IDS 4.0/AIP-SSM/IPS 5.0 y posterior FAQ

Contenido

Introducción

Este documento contesta lo más frecuentemente a las preguntas hechas (FAQ) relacionadas con el Cisco Secure Intrusion Detection System (IDS) 4.0, examen avanzado y (IPS) 5.0 del módulo (AIP SS), y del Cisco Intrusion Prevention System de Servicios de seguridad de la prevención y posterior.

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

IDS 4.0

Q. He instalado IDS MC y SecMon sobre un nuevo servidor y ahora quiero al import all las configuraciones (usuario, dispositivo, y así sucesivamente) del servidor viejo al nuevo. ¿Cómo hago esto?

A. La manera más fácil de realizar esto es criar a su nuevo servidor VMS, y después descubre los sensores con este nuevo cuadro.

Nota: Cuando usted agrega el sensor, no lo agregue manualmente. Marque el cuadro de las **configuraciones del descubrimiento**.

Una vez que se descubre el sensor, impórtelo en el **SecMon**. Todas las configuraciones se guardan en el sensor. Las configuraciones de la firma, los filtros, y así sucesivamente deben parecer después de que usted construya su nuevo servidor. Aseegurese le la actualización IDS MC a las últimas firmas.

Q. El IDS-4215 recibe el `idsPackageMgr: argumento no válido` mensaje de error del mientras que intenta actualizar la división de la recuperación IDS. ¿Qué necesito hacer para resolver este problema?

A. Esto es un problema de fabricación. Algunos clientes recibieron los IDS-4215 con una mala imagen base (4.0). Complete estos pasos.

1. Descargue la imagen de la partición de recuperación (clientes registrados solamente).

2. Aplique la actualización de la imagen de la partición de recuperación con el 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. Una vez que la imagen de la partición de recuperación es aplicada, los 4215 se restablece a una base 4215 de la ejecución normal 4.1(1). `sensor(config)#recover application-partition`

Q. Cuando actualizo de un 2-digit a los sig 3-digit nivele los paquetes, tales como S100 o más adelante, por ejemplo, 4.1(4)S99 a 4.1(4)S100, las funciones del automóvil Update Button falla. ¿Cómo resuelvo este problema?

Nota: Cisco VMS y clientes de CLI no experimenta este problema.

La causa del problema es la lógica de clasificación se utiliza que cuando se analiza el nombre de fichero. Es una clase alfanumérica cuando debe ser numérico. La solución alternativa es utilizar el CLI (o VMS) para actualizar a los paquetes del nivel de los sig 3-digit, tales como S100 o más adelante. Una vez que se completa esto, el automóvil Update Button comienza a funcionar otra vez. Refiera al Id. de bug Cisco CSCef07999 (clientes registrados solamente) para más información.

Q. Qué hace **"el error de la manipulación del token de autenticación".** ¿medio del mensaje de error?

A. Para solucionar este problema, utilice la contraseña predeterminada (Cisco) dos veces y después cambie la contraseña del modo de configuración. El IDS requiere la contraseña predeterminada ser ingresado dos veces.

Por ejemplo:

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

Q. ¿Cómo quito el IDSM del Switch?

A. El módulo debe ser quitado solamente después que usted inhabilita el poder. Complete estos pasos:

1. Del sensor CLI, publique el comando del **powerdown de la restauración**.
2. Una vez que el sensor completa apague, del Switch CLI, publican cualquiera que el **ningún poder habilita el** comando del **módulo (module_number)** para el Cisco IOS o **set module power down el** comando **(del module_number)** para CatOS.
3. Presione el botón del apagar en la cuchilla.
4. Accione físicamente abajo el chasis. Cuando el indicador luminoso de estado visualiza un verde más largo, usted puede quitar el módulo de manera segura.

IPS 5.0 y posterior

Q. Hago evitar configurar pero me confunden sobre cómo configurar el bloqueo en las firmas. ¿Cuál es la diferencia entre el host del bloque y la conexión del bloque?

A. El host del bloque bloquea todos los paquetes de esa dirección de origen. La conexión del bloque bloquea solamente la una conexión basada en la fuente y el destino IP/port. El PIX trabaja de una manera levemente diversa. Para automático evita, el sensor envía el IP de la fuente, el IP de destino, el puerto de origen, y el puerto destino. El PIX bloquea todos los paquetes que originen de esa dirección IP. La información adicional es utilizada por el PIX para quitar esa una conexión de sus tablas de conexiones. Si la conexión no se ha quitado de la tabla de conexiones, después es teóricamente posible que si se quita el evitar poco después de que es aplicado, después la conexión original no pudo haber medido el tiempo hacia fuera todavía. Esto permite que el atacante continúe el ataque en la conexión original. El retiro de la conexión de la tabla se asegura de que la conexión original no se pueda utilizar para continuar el ataque después de que se quite el evitar. El sensor no puede evitar una sola conexión en el PIX porque el PIX no soporta el uso del **comando shun** para evitar una sola conexión. **El comando shun** PIX evita siempre a la dirección de origen sin importar independientemente de si la información de conexión adicional está proporcionada.

