Contenu

Introduction

Ce document décrit comment améliorer l'image et la signature pour le logiciel de capteur de détection de Cisco Intrusion (ID) de la version 4.1 au Système de protection contre les intrusions Cisco (IPS) 5.0 et plus tard.

Remarque: De la version de logiciel 5.x et plus tard, le Cisco IPS remplace des ID de Cisco, qui s'applique jusqu'à la version 4.1.

Remarque: Le capteur ne peut pas télécharger des mises à jour logicielles de Cisco.com. Vous devez télécharger les mises à jour logicielles de Cisco.com à votre ftp server, et puis configurez le capteur afin de les télécharger de votre ftp server.

Référez-vous à installer la section d'image de système d'AIP SSM d'améliorer, de déclassifier, et d'installer des images de système pour la procédure.

Référez-vous à la procédure de récupération de mot de passe pour le capteur d'ID de Cisco et les Modules de services d'ID (IDSM-1, IDSM-2) afin de se renseigner plus sur la façon récupérer l'appliance de Cisco Secure IDS (autrefois NetRanger) et les modules pour des versions 3.x et 4.x.

Remarque: Le trafic d'utilisateur n'obtient pas affecté pendant la mise à jour dans la configuration **intégrée et échec-ouverte** sur l'ASA - AIP SSM.

Remarque: Référez-vous au logiciel de évolution de Cisco IPS de 5.1 à la section 6.x de configurer le capteur de Système de protection contre les intrusions Cisco utilisant l'interface de ligne de commande 6.0 pour plus d'informations sur la procédure pour améliorer l'IPS 5.1 à la version 6.x.

Remarque: Le capteur ne prend en charge pas des serveurs proxys pour les mises à jour automatiques. Les paramètres de proxy sont pour la caractéristique globale de corrélation seulement.

Conditions préalables

Conditions requises

La version de logiciel exigée minimum que vous devez afin d'améliorer à 5.0 est 4.1(1).

Composants utilisés

Les informations dans ce document sont basées sur le matériel d'ID de gamme Cisco 4200 qui exécute la version de logiciel 4.1 (être amélioré à la version 5.0).

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 à Conventions relatives aux conseils techniques Cisco.

Configurez

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

La mise à jour de Cisco 4.1 à 5.0 est disponible comme téléchargement de Cisco.com. Référez-vous à obtenir le logiciel de Cisco IPS pour la procédure que vous utilisez pour accéder à des téléchargements logiciels IPS sur Cisco.com.

Vous pouvez utiliser des méthodes l'unes des répertoriées ici afin d'exécuter la mise à jour :

- Après que vous téléchargiez le fichier de mise à niveau 5.0, référez-vous à Lisez-moi pour la procédure sur la façon dont installer le fichier de mise à niveau 5.0 avec la commande de **mise à jour**. Voyez l'utilisation la section de commande de mise à jour de ce pour en savoir plus de document.
- Si vous configuriez la mise à jour automatique pour votre capteur, copiez le fichier de mise à niveau 5.0 sur le répertoire sur le serveur balayages de ce vos capteur pour des mises à jour. Voyez l'utilisation la section de commande d'automatique-mise à jour de ce pour en savoir plus de document.
- Si vous installez une mise à jour sur votre capteur et le capteur est inutilisable après qu'il redémarre, vous devez réimager votre capteur. Une mise à jour d'un capteur de n'importe quelle version d'ID de Cisco plus tôt que 4.1 exige également de vous d'utiliser la commande de **récupérer** ou le CD de reprise/mise à jour. Voyez la Re-image la section de capteur de ce

pour en savoir plus de document.

Améliorez le capteur

Ces sections expliquent comment utiliser la commande de **mise à jour** d'améliorer le logiciel sur le capteur :

- Aperçu
- Commande et options de mise à jour
- Utilisez la commande de mise à jour

Aperçu

Vous pouvez améliorer le capteur avec ces fichiers, qui ont l'extension .package :

- Mises à jour de signature, par exemple, IPS-sig-S150-minreq-5.0-1.pkg
- Mises à jour d'engine de signature, par exemple, IPS-engine-E2-req-6.0-1.pkg
- Modifications 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 de pack de services, par exemple, IPS-K9-sp-5.0-2.pkg
- Mises à jour de partition de reprise, par exemple, IPS-K9-r-1.1-a-5.0-1.pkg
- Releases de correctif, par exemple, IPS-K9-patch-6.0-1p1-E1.pkg
- Mises à jour de partition de reprise, par exemple, IPS-K9-r-1.1-a-6.0-1.pkg

Une mise à jour de capteur change la version de logiciel du capteur.

Commande et options de mise à jour

Employez la commande **activée paroption** dans le sous-mode d'hôte de service afin de configurer des mises à jour automatiques.

Ces options s'appliquent :

- **par défaut** ? Place la valeur de nouveau à la configuration de paramètres systèmes par défaut.
- **répertoire** ? Répertoire où les fichiers de mise à niveau se trouvent sur le serveur de fichiers.
- **FILE-copie-Protocol** ? Le protocole de copie du fichier l'a utilisé aux fichiers téléchargés du serveur de fichiers. Les valeurs valides sont **FTP** ou **scp**.**Remarque:** Si vous utilisez le SCP, vous devez utiliser la commande de **clé de hôte de ssh** d'ajouter le serveur aux hôtes connus par SSH répertoriez ainsi le capteur peut communiquer avec lui par le SSH. Référez-vous à ajouter des hôtes aux hôtes connus les répertorient pour la procédure.
- **IP address** ? Adresse IP du serveur de fichiers.
- **mot de passe** ? Mot de passe utilisateur pour l'authentification sur le serveur de fichiers.
- **programme-option** ? Programmes quand les mises à jour automatiques se produisent. Mises à jour de établissement du programme de débuts de calendrier aux heures précises des jours spécifiques. L'établissement du programme périodique commence des mises à jour à intervalles périodiques spécifiques.**calendrier-programme** ? Configure les jours de la semaine et des heures du jour que des mises à jour automatiques sont exécuté.**jour-de-semaine** ? Jours de la semaine l'où des automatique-mises à jour sont exécutées. Vous pouvez

sélectionner de plusieurs jours. Les dimanche à samedi sont les valeurs valides.**non** ? Retire une configuration d'entrée ou de sélection.**temps-de-jour** ? Heures du jour à l'où les automatique-mises à jour commencent. Vous pouvez sélectionner de plusieurs périodes. La valeur valide est hh : millimètre [: solides solubles].**périodique-programme** ? Configure le temps que la première mise à jour automatique devrait se produire, et combien de temps attendre entre les mises à jour automatiques.**intervalle** ? Le nombre d'heures à attendre entre les mises à jour automatiques. Les valeurs valides sont de 0 à 8760.**start-time** ? L'heure pour commencer la première mise à jour automatique. La valeur valide est hh : millimètre [: solides solubles].

- **username** ? Nom d'utilisateur pour l'authentification sur le serveur de fichiers.

Pour la procédure IDM pour améliorer le capteur, référez-vous à mettre à jour le capteur.

Utilisez la commande de mise à jour

Vous recevez des erreurs SNMP si vous n'avez pas les paramètres de la **communauté à accès en lecture seule** et de la **communauté en lecture/écriture** configurés avant l'évolution à IPS 6.0. Si vous utilisez le snmp set et/ou **obtenez des** caractéristiques, vous devez configurer les paramètres de la **communauté à accès en lecture seule** et de la **communauté en lecture/écriture** avant que vous amélioriez à IPS 6.0. Dans IPS 5.x, la **communauté à accès en lecture seule** a été placée au public par défaut, et la **communauté en lecture/écriture** a été placée à privé par défaut. Dans IPS 6.0 ces deux options n'ont pas des valeurs par défaut. Si vous ne utilisiez pas le SNMP **obtient** et **place** avec IPS 5.x, par exemple, enable-positionnement-obtenez a été placé à faux, alors il n'y a aucun problème à améliorer à IPS 6.0. Si vous utilisiez le SNMP **obtient** et **place** avec IPS 5.x, par exemple, enable-positionnement-obtenez a été placé pour rectifier, vous devez configurer la **communauté à accès en lecture seule** et les paramètres de la **communauté en lecture/écriture aux** valeurs spécifiques ou à la mise à jour IPS 6.0 échoue.

Vous recevez le message d'erreur suivant :

Remarque: IPS 6.0 refuse des événements de risque fort par défaut. C'est une modification d'IPS 5.x. Afin de changer le par défaut, créez un dépassement d'action d'événement pour le paquet de refuser action intégrée et configurez-le à désactiver. Si l'administrateur ne se rend pas compte de la communauté lecture/écriture puis elles devraient essayer de désactiver le SNMP complètement avant qu'une tentative d'améliorer soit faite afin de retirer ce message d'erreur.

