Contenido

Introducción

Este documento describe cómo actualizar la imagen y la firma para el software del sensor de la detección de intrusos de Cisco (IDS) de la versión 4.1 al (IPS) 5.0 del Cisco Intrusion Prevention System y posterior.

Nota: De la versión de software 5.x y posterior, el IPS de Cisco substituye el Cisco IDS, que es aplicable hasta la versión 4.1.

Nota: El sensor no puede descargar las actualizaciones de software del cisco.com. Usted debe descargar las actualizaciones de software del cisco.com a su servidor FTP, y después configura el sensor para descargarlas de su servidor FTP.

Refiera a instalar la sección de la imagen del sistema AIP-SSM de actualizar, de retroceder, y de instalar las imágenes del sistema para el procedimiento.

Refiera al procedimiento para recuperación de contraseña para el sensor y los módulos de servicios IDS (IDSM-1, IDSM-2) del Cisco IDS para aprender más sobre cómo recuperar el dispositivo del Cisco Secure IDS (antes Netranger) y los módulos para las versiones 3.x y 4.x.

Nota: El tráfico de usuarios no consigue afectado durante la actualización en la configuración **en línea y fracaso-abierta** en el ASA - AIP-SSM.

Nota: Refiera al software del IPS de Cisco que actualiza a partir del 5.1 a la sección 6.x de configurar el sensor de Cisco Intrusion Prevention System usando la interfaz de línea de comando 6.0 para más información sobre el procedimiento para actualizar el IPS 5.1 a la versión 6.x.

Nota: El sensor no soporta los servidores proxy para las actualizaciones autos. Las configuraciones de representación están para la característica global de la correlación solamente.

prerrequisitos

Requisitos

La versión mínima del software requerido que usted necesita para actualizar a 5.0 es 4.1(1).

Componentes Utilizados

La información en este documento se basa en el hardware de las Cisco 4200 Series IDS que funciona con la versión de software 4.1 (ser actualizado a la versión 5.0).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

La actualización de Cisco 4.1 a 5.0 está disponible como descarga del cisco.com. Refiera a obtener el software del IPS de Cisco para el procedimiento que usted utiliza para acceder las descargas del software IPS en el cisco.com.

Usted puede utilizar los métodos uces de los enumerados aquí para realizar la actualización:

- Después de que usted descargue el archivo de 5.0 actualizaciones, refiera al Readme para el procedimiento en cómo instalar el archivo de 5.0 actualizaciones con el **comando upgrade**. Vea el uso la sección de comando upgrade de este documento para más información.
- Si usted configuró la actualización auto para su sensor, copie el archivo de 5.0 actualizaciones al directorio en el servidor que su sensor sondea para las actualizaciones. Vea el uso el comando section de la auto-actualización de este documento para más información.
- Si usted instala una actualización en su sensor y el sensor está inutilizable después de que reinicie, usted debe nueva imagen su sensor. Una actualización de un sensor de cualquier versión del Cisco IDS de 4.1 también le requiere anterior utilizar el comando de la **recuperación** o el CD de la recuperación/de la actualización. Vea la re-imagen la sección del sensor de este documento para más información.

Actualice el sensor

Estas secciones explican cómo utilizar el **comando upgrade** de actualizar el software en el sensor:

Información general

Usted puede actualizar el sensor con estos archivos, que tienen la extensión .package:

- Actualizaciones de firma, por ejemplo, IPS-sig-S150-minreq-5.0-1.pkg
- Actualizaciones del motor de firma, por ejemplo, IPS-engine-E2-req-6.0-1.pkg
- Actualizaciones importantes, por ejemplo, IPS-K9-maj-6.0-1-pkg
- Actualizaciones de menor importancia, por ejemplo, IPS-K9-min-5.1-1.pkg
- Actualizaciones del Service Pack, por ejemplo, IPS-K9-sp-5.0-2.pkg
- Actualizaciones de la división de la recuperación, por ejemplo, IPS-K9-r-1.1-a-5.0-1.pkg
- Distribución de parches, por ejemplo, IPS-K9-patch-6.0-1p1-E1.pkg
- Actualizaciones de la división de la recuperación, por ejemplo, IPS-K9-r-1.1-a-6.0-1.pkg

Una actualización del sensor cambia la versión de software del sensor.

Comando upgrade y opciones

Utilice el **comando enabled de la auto-actualización-opción** en el submode del host del servicio para configurar las actualizaciones automáticas.

Estas opciones se aplican:

- ¿**valor por defecto**? Fija el valor de nuevo a la configuración de valor predeterminado del sistema.
- ¿**directorio**? Directorio donde los archivos de la actualización están situados en el servidor de archivos.
- ¿**ARCHIVO-copia-protocolo**? Protocolo de la copia de archivo usado para descargar los archivos del servidor de archivos. Los valores válidos son **ftp** o **scp**.**Nota:** Si usted utiliza SCP, usted debe utilizar el comando de la **clave de host del ssh** de agregar el servidor a los host sabidos SSH enumera así que el sensor puede comunicar con él con SSH. Refiera a agregar los host a los host sabidos enumeran para el procedimiento.
- ¿**IP address**? Dirección IP del servidor de archivos.
- ¿**contraseña**? Contraseña del usuario para la autenticación en el servidor de archivos.
- ¿**horario-opción**? Horario cuando ocurren las actualizaciones automáticas. Actualizaciones de previsión del comienzo del calendario en los tiempos específicos en los días específicos. Actualizaciones de previsión periódicas del comienzo en los intervalos periódicos específicos.¿**calendario-horario**? Configura los días de la semana y los tiempos del día que las actualizaciones automáticas se realizan.¿**días de la semana**? Días de la semana en los cuales se realizan las auto-actualizaciones. Usted puede seleccionar los días múltiples. De domingo a sábado es los valores válidos.¿**no**? Quita una configuración de la entrada o de la selección.¿**tiempo-de-día**? Épocas del día en el cual las auto-actualizaciones comienzan. Usted puede seleccionar las épocas múltiples. El valor válido es hh: milímetro [: ss].¿**periódico-horario**? Configura el tiempo que la primera actualización automática debe

ocurrir, y cuánto tiempo esperar entre las actualizaciones automáticas.¿**intervalo**? El número de horas a esperar entre las actualizaciones automáticas. Los valores válidos son 0 a 8760.¿**hora de inicio**? El Time Of Day para comenzar la primera actualización automática. El valor válido es hh: milímetro [: ss].
- ¿**username**? Nombre de usuario para la autenticación en el servidor de archivos.

Para el procedimiento IDM para actualizar el sensor, refiera a poner al día el sensor.

Utilice el comando upgrade

Usted recibe los errores de SNMP si usted no tiene los parámetros de la **comunidad de sólo lectura** y de la **comunidad de lectura/escritura** configurados antes de actualizar a IPS 6.0. Si usted está utilizando el **conjunto** SNMP y/o **consigue las** características, usted debe configurar los parámetros de la **comunidad de sólo lectura** y de la **comunidad de lectura/escritura** antes de que usted actualice a IPS 6.0. En IPS 5.x, fijaron a la **comunidad de sólo lectura al** público por abandono, y fijaron a la **comunidad de lectura/escritura al** soldado por abandono. En IPS 6.0 estas dos opciones no tienen valores predeterminados. Si usted no utilizó el SNMP **consigue** y **fija** con IPS 5.x, por ejemplo, el permiso-conjunto-GET fue fijado a falso, después no hay problema a actualizar a IPS 6.0. Si usted utilizó el SNMP **consigue** y **fija** con IPS 5.x, por ejemplo, el permiso-conjunto-GET fue fijado para verdad, usted debe configurar la **comunidad de sólo lectura** y los parámetros de la **comunidad de lectura/escritura a los** valores específicos o a la actualización IPS 6.0 fallan.

Recibe este mensaje de error:

Nota: El IPS 6.0 niega los eventos de alto riesgo por abandono. Esto es un cambio de IPS 5.x. Para cambiar el valor por defecto, cree una invalidación de la acción del evento para el paquete de la negación acción en línea y configurela que se inhabilitará. Si el administrador no es consciente de la comunidad de lectura/grabación entonces ella debe intentar inhabilitar el SNMP totalmente antes de que una tentativa de actualizar se haga para quitar este mensaje de error.

Complete estos pasos para actualizar el sensor:

1. Descargue el archivo principal de la actualización (IPS-K9-maj-5.0-1-S149.rpm.pkg) a un FTP, a SCP, al HTTP, o al servidor HTTPS que es accesible de su sensor.Refiera a obtener el software del IPS de Cisco para el procedimiento en cómo localizar el software en el cisco.com.**Nota:** Usted debe iniciar sesión al cisco.com usando una cuenta con los privilegios criptográficos para descargar el archivo. No cambie el nombre del archivo. Usted debe preservar el nombre del archivo original para que el sensor valide la actualización.**Nota:** No cambie el nombre de fichero. Usted debe preservar el nombre de fichero original para que el sensor valide la actualización.
2. Inicie sesión al CLI usando una cuenta con los privilegios de administrador.
3. Ingrese en el modo de configuración:`sensor#` **`configure terminal`**
4. Actualice el sensor:`sensor(config)#` **`upgrade scp://<username>@<server IP>//upgrade/<file name>`**Ejemplo:**Nota:** Este comando está en dos líneas debido a las razones espaciales.`sensor(config)#` **`upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg`****Nota:** Refiera a los servidores soportados FTP y HTTP/HTTPS para una lista de servidores soportados FTP y HTTP/HTTPS. Refiera a agregar los host a los host sabidos SSH enumeran para más información sobre cómo agregar el servidor de SCP a la lista sabida SSH de los host.
5. Ingrese la contraseña cuando está indicado:`sensor(config)#` **`upgrade`**

```
scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg
```

6. Teclee **sí** para completar la actualización.**Nota:** Las actualizaciones importantes, las actualizaciones de menor importancia, y los paquetes de servicios pudieron forzar un reinicio de los procesos IPS o aún forzar una reinicialización del sensor para completar la instalación. Así pues, hay una interrupción del servicio por lo menos dos minutos. Sin embargo, las actualizaciones de firma no requieren una reinicialización después de que se haga la actualización. Refiera a las actualizaciones de firma de la descarga (clientes registrados solamente) para las últimas actualizaciones.
7. Verifique su nueva versión Sensor:`sensor#`**`show version`**`Application Partition:Cisco Intrusion Prevention System,` **`Version 5.0(1)S149.0`**`OS Version 2.4.26-IDS-smp-bigphysPlatform: ASA-SSM-20Serial Number: 021No license presentSensor up-time is 5 days.Using 490110976 out of 1984704512 bytes of available memory (24% usage)system is using 17.3M out of 29.0M bytes of available disk space (59% usage)application-data is using 37.7M out of 166.6M bytes of available disk space (24 usage)boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)MainApp 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600 RunningAnalysisEngine 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600 RunningCLI 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600Upgrade History: IDS-K9-maj-5.0-1-14:16:00 UTC Thu Mar 04 2004`**`Recovery Partition Version 1.1 - 5.0(1)S149`**`sensor#`**Nota:** Para IPS 5.x, usted recibe un mensaje que estado la actualización sea de tipo desconocido. Usted puede ignorar este mensaje.**Nota:** El sistema operativo reimaged y se quitan todos los archivos que se han puesto en el sensor con la Cuenta de servicio.

Refiera a poner al día el sensor para más información sobre el procedimiento IDM para la actualización del sensor.

Configurar las actualizaciones automáticas

Actualizaciones automáticas

Usted puede configurar el sensor para buscar los nuevos archivos de la actualización en su directorio de la actualización automáticamente. Por ejemplo, varios sensores pueden señalar al mismo directorio remoto del servidor FTP con diversos horario de la actualización, tales como cada 24 horas, o lunes, miércoles, y viernes en 11:00 P.M.

Usted especifica esta información para programar las actualizaciones automáticas:

- Dirección IP del servidor
- La trayectoria del directorio en el servidor de archivos donde el sensor marca para saber si hay actualización clasifía
- Protocolo de la copia de archivo (SCP o FTP)
- Nombre de usuario y contraseña
- Horario de la actualización

Usted debe descargar la actualización del software del cisco.com y copiarla al directorio de la actualización antes de que el sensor pueda sondear para las actualizaciones automáticas.

Nota: Si usted utiliza la actualización automática con AIM-IPS y otros dispositivos o los módulos IPS, aseegurese le poner ambo el 6.0(1) archivo de la actualización, IPS-K9-6.0-1-E1.pkg, y el archivo de la actualización AIM-IPS, IPS-AIM-K9-6.0-4-E1.pkg, en el servidor de actualización automático de modo que AIM-IPS pueda detectar correctamente qué archivo necesita ser descargado y ser instalado automáticamente. Si usted pone solamente 6.0(1) el archivo de la actualización, IPS-K9-6.0-1-E1.pkg, en el servidor de actualización automático, las descargas AIM-IPS y los intentos para instalarlo, que es el archivo incorrecto para AIM-IPS.

Refiera a poner al día el sensor automáticamente para más información sobre el procedimiento IDM para la actualización automática del sensor.

Utilice el comando de la auto-actualización

Vea la sección del comando upgrade y de las opciones de este documento para los comandos del **automóvil Update Button**.

Complete estos pasos para programar las actualizaciones automáticas:

1. Inicie sesión al CLI con una cuenta que tenga privilegios de administrador.
2. Configure el sensor para buscar automáticamente las nuevas actualizaciones en su directorio de la actualización.`sensor#`**`configure terminal`**`sensor(config)#`**`service host`**`sensor(config-hos)#`**`auto-upgrade-option enabled`**
3. Especifique la previsión:Para el calendario que programa, que comienza las actualizaciones en los tiempos específicos en los días específicos:`sensor(config-hos-ena)#`**`schedule-option calendar-schedule`**`sensor(config-hos-ena-cal#`**`days-of-week sunday`**`sensor(config-hos-ena-cal#`**`times-of-day 12:00:00`**Para la previsión periódica, que comienza las actualizaciones en los intervalos periódicos específicos:`sensor(config-hos-ena)#`**`schedule-option periodic-schedule`**`sensor(config-hos-ena-per)#`**`interval 24`**`sensor(config-hos-ena-per)#`**`start-time 13:00:00`**
4. Especifique la dirección IP del servidor de archivos:`sensor(config-hos-ena-per)#`**`exit`**`sensor(config-hos-ena)#`**`ip-address 10.1.1.1`**
5. Especifique el directorio donde los archivos de la actualización están situados en el servidor de archivos:`sensor(config-hos-ena)#`**`directory /tftpboot/update/5.0_dummy_updates`**
6. Especifique el nombre de usuario para la autenticación en el servidor de archivos:`sensor(config-hos-ena)#`**`user-name tester`**
7. Especifique la contraseña del usuario:`sensor(config-hos-ena)#`**`password`**`Enter password[]: `**`******`**`Re-enter password: `**`******`**
8. Especifique el protocolo del servidor de archivos:`sensor(config-hos-ena)#`**`file-copy-protocol ftp`****Nota:** Si usted utiliza SCP, usted debe utilizar el comando de la **clave de host del ssh** para agregar el servidor a los host sabidos SSH enumera así que el sensor puede comunicar con él con SSH. Refiera a agregar los host a los host sabidos enumeran para el procedimiento.
9. Verifique las configuraciones:`sensor(config-hos-ena)#`**`show settings`**` enabled ---------- ---------- schedule-option ---------- ---------- periodic-schedule ---------- ---------- start-time: 13:00:00 interval: 24 hours ---------- ---------- ---------- ip-address: 10.1.1.1 directory: /tftpboot/update/5.0_dummy_updates user-name: tester password: <hidden> file-copy-protocol: ftp default: scp ---------- ----------sensor(config-hos-ena)#`
10. Salga el submode de la auto-actualización:`sensor(config-hos-ena)#`**`exit`**`sensor(config-hos)#`**`exit`**`Apply Changes:?`**`[yes]:`**
11. Presione ENTER para aplicar los cambios o teclear **ningún** para desecharlos.

Rehaga la imagen el sensor

Usted puede nueva imagen su sensor de estas maneras:

- Para los ids appliances con un unidad de Cd-ROM, utilice el CD de la recuperación/de la

actualización.Refiera a usar la sección CD de la recuperación/de la actualización de actualizar, de retroceder, y de instalar las imágenes del sistema para el procedimiento.
- Para todos los sensores, utilice el comando de la **recuperación**.Refiera a recuperar la sección de la partición de aplicación de actualizar, de retroceder, y de instalar las imágenes del sistema para el procedimiento.
- Para el IDS-4215, IPS-4240, e IPS 4255, utilice el ROMMON para restablecer la imagen del sistema.Refiera a instalar la imagen del sistema del IDS-4215 y a instalar el IPS-4240 y IPS-4255 las secciones de la imagen del sistema de actualizar, de retroceder, y de instalar las imágenes del sistema para los procedimientos.
- Para NM-CIDS, utilice el cargador de arranque.Refiera a instalar la sección de la imagen del sistema NM-CIDS de actualizar, de retroceder, y de instalar las imágenes del sistema para el procedimiento.
- Para el IDSM-2, nueva imagen la partición de aplicación de la división del mantenimiento.Refiera a instalar la sección de la imagen del sistema IDSM-2 de actualizar, retrocediendo, y instalando las imágenes del sistema para el procedimiento.
- Para AIP-SSM, la nueva imagen del ASA usando el **módulo 1 del módulo del hw se recupera [configuración |** comando del **inicio]**.Refiera a instalar la sección de la imagen del sistema AIP-SSM de actualizar, de retroceder, y de instalar las imágenes del sistema para el procedimiento.

Información Relacionada

- Página de soporte del Cisco Intrusion Prevention System
- Actualizando, retrocediendo, y instalar las imágenes del sistema para IPS 6.0
- Página del soporte del módulo del sistema de la detección de intrusos de las Cisco Catalyst 6500 Series (IDSM-2)
- Procedimiento para recuperación de contraseña para el sensor y los módulos de servicios IDS 1 del Cisco IDS, IDSM-2)
- Resolver problemas las actualizaciones de la Auto-firma
- Soporte Técnico y Documentación - Cisco Systems