Exemple de configuration de mise à niveau de l'image et de la signature d'IDS 4.1 vers IPS 5.0 et versions ultérieures (AIP-SSM, NM-IDS, IDSM-2)

Table des matières

Introduction

Ce document décrit comment mettre à niveau l'image et la signature du logiciel Cisco Intrusion Detection Sensor (IDS) de la version 4.1 vers Cisco Intrusion Prevention System (IPS) 5.0 et versions ultérieures.

Remarque : à partir de la version 5.x du logiciel et des versions ultérieures, Cisco IPS remplace Cisco IDS, qui est applicable jusqu'à la version 4.1.

Remarque : le capteur ne peut pas télécharger les mises à jour logicielles à partir de Cisco.com. Vous devez télécharger les mises à jour logicielles depuis Cisco.com sur votre serveur FTP, puis configurer le capteur afin de les télécharger depuis votre serveur FTP.

Référez-vous à la section Installation de l'image système AIP-SSM de Mise à niveau, Mise à niveau vers une version antérieure et Installation des images système pour la procédure.

Référez-vous à Procédure de récupération de mot de passe pour les modules Cisco IDS Sensor et IDS Services (IDSM-1, IDSM-2) afin d'en savoir plus sur la façon de récupérer l'appareil Cisco

Secure IDS (anciennement NetRanger) et les modules pour les versions 3.x et 4.x.

Remarque : le trafic utilisateur n'est pas affecté lors de la mise à niveau dans le paramètre en ligne et d'ouverture en panne sur ASA - AIP-SSM.

Remarque : reportez-vous à la section Mise à niveau du logiciel Cisco IPS de 5.1 à 6.x de la section Configuration du capteur du système de prévention des intrusions Cisco à l'aide de l'interface de ligne de commande 6.0 pour plus d'informations sur la procédure de mise à niveau de IPS 5.1 vers la version 6.x.

Remarque : le capteur ne prend pas en charge les serveurs proxy pour les mises à jour automatiques. Les paramètres de proxy sont uniquement destinés à la fonction de corrélation globale.

Conditions préalables

Exigences

La version logicielle minimale requise pour effectuer la mise à niveau vers la version 5.0 est la version 4.1(1).

Composants utilisés

Les informations contenues dans ce document sont basées sur le matériel IDS de la gamme Cisco 4200 qui exécute la version logicielle 4.1 (à mettre à niveau vers la version 5.0).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

La mise à niveau de Cisco 4.1 vers la version 5.0 est disponible en téléchargement sur le site Cisco.com. Référez-vous à Obtention du logiciel IPS Cisco pour la procédure que vous utilisez pour accéder aux téléchargements du logiciel IPS sur Cisco.com.

Vous pouvez utiliser l'une des méthodes répertoriées ici afin d'effectuer la mise à niveau :

- Après avoir téléchargé le fichier de mise à niveau 5.0, reportez-vous au fichier Readme pour

la procédure d'installation du fichier de mise à niveau 5.0 avec la commande upgrade. Consultez la section Utiliser la commande de mise à niveau de ce document pour plus d'informations.

- Si vous avez configuré la mise à jour automatique pour votre capteur, copiez le fichier de mise à niveau 5.0 dans le répertoire du serveur que votre capteur interroge pour les mises à jour. Consultez la section Utiliser la commande auto-upgrade de ce document pour plus d'informations.
- Si vous installez une mise à niveau sur votre capteur et que celui-ci est inutilisable après son redémarrage, vous devez réinstaller votre capteur. La mise à niveau d'un capteur à partir d'une version de Cisco IDS antérieure à la version 4.1 nécessite également l'utilisation de la commande recover ou du CD de récupération/mise à niveau. Pour plus d'informations, reportez-vous à la section Réimage du capteur de ce document.

Mise à niveau du capteur

Les sections suivantes expliquent comment utiliser la commande upgrade pour mettre à niveau le logiciel sur le capteur :

- Aperçu
- Commande et options de mise à niveau
- Utiliser la commande Upgrade

Aperçu

Vous pouvez mettre à niveau le capteur avec ces fichiers, qui ont tous l'extension .pkg :

- Mises à jour des signatures, par exemple, IPS-sig-S150-minreq-5.0-1.pkg
- Mises à jour du moteur de signature, par exemple, IPS-engine-E2-req-6.0-1.pkg
- Mises à jour majeures, par exemple, IPS-K9-maj-6.0-1-pkg
- Mises à jour mineures, par exemple, IPS-K9-min-5.1-1.pkg
- Mises à jour du Service Pack, par exemple, IPS-K9-sp-5.0-2.pkg
- Mises à jour des partitions de récupération, par exemple, IPS-K9-r-1.1-a-5.0-1.pkg
- Versions des correctifs, par exemple, IPS-K9-patch-6.0-1p1-E1.pkg
- Mises à jour des partitions de récupération, par exemple, IPS-K9-r-1.1-a-6.0-1.pkg

Une mise à niveau du capteur modifie la version logicielle du capteur.

Commande et options de mise à niveau

Utilisez la commande auto-upgrade-option enabled dans le sous-mode service host afin de configurer les mises à niveau automatiques.

Ces options s'appliquent :

- default : rétablit la valeur par défaut du système.
- directory : répertoire dans lequel les fichiers de mise à niveau se trouvent sur le serveur de fichiers.
- file-copy-protocol : protocole de copie de fichier utilisé pour télécharger des fichiers à partir du serveur de fichiers. Les valeurs valides sont ftp ou scp.

  Remarque : si vous utilisez SCP, vous devez utiliser la commande ssh host-key pour ajouter le serveur à la liste des hôtes connus SSH afin que le capteur puisse communiquer avec lui via SSH. Reportez-vous à Ajout d'hôtes à la liste des hôtes connus pour la procédure.
- ip-address : adresse IP du serveur de fichiers.
- password : mot de passe utilisateur pour l'authentification sur le serveur de fichiers.
- schedule-option : planifie les mises à niveau automatiques. La planification du calendrier démarre les mises à niveau à des heures spécifiques des jours spécifiques. La planification périodique démarre les mises à niveau à des intervalles périodiques spécifiques.
    - calendar-schedule : configure les jours de la semaine et les heures de la journée pendant lesquels les mises à niveau automatiques sont effectuées.
        - days-of-week : jours de la semaine pendant lesquels les mises à niveau automatiques sont effectuées. Vous pouvez sélectionner plusieurs jours. Les valeurs valides sont comprises entre dimanche et samedi.
        - no : supprime une entrée ou un paramètre de sélection.
        - times-of-day : heure de début des mises à niveau automatiques. Vous pouvez sélectionner plusieurs fois. La valeur valide est hh:mm[:ss].
    - périodique-schedule : configure l'heure à laquelle la première mise à niveau automatique doit avoir lieu et le délai d'attente entre les mises à niveau automatiques.
        - interval : nombre d'heures à attendre entre les mises à niveau automatiques. Les valeurs valides sont comprises entre 0 et 8 760.
        - start-time : heure de début de la première mise à niveau automatique. La valeur valide est hh:mm[:ss].
- user-name : nom d'utilisateur pour l'authentification sur le serveur de fichiers.

Pour la procédure IDM de mise à niveau du capteur, référez-vous à Mise à jour du capteur.

Utiliser la commande Upgrade

Vous recevez des erreurs SNMP si vous n'avez pas les paramètres read-only-community et read-write-community configurés avant la mise à niveau vers IPS 6.0. Si vous utilisez les fonctionnalités set et/ou get de SNMP, vous devez configurer les paramètres de la communauté en lecture seule et de la communauté en lecture-écriture avant de procéder à la mise à niveau vers IPS 6.0. Dans IPS 5.x, la communauté en lecture seule a été définie sur public par défaut et la communauté en lecture-écriture a été définie sur private par défaut. Dans IPS 6.0, ces deux options n'ont pas de valeurs par défaut. Si vous n'avez pas utilisé SNMP gets et sets avec IPS 5.x, par exemple, enable-set-get a été défini sur false, alors il n'y a aucun problème pour mettre à niveau vers IPS 6.0. Si vous avez utilisé SNMP gets et sets avec IPS 5.x, par exemple, enable-set-get a été défini sur true, vous devez configurer les paramètres de la communauté en lecture seule et de la communauté en lecture-écriture sur des valeurs spécifiques ou la mise à niveau d'IPS 6.0 échoue.

Vous recevez le message d'erreur suivant :

```
Error: execUpgradeSoftware : Notification Application "enable-set-get" value set to true,
but "read-only-community" and/or "read-write-community" are set to null. Upgrade may not
continue with null values in these fields.
```

Remarque : IPS 6.0 refuse par défaut les événements à haut risque. Il s'agit d'un changement par rapport à IPS 5.x. Afin de modifier la valeur par défaut, créez un remplacement d'action d'événement pour l'action en ligne deny packet et configurez-la pour être désactivée. Si l'administrateur ne connaît pas la communauté read write, il doit essayer de désactiver complètement SNMP avant de tenter une mise à niveau afin de supprimer ce message d'erreur.

Complétez ces étapes afin de mettre à niveau le capteur :

1. Téléchargez le fichier de mise à jour principal (IPS-K9-maj-5.0-1-S149.rpm.pkg) sur un serveur FTP, SCP, HTTP ou HTTPS accessible depuis votre capteur.

   Référez-vous à Obtention du logiciel Cisco IPS pour la procédure sur la façon de localiser le logiciel sur Cisco.com.

   Remarque : vous devez vous connecter à Cisco.com à l'aide d'un compte disposant de privilèges cryptographiques pour télécharger le fichier. Ne modifiez pas le nom du fichier. Vous devez conserver le nom de fichier d'origine pour que le capteur accepte la mise à jour.

   Remarque : ne modifiez pas le nom du fichier. Vous devez conserver le nom de fichier d'origine pour que le capteur accepte la mise à jour.

2. Connectez-vous à la CLI à l'aide d'un compte disposant de privilèges administrateur.

3. Passez en mode de configuration :

<#root>

sensor#

configure terminal

4. Mettre à niveau le capteur :

<#root>

sensor(config)#

upgrade scp://

@

//upgrade/

Exemple :

Remarque : cette commande est sur deux lignes pour des raisons spatiales.

<#root>

sensor(config)#

**upgrade scp://tester@10.1.1.1//upgrade/
IPS-K9-maj-5.0-1-S149.rpm.pkg**

Remarque : reportez-vous à Serveurs FTP et HTTP/HTTPS pris en charge pour obtenir la liste des serveurs FTP et HTTP/HTTPS pris en charge. Référez-vous à Ajout d'hôtes à la liste d'hôtes connus SSH pour plus d'informations sur la façon d'ajouter le serveur SCP à la liste d'hôtes connus SSH.

5. Entrez le mot de passe lorsque vous y êtes invité :

```
Enter password: ********
Re-enter password: ********
```

6. Tapez yes pour terminer la mise à niveau.

   Remarque : les mises à jour majeures, les mises à jour mineures et les Service Packs peuvent forcer le redémarrage des processus IPS ou même forcer le redémarrage du capteur pour terminer l'installation. Il y a donc une interruption de service d'au moins deux minutes. Toutefois, les mises à jour de signatures ne nécessitent pas de redémarrage une fois la mise à jour terminée. Référez-vous à Télécharger les mises à jour des signatures (clients enregistrés uniquement) pour les dernières mises à jour.

7. Vérifiez la nouvelle version de votre capteur :

<#root>

sensor#

show version

Application Partition:

Cisco Intrusion Prevention System,

Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys

Platform: ASA-SSM-20

Serial Number: 021

No license present

Sensor up-time is 5 days.

Using 490110976 out of 1984704512 bytes of available memory (24% usage)

system is using 17.3M out of 29.0M bytes of available disk space (59% usage)

```
application-data is using 37.7M out of 166.6M bytes of
available disk space (24 usage)

boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

AnalysisEngine   2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

CLI              2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600


Upgrade History:


  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004


Recovery Partition Version 1.1 - 5.0(1)S149


sensor#
```

Remarque : pour IPS 5.x, vous recevez un message indiquant que la mise à niveau est de type inconnu. Vous pouvez ignorer ce message.

Remarque : le système d'exploitation est réimagé et tous les fichiers placés sur le capteur via le compte de service sont supprimés.

Référez-vous à Mise à jour du capteur pour plus d'informations sur la procédure IDM pour la mise à niveau du capteur.

Configuration des mises à niveau automatiques

Mises à niveau automatiques

Vous pouvez configurer le capteur pour qu'il recherche automatiquement les nouveaux fichiers de mise à niveau dans votre répertoire de mise à niveau. Par exemple, plusieurs capteurs peuvent pointer vers le même répertoire de serveur FTP distant avec des calendriers de mise à jour différents, par exemple toutes les 24 heures, ou lundi, mercredi et vendredi à 23 heures.

Vous spécifiez ces informations afin de programmer des mises à niveau automatiques :

- Adresse IP du serveur
- Chemin du répertoire sur le serveur de fichiers où le capteur recherche les fichiers de mise à niveau
- Protocole de copie de fichier (SCP ou FTP)

- Nom d'utilisateur et mot de passe
- Calendrier de mise à niveau

Vous devez télécharger la mise à niveau logicielle à partir du site Cisco.com et la copier dans le répertoire de mise à niveau avant que le capteur puisse interroger les mises à niveau automatiques.

Remarque : si vous utilisez la mise à niveau automatique avec AIM-IPS et d'autres appliances ou modules IPS, veillez à placer le fichier de mise à niveau 6.0(1), IPS-K9-6.0-1-E1.pkg, et le fichier de mise à niveau AIM-IPS, IPS-AIM-K9-6.0-4-E1.pkg, sur le serveur de mise à jour automatique afin qu'AIM-IPS puisse détecter correctement quel fichier doit être téléchargé et installé automatiquement. Si vous placez uniquement le fichier de mise à niveau 6.0(1), IPS-K9-6.0-1-E1.pkg, sur le serveur de mise à jour automatique, AIM-IPS télécharge et tente de l'installer, ce qui est le fichier incorrect pour AIM-IPS.

Référez-vous à Mise à jour automatique du capteur pour plus d'informations sur la procédure IDM pour la mise à niveau automatique du capteur.

Utiliser la commande auto-upgrade

Consultez la section Commandes et options de mise à niveau de ce document pour les commandes auto-update.

Complétez ces étapes afin de planifier des mises à niveau automatiques :

1. Connectez-vous à l'interface de ligne de commande avec un compte disposant de privilèges d'administrateur.
2. Configurez le capteur afin de rechercher automatiquement de nouvelles mises à niveau dans votre répertoire de mise à niveau.

```
<#root>

sensor#

configure terminal

sensor(config)#

service host

sensor(config-hos)#

auto-upgrade-option enabled
```

3. Spécifiez la planification :
    - Pour la planification du calendrier, qui démarre les mises à niveau à des heures spécifiques des jours spécifiques :

```
<#root>
sensor(config-hos-ena)#
schedule-option calendar-schedule
sensor(config-hos-ena-cal#
days-of-week sunday
sensor(config-hos-ena-cal#
times-of-day 12:00:00
```

- Pour la planification périodique, qui démarre les mises à niveau à des intervalles périodiques spécifiques :

```
<#root>
sensor(config-hos-ena)#
schedule-option periodic-schedule
sensor(config-hos-ena-per)#
interval 24
sensor(config-hos-ena-per)#
start-time 13:00:00
```

4. Spécifiez l'adresse IP du serveur de fichiers :

```
<#root>
sensor(config-hos-ena-per)#
exit
sensor(config-hos-ena)#
ip-address 10.1.1.1
```

5. Spécifiez le répertoire dans lequel les fichiers de mise à niveau se trouvent sur le serveur de fichiers :

```
<#root>
sensor(config-hos-ena)#
directory /tftpboot/update/5.0_dummy_updates
```

6. Spécifiez le nom d'utilisateur pour l'authentification sur le serveur de fichiers :

```
<#root>
sensor(config-hos-ena)#
user-name tester
```

7. Spécifiez le mot de passe de l'utilisateur :

```
<#root>
sensor(config-hos-ena)#
password

Enter password[]:
******
Re-enter password:
 ******
```

8. Spécifiez le protocole du serveur de fichiers :

```
<#root>
sensor(config-hos-ena)#
file-copy-protocol ftp
```

Remarque : si vous utilisez SCP, vous devez utiliser la commande ssh host-key afin d'ajouter le serveur à la liste des hôtes connus SSH afin que le capteur puisse communiquer avec lui via SSH. Reportez-vous à Ajout d'hôtes à la liste des hôtes connus pour la procédure.

9. Vérifiez les paramètres :

```
<#root>
sensor(config-hos-ena)#
show settings
```

```
    enabled
    ------------------------------------------
       schedule-option
       ------------------------------------------
          periodic-schedule
          ------------------------------------------
             start-time: 13:00:00
             interval: 24 hours
          ------------------------------------------
       ------------------------------------------
       ip-address: 10.1.1.1
       directory: /tftpboot/update/5.0_dummy_updates
       user-name: tester
       password: <hidden>
       file-copy-protocol: ftp default: scp
    ------------------------------------------
sensor(config-hos-ena)#
```

10. Quittez le sous-mode de mise à niveau automatique :

```
<#root>
sensor(config-hos-ena)#
exit
sensor(config-hos)#
exit

Apply Changes:?
[yes]:
```

11. Appuyez sur Entrée afin d'appliquer les modifications ou tapez no afin de les ignorer.

Réimage du capteur

Vous pouvez redéfinir l'image de votre capteur de différentes manières :

- Pour les appareils IDS équipés d'un lecteur de CD-ROM, utilisez le CD de récupération/mise à niveau.

  Reportez-vous à la section Utilisation du CD de récupération/mise à niveau de Mise à niveau, Mise à niveau et Installation des images système pour la procédure.

- Pour tous les capteurs, utilisez la commande recover.

  Référez-vous à la section Récupération de la partition d'application de Mise à niveau, Mise à niveau et Installation des images système pour la procédure.

- Pour les systèmes IDS-4215, IPS-4240 et IPS-4255, utilisez ROMMON pour restaurer l'image système.

  Référez-vous aux sections Installation de l'image système IDS-4215 et Installation de l'image système IPS-4240 et IPS-4255 des sections Mise à niveau, Mise à niveau vers un niveau inférieur et Installation des images système pour les procédures.

- Pour NM-CIDS, utilisez le chargeur de démarrage.

  Référez-vous à la section Installation de l'image système NM-CIDS de Mise à niveau, Mise à niveau vers une version antérieure et Installation des images système pour la procédure.

- Pour IDSM-2, réinstallez la partition d'application à partir de la partition de maintenance.

  Référez-vous à la section Installation de l'image système IDSM-2 de la section Mise à niveau, mise à niveau et installation des images système pour la procédure.

- Pour AIP-SSM, réinstallez à partir de l'ASA en utilisant le hw-module module 1 recover [configure | boot].

  Référez-vous à la section Installation de l'image système AIP-SSM de Mise à niveau, Mise à niveau vers une version antérieure et Installation des images système pour la procédure.

Informations connexes

- Page d'assistance de Cisco Intrusion Prevention System
- Mise à niveau, rétrogradation et installation des images système pour IPS 6.0
- Page d'assistance du module IDSM-2 (Intrusion Detection System) de la gamme Cisco Catalyst 6500
- Procédure de récupération de mot de passe pour le capteur Cisco IDS et les modules de services IDS (1, IDSM-2)
- Dépannage des mises à jour de signatures automatiques
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.