Procedimento de Recuperação de Senha para o Cisco IDS Sensor e Módulos de Serviços IDS (IDSM-1, IDSM-2)

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Versão de ferramenta IDS 3
Recuperação de senha da ferramenta de IDS que executa a versão 3
Criar nova imagem da ferramenta de IDS essa versão 3 das corridas
Versão de ferramenta IDS 4
Procedimento de recuperação se o nome de usuário de administrador/senha é sabido
Procedimento de recuperação se o username do serviço/senha é sabido
Criar nova imagem a ferramenta de IDS que executa a versão 4
Versão 5 e versão 6 do dispositivo IPS
O Reload, fechou, restaurou, e recuperou o AIP-SSM
Nova imagem a imagem do sistema AIP-SSM
IDSM
Criar nova imagem o IDSM com interruptor que executa o código do Native IOS (IO integrados)
Criar nova imagem o IDSM com interruptor que executa o código híbrido (de Cactos)
ISDM-2
Procedimento de recuperação se o nome de usuário de administrador/senha é sabido
Procedimento de recuperação se o username do serviço/senha é sabido
Criar nova imagem o IDSM-2 com interruptor que executa o código do Native IOS (IO integrados)
Criar nova imagem para o IDSM-2 com interruptor que executa o código híbrido (de Cactos)
Informações Relacionadas

Introdução

Este documento fornece procedimentos de como recuperar seu dispositivo Cisco Secure Intrusion Detection System (IDS) (anteriormente NetRanger) e os módulos para todas as versões.

Pré-requisitos

Requisitos

Se um servidor FTP é precisado, deve apoiar o modo passivo. Os CD da recuperação podem ser obtidos usando a ferramenta de upgrade de produto (clientes registrados somente).

Componentes Utilizados

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

- Versões de ferramenta IDS 3 e 4
- Versões 5 e 6 do dispositivo IPS
- Versão 3 do Módulo IDS (IDSM) e versão 4 IDSM-2

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

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

Versão de ferramenta IDS 3

Duas opções estão disponíveis para o dispositivo da versão 3. Você pode usar o processo de recuperação de senha ou você pode fazer criar nova imagem que usa o CD da recuperação da versão 3. Note que toda a informação está perdida criar nova imagem. O procedimento de recuperação de senha é essencialmente uma recuperação de senha de Solaris. Use somente esta opção se você não tem uma estação de gerenciamento (Cisco Secure Policy Manager (CSPM), VPN/Security Management Solution (VMS), o UNIX Diretor) de que você pode copiar a configuração.

Com versão de ferramenta IDS 3 e mais adiantado, dois nomes de usuário existem “netrangr chamado” e “raiz”. A senha padrão para ambos é “ataque”.

Recuperação de senha da ferramenta de IDS que executa a versão 3

Estes arquivos são necessários a fim recuperar a sua senha.

- Disco do Wizard da configuração de dispositivo de Solaris (disco de inicialização). Você pode transferir os arquivos da site de suporte de Sun .**Nota:** Se este link não trabalha, tente ir ao nível superior da site de suporte de Sun e procurar por *transferências do direcionador de Solaris do disco de inicialização do assistente de configuração de dispositivo* sob direcionadores. O Cisco Systems, Inc. não mantém a site de suporte de Sun e não tem nenhum controle sobre onde o índice é encontrado.
- Solaris para a CD-ROM de Intel (x86).
- Acesso de console à estação de trabalho.

Termine estas etapas a fim recuperar a senha.

1. Introduza o disco de inicialização.
2. Introduza o CD na unidade de Cd-ROM.

3. Desligue a estação de trabalho, espere dez segundos, e gire-os sobre.As inicializações de sistema do disco de inicialização. Após alguma configuração, os displays de tela do assistente de configuração inicial.
4. Pressione o **F3** a fim fazer uma varredura parcial do sistema para dispositivos de inicialização.Quando a varredura for terminada, uma lista de indicadores dos dispositivos.
5. Certifique-se que o dispositivo CD-ROM aparece na lista de dispositivos, e pressiona então o **F2** a fim continuar.Displays de tela uma lista de dispositivos de inicialização.
6. Selecione a **unidade de Cd-ROM**, e pressione então a barra de espaço.Há um “X” ao lado do dispositivo CD-ROM.
7. Pressione o **F2** a fim continuar.Da estação de trabalho as botas agora da CD-ROM.
8. Na tela usada para selecionar um tipo de instale, escolha a **opção 2, Jumpstart**.O sistema continua a carreg.
9. Na alerta para selecionar uma língua, escolha a **opção 0** para o inglês.
10. Na tela seguinte para línguas, escolha a **opção 0** outra vez para o ANSI inglês.O sistema continua a carreg e a tela da instalação solaris aparece.
11. Pressione e guarde a chave de **controle** e o tipo **C** a fim parar o script de instalação e permitir-lhe o acesso à alerta.
12. Tipo **montagem - Ufs /dev/dsk/c0t0d0s0 /mnt F.**“/” Separação é montado agora no ponto de montagem “/mnt”. Aqui de você pode editar o arquivo “/etc/shadow” e remover a senha root.
13. Datilografe o **CD /mnt/etc**.
14. Ajuste o ambiente shell assim que você pode ler os dados corretamente.Datilografe **TERM=ansi**.Datilografe o **TERMO da exportação**.
15. Tipo **sombra de vi**.Você está agora no arquivo da sombra e pode remover a senha. A entrada precisa de ser:
    `root:gNyqp8ohdfxPI:10598::::::` “: ” é um separador de campo e a senha criptografada é o segundo campo.
16. Suprima do segundo campo. Por exemplo,`root:gNyqp8ohdfxPI:10598::::::`émudado a `root::10598::::::`. Isto remove a senha para o usuário de raiz.
17. Digite: **wq!** a fim redigir e parar o arquivo.
18. Remova o disco e a CD-ROM das movimentações.
19. Datilografe o **init 6** a fim recarregar o sistema.
20. Datilografe a **raiz no** início de uma sessão: a alerta e pressiona então **entra**.
21. A imprensa **entra na** solicitação da senha.Você é entrado agora ao sensor do Cisco Secure IDS.

Criar nova imagem da ferramenta de IDS essa versão 3 das corridas

Termine estas etapas a fim criar nova imagem a ferramenta de IDS que executa a versão 3.

Nota: Assegure-se de que um rato não esteja conectado ao sensor antes que você continue.

1. Introduza o CD da recuperação da versão 3 na ferramenta de IDS e recarregue-o.
2. Siga as alertas baseadas em sua instalação até que a recuperação esteja bem sucedida.
3. Entre usando o nome de usuário/senha padrão da “raiz/ataque”.
4. **Sysconfig-sensor** executado a fim reconfigurar o dispositivo.