Q. Qué hace el **"error: No podía recomenzar los servicios de red. El error fatal ha ocurrido. El nodo SE DEBE reiniciar para habilitar alarmar".** ¿medio del mensaje de error?

A. Este error significa que su default gateway es incorrecto o un mensaje de error genérico que significa que el IP, el netmask, o el default gateway son incorrectos. La parte de `fatal el` mensaje significa que después del primer error, la configuración previa era aplicada y también fallada. Sensor emite ifconfig y los **comandos route** y uno o ambos ellos fallan.

Q. Autoupdate falla con el **error el response:500" HTTP del errSystemError "mainApp[343] Cid/E. .** ¿Qué este mensaje de error significa?

A. Este problema pudo ser la característica auto de la actualización, que no trabaja, porque se fija para descargar en incluso una hora. Intente fijar la actualización auto a un tiempo aleatorio; incluso un pequeño desplazamiento de ocho o los minutos de la noche puede reparar este problema.

El problema se resuelve generalmente y el `error: respuesta de error HTTP:` se vean `500 que` es el mensaje de error si usted cambia el tiempo de extracción a un límite NON-por hora.

Nota: El IPS falla el automóvil Update Button de las firmas y de las devoluciones con este mensaje de error:

```
Excepción del AutoUpdate: Name=errSystemError fallado conexión HTTP [1,110]
```

Verifique estos elementos para resolver este problema:

- Verifique si un Firewall está previniendo el sensor del cisco.com que alcanza.
- Verifique si el rutear se convierte en un problema.
- Verifique si el NATing se configura correctamente en el dispositivo de gateway para el dispositivo de flujo descendente.
- Verifique si los credenciales de usuario están correctos.
- Cambie la hora de inicio de la actualización a las horas impares.

Q. Qué hace el **"error: execUpgradeSoftware: AnalysisEngine no puede actualmente ocupado y procesar esta actualización. Espere por favor varios minutos antes de intentar la actualización otra vez.".** ¿medio del mensaje de error?

A. Para resolver este problema, intente recargar el sensor o la nueva imagen el sensor.

Q. Cómo lo hago resuelva la **advertencia del** mensaje de error **Cid/W - el DNS o el proxy de HTTP se requiere para el examen global y la reputación de la correlación que filtran pero no se define ningún DNS o servidores proxy. ¿Agregue un servidor proxy o al servidor DNS HTTP en la configuración de servicio del "host"**?

A. Complete estas tareas para resolver este problema:

- Inhabilite la correlación global.
- Agregue el proxy/Configuración de DNS.

Q. Cómo lo hago resuelva estos errores que el IPS reciba para los problemas de salud globales de la correlación: "**23Jan2010 15:50:39.831 38.001 actualización global de la correlación collaborationApp[655] rep/E A falló: No podido abrir una conexión TLS al servidor HTTP en X.X.82.127:443: Conexión TLS fallada**" y "**actualización global de la correlación collaborationApp[459] rep/E A fallada: Descarga con fallas de ibrs/1.1/drop/default/1296529950: ¿URI no contiene un IP Address válido**"?

A. El IPS no puede llegar a Internet debido a un problema de puerto, por ejemplo, un Firewall en una trayectoria que no tenga los puertos derechos abiertos para el acceso a internet o él puede ser un problema NAT.

Para la correlación global a funcionar totalmente, los contactos del sensor primero con el https update-manifests.ironport.com para autenticar al usuario y después una conexión HTTP descargar las actualizaciones de la CROMATOGRAFÍA GASEOSA. Los archivos que el sensor descarga del HTTP (updates.ironport.com) son los datos de la reputación que la correlación global utiliza. El https update-manifests.ironport.com debe resolver siempre al direccionamiento X.X.82.127, pero la dirección IP HTTP updates.ironport.com puede cambiar, que depende de Internet que usted accede. Usted debe marcar tan la dirección IP. Si se habilita el Filtrado de URL, agregue una excepción para el IP de la interfaz de la Administración de IPS en el filtro URL, de modo que el IPS pueda conectar con Internet.

