Atualização do Módulo do Sistema de Detecção de Intrusão

Índice

Introdução

Este documento explica como executar uma elevação do módulo de Sistema de Detecção de Intrusão da Cisco (IDSM) em um partição de aplicativo, no pacote de serviços, e em uma atualização de assinatura. Para obter mais detalhes sobre como atualizar o Sensor de IDS, consulte o Catalyst 6000 Intrusion Detection System Module.

Pré-requisitos

Requisitos

Antes de tentar utilizar esta configuração, verifique se os seguintes pré-requisitos são atendidos:

- Comece com um IDS Sensor que esteja ativo e ainda se comunicando com o Director até o momento da atualização.
- Você deve ser capaz de utilizar ping, FTP passivo e Telnet com êxito para chegar ao Sensor,

sem interferência de qualquer tipo de firewall ou dispositivo de filtragem de pacote de informação, antes da atualização.
- Verifique se você tem um servidor FTP que suporta o modo passivo.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware:

- Versão de software running modelo 2.5 do sensor IDSM WS-X6381-IDS.
- IDS diretor que executa a versão 2.6 de Solaris, versão x5.01 do HP OpenView, versão de software 2.2.3 S9 do IDS diretor.
- Estação de trabalho da versão 2.8 de Solaris com FTP passivo e acesso do telnet ao sensor e ao diretor.
- Transfira os arquivos das transferências (IDSk9-sig-3.0-2-S10.bin e nrdirUpdate-S10.bin, são usados neste documento).

Nota: As versões exatas utilizadas neste documento podem não estar disponíveis atualmente.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

- O IDS Director é nomeado "dir1" e o endereço IP é 192.168.1.3.
- O sensor IDSM é denominado "idsm" e o endereço IP é 192.168.1.2.
- O ID do host corresponde ao último octeto do endereço IP nos exemplos.
- A identificação de organização é definida como "1."
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor FTP é 10.0.0.1.

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Atualizando a partição do aplicativo IDSM

As etapas a seguir mostram como atualizar o IDSM da versão 2.5(1)S2 do aplicativo para 3.0(1)S4. Salvar a configuração IDSM antes que a elevação, como o disco rígido inteiro IDSM estiver formatada e toda a configuração for perdida.

Instruções passo a passo

Siga as instruções fornecidas abaixo.

1. Abra uma sessão no IDSM e salve a saída do comando show configuration, como exibido no exemplo a seguir.
```
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. Transfira os arquivos apropriados das transferências.O sensor de IDS e os arquivos leia-me estão localizados na seção Cisco IDS Appliance Sensor 3DES. O IDS diretor e os arquivos de leia-me são ficados situado sob a seção do *Cisco IDS Diretor 3DES*. Neste documento, os seguintes arquivos são usados, porém você deve se usar o que arquivos são os mais atuais:
```
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. Coloque os arquivos no diretório apropriado do servidor FTP.Neste exemplo, os arquivos são colocados no diretório raiz. Veja abaixo um exemplo do cliente FTP para o 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. Ajuste a separação da manutenção como o partição ativa, a seguir o console no IDSM à separação da manutenção (o aplicativo é a configuração padrão) e ajuste o parâmetro da configuração de rede do IDSM.No exemplo a seguir, o IDSM está no slot 8 do chassi do 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: Reinicialize o módulo para que as alterações sejam aplicadas.
5. Quando o IDSM terminar a reinicialização, inicie a sessão do IDSM novamente e instale a partição do aplicativo inativa, emitindo o comando ids-installer, como mostrado no exemplo a seguir.
```
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
```

Verificando a atualização da partição do aplicativo

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados

comandos show, o que permite exibir uma análise da saída do comando show.

Recarregue o IDSM de volta ao partição de aplicativo e verifique que a imagem esteve promovida com sucesso, segundo as indicações do exemplo seguinte.

```
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
```

Atualizando o Service Pack do IDSM

Use o seguinte procedimento para atualizar o pacote de serviços IDSN.

1. A sessão no IDSM emitindo o **comando session -** (onde # é o número de módulo), e emite o **comando configure terminal**, segundo as indicações do exemplo seguinte.`idsm#`
   `idsm#`**`configure terminal`**
2. Emita o comando apply ftp://<username@server/dir/filename> para conectar-se por meio de FTP e aplique o service pack, conforme mostrado no exemplo a seguir.`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...
```

Verificando a atualização do service pack

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Inicie uma sessão no IDSM, emitindo o comando session # (em que # é o número do módulo), e emita o comando show configuration, como apresentado no exemplo a seguir.