Versão de ferramenta IDS 4

Procedimento de recuperação se o nome de usuário de administrador/senha é sabido

Se uma senha para uma conta de administrador é sabida, esta conta de usuário pode ser usada a fim restaurar outras senhas do usuário.

Por exemplo, dois nomes de usuário são configurados na ferramenta de IDS chamada “Cisco” e “usuário com direitos de administrador”. A senha para o usuário “Cisco” precisa de ser restaurada, assim que o “usuário com direitos de administrador” entra e restaura a senha.

```
sv8-4-ids4250 login: adminuserPassword:!--- Output is suppressed. idsm2-sv-rack#configure
terminal idsm2-sv-rack(config)#no username cisco idsm2-sv-rack(config)#username cisco priv admin
password 123cisco123 idsm2-sv-rack(config)#exit idsm2-sv-rack#exit sv8-4-ids4250 login: cisco
Password: !--- Output is suppressed. sv8-4-ids4250#
```

Procedimento de recuperação se o username do serviço/senha é sabido

Se uma senha para a conta de serviço é sabida, esta conta de usuário pode ser usada a fim restaurar outras senhas do usuário.

Por exemplo, três nomes de usuário são configurados na ferramenta de IDS nomeada “Cisco”, “usuário com direitos de administrador”, e “serviceuser”. A senha para o usuário “Cisco” precisa de ser restaurada, assim que o “serviceuser” entra e restaura a senha.

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

Nota: A senha root é a mesma que a senha da conta de serviço.

Criar nova imagem a ferramenta de IDS que executa a versão 4

Termine estas etapas a fim criar nova imagem a ferramenta de IDS.

Nota: Assegure-se de que um rato não esteja conectado ao sensor antes que você continue.

1. Introduza o CD da recuperação da versão 4 na ferramenta de IDS e recarregue-o.
2. Siga as alertas baseadas em sua instalação até que a recuperação esteja bem sucedida.
3. Entre usando o nome de usuário/senha padrão que é “Cisco/Cisco”.
4. Execute a instalação a fim reconfigurar o dispositivo.

Versão 5 e versão 6 do dispositivo IPS

O Reload, fechou, restaurou, e recuperou o AIP-SSM

Use estes comandos recarregar, fechado, restauração, recuperar a senha, e recuperar o módulo de Serviços de segurança avançado da inspeção e da prevenção (AIP-SSM) diretamente da

ferramenta de segurança adaptável:

Nota: Você pode inscrever os **comandos hw-module do** modo de exec privilegiado ou do modo de configuração global. Você pode incorporar os comandos ao único modo roteado e ao único modo transparente. Para os dispositivos de segurança adaptáveis que se operam no multi-modo (distribuído ou transparente) do multi-modo você pode somente executar os **comandos hw-module do** contexto do sistema (não dos contextos do administrador ou do usuário).

- **reload do** *slot_number do* **módulo do módulo HW** — Este comando recarrega o software no AIP-SSM sem fazer uma reinicialização de hardware. É eficaz somente quando o AIP-SSM está no estado ascendente.
- **parada programada do** *slot_number do* **módulo do módulo HW** — Este comando fechou o software no AIP-SSM. É eficaz somente quando o AIP-SSM está no estado ascendente.
- *slot_number do* **módulo do módulo HW restaurado** — Este comando executa uma reinicialização de hardware do AIP-SSM. É aplicável quando o cartão está nos estados Up/Down/Unresponsive/Recover.
- **senha-restauração do** *slot_number do* **módulo do módulo HW** — Este comando recupera uma senha no 5500 Series o módulo de Serviços de segurança satisfeito da Segurança de Cisco um ASA e do controle (CSC-SSM) ou o AIP-SSM sem ter que criar nova imagem o dispositivo.**Nota:** Este comando começa o apoio de IPS 6.0 (versão ASA 7.2) e é usado para restaurar a senha de conta do CLI Cisco ao padrão **Cisco**.
- *o slot_number do* **módulo do módulo HW recupera [bota | pare | configurar]** — o comando da **recuperação** indica um grupo de opções interativas para ajustar ou mudar os parâmetros da recuperação. Você pode mudar o parâmetro ou para manter o ajuste existente quando você pressiona **entre**.Para o procedimento que você se usa para recuperar o AIP-SSM, veja a instalação da imagem do sistema AIP-SSM.*o slot_number do* **módulo do módulo HW recupera a bota** — Este comando inicia a recuperação do AIP-SSM. É aplicável somente quando AIP-SSM está no estado ascendente.*o slot_number do* **módulo do módulo HW recupera a parada** — Este comando para a recuperação do AIP-SSM. É aplicável somente quando o AIP-SSM está no estado da recuperação.**Nota:** Se a recuperação AIP-SSM precisa de ser parada, você deve emitir o **módulo 1 do módulo HW recupera o comando stop** dentro de 30 a 45 segundos depois que você começa a recuperação AIP-SSM. Se você espera mais por muito tempo, pode conduzir às consequências inesperadas. Por exemplo, o AIP-SSM pôde vir acima no estado sem resposta.**o módulo 1 do módulo HW recupera configura** — Use este comando configurar parâmetros para a recuperação de módulo. Os parâmetros essenciais são o lugar do endereço IP de Um ou Mais Servidores Cisco ICM NT e da imagem de recuperação TFTP URL.Exemplo:`aip-ssm#`**`hardware-module module 1 recover configure`** `Image URL [tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-1.img]: Port IP Address [10.89.149.226]: VLAN ID [0]: Gateway IP Address [10.89.149.254]:`

Nova imagem a imagem do sistema AIP-SSM

Termine estas etapas a fim instalar a imagem do sistema AIP-SSM:

1. Entre ao ASA.
2. Incorpore o modo enable:`asa>enable`
3. Configurar os ajustes da recuperação para o AIP-SSM:`asa#`**`hw-module module 1 recover configure`** **Nota:** Se você faz um erro na configuração da recuperação, use o **módulo 1 do módulo HW recuperam o comando stop** parar o sistema que reimaging e então você pode

corrigir a configuração.

