Procédure de récupération de mot de passe pour les modules IDS Sensor et IDS Services (IDSM-1, IDSM-2)

Contenu

Introduction

Ce document fournit des procédures sur la façon de récupérer votre appliance de système de détection des intrusions sécurisé Cisco (IDS) (autrefois NetRanger) et les modules pour toutes les versions.

Conditions préalables

Conditions requises

Si un ftp server est nécessaire, il doit prendre en charge le mode passif. Des cd de reprise peuvent être obtenus utilisant l'outil de mise à jour d'un produit (clients enregistrés seulement).

Composants utilisés

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

- Versions 3 et 4 d'appareils d'ID
- Versions 5 et 6 d'appareils IPS
- Version 3 du module IDS (IDSM) et version 4 IDSM-2

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Version 3 d'appareils d'ID

Deux options sont disponibles pour l'appliance de version 3. Vous pouvez utiliser le processus de récupération de mot de passe ou vous pouvez faire une re-image qui utilise le CD de reprise de version 3. Notez que toutes les informations sont perdues sur une re-image. La procédure de récupération de mot de passe est essentiellement une reprise de mot de passe de Solaris. Utilisez seulement cette option si vous n'avez pas une station de Gestion (Cisco Secure Policy Manager (CSPM), la solution de Gestion VPN/Security (VMS), le directeur UNIX) dont vous pouvez copier la configuration.

Avec la version 3 et antérieures d'appareils d'ID, deux noms de l'utilisateur existent « netrangr » appelé et « racine ». Le mot de passe par défaut pour chacun des deux est « attaque ».

Reprise de mot de passe de l'appliance d'ID qui exécute la version 3

Ces fichiers sont nécessaires afin de récupérer votre mot de passe.

- Disque d'assistant de configuration de périphérique de Solaris (disquette de démarrage). Vous pouvez télécharger les fichiers du site Web de support de Sun .**Remarque:** Si ce lien ne fonctionne pas, essayer d'aller au niveau supérieur du site Web de support de Sun et rechercher des *téléchargements de gestionnaire de Solaris de disquette de démarrage d'assistant de configuration de périphérique* sous des gestionnaires. Cisco Systems, Inc. ne met pas à jour le site Web de support de Sun et n'a aucun contrôle d'où le contenu se trouve.
- Solaris pour la CD-ROM d'Intel (x86).
- Accès de console au poste de travail.

Terminez-vous ces étapes afin de récupérer le mot de passe.

1. Insérez la disquette de démarrage.

2. Insérez le CD dans le lecteur de CD-ROM.
3. Arrêtez le poste de travail, attendez dix secondes, et allumez-les.Les démarrages du système à partir de la disquette de démarrage. Après une certaine configuration, les affichages de l'écran d'assistant de configuration initiale.
4. **F-3 de** presse afin de faire un balayage partiel du système pour des périphériques de démarrage.Quand le balayage est de finition, une liste d'affichages de périphériques.
5. Assurez-vous que le périphérique de CD-ROM apparaît dans la liste de périphériques, et puis appuie sur le **F2** afin de continuer.Affichages de l'écran une liste de périphériques de démarrage.
6. Sélectionnez le **lecteur de CD-ROM**, et puis appuyez sur la barre d'espacement.Il y a un « X » à côté du périphérique de CD-ROM.
7. Presse **F2** afin de continuer.Le poste de travail démarre maintenant de la CD-ROM.
8. Sur l'écran utilisé pour sélectionner un type de installez, choisissez l'**Option 2, Jumpstart**.Le système continue à démarrer.
9. Àla demande pour sélectionner un langage, choisissez l'**option 0** pour l'anglais.
10. Àl'écran suivant pour des langages, choisissez l'**option 0** de nouveau pour l'ANSI anglais.Le système continue à démarrer et l'écran d'installation de Solaris apparaît.
11. Appuyez sur et tenez le **C de la touche Ctrl** et de type afin d'arrêter le script d'installation et te permettre l'accès à la demande.
12. **Support de** type **- Ufs /dev/dsk/c0t0d0s0 /mnt F.**« / » Partition est maintenant monté au point de montage « /mnt ». D'ici vous pouvez éditer le fichier « /etc/shadow » et retirer le mot de passe root.
13. **Cd /mnt/etc de** type.
14. Placez l'environnement de shell ainsi vous pouvez lire les données correctement.Type **TERM=ansi**.**TERME d'exportation de** type.
15. **Shadow du** type **vi**.Vous êtes maintenant dans le fichier de shadow et pouvez retirer le mot de passe. L'entrée doit être :
    `root:gNyqp8ohdfxPI:10598::::::` « : » est un séparateur de champ et le mot de passe chiffré est le deuxième champ.
16. Supprimez le deuxième champ. Exemple :`root:gNyqp8ohdfxPI:10598::::::`est changé à `root::10598::::::`. Ceci retire le mot de passe pour l'utilisateur de base.
17. Type **: wq !** afin d'écrire et quitter le fichier.
18. Retirez le disque et la CD-ROM des lecteurs.
19. **Init 6 de** type afin de redémarrer le système.
20. **Racine de** type à la procédure de connexion : la demande et appuient sur alors **entrent**.
21. La presse **entrent à l'**invite du mot de passe.Vous êtes maintenant ouvert une session au capteur de Cisco Secure IDS.