Terminez-vous ces étapes afin d'améliorer le capteur :

1. Téléchargez le fichier de modification majeure (IPS-K9-maj-5.0-1-S149.rpm.pkg) à un serveur de FTP, SCP, de HTTP, ou HTTPS qui est accessible de votre capteur.Référez-vous à obtenir le logiciel de Cisco IPS pour la procédure sur la façon dont localiser le logiciel sur Cisco.com.**Remarque:** Vous devez ouvrir une session à Cisco.com utilisant un compte avec des privilèges cryptographiques afin de télécharger le fichier. Ne changez pas le nom du fichier. Vous devez préserver le nom du fichier d'origine pour que le capteur reçoive la mise à jour.**Remarque:** Ne changez pas le nom du fichier. Vous devez préserver le nom du fichier d'origine pour que le capteur reçoive la mise à jour.
2. Ouvrez une session au CLI utilisant un compte avec des privilèges d'administrateur.
3. Passez en mode de configuration :`sensor#`**`configure terminal`**
4. Améliorez le capteur :`sensor(config)#`**`upgrade scp://<username>@<server IP>//upgrade/<file name>`**Exemple :**Remarque:** Cette commande est sur deux lignes dues aux raisons spatiales.`sensor(config)#`**`upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-`**

S149.rpm.pkg Remarque: Référez-vous aux serveurs pris en charge de FTP et HTTP/HTTPS pour une liste de serveurs pris en charge de FTP et HTTP/HTTPS. Référez-vous à ajouter des hôtes aux hôtes connus par SSH les répertorient pour plus d'informations sur la façon ajouter le serveur SCP à la liste d'hôtes connue par SSH.

5. Entrez le mot de passe une fois incité :`sensor(config)#`**`upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg`**
6. Type **oui** pour se terminer la mise à jour.**Remarque:** Les modifications majeures, les mises à jour mineures, et les packs de services pourraient forcer une reprise des processus IPS ou même forcer une réinitialisation du capteur pour se terminer l'installation. Ainsi, il y a une interruption de service pendant au moins deux minutes. Cependant, les mises à jour de signature n'exigent pas une réinitialisation après que la mise à jour soit faite. Référez-vous aux mises à jour de signature de téléchargement (clients enregistrés seulement) pour les dernières mises à jour.
7. Vérifiez votre nouvelle version de capteur :`sensor#`**`show version`**`Application Partition:Cisco Intrusion Prevention System,` **`Version 5.0(1)S149.0`**`OS Version 2.4.26-IDS-smp-bigphysPlatform: ASA-SSM-20Serial Number: 021No license presentSensor 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 RunningAnalysisEngine 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600 RunningCLI 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600Upgrade 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:** IPS 5.x, vous recevez un message qui énonce que la mise à jour est de type inconnu. Vous pouvez ignorer ce message.**Remarque:** Le système d'exploitation est réimagé et tous les fichiers qui ont été placés sur le capteur par le compte des services sont retirés.

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

Configurer des mises à jour automatiques

Mises à jour automatiques

Vous pouvez configurer le capteur pour rechercher des fichiers de nouvelle mise à jour dans votre répertoire de mise à jour automatiquement. Par exemple, plusieurs capteurs peuvent indiquer le même répertoire serveur ftp distant avec différents programmes de mise à jour, tels que toutes les 24 heures, ou lundi, mercredi, et vendredi à 11:00 P.M.

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

- Adresse IP du serveur
- Chemin du répertoire sur le serveur de fichiers où le capteur vérifie des fichiers de mise à niveau
- Protocole de copie du fichier (SCP ou FTP)
- Nom d'utilisateur et mot de passe
- Programme de mise à jour

Vous devez télécharger la mise à niveau de logiciel de Cisco.com et la copier sur le répertoire de mise à jour avant que le capteur puisse voter pour des mises à jour automatiques.

Remarque: Si vous utilisez la mise à jour automatique avec AIM-IPS et d'autres appliances IPS ou

modules, assurez-vous que vous mettez chacun des deux 6.0(1) le fichier de mise à niveau, 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 automatique de mise à jour de sorte qu'AIM-IPS puisse correctement le détecter qui classe les besoins d'être automatiquement téléchargé et installé. Si vous mettez seulement 6.0(1) le fichier de mise à niveau, IPS-K9-6.0-1-E1.pkg, sur le serveur automatique de mise à jour, des téléchargements AIM-IPS et des essais pour l'installer, qui est le fichier incorrect pour AIM-IPS.

Référez-vous à mettre à jour le capteur automatiquement pour plus d'informations sur la procédure IDM pour la mise à jour automatique du capteur.

Utilisez la commande d'automatique-mise à jour

Voyez la commande de mise à jour et la section Options de ce document pour les commandes d'automatique-**mise à jour**.

Terminez-vous ces étapes afin de programmer des mises à jour automatiques :

1. Ouvrez une session au CLI avec un compte qui a des privilèges d'administrateur.
2. Configurez le capteur afin de rechercher automatiquement des nouvelles mises à jour dans votre répertoire de mise à jour.`sensor#`**`configure terminal`**`sensor(config)#`**`service host`**`sensor(config-hos)#`**`auto-upgrade-option enabled`**
3. Spécifiez l'établissement du programme :Pour le calendrier programmant, qui commence des mises à jour aux heures précises des jours spécifiques :`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 l'établissement du programme périodique, qui commence des mises à jour à intervalles périodiques spécifiques :`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 :`sensor(config-hos-ena-per)#`**`exit`**`sensor(config-hos-ena)#`**`ip-address 10.1.1.1`**
5. Spécifiez le répertoire où les fichiers de mise à niveau se trouvent sur le serveur de fichiers :`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 :`sensor(config-hos-ena)#`**`user-name tester`**
7. Spécifiez le mot de passe de l'utilisateur :`sensor(config-hos-ena)#`**`password`**`Enter password[]: `**`******`**`Re-enter password: `**`******`**
8. Spécifiez le protocole de serveur de fichiers :`sensor(config-hos-ena)#`**`file-copy-protocol ftp`****Remarque:** Si vous utilisez le SCP, vous devez employer la commande de **clé de hôte de ssh** afin d'ajouter le serveur aux hôtes connus par SSH répertoriez ainsi le capteur peut communiquer avec lui par le SSH. Référez-vous à ajouter des hôtes aux hôtes connus les répertorient pour la procédure.
9. Vérifiez les configurations :`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 d'automatique-mise à jour :`sensor(config-hos-ena)#`**`exit`**`sensor(config-hos)#`**`exit`**`Apply Changes:?`**`[yes]:`**
11. Appuyez sur **entrent** afin d'appliquer les modifications ou taper **aucun** afin de les jeter.

Re-image le capteur

Vous pouvez réimager votre capteur de ces manières :

- Pour des appliances d'ID avec un lecteur de CD-ROM, utilisez le CD de reprise/mise à jour.Référez-vous section à utiliser de reprise/mise à jour CD d'améliorer, de déclassifier, et d'installer des images de système pour la procédure.
- Pour tous les capteurs, utilisez la commande de **récupérer**.Référez-vous à récupérer la section de partition d'application d'améliorer, de déclassifier, et d'installer des images de système pour la procédure.
- L'IDS-4215, l'IPS-4240, et l'IPS 4255, utilisation ROMMON de restaurer l'image de système.Référez-vous à installer l'image du système IDS-4215 et à installer des sections d'image du système IPS-4240 et IPS-4255 d'améliorer, de déclassifier, et d'installer des images de système pour les procédures.
- Pour NM-CIDS, utilisez le programme de démarrage.Référez-vous à installer la section d'image de système NM-CIDS d'améliorer, de déclassifier, et d'installer des images de système pour la procédure.
- Pour IDSM-2, réimagez la partition d'application de la partition de maintenance.Référez-vous à installer la section d'image du système IDSM-2 de l'évolution, déclassifiant, et installant des images de système pour la procédure.
- Pour l'AIP SSM, réimagez de l'ASA utilisant le **module 1 de hw-module récupèrent [configurez |** commande de **démarrage]**.Référez-vous à installer la section d'image de système d'AIP SSM d'améliorer, de déclassifier, et d'installer des images de système pour la procédure.

Informations connexes

- Page de support de Système de protection contre les intrusions Cisco
- Améliorant, déclassifiant, et installer des images de système IPS 6.0
- Page de support de module de Detection System d'intrusion de gamme Cisco Catalyst 6500 (IDSM-2)
- Procédure de récupération de mot de passe pour le capteur et les Modules de services 1 d'ID de Cisco d'ID, IDSM-2)
- Dépannage des mises à jour d'Automatique-signature
- Support et documentation techniques - Cisco Systems