4. Especifique o TFTP URL para a imagem do sistema:`Image URL [tftp://0.0.0.0/]:` Exemplo:`Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img`
5. Especifique o comando e a interface de controle do AIP-SSM:`Port IP Address [0.0.0.0]:`Exemplo:`Port IP Address [0.0.0.0]: 10.89.149.231`
6. Deixe o ID de VLAN em 0. `VLAN ID [0]:`
7. Especifique o gateway padrão do AIP-SSM:`Gateway IP Address [0.0.0.0] :`Exemplo:`Gateway IP Address [0.0.0.0]:10.89.149.254`
8. Execute a recuperação:`asa#`**`hw-module module 1 recover boot`**
9. Verifique periodicamente a recuperação até que esteja completa:**Nota:** O estado lê guest@localhost.localdomain # durante a recuperação e lê guest@localhost.localdomain # quando reimaging está completo.`asa#`**`show module 1`** `Mod Card Type Model Serial No. --- ----- -------------------------------------- ------------------ ----------- 0 ASA 5540 Adaptive Security Appliance ASA5540 P2B00000019 1 ASA 5500 Series Security Services Module-20 ASA-SSM-20 P1D000004F4 Mod MAC Address Range Hw Version Fw Version Sw Version --- ------------ ------------------- ------------ ------------ --------------- 0 000b.fcf8.7b1c to 000b.fcf8.7b20 0.2 1.0(7)2 7.0(0)82 1 000b.fcf8.011e to 000b.fcf8.011e 0.1 1.0(7)2 5.0(0.22)S129.0 Mod Status --- ------------------ 0 Up Sys 1 Up asa#` **Nota:** A fim debugar todos os erros que possam acontecer no processo de recuperação, use o comando da **inicialização de módulo debugar** permitir a eliminação de erros do processo reimaging do sistema.
10. A sessão ao AIP-SSM e inicializa o AIP-SSM com o **comando setup**.

IDSM

Não há nenhum método que você pode se usar para executar uma recuperação de senha no IDSM quando a configuração for retida.

Nota: Este procedimento exige o uso da separação da manutenção. Se a senha de partição de manutenção foi mudada e você é incapaz de entrar, o IDSM precisa de ser substituído. Neste caso, Suporte técnico de Cisco do contato para o auxílio.

Criar nova imagem o IDSM com interruptor que executa o código do Native IOS (IO integrados)

Termine estas etapas a fim criar nova imagem o ISDM com um interruptor que execute o código do Native IOS (IO integrados).

1. Carreg o IDSM à separação da manutenção usando o **módulo hdd:2 restaurado** *x do* **módulo HW do** comando switch onde *x* representa o número de slot.`SV9-1#`**`show module 6`** `Mod Ports Card Type Model Serial No. --- ----- -------------------------------------- ---------- --- ----------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- --------------------------------- ------ ----------- ----------- --- ---- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok SV9-1#`**`hw-module module 6 reset hdd:2`** `Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y % reset issued for module 6` *`!--- Output suppressed.`*
2. Certifique-se do IDSM venha em linha usando o **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM tem 2 encontrados no início que indica que o software de partição de manutenção é executado atualmente no IDSM e que o estado é APROVADO.`SV9-1#`**`show module 6`** `Mod Ports Card Type Model Serial No. --- ----- --`

```
---------------------------------- ----------------- ----------- 6 2 Intrusion Detection
System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------------------
------------ ------ ------------ ------------ ------- 6 0002.7e39.2b20 to 0002.7e39.2b21
1.2 4B4LZ0XA 2.5(0) Ok
```

3. Conecte à separação da manutenção IDSM usando o **processador 1. do entalhe** *x da* **sessão do** comando switch.Use o username/senha dos **ciscoids/ataque**.`SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: ciscoidsPassword: maintenance#`
4. Instale a imagem posta em esconderijo a fim criar nova imagem o partição de aplicativo IDSM.Emita o **sistema /cache /show do** comando ids-installer dos diagnósticos a fim verificar que a imagem posta em esconderijo existe.`maintenance#diag maintenance(diag)#ids-installer system /cache /show Details of the cached image: Package Name : IDSMk9-a-3.0-1-S4 Release Info : 3.0-1-S4 Total CAB Files in the package : 5 CAB Files present : 5 CAB Files missing : 0 List of CAB Files missing ----------------------- maintenance(diag)#` Se nenhuma imagem posta em esconderijo existe ou a versão posta em esconderijo não é essa que você quer instalar, continue pisar 5.A fim criar nova imagem o ISDM usando a imagem posta em esconderijo, use o **sistema /cache /install do** comando ids-installer dos diagnósticos.`maintenance(diag)#ids-installer system /cache /install Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is E41E-3608 Extracting the image... !--- Output is suppressed. STATUS: Image has been successfully installed on drive C:\!` Uma vez criar nova imagem terminou, continua a etapa 12.
5. Certifique-se de que o IDSM tem a conectividade IP. Emita o comando ping ip_address.`maintenance#diag maintenance(diag)#ping 10.66.84.1 Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255`
6. Se o IDSM tem a conectividade IP, continue a etapa 11. Se você não tem a conectividade IP, continue com etapas 7 a 9.
7. Certifique-se de que o comando e a interface de controle estão configurados corretamente no interruptor. Emita o comando show run interface Gigx/2.`SV9-1#show run interface Gig6/2 Building configuration... Current configuration : 115 bytes ! interface GigabitEthernet6/2 no ip address switchport switchport access vlan 210 switchport mode access end SV9-1#`
8. Certifique-se de que os parâmetros de comunicação estão configurados corretamente na separação da manutenção IDSM. Emita o **netconfig /view do** comando ids-installer dos diagnósticos.`maintenance#diag maintenance(diag)#ids-installer netconfig /view IP Configuration for Control Port: IP Address : 10.66.84.124 Subnet Mask : 255.255.255.128 Default Gateway : 10.66.84.1 Domain Name Server : 1.1.1.1 Domain Name : cisco Host Name : idsm-sv-rack`
9. Se nenhuns dos parâmetros são ajustados, ou se algum deles necessidade de ser mudado, use os *parâmetros de* **/configure do netconfig do** comando ids-installer dos diagnósticos.`maintenance(diag)#ids-installer netconfig /configure / ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 / dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack STATUS: Network parameters for the config port have been configured ! NOTE: Reset the module for the changes to take effect!`
10. Conectividade IP da verificação outra vez depois que você restaurou o IDSM para que as mudanças tomem o efeito. Se a conectividade IP é ainda uma edição, pesquise defeitos conforme um problema de conectividade IP normal, a seguir continue com etapa 11.
11. Criar nova imagem o partição de aplicativo IDSM. Transfira a imagem usando o **=account /save de** */user dos* **=ip_address do sistema /nw /install /server do ids-instalador do** comando diagnostic **= =file_prefix {***sim/não***} de /prefix do =ftp_path de /dir** onde:*os ip_address* são o

endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor FTP.*a conta* é o usuário ou o nome da conta a ser usados ao registrar no servidor FTP.*salvar* determina se salvar uma cópia da imagem baixada como a cópia posta em esconderijo. Se sim, toda a imagem posta em esconderijo que existir overwritten. Se nenhum, a imagem baixada é instalada no partição inativa mas em uma cópia posta em esconderijo não salvar.*o ftp_path* especifica o diretório no servidor FTP onde os arquivos de imagem são encontrados.*o file_prefix* é o nome de arquivo do arquivo do .DAT na imagem baixada. A imagem baixada consiste em um arquivo com a extensão do .DAT e em diversos arquivos com a extensão .cab. As necessidades do valor do file_prefix de ser o nome do arquivo DAT, até mas não incluindo o sufixo do .DAT.`maintenance#`**`diag`** `maintenance(diag)#`**`ids-installer system /nw /install /server=10.66.64.10 /user=cisco /save=yes /dir='/tftpboot/georgia' /`** `prefix=IDSMk9-a-3.0-1-S4 Please enter login password: ***** Downloading the image.. File 05 of 05 FTP STATUS: Installation files have been downloaded successfully ! Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is 2407-F686 Extracting the image... !--- Output is suppressed. STATUS: Image has been successfully installed on drive C:\!`

12. Carreg o IDSM ao partição de aplicativo usando o **módulo hdd:1 restaurado x do módulo HW do** comando switch.`SV9-1#`**`hw-module module 6 reset hdd:1`** `Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y !-- Output is suppressed.` Igualmente assegure-se de que o interruptor esteja configurado para carreg acima do IDSM no partição de aplicativo. A fim verificar isto, use o **módulo** *x. do* **dispositivo do** comando show bootvar.`SV9-1#`**`show bootvar device module 6`** `[mod:6 ]: SV9-1#` A fim configurar a variável do dispositivo de inicialização para o IDSM, use o **módulo x hdd:1 do dispositivo de inicialização do** comando switch configuration.`SV9-1#`**`configure terminal`** `Enter configuration commands, one per line. End with CNTL/Z. SV9-1(config)#`**`boot device module 6 hdd:1`** `Device BOOT variable = hdd:1 Warning: Device list is not verified. SV9-1(config)#endSV9-1#`**`show bootvar device module 6`** `[mod:6 ]: hdd:1 SV9-1#`
13. Certifique-se do IDSM venha em linha usando o **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM é uma versão do partição de aplicativo, por exemplo *3.0(1)S4*, e de que o estado é APROVADO.`SV9-1#`**`show module 6`** `Mod Ports Card Type Model Serial No. --- ----- ------------------------------------ -------- ---------- ----------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------------------------------- ------ ------------ ------- ------- ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok`
14. Conecte ao IDSM agora que carreg acima no partição de aplicativo e configurar-lo assim que pode comunicar-se ao diretor. Use o comando setup.Uma comunicação com o diretor foi estabelecida uma vez, configuração pode ser transferida ao IDSM.Use o username/senha dos **ciscoids/ataque** a fim entrar.`SV9-1#session slot 6 proc 1`
```
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: ciscoids
Password:#setup --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration diaglog at any prompt. Default settings are in square brackets '[]'. Current Configuration: Configuration last modified Never Sensor: IP Address: 10.0.0.1 Netmask: 255.0.0.0 Default Gateway:Host Name: Not Set Host ID: Not Set Host Port: 45000 Organization Name: Not Set Organization ID: Not Set Director: IP Address: Not Set Host Name: Not Set Host ID: Not Set Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: Not Set Organization ID: Not Set Direct Telnet access to IDSM: disabled Continue with configuration dialog? [yes]: Enter virtual terminal password[]: Enter sensor IP address[10.0.0.1]: 10.66.84.124 Enter sensor netmask [255.0.0.0]: 255.255.255.128 Enter sensor default gateway []: 10.66.84.1 Enter sensor host name []: idsm-sv-rack Enter sensor host id []: 124 Enter sensor host post office port [45000]: Enter sensor organization name []: cisco Enter sensor organization id []: 100 Enter director IP address[]: 10.66.79.249 Enter director host name []: vms1 Enter director
```

```
host id []: 249 Enter director host post office port [45000]: Enter director heart beat
interval [5]: Enter director organization name []: cisco Enter director organization id
[]: 100 Enable direct Telnet access to IDSM? [no]: The following configuration was
entered: Configuration last modified Never Sensor:IP Address: 10.66.84.124 Netmask:
255.255.255.128 Default Gateway: 10.66.84.1 Host Name: idsm-sv-rack Host ID: 124 Host
Port: 45000 Organization Name: cisco Organization ID: 100 Director: IP Address:
10.66.79.249 Host Name: vms1 Host ID: 249 Host Port: 45000 Heart Beat Interval (secs): 5
Organization Name: cisco Organization ID: 100 Direct Telnet access to IDSM: disabled
WARNING: Applying this configuration will cause all configuration files to be initialized
and the card to be rebooted. Apply this configuation?: yes Configuration Saved.
Resetting... !--- Output is suppressed.
```

Criar nova imagem o IDSM com interruptor que executa o código híbrido (de Cactos)

Termine estas etapas a fim criar nova imagem o ISDM com um interruptor que execute o código híbrido (de Cactos).

Nota: Toda a informação é perdida no partição de aplicativo. Não há nenhum método que você pode se usar para executar uma recuperação de senha no IDSM quando você retiver a configuração.

Nota: Este procedimento exige o uso da separação da manutenção. Se a senha de partição de manutenção foi mudada e você é incapaz de entrar, o IDSM precisa de ser substituído. Neste caso, Suporte técnico de Cisco do contato para o auxílio.

1. Carreg o IDSM à separação da manutenção com a **restauração** *x* **hdd:2 do** comando switch.`ltd9-9> (enable) **show module 4** Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ ------------------ --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ------------------- ----------- 4 SAD063000CE Mod MAC-Address(es) Hw Fw Sw --- ------------------------------------ ------ ---------- ---------------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 3.0(5)S23 ltd9-9> (enable)**reset 4 hdd:2** This command will reset module 4. Unsaved configuration on module 4 will be lost Do you want to continue (y/n) [n]? y Module 4 shut down in progress, please don't remove module until shutdown completed. !--- Output is suppressed.`
2. Certifique-se do IDSM venha em linha com o **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM tem 2 encontrados no início que indica que o software de partição de manutenção é executado atualmente no IDSM e que o estado é APROVADO.`ltd9-9> (enable) **show module 4** Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ ------------------ --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ------------------- ---- ------- 4 SAD 063000CEMod MAC-Address(es) Hw Fw Sw --- ------------------------------------ ------ ---------- ---------------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 2.5(0)`
3. Conecte ao IDSM agora que carreg acima na separação da manutenção com a **sessão** *x. do* comando switch.Use o username/senha dos **ciscoids/ataque**.`ltd9-9> (enable)**session 4** Trying IDS-4... Connected to IDS-4. Escape character is '^]'. login: ciscoids Password: maintenance#`
4. Instale a imagem posta em esconderijo a fim criar nova imagem o partição de aplicativo IDSM.Verifique que a imagem posta em esconderijo existe com o uso do **sistema /cache /show do** comando ids-installer dos diagnósticos.`maintenance#**diag** maintenance(diag)#**ids-installer system /cache /show** Details of the cached image: Package Name : IDSMk9-a-3.0-1-S4 Release Info : 3.0-1-S4 Total CAB Files in the package : 5 CAB Files present : 5 CAB Files missing : 0 List of CAB Files missing ------------------------ maintenance(diag)#` Se nenhuma imagem posta em esconderijo existe, ou a versão posta em esconderijo não é

essa que você quer instalar, continue pisar 5.A fim criar nova imagem o ISDM que usa a imagem posta em esconderijo, use o **sistema /cache /install do** comando ids-installer dos diagnósticos.`maintenance(diag)#`**`ids-installer system /cache /install`** `Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is E41E-3608 Extracting the image...` *`!--- Output is suppressed.`* `STATUS: Image has been successfully installed on drive C:\!` Uma vez que a nova imagem terminou, continue a etapa 12.

5. Certifique-se de que o IDSM tem a conectividade IP com o uso do comando ping ip_address.`maintenance#`**`diag`** `maintenance(diag)#`**`ping 10.66.84.1`** `Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255`
6. Se o IDSM tem a conectividade IP, continue a etapa 11. Se você não tem a conectividade IP, continue com etapas 7 a 9.
7. Certifique-se de que o comando e a interface de controle estão configurados corretamente no interruptor com o uso do comando show port status x/2.`ltd9-9> (enable)`**`show port status 4/2`** `Port Name Status Vlan Duplex Speed Type ----- ------------------- ---------- ---------- ------ ----- ------------ 4/2 connected 1 full 1000 Intrusion De`
8. Certifique-se de que os parâmetros de comunicação estão configurados corretamente na separação da manutenção IDSM com o uso o do **netconfig /view do** comando ids-installer dos diagnósticos.`maintenance#`**`diag`** `maintenance(diag)#`**`ids-installer netconfig /view`** `IP Configuration for Control Port: IP Address : 10.66.84.124 Subnet Mask : 255.255.255.128 Default Gateway : 10.66.84.1 Domain Name Server : 1.1.1.1 Domain Name : cisco Host Name : idsm-sv-rack`
9. Se nenhuns dos parâmetros são ajustados, ou se algum deles necessidade de ser mudado, use os *parâmetros de* **/configure do netconfig do** comando ids-installer dos diagnósticos.`maintenance(diag)#` **`ids-installer netconfig /configure / ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 / dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack`**
10. Conectividade IP da verificação outra vez depois que você restaurou o IDSM para que as mudanças tomem o efeito.Se a conectividade IP é ainda uma edição, pesquise defeitos conforme um problema de conectividade IP normal, a seguir continue com etapa 11.
11. Criar nova imagem o partição de aplicativo IDSM. Transfira a imagem com o uso do **=account /save de /user dos =ip_address do sistema /nw /install /server do ids-instalador do** comando diagnostic **= =file_prefix {***sim/não***} de /prefix do =ftp_path de /dir** onde:*os ip_address* são o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor FTP.*a conta* é o usuário ou o nome da conta a ser usados ao registrar no servidor FTP.*salvar* determina se salvar uma cópia da imagem baixada como a cópia posta em esconderijo. Se sim, toda a imagem posta em esconderijo existente overwritten. Se nenhum, a imagem baixada é instalada no partição inativa mas em uma cópia posta em esconderijo não salvar.*o ftp_path* especifica o diretório no servidor FTP onde os arquivos de imagem são encontrados.*o file_prefix* é o nome de arquivo do arquivo do .DAT na imagem baixada. A imagem baixada consiste em um arquivo com a extensão do .DAT e em diversos arquivos com a extensão .cab. O valor do file_prefix deve ser o nome do arquivo DAT, até mas não incluindo o sufixo do .DAT.`maintenance#`**`diag`** `maintenance(diag)#`**`ids-installer system /nw /install /server=10.66.64.10 /user=cisco /save=yes /dir='/tftpboot/georgia' /prefix=IDSMk9-a-3.0-1-S4`** `Please enter login password: ***** Downloading the image.. File 05 of 05 FTP STATUS: Installation files have been downloaded successfully! Validating integrity of the image... PASSED! Formatting drive C:\....Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is 2407-F686 Extracting the image...` *`!--- Output is suppressed.`* `STATUS: Image has been successfully installed on drive C:\!`

12. Carreg o IDSM ao partição de aplicativo com o uso da **restauração** *x* **hdd:1 do** comando switch.`ltd9-9> (enable)`**`reset 4 hdd:1`** `This command will reset module 4. Unsaved configuration on module 4 will be lost Do you want to continue (y/n) [n]? y` *`!--- Output is suppressed.`* Igualmente certifique-se de que o interruptor está configurado a fim carreg acima do IDSM no partição de aplicativo. IUse o comando show boot device x a fim verificar isto.`ltd9-9> (enable)`**`show boot device 4`** `Device BOOT variable =` A fim configurar a variável do dispositivo de inicialização para o IDSM, use o **dispositivo de inicialização ajustado hdd:1** *x. do* comando switch configuration.`ltd9-9> (enable)`**`set boot device hdd:1 4`** `Device BOOT variable = hdd:1 Warning: Device list is not verified but still set in the boot string. ltd9-9> (enable)`**`show boot device 4`** `Device BOOT variable = hdd:1`
13. Certifique-se do IDSM venha em linha com o uso do **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM é uma versão do partição de aplicativo, por exemplo, *3.0(1)S4*, e de que o estado é APROVADO.`ltd9-9> (enable)`**`show module 4`** `Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ---------- --- ------------------ --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ---------- 4 SAD063000CE Mod MAC-Address(es) Hw Fw Sw --- ---------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 3.0(1)S4`
14. Conecte ao IDSM agora que carreg acima no partição de aplicativo e configurar-lo assim que pode comunicar-se ao diretor. Use o comando setup.Entre com o username/senha dos **ciscoids/ataque**.
```
ltd9-9> (enable)session 4
Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:#setup --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration diaglog at any prompt. Default settings are in square brackets '[]'. Current Configuration: Configuration last modified Never Sensor: IP Address: 10.0.0.1 Netmask: 255.0.0.0 Default Gateway: Host Name: Not Set Host ID: Not Set Host Port: 45000 Organization Name: Not Set Organization ID: Not Set Director: IP Address: Not Set Host Name: Not Set Host ID: Not Set Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: Not Set Organization ID: Not Set Direct Telnet access to IDSM: disabled Continue with configuration dialog? [yes]: Enter virtual terminal password[]: Enter sensor IP address[10.0.0.1]: 10.66.84.124 Enter sensor netmask [255.0.0.0]: 255.255.255.128 Enter sensor default gateway []: 10.66.84.1 Enter sensor host name []: idsm-sv-rack Enter sensor host id []: 124 Enter sensor host post office port [45000]: Enter sensor organization name []: cisco Enter sensor organization id []: 100 Enter director IP address[]: 10.66.79.249 Enter director host name []: vms1 Enter director host id []: 249 Enter director host post office port [45000]: Enter director heart beat interval [5]: Enter director organization name []: cisco Enter director organization id []: 100 Enable direct Telnet access to IDSM? [no]: The following configuration was entered: Configuration last modified Never Sensor: IP Address: 10.66.84.124 Netmask: 255.255.255.128 Default Gateway: 10.66.84.1 Host Name: idsm-sv-rack Host ID: 124 Host Port: 45000 Organization Name: cisco Organization ID: 100 Director:IP Address: 10.66.79.249 Host Name: vms1 Host ID: 249 Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: cisco Organization ID: 100 Direct Telnet access to IDSM: disabled WARNING: Applying this configuration will cause all configuration files to be initialized and the card to be rebooted. Apply this configuation?: yes Configuration Saved. Resetting... !--- Output is suppressed.
```

ISDM-2

Procedimento de recuperação se o nome de usuário de administrador/senha é sabido

Se uma senha para uma conta de administrador é sabida, esta conta de usuário pode ser usada a

fim restaurar outras senhas do usuário.

Por exemplo, dois nomes de usuário são configurados no “Cisco nomeado IDSM-2” e no “usuário com direitos de administrador”. A senha para o usuário “Cisco” precisa de ser restaurada, assim que o “usuário com direitos de administrador” entra e restaura a senha.

```
SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type
'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: adminuser
Password: !--- Output is suppressed. idsm2-sv-rack#configure terminal idsm2-sv-rack(config)#no
username cisco idsm2-sv-rack(config)#username cisco priv admin password 123cisco123 idsm2-sv-
rack(config)#exit idsm2-sv-rack#exit [Connection to 127.0.0.61 closed by foreign host] SV9-
1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit'
at the remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: !---
Output is suppressed. idsm2-sv-rack#
```

Procedimento de recuperação se o username do serviço/senha é sabido

Se uma senha para a conta de serviço é sabida, esta conta de usuário pode ser usada a fim restaurar outras senhas do usuário.

Por exemplo, três nomes de usuário são configurados no “Cisco nomeado IDSM-2”, no “usuário com direitos de administrador”, e no “serviceuser”. A senha para o usuário “Cisco” precisa de ser restaurada, assim que o “serviceuser” entra e restaura a senha.

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

Nota: A senha root é a mesma que a senha da conta de serviço.

Criar nova imagem o IDSM-2 com interruptor que executa o código do Native IOS (IO integrados)

Termine estas etapas a fim criar nova imagem o ISDM-2 com um interruptor que execute o código do Native IOS (IO integrados).

Nota: Toda a informação é perdida no partição de aplicativo. Não há nenhum método que você pode se usar a fim executar uma recuperação de senha no IDSM-2 quando a configuração for retida.

1. Carreg o IDSM-2 à separação da manutenção com o uso do **módulo cf:1 restaurado** *x do* **módulo HW do** comando switch onde *x* representa o número de slot e o cf representa “flashes compactos.**Nota:** Se um problema é encontrado usar cf:1, tente usar hdd:2 como uma alternativa.
```
SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- --------
------------------------------ ------------------ ----------- 6 8 Intrusion Detection
System WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ----------------------
------------- ------ ------------ ------------ ------- 6 0030.f271.e3fd to 0030.f271.e404
0.102 7.2(1) 4.1(1)S47 Ok Mod Sub-Module Model Serial Hw Status --- ----------------------
---- --------------- --------------- ------- ------- 6 IDS 2 accelerator board WS-SVC-
IDSUPG 0347FDB6B8 2.0 Ok Mod Online Diag Status --- ------------------- 6 Pass SV9-1#hw-
module module 6 reset cf:1 Device BOOT variable for reset = Warning: Device list is not
```

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

2. Certifique-se do IDSM-2 venha em linha com o uso do **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM-2 tem “m” situado na extremidade e de que o estado é APROVADO.SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- ------------------------------------ ------------------ ----------- 6 8 Intrusion Detection System (MP) WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ------ --------------------------- ------ ------------ ------------ ------- 6 0030.f271.e3fd to 0030.f271.e404 0.102 7.2(1) 1.3(2)m Ok Mod Sub-Module Model Serial Hw Status --- ---------- ---------------- -------------- -------------- ------- ------- 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 Ok Mod Online Diag Status --- ------------------- 6 Pass
3. Conecte ao IDSM-2 agora que carreg acima na separação da manutenção. Use o comando switch **session slot xprocessor 1.**Use o username/senha de convidado**/Cisco**.SV9-1#**session slot 6 processor 1** The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open Cisco Maintenance image login: guest Password: Maintenance image version: 1.3(2) guest@idsm2-sv-rack.localdomain#
4. Certifique-se de que o IDSM-2 tem a conectividade IP. Use o comando ping ip_address.guest@idsm2-sv-rack.localdomain#**ping 10.66.79.193** guest@idsm2-sv-rack.localdomain#**ping 10.66.79.193** PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data. 64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=2.188 msec 64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.014 msec 64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=991 usec 64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.011 msec 64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.019 msec --- 10.66.79.193 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max/mdev = 0.991/1.244/2.188/0.473 ms guest@idsm2-sv-rack.localdomain#
5. Se o IDSM-2 tem a conectividade IP, continue a etapa 14.
6. Certifique-se de que o comando e a interface de controle estão configurados corretamente no interruptor. Use o comando show run **| intrusion detection inc**.SV9-1#**show run | inc intrusion-detection** intrusion-detection module 6 management-port access-vlan 210
7. Certifique-se de que os parâmetros de comunicação estão configurados corretamente na separação da manutenção IDSM-2. Use o comando show ip.guest@idsm2-sv-rack.local domain#**show ip** IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP Broadcast : 10.66.79.223 DNS Name : idsm2-sv-rack.localdomain Default Gateway : 10.66.79.193Nameserver(s) :
8. Se nenhuns dos parâmetros são ajustados, ou se algum deles necessidade de ser mudado, claro eles todos. Use o comando clear ip.guest@idsm2-sv-rack.localdomain#**clear ip** guest@localhost.localdomain#**show ip** IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0 Nameserver(s) :
9. Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT e a informação de máscara na separação da manutenção IDSM-2. Use o comando ip address ip_address netmask.guest@localhost.localdomain#**ip address 10.66.79.210 255.255.255.224**
10. Configurar o gateway padrão na separação da manutenção IDSM-2. Use o comando ip gateway gateway-address.guest@localhost.localdomain#**ip gateway 10.66.79.193**
11. Configurar o hostname na separação da manutenção IDSM-2. Use o comando ip host hostname.Embora isto não seja necessário, ajuda a identificar o dispositivo desde que este igualmente ajusta a alerta.guest@localhost.localdomain#**ip host idsm2-sv-rack** guest@idsm2-sv-rack.localdomain#
12. Você pôde possivelmente precisar de configurar explicitamente seu endereço de broadcast. Use o comando ip broadcast broadcast-address.A configuração padrão basta geralmente.guest@idsm2-sv-rack.localdomain#**ip broadcast 10.66.79.223**
13. Verifique a conectividade IP outra vez. Se a conectividade IP é ainda uma edição, pesquise defeitos conforme um problema de conectividade IP normal e continue com etapa 14.
14. Criar nova imagem o partição de aplicativo IDSM-2. Use o comando upgrade FTP-*URL* **-- instale**.guest@idsm2-sv-rack.localdomain#**upgrade ftp://cisco@10.66.64.10// tftpboot/WS-SVC-**

