Actualización del módulo del sistema de detección de intrusos

Contenido

Introducción

Este documento explica cómo realizar una actualización del módulo de Sistema de detección de intrusos de Cisco (IDSM) en una partición de aplicación, el Service Pack, y una actualización de firma. Para más detalles sobre la actualización del Sensor IDS, consulte el Módulo Intrusion Detection System de Catalyst 6000.+

prerrequisitos

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con los siguientes requisitos previos:

- Comience con un sensor IDS que esté activo y que aún se comunique con el Director, hasta el momento de la actualización.

- Debería poder usar exitosamente ping, FTP pasivo y Telnet a fin de acceder al sensor sin interferencia de ningún firewall o dispositivo de filtrado de paquetes antes de la actualización.
- Asegúrese de que su servidor FTP admite el modo pasivo.

Componentes Utilizados

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

- Versión de software corriente modelo 2.5 del Sensor IDSM WS-X6381-IDS.
- Versión de Solaris corriente 2.6 del director IDS, versión x5.01 del HP OpenView, versión de software 2.2.3 S9 del director IDS.
- Puesto de trabajo de la versión de Solaris 2.8 con el FTP pasivo y el acceso de Telnet al sensor y al director.
- Descargue los archivos de las descargas (IDSk9-sig-3.0-2-S10.bin y nrdirUpdate-S10.bin, se utilizan en este documento).

Nota: Las versiones exactas usadas en este documento pueden no estar disponibles actualmente.

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

- El Director IDS se llama "dir1" y la dirección IP es 192.168.1.3.
- El sensor IDSM es denominado "idsm" y la dirección IP es 192.168.1.2.
- El ID de host coincide con el último octeto de la dirección IP en los ejemplos.
- El ID de la organización se define como "1."
- La dirección IP del servidor FTP es 10.0.0.1.

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

Actualización de la partición de la aplicación IDSM

Los siguientes pasos detallan cómo actualizar el IDSM desde las versiones 2.5(1)S2 a 3.0(1)S4 de la aplicación. Salve la configuración de IDSM antes de que la actualización, como el disco duro entero IDSM sea formatada y cualquier configuración será perdida.

Instrucciones Paso a Paso

Siga las instrucciones proporcionadas abajo.

1. Inicie sesión en el IDSM y guarde el resultado del comando show configuration, como se muestra en el siguiente ejemplo.`Console> (enable) **session 8** Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: **show configuration** Using 37584896 out of 267702272 bytes of available memory ! Using 439668736 out of 4211310592 bytes of available disk space ! Sensor version is : **2.5(1)S0** ! Sensor application status: nr.postofficed running nr.fileXferd running nr.loggerd running nr.packetd running nr.sapd`

```
running Configuration last modified Never Sensor: IP Address: 192.168.1.2 Netmask:
255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host ID: 2 Host Port: 45000
Organization Name: cisco Organization ID: 1 Director: IP Address: 192.168.1.3 Host Name:
dir1 Host ID: 3 Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: cisco
Organization ID: 1 Direct Telnet access to IDSM: disabled
```

