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

Contenu

Introduction

Ce document répond aux questions fréquemment posées (Foires aux questions) liées au système de détection d'intrusion Cisco Secure (ID) 4.0, Advanced Inspection and Prevention Security Services Module (AIP SSM), et Système de protection contre les intrusions Cisco (IPS) 5.0 et plus tard.

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

ID 4.0

Q. J'ai installé des ID MC et SecMon au-dessus d'un nouveau serveur et maintenant je veux aux configurations import all (utilisateur, périphérique, et ainsi de suite) du vieux serveur au neuf. Comment est-ce que je fais ceci ?

A. Le moyen le plus simple d'exécuter ceci est d'amener votre nouveau serveur VMS, et puis découvre les capteurs avec cette nouvelle case.

Remarque: Quand vous ajoutez le capteur, ne l'ajoutez pas manuellement. Cochez la case de **configurations de découvrir**.

Une fois que le capteur est découvert, importez-le dans **SecMon**. Toutes les configurations sont enregistrées sur le capteur. Les configurations de signature, des filtres, et ainsi de suite devraient trouver par hasard après que vous construisiez votre nouveau serveur. Assurez-vous vous des ID MC de mise à jour aux dernières signatures.

Q. IDS-4215 reçoit l'`idsPackageMgr : non valide d'argument` message d'erreur tandis qu'il tente d'améliorer la partition de reprise d'ID. Queest-ce que je dois faire pour résoudre ce problème ?

A. C'est une question de fabrication. Quelques clients ont reçu IDS-4215s avec une mauvaise image de base (4.0). Procédez comme suit :

1. Téléchargez l'image de partition de reprise (clients enregistrés seulement).
2. Appliquez la mise à niveau d'image de partition de reprise par le CLI :
   ```
   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 que l'image de partition de reprise est appliquée, les 4215 est restaurés sur une base 4215 de l'exécution normale 4.1(1).
   ```
   sensor(config)#recover application-partition
   ```

Q. Quand j'améliore d'un 2-digit aux modules de niveau des sig 3-digit, tels que S100 ou plus tard, par exemple, 4.1(4)S99 à 4.1(4)S100, la fonctionnalité d'automatique-mise à jour échoue. Comment résoudre ce problème ?

Remarque: Cisco VMS et les clients CLI n'éprouvent pas cette question.

La cause du problème est la logique la triant qui est utilisée quand le nom du fichier est analysé. C'est un tri alphanumérique quand il devrait être numérique. Le contournement est d'employer le CLI (ou le VMS) pour améliorer aux modules de niveau des sig 3-digit, tels que S100 ou plus tard. Une fois que ceci est terminé, l'automatique-mise à jour commence à fonctionner de nouveau. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCef07999 (clients enregistrés seulement).

Q. Ce qui fait « 1'erreur symbolique de manipulation d'authentification ». moyen de message d'erreur ?

A. Afin de résoudre ce problème, utilisez le mot de passe par défaut (Cisco) deux fois et changez alors le mot de passe du mode de config. Les ID exige du mot de passe par défaut d'être entré deux fois.

Exemple :