Re-image de l'appliance d'ID qui exécute la version 3

Terminez-vous la re-image de ces étapes l'appliance d'ID qui exécute la version 3.

Remarque: Assurez qu'une souris n'est pas connectée au capteur avant que vous poursuiviez.

1. Insérez le CD de reprise de version 3 dans l'appliance d'ID et redémarrez-le.
2. Suivez les demandes basées sur votre installation jusqu'à ce que la reprise soit réussie.
3. Procédure de connexion utilisant le nom d'utilisateur/mot de passe par défaut de la « racine/d'attaque ».

4. Exécutez le sysconfig-**capteur** afin de modifier l'appliance.

Version 4 d'appareils d'ID

Procédure de récupération si le nom d'utilisateur/mot de passe d'administrateur est connu

Si un mot de passe pour un compte administrateur est connu, ce compte utilisateur peut être utilisé afin de remettre à l'état initial d'autres mots de passe utilisateur.

Par exemple, deux noms d'utilisateur sont configurés sur l'appliance d'ID appelée « Cisco » et le « adminuser ». Le mot de passe pour les logins de « adminuser » d'utilisateur « Cisco » doit être remis à l'état initial, ainsi et remet à l'état initial le mot de passe.

```
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#
```

Procédure de récupération si le nom d'utilisateur/mot de passe de service est connu

Si un mot de passe pour le compte des services est connu, ce compte utilisateur peut être utilisé afin de remettre à l'état initial d'autres mots de passe utilisateur.

Par exemple, trois noms d'utilisateur sont configurés sur l'appliance d'ID nommée « Cisco », « adminuser », et « serviceuser ». Le mot de passe pour les logins de « serviceuser » d'utilisateur « Cisco » doit être remis à l'état initial, ainsi et remet à l'état initial le mot de passe.

```
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#
```

Remarque: Le mot de passe root est identique que le mot de passe du compte des services.

appliance d'ID de Re-image qui exécute la version 4

Terminez-vous la re-image de ces étapes l'appliance d'ID.

Remarque: Assurez qu'une souris n'est pas connectée au capteur avant que vous poursuiviez.

1. Insérez le CD de reprise de version 4 dans l'appliance d'ID et redémarrez-le.
2. Suivez les demandes basées sur votre installation jusqu'à ce que la reprise soit réussie.
3. Ouvrez une session utilisant le nom d'utilisateur/mot de passe par défaut qui est « Cisco/Cisco ».
4. Exécutez le **programme d'installation** afin de modifier l'appliance.

Version 5 et version 6 d'appareils IPS

La recharge, a arrêté, a remis à l'état initial, et récupère l'AIP SSM

Utilisez ces commandes de recharger, arrêté, remise, récupérez le mot de passe, et récupérez l'Advanced Inspection and Prevention Security Services Module (AIP SSM) directement de l'appliance de sécurité adaptable :

Remarque: Vous pouvez sélectionner les commandes de **hw-module du** mode d'exécution privilégié ou du mode de configuration globale. Vous pouvez sélectionner les commandes en mode conduit simple et choisir le mode transparent. Pour les périphériques de sécurité adaptatifs qui fonctionnent dans la multimode (conduite ou transparente) de multimode vous pouvez seulement exécuter le **hw-module** commande du contexte de système (pas des contextes d'administrateur ou d'utilisateur).