IDSM2-K9-a-4.1-1-S47.bin.gz --install Downloading the image. This may take several minutes... Password for cisco@10.66.64.10: 500 'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not understood. ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz (unknown size)/tmp/upgrade.gz [|] 65259K 66825226 bytes transferred in 71.40 sec (913.99k/sec) Upgrade file ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz is downloaded. Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing it [y|N]: y Proceeding with upgrade. Please do not interrupt. If the upgrade is interrupted or fails, boot into Maintenance image again and restart upgrade. Creating IDS application image file... Initializing the hard disk... Applying the image, this process may take several minutes... Performing post install, please wait... Application image upgrade complete. You can boot the image now.

15. Carreg o IDSM-2 ao partição de aplicativo. Use o **módulo hdd:1 restaurado** *x do* **módulo HW do** comando switch.SV9-1#**hw-module module 6 reset hdd:1** Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y % reset issued for module 6 *!--- Output is suppressed.* Alternativamente, você pode usar o **comando reset no** IDSM-2 enquanto a variável do dispositivo de inicialização é ajustada corretamente.A fim verificar a configuração variável do dispositivo de inicialização para ver se há o IDSM-2, use o **módulo bootvar** *x. do* **dispositivo da mostra do** comando switch.SV9-1#**show bootvar device module 6** [mod:6]: SV9-1# A fim configurar a variável do dispositivo de inicialização para o IDSM-2, use o **módulo** *x* **hdd:1 do dispositivo de inicialização do** comando switch configuration.SV9-1#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. SV9-1(config)#boot device module 6 hdd:1 Device BOOT variable = hdd:1 Warning: Device list is not verified. SV9-1(config)#exitSV9-1#**show bootvar device module 6** [mod:6]: hdd:1 A fim restaurar o IDSM-2 através da separação CLI da manutenção, use o comando reset.guest@idsm2-sv-rack.localdomain#**reset** *!--- Output is suppressed.*
16. Certifique-se do IDSM-2 venha em linha. Use o **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM-2 é uma versão do partição de aplicativo, por exemplo *4.1(1)S47* e de que o estado é APROVADO.SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- ------------------------------------ -------- ---------- ----------- 6 8 Intrusion Detection System WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ---------------------------------- ------ ------------ ------- ------- ------- 6 0030.f271.e3fd to 0030.f271.e404 0.102 7.2(1) 4.1(1)S47 Ok Mod Sub-Module Model Serial Hw Status --- -------------------------- -------------- ------------ --- ------- ------- 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 Ok Mod Online Diag Status --- ------------------- 6 Pass
17. Conecte ao IDSM-2 agora que carreg acima no partição de aplicativo. Use o **processador 1. do entalhe** *x da* **sessão do** comando switch.Use o username/senha de **Cisco/Cisco**.SV9-1#**session slot 6 proc 1** The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: You are required to change your password immediately (password aged) Changing password for cisco (current) UNIX password: New password: Retype new password: *!--- Output is suppressed.*
18. Configurar o IDSM-2. Use o comando setup.sensor#**setup** --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration:networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway 10.1.9.1 hostname sensor telnet Option disabled accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit Current time: Sat Sep 20 23:34:53 2003 Setup Configuration last modified: Sat Sep 20 23:32:38 2003 Continue with configuration dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]: 10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The following configuration was entered. networkParams ipAddress 10.66.79.210 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit

```
exit service webServer general ports 443 exit exit [0] Go to the command prompt without
saving this config. [1] Return back to the setup without saving this config. [2] Save this
configuration and exit setup.Enter your selection [2]:Configuration Saved. sensor#
```

Criar nova imagem para o IDSM-2 com interruptor que executa o código híbrido (de Cactos)

Termine estas etapas a fim criar nova imagem o ISDM-2 com um interruptor que execute o código híbrido (de Cactos).

1. Carreg o IDSM-2 na separação da manutenção. Use a **restauração** *x* **hdd:2 do** comando switch.**Nota:** Se um problema é encontrado usar hdd:2, tente usar cf:1 como uma alternativa.
```
SV9-1> (enable)show module 6 Mod Slot Ports Module-Type Model Sub Status --- ---
- ----- ------------------------ ------------------ --- -------- 6 6 8 Intrusion
Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- -------------------- ---
-------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ----------------------------------
--- ------ ---------- ----------------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102
7.2(1) 4.1(1)S47 Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ----------------------
- ------------------- ----------- ------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG
0347FDB6B8 2.0 SV9-1> (enable)reset 6 hdd:2 This command will reset module 6. Unsaved
configuration on module 6 will be lost Do you want to continue (y/n) [n]? y Module 6 shut
down in progress, please don't remove module until shutdown completed. !--- Output is
suppressed.
```
2. Certifique-se do IDSM-2 venha em linha. Use o **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM-2 tem “m” situado na extremidade que indica que as corridas do software de partição de manutenção atualmente e que o estado é APROVADO.
```
SV9-1> (enable)show module 6 Mod Slot Ports Module-Type Model Sub
Status --- ---- ----- ------------------------ ------------------ --- -------- 6 6 8
Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- --------------
------ ----------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- -------------------------
------------ ------ ---------- ----------------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c
0.102 7.2(1) 1.3(2)m Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ------------------
----- ------------------- ----------- ------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG
0347FDB6B8 2.0
```
3. Conecte ao IDSM-2 agora que carreg acima na separação da manutenção. Use a **sessão** *x. do* comando switch.Use o username/senha de convidado**/Cisco**.
```
SV9-1> (enable)session 6 Trying IDS-6... Connected to IDS-6. Escape character is '^]'. Cisco Maintenance image
login: guest Password: Maintenance image version: 1.3(2) guest@idsm2-sv-rack.localdomain#
```
4. Certifique-se de que o IDSM-2 tem a conectividade IP. Use o comando ping ip_address.
```
guest@idsm2-sv-rack.localdomain#ping 10.66.79.193 PING 10.66.79.193
(10.66.79.193) from 10.66.79.210 : 56(84) bytes of data. 64 bytes from 10.66.79.193:
icmp_seq=0 ttl=255 time=1.035 msec 64 bytes from 10.66.79.193: icmp_seq=1 ttl=255
time=1.041 msec 64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=1.066 msec 64 bytes
from 10.66.79.193: icmp_seq=3 ttl=255 time=1.074 msec 64 bytes from 10.66.79.193:
icmp_seq=4 ttl=255 time=1.026 msec --- 10.66.79.193 ping statistics --- 5 packets
transmitted, 5 packets received, 0% packet loss round-trip min/avg/max/mdev =
1.026/1.048/1.074/0.034 ms
```
5. Se o IDSM-2 tem a conectividade IP, continue a etapa 14.
6. Certifique-se de que o comando e a interface de controle estão configurados corretamente no interruptor. Use o comando show port status x/2.
```
SV9-1> (enable)show port status 6/2 Port
Name Status Vlan Duplex Speed Type ----- ------------------- ---------- ---------- ------
----- ------------ 6/2 connected 210 full 1000 Intrusion De
```
7. Certifique-se de que os parâmetros de comunicação estão configurados corretamente na separação da manutenção IDSM-2. Use o comando show ip.
```
guest@idsm2-sv-
rack.localdomain#show ip IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP
Broadcast : 10.255.255.255 DNS Name : idsm2-sv-rack.localdomain Default Gateway :
```

10.66.79.193 Nameserver(s) :

8. Se nenhuns dos parâmetros são ajustados ou se algum deles necessidade de ser mudado, claro eles todos com o uso do comando clear ip.guest@idsm2-sv-rack.localdomain#**clear ip** guest@localhost.localdomain#**show ip** IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0
9. Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT e a informação de máscara na separação da manutenção IDSM-2. Use o comando ip address ip_address netmask.guest@localhost.localdomain#**ip address 10.66.79.210 255.255.255.224** guest@localhost.localdomain#
10. Configurar o gateway padrão na separação da manutenção IDSM-2. Use o comando ip gateway gateway-address.guest@localhost.localdomain#**ip gateway 10.66.79.193** guest@localhost.localdomain#
11. Configurar o hostname na separação da manutenção IDSM-2. Use o comando ip host hostname.Embora isto não seja necessário, ajuda a identificar o dispositivo desde que este igualmente ajusta a alerta.guest@localhost.localdomain#**ip host idsm2-sv-rack** guest@idsm2-sv-rack.localdomain#
12. Você pôde possivelmente precisar de configurar explicitamente seu endereço de broadcast. Use o comando ip broadcast broadcast-address.A configuração padrão basta geralmente.guest@idsm2-sv-rack.localdomain#**ip broadcast 10.66.79.223**
13. Verifique a conectividade IP outra vez. Se a conectividade IP é ainda uma edição, pesquise defeitos conforme um problema de conectividade IP normal a seguir continue com etapa 14.
14. Criar nova imagem o partição de aplicativo IDSM-2. Use o comando upgrade FTP-*URL* **--instale**.guest@idsm2-sv-rack.localdomain#**upgrade ftp://cisco@10.66.64.10// tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz --install** Downloading the image. This may take several minutes... Password for cisco@10.66.64.10:500 'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not understood.ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz (unknown size)/tmp/upgrade.gz [|] 65259K 66825226 bytes transferred in 71.37 sec (914.35k/sec) Upgrade file ftp://cisco@10.66.64.10//tftpboot/ WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz is downloaded. Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing it [y|N]: y Proceeding with upgrade. Please do not interrupt. If the upgrade is interrupted or fails, boot into Maintenance image again and restart upgrade. Creating IDS application image file... Initializing the hard disk...Applying the image, this process may take several minutes...Performing post install, please wait...Application image upgrade complete. You can boot the image now.
15. Carreg o IDSM-2 ao partição de aplicativo. Use a **restauração** *x* **hdd:1 do** comando switch.SV9-1> (enable)**reset 6 hdd:1** This command will reset module 6. Unsaved configuration on module 6 will be lost Do you want to continue (y/n) [n]? y Module 6 shut down in progress, please don't remove module until shutdown completed. *!--- Output is suppressed.* Alternativamente, você pode usar o **comando reset no** IDSM-2 enquanto o a variável do dispositivo de inicialização é ajustada corretamente.A fim verificar a configuração variável do dispositivo de inicialização para ver se há o IDSM-2, use o **dispositivo de inicialização** *x. da* **mostra do** comando switch.SV9-1> (enable)**show boot device 6** Device BOOT variable = (null) (Default boot partition is hdd:1) Memory-test set to PARTIAL A fim configurar a variável do dispositivo de inicialização para o IDSM-2, use o **dispositivo de inicialização ajustado hdd:1** *x. do* comando switch configuration.SV9-1> (enable)**set boot device hdd:1 6** Device BOOT variable = hdd:1 Memory-test set to PARTIAL Warning: Device list is not verified but still set in the boot string. SV9-1> (enable) **show boot device 6** Device BOOT variable = hdd:1 Memory-test set to PARTIAL A fim restaurar o IDSM-2 através da separação CLI da manutenção, use o comando reset.guest@idsm2-sv-rack.localdomain#**reset** *!--- Output is suppressed.*
16. Certifique-se do IDSM-2 venha em linha. Use o **módulo show** *x. do* comando switch.Certifique-se de que a versão de software IDSM-2 é uma versão do partição de

aplicativo, por exemplo *4.1(1)S47,* e de que o estado é APROVADO.`SV9-1> (enable)`**`show module 6`** `Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ---------- --- ------------------ --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- ------------------- ----------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ---------- ------ ---------- -------- --------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47 Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ---------- ------------------ ------- ---- ------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0`

17. Conecte ao IDSM-2 agora que carreg acima no partição de aplicativo. Use a **sessão** *x. do* comando switch.Use o username/senha de **Cisco/Cisco**.`SV9-1> (enable)`**`session 6`** `Trying IDS-6... Connected to IDS-6. Escape character is '^]'. login: cisco Password: You are required to change your password immediately (password aged) Changing password for cisco (current) UNIX password: New password: Retype new password:` *`!--- Output is suppressed.`*
18. Configurar o IDSM-2 com o uso do comando setup.`sensor#`**`setup`** `--- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway 10.1.9.1 hostname sensor telnetOption disabled accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit Current time: Sat Sep 20 21:39:29 2003 Setup Configuration last modified: Sat Sep 20 21:36:30 2003 Continue with configuration dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]: 10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The following configuration was entered. networkParams ipAddress 10.66.79.210 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit [0] Go to the command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration and exit setup. Enter your selection[2]: Configuration Saved. sensor#`

Informações Relacionadas

- Cisco IDS Unix Director
- Módulo de serviços do sistema de detecção de intrusões do Catalyst 6500 Series (IDSM-1)
- Módulo de serviços do sistema de detecção de intrusões do Catalyst 6500 Series (IDSM-2)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems