Actualización de la imagen y la firma IDS 4.1 a IPS 5.0 y posterior (AIP-SSM, NM-IDS, IDSM-2) Ejemplo de configuración

Contenido

Introducción

Este documento describe cómo actualizar la imagen y la firma del software Cisco Intrusion Detection Sensor (IDS) de la versión 4.1 a Cisco Intrusion Prevention System (IPS) 5.0 y versiones posteriores.

Nota: A partir de la versión de software 5.x y posteriores, Cisco IPS sustituye a Cisco IDS, que es aplicable hasta la versión 4.1.

Nota: El sensor no puede descargar actualizaciones de software desde Cisco.com. Debe descargar las actualizaciones de software desde Cisco.com a su servidor FTP y luego configurar el sensor para descargarlas desde su servidor FTP.

Refiérase a la sección Instalación de la Imagen del Sistema AIP-SSM de Actualización, Desactualización e Instalación de Imágenes del Sistema para el procedimiento.

Consulte Procedimiento de recuperación de contraseña para el sensor IDS de Cisco y los módulos de servicios IDS (IDSM-1, IDSM-2) para obtener más información sobre cómo recuperar el dispositivo Cisco Secure IDS (anteriormente NetRanger) y los módulos para las versiones 3.x y 4.x.

Nota: El tráfico de usuario no se ve afectado durante la actualización en la configuración en línea y fallo-apertura en ASA - AIP-SSM.

Nota: Refiérase a la sección Actualización del Software IPS de Cisco de 5.1 a 6.x de Configuración del Sensor del Sistema de Prevención de Intrusiones de Cisco Usando la Interfaz de Línea de Comandos 6.0 para obtener más información sobre el procedimiento para actualizar IPS 5.1 a la versión 6.x.

Nota: El sensor no admite servidores proxy para actualizaciones automáticas. La configuración de proxy es sólo para la función de correlación global.

Prerequisites

Requirements

La versión de software mínima necesaria para actualizar a 5.0 es 4.1(1).

Componentes Utilizados

La información de este documento se basa en el hardware IDS de Cisco serie 4200 que ejecuta la versión de software 4.1 (para actualizarse 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). If your network is live, make sure that you understand the potential impact of any command.

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 para su descarga en Cisco.com. Consulte Obtención de software IPS de Cisco para obtener información sobre el procedimiento que debe seguir para acceder a las descargas de software IPS en Cisco.com.

Puede utilizar cualquiera de los métodos enumerados aquí para realizar la actualización:

- Después de descargar el archivo de actualización 5.0, consulte el archivo Léame para obtener información sobre cómo instalar el archivo de actualización 5.0 con el comando upgrade. Vea la sección Uso del Comando Upgrade de este documento para obtener más información.

- Si ha configurado la actualización automática para el sensor, copie el archivo de actualización 5.0 en el directorio del servidor en el que el sensor sondea las actualizaciones. Vea la sección Uso del Comando auto-upgrade de este documento para obtener más información.
- Si instala una actualización en el Sensor y el Sensor no se puede utilizar después de que se reinicie, debe volver a crear una imagen del Sensor. Una actualización de un sensor desde cualquier versión de Cisco IDS anterior a la 4.1 también requiere que utilice el comando recover o el CD de recuperación/actualización. Consulte la sección Re-image the Sensor de este documento para obtener más información.

Actualización del sensor

Estas secciones explican cómo utilizar el comando upgrade para actualizar el software en el Sensor:

- Overview
- Comando de actualización y opciones
- Utilizar el comando Actualizar

Overview

Puede actualizar el sensor con estos archivos, todos con la extensión .pkg:

- Actualizaciones de firmas, por ejemplo, IPS-sig-S150-minreq-5.0-1.pkg
- Actualizaciones del motor de firmas, por ejemplo, IPS-engine-E2-req-6.0-1.pkg
- Actualizaciones principales, por ejemplo, IPS-K9-classif-6.0-1-pkg
- Actualizaciones menores, por ejemplo, IPS-K9-min-5.1-1.pkg
- Actualizaciones de Service Pack, por ejemplo, IPS-K9-sp-5.0-2.pkg
- Actualizaciones de particiones de recuperación, por ejemplo, IPS-K9-r-1.1-a-5.0-1.pkg
- Versiones de parches, por ejemplo, IPS-K9-patch-6.0-1p1-E1.pkg
- Actualizaciones de particiones de 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 de actualización y opciones

Utilice el comando auto-upgrade-option enabled en el submodo de host de servicio para configurar las actualizaciones automáticas.

Se aplican estas opciones:

- default: permite volver a establecer el valor en la configuración por defecto del sistema.
- directorio: directorio en el que se encuentran los archivos de actualización en el servidor de archivos.
- file-copy-protocol: protocolo de copia de archivos utilizado para descargar archivos del servidor de archivos. Los valores válidos son ftp o scp.

  Nota: Si utiliza SCP, debe utilizar el comando ssh host-key para agregar el servidor a la lista de hosts conocidos de SSH para que el Sensor pueda comunicarse con él a través de SSH. Consulte Adición de Hosts a la Lista de Hosts Conocidos para obtener información sobre el procedimiento.
- ip-address: dirección IP del servidor de archivos.
- password: contraseña de usuario para la autenticación en el servidor de archivos.
- opción de programación: programa cuándo se producen las actualizaciones automáticas. La programación del calendario inicia actualizaciones a horas específicas en días específicos. La programación periódica inicia actualizaciones a intervalos periódicos específicos.
  - calendar-schedule: configura los días de la semana y las horas del día en que se realizan las actualizaciones automáticas.
    - días de la semana: días de la semana en los que se realizan las actualizaciones automáticas. Puede seleccionar varios días. De domingo a sábado son los valores válidos.
    - no: elimina una entrada o una configuración de selección.
    - horas del día: horas del día en las que comienzan las actualizaciones automáticas. Puede seleccionar varias veces. El valor válido es hh:mm[:ss].
  - periodic-schedule: configura el tiempo que debe ocurrir la primera actualización automática y el tiempo de espera entre las actualizaciones automáticas.
    - intervalo: el número de horas de espera entre actualizaciones automáticas. Los valores válidos son de 0 a 8760.
    - start-time: la hora del día a la que se iniciará la primera actualización automática. El valor válido es hh:mm[:ss].
- user-name: nombre de usuario para la autenticación en el servidor de archivos.

Para conocer el procedimiento de IDM para actualizar el sensor, consulte Actualización del sensor.

Utilizar el comando Actualizar

Recibe errores SNMP si no tiene los parámetros read-only-community y read-write-community configurados antes de actualizar a IPS 6.0. Si utiliza las funciones set y/o get de SNMP, debe configurar los parámetros read-only-community y read-write-community antes de actualizar a IPS 6.0. En IPS 5.x, la comunidad de sólo lectura se configuró en pública de forma predeterminada, y la comunidad de lectura y escritura se configuró en privada de forma predeterminada. En IPS 6.0, estas dos opciones no tienen valores predeterminados. Si no utilizó SNMP gets y sets con IPS 5.x, por ejemplo, enable-set-get se estableció en false, entonces no hay problema para actualizar a IPS 6.0. Si utilizó SNMP gets y sets con IPS 5.x, por ejemplo, enable-set-get se estableció en true, debe configurar los parámetros read-only-community y read-write-community en valores específicos o la actualización de IPS 6.0 falla.

Recibe este mensaje de error:

```
Error: execUpgradeSoftware : Notification Application "enable-set-get" value set to true,
but "read-only-community" and/or "read-write-community" are set to null. Upgrade may not
continue with null values in these fields.
```

Nota: IPS 6.0 deniega los eventos de alto riesgo de forma predeterminada. Este es un cambio de IPS 5.x. Para cambiar el valor predeterminado, cree un reemplazo de acción de evento para la acción de negación de paquetes en línea y configúrelo para que se inhabilite. Si el administrador no es consciente de la comunidad de lectura y escritura, debe intentar desactivar SNMP completamente antes de realizar un intento de actualización para eliminar este mensaje de error.

Complete estos pasos para actualizar el Sensor:

1. Descargue el archivo de actualización principal (IPS-K9-classified-5.0-1-S149.rpm.pkg) a un servidor FTP, SCP, HTTP o HTTPS al que pueda acceder desde el sensor.

   Consulte Obtención de software Cisco IPS para obtener información sobre cómo localizar el software en Cisco.com.

   Nota: Debe iniciar sesión en Cisco.com con una cuenta con privilegios criptográficos para descargar el archivo. No cambie el nombre de archivo. Debe conservar el nombre de archivo original para que el sensor acepte la actualización.

   Nota: No cambie el nombre de archivo. Debe conservar el nombre de archivo original para que el sensor acepte la actualización.

2. Inicie sesión en la CLI mediante una cuenta con privilegios de administrador.

3. Ingrese en el modo de configuración:

   <#root>

   ```
   sensor#
   ```

   configure terminal

4. Actualice el sensor:

<#root>

```
sensor(config)#
upgrade scp://
```

@

//upgrade/

Ejemplo:

Nota: Este comando está en dos líneas debido a razones espaciales.

<#root>

```
sensor(config)#
upgrade scp://tester@10.1.1.1//upgrade/
IPS-K9-maj-5.0-1-S149.rpm.pkg
```

Nota: Consulte Servidores FTP y HTTP/HTTPS Soportados para obtener una lista de los servidores FTP y HTTP/HTTPS soportados. Consulte Adición de Hosts a la Lista de Hosts Conocidos de SSH para obtener más información sobre cómo agregar el servidor SCP a la

lista de hosts conocidos de SSH.

5. Introduzca la contraseña cuando se le solicite:

```
Enter password: ********
Re-enter password: ********
```

6. Escriba yes para completar la actualización.

   Nota: Las actualizaciones importantes, las actualizaciones menores y los Service Packs pueden forzar un reinicio de los procesos IPS o incluso forzar un reinicio del sensor para completar la instalación. Por lo tanto, se produce una interrupción del servicio durante al menos dos minutos. Sin embargo, las actualizaciones de firmas no requieren un reinicio una vez que se ha realizado la actualización. Refiérase a Descargar Actualizaciones de Firmas (sólo para clientes registrados) para obtener las últimas actualizaciones.

7. Compruebe la nueva versión del sensor:

<#root>

```
sensor#
show version

Application Partition:

Cisco Intrusion Prevention System,
Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: ASA-SSM-20
Serial Number: 021
No license present
Sensor 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  Running

AnalysisEngine   2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

CLI              2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600


Upgrade 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, recibe un mensaje que indica que la actualización es de tipo desconocido. Puede ignorar este mensaje.

Nota: El sistema operativo se recrea y se eliminan todos los archivos que se han colocado en el sensor a través de la cuenta de servicio.

Consulte Actualización del sensor para obtener más información sobre el procedimiento IDM para la actualización del sensor.

Configuración de actualizaciones automáticas

Actualizaciones automáticas

Puede configurar el sensor para que busque automáticamente nuevos archivos de actualización en el directorio de actualización. Por ejemplo, varios sensores pueden señalar al mismo directorio de servidor FTP remoto con diferentes programaciones de actualización, como cada 24 horas o los lunes, miércoles y viernes a las 23:00 horas.

Especifique esta información para programar actualizaciones automáticas:

- Dirección IP del servidor
- Ruta del directorio del servidor de archivos en el que el sensor comprueba los archivos de actualización
- Protocolo de copia de archivos (SCP o FTP)
- Nombre de usuario y contraseña
- Programación de actualización

Debe descargar la actualización de software de Cisco.com y copiarla en el directorio de

actualización antes de que el sensor pueda sondear para obtener actualizaciones automáticas.

Nota: Si utiliza la actualización automática con AIM-IPS y otros dispositivos o módulos IPS, asegúrese de colocar el archivo de actualización 6.0(1), IPS-K9-6.0-1-E1.pkg, y el archivo de actualización AIM-IPS, IPS-AIM-K9-6.0-4-E1.pkg, en el servidor de actualización automática para que AIM-IPS pueda detectar correctamente qué archivo debe descargarse e instalarse automáticamente. Si sólo coloca el archivo de actualización 6.0(1), IPS-K9-6.0-1-E1.pkg, en el servidor de actualización automática, AIM-IPS se descarga e intenta instalarlo, que es el archivo incorrecto para AIM-IPS.

Consulte Actualización automática del sensor para obtener más información sobre el procedimiento IDM para la actualización automática del sensor.

Utilice el comando auto-upgrade

Consulte la sección Comando y opciones de actualización de este documento para ver los comandos auto-update.

Complete estos pasos para programar actualizaciones automáticas:

1. Inicie sesión en la CLI con una cuenta que tenga privilegios de administrador.
2. Configure el sensor para buscar automáticamente nuevas actualizaciones en su directorio de actualizaciones.

```
<#root>

sensor#

configure terminal

sensor(config)#

service host

sensor(config-hos)#

auto-upgrade-option enabled
```

3. Especifique la planificación:
   - Para la programación de calendarios, que inicia actualizaciones a horas específicas en días específicos:

```
<#root>

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 programación periódica, que inicia las actualizaciones a intervalos periódicos específicos:

```
<#root>
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:

```
<#root>
sensor(config-hos-ena-per)#
exit
sensor(config-hos-ena)#
ip-address 10.1.1.1
```

5. Especifique el directorio en el que se encuentran los archivos de actualización en el servidor de archivos:

```
<#root>
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:

```
<#root>
```

```
sensor(config-hos-ena)#
user-name tester
```

7. Especifique la contraseña del usuario:

```
<#root>
sensor(config-hos-ena)#
password

Enter password[]:
******
Re-enter password:
 ******
```

8. Especifique el protocolo del servidor de archivos:

```
<#root>
sensor(config-hos-ena)#
file-copy-protocol ftp
```

Nota: Si utiliza SCP, debe utilizar el comando ssh host-key para agregar el servidor a la lista de hosts conocidos de SSH de modo que el Sensor pueda comunicarse con él a través de SSH. Consulte Adición de Hosts a la Lista de Hosts Conocidos para obtener información sobre el procedimiento.

9. Compruebe los parámetros:

```
<#root>
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. Salir del submodo de actualización automática:

    ```
    <#root>
    sensor(config-hos-ena)#
    exit
    sensor(config-hos)#
    exit

    Apply Changes:?
    [yes]:
    ```

11. Presione Enter para aplicar los cambios o escriba no para descartarlos.

Recreación de la imagen del sensor

Puede recrear imágenes del sensor de las siguientes maneras:

- En el caso de dispositivos IDS con unidad de CD-ROM, utilice el CD de recuperación/actualización.

  Refiérase a la sección Uso del CD de Recuperación/Upgrade de Actualización,

Desactualización e Instalación de Imágenes del Sistema para obtener el procedimiento.

- Para todos los sensores, utilice el comando recover.

  Refiérase a la sección Recuperación de la Partición de Aplicación de Actualización, Desactualización e Instalación de Imágenes del Sistema para obtener el procedimiento.

- Para IDS-4215, IPS-4240 e IPS 4255, utilice ROMMON para restaurar la imagen del sistema.

  Consulte las secciones Instalación de la Imagen del Sistema IDS-4215 e Instalación de la Imagen del Sistema IPS-4240 e IPS-4255 de Actualización, Desactualización e Instalación de Imágenes del Sistema para ver los procedimientos.

- Para NM-CIDS, utilice el cargador de arranque.

  Refiérase a la sección Instalación de la Imagen del Sistema NM-CIDS de Actualización, Desactualización e Instalación de Imágenes del Sistema para el procedimiento.

- Para IDSM-2, recree la partición de la aplicación desde la partición de mantenimiento.

  Refiérase a la sección Instalación de la Imagen del Sistema IDSM-2 de Actualización, Desactualización e Instalación de Imágenes del Sistema para el procedimiento.

- Para AIP-SSM, recree la imagen del ASA usando el hw-module module module 1 recover [configure | boot].

  Refiérase a la sección Instalación de la Imagen del Sistema AIP-SSM de Actualización, Desactualización e Instalación de Imágenes del Sistema para el procedimiento.

Información Relacionada

- Página de soporte del sistema Cisco Intrusion Prevention
- Actualización, Desactualización e Instalación de Imágenes del Sistema para IPS 6.0
- Página de soporte del módulo del sistema de detección de intrusiones (IDSM-2) de Cisco Catalyst serie 6500
- Procedimiento de recuperación de contraseña para el sensor IDS de Cisco y los módulos de servicios IDS (1, IDSM-2)
- Solución de problemas de actualizaciones de firma automática
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).