2. Descargue los archivos apropiados de las descargas.Los archivos Léame e IDS Sensor están ubicados en la sección 3DES de Cisco IDS Appliance Sensor. El director IDS y los archivos Léame están situados bajo sección del *Cisco IDS Director 3DES*. En este documento, se utilizan los archivos siguientes, no obstante usted debe utilizar cualesquiera archivos son los más actuales:`IDSMk9-a-3.0-1-S4.readme`
```
IDSMk9-a-3.0-1-S4-1.cab
IDSMk9-a-3.0-1-S4-2.cab
IDSMk9-a-3.0-1-S4-3.cab
IDSMk9-a-3.0-1-S4-4.cab
IDSMk9-a-3.0-1-S4-5.cab
IDSMk9-a-3.0-1-S4.dat
```
3. Ponga los archivos en el directorio apropiado del servidor FTP.En este ejemplo, los archivos se colocan en el directorio raíz. El siguiente es un ejemplo de salida del cliente FTP al servidor FTP.`user@solariswkstn% ftp user@solariswkstn Connected to solariswkstn.cisco.com. 220 solariswkstn FTP server (SunOS 5.8) ready. Name (solariswkstn:username): user 331 Password required for user. Password: 230 User user logged in. Remote system type is UNIX. Using binary mode to transfer files. ftp> pwd 250 CWD command successful. 257 "/" is current directory. ftp> ls 227 Entering Passive Mode (10,0,0,1,169,229) 150 ASCII data connection for /bin/Ls (10.0.0.1,43494) (0 bytes). total 110878 -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:34 IDSMk9-a-3.0-1-S4-1.cab -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:22 IDSMk9-a-3.0-1-S4-2.cab -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:24 IDSMk9-a-3.0-1-S4-3.cab -rw-r--r-- 1 jlimbo cisco 10000384 May 11 15:24 IDSMk9-a-3.0-1-S4-4.cab -rw-r--r-- 1 jlimbo cisco 1126530 May 11 15:23 IDSMk9-a-3.0-1-S4-5.cab -rw-r--r-- 1 jlimbo cisco 600 May 11 15:20 IDSMk9-a-3.0-1-S4.dat 226 ASCII Transfer complete. ftp> exit 221 Goodbye. user@solariswkstn%`
4. Fije la división del mantenimiento como la partición activa, después consola en el IDSM a la división del mantenimiento (la aplicación es la configuración predeterminada) y fije el parámetro de la configuración de red del IDSM.En el siguiente ejemplo, el IDSM se encuentra en la ranura 8 del chasis Catalyst 6509.`Console> (enable) set boot device hdd:2 Console> (enable) reset 8 This command will reset module 8. Unsaved configuration on module 8 will be lost Do you want to continue (y/n) [n]? y Module 8 shut down in progress, please don't remove module until shutdown completed. Console> (enable) Module 8 shutdown completed. Module resetting... Console> (enable) session 8 Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: maintenance# maintenance# diag maintenance(diag)#ids-installer netconfig /configure /ip=192.168.1.2 /subnet=255.255.255.0 /gw=192.168.1.1 STATUS: Network parameters for the config port have been configured!`
   Nota: Reinicie el módulo para que los cambios tengan efecto.
5. Una vez que IDSM ha finalizado el reinicio, vuelva a la sesión en ISDM e instale la partición de la aplicación inactiva al ejecutar el comando ids-installer, según se muestra en el siguiente ejemplo.`Console> (enable) session 8 Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: maintenance# diag maintenance(diag)# ids-installer system /nw /install /server=10.0.0.1 /user=user /save=yes /dir='//' /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 E893-5968 Extracting the image... ########################## ----snip----- STATUS: Image has been successfully installed on drive C:\! maintenance(diag)# exit`

Cómo verificar la actualización de la partición de la aplicación

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos

comandos “show” y ver un análisis del resultado de estos comandos.

Reinicie el IDSM de nuevo a la partición de aplicación y verifiquelo que la imagen se ha actualizado con éxito, tal y como se muestra en del siguiente ejemplo.

```
Console> (enable) set boot device hdd:1 Console> (enable) reset 8 This command will reset module
8. Unsaved configuration on module 8 will be lost Do you want to continue (y/n) [n]? y Module 8
shut down in progress, please don't remove module until shutdown completed. Console> (enable)
Module 8 shutdown completed. Module resetting... Console> (enable) session 8 Trying IDS-8...
Connected to IDS-8. Escape character is '^]'. login: ciscoids Password: idsm# show configuration
Using 48259072 out of 267702272 bytes of available memory ! Using 504688640 out of 4211310592
bytes of available disk space ! Sensor version is : 3.0(1)S4 ! Sensor application status:
nr.postofficed running nr.fileXferd running nr.loggerd running nr.packetd running nr.sapd
running Configuration last modified Wed May 01 01:03:56 2002 Sensor: IP Address: 192.168.1.2
Netmask: 255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host ID: 2 Host Port: 45000
Organization Name: cisco Organization ID: 1 Director: IP Address: 192.168.1.3 Host Name: dir1
Host ID: 3 Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: cisco Organization
ID: 1
```

Actualización de IDSM Service Pack

Utilice el siguiente procedimiento para poner al día el Service Pack IDSN.

1. La sesión en el IDSM publicando el **comando session -** (donde # está el número de módulo), y publica el **comando configure terminal**, tal y como se muestra en del siguiente ejemplo.`idsm#`
   `idsm#`**`configure terminal`**
2. Envíe el comando ftp://<username@server/dir/filename> para conectarse a través del FTP y aplique el service pack según se muestra en el siguiente ejemplo.`idsm(config)#`**`apply ftp://user@10.0.0.1//IDSMk9-sp-3.0-3-S10.exe`** `WARNING: Installing Service Pack will temporarily disable IDS. Continue with IDS Service Pack install?: y Enter the FTP user password: ********* Connecting to site... Receiving file.` **`Installing as 3.0(3)S10`** `Installing files from Service Pack 3.0(2) Installing files from Signature Update 10 Starting NetRanger Signatures Merging Utility... Checking file: C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf... Adding signature: SigOfGeneral 993 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3111 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3112 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3114 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3160 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3162 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3454 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3455 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 4060 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 4101 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 4601 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5158 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5159 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5160 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5161 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5162 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5163 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5164 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5165 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5166 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5167 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5168 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding`

```
signature: SigOfGeneral 5169 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5170 to C:\Program Files\ Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5171 to C:\Program
Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5172 to
C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
5173 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 5174 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 5175 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5176 to C:\Program Files\ Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 6197 to C:\Program
Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 6901 to
C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
6902 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 6903 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 6910 to C:\Program Files\ Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 6920 to C:\Program Files\ Cisco
Systems\Netranger/etc/packetd.conf. Installing files from Service Pack 3.0(3) The Install
for IDSM Service Pack file IDSMk9-sp-3.0-3-S10.exe was successful 2002 May 13 18:29:34
%PAGP-5-PORTFROMSTP:Port 8/1 left bridge port 8/1 2002 May 13 18:29:34 %DTP-5-
NONTRUNKPORTON:Port 8/1 has become non-trunk Systems needs to be restarted. Rebooting...
Module 8 shut down in progress, please don't remove module until shutdown completed.
idsm(config)# Console> (enable) Module 8 shutdown completed. Module resetting...
```

Cómo verificar la actualización del Service Pack

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Inicie sesión en el IDSM al ejecutar el comando sesión # (# es el número del módulo) y ejecute el comando show configuration, tal como se muestra en el siguiente ejemplo.

```
idsm#show configuration Using 46059520 out of 267702272 bytes of available memory ! Using
466886656 out of 4211310592 bytes of available disk space ! Sensor version is : 3.0(3)S10 !
Sensor application status: nr.postofficed running nr.fileXferd running nr.loggerd running
nr.packetd running nr.sapd running Configuration last modified Fri May 10 23:02:57 2002 Sensor:
IP Address: 192.168.1.2 Netmask: 255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host
ID: 2 Host Port: 45000 Organization Name: cisco Organization ID: 1 Director: IP Address:
192.168.1.3 Host Name: dir1 Host ID: 3 Host Port: 45000 Heart Beat Interval (secs): 5
Organization Name: cisco Organization ID: 1 Direct Telnet access to IDSM: enabled Current access
list entries: [1] 192.168.1.0 0.0.0.255 idsm#
```

Actualización de las firmas IDSM

Utilice el siguiente procedimiento para actualizar las firmas ISDM.

1. La sesión en el IDSM publicando el **comando session -** (donde # está el número de módulo), y publica el **comando configure terminal**, tal y como se muestra en del siguiente ejemplo.`idsm#`
   `idsm#configure terminal`
2. Ejecute el comando apply ftp://<nombredeusuario@servidor/directorio/nombredelarchivo> para conectarse a través de FTP y aplique las firmas IDSM como se muestra en el siguiente ejemplo:`idsm(config)#apply ftp://user@10.0.0.1//IDSMk9-sig-3.0-3-S13.exe WARNING:`
   `Installing Signature Update will temporally disable IDS. Continue with IDS Signature Update`
   `install?: % Please answer 'yes' or 'no'. Continue with IDS Signature Update install?: yes`
   `Enter the FTP user password: ********* Connecting to site... Receiving file. WARNING!!!`
   `Installation of this IDSM Signature Update will now prevent unistalling of the current IDSM`
   `Service Pack 3.0(3). WARNING!!! To uninstall IDSM Service Pack 3.0(3) you will need to`
   `first uninstall this IDSM Signature Update. Starting NetRanger Signatures Merging`

```
Utility... Checking file: C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf...
Adding signature: SigOfGeneral 1107 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3116 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3117 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
3118 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 3119 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 3120 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 3163 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3403 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 3456 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
3501 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 3651 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 4507 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5178 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5179 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5180 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
5181 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 5182 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 5183 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5184 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5188 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5191 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral
5194 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature:
SigOfGeneral 5195 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. Adding
signature: SigOfGeneral 5196 to C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf.
Adding signature: SigOfGeneral 5197 to C:\Program Files\Cisco
Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5199 to C:\Program
Files\Cisco Systems\Netranger/etc/packetd.conf. Adding signature: SigOfGeneral 5200 to
C:\Program Files\Cisco Systems\Netranger/etc/packetd.conf. The Install for IDSM Signature
Update file IDSMk9-sig-3.0-3-S13.exe was successful Systems needs to be restarted.
Rebooting... Module 8 shut down in progress, please don't remove module until shutdown
completed. idsm(config)# Console> (enable) Module 8 shutdown completed. Module resetting...
2002 May 13 18:58:08 %SYS-3-SUP_OSBOOTSTATUS:Starting IDSM Diagnostics 2002 May 13 18:58:50
%SYS-3-SUP_OSBOOTSTATUS:IDSM diagnostics completed successfully. 2002 May 13 18:58:56 %SYS-
5-MOD_OK:Module 8 is online 2002 May 13 18:58:56 %PAGP-5-PORTFROMSTP:Port 8/1 left bridge
port 8/1 2002 May 13 18:58:56 %DTP-5-TRUNKPORTON:Port 8/1 has become dot1q trunk 2002 May
13 18:58:56 %PAGP-5-PORTTOSTP:Port 8/2 joined bridge port 8/2 2002 May 13 18:58:57 %SYS-3-
MOD_PORTINTFINSYNC:Port Interface in sync for Module 8 2002 May 13 18:58:57 %PAGP-5-
PORTTOSTP:Port 8/1 joined bridge port 8/1 Console> (enable) Console> (enable) session 8
Trying IDS-8... Connected to IDS-8. Escape character is '^]'. login: ciscoids Password:
```

Verificación de la actualización de firmas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Inicie sesión en el IDSM al ejecutar el comando sesión # (# es el número del módulo) y ejecute el comando show configuration, tal como se muestra en el siguiente ejemplo.

```
idsm#show configuration Using 46014464 out of 267702272 bytes of available memory ! Using
470089728 out of 4211310592 bytes of available disk space ! Sensor version is : 3.0(3)S13 !
Sensor application status: nr.postofficed running nr.fileXferd running nr.loggerd running
nr.packetd running nr.sapd running Configuration last modified Fri May 10 23:02:57 2002 Sensor:
IP Address: 192.168.1.2 Netmask: 255.255.255.0 Default Gateway: 192.168.1.1 Host Name: idsm Host
ID: 2 Host Port: 45000 Organization Name: cisco Organization ID: 1 Director: IP Address:
192.168.1.3 Host Name: dir1 Host ID: 3 Host Port: 45000 Heart Beat Interval (secs): 5
Organization Name: cisco Organization ID: 1 Direct Telnet access to IDSM: enabled Current access
```

```
list entries: [1] 192.168.1.0 0.0.0.255 idsm#
```

Actualizar el IDSM2

Las secciones siguientes proporcionan la información sobre actualizar el ISDM2.

Actualizar la división del mantenimiento

Para actualizar la división del mantenimiento a partir del 1.3.1 a 1.3.2, inicie la cuchilla IDSM2 en la partición de aplicación publicando los siguientes comandos en el Switch.

```
reset <mod> hdd:1

Console> (enable) reset 5 hdd:1
```

```
idsm-2#show version Application Partition: Cisco Systems Intrusion Detection Sensor, Version
4.0(1)S41 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDS2-XL Sensor up-time is 43 min. Using
748920832 out of 1979682816 bytes of available memory (37% usage) Using 997M out of 17G bytes of
available disk space (6% usage) MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running Logger
2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running NetworkAccess 2003_Jan_23_02.00
(Release) 2003-01-23T02:00:25-0600 Running TransactionSource 2003_Jan_23_02.00 (Release) 2003-
01-23T02:00:25-0600 Running WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600 Upgrade History: No upgrades
installed Maintenance Partition Version 1.3(1) idsm-2(config)#upgrade ftp://user@10.1.1.1/mp.1-
3-2.bin.gz Password: ******** Warning: Executing this command will re-image the maintenance
partition. The system may be rebooted to complete the upgrade. Continue with upgrade? : yes
```

La re-imagen es una vez completa y el sistema ha reiniciado, una **versión de la demostración** permitirá que usted confirme que la actualización fuera acertada.

```
idsm-2#show version Application Partition: Cisco Systems Intrusion Detection Sensor, Version
4.0(1)S41 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDS2-XL Using 762945536 out of 1979682816
bytes of available memory (38% usage) Using 1007M out of 17G bytes of available disk space (7%
usage) MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running AnalysisEngine
2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running Authentication 2003_Jan_23_02.00
(Release) 2003-01-23T02:00:25-0600 Running Logger 2003_Jan_23_02.00 (Release) 2003-01-
23T02:00:25-0600 Running NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running WebServer
2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running CLI 2003_Jan_17_18.33 (Release)
2003-01-17T18:33:18-0600 Upgrade History: No upgrades installed Maintenance Partition Version
1.3(2)
```

Reimaging la partición de aplicación de la división del mantenimiento

Precaución: Después de rehacer la imagen el módulo IDS, usted debe inicializar el módulo IDS usando el **comando setup**. Este proceso quita toda la Configuración del sensor y nuevas imágenes la partición de aplicación. Este proceso debe ser utilizado solamente si la partición de aplicación es corrupta o inaccesible. Si la partición de aplicación es accesible, para evitar la configuración actual perdidosa, utilice la actualización de la imagen de menor tamaño para actualizar de la partición de aplicación sí mismo.

1. Inicie en la división del mantenimiento publicando los siguientes comandos en el Switch.`reset <mod> cf:1`

   ```
   Console> (enable)reset 5 cf:1 This command will reset module 5. Unsaved configuration on
   ```

```
module 5 will be lost Do you want to continue (y/n) [n]? y SendShutDownMsg: shut down
module 5 no responce, reset module... Module 5 experienced problems during shutdown. It may
take several minutes to come online. Console> (enable) 2003 Sep 02 14:01:55 %SYS-3-
SUP_OSBOOTSTATUS:MP OS Boot Status: f inished booting Console> (enable) Console> (enable)
sess 5 Trying IDS-5... Connected to IDS-5. Escape character is '^]'. Cisco Maintenance
image
```

2. Registro en el módulo IDS ingresando el nombre de usuario y contraseña siguiente.`login: guest Password: cisco Maintenance image version: 1.3(2) guest@localhost.localdomain#ip address 172.16.171.22 255.255.255.192 guest@localhost.localdomain#ip gateway 172.16.171.1`
3. Ingrese al modo terminal de configuración que usa el **comando configure terminal**.
4. Realice la nueva imagen usando el comando del **file> del ftp server IP>/<directory path>/<image del <user>@< de ftp:// de la actualización**.A le indicarán que ingrese la contraseña del servidor FTP (si procede). También a le indicarán que proceda con la instalación. Ingrese **y** para continuar.`guest@localhost.localdomain#upgrade ftp://user@10.1.1.1/ WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz ftp://user@10.1.1.1//home/user/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz (unknown size) /tmp/upgrade.gz [-] 65259K 66825226 bytes transferred in 13.38 sec (4878.70k/sec) Upgrade file ftp://user@10.1.1.1//home/user/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. guest@localhost.localdomain#exit logout`
5. Reinicie el módulo IDS a la partición de aplicación ingresando el **comando reset <module number> hdd:1**.`Console> (enable)reset 5 hdd:1 This command will reset module 5. Unsaved configuration on module 5 will be lost Do you want to continue (y/n) [n]? y Module 5 shut down in progress, please don't remove module until shutdown completed. Console> (enable) Module 5 shutdown completed. Module resetting...`
6. Cuando el módulo IDS ha reiniciado, marque la versión de software.**Nota:** Esto se puede también utilizar para comprobar.`Console> (enable) Console> (enable)sess 5 Trying IDS-5... Connected to IDS-5. 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: ***NOTICE*** This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto If you require further assistance please contact us by sending email to export@cisco.com. sensor# sensor#show version Application Partition: Cisco Systems Intrusion Detection Sensor, Version 4.1(1)S47 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDSM2-BUN Sensor up-time is 4 min. Using 701689856 out of 1979682816 bytes of available memory (35% usage) Using 527M out of 17G bytes of available disk space (4% usage) MainApp 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running AnalysisEngine 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running Authentication 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running Logger 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running NetworkAccess 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running TransactionSource 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running WebServer 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running CLI 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Upgrade History: No upgrades installed Maintenance Partition Version 1.3(2)`
7. Inicie sesión a la partición de aplicación CLI e inicialice el módulo IDS, usando el **comando setup**.

Actualización de la imagen de menor tamaño

Esta actualización se puede utilizar en las situaciones donde está todavía accesible la partición de aplicación, pero solamente la parte de esta aplicación está quebrada. Con respecto a usar la imagen completa recrear imagen la partición de aplicación, la imagen de menor tamaño conserva las Configuraciones del sensor.

Para instalar la actualización de menor importancia, siga los siguientes pasos:

1. Registro en el CLI usando una cuenta con los privilegios de administrador.
2. Ingrese al modo de configuración publicando el **comando configure terminal**.
3. Teclee el **comando upgrade [URL]/<filename>** de actualizar el sensor.**El [URL]** es el Uniform Resource Locator que señala a donde se localiza el paquete de la actualización de firma. Por ejemplo, para extraer la actualización vía el FTP, ingrese el siguiente: **upgrade ftp://<username>@<ip-address>//<directory>/<filename>** Los métodos disponibles del transporte son SCP, FTP, HTTP, o HTTPS.
4. Ingrese la contraseña apropiada cuando está indicado.
5. Para completar la actualización, teclee **sí** cuando está indicado.

Actualizar el Service Pack IDSM2 o las firmas

Utilice el siguiente procedimiento para actualizar el saco o las firmas del servicio ISDM2.

1. Para actualizar el sensor con un Service Pack o una firma, inicie para arriba en la partición de aplicación.`sensor24#`**`show version`** `Application Partition: Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S41 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDS2-XL Sensor up-time is 16:45. Using 377667584 out of 1979682816 bytes of available memory (19% usage) Using 765M out of 17G bytes of available disk space (5% usage) MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 NotRunning Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running Logger 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600 Upgrade History: No upgrades installed Maintenance Partition Version 1.3(2)`
2. Registro en el módulo IDS CLI.
3. Ingrese el modo configurado terminal usando el **comando configure terminal**.
4. Ingrese el comando del **file> del paquete del ftp server IP>/<directory path>/<service del <user>@< de ftp:// de la actualización** de instalar el Service Pack y cuando está indicado, el tipo **y** para confirmar la instalación.Las reinicializaciones del módulo cuando la instalación es completa.`sensor24#`**`configure terminal`** `sensor24(config)#`**`upgrade ftp://user@10.1.1.1/IDS-K9-min-4.1-1-S47.rpm.pkg`** `Password: ******** Warning: Executing this command will apply a minor version upgrade to the application partition. The system may be rebooted to complete the upgrade. Continue with upgrade? : yes Broadcast message from root (Sat Sep 20 17:59:09 2003): Applying update IDS-K9-min-4.1-1-S47. Shutting down all CIDS processes. All connections will be terminated. The system will be rebooted upon completion of the update. Console> Module 5 shut down in progress, please don't remove module until shutdown completed. Console> Module 5 shutdown completed. Module resetting...`
5. Después de que el módulo haya reiniciado, ingrese el Switch CLI y marque la versión.**Nota:** Esto se puede también utilizar para comprobar.`sensor24#`**`show version`**
   `Application Partition: Cisco Systems Intrusion Detection Sensor, Version 4.1(1)S47 OS Version 2.4.18-5-phoenix Platform: WS-SVC-IDSM2-BUN Sensor up-time is 6 min. Using 401248256 out of 1979682816 bytes of available memory (20% usage) Using 872M out of 17G bytes of available disk space (6% usage) MainApp 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running AnalysisEngine 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-`

```
0500 Running Authentication 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running
Logger 2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running NetworkAccess
2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running TransactionSource
2003_Jun_20_06.00 (Release) 2003-06-20T05:53:31-0500 Running WebServer 2003_Jun_20_06.00
(Release) 2003-06-20T05:53:31-0500 Running CLI 2003_Jun_20_06.00 (Release) 2003-06-
20T05:53:31-0500 Upgrade History: * IDS-maj-4.0-1-S41 12:41:04 UTC Tue Apr 29 2003 IDS-K9-
min-4.1-1-S47.rpm.pkg 17:59:06 UTC Sat Sep 20 2003 Maintenance Partition Version 1.3(2)
sensor24#
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Página de soporte de Cisco Secure Intrusion Detection
- Inscriba al Cisco IDS las notificaciones de actualización activa
- Documentación para Netranger
- Soporte Técnico - Cisco Systems