- **recharge de** *slot_number de* **module de hw-module** — Ce commandes reload le logiciel sur l'AIP SSM sans faire une réinitialisation du matériel. Il est efficace seulement quand l'AIP SSM est dans l'état haut.
- **arrêt de** *slot_number de* **module de hw-module** — Cette commande a arrêté le logiciel sur l'AIP SSM. Il est efficace seulement quand l'AIP SSM est dans l'état haut.
- *slot_number de* **module de hw-module remis à l'état initial** — Cette commande exécute une réinitialisation du matériel de l'AIP SSM. Il s'applique quand la carte est dans l'haut/bas/insensible/récupère des états.
- **mot de passe-remise de** *slot_number de* **module de hw-module** — Cette commande récupère un mot de passe sur un Content Security and Control Security Services Module de gamme de Cisco ASA 5500 (CSC-SSM) ou l'AIP SSM sans doit re-image le périphérique.**Remarque:** Cette commande commence le support à partir d'IPS 6.0 (version ASA 7.2) et est utilisée pour restaurer le mot de passe de compte de Cisco CLI sur **Cisco** par défaut.
- *le slot_number de* **module de hw-module récupèrent [démarrage | arrêt | configurez]** — la commande de **récupérer** présente un ensemble d'options interactives pour placer ou changer les paramètres de reprise. Vous pouvez changer le paramètre ou garder la configuration existante quand vous appuyez sur **entrez**.Pour la procédure que vous utilisez pour récupérer l'AIP SSM, voyez installer l'image de système d'AIP SSM.*le slot_number de* **module de hw-module récupèrent le démarrage** — Cette commande initie la reprise de l'AIP SSM. Il s'applique seulement quand l'AIP SSM est dans l'état haut.*le slot_number de* **module de hw-module récupèrent l'arrêt** — Cette commande arrête la reprise de l'AIP SSM. Il s'applique seulement quand l'AIP SSM est dans l'état de récupérer.**Remarque:** Si la reprise d'AIP SSM doit être arrêtée, vous devez émettre le **module 1 de hw-module récupérez la** commande d'**arrêt** dans 30 à 45 secondes après que vous commencez la reprise d'AIP SSM. Si vous attendez plus long, il peut mener aux conséquences inattendues. Par exemple, l'AIP SSM pourrait monter dans l'état insensible.**le module 1 de hw-module récupèrent configurent** — Utilisez cette commande de configurer des paramètres pour la reprise de module. Les paramètres essentiels sont l'emplacement URL d'adresse IP et d'image TFTP de reprise.Exemple :`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]:`

Réimagez l'image de système d'AIP SSM

Terminez-vous ces étapes afin d'installer l'image de système d'AIP SSM :

1. Procédure de connexion à l'ASA.

2. Écrivez le mode enable :`asa>enable`
3. Configurez les configurations de reprise pour l'AIP SSM :`asa#hw-module module 1 recover configure` **Remarque:** Si vous faites une erreur dans la configuration de reprise, utilisez le **module 1 de hw-module récupèrent la** commande d'**arrêt** de cesser le système réimager et alors vous pouvez corriger la configuration.
4. Spécifiez l'URL TFTP pour l'image de système :`Image URL [tftp://0.0.0.0/]:` Exemple :`Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img`
5. Spécifiez l'interface de commandement et de contrôle de l'AIP SSM :`Port IP Address [0.0.0.0]`:Exemple :`Port IP Address [0.0.0.0]: 10.89.149.231`
6. Laissez l'ID DE VLAN à 0. `VLAN ID [0]:`
7. Spécifiez la passerelle par défaut de l'AIP SSM :`Gateway IP Address [0.0.0.0]` :Exemple :`Gateway IP Address [0.0.0.0]:10.89.149.254`
8. Exécutez la reprise :`asa#hw-module module 1 recover boot`
9. Vérifiez périodiquement la reprise jusqu'à ce qu'elle soit complète :**Remarque:** L'état lit guest@localhost.localdomain # pendant la reprise et lit guest@localhost.localdomain # quand réimager est complet.`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#` **Remarque:** Afin de mettre au point toutes les erreurs qui pourraient se produire dans le processus de reprise, utilisez la commande de module-**démarrage de débogage** d'activer l'élimination des imperfections du système réimageant le processus.
10. La session à l'AIP SSM et initialisent l'AIP SSM avec la **commande setup**.

IDSM

Il y a aucune méthode que vous ne pouvez employer pour exécuter une reprise de mot de passe sur l'IDSM tandis que la configuration est retenue.