Este error ocurre cuando hay corrupción en una actualización anterior de la CROMATOGRAFÍA GASEOSA:

```
actualización global de la correlación collaborationApp[459] rep/E A fallada: Descarga con
fallas de ibrs/1.1/drop/default/1296529950: URI no contiene un IP Address válido
```

Este problema puede ser corregido generalmente apagando el servicio de la CROMATOGRAFÍA GASEOSA y después dándole vuelta detrás encendido. En el IDM, elija la configuración > las directivas > correlación > examen/reputación globales, fije el examen global de la correlación (y la reputación que filtra si encendido) a apagado, aplique los cambios, espere 10 minutos, gire las características, y monitoree.

Q. **La actualización global de la correlación A fallada: openConnection: IpAddrException cogido badAddrString. Incapaz de utilizar el proxy de HTTP global de la correlación y las configuraciones DNS. Verifique la conexión y el intento otra vez.** el mensaje de error se recibe en "la categoría del error de la actualización de la reputación". ¿Cómo resuelvo este problema?

A. Verifique estos elementos:

- Usted debe tener una licencia válida IPS para permitir que las características globales de la correlación funcionen.
- Usted debe tener un servidor proxy HTTP o un servidor DNS configurado para permitir que las características globales de la correlación funcionen.
- Porque las actualizaciones globales de la correlación ocurren a través de la interfaz de administración del sensor, los Firewall deben permitir el tráfico tcp 443/80 y UDP 53.
- Aseegurese su sensor soporta las características globales de la correlación. Si usted no quiere esto, inhabilite la característica global de la Colaboración del IDM:Van a la **configuración >** a las **directivas >** la **correlación >** el **examen/la reputación globales**, y fijan el examen global de la correlación (y la reputación que filtra si **encendido**) a **apagado**.

Q. Cómo lo hago resuelva **"la actualización global de la correlación fallada: openConnection: ¿**Error **badAddrString cogido de IpAddrException"** que el IPS recibe para el problema de salud global de la correlación?

A. Si usted utiliza la correlación global (CROMATOGRAFÍA GASEOSA) entonces aseegurese que la resolución de nombre trabaja, por ejemplo, el DNS es accesible. También marque si hay un puerto bloqueado 53 del Firewall. Si no, usted puede apagar la característica de la CROMATOGRAFÍA GASEOSA si usted desea librarse de este mensaje.

Q. ¿Cómo resuelvo la **excepción al inicializar la conexión al** mensaje de error de **MySQL** que recibo cuando inicio IME del navegador?

A. Este problema ocurre generalmente cuando tentativa del cliente de ejecutar IME en los sistemas operativos sin apoyo, tales como Windows 7.

Q. Cómo lo hago resuelva el **"título: IDM en el vendedor 88-nsmc-c1: Categoría del Cisco Systems, Inc.: Los recursos del TARRO del error del archivo del lanzamiento en el archivo JNLP no son firmados por el mismo certificado". ¿o "error que conecta con el sensor, no podido para crear el sensor x.x.x.x:443 que sale** error del **idm"** que el IDM recibe, que sucede durante el lanzamiento de la aplicación?

A. Borre el caché del buscador para resolver este problema.

Q. ¿Es el modo asimétrico en el IPS configurable si usted utiliza el GUI?

A. En la versión 6.0, modo asimétrico en el IPS que es configurable usando el CLI solamente y no disponible en el GUI. Pero, en la versión 6.1 esta característica está también disponible en el GUI.

Q. ¿Cómo resuelvo el problema del tiempo de espera con el sensor IPS?

A. Para resolver este problema, habilite el modo asimétrico que procesa para permitir que el sensor sincronice el estado con el flujo y mantenga el examen para esos motores que no requieran a las ambas direcciones. Utilice esta configuración:

```
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
```

El problema del tiempo de espera ocurre cuando la acción de la negación en línea y niega el paquete se habilita para cada firma en VS0. Habilitar todas las firmas dará lugar al tiempo de espera como el IPS examina cada paquete que pasa a través. Es bueno habilitar solamente la firma específica requerida según el flujo del tráfico de la red para resolver el problema del tiempo de espera.

Q. ¿AIP-SSM ayuda a bloquear Skype?

A. El PIX/ASA no puede bloquear el tráfico de Skype. Skype tiene la capacidad de negociar los puertos dinámicos, y de utilizar el tráfico encriptado. Con el tráfico encriptado, es virtualmente imposible detectarlo pues no hay modelos a buscar.

Usted podría utilizar eventual un IPS de Cisco (sistema de prevención de intrusiones) /AIP-SSM. Tiene algunas firmas que puedan detectar a un cliente de Windows Skype que conecte con Skype el servidor para sincronizar su versión. Esto se hace generalmente cuando inician al cliente la conexión. Cuando el sensor coge la conexión inicial de Skype, usted puede poder encontrar a la persona que utiliza el servicio, y bloquea todas las conexiones iniciadas de su dirección IP.