```
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#
```

Atualizando assinaturas de IDSM

Use o seguinte procedimento para promover as assinaturas de ISDM.

1. A sessão no IDSM emitindo o **comando session -** (onde # é o número de módulo), e emite o **comando configure terminal**, segundo as indicações do exemplo seguinte.`idsm# idsm#configure terminal`
2. Emita o comando apply ftp://<username@server/dir/filename> para conectar por FTP e aplique as assinaturas de IDSM, como mostrado no seguinte exemplo:`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:
```

Verificando a atualização da assinatura

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Inicie uma sessão no IDSM, emitindo o comando session # (em que # é o número do módulo), e emita o comando show configuration, como apresentado no exemplo a seguir.

```
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#
```

Promovendo o IDSM2

As seguintes seções fornecem a informação em promover o ISDM2.

Promovendo a separação da manutenção

Para promover a separação da manutenção de 1.3.1 a 1.3.2, carreg a lâmina IDSM2 no partição de aplicativo emitindo os comandos seguintes no interruptor.

```
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
```

Uma vez criar nova imagem está completo e o sistema recarregou, uma **versão da mostra** permitirá que você confirme que a elevação era bem sucedida.

```
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 o partição de aplicativo da separação da manutenção

Cuidado: Após ter criar nova imagem o Módulo IDS, você deve inicializar o Módulo IDS usando o **comando setup**. Este processo remove toda a configuração de sensor e novas imagens o partição de aplicativo. Este processo deve ser usado somente se o partição de aplicativo é corrompido ou inacessível. Se o partição de aplicativo é acessível, para evitar configuração atual perdedora, use a elevação da imagem menor para promover do partição de aplicativo próprio.

1. Bota na separação da manutenção emitindo os comandos seguintes no interruptor.`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. Log no Módulo IDS incorporando o seguinte nome de usuário e senha.`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. Incorpore o modo terminal de configuração usando o **comando configure terminal**.
4. Execute a nova imagem usando o comando do **file> do ftp server IP>/<directory path>/<image do <user>@< de ftp:// da elevação**.Você será alertado incorporar a senha do servidor FTP (se for necessário). Você será alertado igualmente continuar com a instalação. Incorpore **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. Recarregue o Módulo IDS ao partição de aplicativo inscrevendo o **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. Quando o Módulo IDS recarregou, verifique a versão de software.**Nota:** Isto pode igualmente ser usado para efeitos de verificação.`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. Entre ao partição de aplicativo CLI e inicialize o Módulo IDS, usando o **comando setup**.

Elevação da imagem menor

Esta atualização pode ser usada nas situações onde o partição de aplicativo é ainda acessível, mas somente parte de este aplicativo é quebrado. Em relação a usar a imagem completa à nova imagem o partição de aplicativo, a imagem menor retém as configurações de sensor.

Para instalar a atualização menor, siga estas etapas:

1. Log no CLI usando uma conta com privilégios do administrado.
2. Incorpore o modo de configuração emitindo o **comando configure terminal**.
3. Datilografe o **comando upgrade [URL]/<filename>** promover o sensor.**O [URL]** é o Uniform Resource Locator que aponta a onde o pacote da atualização de assinatura é encontrado. Por exemplo, para recuperar a atualização através do FTP, entre no seguinte: **upgrade ftp://<username>@<ip-address>//<directory>/<filename>** Os métodos disponíveis do transporte são SCP, FTP, HTTP, ou HTTPS.
4. Incorpore a senha apropriada quando alertado.
5. Para terminar **sim a** elevação, tipo quando alertado.

Promovendo o pacote de serviços IDSM2 ou as assinaturas

Use o seguinte procedimento para promover o saco ou as assinaturas do serviço ISDM2.

1. Para promover o sensor com um pacote de serviços ou uma assinatura, bota acima no partição de aplicativo.`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. Log no Módulo IDS CLI.
3. Enter configura o modo terminal usando o **comando configure terminal**.
4. Incorpore o comando do **file> do bloco do ftp server IP>/<directory path>/<service do <user>@< de ftp:// da elevação** instalar o pacote de serviços e quando alertado, o tipo **y** para confirmar a instalação.As repartições do módulo quando a instalação estiver 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. Depois que o módulo recarregou, incorpore o interruptor CLI e verifique a versão.**Nota:** Isto pode igualmente ser usado para efeitos de verificação.`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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Página de suporte do Cisco Secure Intrusion Detection
- Subscreva às Notificações de atualização ativa do Cisco IDS
- Documentação para Netranger
- Suporte Técnico - Cisco Systems