```
sensor(config)#recover application-partition
```

Q. Comment est-ce que je retire l'IDSM du commutateur ?

A. Le module devrait être retiré seulement après que vous désactivez l'alimentation. Procédez comme suit :

1. Du capteur CLI, émettez la commande de **powerdown de remise**.
2. Une fois que le capteur se termine l'arrêt, du commutateur CLI, question ou l'**aucune** commande de **module de power enable (module_number)** pour le Cisco IOS ou la **mise hors tension de module de positionnement (module_number)** commandez pour CatOS.
3. Appuyez sur le bouton **shutdown** sur la lame.
4. Arrêtez physiquement le châssis. Quand le voyant d'état affiche un plus long vert, vous pouvez retirer le module sans risque.

IPS 5.0 et plus tard

Q. Je fais configurer l'évitement mais je suis confondu au sujet de la façon configurer le blocage sur les signatures. Quelle est la différence entre l'hôte de bloc et la connexion de bloc ?

A. L'hôte de bloc bloque tous les paquets de cette adresse source. La connexion de bloc bloque seulement l'une connexion basée sur la source et la destination IP/port. Le PIX fonctionne d'une manière légèrement différente. Pour automatique évite, le capteur envoie le source ip, l'IP de destination, le port de source, et la destination port. Le PIX bloque tous les paquets qui proviennent de cette adresse IP. Les informations complémentaires sont utilisées par le PIX pour enlever cette une connexion de ses tables de connexion. Si la connexion n'a pas été enlevée de la table de connexion, alors il est théoriquement possible que si l'évitement est enlevé peu de temps après qu'il est appliqué, alors la connexion d'origine ne pourrait pas avoir chronométré encore. Ceci permet à l'attaquant pour continuer l'attaque sur la connexion d'origine. La suppression de la connexion de la table s'assure que la connexion d'origine ne peut pas être utilisée pour continuer l'attaque après que l'évitement soit enlevé. Le capteur ne peut pas éviter une connexion unique sur le PIX parce que le PIX ne prend en charge pas l'utilisation de la commande d'**évitement** afin d'éviter une connexion unique. Les PIX **évitent la** commande évitent toujours l'adresse source indépendamment de si les informations de connexion supplémentaires sont fournies.

Q. Ce qui fait la **« erreur : N'a pas pu redémarrer les services réseau. L'erreur fatale s'est produite. Le noeud DOIT être redémarré pour activer l'alarme ».** moyen de message d'erreur ?

A. Cette erreur signifie que votre passerelle par défaut est incorrecte ou un message d'erreur générique qui signifie que l'IP, le netmask, ou la passerelle par défaut sont incorrects. La partie `mortelle du` message signifie qu'après la première panne, la configuration précédente était appliquée et également manquée. Le capteur émet l'**ifconfig** et l'**artère** commande et on ou chacun d'eux échoue.

Q. Autoupdate échoue avec l'**erreur response:500" de HTTP d'errSystemError "mainApp[343] cid/e. .** Que ce message d'erreur signifie-t-il ?

A. Cette question pourrait être la caractéristique automatique de mise à jour, qui ne fonctionne pas, parce qu'elle est placée pour la télécharger même à une heure. Essayez de placer la mise à jour automatique à un temps aléatoire ; même un petit décalage de huit ou les minutes de nuit peut réparer ce problème.

Généralement la question est résolue et l'`erreur : réponse d'erreur de HTTP : 500 que le` message d'erreur est soient vus si vous changez le temps de récupération à une borne non-horaire.

Remarque: L'IPS échoue l'automatique-mise à jour des signatures et retourne avec ce message d'erreur :

```
Exception d'AutoUpdate : La connexion HTTP a manqué name=errSystemError [1,110]
```

Vérifiez ces éléments afin de résoudre ce problème :

- Vérifiez si un Pare-feu empêche le capteur de Cisco.com de atteinte.

- Vérifiez si l'acheminement devient une question.
- Vérifiez si NATing est correctement configuré sur le périphérique de passerelle pour le périphérique en aval.
- Vérifiez si les identifiants utilisateurs sont corrects.
- Changez l'heure de début de mise à jour aux heures impaires.

Q. Ce qui fait la **« erreur : execUpgradeSoftware : AnalysisEngine ne peut pas actuellement occupé et traiter cette mise à jour. Veuillez attendre plusieurs minutes avant de tenter la mise à jour de nouveau. ».** moyen de message d'erreur ?

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

Q. Comment fais je résolvez l'**avertissement du** message d'erreur **Cid/W - des DN ou le proxy HTTP est exigés pour l'inspection globale et la réputation de corrélation filtrant mais aucun DN ou serveur proxy n'est défini. Ajoutez un serveur proxy ou un serveur DNS de HTTP dans la configuration de service de « hôte »** ?

A. Terminez-vous ces tâches afin de résoudre ce problème :

- Corrélation globale de débronchement.
- Ajoutez le proxy/configuration de dn.

Q. Comment fais je résolvez ces erreurs que l'IPS reçoit pour des problèmes de santés globaux de corrélation : « **23Jan2010 15:50:39.831 38.001 mise à jour globale de corrélation collaborationApp[655] rep/E A a manqué : Pour ouvrir une connexion de TLS au serveur HTTP à X.X.82.127:443 : La connexion de TLS a manqué** » et « la **mise à jour globale de corrélation collaborationApp[459] rep/E A a manqué : Téléchargement défectueux d'ibrs/1.1/drop/default/1296529950 : L'URI ne contient pas un IP address valide** » ?

A. L'IPS ne peut pas arriver à l'Internet en raison d'un problème de port, par exemple, un Pare-feu dans un chemin qui n'a pas les ports droits ouverts pour l'accès Internet ou lui peut être une question NAT.

Pour la corrélation globale à fonctionner complètement, les contacts de capteur d'abord par des https **update-manifests.ironport.com** afin d'authentifier l'utilisateur et une connexion HTTP puis télécharger des mises à jour de CHROMATOGRAPHIE GAZEUSE. Les fichiers que le capteur télécharge du HTTP (updates.ironport.com) sont les données de réputation que la corrélation globale utilise. Les https update-manifests.ironport.com devraient toujours les résoudre à l'adresse X.X.82.127, mais l'**adresse IP d'**updates.ironport.com de HTTP **peut changer**, qui dépend de l'Internet que vous accédez à. Ainsi vous devez vérifier l'adresse IP. Si le Filtrage URL est activé, ajoutez une exception pour l'IP d'interface de Gestion IPS dans le filtre URL, de sorte que l'IPS puisse se connecter à l'Internet.

Cette erreur se produit quand il y a de corruption dans une mise à jour précédente de CHROMATOGRAPHIE GAZEUSE :