Q. ¿Por qué hace el `flap de` detección de la interfaz o fueron con frecuencia al estado inactivo en el IPS?

A. Durante una actualización de firma y las reconfiguraciones, las paradas del sensorApp para procesar los paquetes como ella procesan las nuevas firmas en la actualización. El driver de red detecta que el sensorApp ha parado y tira de cualquier nuevo paquete del buffer. El driver de red hace tan diversas cosas, que depende de la configuración y del modelo del sensor:

Interfaz promiscua — Trae el link abajo en las interfaces, y trae la salvaguardia del link una vez que el sensorApp comienza a monitorear otra vez.

Interfaz en línea o pares en línea de Vlan — Depende de la configuración de puente:

- **Auto de puente** — El driver mantiene el link ascendente y comienza a pasar los paquetes a través sin el análisis. Entonces invierte de nuevo a enviar los paquetes a través del sensorApp una vez que el sensorApp comienza a monitorear otra vez.
- **Puente apagado** — El driver trae el link abajo en las interfaces, que es lo mismo que en el modo promiscuo, y las trae de reserva una vez que el sensorApp comienza a monitorear otra vez.

Así pues, si el app del sensor no tira de los paquetes del buffer, que ocurre posiblemente porque no hay interfaz configurada para procesar los paquetes, después el driver puede poner la interfaz en un `estado inactivo`.

Se ven estos registros cuando la interfaz de detección agita:

```
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. ¿El sensor IDS o del Sistema de prevención de intrusiones (IPS) mantiene un

historial de contraseñas?

A. No, el sensor no mantiene un historial de contraseñas. Las contraseñas no son viewable en cualquier momento.

Q. ¿El sensor IDS o del Sistema de prevención de intrusiones (IPS) apoya al servidor de Syslog para enviar los registros?

A. No.

Q. ¿Cuál es el límite máximo de salvar los eventos en el IPS?

A. El evento local del sensor salva solamente el 30 MB y comienza a sobregrabarse una vez que se alcanza el límite del 30 MB. Este límite es no configurable.

Q. ¿Cómo escribo una firma para detectar el [a-z] del foto \ el archivo del .zip en entrante o correo electrónico saliente?

A. Utilice el STRING.TCP para escribir una firma que detecte la conexión. Busque algo similar a esto:

```
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. ¿Cómo usted configura el descanso del FTP cliente?

A. Ejecute estos comandos:

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

Q. ¿Cómo usted convierte el tiempo de la hora de inicio y del final en el iplog-estatus a un formato legible?

A. Esta salida es una representación decimal de la hora actual desde el UNIX epoc. Utilice a una calculadora epoc UNIX tal como la que está localizada en el sitio de la calculadora de la fecha/de la hora de UNIX. Ingrese los primeros 10 dígitos porque esta calculadora es granular solamente a los segundos, y los IDS almacenos nanosegundos. Esto significa que los nueve dígitos más recientes están pelados. Desde el principio tiempo en esta salida, `1084798479 = lunes el 17 de mayo 12:54:39 2004 (GMT)` es lo que usted recibe.

