IDS 4.0/AIP-SSM/IPS 5.0 et versions ultérieures - Forum Aux Questions

Contenu

Introduction

Ce document répond aux questions les plus fréquemment posées (FAQ) concernant Cisco Secure Intrusion Detection System (IDS) 4.0, Advanced Inspection and Prevention Security Services Module (AIP SSM) et Cisco Intrusion Prevention System (IPS) 5.0 et versions ultérieures.

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

IDS 4.0

Q. J'ai installé IDS MC et SecMon sur un nouveau serveur et maintenant je veux importer toutes les configurations (utilisateur, périphérique, etc.) de l'ancien serveur vers le nouveau. Comment faire ?

A. La façon la plus simple d'effectuer ceci est d'amener votre nouveau serveur VMS, puis de découvrir les capteurs avec cette nouvelle boîte.

Remarque : Lorsque vous ajoutez le capteur, ne l'ajoutez pas manuellement. Cochez la case **paramètres de découverte**.

Une fois le capteur détecté, importez-le dans **SecMon**. Toutes les configurations sont enregistrées sur le capteur. Les paramètres de signature, les filtres, etc., doivent être détectés après la création de votre nouveau serveur. Veillez à mettre à jour IDS MC avec les dernières signatures.

Q. IDS-4215 reçoit `idsPackageMgr :` message d'erreur `d'argument non valide` lors de la mise à niveau de la partition de récupération IDS. Que dois-je faire pour résoudre ce problème ?

A. C'est un problème de fabrication. Certains clients ont reçu des IDS-4215 avec une mauvaise image de base (4.0). Procédez comme suit :

1. Téléchargez l'image de partition de récupération (clients enregistrés uniquement).

2. Appliquer la mise à niveau de l'image de partition de récupération via l'interface de ligne de commande :
```
sensor#configure terminal
sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/
    IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg
```

3. Une fois l'image de partition de récupération appliquée, le 4215 est restauré à une base 4.1(1) 4215 normale.
```
sensor(config)#recover application-partition
```

Q. Lorsque je mets à niveau un paquet de niveau SIG à 2 chiffres vers un paquet de niveau SIG à 3 chiffres, tel que S100 ou ultérieur, par exemple, 4.1(4)S99 vers 4.1(4)S100, la fonctionnalité de mise à jour automatique échoue. Comment résoudre ce problème ?

Remarque : les clients Cisco VMS et CLI ne rencontrent pas ce problème.

La cause du problème est la logique de tri utilisée lors de l'analyse du nom de fichier. Il s'agit d'un tri alphanumérique lorsqu'il doit être numérique. La solution de contournement est d'utiliser l'interface de ligne de commande (ou VMS) pour mettre à niveau des packages de niveau SIG à 3 chiffres, tels que S100 ou version ultérieure. Une fois cette opération terminée, la mise à jour automatique recommence à fonctionner. Référez-vous à l'ID de bogue Cisco CSCef07999 (clients enregistrés uniquement) pour plus d'informations.

Q. Qu'est-ce que l'`erreur de manipulation de jeton d'authentification ?` message d'erreur ?

A. Afin de résoudre ce problème, utilisez le mot de passe par défaut (cisco) deux fois, puis modifiez le mot de passe en mode de configuration. L'IDS nécessite que le mot de passe par défaut soit entré deux fois.

Exemple :

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re-enter new password: ***
```

Q. Comment supprimer l'IDSM du commutateur ?

A. Le module ne doit être retiré qu'après avoir désactivé l'alimentation. Procédez comme suit :

1. À partir de l'interface de ligne de commande du capteur, exécutez la commande **reset powerdown**.
2. Une fois le capteur arrêté, à partir de l'interface de ligne de commande du commutateur, émettez la commande **no power enable module (module_number)** pour Cisco IOS ou la commande **set module power down (module_number)** pour CatOS.
3. Appuyez sur le bouton shutdown sur la lame.
4. Arrêtez physiquement le châssis. Lorsque le voyant d'état affiche un vert plus long, vous

pouvez retirer le module en toute sécurité.

IPS 5.0 et versions ultérieures

Q. J'ai configuré le contournement, mais je ne sais pas comment configurer le blocage sur les signatures. Quelle est la différence entre un hôte de bloc et une connexion de bloc ?

A. Bloquer l'hôte bloque tous les paquets de cette adresse source. Bloquer la connexion bloque uniquement la connexion unique en fonction de l'adresse IP/du port source et de destination. Le PIX fonctionne d'une manière légèrement différente. Pour les mises hors tension automatiques, le capteur envoie l'adresse IP source, l'adresse IP de destination, le port source et le port de destination. Le PIX bloque tous les paquets qui proviennent de cette adresse IP. Les informations supplémentaires sont utilisées par le PIX pour supprimer cette connexion de ses tables de connexion. Si la connexion n'a pas été supprimée de la table de connexion, il est théoriquement possible que si le shun est supprimé peu après son application, la connexion d'origine n'ait pas encore expiré. Cela permet au pirate de poursuivre l'attaque sur la connexion d'origine. La suppression de la connexion de la table garantit que la connexion d'origine ne peut pas être utilisée pour poursuivre l'attaque après la suppression du shun. Le capteur ne peut pas ignorer une seule connexion sur le PIX, car le PIX ne prend pas en charge l'utilisation de la commande **shun** afin d'éviter une seule connexion. La commande **shun** PIX désactive toujours l'adresse source, que les informations de connexion supplémentaires soient fournies ou non.

Q. Qu'est-ce que l'**erreur ? Impossible de redémarrer les services réseau. Une erreur fatale s'est produite. Le noeud DOIT être redémarré pour activer l'alarme ».** message d'erreur ?

A. Cette erreur signifie que votre passerelle par défaut est incorrecte ou un message d'erreur générique qui signifie que l'adresse IP, le masque de réseau ou la passerelle par défaut sont incorrects. La partie `Fatal` du message signifie qu'après la première défaillance, la configuration précédente a été appliquée et a également échoué. Le capteur émet des commandes **ifconfig** et **route** et l'une d'elles ou les deux échoue.

Q. La mise à jour automatique échoue avec la **« mainApp[343] Cid/E errSystemError http erreur response:500 ».** . Que signifie ce message d'erreur ?

A. Ce problème peut être la fonctionnalité de mise à jour automatique, qui ne fonctionne pas, car elle est configurée pour être téléchargée à une heure pair. Essayez de définir la mise à jour automatique sur une durée aléatoire ; même un léger décalage de huit ou de nuit minutes peut résoudre ce problème.

En général, le problème est résolu et l'`erreur : réponse d'erreur http :` Un message d'erreur `500` s'affiche si vous modifiez l'heure de récupération sur une limite non horaire.

Remarque : IPS échoue la mise à jour automatique des signatures et renvoie le message d'erreur suivant :

```
Exception AutoUpdate : Échec de la connexion HTTP [1,110] name=errSystemError
```

Vérifiez ces éléments afin de résoudre ce problème :

- Vérifiez si un pare-feu empêche le capteur d'atteindre Cisco.com.
- Vérifiez si le routage pose problème.
- Vérifiez si NATing est correctement configuré sur le périphérique de passerelle pour le périphérique en aval.
- Vérifiez si les informations d'identification de l'utilisateur sont correctes.
- Remplacer l'heure de début de la mise à jour par des heures impaires.

Q. Qu'est-ce que l'**erreur ? execUpgradeSoftware : AnalysisEngine est actuellement occupé et ne peut pas traiter cette mise à jour. Veuillez patienter plusieurs minutes avant de réessayer de mettre à jour. »** message d'erreur ?

A. Afin de résoudre ce problème, essayez de recharger le capteur ou de réinstaller le capteur.

Q. Comment résoudre le message d'erreur **Avertissement Cid/W - Le proxy DNS ou HTTP est requis pour l'inspection de corrélation globale et le filtrage de réputation, mais aucun serveur DNS ou proxy n'est défini.Ajoutez un serveur proxy HTTP ou un serveur DNS dans la configuration du service 'host'** ?

A. Effectuez ces tâches afin de résoudre ce problème :

- Désactivez la corrélation globale.
- Ajoutez la configuration proxy/dns.

Q. Comment résoudre les erreurs qu'IPS reçoit pour les problèmes d'intégrité de corrélation globale ? "**23 janv. 2010 15:50:39.831 38.001 collaborationApp[655] rep/E Une mise à jour de corrélation globale a échoué : Échec de l'ouverture d'une connexion TLS au serveur HTTP à X.X.82.127:443 : Échec de la connexion TLS**" et "**collaborationApp[459] rep/E Une mise à jour de corrélation globale a échoué : Échec du téléchargement d'ibrs/1.1/drop/default/1296529950 : L'URI ne contient pas d'adresse IP valide**" ?

A. IPS ne peut pas accéder à Internet en raison d'un problème de port, par exemple, un pare-feu dans un chemin qui ne dispose pas des ports appropriés ouverts pour l'accès Internet ou il peut s'agir d'un problème de NAT.

Pour que la corrélation globale fonctionne complètement, le capteur commence par contacter via https **update-manifestes.ironport.com** afin d'authentifier l'utilisateur, puis une connexion HTTP pour télécharger les mises à jour GC. Les fichiers que le capteur télécharge à partir du HTTP (update.ironport.com) sont les données de réputation utilisées par la corrélation globale. Le fichier https update-manifests.ironport.com doit toujours se résoudre à l'adresse X.X.82.127, mais l'adresse IP http **update.ironport.com** peut changer, selon l'Internet auquel vous accédez. Vous devez donc vérifier l'adresse IP. Si le filtrage d'URL est activé, ajoutez une exception pour l'adresse IP de l'interface de gestion IPS dans le filtre d'URL, afin qu'IPS puisse se connecter à Internet.

Cette erreur se produit lorsqu'il y a corruption dans une mise à jour GC précédente :

```
collaborationApp[459] rep/E A global correlation update failed: Échec du téléchargement
d'ibrs/1.1/drop/default/1296529950 : L'URI ne contient pas d'adresse IP valide
```

Ce problème peut généralement être corrigé en désactivant le service GC, puis en le réactivant. Dans IDM, choisissez **Configuration > Policies > Global Correlation > Inspection/réputation**,

définissez Global Correlation Inspection (and Reputation Filtering if On) sur Off, appliquez les modifications, attendez 10 minutes, activez les fonctionnalités et surveillez.

Q. La `mise à jour de corrélation globale a échoué : openConnection : IpAddrException badAddrString pris. Impossible d'utiliser le proxy HTTP de corrélation globale et les paramètres DNS. Vérifiez la connexion et réessayez.` un message d'erreur est reçu dans la catégorie « Échec de la mise à jour de réputation ». Comment faire pour résoudre ce problème ?

A. Vérifiez ces éléments :

- Vous devez disposer d'une licence IPS valide pour permettre le fonctionnement des fonctionnalités de corrélation globale.
- Un serveur proxy HTTP ou un serveur DNS doit être configuré pour permettre le fonctionnement des fonctionnalités de corrélation globale.
- Comme les mises à jour de corrélation globale se produisent via l'interface de gestion des capteurs, les pare-feu doivent autoriser le trafic tcp 443/80 et udp 53.
- Assurez-vous que votre capteur prend en charge les fonctionnalités de corrélation globale. Si vous ne le souhaitez pas, désactivez la fonctionnalité de collaboration globale à partir d'IDM :Accédez à Configuration > Policies > Global Correlation > Inspection/Réputation, et définissez Global Correlation Inspection (and Reputation Filtering if On) sur Off.

Q. Comment résoudre le `« échec d'une mise à jour de corrélation globale : openConnection : Erreur IpAddrException badAddrString »` reçue par IPS pour un problème d'intégrité de corrélation globale ?

A. Si vous utilisez la corrélation globale (GC), assurez-vous que la résolution de noms fonctionne, par exemple, le DNS est accessible. Vérifiez également si un pare-feu bloque le port 53. Sinon, vous pouvez désactiver la fonction GC si vous souhaitez supprimer ce message.

Q. Comment résoudre l'`exception lors de l'initialisation de la connexion au MySQL` message d'erreur que je reçois lors du lancement d'IME à partir du navigateur ?

A. Ce problème se produit généralement lorsque le client tente d'exécuter IME sur des systèmes d'exploitation non pris en charge, tels que Windows 7.

Q. Comment résoudre le `" Titre : IDM sur 88-nsmc-c1 Fournisseur : Cisco Systems, Inc. Catégorie : Les ressources JAR d'erreur de fichier de lancement dans le fichier JNLP ne sont pas signées par le même certificat ». ou « Erreur lors de la connexion au capteur, échec de la création du capteur x.x.x.x:443 idm »` erreur reçue par IDM, qui se produit lors du lancement de l'application ?

A. Effacez le cache du navigateur afin de résoudre ce problème.

Q. Le mode asymétrique sur IPS est-il configurable si vous utilisez l'interface utilisateur graphique ?

A. Dans la version 6.0, mode asymétrique sur IPS configurable à l'aide de l'interface de ligne de

commande uniquement et non disponible sur l'interface utilisateur graphique. Mais dans la version 6.1, cette fonctionnalité est également disponible dans l'interface utilisateur graphique.

Q. Comment résoudre le problème de latence avec le capteur IPS ?

A. Afin de résoudre ce problème, activez le traitement en mode asymétrique afin de permettre au capteur de synchroniser l'état avec le flux et de maintenir l'inspection pour les moteurs qui ne nécessitent pas les deux directions. Utilisez cette configuration :

```
IPS_Sensor#configure terminal
IPS_Sensor(config)#service analysis-engine
IPS_Sensor(config-ana)#virtual-sensor vs0
IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

Le problème de latence se produit lorsque l'action de refus en ligne et le paquet de refus sont activés pour chaque signature dans VS0. L'activation de toutes les signatures entraînera une latence lorsque IPS inspectera chaque paquet passant par. Il est bon d'activer uniquement la signature spécifique requise conformément au flux de trafic réseau afin de résoudre le problème de latence.

Q. AIP-SSM bloque-t-il Skype ?

A. Le PIX/ASA ne peut pas bloquer le trafic skype. Skype est capable de négocier des ports dynamiques et d'utiliser du trafic crypté. Grâce au trafic chiffré, il est pratiquement impossible de le détecter, puisqu'il n'existe aucun modèle à rechercher.

Vous pourriez éventuellement utiliser un système de prévention des intrusions (IPS)/AIP-SSM de Cisco. Certaines des signatures de ces systèmes sont capables de détecter un client Skype Windows qui se connecte au serveur Skype pour synchroniser sa version. Ceci a généralement lieu lorsque le client lance la connexion. Quand le capteur détecte la connexion Skype initiale, vous pouvez rechercher l'utilisateur du service et bloquer toutes les connexions lancées à partir de son adresse IP.

Q. Pourquoi l'interface de détection `clignote-t-elle` ou passe-t-elle souvent à l'état down dans IPS ?

A. Lors d'une mise à jour et d'une reconfiguration des signatures, le capteurApp s'arrête pour traiter les paquets lors du traitement des nouvelles signatures dans la mise à jour. Le pilote réseau détecte que le capteurApp s'est arrêté et extrait tout nouveau paquet de la mémoire tampon. Le pilote réseau fait donc des choses différentes, qui dépendent de la configuration et du modèle de capteur :

Interface promiscuous : elle désactive la liaison sur les interfaces et la réactive une fois que le capteurApp recommence à surveiller.

Inline Interface ou Inline Vlan Pair : dépend du paramètre de contournement :

- Ignorer l'Auto : le pilote maintient la liaison active et commence à transmettre les paquets sans analyse. Il retourne ensuite à l'envoi des paquets par le capteurApp une fois que le capteurApp recommence à surveiller.

- **Contournement désactivé** : le pilote désactive la liaison sur les interfaces, ce qui est identique au mode promiscuité, et les réactive une fois que le capteurApp recommence à surveiller.

Ainsi, si l'application de capteur n'extrait pas les paquets de la mémoire tampon, ce qui peut se produire parce qu'il n'y a aucune interface configurée pour traiter les paquets, alors le pilote peut mettre l'interface dans un état `down`.

Ces journaux sont visibles lorsque l'interface de détection clignote :

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

Q. Le capteur IDS ou IPS (Intrusion Prevention System) conserve-t-il un historique des mots de passe ?

A. Non, le capteur ne conserve pas d'historique des mots de passe. Les mots de passe ne sont pas visibles à tout moment.

Q. Le capteur IDS ou IPS prend-il en charge le serveur syslog pour envoyer des journaux ?

A. No.

Q. Quelle est la limite maximale de stockage des événements dans IPS ?

A. L'événement local du capteur ne stocke que 30 Mo et commence à se remplacer une fois la limite de 30 Mo atteinte. Cette limite n'est pas configurable.

Q. Comment écrire une signature pour détecter un fichier foto[a-z]\.zip dans un e-mail entrant ou sortant ?

A. Utilisez STRING.TCP afin d'écrire une signature qui détecte la pièce jointe. Recherchez quelque chose de similaire :

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["][Ff][Oo]
             [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
ResetAfterIdle 15
ServicePorts 25
StorageKey =STREAM
```

Q. Comment configurez-vous le délai d'attente du client FTP ?

A. Émettez les commandes suivantes :

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

Q. Comment convertissez-vous l'heure de début et l'heure de fin dans l'état iplog en un format lisible ?

A. Ce résultat est une représentation décimale de l'heure actuelle depuis l'époque UNIX. Utilisez un calculateur époc UNIX tel que celui situé sur le site UNIX Date/Time Calculator . Entrez les 10 premiers chiffres car cette calculatrice est granulaire à quelques secondes seulement, et le système IDS stocke les nanosecondes. Cela signifie que les neuf derniers chiffres sont supprimés. À partir de l'heure de début dans ce résultat, `1084798479 = Lun Mai 17 12:54:39 2004 (GMT)` est ce que vous recevez.

Àpartir de l'interface de ligne de commande, entrez **iplog-status** afin de recevoir cette sortie :

```
"
Log ID:              138343946
IP Address:          xxx.xxx.xxx.xxx
Group:               0
Status:              completed
Start Time:          1084798479512524000
End Time:            1084798510136582000
Bytes Captured:      2833
Packets Captured:    14
"
```

Q. La **« IOException lors de l'obtention du certificat : java.security.cert.CertificateExpiredException ».** apparaît. Comment cela peut-il être résolu ?

A. Afin de résoudre ce message d'erreur, connectez-vous à AIP-SSM et émettez la commande **tls generate-key** en mode d'exécution privilégié, comme illustré dans cet exemple :

```
sensor#tls generate-key
```

Remarque : Cette résolution d'utilisation de la commande **tls generate-key** résout également le problème de l'incapacité d'AIP-SSM à se connecter à IME.

Q. L'**IOException : Connexion refusée:connexion. Le serveur IME ne répond pas. Vérifiez s'il est en cours d'exécution »,** un message d'erreur s'affiche pendant que j'ajoute IPS dans IME. Comment résoudre ce problème ?

A. Afin de résoudre ce message d'erreur, choisissez **Panneau de configuration > Outils d'administration > Services** et redémarrez les services IME.

Q. Le message d'erreur **Impossible de vérifier la configuration nom d'utilisateur/mot de passe[IOEXception - connect timed out]** est reçu lorsque j'ajoute un capteur IPS à l'IME. Comment résoudre ce problème ?

A. Cela indique une communication interrompue entre l'IME et le capteur IPS. Assurez-vous qu'aucun logiciel ne bloque le SDEE.

Q. La **« Réponse d'erreur du serveur IME : Erreur inconnue (consultez le fichier journal dans le répertoire journal de l'installation)" .** apparaît. Comment résoudre ce problème ?

A. Afin de résoudre ce message d'erreur, vérifiez que l'adresse IP correcte est utilisée lorsque vous ajoutez IPS dans IME et vérifiez également tout pare-feu logiciel exécuté sur l'ordinateur IME, qui peut bloquer la connexion.

Q. Le capteur IDS ou IPS peut-il envoyer des alertes par e-mail ?

A. Le capteur IDS n'est pas en mesure d'envoyer des alertes par e-mail par lui-même. Le Moniteur de sécurité lorsqu'il est utilisé avec IDS peut envoyer des notifications par e-mail lorsqu'une règle d'événement est déclenchée par le capteur.

Référez-vous à Configurer les notifications par courrier électronique pour plus d'informations sur la façon de configurer les notifications par courrier électronique avec Security Monitor.

Cisco IPS Manager Express (IME) peut être configuré pour envoyer un message de notification par e-mail (alertes) lorsque les règles d'événement sont déclenchées par les capteurs Cisco IPS. Reportez-vous à IPS 6.X et versions ultérieures : Exemple de configuration de notifications par e-mail à l'aide d'IME pour plus d'informations.

Q. L'**erreur : Impossible de communiquer avec mainApp (getVersion). Contactez votre administrateur système.** un message d'erreur s'affiche lorsque j'essaie de me connecter à mon capteur. Comment résoudre ce problème ?

A. Redémarrez le capteur afin de résoudre ce problème.

Q. L'**avertissement : AVERTISSEMENT : Ressources insuffisantes disponibles pour combiner tous les index personnalisés actuellement actifs. Certaines alertes ne s'allument pas. Envisagez de retirer des signatures jusqu'à ce que ce message ne se produise plus.** le message d'erreur s'affiche lors du réglage de la signature sur mon capteur. Comment résoudre ce problème ?

A. Retirer les signatures qui ne sont pas utilisées afin de résoudre ce problème et également le nombre de signatures de clients avec des index doit être réduit. De plus, il n'est pas recommandé d'utiliser des métacaractères ***** et **+** dans les index.

Q. Pourquoi des problèmes de latence surviennent-ils sur les capteurs IPS (Intrusion Prevention System) de Cisco ? Comment résoudre ce problème ?

A. Le problème de latence peut se produire en raison du routage asymétrique. Essayez de désactiver la signature 1330 afin de résoudre ce problème.

Q. Est-il possible de désactiver SSHv1 et de ne laisser que SSHv2 activé sur les capteurs IPS (Intrusion Prevention System) de Cisco ?

A. Pour le moment, il n'est pas possible de désactiver SSHv1 et de ne laisser que SSHv2 activé. SSHv1 et SSHv2 sont tous deux activés ensemble et ne peuvent pas être désactivés individuellement.

Q. L'**erreur : Une erreur s'est produite au niveau du capteur lors de la mise à jour, message du capteur = La mise à jour nécessite 115 000 Ko dans /usr/cids/idsRoot/var, il n'y a que 110 443 Ko disponibles.** apparaît lorsque je mets à niveau le capteur vers la version 4.1(5). Comment résoudre ce problème ?

A. Ce message d'erreur se produit en raison d'une mémoire insuffisante dans le capteur.

Effectuez ces tâches afin de résoudre ce problème :

1. Se connecter au compte de service et devenir racine
2. Supprimez les répertoires suivants comme indiqué ci-dessous :
   ```
   # rm -rf /usr/cids/idsRoot/var/updates/files/S69
   # rm -rf /usr/cids/idsRoot/var/updates/files/common
   # rm /usr/cids/idsRoot/var/virtualSensor/*
   # rm /usr/cids/idsRoot/var/.tmp/*
   ```
3. Essayez maintenant de mettre à niveau le capteur. Référez-vous à l'ID de bogue Cisco CSCsb81288 (clients enregistrés uniquement) pour plus d'informations.

Q. J'obtiens le message d'erreur **mainApp[396] cplane/E - accept() call retourné -1** dans le journal sur ASA. Comment résoudre cette erreur ?

A. Le message d'erreur `mainApp[396] cplane/E Error - accept() a renvoyé -1` indique que le serveur Web ne peut pas lire le fichier, et le programme accept() a échoué, ce qui donne des descripteurs de fichier quand il y a des connexions TLS. Mais ce fichier n'est pas nécessaire pour un comportement normal. C'est inoffensif.

Q. Comment résoudre l'**exception de connexion TLS de tls/W errTransport WebSession::sessionTask :** message d'erreur **handshake incomplet** ?

A. Ce message d'erreur indique que le certificat n'est plus valide sur le module. Complétez ces étapes afin de résoudre le problème :

1. Régénérer le certificat à partir de l'interface de ligne de commande :Connectez-vous à la ligne de commande du capteur.Émettez la commande **tls generate**, puis appuyez sur **Entrée**. Notez les empreintes qui s'affichent.
2. Saisissez le nouveau certificat dans IME :Ouvrez l'IME et localisez le nom du capteur dans la liste de la page d'accueil.Cliquez avec le bouton droit sur le capteur, puis cliquez sur **Modifier**.Lorsque vous accédez à l'écran Edit Device (Modifier le périphérique), cliquez sur **OK**. Ignorez tout avertissement de ne pas pouvoir récupérer le temps du capteur.Le nouveau certificat de sécurité (celui que vous venez de générer) vous sera demandé. Vérifiez que les empreintes correspondent, puis cliquez sur **Oui**.Après plusieurs secondes, le capteur doit afficher à nouveau « Connecté » dans l'état de l'événement.

Q. Lorsque je tente de me connecter à IPS, je reçois ce message d'erreur : `errSystemError-ct-capteurAPP.450 ne répond pas, échec de clientpipe.` Comment est-ce que je peux résoudre cette erreur ?

A. Afin de résoudre cette erreur, utilisez la commande **reset** afin de redémarrer l'IPS.

Q. L'heure de l'AIP-SSM diffère de celle de l'ASA (Adaptive Security Appliance) de Cisco. Comment résoudre ce problème ?

A. Afin de résoudre ce problème, utilisez le serveur NTP pour synchroniser l'heure sur Cisco Adaptive Security Appliance (ASA) et AIP-SSM.

Référez-vous à Configuration de NTP sur les capteurs IPS pour plus d'informations.

Q. Comment puis-je appliquer plusieurs capteurs virtuels sur AIP-SSM ?

A. Les capteurs virtuels sur AIP-SSM ne peuvent pas être appliqués par interface, car l'AIP-SSM n'a qu'une seule interface. Lorsque vous créez plusieurs capteurs virtuels, vous devez affecter cette interface à un seul capteur virtuel. Vous n'avez pas besoin de désigner une interface pour les autres capteurs virtuels.

Après avoir créé des capteurs virtuels, vous devez les mapper à un contexte de sécurité sur l'appareil de sécurité adaptatif (ASA) à l'aide de la commande **allos-ips**. Vous pouvez mapper de nombreux contextes de sécurité à de nombreux capteurs virtuels. Référez-vous à la section *Affectation de capteurs virtuels aux contextes d'appareils de sécurité adaptatifs* de Configuration d'AIP-SSM pour plus d'informations.

Q. Quel est le nombre maximal de capteurs virtuels pris en charge par AIP-SSM ?

A. Quatre capteurs virtuels maximum peuvent être pris en charge.

Q. Si j'utilise SSH ou IDM pour me connecter à IPS, est-il possible de configurer IPS 4240/IDSM/IDSM2 afin de valider les utilisateurs administratifs sur un serveur RADIUS/TACACS+ ?

A. Il n'est pas possible avec un serveur TACACS+ mais RADIUS est pris en charge à partir de la version IPS 7.0.(4)E4. Reportez-vous aux sections *Informations nouvelles et modifiées* et *Restrictions et limitations* des Notes de publication pour Cisco Intrusion Prevention System 7.0(4)E4 pour plus d'informations. Référez-vous également à IPS 7.X : Exemple de configuration de l'authentification de connexion utilisateur utilisant ACS 5.X comme serveur Radius pour un exemple de configuration.

Q. Quel est l'impact de la licence expirée sur la fonctionnalité IPS ?

A. La seule incidence d'une licence expirée sur le capteur est qu'elle arrête les mises à jour de signature.

Q. Les mises à jour des signatures IPS ont-elles un impact sur les services ou la connectivité réseau ?

A. Non. Les mises à jour des signatures IPS n'ont pas d'impact sur les services ou la connectivité réseau.

Q. Quelle est l'URL exacte que je dois saisir pour que le module IPS se mette à jour automatiquement avec les dernières signatures ?

A. Le lien nécessaire pour permettre au module IPS de se mettre à jour automatiquement avec la dernière signature est le suivant : https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl.

Vous devez utiliser votre ID utilisateur et votre mot de passe Cisco pour terminer la mise à jour du module IPS.

Remarque : dans le train de code 6.x, les mises à jour automatiques de Cisco.com ne sont pas prises en charge. Vous devez télécharger manuellement les fichiers de signature et les appliquer au capteur. Il existe une fonction de mise à jour automatique dans le code 6.x ; cependant, cela n'est possible qu'à partir d'un serveur de fichiers local dans lequel les fichiers de signature doivent également être téléchargés manuellement.

Q. Le capteur IPS est-il vulnérable à la vulnérabilité de piratage de session de transfert de port X11 ?

A. Non. Il n'est pas vulnérable pour les raisons suivantes :

- Le capteur ne dispose pas de bibliothèques X11. Par conséquent, il n'y a aucune session à pirater.
- Le transfert de port X11 n'est pas activé dans la configuration SSH.
- IPv6 n'est pas compilé dans le noyau du capteur. Cela est nécessaire pour exploiter la vulnérabilité.

Q. Pourquoi l'AIP-SSM n'affiche-t-il aucun journal lorsque l'ASA affiche de nombreux journaux d'avertissement et d'attaque ?

A. Cela se produit parce que lorsque l'ASA bloque quelque chose, il n'est pas transmis à l'IPS pour inspection en double. Par conséquent, vous ne pouvez pas voir de journaux en double sur l'ASA et l'IPS.

Q. Après qu'un utilisateur a déployé le jeu de signatures S518, le message d'erreur "`InvalidValue : Editng string-xl-tcp sig XXXX n'a AUCUN effet dans cette version`" se produit. Pourquoi ?

A. Voici le message d'erreur complet :

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=-240 timeZone=GMT-05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string-xl-tcp
sig 21619 has NO effect
```

Ce problème survient car le moteur string-xl-tcp ou string-tcp-xl n'est pas pris en charge sur le matériel. Pour plus de détails, reportez-vous aux notes de version du moteur IPS E4.

Q. Lorsque je mets à jour automatiquement les signatures sur un ASA-SSM-10 avec la fonction de mise à jour automatique, je reçois ce message d'erreur : **Aucun package de mise à jour automatique installable trouvé sur l'état du serveur=true.** Comment puis-je résoudre ce problème ?

A. Cette sortie affiche le message d'erreur complet :

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi-bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Cette erreur a été générée et les signatures ne sont pas mises à jour automatiquement car la définition de signature est mise à jour après que S479 ait besoin du moteur E4. Pour résoudre ce problème, vous devez mettre à niveau manuellement le capteur vers 7.0(2)E4.

Remarque : Le capteur ne peut pas se mettre automatiquement à niveau vers E4 car il nécessite 7.0(2) et un redémarrage du capteur.

Q. La fonction de mise à jour automatique du module IPS 5.0 pour NIDS ne fonctionne pas. Comment puis-je résoudre ce problème ?

A. Cette sortie affiche le message d'erreur complet :

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

Ce problème se produit en raison d'un style de liste de répertoire incorrect avec le serveur FTP. Afin de résoudre ce problème, passez aux listes de répertoires de type UNIX à partir des listes de répertoires de style MS-DOS existantes.

Afin de modifier les paramètres de la liste des répertoires, sélectionnez **Démarrer > Fichiers programme > Outils d'administration** afin d'ouvrir Internet Services Manager. Ensuite, accédez à l'onglet Home Directory et modifiez le style de liste des répertoires de MS-DOS à UNIX.

Q. IPS-4255 reçoit le message d'erreur SensorApp échoue dans TcpRootNode::expireNow() lors d'une mise à niveau. Comment faire pour résoudre ce problème ?

A. Ce problème est dû à la défaillance du moteur d'analyse et est traité dans l'ID de bogue Cisco CSCtb39179 (clients enregistrés uniquement). Mettez à niveau le capteur vers la version 7.0(4)E4 afin de résoudre ce problème.

Q. Lorsque je tente d'effectuer une mise à jour de licence après avoir acheté une nouvelle licence, le périphérique signale cette erreur : **« Échec de la mise à jour de la licence sur le capteur. » « errExpiredLicense-La nouvelle date d'expiration de la licence est**

antérieure à la date d'expiration de la licence actuelle. » Comment puis-je résoudre ce problème ?

A. Ce problème se produit lorsque le fichier de licence reçu n'est pas valide. Pour obtenir un fichier de licence valide, connectez-vous à Cisco.com en tant qu'utilisateur enregistré et téléchargez le fichier de licence approprié. Une fois que vous avez obtenu le fichier de licence valide, installez-le sur votre capteur.

Si vous installez le nouveau fichier de licence et que vous recevez toujours une erreur, il se peut qu'il y ait un problème avec le fichier de licence non valide existant. Afin de résoudre ce problème, procédez comme suit pour supprimer le fichier de licence non valide existant :

1. Connectez-vous au compte de service en saisissant votre nom d'utilisateur de compte de service.Si vous n'avez pas de compte de service, ouvrez la ligne de commande IPS, passez en mode de configuration et entrez cette commande**username** ***name*** **privilège service password mot de** ***passe***
```
ciscoasa# session 1
Opening command session with slot 1.

Connected to slot 1. Escape character sequence is 'CTRL-^X'.
login:
Password:

IPS#
IPS#conf t
IPS(config)# username name privilege service password password
```
2. Une fois connecté à votre compte de service, entrez la commande **su** afin d'accéder à root (en utilisant le même mot de passe que le compte de service).
3. Supprimez les fichiers du répertoire /usr/cids/idsRoot/shared/.**Remarque :** ne supprimez pas le fichier host.conf.Entrez la commande **cd /usr/cids/idsRoot/shared/shared/** afin d'accéder au répertoire partagé.Entrez la commande **ls** afin d'afficher les fichiers dans le répertoire.Entrez la commande **rm** ***file_name*** afin de supprimer les fichiers.**Remarque :** ne supprimez pas le fichier host.conf.
4. Entrez la commande **/etc/init.d/cids restart** pour redémarrer le capteur.
5. Installez la nouvelle licence.

Un bogue Cisco a été déposé pour traiter ce comportement. Pour plus d'informations, consultez CSCtg76339 (clients enregistrés uniquement).

Q. Que fait le **message d'erreur : IpLog 1712041197 s'est terminé tôt en raison d'un manque de gestionnaires de fichiers. name=Moyenne du** message d'erreur **ErrLimitExceeded** ? Comment faire pour résoudre ce problème ?

A. Cette erreur est causée par un nombre excessif de paquets sur la journalisation IP. Désactivez la fonction de journalisation IP afin de résoudre ce problème. La journalisation IP est destinée uniquement au dépannage ; Cisco recommande de ne pas l'activer pour toutes les signatures.

Q. Je reçois cette erreur lorsque je mets à jour le capteur de s550 vers s551 : **Impossible d'analyser la configuration actuelle pour le composant « signatureDefinition » et l'instance « sig0 ».** Comment puis-je résoudre ce problème ?

A. La modification de la signature 23899.0 entraîne ce problème. Référez-vous à l'ID de bogue

Cisco CSCtn84552 (clients enregistrés uniquement) pour plus d'informations.

Q. Je reçois cette erreur sur le capteur : **Erreur : autoUpdate a correctement sélectionné un package dans le service de localisation cisco.com, mais le téléchargement du package a échoué : Échec de réception de la réponse HTTP.** Comment puis-je résoudre ce problème ?

A. Vérifiez si le filtrage d'URL, le filtrage de contenu ou un serveur proxy empêche la mise à jour automatique de se produire. Assurez-vous que autoUpdate n'est pas bloqué et vérifiez également que les informations d'identification de l'utilisateur fournies sont correctes.

Q. Je reçois ce message d'erreur XML sur le capteur IPS qui fonctionne avec la version 6.2(3)E4 : **errorMessage : Le logiciel IPS a tenté d'écrire des données XML non valides pour (jeton). Les caractères XML non valides ont été remplacés par '*'.** Comment puis-je résoudre ce problème ?

A. Ce comportement a été traité par l'ID de bogue Cisco CSCsq50873 (clients enregistrés uniquement). Il s'agit d'un problème cosmétique qui ne crée pas de surcharge opérationnelle, à l'exception de la quantité excessive de journaux reçus. Une solution de contournement temporaire consiste à supprimer la configuration NTP sur le capteur. Pour une solution permanente, mettez à niveau vers une version dans laquelle ce bogue est corrigé.

Q. Pourquoi la station de travail IME établit-elle des connexions constantes aux serveurs gérés malgré la fermeture du client ?

A. IME fonctionne comme deux services Windows et le client GUI. Lorsque le client est fermé, les deux services Windows (Cisco IPS Manager Express et MySQL-IME) continuent d'exécuter et de collecter des événements à partir des capteurs gérés et de les stocker dans la base de données locale MySQL ; cela permet d'établir des rapports historiques.

Le client IME doit ouvrir un seul abonnement SDEE au capteur géré et réutiliser cet abonnement pour une activité ultérieure de récupération d'événements. La connectivité constante entre la station de travail IME et les capteurs gérés est un comportement attendu.

Q. Le module AIP-SSM peut-il être utilisé comme cible SPAN ?

A. Non. Le module AIP-SSM ne peut pas être utilisé en tant que cible SPAN, car il est utilisé uniquement pour surveiller le trafic circulant via l'interface ASA.

Q. Pourquoi une utilisation élevée du processeur est-elle observée après la mise à niveau du système IPS vers le moteur E3 ?

A. Avec les mises à jour du moteur E3, l'IPS utilise un autre algorithme pour gérer son temps d'inactivité et passe plus de temps à interroger les paquets pour réduire la latence. Cette vérification accrue entraîne une augmentation correspondante de l'utilisation du processeur. La bonne façon de mesurer le CPU dans E3 n'est pas par l'utilisation du CPU, mais par le **pourcentage de charge de paquet** qui indique l'utilisation correcte du CPU.

Q. Pourquoi le voyant d'état de santé devient-il ROUGE de façon intermittente sur mon dispositif IPS ?

A. Cela peut se produire en raison d'un certificat incorrect sur la station de gestion distante, de l'exécution de logiciels tels que CS-MARS, CSM, IEV, VMS-IDS/IPSMC, etc. Afin de résoudre ce problème, procédez comme suit :

1. Appliquez le certificat TLS du capteur sur la station de gestion distante.
2. Configurez un serveur DNS valide.

Q. Comment empêcher l'IPS de retarder le trafic HTTP lors de sa traversée des interfaces ?

A. La configuration du capteur pour qu'il fonctionne en mode asymétrique résoudra le problème. Afin de placer le capteur dans une protection de mode asymétrique, procédez comme suit :

1. Accédez à **Configuration > Policies > IPS policies**.
2. Double-cliquez sur **capteur virtuel**.
3. Accédez aux **options avancées**.
4. Sous Mode de normalisation, sélectionnez **Protection du mode asymétrique**.
5. Click OK.
6. Redémarrez l'unité afin que les modifications prennent effet.

Informations connexes

- Page d'assistance Cisco Secure Intrusion Prevention System
- Dépannage d'AIP-SSM
- Avis de champs relatifs aux produits de sécurité (y compris CiscoSecure Intrusion Detection)
- Support et documentation techniques - Cisco Systems