الأسئلة المتداولة حول IDS 4.0/AIP-SSM/IPS 5.0 والإصدارات الأحدث

المحتويات

المقدمة

يجيب هذا المستند على الأسئلة الأكثر شيوعا (FAQs) المتعلقة بنظام اكتشاف الاقتحام الآمن (IDS) 4.0 من Cisco ووحدة خدمات الأمان والفحص والمنع المتقدم (AIP SSM) ونظام منع الاقتحام (IPS) 5.0 من Cisco والإصدارات الأحدث.

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

IDS 4.0

س. لقد قمت بتثبيت IDS MC و SecMon على خادم جديد والآن أريد إستيراد جميع التكوينات (المستخدم والجهاز وما إلى ذلك) من الخادم القديم إلى الخادم الجديد. كيف أفعل هذا؟

أ. أسهل طريقة للقيام بذلك هي أن تستحضر خادم VMS الجديد الخاص بك، ثم تكتشف أجهزة الاستشعار مع هذا الصندوق الجديد.

ملاحظة: عند إضافة المستشعر، لا تضيفه يدويا. حدد مربع **إعدادات اكتشاف**.

بمجرد اكتشاف المستشعر، قم باستيراده إلى **SecMon**. يتم حفظ جميع التكوينات على المستشعر. إعدادات التوقيع، المرشحات، وهكذا دواليك يجب أن تظهر بعد أن تقوم ببناء خادمك الجديد. تأكد من تحديث IDS MC إلى أحدث التوقيعات.

Q. IDS-4215 يستلم `IdsPackageMgr:` رسالة خطأ أثناء محاولة ترقية قسم إسترداد IDS. ما الذي يجب علي فعله لحل هذه المشكلة؟

أ. هذه قضية تصنيع. تلقى بعض العملاء IDS-4215s مع صورة أساسية سيئة (4.0). أكمل الخطوات التالية.

1. قم بتنزيل صورة قسم الاسترداد (العملاء المسجلون فقط).
2. تطبيق ترقية صورة قسم الاسترداد من خلال CLI (واجهة سطر الأوامر):

```
sensor#configure terminal
/sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH
IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg
```

3. بمجرد تطبيق صورة قسم الاسترداد، تتم إستعادة 4215 إلى قاعدة عادية تعمل بنظام 4.1(1) 4215.

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

س. عند الترقية من حزم مستوى مجموعة sig ذات أرقام 2 إلى 3 أرقام، مثل S100 أو إصدار أحدث، على سبيل المثال، من S99(4)4.1 إلى S100(4)4.1، تفشل وظيفة التحديث التلقائي. كيف يمكنني إصلاح هذا؟

ملاحظة: لا يواجه عملاء Cisco VMS و CLI هذه المشكلة.

سبب المشكلة هو منطق الفرز الذي يتم إستخدامه عند تحليل اسم الملف. هو ترتيب أبجدي رقمي عندما يجب أن يكون رقميا. الحل البديل هو إستخدام واجهة سطر الأوامر (CLI) (أو VMS) للترقية إلى حزم مستوى مجموعة توصيل من 3 أرقام، مثل S100 أو أحدث. بمجرد اكتمال ذلك، يبدأ التحديث التلقائي في العمل مرة أخرى. راجع معرف تصحيح الأخطاء من Cisco CSCef07999 (العملاء المسجلون فقط) للحصول على مزيد من المعلومات.

س. ماذا تعني ▪ ▪. رسالة الخطأ؟

a. in order to حللت هذا إصدار، استعملت تقصير كلمة (cisco) مرتين وبعد ذلك غيرت الكلمة من ال config أسلوب. تتطلب المعرفات إدخال كلمة المرور الافتراضية مرتين.

على سبيل المثال:

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

س. كيف أنا أزيل ال IDSM من مفتاح؟

أ. يجب إزالة الوحدة النمطية فقط بعد تعطيل الطاقة. أكمل الخطوات التالية:

1. من واجهة سطر الأوامر (CLI) الخاصة بالمستشعر، قم بإصدار الأمر **reset powerdown**.
2. بمجرد أن يتم المستشعر إيقاف التشغيل، من واجهة سطر الأوامر (CLI) الخاصة بالمحول، قم بإصدار الأمر **no power enable module (module_number)** ل Cisco IOS أو الأمر **set module power down (module_number)** ل CatOS.
3. اضغط على زر إيقاف التشغيل في الخادم النصلي.
4. قم بتشغيل الهيكل فعليا. عندما يعرض مصباح الحالة لون أخضر أطول، يمكنك إزالة الوحدة النمطية بأمان.

