Обновление системы обнаружения несанкционированного модуля

Содержание

Введение

Этот документ объясняет, как выполнить Модуль Cisco Intrusion Detection System (IDSM) обновление на разделе установки приложения, пакете обновления и обновлении подписи. Для получения дополнительной информации по модернизации модуля IDS Sensor обратитесь к разделу "Модуль системы обнаружения вторжений для Catalyst 6000".

Предварительные условия

Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются следующие условия:

- Начните с включенного сенсора IDS, который еще обменивается информацией с Director, пока не наступило время обновления.

- Перед обновлением следует убедиться, что можно успешно использовать ping, пассивный FTP и Telnet для доступа к сенсору без вмешательства межсетевого экрана или устройства фильтрации пакетов.
- Убедитесь, что ваш FTP-сервер поддерживает пассивный режим.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения и оборудования:

- Модель WS-X6381-IDS Датчика IDSL, работающая под управлением ПО версии 2.5.
- IDS Director рабочая версия 2.6 Solaris, версия x5.01 HP OpenView, Версия программного обеспечения 2.2.3 S9 IDS Director.
- Рабочая станция версии 2.8 Solaris с пассивным FTP и Telnet обращается к Датчику и Управляющему узлу.
- Загрузите файлы от Загрузок (IDSk9-sig-3.0-2-S10.bin и nrdirUpdate-S10.bin, используются в этом документе).

Примечание: Точные версии, используемые в данном документе, могут быть недоступны в настоящий момент.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

- IDS Director обозначается "dir1," а IP-адрес - 192.168.1.3.
- Датчик IDSM называется "idsm", его IP-адрес: 192.168.1.2.
- Код хоста совпадает с последним октетом IP-адреса в примерах.
- Идентификатор организации определен как "1".
- IP-адрес сервера FTP 10.0.0.1.

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Обновление раздела приложений IDSM

Следующие действия показывают порядок обновления IDSM с версии приложения 2.5(1)S2 на версию 3.0(1)S4. Сохраните конфигурацию IDSM перед обновлением, поскольку весь жесткий диск IDSM будет отформатирован, и любая конфигурация будет потеряна.

Пошаговые инструкции

Следуйте приведенным ниже инструкциям.

1. **Создайте сеанс IDSM и сохраните выходные данные команды show configuration, как показано в следующем примере.**
```
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. Загрузите соответствующие файлы от Загрузок.*Датчик IDS и файлы предварительных сведений находятся в разделе Cisco IDS Appliance Sensor 3DES.* IDS Director и файлы предварительных сведений расположены под разделом *3DES Cisco IDS Director*. В этом документе используются следующие файлы, однако необходимо использовать любые файлы, являются актуальнейшими: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. Разместите файлы в соответствующий каталог сервера FTP.В этом примере файлы размещены в корневом каталоге. Ниже приведен образец выхода от FTP-клиента на FTP-сервер.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. Установите разделение Обслуживания как активный раздел, затем консоль в IDSM к разделению обслуживания (приложение является настройкой по умолчанию), и установите параметр конфигурации сети IDSM.В следующем примере IDSM в слоте 8 шасси 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! **Примечание:** Для вступления в действие изменений перезапустите модуль.
5. **Как только IDSM закончит перезагрузку, верните сеанс в IDSM и установите неактивный раздел приложения, выдав команду ids-installer, как показано в следующем примере.**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

Проверка обновления разделов приложений

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Перезагрузите IDSM назад к разделу установки приложения и проверьте, что образ был успешно обновлен, как показано в следующем примере.

```
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
```

Обновление IDSM Service Pack

Используйте следующую процедуру для обновления пакета обновления IDSN.

1. Сеанс в IDSM путем запуска **сеанса #** команда (где # является номером модуля), и выполняет **команду configure terminal**, как показано в следующем примере.
```
idsm#
idsm#configure terminal
```
2. **Для установления соединения по протоколу FTP и применения пакетов обновления выполните команду apply ftp://<имя_пользователя@сервер/каталог/имя_файла> (см. пример ниже).**
```
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...
```

Проверка обновления с помощью пакета обновления

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Создайте сеанс в модуле IDSM с помощью команды session # (где "#" - номер модуля), после чего подайте команду show configuration, как показано в следующем примере.

```
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#
```

Обновление подписей IDSM

Используйте следующую процедуру для обновления подписей ISDM.

1. Сеанс в IDSM путем запуска **сеанса #** команда (где # является номером модуля), и выполняет **команду configure terminal**, как показано в следующем примере.`idsm#`
   `idsm#configure terminal`
2. *Для установления соединения по протоколу FTP и применения подписей IDSM выполните команду apply ftp://<имя_пользователя@сервер/каталог/имя_файла> (см. пример ниже):*`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:
```

Проверка обновления подписи

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

Создайте сеанс в модуле IDSM с помощью команды session # (где "#" - номер модуля), после чего подайте команду show configuration, как показано в следующем примере.

```
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#
```

Обновление IDSM2

Следующие разделы предоставляют сведения об обновлении ISDM2.

Обновление разделения Maintenence

Для обновления Разделения Обслуживания от 1.3.1 до 1.3.2 загрузите блейд IDSM2 в Разделе установки приложения путем запуска следующих команд в коммутаторе.

```
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
```

Как только повторно захватывание образ завершено, и система перезагрузила, **show version** позволит вам подтверждать, что обновление было успешно.

```
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)
```

Повторно захватывание образ раздела установки приложения от разделения Maintenence

Внимание. : После повторно захватывания образ Модуля IDS необходимо инициализировать Модуль IDS с помощью команды **настройки**. Этот процесс удаляет всю конфигурацию сенсора и повторно захватывает образ раздел установки приложения. Этот процесс должен использоваться, только если Раздел установки приложения поврежден или недоступен. Если Раздел установки приложения доступен, чтобы избежать терять текущую

конфигурацию, используйте Обновление Меньшего образа для обновления от самого Раздела установки приложения.

1. Начальная загрузка в Разделение Обслуживания путем запуска следующих команд на коммутаторе.`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. Войдите в Модуль IDS путем ввода следующего имени пользователя и пароля.`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. Введите терминальный режим настройки с помощью **команды configure terminal**.
4. Выполните повторно захватывать образ использование **обновления ftp://<user> <IP ftp-сервера> / <путь к каталогу> /** команда **<image file>**.Вам предложат ввести пароль сервера FTP (при необходимости). Вам также предложат продолжить установку. Введите **y** для продолжения.`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. Перезагрузите Модуль IDS к разделу установки приложения путем ввода **команды 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. Когда Модуль IDS перезагрузит, проверьте версию программного обеспечения.**Примечание:** Это может также использоваться в целях проверки.`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. Войдите к CLI раздела установки приложения и инициализируйте Модуль IDS, с помощью команды **настройки**.

Обновление меньшего образа

Это обновление может использоваться в ситуациях, где раздел установки приложения все еще доступен, но только сломана часть этого приложения. По сравнению с использованием полного образа, чтобы повторно захватить образ Раздел установки приложения, меньший образ сохраняет конфигурации сенсора.

Для установки незначительного обновления выполните эти действия:

1. Войдите в CLI с помощью учетной записи с администраторскими привилегиями.
2. Введите режим конфигурации путем запуска **команды configure terminal**.
3. Введите **обновление [URL] /** команда **<filename>** для обновления датчика.**[URL]** является обращением Uniform Resource Locator туда, где расположен пакет обновления подписи. Например, для получения обновления через FTP введите придерживающееся:
   `upgrade ftp://<username>@<ip-address>//<directory>/<filename>` Доступные транспортные методы являются SCP, FTP, HTTP или HTTPS.
4. Введите соответствующий пароль, когда предложено.
5. Для завершения обновления введите **да**, когда предложено.

Обновление пакета обновления IDSM2 или подписей

Используйте следующую процедуру для обновления sack сервиса ISDM2 или подписей.

1. Для обновления датчика с пакетом обновления или подписью загрузитесь в Разделе установки приложения.`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. Войдите в CLI Модуля IDS.
3. Перейдите в режим configure terminal с помощью **команды configure terminal**.
4. Введите **обновление ftp://<user> <IP ftp-сервера> / <путь к каталогу> /** команда **<service pack file>** для установки пакета обновления и, когда предложено, **тип y** для подтверждения установки.Перезагрузки модуля, когда установка завершена.`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. После того, как модуль перезагрузил, вводит CLI коммутатора и проверяет версию.**Примечание:** Это может также использоваться в целях проверки.`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#`

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Страница поддержки системы обнаружения несанкционированного доступа Cisco
- Подпишитесь на активные уведомления об обновлении Cisco IDS
- Документация по Netranger
- Техническая поддержка - Cisco Systems