Remarque: Cette procédure exige l'utilisation de la partition de maintenance. Si le mot de passe de partition de maintenance a été changé et vous ne pouvez pas ouvrir une session, l'IDSM doit être remplacé. Dans ce cas, support technique de Cisco de contact pour l'assistance.

Re-image IDSM avec le commutateur qui exécute le code indigène IOS (IOS intégré)

Terminez-vous la re-image de ces étapes l'ISDM avec un commutateur qui exécute le code indigène IOS (IOS intégré).

1. Démarrez l'IDSM à la partition de maintenance utilisant le **module hdd:2 remis à l'état initial par** *X de* **hw-module de** commande du commutateur où *x* signifie le nombre d'emplacement.`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. Vérifiez que l'IDSM est livré en ligne utilisant le **show module** *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM a 2 situés au début qui indique que le logiciel de partition de maintenance fonctionne actuellement sur l'IDSM et que l'état est CORRECT.`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. Connectez à la partition de maintenance IDSM utilisant le **processeur 1. de la session slot** *X de* commande du commutateur.Utilisez le nom d'utilisateur/mot de passe des **ciscoids/attaque**.`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. Installez la re-image cachée d'image la partition d'application IDSM.Émettez le **système /cache /show d'id-installateur de** commande de diagnostics afin de vérifier que l'image cachée 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)#` Si aucune image cachée n'existe ou la version cachée n'est pas celle que vous voulez installer, passez à l'étape 5.La re-image l'ISDM utilisant l'image cachée, utilisent le **système /cache /install d'id-installateur de** commande de diagnostics.`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:\!` Une fois que la re-image s'est terminée, passez à l'étape 12.
5. Assurez-vous que l'IDSM a la connectivité IP. Émettez les *ip_address de* commande ping.`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. Si l'IDSM a la connectivité IP, passez à l'étape 11. Si vous n'avez pas la connectivité IP, procédez aux étapes 7 à 9.
7. Assurez-vous que l'interface de commandement et de contrôle est configurée correctement sur le commutateur. Émettez l'**interface Gigx/2 de passage d'exposition de** commande.`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. Assurez-vous que les paramètres de transmission sont configurés correctement sur la partition de maintenance IDSM. Émettez le **netconfig /view d'id-installateur de** commande de diagnostics.`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. Si aucun des paramètres n'est placé, ou si de eux le besoin d'être changé, utilisez les *paramètres de* **/configure de netconfig d'id-installateur de** commande de diagnostics.`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. Connectivité IP de contrôle de nouveau après que vous ayez remis à l'état initial l'IDSM pour les modifications pour prendre effet. Si la connectivité IP est toujours une question,

dépannez selon un problème de connectivité IP normal, alors procédez à l'étape 11.