Del CLI, ingrese el iplog-**estatus** para recibir esta salida:

```
"
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. **El "IOException cuando intento para conseguir el certificado: java.security.cert.CertificateExpiredException".** el mensaje de error aparece. ¿Cómo esto puede ser resuelta?

A. Para solucionar este mensaje de error, el login en el AIP-SSM y publicar el comando de la generar-clave de los tls en el modo EXEC privilegiado tal y como se muestra en de este ejemplo:

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

Nota: Esta resolución de usar la generar-clave de los tls del comando también resuelve la aplicación AIP-SSM que no puede conectar con el IME.

Q. **El "IOException: Conexión rechazada: conecte. El servidor IME IME no está respondiendo. Marque por favor si está funcionando con el"** mensaje de error aparece mientras que agrego el IPS en IME. ¿Cómo puede este problema ser resuelto?

A. Para solucionar este mensaje de error, elija el **> Services (Servicios) del panel de control > de las herramientas de administración** y recomience los servicios IME.

Q. **No podría verificar el nombre de usuario de los config/el** mensaje de error del **[IOException - connect timed out] de la contraseña** se recibe cuando agrego un sensor IPS al IME. ¿Cómo puede este problema ser resuelto?

A. Esto indica la comunicación quebrada entre el IME y el sensor IPS. Aseegurese que no hay software que bloquea el SDEE.

Q. **La "respuesta de error del servidor IME: Error desconocido (archivo del registro del control en el directorio del registro de la instalación)".** el mensaje de error aparece. ¿Cómo puede este problema ser resuelto?

A. Para solucionar este mensaje de error, verifique que la dirección IP correcta está utilizada cuando usted agrega el IPS en IME y también marca cualquier Firewall de software que se esté ejecutando en el ordenador IME, que puede bloquear la conexión.

Q. ¿Puede el sensor IDS o del Sistema de prevención de intrusiones (IPS) enviar las alertas del correo electrónico?

A. El sensor IDS no tiene la capacidad de enviar las alertas del correo electrónico en sus los propio. El monitor de la Seguridad cuando está utilizado con el IDS tiene la capacidad de enviar las notificaciones por correo electrónico cuando una regla del evento es accionada por el sensor.

Refiera a las notificaciones por correo electrónico de la configuración para más información sobre cómo configurar las notificaciones por correo electrónico con el monitor de la Seguridad.

El administrador del IPS de Cisco expreso (IME) puede ser configurado para enviar el mensaje de la notificación por correo electrónico (alertas) cuando las reglas del evento son accionadas por los sensores del IPS de Cisco. Refiera a IPS 6.X y posterior: Notificaciones por correo electrónico usando el ejemplo de configuración IME para más información.

Q. **El error: No puede comunicar con el mainApp (getVersion). Entre en contacto por favor a su administrador de sistema.** el mensaje de error aparece cuando intento conectar con mi sensor. ¿Cómo puede este problema ser resuelto?

A. Reinicie el sensor para resolver este problema.

Q. **La advertencia: ADVERTENCIA: Recursos insuficientes disponibles combinar todos actualmente - regexes de encargo activos. Algunas alertas no encenderán. Las firmas reservadas Consider hasta este mensaje ocurren no más.** el mensaje de error aparece firma que ajusta en mi sensor. ¿Cómo puede este problema ser resuelto?

A. Retire las firmas que son paradas para resolver este problema y también el número de firmas del cliente con los regexes debe ser reducido. También, no se recomienda para utilizar ***** y **+ los** metacharacters en los regexes.

Q. ¿Por qué los problemas del tiempo de espera ocurren en los sensores del (IPS) del Cisco Intrusion Prevention System? ¿Cómo puede este problema ser resuelto?

A. El problema del tiempo de espera puede ocurrir debido al Asymmetric Routing. Intente inhabilitar la firma 1330 para resolver este problema.

Q. ¿Es posible inhabilitar SSHv1 y dejar solamente el SSHv2 habilitado en los sensores del (IPS) del Cisco Intrusion Prevention System?

A. Ahora no es posible inhabilitar SSHv1 y dejar solamente SSHv2 habilitado. SSHv1 y SSHv2 se habilitan juntos y no se pueden inhabilitar individualmente.

Q. **El error: Un error ocurrió en el sensor durante la actualización, mensaje del sensor = la actualización requiere 115000 KB en /usr/cids/idsRoot/var, allí es solamente 110443 KB de disponible.** el mensaje aparece cuando actualizo el sensor a la versión 4.1(5). ¿Cómo puede este problema ser resuelto?

A. Este mensaje de error ocurre debido a memoria insuficiente en el sensor.

Complete estas tareas para resolver este problema:

1. Registro en la Cuenta de servicio y la raíz convertida
2. Quite los directorios siguientes como se muestra abajo: `# 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. Ahora intente actualizar el sensor. Refiera al Id. de bug Cisco CSCsb81288 (clientes registrados solamente) para más información.

Q. Consigo el `error mainApp[396] cplane/E - la llamada del accept() devolvió el` mensaje de error `-1` en el inicio ASA. ¿Cómo puede este error ser resuelto?

A. `El error mainApp[396] cplane/E - la llamada del accept() devolvió el` mensaje de error `-1` indica que el servidor Web no puede leer el archivo, y el programa del accept() fallado, que rinde las descripciones del archivo cuando existen las conexiones TLS. Pero este archivo no es necesario para el comportamiento normal. Es inofensivo.

Q. Cómo lo hago resuelva el `errTransport WebSession tls/W:: excepción de la conexión TLS del sessionTask:` ¿mensaje de error `incompleto del apretón de manos`?

A. Este mensaje de error indica que el certificado es no más válido en el módulo. Complete estos pasos para resolver el problema:

1. Regenere el certificado del CLI:Inicie sesión a la línea de comando del sensor.Publique los **tls generan el** comando, y el Presione ENTER. Observe las huellas dactilares se visualizan que.
2. Tire del nuevo certificado adentro a IME:Abra el IME y localice el nombre del sensor en la lista en el Home Page.Haga clic con el botón derecho del ratón el sensor, y el tecleo **edita**.Cuando usted alcanza a la pantalla del dispositivo del editar, haga clic la **AUTORIZACIÓN**. Desvíe cualquier advertencia sobre no poder extraer el tiempo del sensor.Le indicarán con el nuevo Security Certificate (el que usted acaba de generar). Marque para aseegurarse la coincidencia de las huellas dactilares, y haga clic **sí**.Después de varios segundos, el sensor debe mostrar “conectado” en el estado del evento otra vez.

Q. Cuando intento iniciar sesión al IPS, recibo este mensaje de error: `errSystemError-ct-sensorAPP.450 que no responde, clientpipe fallado.` ¿Cómo puedo resolver este error?

A. Para resolver este error, utilice el comando reset para reiniciar el IPS.

Q. El tiempo en AIP-SSM diferencia a partir del tiempo en el dispositivo de seguridad adaptante de Cisco (ASA). ¿Cómo puede este problema ser resuelto?

A. Para resolver este problema, utilice al servidor NTP para sincronizar el tiempo en la Seguridad adaptante Appliance(ASA) y AIP-SSM de Cisco.

Refiera a configurar el NTP en los sensores IPS para más información.

Q. ¿Cómo puedo aplicar los sensores virtuales múltiples en AIP-SSM?

A. Los sensores virtuales en AIP-SSM no pueden ser aplicados por la interfaz porque el AIP-SSM tiene solamente una interfaz. Cuando usted crea los sensores virtuales múltiples, usted debe asignar esta interfaz a solamente un sensor virtual. Usted no necesita señalar una interfaz para los otros sensores virtuales.

Después de que usted cree los sensores virtuales, usted debe asociarlos a los contextos de seguridad en el dispositivo de seguridad adaptante (ASA) usando el comando afectar un aparato-**IPS**. Usted puede asociar muchos contextos de seguridad a muchos sensores virtuales. Refiera a los *sensores virtuales de asignación a la* sección *adaptante de los contextos del dispositivo de seguridad de* configurar AIP-SSM para más información.

Q. ¿Cuál es el número máximo de sensores virtuales soportados por AIP-SSM?

A. Un número máximo de cuatro sensores virtuales puede ser soportado.

Q. ¿Si utilizo SSH o el IDM para iniciar sesión al IPS después es él posible configurar el IPS 4240/IDSM/IDSM2 para validar a los usuarios administradores contra un servidor RADIUS/TACACS+?

A. No es posible con un servidor TACACS+ pero el RADIUS se soporta de la versión IPS 7.0.(4)E4. Refiera secciones *nuevas y de la información cambiada* y de las *restricciones y de las limitaciones de los* Release Note para el Cisco Intrusion Prevention System 7.0(4)E4 para más información. También, refiera a IPS 7.X: Autenticación de ingreso del usuario al sistema usando ACS 5.X como ejemplo de la configuración de servidor de RADIUS para una configuración de muestra.

Q. ¿Cuál es el impacto de la licencia expirada en el funcationality IPS?

A. El único impacto que una licencia expirada tiene en el sensor es que para las actualizaciones de firma.

Q. ¿Las actualizaciones de firma IPS tienen un impacto en los servicios o la conectividad de red?

A. No. Las actualizaciones de firma IPS no tienen un impacto en los servicios o la conectividad de red.

Q. ¿Cuál es el URL exacto que necesito ingresar para que el módulo ips se ponga al día automáticamente con las últimas firmas?

A. El link requerido para permitir que el módulo ips se ponga al día automáticamente con la última firma es: https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl.

Usted debe utilizar su identificación del usuario y contraseña de Cisco para completar la actualización del módulo ips.

Nota: En el tren 6.x del código, las actualizaciones automáticas del cisco.com no se soportan. Usted debe descargar manualmente los archivos de firma y aplicarlos al sensor. Hay una función del automóvil Update Button en el código 6.x; sin embargo, esto es posible solamente de un servidor de archivo local en quien los archivos de firma se deban descargar manualmente también.

Q. ¿El sensor IPS vulnerable al X11 vira la vulnerabilidad del secuestro hacia el lado de babor de la sesión de la expedición?

A. No. No es vulnerable por estas razones:

- El sensor no tiene bibliotecas X11. Por lo tanto no hay sesiones a secuestrar.
- La expedición del puerto X11 no se habilita en la configuración SSH.
- El IPv6 no se compila en el corazón del sensor. Esto se requiere para explotar la vulnerabilidad.

Q. ¿Por qué el AIP-SSM no muestra ninguna registros cuando el ASA muestra el un montón de registros de la advertencia y del ataque?

A. Esto sucede porque cuando el ASA bloquea algo, no se pasa al IPS para el examen duplicado. Por lo tanto, usted no puede ver que el duplicado abre una sesión el ASA y el IPS.

Q. Después de que un usuario despliegue el conjunto de firmas S518, el "**invalidValue: El sig de Editng cadena-XL-TCP no tiene NINGÚN efecto en esta versión**" mensaje de error de ocurre. ¿por qué?

A. Éste es el mensaje de error completo:

```
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
```

Este problema sube porque cadena-XL-TCP o el motor cadena-TCP-XL no se soporta en el hardware. Para más detalles, refiera a los Release Note del motor E4 IPS.

Q. Cuando pongo al día automáticamente las firmas en un ASA-SSM-10 con la característica auto de la actualización, recibo este mensaje de error: **Paquete de actualización auto no instalable encontrado en el status=true del servidor.** ¿Cómo puedo resolver este problema?

A. Esta salida muestra el mensaje de error completo:

```
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
```

Se ha generado este error y las firmas no se ponen al día automáticamente porque las actualizaciones de la definición de la firma después de S479 requieren el motor E4. Para resolver esto, usted necesita actualizar manualmente el sensor a 7.0(2)E4.

Nota: El sensor no puede actualizarse automáticamente al E4 porque requiere 7.0(2) y una reinicialización del sensor.

Q. El feauture auto de la actualización en el IPS 5.0 para el módulo NID no está trabajando. ¿Cómo puedo resolver este problema?

A. Esta salida muestra el mensaje de error completo:

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

Este problema ocurre debido a un estilo incorrecto del listado del directorio con el servidor FTP. Para resolver esto, los listados del directorio del Unix-estilo del Switch de MS-DOS existente diseñan los listados del directorio.

Para modificar las configuraciones del listado del directorio, **>** Program Files (Archivos de programa) selecto del **comienzo > Administrative Tools** para abrir al administrador de servicios de Internet. Después vaya a la lengueta del directorio de inicio y cambie el estilo del listado del directorio de MS-DOS a UNIX.

Q. IPS-4255 recibe el SensorApp falla en TcpRootNode:: mensaje de error del expireNow() durante una actualización. ¿Cómo resuelvo este problema?

A. Este problema es debido al error del motor del análisis y se dirige en el Id. de bug Cisco CSCtb39179 (clientes registrados solamente). Actualice el sensor a la versión 7.0(4)E4 para reparar este problema.

Q. Cuando intento realizar una actualización de la licencia después de que el purchanse I un nuevo autorice los informes sobre dispositivos este error: **"No podido poner al día la licencia en el sensor." el "errExpiredLicense-The que expira la nueva licencia fecha es más viejo que expira la licencia actual fecha."** ¿Cómo puedo resolver este problema?

A. Este problema ocurre cuando el archivo de licencia recibido es inválido. Para obtener un archivo de la licencia válida, inicie sesión al cisco.com como usuario registrado, y descargue el archivo de licencia apropiado. Una vez que usted obtiene el archivo de la licencia válida, instalelo en su sensor.

Si usted instala el nuevo archivo de licencia y le todavía reciba un error, pudo haber un problema con el archivo existente de la licencia inválida. Para resolver este problema, complete estos pasos para borrar el archivo existente de la licencia inválida:

1. Inicie sesión a la Cuenta de servicio tecleando su Nombre de usuario de la Cuenta de servicio.Si usted no tiene una Cuenta de servicio, abra la línea de comando IPS, ingrese al modo de configuración, y ingrese este comando**password password del servicio del privilegio del** *nombre del* **nombre de usuario**
   ```
   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. Una vez que usted inicia sesión a su Cuenta de servicio, ingrese el **comando su** para ir a arraigar (usando la misma contraseña que la Cuenta de servicio).
3. Borre los archivos en el directorio de /usr/cids/idsRoot/shared/.**Nota:** No borre el archivo

host.conf.Ingrese el comando **cd de /usr/cids/idsRoot/shared/** para ir al directorio compartido.Ingrese el **comando ls** para ver los archivos en el directorio.Ingrese el comando del *file_name del* **rm** para quitar los archivos.**Nota:** No borre el archivo host.conf.

4. Ingrese el comando del **reinicio de /etc/init.d/cids** de recomenzar el sensor.
5. Instale la nueva licencia.

Un bug Cisco se ha clasifiado para dirigir este comportamiento. Para más información, refiera a CSCtg76339 (clientes registrados solamente).

Q. Qué hace el `errorMessage: IpLog 1712041197 terminó debido temprano faltar de los asideros de archivo.` ¿medio `name=ErrLimitExceeded del` mensaje de error? ¿Cómo resuelvo este problema?

A. Este error es causado por una cantidad excesiva de paquetes en el registro IP. Inhabilite la característica de registro IP para resolver este problema. El registro IP se significa para resolver problemas solamente; Cisco recomienda que usted no lo habilita para todas las firmas.

Q. Recibo este error cuando pongo al día el sensor de s550 a s551: `No puede analizar la configuración actual para el “signatureDefinition componente” y el caso el "sig0".` ¿Cómo puedo resolver este problema?

A. La modificación de la firma 23899.0 causa este problema. Refiera al Id. de bug Cisco CSCtn84552 (clientes registrados solamente) para más información.

Q. Recibo este error en el sensor: `Error: el autoUpdate seleccionó con éxito un paquete del servicio del localizador del cisco.com, sin embargo, descarga del paquete fallada: No podido recibir el HTTP de respuesta.` ¿Cómo puedo resolver este problema?

A. Marque si hay Filtrado de URL, filtrado de contenido, o un presente del servidor proxy que está bloqueando el autoUpdate del suceso. Aseegurese que el autoUpdate no se está bloqueando y también verifique que los credenciales de usuario proporcionados estén correctos.

Q. Recibo este mensaje de error XML en el sensor IPS que se ejecuta con la versión 6.2(3)E4: `errorMessage: El IPS de software intentó escribir los datos XML inválidos para (token). Los caracteres inválidos XML fueron substituidos por “*”.` ¿Cómo puedo resolver este problema?

A. Este comportamiento ha sido dirigido por el Id. de bug Cisco CSCsq50873 (clientes registrados solamente). Esto es un problema estético y no crea ningunos gastos indirectos operativos a menos que la cantidad excesiva de registros que son recibidos. Una solución provisoria es quitar la configuración relacionada NTP en el sensor. Para una solución permanente, actualización a una versión en la cual se repara este bug.

Q. ¿Por qué el puesto de trabajo IME hace las conexiones constantes a los servidores manejados a pesar del cliente que es cerrado?

A. IME funciona como dos servicios de Windows y el GUI del cliente. Cuando el cliente es cerrado, los dos servicios de Windows (administrador del IPS de Cisco expreso y MySQL-IME) continúan funcionando con y recogiendo los eventos de los sensores manejados y salvándolos en

la base de datos MySQL local; esto permite para que la información histórica ocurra.

El cliente IME debe abrir una sola suscripción SDEE en el sensor manejado, y reutiliza esta suscripción para la actividad subsiguiente de la extracción del evento. La Conectividad constante del puesto de trabajo IME a los sensores manejados es conducta esperada.

Q. ¿Se puede el módulo AIP-SSM utilizar como blanco del SPAN?

A. No. El módulo AIP-SSM no se puede utilizar pues una blanco del SPAN como se utiliza para monitorear solamente el tráfico que atraviesa la interfaz ASA.

Q. ¿Por qué CPU elevada se observa el uso después de que el IPS se actualice al motor E3?

A. Con las actualizaciones del motor E3, el IPS utiliza un diverso algoritmo para manejar su tiempo de inactividad y pasa más interrogación del tiempo para que los paquetes reduzcan el tiempo de espera. Esto el marcar creciente causa un aumento correspondiente en el USO de la CPU. La manera correcta de medir el CPU en el E3 está no por el USO de la CPU, sino por el **porcentaje de la carga de paquete** que muestra la utilización de la CPU correcta.

Q. ¿Por qué es el torneado del LED de estado de la salud ROJO intermitentemente en mi dispositivo IPS?

A. Esto podía suceder debido a un certificado incorrecto en la estación remota del maanagement, el software corriente tal como CS-MARS, el CS, el IEV, VMS-IDS/IPSMC, el etc. para resolver este problema, completa estos pasos:

1. Aplique el certificado de TLS del sensor en la estación de la administración remota.
2. Configure un servidor de los DN válidos.

Q. ¿Cómo se puede el IPS parar de retrasar el tráfico HTTP mientras que atraviesa sus interfaces?

A. Configurar el sensor para trabajar en el modo asimétrico resolverá el problema. Para poner el sensor en la protección asimétrica del modo, complete estos pasos:

1. Vaya a la **configuración** > a las **directivas** > a las **directivas IPS**.
2. Haga doble clic el **sensor virtual**.
3. Vaya **a avanzar las opciones**.
4. Bajo normalice el modo, seleccionan la **protección asimétrica del modo**.
5. Haga clic en OK.
6. Reinicie la unidad para que los cambios tomen el efecto.

Información Relacionada

- Cisco asegura la página de soporte del sistema de prevención de intrusiones
- Troubleshooting AIP-SSM
- Field Notice de seguridad del producto (CiscoSecure Intrusion Detection incluyendo)

- Soporte Técnico y Documentación - Cisco Systems