre de usuario del administrador/la contraseña
Procedimiento de recuperación si se sabe el nombre de usuario/la contraseña del servicio
Rehaga la imagen el IDSM-2 con el Switch que funciona con el código del Native IOS (IOS integrado)
Rehaga la imagen para el IDSM-2 con el Switch que funciona con el código híbrido (de CatOS)
Información Relacionada

Introducción

Este documento proporciona procedimientos para recuperar su dispositivo Cisco Secure Intrusion Detection System (IDS) (antes NetRanger) y los módulos de todas las versiones.

prerrequisitos

Requisitos

Si un servidor FTP es necesario, debe apoyar al modo pasivo. Los Cdes de la recuperación se pueden obtener usando la Herramienta de actualización del producto (clientes registrados solamente).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Artefactos IDS versión 3 y 4
- Versiones 5 y 6 del dispositivo IPS
- Versión 3 del módulo IDS (IDSM) y versión 4 IDSM-2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Artefacto IDS versión 3

Dos opciones están disponibles para el dispositivo de la versión 3. Usted puede utilizar el proceso de recuperación de contraseña o usted puede hacer una re-imagen que utilice el CD de la recuperación de la versión 3. Observe que toda la información está perdida en una re-imagen. El procedimiento para recuperación de contraseña es esencialmente una recuperación de contraseña de Solaris. Utilice solamente esta opción si usted no tiene una estación de administración (Cisco Secure Policy Manager (CSPM), solución de administración de seguridad/VPN (VMS), el UNIX Director) de las cuales usted puede copiar la configuración.

Con el Artefacto IDS versión 3 y anterior, dos nombres de usuario existen “netrangr llamado” y “raíz”. La contraseña predeterminada para ambas es “ataque”.

Recuperación de contraseña del ids appliance que funciona con la versión 3

Estos archivos son necesarios para recuperar su contraseña.

- Disco del Asistente. de la configuración del dispositivo de Solaris (disco de arranque). Usted puede descargar los archivos del sitio Web de soporte técnico de Sun .**Nota:** Si este link no trabaja, intentar ir al nivel superior del sitio Web de soporte técnico de Sun y buscar para las *descargas del driver de Solaris del disquete de arranque del ayudante de configuración del dispositivo* bajo los drivers. El Cisco Systems, Inc. no mantiene el sitio Web de soporte técnico de Sun y no tiene ningún control sobre donde se localiza el contenido.
- Solaris para el CD-ROM de Intel (x86).
- Acceso a la consola al puesto de trabajo.

Complete estos pasos para recuperar la contraseña.

1. Inserte el disco de arranque.
2. Inserte el CD en el unidad de Cd-ROM.
3. Apague el puesto de trabajo, espere diez segundos, y gírelos.Los arranques del sistema del disco de arranque. Después de una cierta configuración, las visualizaciones de la pantalla del ayudante de configuración inicial.
4. Presione el **F3** para hacer una exploración parcial del sistema para los dispositivos de arranque.Cuando se acaba la exploración, una lista de visualizaciones de los dispositivos.
5. Aseegurese el dispositivo CD-ROM aparece en la lista de dispositivos, y después presiona el **F2** para continuar.Visualizaciones de la pantalla una lista de dispositivos de arranque.
6. Seleccione el **unidad de Cd-ROM**, y después presione la barra de espacio.Hay un “X” al lado del dispositivo CD-ROM.
7. Presione el **F2** para continuar.El puesto de trabajo ahora inicia del CD-ROM.
8. En la pantalla usada para seleccionar un tipo de instale, elija la **opción 2, Jumpstart**.El sistema continúa iniciando.
9. En el prompt para seleccionar un lenguaje, elija la **opción 0** para el inglés.
10. En la siguiente pantalla para los lenguajes, elija la **opción 0** otra vez para el ANSI inglés.El sistema continúa iniciando y la pantalla de la instalación de Solaris aparece.
11. Presione y sostenga el **C de la tecla de control** y del tipo para parar la secuencia de comandos de instalación y no prohibirle el acceso al prompt.
12. **Soporte del** tipo **- Ufs /dev/dsk/c0t0d0s0 /mnt F.**“/” División ahora se monta en la punta de soporte “/mnt”. Aquí de usted puede editar el archivo “/etc/shadow” y quitar la contraseña de raíz.
13. Teclee **/mnt/etc cd**.
14. Fije entorno de shell así que usted puede leer los datos correctamente.Tipo **TERM=ansi**.**TÉRMINO de la exportación del** tipo.
15. **Sombra del** tipo **VI**.Usted ahora está en el archivo de la sombra y puede quitar la contraseña. La entrada necesita ser:
    `root:gNyqp8ohdfxPI:10598::::::` “: ” es un Separador de campo y la contraseña encriptada es el segundo campo.
16. Borre el segundo campo. Por ejemplo,`root:gNyqp8ohdfxPI:10598::::::`se cambia a **`root::10598::::::.`** Esto quita la contraseña para el usuario raíz.
17. Tipo: **¡wq!** para escribir y salir el archivo.
18. Quite el disco y el CD-ROM de las unidades.
19. Teclee el **init 6** para reiniciar el sistema.
20. Teclee la **raíz** en el login: pronto y entonces Presione ENTER.
21. Presione ENTER en el prompt de contraseña.Le ahora abren una sesión al sensor del Cisco Secure IDS.