11. Re-image la partition d'application IDSM. Téléchargez l'image utilisant le **=account /save de** */user de* **=ip_address de système /nw /install /server d'id-installateur de** commande de diagnostic **= =file_prefix {***oui/non***} de /prefix de =ftp_path de /dir** où :*les ip_address* est l'adresse IP du ftp server.*le compte* est l'utilisateur ou le nom du compte à utiliser en se connectant dans le ftp server.*sauvegardez* détermine si sauvegarder une copie de l'image téléchargée comme copie cachée. Si oui, n'importe quelle image cachée qui existe est remplacée. Si aucun, l'image téléchargée est installée sur la partition inactive mais une copie cachée n'est pas enregistré.*le ftp_path* spécifie le répertoire sur le ftp server où les fichiers d'image se trouvent.*le file_prefix* est le nom du fichier du fichier .dat dans l'image téléchargée. L'image téléchargée se compose d'un fichier avec l'extension .dat et de plusieurs fichiers avec l'extension .cab. La valeur de file_prefix doit être le nom du fichier DAT, jusqu'à la limite du suffixe .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. Démarrez l'IDSM à la partition d'application utilisant le **module hdd:1 remis à l'état initial par X de hw-module de** commande du commutateur.`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.` Assurez-vous également que le commutateur est configuré pour initialiser l'IDSM dans la partition d'application. Afin de vérifier ceci, utilisez le **module** *X. de* **périphérique de show bootvar de** commande.`SV9-1#show bootvar device module 6 [mod:6 ]: SV9-1#` Afin de configurer la variable de périphérique de démarrage pour l'IDSM, utilisez le **module X hdd:1 de périphérique de démarrage de** commande de configuration de commutateur.`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. Vérifiez que l'IDSM est livré en ligne utilisant le **show module** *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM est une version de partition d'application, par exemple *3.0(1)S4*, et que l'état est CORRECT.`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. Connectez à l'IDSM maintenant qu'il a initialisé dans la partition d'application et configurez-la ainsi elle peut communiquer au directeur. Utilisez l'**installation de** commande.Une fois la transmission avec le directeur a été établie, configuration peut être téléchargée à l'IDSM.Employez le nom d'utilisateur/mot de passe des **ciscoids/attaque** afin d'ouvrir une session.`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.
```

Re-image IDSM avec le commutateur qui exécute le code hybride (de CatOS)

Terminez-vous la re-image ISDM de ces étapes avec un commutateur qui exécute le code hybride (de CatOS).

Remarque: Toutes les informations sont perdues sur la partition d'application. Il y a aucune méthode que vous ne pouvez employer pour exécuter une reprise de mot de passe sur l'IDSM tandis que vous retenez la configuration.

Remarque: Cette procédure exige l'utilisation de la partition de maintenance. Si le mot de passe de partition de maintenance a été changé et vous ne pouvez pas ouvrir une session, l'IDSM doit être remplacé. Dans ce cas, support technique de Cisco de contact pour l'assistance.

1. Démarrez l'IDSM à la partition de maintenance avec la **remise** *X* **hdd:2 de** commande du commutateur.
```
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. Vérifiez que l'IDSM est livré en ligne avec le **show module** *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM a 2 situés au début qui indique que le logiciel de partition de maintenance fonctionne actuellement sur l'IDSM et que l'état est CORRECT.
```
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. Connectez à l'IDSM maintenant qu'il a initialisé dans la partition de maintenance avec la **session** *X. de* commande du commutateur.Utilisez le nom d'utilisateur/mot de passe des **ciscoids/attaque**.
```
ltd9-9> (enable)session 4 Trying IDS-4... Connected to IDS-4. Escape
character is '^]'. login: ciscoids Password: maintenance#
```
4. Installez la re-image cachée d'image la partition d'application IDSM.Vérifiez que l'image cachée existe avec l'utilisation du **système /cache /show d'id-installateur de** commande de

diagnostics.`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)#` Si aucune image cachée n'existe, ou la version cachée n'est pas celle que vous voulez installer, passez à l'étape 5.La re-image l'ISDM qui utilise l'image cachée, utilisent le **système /cache /install d'id-installateur de** commande de diagnostics.`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:\!` Une fois le réimager s'est terminé, passe à l'étape 12.

5. Assurez-vous que l'IDSM a la connectivité IP avec l'utilisation des *ip_address de* commande ping.`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. Si l'IDSM a la connectivité IP, passez à l'étape 11. Si vous n'avez pas la connectivité IP, procédez aux étapes 7 à 9.
7. Assurez-vous que l'interface de commandement et de contrôle est configurée correctement sur le commutateur avec l'utilisation du **show port status** *x/2 de* commande.`ltd9-9> (enable)show port status 4/2 Port Name Status Vlan Duplex Speed Type ----- ---------- ---- ---------- ---------- ------ ----- ------------ 4/2 connected 1 full 1000 Intrusion De`
8. Assurez-vous que les paramètres de transmission sont configurés correctement sur la partition de maintenance IDSM avec l'utilisation le du **netconfig /view d'id-installateur de** commande de diagnostics.`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. Si aucun des paramètres n'est placé, ou si de eux le besoin d'être changé, utilisez les *paramètres de* **/configure de netconfig d'id-installateur de** commande de diagnostics.`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. Connectivité IP de contrôle de nouveau après que vous ayez remis à l'état initial l'IDSM pour les modifications pour prendre effet.Si la connectivité IP est toujours une question, dépannez selon un problème de connectivité IP normal, alors procédez à l'étape 11.
11. Re-image la partition d'application IDSM. Téléchargez l'image avec l'utilisation du **=account /save de /user de =ip_address de système /nw /install /server d'id-installateur de** commande de diagnostic **= =file_prefix {***oui/non***} de /prefix de =ftp_path de /dir** où :*les ip_address* est l'adresse IP du ftp server.*le compte* est l'utilisateur ou le nom du compte à utiliser en se connectant dans le ftp server.*sauvegardez* détermine si sauvegarder une copie de l'image téléchargée comme copie cachée. Si oui, n'importe quelle image cachée existante est remplacée. Si aucun, l'image téléchargée est installée sur la partition inactive mais une copie cachée n'est pas enregistré.*le ftp_path* spécifie le répertoire sur le ftp server où les fichiers d'image se trouvent.*le file_prefix* est le nom du fichier du fichier .dat dans l'image téléchargée. L'image téléchargée se compose d'un fichier avec l'extension .dat et de plusieurs fichiers avec l'extension .cab. La valeur de file_prefix devrait être le nom du fichier DAT, jusqu'à la limite du suffixe .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. Démarrez l'IDSM à la partition d'application avec l'utilisation de la **remise** *X* **hdd:1 de** commande du commutateur.`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.` Assurez-vous également que le commutateur est configuré afin d'initialiser l'IDSM dans la partition d'application. IUse le **périphérique** *X de* **show boot de** commande afin de vérifier ceci.`ltd9-9> (enable)`**`show boot device 4`** `Device BOOT variable =` Afin de configurer la variable de périphérique de démarrage pour l'IDSM, utilisez le **périphérique de démarrage réglé hdd:1** *X. de* commande de configuration de commutateur.`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. Vérifiez que l'IDSM est livré en ligne avec l'utilisation du **show module** *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM est une version de partition d'application, par exemple, *3.0(1)S4*, et que l'état est CORRECT.`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. Connectez à l'IDSM maintenant qu'il a initialisé dans la partition d'application et configurez-la ainsi elle peut communiquer au directeur. Utilisez l'**installation de** commande.Ouvrez une session avec le nom d'utilisateur/mot de passe des **ciscoids/attaque**.