IPS 5.0 والإصدارات الأحدث

س. لقد تجنبت التهيئة لكنني احترت حول كيفية تكوين الحظر على التوقيعات. ما الفرق بين مضيف الحظر واتصال الحظر؟

أ. حظر المضيف لكافة الحزم من عنوان المصدر هذا. حظر الاتصال يحظر فقط اتصال واحد استنادا إلى منفذ/IP للمصدر والوجهة. يعمل ال PIX بطريقة مختلفة قليلا. ل تلقائي ميناء، يرسل المستشعر المصدر ip، غاية ip، مصدر ميناء، وغاية ميناء. يقوم PIX بحظر جميع الحزم التي تنشأ من عنوان IP هذا. يستخدم PIX المعلومات الإضافية لإزالة هذا الاتصال الواحد من جداول الاتصال الخاصة به. إذا لم تتم إزالة الاتصال من جدول الاتصال، فمن الممكن نظريا إذا تمت إزالة كلمة المرور بعد فترة وجيزة من تطبيقها، فقد لا تكون مهلة الاتصال الأصلي قد انتهت بعد. وهذا يسمح للمهاجم بمواصلة الهجوم على الاتصال الأصلي. تضمن عملية إزالة الاتصال من الجدول عدم إمكانية إستخدام الاتصال

الأصلي لمتابعة الهجوم بعد إزالة القطع. لا يمكن للمستشعر تجنب اتصال واحد على PIX لأن PIX لا يدعم إستخدام الأمر shun لتجنب اتصال واحد. يتجنب أمر PIX عنوان المصدر دائما بغض النظر عما إذا كانت معلومات الاتصال الإضافية يتم توفيرها أم لا.

س. ما : . . . تعني رسالة الخطأ؟

أ. يعني هذا الخطأ أن العبارة الافتراضية غير صحيحة أو رسالة خطأ عامة تعني أن البوابة الافتراضية أو IP أو netmask غير صحيحة. يعني الجزء من الرسالة أنه بعد الفشل الأول، تم تطبيق التكوين السابق وفشل أيضا. يصدر المستشعر أمر ifconfig وroute ويفشل واحد أو كلا منهم.

Q. Autoupdate يفشل مع "mainApp[343] Cid/E errSystemError http error response:500". رسالة خطأ. ماذا تعني رسالة الخطأ هذه؟

أ. قد تكون هذه المشكلة ميزة التحديث التلقائي، والتي لا تعمل، لأنها مضبوطة للتنزيل في ساعة زوجية. حاول تعيين التحديث التلقائي على وقت عشوائي، حتى لو كانت إزاحة صغيرة لمدة ثماني دقائق أو ليلية يمكن إصلاح هذه المشكلة.

وبشكل عام، يتم حل المشكلة رسالة الخطأ 500:http خطأ إذا قمت بتغيير وقت الاسترداد إلى حد غير الساعة.

ملاحظة: يفشل IPS في التحديث التلقائي للتوقيعات وعمليات الإرجاع مع رسالة الخطأ هذه:

```
HTTP [1110] name=errSystemError   :AutoUpdate
```

تحقّق من هذه العناصر لحل هذه المشكلة:

- تحقق مما إذا كان هناك جدار حماية يمنع المستشعر من الوصول إلى Cisco.com.
- تحقق مما إذا أصبح التوجيه مشكلة.
- دققت إن NATing يكون شكلت بشكل صحيح على العبارة أداة ل ال تدفق أداة.
- تحقق مما إذا كانت بيانات اعتماد المستخدم صحيحة.
- قم بتغيير وقت بدء التحديث إلى ساعات فردية.

Q. ماذا يعمل ": execUpgradeSoftware: AnalysisEngine . . هل تعني رسالة الخطأ؟

أ. لحل هذه المشكلة، حاول إعادة تحميل المستشعر أو إعادة تصوره.

س. كيف يمكنني حل رسالة الخطأ HTTP DNS - CID/W Warning DNS . DNS HTTP ..."؟

أ. أتمت هذا مهمة in order to حللت هذا إصدار:

- تعطيل الارتباط العمومي.
- إضافة تكوين الوكيل/DNS.

Q. كيف يمكنني حل هذه الأخطاء التي يستلمها IPS للمشاكل الصحية للارتباط العالمي: 23Jan2010 15:50:39.831 38.001 collaborationApp[655] HTTP TLS :X.X.82.127:443 TLS" و"CollaborationApp[459] rep/E :IBRS/1.1/drop/default/1296529950 : IP URI "؟"

a. IPS يعجز أن يحصل إلى الإنترنت بسبب ميناء إصدار، مثلا، جدار حماية في ممر أن لا يتلقى الميناء مناسب مفتوح ل الإنترنت أو هو يستطيع كنت nat إصدار.

بالنسبة إلى الارتباط العمومي الذي يعمل بشكل كامل، يقوم المستشعر أولا بالاتصال من خلال **update-manifses.ironport.com** لمصادقة المستخدم ومن ثم اتصال HTTP لتنزيل تحديثات GC. الملفات التي يقوم المستشعر بتنزيلها من updates.ironport.com) HTTP) هي بيانات السمعة التي يستخدمها الارتباط العالمي. يجب أن يتم حل https update-manifests.ironport.com دائما إلى عنوان X.X.82.127، ولكن يمكن تغيير عنوان IP **http update.ironport.com**، وهذا يعتمد على الإنترنت الذي تصل إليه. لذلك أنت ينبغي فحصت العنوان. إذا تم تمكين تصفية URL، فقم بإضافة إستثناء ل IP لواجهة إدارة IPS في عامل تصفية URL، حتى يمكن ل IPS الاتصال بإنترنت.

يحدث هذا الخطأ عندما يكون هناك تلف في تحديث سابق ل GC:

```
IP   URI   :iBRS/1.1/drop/default/1296529950   :   Collaboration App[459] rep/E
```

يمكن عادة تصحيح هذه المشكلة عن طريق إيقاف تشغيل خدمة GC ثم إعادة تشغيلها مرة أخرى. في IDM، أختر **التكوين > السياسات > الارتباط العالمي > الفحص/السمعة**، وقم بتعيين فحص الارتباط العالمي (و**تصفية السمعة** إذا كان **قيد التشغيل**) على **إيقاف التشغيل**، وقم بتطبيق التغييرات، والانتظار لمدة 10 دقائق، وتشغيل الميزات، والمراقبة.

Q. **. تم إستلام .DNS HTTP .OpenConnection: Caught IpAddrException BadAddrString : رسالة خطأ في الفئة "فشل تحديث السمعة". كيف يمكنني حل هذه المشكلة؟**

ألف - التحقق من هذه العناصر:

- يجب أن يكون لديك ترخيص IPS صالح للسماح لميزات الارتباط العام بالعمل.
- يجب أن يكون لديك خادم وكيل HTTP أو خادم DNS تم تكوينه للسماح لميزات الارتباط العام بالعمل.
- نظرا لأن تحديثات الارتباط العام تحدث من خلال واجهة إدارة المستشعر، فيجب أن تسمح جدران الحماية بحركة مرور TCP 443/80 و UDP 53.
- تأكد من أن جهاز الاستشعار يدعم ميزات الارتباط العام. إذا لم تكن ترغب في هذا، فقم بتعطيل ميزة التعاون العام من IDM:انتقل إلى التكوين > السياسات > الارتباط العالمي>**الفحص/السمعة**، وقم بتعيين فحص الارتباط العالمي (وتصفية السمعة إذا كان **قيد التشغيل**) على إيقاف التشغيل.

Q. كيف يمكنني حل " OpenConnection: Caught IpAddrExceptionBadAddrString :" الخطأ الذي يستلمه IPS لمشكلة صحة الارتباط العالمي؟

أ. إذا كنت تستخدم الارتباط العالمي (GC) فتأكد من عمل تحليل الاسم، على سبيل المثال، DNS يمكن الوصول إليه. تحقق أيضا من وجود منفذ 53 محظور على جدار الحماية. وإلا، يمكنك إيقاف تشغيل ميزة GC إذا كنت ترغب في التخلص من هذه الرسالة.

س. كيف يمكنني حل برسالة خطأ MySQL التي أتلقاها عند تشغيل IME من المستعرض؟

أ. تحدث هذه المشكلة عادة عندما يحاول العميل تشغيل IME على أنظمة تشغيل غير مدعومة، مثل Windows 7.

س. كيف يمكنني حل : IDM .nsmc-c1: Cisco Systems Inc-88 : JNLP JAR ." " خطأ x.x.x.x.x:443 الذي IDM أثناء تشغيل التطبيق؟

أ. امسح التخزين المؤقت للمستعرض من أجل حل هذه المشكلة.

Q. هل الوضع غير المتماثل على IPS قابل للتكوين إذا كنت تستخدم واجهة المستخدم الرسومية؟

أ. في الإصدار 6.0، الوضع غير المتماثل في IPS القابل للتكوين باستخدام CLI فقط وغير متوفر على واجهة المستخدم الرسومية (GUI). غير أن هذه الميزة، في الإصدار 6.1، متاحة أيضا في واجهة المستخدم الرسومية (GUI).

س. كيف يمكنني حل مشكلة زمن الوصول باستخدام مستشعر IPS؟

أ. لحل هذه المشكلة، قم بتمكين معالجة الوضع غير المتماثل للسماح للمستشعر بمزامنة الحالة مع التدفق والمحافظة على فحص تلك المحركات التي لا تتطلب كلا الاتجاهين. أستخدم هذا التكوين:

```
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
```

تحدث مشكلة زمن الوصول عندما يكون إجراء الرفض مضمنا وحزمة الرفض ممكنة لكل توقيع في VS0. سيؤدي تمكين جميع التوقيعات إلى زمن وصول حيث يقوم IPS بفحص كل حزمة تمر من خلاله. من الجيد تمكين التوقيع المحدد المطلوب فقط وفقا لتدفق حركة مرور الشبكة لحل مشكلة زمن الوصول.

س. هل يساعد AIP-SSM في حظر Skype؟

أ. يتعذر على PIX/ASA حظر حركة مرور Skype. ويملك Skype القدرة على التفاوض بشأن المنافذ الديناميكية واستخدام حركة مرور مشفرة. فمع حركة المرور المشفرة، من المستحيل فعليا اكتشافها حيث لا توجد أنماط للبحث عنها.

يمكنك أخيرا إستخدام Cisco IPS (نظام منع الاقتحام)/AIP-SSM. يحتوي على بعض التوقيعات التي يمكنها اكتشاف عميل Windows Skype الذي يتصل بخادم Skype لمزامنة إصداره. يتم ذلك عادة عند بدء اتصال العميل. عندما يقوم المستشعر بتشغيل اتصال Skype الأولي، يمكنك العثور على الشخص الذي يستخدم الخدمة، ومنع كافة الاتصالات التي تم بدؤها من عنوان IP الخاص به.

س. لماذا واجهة الاستشعار أو غالبا ما تنتقل إلى الحالة السفلى في IPS؟

أ. أثناء تحديث التوقيع وإعادة التكوينات، يتوقف SensorApp عن معالجة الحزم أثناء معالجة التوقيعات الجديدة في التحديث. يقوم برنامج تشغيل الشبكة باكتشاف إيقاف SensorApp وسحب أي حزم جديدة من المخزن المؤقت. ولهذا فإن برنامج تشغيل الشبكة يقوم بأمور مختلفة، والتي تعتمد على نموذج التهيئة والمستشعر:

الواجهة المختلطة — تعمل على تقليل الارتباط على الواجهات، ثم تعمل على إعادة الاتصال مرة أخرى بمجرد أن يبدأ SensorApp في المراقبة مرة أخرى.

الواجهة الداخلية أو زوج شبكات VLAN الداخلي— يعتمد على إعداد الالتفاف:

- **تجاوز تلقائي**— يحافظ السائق على الرابط ويبدأ بتمرير الحزم من دون تحليل. ثم يعود مرة أخرى لإرسال الحزم من خلال SensorApp بمجرد أن يبدأ SensorApp في المراقبة مرة أخرى.
- **إيقاف التشغيل الالتفافي** — يقوم برنامج التشغيل بإنزال الارتباط على الواجهات، وهو نفس الشيء كما هو الحال في وضع الاختلاط، ويقوم بإعادتها إلى أعلى بمجرد بدء SensorApp في المراقبة مرة أخرى.

لذلك، إذا لم يقوم تطبيق المستشعر بسحب الحزم من المخزن المؤقت، والذي قد يحدث بسبب عدم وجود واجهة تم تكوينها لمعالجة الحزم، فيمكن حينئذ لبرنامج التشغيل وضع الواجهة في حالة .

وتشاهد هذه السجلات عند رفرفة واجهة الاستشعار:

```
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
```

س. هل يحتفظ مستشعر نظام منع التسلل (IPS) أو المعرفات بمحفوظات لكلمة المرور؟

أ. لا، لا يحتفظ المستشعر بمحفوظات كلمة المرور. لا يمكن عرض كلمات المرور في أي وقت.

س. هل يدعم مستشعر نظام منع التسلل (IPS) والمعرفات خادم syslog لإرسال السجلات؟

أ. لا.

س. ما هو الحد الأقصى لتخزين الأحداث في IPS؟

أ. يخزن الحدث المحلي للمستشعر 30 ميغابايت فقط ويبدأ في الكتابة فوق نفسه بمجرد الوصول إلى حد 30 ميغابايت. هذا الحد غير قابل للتكوين.

س. كيف اكتب توقيع لاكتشاف ملف FOTO[a-z]\.zip في أي بريد إلكتروني وارد أو صادر؟

أ. أستخدم String.TCP in order to كتبت توقيع أن يكشف المرفق. ابحث عن شيء مشابه لهذا:

```
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
```

س. كيف يمكنك تكوين مهلة عميل FTP؟

a. أصدرت هذا أمر:

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

س. كيف يمكنك تحويل وقت البدء ووقت الانتهاء في حالة iplog إلى تنسيق يمكن قراءته؟

ألف - يمثل هذا الناتج تمثيلا عشري للوقت الحالي منذ فترة عمل نظام يونيكس. أستخدم حاسبة UNIX ePOC مثل تلك الموجودة في موقع حاسبة تاريخ/وقت UNIX . أدخل أول 10 أرقام لأن هذه الآلة الحاسبة محبة للثواني فقط، وتخزن IDS نانو ثواني. هذا يعني أن آخر تسعة أرقام يتم نزعها. من وقت البداية في هذا المخرج، `1084798479 = mon 17 12:54:39 2004 (GMT)` هو ما تستلمه.

من ال CLI، دخلت iplog-status in order to إستلمت هذا إنتاج:

```
"
                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
"
```

س. "IOeXception : "java.security.cert.CertificateExpiredException.تظهر رسالة الخطأ. فكيف يمكن حل ذلك؟

أ. لحل رسالة الخطأ هذه، قم بتسجيل الدخول إلى AIP-SSM وأصدر الأمر tls generate-key في وضع EXEC ذي الامتيازات كما هو موضح في هذا المثال:

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

ملاحظة: هذا الحل لاستخدام الأمر tls generate-key يحل أيضا مسألة عدم قدرة AIP-SSM على الاتصال ب IME.

س. "IOeXeption: :. IME IME . تظهر رسالة الخطأ أثناء إضافة IPS في IME. كيف يمكن حل هذه المشكلة؟

أ. لحل رسالة الخطأ هذه، أختر **لوحة التحكم > أدوات الإدارة > الخدمات** وأعد تشغيل خدمات IME.

س. [- IOexCeption] / يتم إستلام رسالة خطأ عند إضافة مستشعر IPS إلى IME. كيف يمكن حل هذه المشكلة؟

ألف - يشير ذلك إلى انقطاع الاتصال بين نظام IME ومستشعر نظام منع الاختراق. تأكد من عدم وجود برنامج يمنع SDEE.

س. " IME: ( ) . تظهر رسالة خطأ. كيف يمكن حل هذه المشكلة؟

أ. لحل رسالة الخطأ هذه، تحقق من إستخدام عنوان IP الصحيح عند إضافة IPS في IME وكذلك التحقق من أي جدار حماية برنامج قيد التشغيل على كمبيوتر IME، الذي يمكنه حظر الاتصال.

س. هل يمكن لمستشعر نظام منع التسلل (IPS) أو المعرفات إرسال تنبيهات عبر البريد الإلكتروني؟

أ. لا يملك مستشعر IDS القدرة على إرسال تنبيهات البريد الإلكتروني بمفرده. يتمتع "مراقب الأمان" عند إستخدامه مع "معرفات الهوية" بالقدرة على إرسال إعلامات البريد الإلكتروني عند تشغيل "قاعدة الأحداث" بواسطة المستشعر.

ارجع إلى تكوين إعلامات البريد الإلكتروني للحصول على مزيد من المعلومات حول كيفية تكوين إعلامات البريد الإلكتروني مع مراقبة الأمان.

يمكن تكوين IME) Cisco IPS Manager Express) لإرسال رسالة إعلام البريد الإلكتروني (تنبيهات) عند تشغيل قواعد الأحداث بواسطة أجهزة إستشعار Cisco IPS. ارجع إلى IPS 6.x والإصدارات الأحدث: إعلامات البريد الإلكتروني باستخدام مثال تكوين IME للحصول على مزيد من المعلومات.

س. : .(mainApp (getVersion . تظهر رسالة خطأ عند محاولة الاتصال بالمستشعر الخاص بي.

كيف يمكن حل هذه المشكلة؟

ألف - إعادة تشغيل المستشعر لحل هذه المشكلة.

س - : : . . تظهر رسالة الخطأ وهي توليف التوقيع على جهاز الاستشعار الخاص بي. كيف يمكن حل هذه المشكلة؟

أ. قم بتقاعد التوقيعات غير المستخدمة لحل هذه المشكلة، كما يجب تقليل عدد توقيعات العملاء ذات الأنظمة. كما لا يوصى باستخدام * و+ الحروف الأولية في الأنظمة.

q. لماذا تحدث مشكلات زمن الوصول على أجهزة إستشعار نظام منع التسلل (IPS) من Cisco؟ كيف يمكن حل هذه المشكلة؟

أ. يمكن أن تحدث مشكلة زمن الوصول بسبب التوجيه المتزامن. حاولت أن يعجز التوقيع 1330 in order to حللت هذا إصدار.

س. هل من الممكن تعطيل SSHv1 وترك فقط SSHv2 الذي تم تمكينه على أجهزة إستشعار نظام منع التسلل (IPS) من Cisco؟

أ. من غير الممكن الآن تعطيل SSHv1 وترك SSHv2 فقط ممكنا. يتم تمكين كلا من SSHv1 و SSHv2 معا ولا يمكن تعطيلهما بشكل فردي.

س. : = 115000 110443 usr/cids/idsRoot/var/ . تظهر الرسالة عندما أقوم بترقية المستشعر إلى الإصدار 4.1(5). كيف يمكن حل هذه المشكلة؟

أ. تحدث رسالة الخطأ هذه بسبب عدم كفاية الذاكرة في المستشعر.

أتمت هذا مهمة in order to حللت هذا إصدار:

1. تسجيل الدخول إلى حساب الخدمة ليصبح الجذر
2. إزالة الأدلة التالية كما هو موضح أدناه:

```
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. حاول الآن ترقية المستشعر. راجع معرف تصحيح الأخطاء من CSCsb81288 Cisco (العملاء المسجلون فقط) للحصول على مزيد من المعلومات.

Q. احصل على مستوى/EMainApp[396] - () - رسالة الخطأ -1 في ASA الخاص بتسجيل الدخول. كيف يمكن حل هذا الخطأ؟

أ. يشير رسالة الخطأ mainApp[396] Cplane/E - () -1 إلى أن خادم ويب لا يمكنه قراءة الملف، وقد فشل البرنامج "قبول()"، مما ينتج واصفات الملفات عند وجود إتصالات TLS. ولكن هذا الملف ليس ضروريا للسلوك العادي. انه غير مؤذ.

Q. كيف يمكنني حل TLS/W Transport WebSession::sessionTask TLS Connection Exception: Handshake Incomplete Error Message؟

أ. تشير رسالة الخطأ هذه إلى أن الشهادة لم تعد صالحة على الوحدة النمطية. أتمت هذا steps in order to حللت

الإصدار:

1. إعادة إنشاء الشهادة من واجهة سطر الأوامر:سجل الدخول إلى سطر أوامر المستشعر.قم بإصدار الأمر **tls generate**، واضغط **enter**. لاحظ بصمات الأصابع المعروضة.
2. اسحب الشهادة الجديدة إلى IME:افتح IME وحدد اسم المستشعر في القائمة على الصفحة الرئيسية.انقر بزر الماوس الأيمن فوق أداة الاستشعار، ثم انقر فوق **تحرير**.عندما تصل إلى شاشة تحرير الجهاز، انقر فوق **موافق**. تجاوز أي تحذير حول عدم القدرة على إسترداد وقت المستشعر.ستتم مطالبتك باستخدام شهادة الأمان الجديدة (الشهادة التي قمت بتوليدها للتو). تحقق للتأكد من مطابقة بصمات الأصابع، وانقر **نعم**.بعد عدة ثوان، يجب أن يظهر المستشعر "متصل" في "حالة الحدث" مرة أخرى.

Q. عندما أحاول تسجيل الدخول إلى IPS، أستلم رسالة الخطأ هذه: `errSystemError-ct-sensorAPP.450` . كيف يمكنني حل هذا الخطأ؟

a. لحل هذا الخطأ، أستخدم الأمر **reset** لإعادة تمهيد IPS.

q. يختلف الوقت على AIP-SSM عن الوقت على جهاز الأمان القابل للتكيف (ASA) من Cisco. كيف يمكن حل هذه المشكلة؟

أ. لحل هذه المشكلة، أستخدم خادم NTP لمزامنة الوقت على جهاز الأمان القابل للتكيف (ASA) من Cisco وبروتوكول AIP-SSM.

راجع تكوين بروتوكول وقت الشبكة (NTP) على أجهزة إستشعار IPS للحصول على مزيد من المعلومات.

س - كيف يمكنني تطبيق أجهزة إستشعار افتراضية متعددة على AIP-SSM؟

ألف - لا يمكن تطبيق أجهزة الاستشعار الظاهرية على AIP-SSM لكل واجهة لأن AIP-SSM لديها واجهة واحدة فقط. عند إنشاء أجهزة إستشعار افتراضية متعددة، يجب تعيين هذه الواجهة لمستشعر ظاهري واحد فقط. لا تحتاج إلى تعيين واجهة لأجهزة الاستشعار الظاهرية الأخرى.

بعد إنشاء أجهزة إستشعار افتراضية، يجب تعيينها إلى سياق أمان في جهاز الأمان القابل للتكيف (ASA) باستخدام الأمر **distribute-ips**. يمكنك تعيين العديد من سياقات الأمان للعديد من أجهزة الاستشعار الظاهرية. راجع قسم *تكوين AIP-SSM* في تكوين AIP-للحصول على مزيد من المعلومات حول تعيين أجهزة الاستشعار الظاهرية لسياقات جهاز الأمان القابل للتكيف.

س - ما هو الحد الأقصى لعدد أجهزة الاستشعار الافتراضية التي تدعمها AIP-SSM؟

ألف - يمكن دعم عدد أقصاه أربعة أجهزة إستشعار افتراضية.

س. إذا كنت تستخدم SSH أو IDM لتسجيل الدخول إلى IPS، فهل من الممكن تكوين IPS 4240/IDSM/IDSM2 للتحقق من المستخدمين الإداريين مقابل خادم RADIUS/TACACS+؟

أ. لا يمكن إستخدام خادم TACACS+ ولكن RADIUS مدعوم من إصدار IPS 7.0.(4)E4. راجع أقسام *المعلومات الجديدة والمغيرة* والقيود من ملاحظات الإصدار الخاصة بنظام Cisco لمنع الاقتحام 7.0(4)E4 للحصول على مزيد من المعلومات. راجع أيضا IPS 7.x: مصادقة تسجيل دخول المستخدم باستخدام ACS 5.x كمثال تكوين خادم RADIUS للحصول على نموذج التكوين.

س. ما هو تأثير الترخيص الذي انتهت صلاحيته على وظيفة نظام منع التسلل (IPS)؟

ألف - الأثر الوحيد للترخيص المنتهي الصلاحية على المستشعر هو أنه يوقف تحديثات التوقيع.

س. هل تؤثر تحديثات توقيع IPS على الخدمات أو اتصال الشبكة؟

أ. لا. لا تؤثر تحديثات توقيع IPS على الخدمات أو اتصال الشبكة.

س. ما هو محدد موقع المعلومات (URL) الذي أحتاج إلى إدخاله لكي يتم تحديث الوحدة النمطية ل IPS تلقائيا باستخدام أحدث التوقيعات؟

أ. الرابط المطلوب للسماح لوحدة IPS بالتحديث تلقائيا مع أحدث توقيع هو: https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl.

يجب عليك إستخدام معرف مستخدم Cisco وكلمة المرور الخاصين بك لإكمال تحديث وحدة IPS النمطية.

ملاحظة: لا يتم دعم التحديثات التلقائية من Cisco.com في مسار الرمز x.6. يجب تنزيل ملفات التوقيع يدويا وتطبيقها على المستشعر. هناك وظيفة تحديث تلقائي في كود x.6، على أي حال، هذا ممكن فقط من خادم ملف محلي حيث يجب تنزيل ملفات التوقيع يدويا أيضا.

س. هل مستشعر IPS قابل للتعرض لحادث إختطاف جلسة إعادة توجيه المنفذ X11 ؟

أ. لا. ليست معرضة لهذه الأسباب:

- لا يحتوي المستشعر على مكتبات X11. لذلك ليس هناك جلسات للخطف.
- لم يتم تمكين إعادة توجيه المنفذ X11 في تكوين SSH.
- لم يتم تحويل IPv6 إلى عنصر kernel الخاص بالمستشعر. وهذا أمر مطلوب من أجل إستغلال حالة الضعف.

س - لماذا لا تظهر AIP-SSM أي سجلات عندما يظهر ASA الكثير من سجلات التحذير والهجوم؟

أ. يحدث هذا لأنه عندما يقوم ASA بحجب شيء ما، لا يتم تمريره إلى IPS لإجراء فحص متكرر. لذلك، لا يمكنك رؤية السجلات المكررة على ASA و IPS.

س. بعد أن يقوم المستخدم بنشر مجموعة التوقيع S518، تظهر رسالة الخطأ `invalidValue:Editng string-xl-tcp sig xxxx` ". لماذا؟

أ. هذه هي رسالة الخطأ الكاملة:

```
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
```

يقع هذا إصدار لأن ال string-xl-tcp أو string-tcp-xl محرك لا يساند على الجهاز. لمزيد من التفاصيل، ارجع إلى ملاحظات إصدار محرك IPS E4.

س. عندما أقوم تلقائيا بتحديث التوقيعات على ASA-SSM-10 باستخدام ميزة التحديث التلقائي، أستلم رسالة الخطأ هذه: `true=` كيف يستطيع أنا حللت هذا إصدار؟

أ. يعرض هذا الإخراج رسالة الخطأ الكاملة:

```
: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
```

تم إنشاء هذا الخطأ ولا يتم تحديث التوقيعات تلقائيا لأن تحديثات تعريف التوقيع بعد S479 تتطلب محرك E4. لحل هذه المشكلة، يلزمك ترقية المستشعر يدويا إلى E4(2)7.0.

ملاحظة: يتعذر على المستشعر ترقية نفسه تلقائيا إلى E4 لأنه يتطلب 7.0(2) وإعادة تشغيل المستشعر.

س. ميزة التحديث التلقائي على IPS 5.0 للوحدة النمطية NDS لا تعمل. كيف يستطيع أنا حللت هذا إصدار؟

أ. يعرض هذا الإخراج رسالة الخطأ الكاملة:

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

تحدث هذه المشكلة بسبب نمط سرد دليل غير صحيح مع خادم FTP. لحل هذه المشكلة، قم بالتبديل إلى قوائم دليل نمط UNIX من قوائم دليل أنماط MS-DOS الموجودة.

لتعديل إعدادات سرد الدليل، حدد **ابدأ > ملفات البرنامج > أدوات إدارية** لفتح إدارة خدمات الإنترنت. ثم انتقل إلى علامة التبويب الدليل الرئيسي وقم بتغيير نمط سرد الدليل من MS-DOS إلى UNIX.

q. يتلقى IPS-4255 المستشعرApp يفشل في TcpRootNode::ExpiredNow() خطأ رسالة أثناء ترقية. كيف يمكنني حل هذه المشكلة؟

a. يرجع هذا إصدار إلى فشل محرك التحليل وعالجت في cisco بق CSCtb39179 id (بسجل زبون فقط). قم بترقية المستشعر إلى الإصدار E4(4)7.0 من أجل إصلاح هذه المشكلة.

س. عند محاولة إجراء تحديث ترخيص بعد إجراء ترخيص جديد، يقوم الجهاز بالإعلام عن هذا الخطأ: " ." errExpiredLicense" - ." كيف يستطيع أنا حللت هذا إصدار؟

أ. تحدث هذه المشكلة عندما يكون ملف الترخيص المستلم غير صالح. للحصول على ملف ترخيص صالح، قم بتسجيل الدخول إلى موقع Cisco.com كمستخدم مسجل، وقم بتنزيل ملف الترخيص المناسب. بمجرد حصولك على ملف الترخيص الصحيح، قم بتثبيته على جهاز الاستشعار الخاص بك.

إذا قمت بتثبيت ملف الترخيص الجديد ولا تزال تتلقى خطأ، فقد يكون هناك مشكلة في ملف الترخيص غير الصالح الموجود. لحل هذه المشكلة، أكمل الخطوات التالية لحذف ملف الترخيص غير الصالح الموجود:

1. سجل الدخول إلى حساب الخدمة بكتابة اسم مستخدم حساب الخدمة الخاص بك.إذا لم يكن لديك حساب خدمة، فافتح سطر الأوامر IPS، وأدخل وضع التكوين، وأدخل هذا الأمر*كلمة مرور* ***خدمة امتياز*** *اسم المستخدم*

```
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. بمجرد تسجيل الدخول إلى حساب الخدمة الخاص بك، أدخل الأمر **su** للانتقال إلى الجذر (باستخدام نفس كلمة المرور الخاصة بحساب الخدمة).
3. احذف الملفات الموجودة في الدليل /usr/cids/idsRoot/shared/.**ملاحظة:** لا تقم بحذف ملف host.conf.أدخل الأمر **cd /usr/cids/idsRoot/shared/**للانتقال إلى الدليل المشترك.أدخل الأمر **ls** لعرض الملفات في الدليل.أدخل الأمر **rm** *file_name* لإزالة الملفات.**ملاحظة:** لا تقم بحذف ملف host.conf.
4. أدخل الأمر **etc/init.d/cids restart/** لإعادة تشغيل المستشعر.
5. قم بتثبيت الترخيص الجديد.

تم تصنيف خطأ Cisco لمعالجة هذا السلوك. أحلت ل كثير معلومة، CSCtg76339 (يسجل زبون فقط).

س. ماذا : IpLog 1712041197 . name=ErrLimitExceeded رسالة الخطأ؟ كيف يمكنني حل هذه المشكلة؟

أ. يحدث هذا الخطأ بسبب الكمية الزائدة من الحزم على تسجيل IP. قم بتعطيل ميزة تسجيل IP لحل هذه المشكلة. يتم قصد تسجيل IP لاستكشاف الأخطاء وإصلاحها فقط؛ توصي Cisco بعدم تمكينه لجميع التوقيعات.

س. لقد تلقيت هذا الخطأ عندما أقوم بتحديث المستشعر من s550 إلى s551: "sig0" "signatureDefinition". كيف يستطيع أنا حللت هذا إصدار؟

ألف- سبب هذه المسألة هو تعديل التوقيع 23899.0. راجع معرف تصحيح الأخطاء من CSCtn84552 (Cisco العملاء المسجلون فقط) للحصول على مزيد من المعلومات.

Q. لقد تلقيت هذا الخطأ على المستشعر: : AutoUpdate cisco.com : HTTP. كيف يستطيع أنا حللت هذا إصدار؟

أ. تحقق مما إذا كانت هناك تصفية URL أو تصفية محتوى أو خادم وكيل يمنع حدوث AutoUpdate. تأكد من عدم منع AutoUpdate وتحقق أيضا من صحة بيانات اعتماد المستخدم المقدمة.

Q. أنا أستلم رسالة خطأ XML هذه على مستشعر IPS الذي يعمل بالإصدار E4:(3)6.2 :ErrorMessage IPS XML ( ). XML () '*'. كيف يستطيع أنا حللت هذا إصدار؟

أ. تمت معالجة هذا السلوك بواسطة معرف تصحيح الأخطاء من CSCsq50873 (Cisco العملاء المسجلون فقط). وهذه مسألة تجميلية ولا تنشئ أية تكاليف تشغيلية باستثناء الكمية الزائدة من السجلات التي يتم إستلامها. الحل البديل المؤقت هو إزالة التكوين المرتبط ب NTP على المستشعر. للحصول على حل دائم، قم بالترقية إلى إصدار يتم فيه إصلاح هذا الخطأ.

س. لماذا تقوم محطة عمل IME بإجراء إتصالات مستمرة بالخوادم المدارة على الرغم من إغلاق العميل؟

يعمل نظام المعلومات الإدارية المتكامل كخدمتين من خدمات Windows وعميل واجهة المستخدم الرسومية. عند إغلاق العميل، تستمر خدمتا Windows (Cisco IPS Manager Express و MySQL-IME) في تشغيل الأحداث وتجميعها من أجهزة الاستشعار المدارة وتخزينها في قاعدة بيانات MySQL المحلية، وهذا يسمح بظهور تقارير تاريخية.

يجب على عميل IME فتح اشتراك SDEE واحد للمستشعر المدار وإعادة إستخدام هذا الاشتراك لنشاط إسترداد الحدث اللاحق. ومن المتوقع أن يحدث اتصال دائم من محطة العمل IME بأجهزة الاستشعار المدارة.

س. يستطيع AIP-SSM استعملت وحدة نمطية كفسحة بين دعامتين غاية؟

أ. لا يمكن إستخدام وحدة AIP-SSM النمطية كفسحة بين دعامتين هدف حيث أنها تستخدم فقط لمراقبة حركة المرور المتدفقة عبر واجهة ASA.

س. لماذا تتم ملاحظة إستخدام عال لوحدة المعالجة المركزية بعد ترقية IPS إلى محرك E3؟

أ. باستخدام تحديثات محرك E3، يستخدم نظام منع التسلل (IPS) خوارزمية مختلفة لإدارة وقت الخمول الخاص به وينفق المزيد من الوقت في البحث عن الحزم للحد من زمن الوصول. تؤدي هذه الزيادة في الفحص إلى حدوث زيادة مقابلة في إستخدام وحدة المعالجة المركزية. لا يتم تحديد الطريقة الصحيحة لقياس وحدة المعالجة المركزية (CPU) في E3 بواسطة إستخدام وحدة المعالجة المركزية (CPU)، ولكن بواسطة **النسبة المئوية لتحميل الحزمة** التي تظهر إستخدام وحدة المعالجة المركزية الصحيح.

س. لماذا تحول مؤشر LED الخاص بالحالة الصحية إلى الأحمر بشكل متقطع على جهاز الآي بي إس؟

أ. قد يحدث ذلك بسبب وجود شهادة غير صحيحة في محطة الإدارة البعيدة، أو بسبب تشغيل برامج مثل CS-MARS و CSM و IEV و VMS-IDS/IPSMC، إلخ. لحل هذه المشكلة، أكمل الخطوات التالية:

1. تطبيق شهادة TLS الخاصة بالمستشعر على محطة الإدارة عن بعد.
2. قم بتكوين خادم DNS صالح.

س. كيف يمكن إيقاف IPS من تأخير حركة مرور HTTP أثناء عبور واجهات HTTP؟

أ. تكوين المستشعر للعمل في الوضع غير المتماثل سيحل المشكلة. لوضع المستشعر في حماية الوضع غير المتماثل، أكمل الخطوات التالية:

1. انتقل إلى **التكوين** > **السياسات** > **سياسات IPS**.
2. انقر نقرا مزدوجا فوق **المستشعر الظاهري**.
3. انتقل إلى **الخيارات المتقدمة**.
4. تحت وضع التطبيع، حدد **حماية الوضع غير المتماثل**.
5. وانقر فوق **OK**.
6. أعد تمهيد الوحدة لكي تسري التغييرات.

معلومات ذات صلة

- صفحة دعم نظام منع التسلل الآمن من Cisco
- أستكشاف أخطاء AIP-SSM وإصلاحها
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك اكتشاف إقتحام CiscoSecure)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).