```
la mise à jour globale de corrélation collaborationApp[459] rep/E A a manqué : Téléchargement
défectueux d'ibrs/1.1/drop/default/1296529950 : L'URI ne contient pas un IP address valide
```

Cette question peut habituellement être corrigée en arrêtant le service de CHROMATOGRAPHIE GAZEUSE et en le tournant alors de retour en fonction. Dans IDM, choisissez la **configuration >**

les stratégies > corrélation > inspection/réputation globales, placez l'inspection globale de corrélation (et la réputation filtrant si en fonction) à hors fonction, appliquez les modifications, attendez 10 minutes, allumez les caractéristiques, et les surveillez.

Q. `La mise à jour globale de corrélation A a manqué : openConnection : IpAddrException attrapé badAddrString. Incapable d'utiliser le proxy HTTP de corrélation et les configurations globaux de DN. Vérifiez la connexion et l'essai de nouveau.` le message d'erreur est reçu dans la catégorie « de panne de mise à jour de réputation ». Comment faire pour résoudre ce problème ?

A. Vérifiez ces éléments :

- Vous devez avoir un permis valide IPS afin de permettre aux caractéristiques globales de corrélation pour fonctionner.
- Vous devez faire configurer un serveur proxy de HTTP ou un serveur DNS afin de permettre aux caractéristiques globales de corrélation pour fonctionner.
- Puisque les mises à jour globales de corrélation se produisent par l'interface de gestion de capteur, les Pare-feu doivent permettre le TCP 443/80 et le trafic de l'UDP 53.
- Assurez-vous que votre capteur prend en charge les caractéristiques globales de corrélation. Si vous ne voulez pas ceci, désactivez la configuration globale de Collaboration d'IDM :Allez à la configuration > aux stratégies > corrélation > inspection/réputation globales, et placez l'inspection globale de corrélation (et la réputation filtrant si en fonction) à hors fonction.

Q. Comment fais je résolvez `« de la mise à jour globale de corrélation a manqué : openConnection : Erreur badAddrString décelée d'IpAddrException »` que l'IPS reçoit pour le problème de santés global de corrélation ?

A. Si vous utilisez la corrélation globale (CHROMATOGRAPHIE GAZEUSE) puis assurez-vous que la résolution de noms fonctionne, par exemple, les DN est accessible. Vérifiez également s'il y a un port bloqué par Pare-feu 53. Autrement, vous pouvez arrêter la caractéristique de CHROMATOGRAPHIE GAZEUSE si vous souhaitez se débarasser de ce message.

Q. Comment est-ce que je résous l'`exception en initialisant la connexion au` message d'erreur de `MySQL` que je reçois quand je lance IME du navigateur ?

A. Cette question se produit habituellement quand tentative de client d'exécuter IME sur les systèmes d'exploitation sans support, tels que le Windows 7.

Q. Comment fais je résolvez le `« titre : IDM sur le constructeur 88-nsmc-c1 : Catégorie de Cisco Systems, Inc. : Des ressources en POT d'erreurs de fichier de lancement dans le fichier JNLP ne sont pas signées par le même certificat ». ou « erreur se connectant au capteur, pour créer le capteur x.x.x.x:443` erreur `quittant idm »` qu'IDM reçoit, qui se produit pendant le lancement de l'application ?

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

Q. Le mode asymétrique sur l'IPS est-il configurable si vous utilisez le GUI ?

A. Dans la version 6.0, mode asymétrique sur l'IPS qui est configurable utilisant le CLI seulement et non disponible sur le GUI. Mais, dans la version 6.1 cette caractéristique est également disponible dans le GUI.

Q. Comment est-ce que je résous le problème de latence avec le capteur IPS ?

A. Afin de résoudre ce problème, activez le mode asymétrique traitant afin de permettre au capteur pour synchroniser l'état avec l'écoulement et pour mettre à jour l'inspection pour ces engines qui n'exigent 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
```

La question de latence se produit quand l'en ligne d'action de refuser et refuse le paquet sont activées pour chaque signature dans VS0. L'activation de toutes les signatures aura comme conséquence la latence comme l'IPS examine traverser chaque de paquet. Il est bon d'activer seulement la signature spécifique exigée selon l'écoulement du trafic réseau afin de résoudre le problème de latence.

Q. L'AIP SSM aide-t-il à bloquer Skype ?

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

Vous pourriez par la suite utiliser un Cisco IPS (système de prévention des intrusions) /AIP-SSM. 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 fait l'instabilité de détection d'interface ou va fréquemment à l'état d'indisponibilité dans l'IPS ?

A. Pendant une mise à jour et les reconfigurations de signature, les arrêts de sensorApp pour traiter des paquets en tant qu'elle traite les nouvelles signatures dans la mise à jour. Le pilote réseau détecte que le sensorApp a arrêté et tire tous les nouveaux paquets de la mémoire tampon. Ainsi le pilote réseau fait différentes choses, qui dépend de la configuration et du modèle de capteur :

Interface promiscueuse — Elle apporte le lien vers le bas sur les interfaces, et apporte le lien sauvegardent une fois que des débuts de sensorApp pour surveiller de nouveau.

Paires intégrées de VLAN d'interface ou d'en ligne — Il dépend de la configuration de contournement :

- **Automatique de contournement** — Le gestionnaire maintient le lien haut et commence à passer des paquets sans analyse. Il revient à alors envoyant les paquets par le sensorApp

une fois que des débuts de sensorApp pour surveiller de nouveau.
- **Contournement hors fonction** — Le gestionnaire apporte le lien vers le bas sur les interfaces, qui est identique qu'en mode promiscueux, et les apporte sauvegardent une fois que le sensorApp commence à surveiller de nouveau.

Ainsi, si l'app de capteur ne tire pas des paquets de la mémoire tampon, qui se produit probablement parce qu'il n'y a aucune interface configurée pour traiter des paquets, puis le gestionnaire peut mettre l'interface dans un état d'indisponibilité.

Ces logs sont vus quand l'interface de détection s'agite :

```
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
```

Q. Le capteur d'ID ou de Système de prévention d'intrusion (IPS) met-il à jour un historique de mot de passe ?

A. Non, le capteur ne met pas à jour un historique de mot de passe. Les mots de passe ne sont pas visualisables à tout moment.

Q. Le serveur de Syslog de support de capteur d'ID ou de Système de prévention d'intrusion (IPS) envoie-t-il des logs ?

A. No.

Q. Quelle est la limite maximum d'enregistrer des événements dans l'IPS ?

A. L'événement local du capteur enregistre seulement 30 Mo et commence à se remplacer une fois que la limite du Mo 30 est atteinte. Cette limite est non-configurable.

Q. Comment font j'écrivent signature pour détecter le foto [fichier] d'a-z \ .zip dans n'importe quel email entrant ou sortant ?

A. Employez le STRING.TCP afin d'écrire une signature qui détecte la connexion. Recherchez quelque chose semblable à ceci :

```
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
```

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

A. Émettez les commandes suivantes :

```
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
```

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

A. Cette sortie est une représentation décimale du temps en cours depuis l'epoc UNIX. Utilisez une calculatrice d'epoc UNIX telle que celle située au site de calculatrice de date/heure UNIX. Écrivez les 10 premiers chiffres parce que cette calculatrice est granulaire seulement aux secondes, et les ID enregistre des nanosecondes. Ceci signifie que les neuf derniers chiffres sont décollés. Dès le début temps dans cette sortie, est `1084798479 = Lun 20h04 (GMT) du 17 mai 12:54:39` ce que vous recevez.

Du CLI, écrivez l'iplog-**état** 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. **Le « IOException quand essai pour obtenir le certificat : java.security.cert.CertificateExpiredException ».** apparaît. Comment est-ce que ceci peut être résolu ?

A. Afin de résoudre ce message d'erreur, procédure de connexion dans l'AIP SSM et émettre la commande de générer-clé de tls dans le mode d'exécution privilégié suivant les indications de cet exemple :

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

Remarque: Cette résolution d'utiliser la générer-clé de tls de commande résout également le problème de l'AIP SSM ne pouvant pas se connecter à l'IME.

Q. **Le « IOException : Connexion refusée : connectez. Le serveur IME IME ne répond pas. Vérifiez s'il vous plaît s'il exécute le »** message d'erreur apparaît tandis que j'ajoute l'IPS dans IME. Comment cette question peut-elle être résolue ?

A. Afin de résoudre ce message d'erreur, choisissez le **panneau de configuration > les outils administrateur > les services** et redémarrez les services IME.

Q. **Ne pourrait pas vérifier le** message d'erreur de **nom d'utilisateur/mot de passe de config [IOException - connectez chronométré]** est reçu quand j'ajoute un capteur IPS à l'IME. Comment cette question peut-elle être résolue ?

A. Ceci indique la transmission cassée entre l'IME et le capteur IPS. Assurez-vous qu'il n'y a aucun logiciel qui bloque le SDEE.

Q. **La « réponse d'erreur du serveur IME : Erreur inconnue (fichier journal de contrôle dans le répertoire du log de l'installation) ».** apparaît. Comment cette question peut-elle être résolue ?

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

Q. Le capteur d'ID ou de Système de prévention d'intrusion (IPS) peut-il envoyer des alertes par courrier électronique ?

A. Le capteur d'ID n'a pas la capacité d'envoyer des alertes par courrier électronique seule. Le contrôleur de sécurité une fois utilisé avec des ID a la capacité d'envoyer des notifications électroniques quand une règle d'événement est déclenchée par le capteur.

Référez-vous configurent des notifications par courrier électronique pour plus d'informations sur la façon configurer des notifications électroniques avec le contrôleur de sécurité.

Le Cisco IPS Manager Express (IME) peut être configuré pour envoyer le message de notification électronique (alertes) quand des règles d'événement sont déclenchées par des capteurs de Cisco IPS. Référez-vous à IPS 6.X et plus tard : Notifications électroniques utilisant le pour en savoir plus d'exemple de configuration IME.

Q. **L'erreur : Ne peut pas communiquer avec le mainApp (getVersion). Veuillez contacter votre administrateur système.** le message d'erreur apparaît quand j'essaye de me connecter à mon capteur. Comment cette question peut-elle être résolue ?

A. Redémarrez le capteur afin de résoudre ce problème.

Q. **L'avertissement : AVERTISSEMENT : Ressources insuffisantes disponibles pour combiner tous actuellement - expressions régulières faites sur commande actives. Quelques alertes ne se déclencheront pas. Les signatures réservées Consider jusqu'à ce message ne se produit plus.** le message d'erreur apparaît signature accordant sur mon capteur. Comment cette question peut-elle être résolue ?

A. Retirez les signatures qui sont non utilisables afin de résoudre ce problème et également le nombre de signatures de client avec des expressions régulières devrait être réduit. En outre, il n'est pas recommandé pour l'utiliser ***** et **+ des** métacaractères dans les expressions régulières.

Q. Pourquoi les questions de latence se produisent-elles sur des capteurs du Système de protection contre les intrusions Cisco (IPS) ? Comment cette question peut-elle être résolue ?

A. La question 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 laisser seulement le SSHv2 activé sur les capteurs du Système de protection contre les intrusions Cisco (IPS) ?

A. En ce moment il n'est pas possible de désactiver SSHv1 et de laisser seulement SSHv2 activé. SSHv1 et SSHv2 sont activés ensemble et ne peuvent pas être désactivés individuellement.

Q. **L'erreur : Une erreur s'est produite au capteur pendant la mise à jour, message de capteur = la mise à jour exige 115000 KO dans /usr/cids/idsRoot/var, là sont seulement 110443 KO disponibles.** le message apparaît quand j'améliore le capteur à la version 4.1(5). Comment cette question peut-elle être résolue ?

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

Terminez-vous ces tâches afin de résoudre ce problème :

1. Connectez-vous dans le compte des services et devenez racine
2. Enlevez les répertoires suivants comme affiché ci-dessous :

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

3. Maintenant essai pour améliorer le capteur. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCsb81288 (clients enregistrés seulement).

Q. J'obtiens l'**erreur mainApp[396] cplane/E - l'appel d'accept() a renvoyé le** message d'erreur **-1** dans le login ASA. Comment cette erreur peut-elle être résolue ?

A. `L'erreur mainApp[396] cplane/E - l'appel d'accept() a renvoyé le` message d'erreur `-1` indique que le serveur Web ne peut pas indiquer le fichier, et le programme d'accept() a manqué, qui des descripteurs de fichier de rendements quand les connexions de TLS existent. Mais ce fichier n'est pas nécessaire pour le comportement normal. C'est inoffensif.

Q. Comment fais je résolvez l'**errTransport WebSession tls/W : : exception de connexion de TLS de sessionTask :** message d'erreur **inachevé de prise de contact** ?

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

1. Régénérez le certificat du CLI :Procédure de connexion à la ligne de commande de capteur.Émettez le **tls génèrent la** commande, et l'appuient sur **entrent**. Notez les empreintes digital qui sont affichées.
2. Tirez le nouveau certificat dedans à IME :Ouvrez l'IME et localisez le nom de capteur dans la liste sur la page d'accueil.Cliquez avec le bouton droit le capteur, et cliquez sur Edit.Quand vous atteignez l'écran de périphérique d'éditer, cliquez sur OK. Sautez n'importe quel avertissement au sujet de ne pas pouvoir récupérer le temps de capteur.Vous serez incité avec le nouveau Security Certificate (celui que vous avez juste généré). Vérifiez pour s'assurer que les empreintes digital s'assortissent, et cliquent sur **oui**.Après plusieurs secondes, le capteur devrait afficher en cas l'état « connecté » de nouveau.

Q. Quand je tente d'ouvrir une session à l'IPS, je reçois ce message d'erreur : `errSystemError-ct-sensorAPP.450 ne répondant pas, clientpipe a manqué.` Comment est-ce que je peux résoudre cette erreur ?

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

Q. Le temps sur l'AIP SSM diffère du temps sur l'appliance de sécurité adaptable Cisco (ASA). Comment cette question peut-elle être résolue ?

A. Afin de résoudre ce problème, utilisez le serveur de NTP pour synchroniser le temps sur la Sécurité adaptative Appliance(ASA) de Cisco et l'AIP SSM.

Référez-vous à configurer le NTP sur le pour en savoir plus de capteurs IPS.

Q. Comment est-ce que je peux appliquer de plusieurs capteurs virtuels sur l'AIP SSM ?

A. Les capteurs virtuels sur l'AIP SSM ne peuvent pas être appliqués par interface parce que l'AIP SSM a seulement une interface. Quand vous créez de plusieurs capteurs virtuels, vous devez assigner cette interface à seulement un capteur virtuel. Vous n'avez pas besoin d'indiquer une interface pour les autres capteurs virtuels.

Après que vous créiez les capteurs virtuels, vous devez les tracer à un contexte de sécurité sur l'appliance de sécurité adaptable (ASA) utilisant la commande allouer-**IPS**. Vous pouvez tracer beaucoup de contextes de sécurité à beaucoup de capteurs virtuels. Référez-vous aux *capteurs virtuels assignants à la* section de *contextes d'appliance de sécurité adaptable de* configurer le pour en savoir plus d'AIP SSM.

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

A. Un nombre maximal de quatre capteurs virtuels peut être pris en charge.

Q. Si je l'utilise est-ce que SSH ou l'IDM afin d'ouvrir une session à l'IPS alors est lui possible de configurer l'IPS 4240/IDSM/IDSM2 afin de valider les utilisateurs administratifs contre un serveur RADIUS/TACACS+ ?

A. Il n'est pas possible avec un serveur TACACS+ mais RADIUS est pris en charge de la release IPS 7.0.(4)E4. Référez-vous aux sections *nouvelles et changées de l'information* et de *restrictions et limites des* notes de mise à jour pour le pour en savoir plus du Système de protection contre les intrusions Cisco 7.0(4)E4. En outre, référez-vous à IPS 7.X : Authentification d'ouverture de session utilisateur utilisant ACS 5.X comme exemple de configuration du serveur RADIUS pour une configuration d'échantillon.

Q. Quelle est l'incidence du permis expiré sur le funcationality IPS ?

A. La seule incidence qu'un permis expiré a sur le capteur est qu'elle arrête les mises à jour de signature.

Q. Les mises à jour de signature IPS ont-elles une incidence sur les services ou la

connexion réseau ?

A. No. Les mises à jour de signature IPS n'ont pas une incidence sur les services ou la connexion réseau.

Q. Quel est l'URL précis que je dois écrire pour que le module IPS mette à jour automatiquement avec les dernières signatures ?

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

Vous devez employer votre user-id et mot de passe de Cisco pour se terminer la mise à jour du module IPS.

Remarque: Dans la série 6.x de code, des mises à jour automatiques de Cisco.com ne sont pas prises en charge. Vous devez manuellement télécharger les fichiers de signatures et les appliquer au capteur. Il y a une fonction d'automatique-mise à jour dans le code 6.x ; cependant, c'est possible seulement d'un serveur de fichier local en lequel les fichiers de signatures doivent manuellement être aussi bien téléchargés.

Q. Le capteur IPS vulnérable à la session de la transmission du port X11 détourne-il la vulnérabilité ?

A. No. Il n'est pas vulnérable pour ces raisons :

- Le capteur n'a pas les bibliothèques X11. Par conséquent il n'y a aucune session à la détourner.
- La transmission du port X11 n'est pas activée dans la configuration de SSH.
- L'IPv6 n'est pas compilé dans le noyau de capteur. Ceci est exigé afin d'exploiter la vulnérabilité.

Q. Pourquoi l'AIP SSM n'affiche-t-il pas des logs quand l'ASA affiche l'abondance des logs d'avertissement et d'attaque ?

A. Ceci se produit parce que quand l'ASA bloque quelque chose, il n'est pas passé à l'IPS pour l'inspection en double. Par conséquent, vous ne pouvez pas voir que le doublon ouvre une session l'ASA et l'IPS.

Q. Après qu'un utilisateur déploie le positionnement de la signature S518, le « **invalidValue : Le sig de chaîne-XL-TCP d'Editng n'a AUCUN effet** message d'erreur **dans cette version** » se produit. Pourquoi ?

A. C'est le message d'erreur complet :

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

Cette question est soulevée parce que le chaîne-XL-TCP ou l'engine chaîne-TCP-XL n'est pas

pris en charge sur le matériel. Pour plus de détails, référez-vous aux notes de mise à jour en engine E4 IPS.

Q. Quand je mets à jour automatiquement des signatures sur un ASA-SSM-10 avec la configuration automatique de mise à jour, je reçois ce message d'erreur : **Aucun module automatique installable de mise à jour ne fondent sur le status=true de serveur.** Comment puis-je résoudre ce problème ?

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

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

Cette erreur a été générée et les signatures ne mettent pas à jour automatiquement parce que les mises à jour de définition de signature après S479 exigent l'engine E4. Afin de résoudre ceci, vous devez améliorer manuellement le capteur à 7.0(2)E4.

Remarque: Le capteur ne peut pas s'améliorer automatiquement à E4 parce qu'il exige 7.0(2) et une réinitialisation du capteur.

Q. Le feauture automatique de mise à jour sur l'IPS 5.0 pour le module NIDS ne fonctionne pas. Comment puis-je résoudre ce problème ?

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

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

Cette question se produit en raison d'un style inexact de liste de répertoires avec le ftp server. Afin de résoudre ceci, commutez aux listes de répertoires de style de l'UNIX des listes de répertoires existantes de style de MS-DOS.

Afin de modifier les configurations de liste de répertoires, **début** choisi > **fichiers** > **outils d'administration de programme** afin d'ouvrir le gestionnaire de Services Internet. Alors allez à l'onglet de répertoire home et changez le style de liste de répertoires du MS-DOS à l'UNIX.

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

A. Cette question est due à la panne de l'engine d'analyse et est adressée dans l'ID de bogue Cisco CSCtb39179 (clients enregistrés seulement). Améliorez le capteur à la version 7.0(4)E4 afin de réparer cette question.

Q. Quand je tente d'exécuter une mise à jour de permis après que le purchanse l un nouveau permis le périphérique signale cette erreur : **« Manqué à l'update license sur le capteur. » le « errExpiredLicense-The que le nouveau permis expirent date est plus ancien que le**

permis en cours expirent date. » Comment puis-je résoudre ce problème ?

A. Cette question se produit quand le fichier de licence reçu est non valide. Pour obtenir un fichier de licence valide, ouvrez une session à Cisco.com en tant qu'utilisateur enregistré, et téléchargez le fichier de licence approprié. Une fois que vous obtenez le fichier de licence valide, installez-le sur votre capteur.

Si vous installez le nouveaux fichier de licence et vous recevez toujours une erreur, il pourrait y a une question avec le fichier de licence non valide existant. Afin de résoudre ce problème, terminez-vous ces étapes pour supprimer le fichier de licence non valide existant :

1. Ouvrez une session au compte des services en tapant votre nom d'utilisateur de compte des services.Si vous n'avez pas un compte des services, ouvrez la ligne de commande IPS, écrivez le mode de configuration, et sélectionnez cette commande**password password de service de privilège de *nom de* nom d'utilisateur**

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

2. Une fois que vous ouvrez une session à votre compte des services, sélectionnez la commande du **su** afin d'aller s'enraciner (utilisant le même mot de passe que le compte des services).
3. Supprimez les fichiers dans le répertoire de /usr/cids/idsRoot/shared/.**Remarque:** Ne supprimez pas le fichier host.conf.Sélectionnez la commande de **/usr/cids/idsRoot/shared/ de cd** afin d'aller au répertoire partagé.Sélectionnez la commande **LS** afin de visualiser les fichiers dans le répertoire.Sélectionnez la commande de *file_name de* ***rm*** afin de retirer les fichiers.**Remarque:** Ne supprimez pas le fichier host.conf.
4. Sélectionnez la commande de **reprise de /etc/init.d/cids** de redémarrer le capteur.
5. Installez le nouveau permis.

Une bogue Cisco a été classée pour adresser ce comportement. Le pour en savoir plus, se rapportent à CSCtg76339 (clients enregistrés seulement).

Q. Ce qui fait l'**errorMessage : IpLog 1712041197 a terminé dû tôt pour manquer des traitements de fichier.** moyen **name=ErrLimitExceeded de** message d'erreur ? Comment faire pour résoudre ce problème ?

A. Cette erreur est provoqué par par une quantité excessive de paquets sur se connecter IP. Désactivez la fonctionnalité de journalisation IP afin de résoudre ce problème. Se connecter IP est signifié pour dépanner seulement ; Cisco recommande que vous ne l'activiez pas pour toutes les signatures.

Q. Je reçois cette erreur quand je mets à jour le capteur de s550 à s551 : **Ne peut pas analyser le config en cours pour le « signatureDefinition » composant et l'exemple "sig0".** Comment puis-je résoudre ce problème ?

A. La modification de la signature 23899.0 entraîne cette question. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCtn84552 (clients enregistrés seulement).

Q. Je reçois cette erreur sur le capteur : **Erreur : l'autoUpdate a avec succès sélectionné un**

module du service de localisateur de cisco.com, cependant, le téléchargement de module a manqué : Pour recevoir la réponse de HTTP. Comment puis-je résoudre ce problème ?

A. Vérifiez s'il y a Filtrage URL, filtrage selon le contenu, ou un présent de serveur proxy qui bloque l'autoUpdate de l'événement. Assurez-vous qu'autoUpdate n'est pas bloqué et vérifiez également que les identifiants utilisateurs fournis sont corrects.

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

A. Ce comportement a été adressé par l'ID de bogue Cisco CSCsq50873 (clients enregistrés seulement). C'est une question cosmétique et ne crée pas n'importe quel temps système opérationnel à moins que la quantité excessive de logs étant reçus. Un contournement provisoire est de retirer la configuration associée par NTP sur le capteur. Pour une solution permanente, mise à jour à une version dans laquelle cette bogue est réparée.

Q. Pourquoi le poste de travail IME établit-il les rapports constants aux serveurs gérés en dépit du client étant fermé ?

A. IME fonctionne comme deux services windows et client GUI. Quand le client est fermé, les deux services windows (Cisco IPS Manager Express et MySQL-IME) continuent à exécuter et collecter des événements des capteurs gérés et aux enregistrer dans la base de données mysql locale ; ceci tient compte pour que le rapport historique se produise.

Le client IME devrait ouvrir un abonnement simple SDEE au capteur géré, et réutilise cet abonnement pour l'activité ultérieure de récupération d'événement. La Connectivité constante du poste de travail IME aux capteurs gérés est comportement prévu.

Q. Le module d'AIP SSM peut-il être utilisé comme cible d'ENVERGURE ?

A. No. Le module d'AIP SSM ne peut pas être utilisé car une cible d'ENVERGURE comme il est utilisé pour surveiller seulement le trafic traversant l'interface ASA.

Q. Pourquoi est-ce qu'on observe l'utilisation du CPU élevée après que l'IPS soit mis à jour à l'engine d'E3 ?

A. Avec des mises à jour d'engine d'E3, l'IPS utilise un algorithme différent pour gérer son temps d'inactivité et passe plus d'interrogation de temps pour que les paquets réduisent la latence. Ceci vérifier accru entraîne une augmentation correspondante de l'utilisation du CPU. La manière correcte de mesurer la CPU dans l'E3 est non par l'utilisation du CPU, mais par le **pourcentage de chargement de paquet** qui affiche l'utilisation du processeur correcte.

Q. Pourquoi la rotation de l'état de santés DEL est-elle ROUGE par intermittence sur mon appliance IPS ?

A. Ceci a pu se produire en raison d'un certificat incorrect sur la station distante de maanagement, du logiciel courant tel que CS-MARS, du CSM, de l'IEV, du VMS-IDS/IPSMC, etc. afin de résoudre

ce problème, se terminent ces étapes :

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

Q. Comment l'IPS peut-il être arrêté de retarder le trafic du HTTP tout en traversant ses interfaces ?

A. Configurant le capteur pour fonctionner en mode asymétrique résoudra le problème. Afin de mettre le capteur dans la protection asymétrique de mode, terminez-vous ces étapes :

1. Allez à la **configuration** > aux **stratégies** > aux **stratégies IPS**.
2. **Capteur virtuel de** double clic.
3. Allez **avancer des options**.
4. Sous normalisez le mode, **protection asymétrique** choisie de **mode**.
5. Cliquez sur **OK**.
6. Redémarrez l'unité pour que les modifications les prennent effet.

Informations connexes

- Page de support Cisco Secure de système de prévention des intrusions
- Dépannage d'AIP-SSM
- Notes de terrain relatives aux produits de sécurité (détection y compris d'intrusion de CiscoSecure)
- Support et documentation techniques - Cisco Systems