```
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

Procédure de récupération si le nom d'utilisateur/mot de passe d'administrateur est connu

Si un mot de passe pour un compte administrateur est connu, ce compte utilisateur peut être utilisé afin de remettre à l'état initial d'autres mots de passe utilisateur.

Par exemple, deux noms d'utilisateur sont configurés sur « Cisco » nommé par IDSM-2 et le « adminuser ». Le mot de passe pour les logins de « adminuser » d'utilisateur « Cisco » doit être remis à l'état initial, ainsi et remet à l'état initial le mot de passe.

```
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#
```

Procédure de récupération si le nom d'utilisateur/mot de passe de service est connu

Si un mot de passe pour le compte des services est connu, ce compte utilisateur peut être utilisé afin de remettre à l'état initial d'autres mots de passe utilisateur.

Par exemple, trois noms d'utilisateur sont configurés sur « Cisco » nommé par IDSM-2, le « adminuser », et le « serviceuser ». Le mot de passe pour les logins de « serviceuser » d'utilisateur « Cisco » doit être remis à l'état initial, ainsi et remet à l'état initial le mot de passe.

```
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#
```

Remarque: Le mot de passe root est identique que le mot de passe du compte des services.

Re-image IDSM-2 avec le commutateur qui exécute le code indigène IOS (IOS intégré)

Terminez-vous la re-image ISDM-2 de ces étapes avec un commutateur qui exécute le code indigène IOS (IOS intégré).

Remarque: Toutes les informations sont perdues sur la partition d'application. Il y a aucune méthode que vous ne pouvez employer afin d'exécuter une reprise de mot de passe sur l'IDSM-2 tandis que la configuration est retenue.

1. Démarrez l'IDSM-2 à la partition de maintenance avec l'utilisation du **module cf:1 remis à l'état initial par** *X de* **hw-module de** commande du commutateur où *x* signifie le nombre d'emplacement et le Cf signifie les « compacts flashs.**Remarque:** Si un problème est produit utilisant cf:1, essayez d'utiliser hdd:2 comme alternative.
```
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. Vérifiez que l'IDSM-2 est livré en ligne avec l'utilisation du **show module** *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM-2 a « m » situé à l'extrémité et que l'état est CORRECT.`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. Connectez à l'IDSM-2 maintenant qu'il a initialisé dans la partition de maintenance. Utilisez le *xprocessor* **1. de session slot de** commande du commutateur.Utilisez le nom d'utilisateur/mot de passe de l'**invité/du 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. Assurez-vous que l'IDSM-2 a la connectivité IP. Utilisez les *ip_address de* commande ping.`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. Si l'IDSM-2 a la connectivité IP, passez à l'étape 14.
6. Assurez-vous que l'interface de commandement et de contrôle est configurée correctement sur le commutateur. Utilisez le **passage d'exposition de** commande **| détection d'intrusion inc**.`SV9-1#show run | inc intrusion-detection intrusion-detection module 6 management-port access-vlan 210`
7. Assurez-vous que les paramètres de transmission sont configurés correctement sur la partition de la maintenance IDSM-2. Utilisez le **show ip de** commande.`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. Si aucun des paramètres n'est placé, ou si de eux le besoin d'être changé, clair ils tous. Utilisez l'**IP d'espace libre de** commande.`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. Configurez l'adresse IP et les informations de masque sur la partition de la maintenance IDSM-2. Utilisez le *netmask d'ip_address d*'**IP address de** commande.`guest@localhost.localdomain#ip address 10.66.79.210 255.255.255.224`
10. Configurez la passerelle par défaut sur la partition de la maintenance IDSM-2. Utilisez la passerelle-*adresse de* **passerelle d'IP de** commande.`guest@localhost.localdomain#ip gateway 10.66.79.193`
11. Configurez l'adresse Internet sur la partition de la maintenance IDSM-2. Utilisez l'*adresse Internet d*'**hôte d'IP de** commande.Bien que ce ne soit pas nécessaire, il aide à identifier le périphérique puisque ceci place également la demande.`guest@localhost.localdomain#ip host idsm2-sv-rack guest@idsm2-sv-rack.localdomain#`

12. Vous pourriez probablement devoir configurer votre adresse d'émission explicitement. Utilisez l'émission-*adresse d'*émission d'IP de commande.La valeur par défaut suffit habituellement.`guest@idsm2-sv-rack.localdomain#`**`ip broadcast 10.66.79.223`**
13. Vérifiez la connectivité IP de nouveau. Si la connectivité IP est toujours une question, dépannez selon un problème de connectivité IP normal et procédez à l'étape 14.
14. Re-image la partition de l'application IDSM-2. Utilisez le FTP-*URL de* mise à jour de commande --installez.`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. Démarrez l'IDSM-2 à la partition d'application. Utilisez le module hdd:1 remis à l'état initial par *X de* hw-module de commande du commutateur.`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.` Alternativement, vous pouvez utiliser la commande de remise sur l'IDSM-2 tant que la variable de périphérique de démarrage est placée correctement.Afin de vérifier la configuration variable de périphérique de démarrage pour l'IDSM-2, utilisez le module *X. de* périphérique de show bootvar de commande du commutateur.`SV9-1#`**`show bootvar device module 6`** `[mod:6 ]: SV9-1#` Afin de configurer la variable de périphérique de démarrage pour l'IDSM-2, utilisez le module *X* hdd:1 de périphérique de démarrage de commande de configuration de commutateur.`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` Afin de remettre à l'état initial l'IDSM-2 par l'intermédiaire de la partition CLI de maintenance, utilisez la remise de commande.`guest@idsm2-sv-rack.localdomain#`**`reset`** *`!--- Output is suppressed.`*
16. Vérifiez que l'IDSM-2 est livré en ligne. Utilisez le show module *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM-2 est une version de partition d'application, par exemple *4.1(1)S47* et que l'état est CORRECT.`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. Connectez à l'IDSM-2 maintenant qu'il a initialisé dans la partition d'application. Utilisez le processeur 1. de la session slot *X de* commande du commutateur.Utilisez le nom d'utilisateur/mot de passe de Cisco/de 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. Configurez l'IDSM-2. Utilisez l'installation de commande.`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#
```

Re-image pour IDSM-2 avec le commutateur qui exécute le code hybride (de CatOS)

Terminez-vous la re-image de ces étapes l'ISDM-2 avec un commutateur qui exécute le code hybride (de CatOS).