Re-imagen del ids appliance que funciona con la versión 3

Complete estos pasos para rehacer la imagen el ids appliance que funciona con la versión 3.

Nota: Asegúrese que un ratón no esté conectado con el sensor antes de que usted proceda.

1. Inserte el CD de la recuperación de la versión 3 en el ids appliance y reinicielo.
2. Siga los prompts basados en su configuración hasta que la recuperación sea acertada.
3. Inicie sesión usando el nombre de usuario/contraseña predeterminado de la “raíz/del ataque”.

4. **Sysconfig-sensor** funcionado con para configurar de nuevo el dispositivo.

Artefacto IDS versión 4

Procedimiento de recuperación si se sabe el nombre de usuario del administrador/la contraseña

Si una contraseña para una cuenta del administrador se sabe, esta cuenta de usuario se puede utilizar para reajustar otras contraseñas del usuario.

Por ejemplo, dos nombres de usuario se configuran en el ids appliance llamado “Cisco” y “adminuser”. La contraseña para el usuario “Cisco” necesita ser reajustada, así que el “adminuser” abre una sesión y reajusta la contraseña.

```
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#
```

Procedimiento de recuperación si se sabe el nombre de usuario/la contraseña del servicio

Si una contraseña para la Cuenta de servicio se sabe, esta cuenta de usuario se puede utilizar para reajustar otras contraseñas del usuario.

Por ejemplo, tres nombres de usuario se configuran en el ids appliance nombrado “Cisco”, “adminuser”, y “serviceuser”. La contraseña para el usuario “Cisco” necesita ser reajustada, así que el “serviceuser” abre una sesión y reajusta la contraseña.

```
sv8-4-ids4250 login: tacPassword:
!--- Output is suppressed. bash-2.05a$ su root Password: [root@sv8-4-ids4250 serviceuser]#passwd
cisco Changing password for user cisco. New password: Retype new password: passwd: all
authentication tokens updated successfully. [root@sv8-4-ids4250 serviceuser]#exit exit bash-
2.05a$ exit logout sv8-4-ids4250 login: cisco Password: !--- Output is suppressed. sv8-4-
ids4250#
```

Nota: La contraseña de raíz es lo mismo que la contraseña de la Cuenta de servicio.

Ids appliance de la re-imagen que funciona con la versión 4

Complete estos pasos para rehacer la imagen el ids appliance.

Nota: Asegúrese que un ratón no esté conectado con el sensor antes de que usted proceda.

1. Inserte el CD de la recuperación de la versión 4 en el ids appliance y reinicielo.
2. Siga los prompts basados en su configuración hasta que la recuperación sea acertada.
3. Inicie sesión usando el nombre de usuario/contraseña predeterminado que es “Cisco/Cisco”.
4. Funcione con la **configuración** para configurar de nuevo el dispositivo.

Versión 5 y versión 6 del dispositivo IPS

La recarga, apaga, reajustó, y recupera el AIP-SSM

Utilice estos comandos de recargar, apagado, restauración, de recuperar la contraseña, y de recuperar el módulo de Servicios de seguridad avanzado del examen y de la prevención (AIP-SSM) directamente del dispositivo de seguridad adaptante:

Nota: Usted puede ingresar los **comandos hw-module del** modo EXEC privilegiado o del modo de configuración global. Usted puede ingresar los comandos en el solo modo ruteado y el solo modo transparente. Para los dispositivos de seguridad adaptantes que actúan en con varios modos de funcionamiento (con varios modos de funcionamiento ruteada o transparente) usted puede ejecutar solamente los **comandos hw-module del** contexto del sistema (no de los contextos del administrador o del usuario).

- **recarga del** *slot_number del* **módulo del módulo del hw** — Este comando recarga el software en el AIP-SSM sin hacer un reinicio de hardware. Es eficaz solamente cuando el AIP-SSM está en el estado ascendente.
- *el slot_number del* **módulo del módulo del hw apaga** — Este comando apaga el software en el AIP-SSM. Es eficaz solamente cuando el AIP-SSM está en el estado ascendente.
- *slot_number del* **módulo del módulo del hw reajustado** — Este comando realiza un reinicio de hardware del AIP-SSM. Es aplicable cuando el indicador luminoso LED amarillo de la placa muestra gravedad menor está en los estados Up/Down/Unresponsive/Recover.
- **contraseña-restauración del** *slot_number del* **módulo del módulo del hw** — Este comando recupera una contraseña en las 5500 Series el módulo de Servicios de seguridad contento de la Seguridad de Cisco un ASA y del control (CSC-SSM) o el AIP-SSM sin tener que rehacer la imagen el dispositivo.**Nota:** Este comando enciende el soporte de IPS 6.0 (versión ASA 7.2) y se utiliza para restablecer la contraseña de la cuenta del CLI de Cisco al **Cisco** predeterminado.
- *el slot_number del* **módulo del módulo del hw se recupera [inicio | pare | configuración]** — el comando de la **recuperación** visualiza un conjunto de las opciones interactivas para fijar o cambiar los parámetros de la recuperación. Usted puede cambiar el parámetro o guardar la configuración existente cuando usted Presione ENTER.Para el procedimiento que usted utiliza para recuperar el AIP-SSM, vea instalar la imagen del sistema AIP-SSM.*el slot_number del* **módulo del módulo del hw recupera el inicio** — Este comando inicia la recuperación del AIP-SSM. Es aplicable solamente cuando AIP-SSM está en el estado ascendente.*el slot_number del* **módulo del módulo del hw recupera la parada** — Este comando para la recuperación del AIP-SSM. Es aplicable solamente cuando el AIP-SSM está en el estado de la recuperación.**Nota:** Si la recuperación AIP-SSM necesita ser parada, usted debe publicar el **módulo 1 del módulo del hw recupera el comando stop** en el plazo de 30 a 45 segundos después de que usted comienza la recuperación AIP-SSM. Si usted espera más de largo, puede llevar a las consecuencias inesperadas. Por ejemplo, el AIP-SSM pudo subir en el estado insensible.**el módulo 1 del módulo del hw recupera la configuración** — Utilice este comando de configurar los parámetros para la recuperación del módulo. Los parámetros esenciales son la ubicación de la dirección IP y de la imagen de recuperación TFTP URL.Ejemplo:

```
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]:
```

Nueva imagen la imagen del sistema AIP-SSM

Complete estos pasos para instalar la imagen del sistema AIP-SSM:

1. Inicie sesión al ASA.
2. Ingrese el enable mode:`asa>enable`
3. Configure las configuraciones de la recuperación para el AIP-SSM:`asa#hw-module module 1 recover configure` **Nota:** Si usted hace un error en la configuración de la recuperación, utilice el **módulo 1 del módulo del hw recuperan el comando stop** de parar el sistema reimaging y entonces usted puede corregir la configuración.
4. Especifique el TFTP URL para la imagen del sistema:`Image URL [tftp://0.0.0.0/]:` Ejemplo:`Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img`
5. Especifique el comando y la interfaz de control del AIP-SSM:`Port IP Address [0.0.0.0]:`Ejemplo:`Port IP Address [0.0.0.0]: 10.89.149.231`
6. Deje el VLAN ID en 0. `VLAN ID [0]:`
7. Especifique el default gateway del AIP-SSM:`Gateway IP Address [0.0.0.0] :`Ejemplo:`Gateway IP Address [0.0.0.0]:10.89.149.254`
8. Ejecute la recuperación:`asa#hw-module module 1 recover boot`
9. Marque periódicamente la recuperación hasta que sea completa:**Nota:** El estatus lee guest@localhost.localdomain # durante la recuperación y lee guest@localhost.localdomain # cuando el reimaging es completo.`asa#show module 1 Mod Card Type Model Serial No. --- ----- ------------------------------------ ------------------ ----------- 0 ASA 5540 Adaptive Security Appliance ASA5540 P2B00000019 1 ASA 5500 Series Security Services Module-20 ASA-SSM-20 P1D000004F4 Mod MAC Address Range Hw Version Fw Version Sw Version --- ------------ ------------------- ------------ ------------ --------------- 0 000b.fcf8.7b1c to 000b.fcf8.7b20 0.2 1.0(7)2 7.0(0)82 1 000b.fcf8.011e to 000b.fcf8.011e 0.1 1.0(7)2 5.0(0.22)S129.0 Mod Status --- ------------------ 0 Up Sys 1 Up asa#` **Nota:** Para hacer el debug de cualquier error que pudiera suceder en el proceso de recuperación, utilice el comando del **arranque del módulo del debug** de habilitar el debugging del proceso reimaging del sistema.
10. La sesión al AIP-SSM e inicializa el AIP-SSM con el **comando setup**.

IDSM

No hay método que usted puede utilizar para realizar una recuperación de contraseña en el IDSM mientras que se conserva la configuración.

Nota: Este procedimiento requiere el uso de la división del mantenimiento. Si se ha cambiado la contraseña de partición del mantenimiento y usted no puede iniciar sesión, el IDSM necesita ser substituido. En este caso, Soporte técnico de Cisco del contacto para la ayuda.

Rehaga la imagen el IDSM con el Switch que funciona con el código del Native IOS (IOS integrado)

Complete estos pasos para rehacer la imagen el ISDM con un Switch que funcione con el código del Native IOS (IOS integrado).

1. Inicie el IDSM a la división del mantenimiento usando el **módulo hdd:2 reajustado** *x del* **módulo del hw del** comando switch donde significa *x el* número de slot.`SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- ------------------------------------ ----------- ------------ ----------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------------------------------- ------ ------------ ------ ------ ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok SV9-1#hw-module module 6 reset hdd:2 Device BOOT variable for reset = Warning: Device list is not verified.`

```
Proceed with reload of module? [confirm]y % reset issued for module 6 !--- Output
suppressed.
```

2. Marque que el IDSM viene en línea usando el **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM tiene 2 localizados al principio que indica que el software de partición de mantenimiento se ejecuta actualmente en el IDSM y que el estatus es ACEPTABLE.`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. Conecte con la división del mantenimiento IDSM usando el **procesador 1. del slot** *x de la* **sesión del** comando switch.Utilice el nombre de usuario/la contraseña del **ciscoids/ataque**.`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. Instale la imagen ocultada para rehacer la imagen la partición de aplicación IDSM.Publique el **sistema /cache /show del** comando ids-installer de los diagnósticos para verificar que existe la imagen ocultada.`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)#` Si existe ninguna imagen ocultada o la versión ocultada no es la que usted quiere instalar, proceda al paso 5.Para rehacer la imagen el ISDM usando la imagen ocultada, utilice el **sistema /cache /install del** comando ids-installer de los diagnósticos.`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:\!` La re-imagen ha completado, procede una vez al paso 12.
5. Aseegurese que el IDSM tiene conectividad del IP. Publique el comando ping ip_address.`maintenance#`**`diag`** `maintenance(diag)#`**`ping 10.66.84.1`** `Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255`
6. Si el IDSM tiene conectividad del IP, proceda al paso 11. Si usted no tiene conectividad del IP, proceda con los pasos 7 a 9.
7. Aseegurese que el comando y la interfaz de control está configurado correctamente en el Switch. Publique el comando show run interface Gigx/2.`SV9-1#`**`show run interface Gig6/2`** `Building configuration... Current configuration : 115 bytes ! interface GigabitEthernet6/2 no ip address switchport switchport access vlan 210 switchport mode access end SV9-1#`
8. Aseegurese que los parámetros de comunicación están configurados correctamente en la división del mantenimiento IDSM. Publique el **netconfig /view del** comando ids-installer de los diagnósticos.`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. Si no se fija ningunos de los parámetros, o si alguno de ellos necesidad de ser cambiado, utilice los *parámetros de* **/configure del netconfig del** comando ids-installer de los diagnósticos.`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. Conectividad del IP del control otra vez después de que usted haya reajustado el IDSM para que los cambios tomen el efecto. Si la conectividad del IP sigue siendo un problema,

resuelva problemas según un problema de conectividad IP normal, después proceda con el paso 11.

11. Rehaga la imagen la partición de aplicación IDSM. Descargue la imagen usando el **=account /save de** */user de los* **=ip_address del sistema /nw /install /server del ids-instalador del** comando diagnostic **= =file_prefix {***sí/no***} de /prefix del =ftp_path de /dir** donde:*los ip_address* son la dirección IP del servidor FTP.*la cuenta* es el usuario o el nombre de la cuenta que se utilizarán al registrar en el servidor FTP.*salve* determina si salvar una copia de la imagen descargada como la copia ocultada. Si sí, cualquier imagen ocultada que exista está sobregrabada. Si ningún, la imagen descargada está instalada en la partición desactivada pero una copia ocultada no se guarda.*el ftp_path* especifica el directorio en el servidor FTP donde se localizan los archivos de imagen.*el file_prefix* es el nombre del archivo del archivo del .dat en la imagen descargada. La imagen descargada consiste en un archivo con la extensión del .dat y varios archivos con la extensión .cab. El valor del file_prefix necesita ser el nombre del archivo DAT, hasta pero no incluyendo el sufijo del .dat.`maintenance#diag maintenance(diag)#ids-installer system /nw /install /server=10.66.64.10 /user=cisco /save=yes /dir='/tftpboot/georgia' / prefix=IDSMk9-a-3.0-1-S4 Please enter login password: ***** Downloading the image.. File 05 of 05 FTP STATUS: Installation files have been downloaded successfully ! Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is 2407-F686 Extracting the image... !--- Output is suppressed. STATUS: Image has been successfully installed on drive C:\!`
12. Inicie el IDSM a la partición de aplicación usando el **módulo hdd:1 reajustado x del módulo del hw del** comando switch.`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.` También asegúrese de que el Switch esté configurado para iniciar encima del IDSM en la partición de aplicación. Para marcar esto, utilice el **device module** *x. del* comando show bootvar.`SV9-1#show bootvar device module 6 [mod:6 ]: SV9-1#` Para configurar la variable del dispositivo de arranque para el IDSM, utilice el **módulo x hdd:1 del dispositivo de arranque del** comando switch configuration.`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. Marque que el IDSM viene en línea usando el **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM es una versión de la partición de aplicación, por ejemplo *3.0(1)S4*, y que el estatus es ACEPTABLE.`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. Conecte con el IDSM ahora que ha iniciado para arriba en la partición de aplicación y configurela así que puede comunicar al director. Utilice el comando setup.La comunicación con el director se ha establecido una vez, configuración se puede descargar al IDSM.Utilice el nombre de usuario/la contraseña del **ciscoids/ataque** para iniciar sesión.`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.
```

Rehaga la imagen el IDSM con el Switch que funciona con el código híbrido (de CatOS)

Complete estos pasos para rehacer la imagen el ISDM con un Switch que funcione con el código híbrido (de CatOS).

Nota: Toda la información se pierde en la partición de aplicación. No hay método que usted puede utilizar para realizar una recuperación de contraseña en el IDSM mientras que usted conserva la configuración.

Nota: Este procedimiento requiere el uso de la división del mantenimiento. Si se ha cambiado la contraseña de partición del mantenimiento y usted no puede iniciar sesión, el IDSM necesita ser substituido. En este caso, Soporte técnico de Cisco del contacto para la ayuda.

1. Inicie el IDSM a la división del mantenimiento con la **restauración** *x* **hdd:2 del** comando switch.`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. Marque que el IDSM viene en línea con el **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM tiene 2 localizados al principio que indica que el software de partición de mantenimiento se ejecuta actualmente en el IDSM y que el estatus es ACEPTABLE.`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. Conecte con el IDSM ahora que ha iniciado para arriba en la división del mantenimiento con la **sesión** *x. del* comando switch.Utilice el nombre de usuario/la contraseña del **ciscoids/ataque**.`ltd9-9> (enable)session 4 Trying IDS-4... Connected to IDS-4. Escape character is '^]'. login: ciscoids Password: maintenance#`

4. Instale la imagen ocultada para rehacer la imagen la partición de aplicación IDSM.Verifique que la imagen ocultada exista con el uso del **sistema /cache /show del** comando ids-installer de los diagnósticos.`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)#` Si existe ninguna imagen ocultada, o la versión ocultada no es la que usted quiere instalar, proceda al paso 5.Para rehacer la imagen el ISDM que utiliza la imagen ocultada, utilice el **sistema /cache /install del** comando ids-installer de los diagnósticos.`maintenance(diag)#**ids-installer system /cache /install** Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is E41E-3608 Extracting the image... *!--- Output is suppressed.* STATUS: Image has been successfully installed on drive C:\!` Una vez que la nueva imagen ha completado, proceda al paso 12.
5. Aseegurese que el IDSM tiene conectividad del IP con el uso del comando ping ip_address.`maintenance#**diag** maintenance(diag)#**ping 10.66.84.1** Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255`
6. Si el IDSM tiene conectividad del IP, proceda al paso 11. Si usted no tiene conectividad del IP, proceda con los pasos 7 a 9.
7. Aseegurese que el comando y la interfaz de control está configurado correctamente en el Switch con el uso del comando show port status x/2.`ltd9-9> (enable)**show port status 4/2** Port Name Status Vlan Duplex Speed Type ----- ------------------- ---------- ---------- ---- ----- ----- ------------ 4/2 connected 1 full 1000 Intrusion De`
8. Aseegurese que los parámetros de comunicación están configurados correctamente en la división del mantenimiento IDSM con el uso el **netconfig /view del** comando ids-installer de los diagnósticos.`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. Si no se fija ningunos de los parámetros, o si alguno de ellos necesidad de ser cambiado, utilice los *parámetros de* **/configure del netconfig del** comando ids-installer de los diagnósticos.`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. Conectividad del IP del control otra vez después de que usted haya reajustado el IDSM para que los cambios tomen el efecto.Si la conectividad del IP sigue siendo un problema, resuelva problemas según un problema de conectividad IP normal, después proceda con el paso 11.
11. Rehaga la imagen la partición de aplicación IDSM. Descargue la imagen con el uso del **=account /save de /user de los =ip_address del sistema /nw /install /server del ids-instalador del** comando diagnostic **= =file_prefix {*sí/no*} de /prefix del =ftp_path de /dir** donde:*los ip_address* son la dirección IP del servidor FTP.*la cuenta* es el usuario o el nombre de la cuenta que se utilizarán al registrar en el servidor FTP.*salve* determina si salvar una copia de la imagen descargada como la copia ocultada. Si sí, cualquier imagen ocultada existente está sobregrabada. Si ningún, la imagen descargada está instalada en la partición desactivada pero una copia ocultada no se guarda.*el ftp_path* especifica el directorio en el servidor FTP donde se localizan los archivos de imagen.*el file_prefix* es el nombre del archivo del archivo del .dat en la imagen descargada. La imagen descargada consiste en un archivo con la extensión del .dat y varios archivos con la extensión .cab. El valor del file_prefix debe ser el nombre del archivo DAT, hasta pero no incluyendo el sufijo

del .dat.`maintenance#`**`diag`** `maintenance(diag)#`**`ids-installer system /nw /install /server=10.66.64.10 /user=cisco /save=yes /dir='/tftpboot/georgia'`** `/prefix=IDSMk9-a-3.0-1-S4 Please enter login password: ***** Downloading the image.. File 05 of 05 FTP STATUS: Installation files have been downloaded successfully! Validating integrity of the image... PASSED! Formatting drive C:\....Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is 2407-F686 Extracting the image... !--- Output is suppressed. STATUS: Image has been successfully installed on drive C:\!`

12. Inicie el IDSM a la partición de aplicación con el uso de la **restauración *x* hdd:1 del** comando switch.`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.` También aseegurese que el Switch está configurado para iniciar encima del IDSM en la partición de aplicación. IUse el comando show boot device x para marcar esto.`ltd9-9> (enable)`**`show boot device 4`** `Device BOOT variable =` Para configurar la variable del dispositivo de arranque para el IDSM, utilice el **dispositivo de arranque determinado hdd:1** *x. del* comando switch configuration.`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. Marque que el IDSM viene en línea con el uso del **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM es una versión de la partición de aplicación, por ejemplo, *3.0(1)S4*, y que el estatus es ACEPTABLE.`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. Conecte con el IDSM ahora que ha iniciado para arriba en la partición de aplicación y configurela así que puede comunicar al director. Utilice el comando setup.Inicie sesión con el nombre de usuario/la contraseña del **ciscoids/ataque**.`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

Procedimiento de recuperación si se sabe el nombre de usuario del administrador/la contraseña

Si una contraseña para una cuenta del administrador se sabe, esta cuenta de usuario se puede utilizar para reajustar otras contraseñas del usuario.

Por ejemplo, dos nombres de usuario se configuran en el “Cisco nombrado IDSM-2” y el “adminuser”. La contraseña para el usuario “Cisco” necesita ser reajustada, así que el “adminuser” abre una sesión y reajusta la contraseña.

```
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#
```

Procedimiento de recuperación si se sabe el nombre de usuario/la contraseña del servicio

Si una contraseña para la Cuenta de servicio se sabe, esta cuenta de usuario se puede utilizar para reajustar otras contraseñas del usuario.

Por ejemplo, tres nombres de usuario se configuran en el “Cisco nombrado IDSM-2”, el “adminuser”, y el “serviceuser”. La contraseña para el usuario “Cisco” necesita ser reajustada, así que el “serviceuser” abre una sesión y reajusta la contraseña.

```
SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type
'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: serviceuser
Password: !--- Output is suppressed. bash-2.05a$ su root Password: [root@idsm2-sv-rack
serviceuser]#passwd cisco Changing password for user cisco. New password: Retype new password:
passwd: all authentication tokens updated successfully. [root@idsm2-sv-rack serviceuser]# exit
exit bash-2.05a$ exit logout [Connection to 127.0.0.61 closed by foreign host] SV9-1#session
slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit' at the
remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: !--- Output
is suppressed. idsm2-sv-rack#
```

Nota: La contraseña de raíz es lo mismo que la contraseña de la Cuenta de servicio.

Rehaga la imagen el IDSM-2 con el Switch que funciona con el código del Native IOS (IOS integrado)

Complete estos pasos para rehacer la imagen el ISDM-2 con un Switch que funcione con el código del Native IOS (IOS integrado).

Nota: Toda la información se pierde en la partición de aplicación. No hay método que usted puede utilizar para realizar una recuperación de contraseña en el IDSM-2 mientras que se conserva la configuración.

1. Inicie el IDSM-2 a la división del mantenimiento con el uso del **módulo cf:1 reajustado** *x del* **módulo del hw del** comando switch donde significa *x* Flashes compacta de la significa del

número de slot y de los cf los ".**Nota:** Si un problema se encuentra usando cf:1, intente utilizar hdd:2 como alternativa.SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- ---------- ---------- ---------- 6 8 Intrusion Detection System WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ---------- ---------- ---------- ------ 6 0030.f271.e3fd to 0030.f271.e404 0.102 7.2(1) 4.1(1)S47 Ok Mod Sub-Module Model Serial Hw Status --- ---------- ---------- ---------- ------- 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 Ok Mod Online Diag Status --- ---------- 6 Pass SV9-1#**hw-module module 6 reset cf:1** Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y % reset issued for module 6 *!--- Output is suppressed.*

2. Marque que el IDSM-2 viene en línea con el uso del **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM-2 tiene "m" situado en el extremo y que el estatus es ACEPTABLE.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. Conecte con el IDSM-2 ahora que ha iniciado para arriba en la división del mantenimiento. Utilice el comando switch **session slot xprocessor 1.**Utilice el nombre de usuario/la contraseña del invitado**/el 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. Aseegurese que el IDSM-2 tiene conectividad del IP. Utilice el comando 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. Si el IDSM-2 tiene conectividad del IP, proceda al paso 14.
6. Aseegurese que el comando y la interfaz de control está configurado correctamente en el Switch. Utilice el comando show run **| detección de intrusos inc.**SV9-1#**show run | inc intrusion-detection** intrusion-detection module 6 management-port access-vlan 210
7. Aseegurese que los parámetros de comunicación están configurados correctamente en la división del mantenimiento IDSM-2. Utilice el comando show ip.guest@idsm2-sv-rack.local domain#**show ip** IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP Broadcast : 10.66.79.223 DNS Name : idsm2-sv-rack.localdomain Default Gateway : 10.66.79.193Nameserver(s) :
8. Si no se fija ningunos de los parámetros, o si alguno de ellos necesidad de ser cambiado, claro ellos todos. Utilice el comando clear ip.guest@idsm2-sv-rack.localdomain#**clear ip** guest@localhost.localdomain#**show ip** IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0 Nameserver(s) :
9. Configure la dirección IP y la información de máscara en la división del mantenimiento IDSM-2. Utilice el comando ip address ip_address netmask.guest@localhost.localdomain#**ip address 10.66.79.210 255.255.255.224**
10. Configure el default gateway en la división del mantenimiento IDSM-2. Utilice el comando ip gateway gateway-address.guest@localhost.localdomain#**ip gateway 10.66.79.193**
11. Configure el nombre de host en la división del mantenimiento IDSM-2. Utilice el comando ip host hostname.Aunque esto no sea necesario, ayuda a identificar el dispositivo puesto que éste también fija el prompt.guest@localhost.localdomain#**ip host idsm2-sv-rack** guest@idsm2-

sv-rack.localdomain#

12. Usted puede ser que necesite posiblemente configurar a su dirección de broadcast explícitamente. Utilice el comando ip broadcast broadcast-address.La configuración predeterminada es suficiente generalmente.guest@idsm2-sv-rack.localdomain#**ip broadcast 10.66.79.223**
13. Marque la conectividad del IP otra vez. Si la conectividad del IP sigue siendo un problema, resuelva problemas según un problema de conectividad IP normal y proceda con el paso 14.
14. Rehaga la imagen la partición de aplicación IDSM-2. Utilice el comando upgrade FTP-*URL* **--instale**.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. Inicie el IDSM-2 a la partición de aplicación. Utilice el **módulo hdd:1 reajustado** *x del* **módulo del hw del** comando switch.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.* Alternativamente, usted puede utilizar el **comando reset** en el IDSM-2 mientras la variable del dispositivo de arranque se fije correctamente.Para marcar la configuración de la variable del dispositivo de arranque para el IDSM-2, utilice el **device module bootvar** *x. de la* **demostración del** comando switch.SV9-1#**show bootvar device module 6** [mod:6]: SV9-1# Para configurar la variable del dispositivo de arranque para el IDSM-2, utilice el **módulo** *x* **hdd:1 del dispositivo de arranque del** comando switch configuration.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 Para reajustar el IDSM-2 vía la división CLI del mantenimiento, utilice el comando reset.guest@idsm2-sv-rack.localdomain#**reset** *!--- Output is suppressed.*
16. Marque que viene el IDSM-2 en línea. Utilice el **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM-2 es una versión de la partición de aplicación, por ejemplo *4.1(1)S47* y que el estatus es ACEPTABLE.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. Conecte con el IDSM-2 ahora que ha iniciado para arriba en la partición de aplicación. Utilice el **procesador 1. del slot** *x de la* **sesión del** comando switch.Utilice el nombre de usuario/la contraseña de **Cisco/de 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. Configure el IDSM-2. Utilice el comando setup.sensor#**setup** --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current

```
Configuration:networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway
10.1.9.1 hostname sensor telnet Option disabled accessList ipAddress 10.0.0.0 netmask
255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service
webServer general ports 443 exit exit Current time: Sat Sep 20 23:34:53 2003 Setup
Configuration last modified: Sat Sep 20 23:32:38 2003 Continue with configuration
dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]:
10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default
gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server
port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The
following configuration was entered. networkParams ipAddress 10.66.79.210 netmask
255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress
10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit
exit service webServer general ports 443 exit exit [0] Go to the command prompt without
saving this config. [1] Return back to the setup without saving this config. [2] Save this
configuration and exit setup.Enter your selection [2]:Configuration Saved. sensor#
```

Rehaga la imagen para el IDSM-2 con el Switch que funciona con el código híbrido (de CatOS)

Complete estos pasos para rehacer la imagen el ISDM-2 con un Switch que funcione con el código híbrido (de CatOS).

1. Inicie el IDSM-2 en la división del mantenimiento. Utilice la **restauración** *x* **hdd:2 del** comando switch.**Nota:** Si un problema se encuentra usando hdd:2, intente utilizar cf:1 como alternativa.`SV9-1> (enable)`**`show module 6`** `Mod Slot Ports Module-Type Model Sub Status --- --- - ----- ------------------------- ------------------- --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- ------------------- --- -------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ---------------------------------- --- ------ ---------- ----------------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47 Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ---------------------- - ------------------ ----------- ------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 SV9-1> (enable)`**`reset 6 hdd:2`** `This command will reset module 6. Unsaved configuration on module 6 will be lost Do you want to continue (y/n) [n]? y Module 6 shut down in progress, please don't remove module until shutdown completed.` *`!--- Output is suppressed.`*
2. Marque que viene el IDSM-2 en línea. Utilice el **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM-2 tiene “m” situado en el extremo que indica que los funcionamientos del software de partición de mantenimiento actualmente y que el estatus es ACEPTABLE.`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. Conecte con el IDSM-2 ahora que ha iniciado para arriba en la división del mantenimiento. Utilice la **sesión** *x. del* comando switch.Utilice el nombre de usuario/la contraseña del invitado**/el 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. Aseegurese que el IDSM-2 tiene conectividad del IP. Utilice el comando 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. Si el IDSM-2 tiene conectividad del IP, proceda al paso 14.
6. Aseegurese que el comando y la interfaz de control está configurado correctamente en el Switch. Utilice el comando show port status x/2.`SV9-1> (enable)`**`show port status 6/2`** `Port Name Status Vlan Duplex Speed Type ----- ------------------- ---------- ---------- ------ ----- ------------ 6/2 connected 210 full 1000 Intrusion De`
7. Aseegurese que los parámetros de comunicación están configurados correctamente en la división del mantenimiento IDSM-2. Utilice el comando show ip.`guest@idsm2-sv-rack.localdomain#`**`show ip`** `IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP Broadcast : 10.255.255.255 DNS Name : idsm2-sv-rack.localdomain Default Gateway : 10.66.79.193 Nameserver(s) :`
8. Si no se fija ningunos de los parámetros o si alguno de ellos necesidad de ser cambiado, claro ellos todos con el uso del comando clear ip.`guest@idsm2-sv-rack.localdomain#`**`clear ip`** `guest@localhost.localdomain#`**`show ip`** `IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0`
9. Configure la dirección IP y la información de máscara en la división del mantenimiento IDSM-2. Utilice el comando ip address ip_address netmask.`guest@localhost.localdomain#`**`ip address 10.66.79.210 255.255.255.224`** `guest@localhost.localdomain#`
10. Configure el default gateway en la división del mantenimiento IDSM-2. Utilice el comando ip gateway gateway-address.`guest@localhost.localdomain#`**`ip gateway 10.66.79.193`** `guest@localhost.localdomain#`
11. Configure el nombre de host en la división del mantenimiento IDSM-2. Utilice el comando ip host hostname.Aunque esto no sea necesario, ayuda a identificar el dispositivo puesto que éste también fija el prompt.`guest@localhost.localdomain#`**`ip host idsm2-sv-rack`** `guest@idsm2-sv-rack.localdomain#`
12. Usted puede ser que necesite posiblemente configurar a su dirección de broadcast explícitamente. Utilice el comando ip broadcast broadcast-address.La configuración predeterminada es suficiente generalmente.`guest@idsm2-sv-rack.localdomain#`**`ip broadcast 10.66.79.223`**
13. Conectividad del IP del control otra vez. Si la conectividad del IP sigue siendo un problema, el Troubleshooting según un problema de conectividad IP normal después procede con el paso 14.
14. Rehaga la imagen la partición de aplicación IDSM-2. Utilice el comando upgrade FTP-*URL* **--instale**.`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. Inicie el IDSM-2 a la partición de aplicación. Utilice la **restauración** *x* **hdd:1 del** comando switch.`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.`* Alternativamente, usted puede utilizar el **comando reset** en el IDSM-2 mientras el variable del dispositivo de arranque se fije correctamente.Para marcar la configuración de la variable del dispositivo de arranque para el IDSM-2, utilice el **dispositivo de arranque** *x. de la* **demostración del** comando switch.`SV9-1> (enable)`**`show boot device 6`** `Device BOOT`

variable = (null) (Default boot partition is hdd:1) Memory-test set to PARTIAL Para configurar la variable del dispositivo de arranque para el IDSM-2, utilice el **dispositivo de arranque determinado hdd:1** *x. del* comando switch configuration.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 Para reajustar el IDSM-2 vía la división CLI del mantenimiento, utilice el comando reset.guest@idsm2-sv-rack.localdomain#**reset** *!--- Output is suppressed.*

16. Marque que viene el IDSM-2 en línea. Utilice el **módulo show** *x. del* comando switch.Aseegurese que la versión de software IDSM-2 es una versión de la partición de aplicación, por ejemplo *4.1(1)S47,* y que el estatus es ACEPTABLE.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. Conecte con el IDSM-2 ahora que ha iniciado para arriba en la partición de aplicación. Utilice la **sesión** *x. del* comando switch.Utilice el nombre de usuario/la contraseña de **Cisco/de 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. Configure el IDSM-2 con el uso del comando setup.sensor#**setup** --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway 10.1.9.1 hostname sensor telnetOption disabled accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit Current time: Sat Sep 20 21:39:29 2003 Setup Configuration last modified: Sat Sep 20 21:36:30 2003 Continue with configuration dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]: 10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The following configuration was entered. networkParams ipAddress 10.66.79.210 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit [0] Go to the command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration and exit setup. Enter your selection[2]: Configuration Saved. sensor#

Información Relacionada

- Cisco IDS Unix Director
- Módulo de servicios del sistema de la detección de intrusos de las Catalyst 6500 Series (IDSM-1)
- Módulo de servicios del sistema de la detección de intrusos de las Catalyst 6500 Series (IDSM-2)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems