Mise à niveau du module du système de détection des intrusions (IDS, Intrusion Detection System).

Contenu

Introduction

Ce document explique comment exécuter une mise à jour du module de Detection System de Cisco Intrusion (IDSM) sur une partition d'application, le pack de services, et une mise à jour de signature. Pour plus de détails sur améliorer le capteur d'ID, référez-vous au module de système de détection d'intrusion du Catalyst 6000.

Conditions préalables

Conditions requises

Avant d'essayer cette configuration, veuillez vous assurer que vous remplissez les conditions préalables suivantes :

- Commencez par un capteur d'ID qui communique et toujours avec le directeur jusqu'à la période de la mise à jour.
- Vous devriez pouvoir employer avec succès le ping, le FTP passif, et le telnet pour obtenir au capteur sans interférence de n'importe quel tri de périphérique de Pare-feu ou de filtrage des paquets avant la mise à jour.
- Veillez-vous pour avoir un ftp server qui prend en charge le mode passif.

Composants utilisés

Les informations de ce document sont basées sur les versions de logiciel et matériel suivantes :

- Version de logiciel courante 2.5 du modèle WS-X6381-IDS de capteur IDSM.
- Version Solaris courante 2.6 d'IDS Director, version x5.01 de HP OpenView, version de logiciel 2.2.3 S9 d'IDS Director.
- Poste de travail de la version Solaris 2.8 avec le FTP passif et l'accès de telnet au capteur et au directeur.
- Téléchargez les fichiers des téléchargements (IDSk9-sig-3.0-2-S10.bin et nrdirUpdate-S10.bin, sont utilisés dans ce document).

Remarque: Les versions exactes utilisées dans ce document peuvent ne pas être actuellement disponibles.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

- L'IDS Director est nommée "dir1," et l'adresse IP est 192.168.1.3.
- Le capteur IDSM est nommé « idsm, » et l'adresse IP est 192.168.1.2.
- L'ID d'hôte apparie le dernier octet de l'adresse IP dans les exemples.
- L'ID d'organisation est défini en tant que "1."
- L'adresse IP serveuse ftp est 10.0.0.1.

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Évolution de la partition d'application IDSM

Les étapes suivantes t'affichent comment améliorer l'IDSM des versions 2.5(1)S2 à 3.0(1)S4 d'application. Sauvegardez la configuration IDSM avant que la mise à jour, comme disque dur entier IDSM soit formatée et n'importe quelle configuration sera perdue.

Instructions pas à pas

Suivez les instructions fournies ci-dessous.

1. La session dans l'IDSM et sauvegardent la sortie de la commande de **configuration d'exposition**, suivant les indications de l'exemple suivant.`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. Téléchargez les fichiers appropriés des téléchargements.Les ID capteur et fichiers readmes se trouvent sous la section du *capteur 3DES d'appareils d'ID de Cisco*. L'IDS Director et les fichiers readmes se trouvent sous la section de l'*IDS Director 3DES de Cisco*. Dans ce document, les fichiers suivants sont utilisés, toutefois vous devriez utiliser Qu'est ce que fichiers sont la plupart de courant :
```
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. Placez les fichiers dans le répertoire approprié du ftp server.Dans cet exemple, les fichiers sont placés dans le répertoire racine. Ce qui suit est sortie témoin du client FTP au ftp server.
```
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. Placez la partition de maintenance en tant que la partition active, puis console dans l'IDSM à la partition de maintenance (l'application est la valeur par défaut) et placez le paramètre de configuration réseau de l'IDSM.Dans l'exemple suivant, l'IDSM est dans l'emplacement 8 du châssis du 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!
```
   Remarque: Remettez à l'état initial le module pour les modifications pour le prendre effet.
5. Une fois que l'IDSM a terminé la réinitialisation, la session de nouveau dans l'IDSM et installent la partition inactive d'application en émettant la commande d'id-**installateur**, suivant les indications de l'exemple suivant.
```
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
```

Vérifier la mise à jour de partition d'application

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Redémarrez l'IDSM de nouveau à la partition d'application et le vérifiez que l'image a été avec succès mise à jour, suivant les indications de l'exemple suivant.

```
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
```

Évolution du Service Pack IDSM

Employez la procédure suivante pour mettre à jour le pack de services IDSN.

1. La session dans l'IDSM en émettant la **session # la** commande (où # est le numéro de module), et émettent la commande de **configure terminal**, suivant les indications de l'exemple suivant.
```
idsm#
idsm#configure terminal
```
2. Émettez l'**application ftp:// < la** commande d'**username@server /dir/filename>** de se connecter par le FTP, et appliquez le pack de services, suivant les indications de l'exemple suivant.
```
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...
```

Vérifier la mise à jour de Service Pack

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

La session dans l'IDSM en émettant la **session # la** commande (où # est le numéro de module), et émettent la commande de **configuration d'exposition**, suivant les indications de l'exemple suivant.

```
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#
```

Évolution des signatures IDSM

Employez la procédure suivante pour améliorer les signatures ISDM.

1. La session dans l'IDSM en émettant la **session # la** commande (où # est le numéro de module), et émettent la commande de **configure terminal**, suivant les indications de l'exemple suivant.
```
idsm#
idsm#configure terminal
```
2. Émettez l'**application ftp:// <** *la* commande d'*username@server /dir/filename***>** de se connecter par le FTP, et appliquez les signatures IDSM, suivant les indications de l'exemple suivant :
```
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:
```

Vérifier la mise à jour de signature

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

La session dans l'IDSM en émettant la **session # la** commande (où # est le numéro de module), et émettent la commande de **configuration d'exposition**, suivant les indications de l'exemple suivant.

```
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#
```

Évolution de l'IDSM2

Les sections suivantes fournissent des informations sur améliorer l'ISDM2.

Évolution de la partition de maintenance

Pour améliorer la partition de maintenance de 1.3.1 à 1.3.2, démarrez la lame IDSM2 dans la partition d'application en émettant les commandes suivantes sur le commutateur.

```
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
```

Une fois que la re-image est complète et le système a redémarré, un **show version** te permettra pour confirmer que la mise à jour était réussie.

```
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)
```

Réimager la partition d'application de la partition de maintenance

Attention : Après nouvelle création d'images le module IDS, vous devez initialiser le module IDS utilisant la **commande setup**. Ce processus retire toute la configuration de capteur et réimage la partition d'application. Ce processus devrait être utilisé seulement si la partition d'application est corrompue ou inaccessible. Si la partition d'application est accessible, pour éviter la configuration en cours perdante, employez la mise à niveau d'image mineure pour améliorer de la partition d'application elle-même.

1. Démarrage dans la partition de maintenance en émettant les commandes suivantes sur le commutateur.`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. Connectez-vous dans le module IDS en écrivant le nom d'utilisateur et mot de passe suivant.`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. Écrivez le mode terminal de configuration utilisant la commande de **configure terminal**.
4. Exécutez le réimager utilisant la commande de **file> du ftp server IP>/<directory path>/<image de <user>@< de ftp:// de mise à jour**.Vous serez incité à entrer le mot de passe serveur ftp (s'il y a lieu). Vous serez également incité à poursuivre l'installation. Écrivez **y** pour continuer.`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. Redémarrez le module IDS à la partition d'application en écrivant la commande du **number> hdd:1 de <module de remise**.`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. Quand le module IDS a redémarré, vérifiez la version de logiciel.**Remarque:** Ceci peut également être utilisé pour la vérification.`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. Ouvrez une session à la partition CLI d'application et initialisez le module IDS, utilisant la **commande setup**.

Mise à niveau d'image mineure

Cette mise à jour peut être utilisée dans les situations où la partition d'application est encore accessible, mais seulement une partie de cette application est cassée. Par rapport à employer la pleine image pour réimager la partition d'application, l'image mineure retient les configurations de capteur.

Pour installer la mise à jour mineure, suivez ces étapes :

1. Connectez-vous dans le CLI utilisant un compte avec des privilèges d'administrateur.
2. Écrivez le mode de configuration en émettant la commande de **configure terminal**.
3. Introduisez la commande de la **mise à jour [URL]/<filename>** d'améliorer le capteur.**[URL]** est l'uniform resource locator indiquant où le module de mise à jour de signature se trouve. Par exemple, pour récupérer la mise à jour par l'intermédiaire du FTP, entrez dans ce qui suit : **upgrade ftp://<username>@<ip-address>//<directory>/<filename>** Les méthodes disponibles de transport sont SCP, FTP, HTTP, ou HTTPS.
4. Entrez le mot de passe approprié une fois incité.
5. Pour se terminer la mise à jour, tapez **oui** une fois incité.

Évolution du Service Pack IDSM2 ou des signatures

Employez la procédure suivante pour améliorer le sac ou les signatures au service ISDM2.

1. Pour améliorer le capteur avec un pack de services ou une signature, amorce dans la partition d'application.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. Connectez-vous dans le module IDS CLI.
3. Entrez le mode de configure terminal utilisant la commande de **configure terminal**.
4. Sélectionnez la commande de **file> de paquet du ftp server IP>/<directory path>/<service de <user>@< de ftp:// de mise à jour** d'installer le pack de services et une fois incité, le type **y** à confirmer l'installation.Les réinitialisations de module quand l'installation est complète.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. Après que le module ait redémarré, écrivez le commutateur CLI et vérifiez la version.**Remarque:** Ceci peut également être utilisé pour la vérification.
```
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#
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Page Cisco Secure de prise en charge de la détection d'intrusion
- Abonnez-vous aux notifications actives de mise à jour d'ID de Cisco
- Documentation pour NetRanger
- Support technique - Cisco Systems