1. Démarrez l'IDSM-2 dans la partition de maintenance. Utilisez la **remise** *X* **hdd:2 de** commande du commutateur.**Remarque:** Si un problème est produit utilisant hdd:2, essayez d'utiliser cf:1 comme alternative.
```
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. Vérifiez que l'IDSM-2 est livré en ligne. Utilisez le **show module** *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM-2 a « m » situé à l'extrémité qui indique que les passages de logiciel de partition de maintenance actuellement et que l'état est CORRECT.
```
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. Connectez à l'IDSM-2 maintenant qu'il a initialisé dans la partition de maintenance. Utilisez la **session** *X. de* commande du commutateur.Utilisez le nom d'utilisateur/mot de passe de l'**invité/du 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. Assurez-vous que l'IDSM-2 a la connectivité IP. Utilisez les *ip_address de* commande ping.
```
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. Si l'IDSM-2 a la connectivité IP, passez à l'étape 14.
6. Assurez-vous que l'interface de commandement et de contrôle est configurée correctement sur le commutateur. Utilisez le **show port status** *x/2 de* commande.`SV9-1> (enable)`**`show port status 6/2`** `Port Name Status Vlan Duplex Speed Type ----- ------------------ ---------- ---------- ------ ----- ------------ 6/2 connected 210 full 1000 Intrusion De`
7. Assurez-vous que les paramètres de transmission sont configurés correctement sur la partition de la maintenance IDSM-2. Utilisez le **show ip de** commande.`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. Si aucun des paramètres n'est placé ou si de eux le besoin d'être changé, clair ils tous avec l'utilisation de l'**IP d'espace libre de** commande.`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. Configurez l'adresse IP et les informations de masque sur la partition de la maintenance IDSM-2. Utilisez le *netmask d'ip_address d'***IP address de** commande.`guest@localhost.localdomain#`**`ip address 10.66.79.210 255.255.255.224`** `guest@localhost.localdomain#`
10. Configurez la passerelle par défaut sur la partition de la maintenance IDSM-2. Utilisez la passerelle-*adresse de* **passerelle d'IP de** commande.`guest@localhost.localdomain#`**`ip gateway 10.66.79.193`** `guest@localhost.localdomain#`
11. Configurez l'adresse Internet sur la partition de la maintenance IDSM-2. Utilisez l'*adresse Internet d'***hôte d'IP de** commande.Bien que ce ne soit pas nécessaire, il aide à identifier le périphérique puisque ceci place également la demande.`guest@localhost.localdomain#`**`ip host idsm2-sv-rack`** `guest@idsm2-sv-rack.localdomain#`
12. Vous pourriez probablement devoir configurer votre adresse d'émission explicitement. Utilisez l'émission-*adresse d'***émission d'IP de** commande.La valeur par défaut suffit habituellement.`guest@idsm2-sv-rack.localdomain#`**`ip broadcast 10.66.79.223`**
13. Connectivité IP de contrôle de nouveau. Si la connectivité IP est toujours une question, dépannez selon un problème de connectivité IP normal alors procédez à l'étape 14.
14. Re-image la partition de l'application IDSM-2. Utilisez le FTP-*URL de* **mise à jour de** commande **--installez**.`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. Démarrez l'IDSM-2 à la partition d'application. Utilisez la **remise** *X* **hdd:1 de** commande du commutateur.`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.`* Alternativement, vous pouvez utiliser la commande de **remise** sur l'IDSM-2 tant que la la variable de périphérique de démarrage est placée correctement.Afin de vérifier la configuration variable de périphérique de démarrage pour l'IDSM-2, utilisez le **périphérique** *X. de* **show boot de** commande du commutateur.`SV9-1> (enable)`**`show boot device 6`** `Device BOOT variable = (null) (Default boot partition is hdd:1) Memory-test set to PARTIAL` Afin de configurer la variable de périphérique de démarrage pour l'IDSM-2, utilisez le

périphérique de démarrage réglé hdd:1 *X. de* commande de configuration de commutateur.
```
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
```
Afin de remettre à l'état initial l'IDSM-2 par l'intermédiaire de la partition CLI de maintenance, utilisez la **remise de** commande.
```
guest@idsm2-sv-rack.localdomain#reset !--- Output is suppressed.
```

16. Vérifiez que l'IDSM-2 est livré en ligne. Utilisez le **show module** *X. de* commande du commutateur.Assurez-vous que la version de logiciel IDSM-2 est une version de partition d'application, par exemple *4.1(1)S47,* et que l'état est CORRECT.
```
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. Connectez à l'IDSM-2 maintenant qu'il a initialisé dans la partition d'application. Utilisez la **session** *X. de* commande du commutateur.Utilisez le nom d'utilisateur/mot de passe de **Cisco/de 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. Configurez l'IDSM-2 avec l'utilisation de l'**installation de** commande.
```
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#
```

Informations connexes

- Directeur Cisco IDS Unix
- Module de services de Detection System d'intrusion de gamme Catalyst 6500 (IDSM-1)
- Module de services de Detection System d'intrusion de gamme Catalyst 6500 (IDSM-2)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems