Preguntas frecuentes sobre Cisco Secure Intrusion Detection System (versiones 3.1 y anteriores)

Contenido

Introducción

Este documento contiene las preguntas frecuentes (FAQ) sobre el Cisco Secure Intrusion Detection System (IDS), conocido antes como Netranger, las versiones 3.1 y anteriores.

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

General

Q. ¿Dónde puedo encontrar la información adicional en el Cisco Secure IDS?

A. Refiérase al Conjunto completo de Documentación del Producto para más información sobre el Cisco Secure IDS.

Q. ¿Cómo pongo al día las firmas para mi sistema IDS entero (sensor IDS + software de administración IDS)?

A. Usted tiene que actualizar las firmas del sensor y de la plataforma de administración por separado. Observe que el software de administración no puede *aprender las* firmas del sensor, así que debe ser puesto al día también. Descargue el último archivo de actualización de firma para cada aplicación de las descargas seguras de Cisco (clientes registrados solamente). Los archivos Léame disponibles en la misma ubicación contienen las instrucciones para el procedimiento de actualización.

Q. ¿Dónde puedo encontrar una lista completa de firmas?

A. La lista de firmas IDS está disponible a través de la enciclopedia segura de Cisco (clientes registrados solamente).

Q. ¿Cuál es la contraseña predeterminada para los usuarios en los ID DE UNIX y el Sensor independiente?

A. En el Sensor independiente de los ID DE UNIX y el software de administración IDS, la contraseña predeterminada es “ataque” para el **netrangr** y la **raíz de los** usuarios. Cuando usted publica el **comando su** de hacer el usuario raíz, la contraseña predeterminada es “ataque.” En la cuchilla del módulo intrusion detection system (IDSM), la contraseña predeterminada es “ataque” para el **ciscoids del** nombre de usuario.

Q. ¿Cómo consigo una cuchilla del módulo intrusion detection system (IDSM) para vaciar sus configuraciones?

A. Usted necesita a un servidor FTP local así que usted puede cargar las configuraciones.

1. Ingrese este comando del modo de diagnóstico en la cuchilla.

   report systemstatus site *<ftp_target_ip_address>* **user** *<ftpusername>* **dir** *<directoryname>*
2. Teclee **y** para continuar cuando está pedido “Continue que genera el informe del sistema?”.
3. Teclee la contraseña FTP de su usuario específicado cuando le indican. Cuando el proceso es completo, usted recibe un mensaje que estado si el proceso falló o si el archivo fue enviado.

Q. ¿Cuando instalo/la desinstalación IDS, dónde se localizan los archivos del registro?

A. Los registros de la instalación/de la actualización se pueden encontrar en estas ubicaciones:

- Los registros de la instalación del director están en /var/adm/nrInstall.log.
- Los registros de la actualización del Service Pack del sensor están en /usr/nr/sp-update/.
- Los registros de la actualización de firma están en /usr/nr/sig-update/.

Q. ¿Qué firmas están disponibles en el PIX para el IDS?

A. El IDS está disponible solamente para PIX 6.0 y posterior. Las firmas se contienen en los mensajes de Syslog 400000 a 400051, designado los mensajes de firma del Cisco Secure IDS. Refiera a la documentación de los mensajes del registro del sistema PIX para más información sobre cada firma.

Q. ¿Puedo ser notificado cuando se liberan las actualizaciones de firma?

A. Firme para arriba para las notificaciones de actualización activa del Cisco IDS para recibir las alertas del email para las noticias sobre productos relacionadas con el Cisco Secure IDS.

Q. ¿Qué aplicaciones debo utilizar para manejar mi sensor IDS, y cuál es la diferencia entre ellas?

A. Antes de la versión 3.1, las opciones de administración son utilizar el Cisco Secure Policy Manager (CSPM) o el UNIX Director. La diferencia principal entre los dos es que el CSPM se ejecuta como aplicación independiente en un Servidor Windows, mientras que el UNIX Director se

ejecuta encima del HP OpenView en un servidor Solaris de UNIX. Con IDS 3.1, los sensores se pueden también manejar con el IDS Event Viewer (IEV) instalado en un PC o que usa el IDS Device Manager, que es parte del sensor de la versión 3.1. Habilitan al administrador de dispositivo por abandono usando el Secure Socket Layer (SSL) después de que usted configure el sensor.

Q. ¿Dónde puedo obtener el software del Software Development Kit (SDK)?

A. El software SDK no está disponible para el público.

Sensor IDS

Q. ¿Cuál es la diferencia entre las versiones Sensores 3.x y 4.x?

A. La versión 4.0 ofrece varias nuevas funciones. La nueva función más notable es comando line interface(cli) similar a Cisco IOS®.

Q. ¿Cómo hacen I duro cifraron la velocidad de la interfaz en el IDS?

A. La configuración dura la velocidad/el duplex en 3.x y el código 4.0 no se soporta y hay un bug contra la petición de la característica (Id. de bug Cisco CSCdy43054 (clientes registrados solamente)). La característica está disponible en el código 5.0, que está disponible ahora en configurar las interfaces.

Q. ¿Cómo actualizo mi software sensor de la versión 3.0 a 3.1?

A. Los clientes pueden descargar el archivo de la actualización para la versión 3.1 de las descargas seguras de Cisco (clientes registrados solamente).

Q. ¿Cómo actualizo mi software sensor de la versión 2.5 a 3.0?

A. Los clientes pueden descargar el archivo de la actualización para la versión 3.0 de las descargas seguras de Cisco (clientes registrados solamente). Instale la actualización de software de la misma manera que el Service Pack y las actualizaciones de firma están instalados en la versión 2.5. El procedimiento se describe detalladamente en la versión 3.0 de la nota de la Configuración del sensor del Cisco IDS.

Q. ¿Cómo actualizo mi software sensor de la versión 2.2 a 3.0?

A. El archivo de la actualización del 3.0 se puede descargar de las descargas seguras de Cisco (clientes registrados solamente), pero este archivo no puede poner al día las versiones antes de 2.5. Usted debe utilizar el CD de la actualización/de la recuperación disponible a través de la Herramienta de actualización del producto (clientes registrados solamente) para actualizar de la versión de software 2.2 al 3.0. El numero de parte para este CD es IDS-SW-U.

Note: Usted debe tener un contrato de servicio técnico válido para pedir el CD de la actualización/de la recuperación.

Q. He asociado un teclado y un monitor a mi sensor, pero no inicia correctamente.

¿Qué debo hacer?

A. Verifique que usted esté utilizando un teclado y un monitor soportados. Algunas marcas y modelos no son compatibles con el Cisco Secure IDS y evitan que el sensor IDS inicie correctamente. Refiera a la falla de arranque del Dispositivo Secure IDS de Cisco para los detalles específicos de la marca.

Q. En la sección IDS de las descargas seguras de Cisco, veo dos tipos de archivos de la actualización (Service Pack y firma). ¿Cuál es la diferencia entre estos archivos?

A. Cada uno de estos archivos contiene un conjunto específico de las actualizaciones de software o de las adiciones, según lo indicado por las convenciones para nombres explicadas aquí.

- La actualización del Service Pack para el software del dispositivo de sensor IDS contiene la mejora al software así como a los arreglos del bug de aplicación central del sensor IDS. Por ejemplo, un archivo nombrado **IDSk9-sp-3.0-5-S17.bin** incluye las actualizaciones al conjunto de firmas más número 17 de la versión de software 3.0(5).
- El archivo de actualización de firma contiene solamente las actualizaciones de las firmas (huellas dactilares del ataque). Por ejemplo, un archivo nombrado **IDSk9-sig-3.0-5-S18.bin** contiene el conjunto de firmas número 18 para 3.0(5) el software sensor.

Los clientes pueden descargar estos archivos del sitio de las descargas seguras de Cisco (clientes registrados solamente).

Q. ¿Cómo puedo decir si un sensor se configura correctamente para evitar a un router?

A. Inicie sesión al sensor como **netrangr del** usuario y ejecute este comando:

```
nrgetbulk <appID> <sensorHostID> <sensorOrgID> <priority> <token>
```

Usted debe recibir una respuesta similar "***<ip_address> al*** Active", ese las demostraciones la dirección IP del dispositivo que evita usado para bloquear los ataques. Esta salida muestra un ejemplo de la sintaxis de los comandos y de la respuesta esperada:

```
netrangr@sensor:/usr/nr
>nrgetbulk 10003 38 1000 1 NetDeviceStatus
10.48.66.68 Active
Success
```

Usted puede también iniciar sesión al router y publicar el **comando who** de ver si se abre una sesión el sensor.

Q. Estoy consiguiendo un mensaje de error que indique el valor no configurado cuando publico el comando nrconns. ¿Cómo puedo resolver este problema?

A. Este mensaje de error indica los problemas potenciales con los archivos de /usr/nr/etc/routes y/o de /usr/nr/etc/hosts en su sensor. … Los archivos /routes definen las comunicaciones vía

correo entre el sensor y el director. … Los archivos /hosts definen los nombres y los IP Addresses de los sensores y de los directores.

Usted puede también iniciar sesión como raíz de usuario, funciona con el **comando sysconfig-sensor**, y ingresa su Información de infraestructura de comunicaciones IDS otra vez.

Q. ¿Cómo utilizo el FTP para copiar los archivos del registro del sensor para salvarlos en algún otro lugar?

A. Refiera a los archivos del registro de copiado IP que se verán para más información sobre este procedimiento.

Q. ¿Qué sucedió a la daemon del configd en las versiones 2.5 y 3.1 del software sensor?

A. El configd es la daemon que procesa los comandos all en los directores así como los sensores de UNIX en la base del código 2.2.x. En la base del código de 2.5 y del 3.0, estas funciones se han absorbido en las otras daemones y la daemon del configd existe no más.

Q. Cuando pongo al día las firmas en el sensor, consigo el `ERROR: No podía determinar el tipo de Netranger del archivo de los daemon. Incapaz de ponerse al día.”` . ¿Qué debo hacer sobre esto?

A. Edite el archivo de /usr/nr/etc/daemons en el sensor para asegurarse de que el nr.packetd está en la lista de la daemon. Después pare y comience los servicios.

Q. ¿En el IDS 4210, que es la interfaz de control y que es la interfaz de rastreo?

A. La interfaz de control en el top es **iprb1:** , y la interfaz de rastreo en la parte inferior es **iprb0:**.

Q. ¿Por qué veo solamente una interfaz cuando publico el `comando ifconfig -a` en mi sensor?

A. **El comando ifconfig** debe mostrar solamente la interfaz de control. El otro interfaz (la interfaz de rastreo) todavía es utilizado por el sensor, pero los usuarios no se supone para poder verlo. Si usted necesita ver esta interfaz, inicie sesión como raíz y publique el **comando ifconfig -a** de determinar los nombres de la interfaz. Publique el **comando ifconfig <interface> plumb** de marcar el estatus de una interfaz particular.

Q. ¿Cómo puedo poner en hard-code la velocidad de la interfaz en el sensor?

A. Poner en hard-code la velocidad de la interfaz en el sensor no debe ser necesaria y no es soportada por el Soporte técnico de Cisco. Si el Switch se fija para el autonegotiation, la interfaz negocia la velocidad con el Switch al cual se asocia. El tráfico de la red al sensor es unidireccional (es decir el sensor recibe). Por lo tanto, es generalmente adecuado si el Switch muestra que 100 semidúplexes se ha negociado (la suposición es que el puerto del switch es 100 M).

Director de UNIX

Q. ¿Puedo utilizar el nuevo sensor del 3.0 con una versión del director 2.2.x?

A. Sí, pero usted debe actualizar su software Director a la versión 2.2.3 o posterior. Los clientes registrados pueden descargar estos archivos de las descargas seguras de Cisco (clientes registrados solamente).

Q. ¿Cómo puedo decir qué versión del Director daemon (Demonio director) estoy utilizando?

A. Publique el comando de **/usr/nr/VERSION del gato** y marque el número de la versión que la salida contiene.

Note: La salida del **comando nrvers** en el director le dice que la versión de las daemones que funcionan con en el director, solamente ella no le dice la versión del software Director sí mismo.

Q. ¿Cómo consigo a un director vaciar su configuración?

A. Inicie sesión como **netrangr del** usuario y ejecute el script /usr/nr/bin/director/nrCollectInfo para enviar la información de la configuración a un archivo nombrado /usr/nr/var/tmp/Report_For_Director.html.

Q. Tengo muchos errores (potencialmente más de 1,000) en mi visualización del HP OpenView. Los borro, pero guardan el volverse. ¿por qué?

A. Si el director IDS consigue inundado con los errores y no puede visualizarlos todos, comienza a mitigar a un archivo. Pare las daemones IDS y salga cualquier correspondencia del OpenView que usted tenga abierto para librarse del archivo. Borre el archivo **/usr/nr/var/nrDirmap.buffer.default**, después recomience las daemones IDS y su correspondencia del OpenView.

Q. Estoy teniendo problemas que consiguen las alarmas sobre la correspondencia del HP OpenView. Mantengo el conseguir de los errores /usr/nr/var/errors.nrdirmap. ¿Qué debo hacer?

A. En los IDS versión antes de 2.2.2, la cosa más fácil a hacer es limpiar hacia fuera la base de datos OpenView. Las vidas de la base de datos en /var/opt/OV/share/databases/openview. Complete estos pasos para borrar la base de datos OpenView.

1. Cierre todos las correspondencias abiertas del OpenView con el **comando ovstop**, después pare los servicios IDS con el **comando nrstop**.
2. Inicie sesión como la raíz de usuario y problema **/usr/nr/bin/director/nrDeleteOVwDb**.
3. Quite todos los archivos “error.*” en el directorio de /usr/nr/var (por ejemplo, errors.configd).
4. Recomience los servicios con el **comando nrstart**, después recomience el OpenView con el **comando ovstart**. **Note**: En la versión director 2.2.2, usted puede quitar solamente a la parte de IDS la base de datos OpenView en vez de la base de datos entera. Este procedimiento se describe en la guía de configuración del director IDS.

Q. No puedo conseguir las alarmas en mi correspondencia del OpenView. El archivo de /usr/nr/var/errors.postofficed en el director contiene los mensajes que

dicen el nrdirmap no se autorizan para ejecutarse en esta máquina. ¿Cómo resuelvo este problema?

A. Ejecute este comando.

```
cp /usr/nr/etc/.lt/license-all.lic /usr/nr/etc/licenses
```

Asegúrese de que el **netrangr del** usuario posea los archivos, después recomienzan los servicios IDS.

Q. Cuando funciono con la utilidad nrConfigure y el clic doble en el director, consigo este mensaje: “Incapaz de encontrar el tipo del sensor para el *<director_name>*. Marque por favor que el postoffice y el packetd se están ejecutando”. ¿Qué debo hacer?

A. El problema ocurre porque el nrConfigure ve el proceso del packetd en el archivo de las daemones del director (que no debe). Cuando el nrConfigure pregunta al director para su versión como si fuera un sensor, el director no puede responder con una versión Sensor.

Complete estos pasos para resolver este problema.

1. Edite el archivo de /usr/nr/etc/daemons y quite las entradas para el nr.packetd, nr.sensord, y nr.managed, puesto que estos procesos deben ejecutarse solamente en el sensor.
2. Pare los servicios con el **comando nrstop**, después recomience los servicios con el **comando nrstart**.
3. Asegúrese de que se haya apagado el nrConfigure.
4. Comience el OpenView con el **comando ovw**.
5. Seleccione **Security > Advanced > Nrconfigure Db > Delete** para borrar la base de datos nrConfigure corrompida.
6. Ingrese **sí** cuando está pedido proceder.
7. Resalte su director y todos sus sensores en ventana principal de OpenView.
8. Seleccione la **Seguridad > avanzó > nrConfigure DB > crean** para crear una nueva base de datos nrConfigure con las versiones de la configuración actual de las máquinas.

Q. ¿Cómo mantengo aplicación nrdirmap de ser habilitado por abandono en las correspondencias del OpenView?

A. Los usuarios que ejecutan la aplicación IDS en el UNIX Director pueden también ejecutar otras aplicaciones en el OpenView. Esto no se aconseja, pero a veces no puede ser evitada. El problema es que el nrdirmap está habilitado por abandono para cada correspondencia del OpenView, que no es deseable cuando otras aplicaciones se ejecutan en el OpenView.

Complete estos pasos en el UNIX Director para cambiar el valor por defecto de modo que usted pueda elegir que las correspondencias tienen nrdirmap habilitado en ellos.

1. Inicie sesión como **netrangr del** usuario.
2. Teclee el **$OV_REGISTRATION/C. cd** (OV_REGISTRATION está la parte de su variable de

entorno. El trayecto habitual es /etc/opt/OV/share/registration/C.)
3. El tipo **su arraiga**.
4. Edite el archivo del nrdirmap y cambie la línea del “comando” como esta salida muestra:

```
Command -Shared -Initial "nrdirmap";
!--- Changes to: Command -Shared -Initial "nrdirmap -d";
```

5. Salve el archivo del nrdirmap.
6. Recicle el OpenView. Ahora, cuando una correspondencia se trae para arriba con el **comando ovw**, tecleando el **ps - ef | el dirmap del grep** debe rendir la salida similar a ésa mostrada aquí. Observe el `nrdirmap` con `- el` Switch `d`.

```
>ps -ef | grep dirmap
netrangr 7175 6820 0 09:50:47 pts/2 0:00 grep dirmap
netrangr 7158 7152 0 09:50:21 ? 0:00 nrdirmap -d
```

Las nuevas correspondencias creadas en el OpenView ahora no tienen nrdirmap habilitado por abandono. Si usted quiere crear una correspondencia con el nrdirmap instalado, usted debe hacerlo del OpenView GUI, pues este procedimiento explica.

1. Del menú de OpenView principal, elija el **Map > nuevo** y ingrese un nombre para la nueva correspondencia.
2. Bajo aplicaciones configurables, usted debe ver el Netranger/director. Elija el **Netranger/director** y haga clic la **configuración para este mapa**.
3. ¿Para la opción que dice “se debe el nrdirmap habilitar para esta correspondencia? ”, elija **verdad** si usted quiere habilitar el nrdirmap.
4. Elija **verifican** y hacen clic la **AUTORIZACIÓN**.

Q. Actualicé a la versión director 2.2.3, y ahora no puedo fijar la gravedad del evento a un llano más altamente de 5, aunque podría hacer tan en las versiones anteriores. ¿Por qué ocurre esto?

A. Los niveles de gravedad se han cambiado en la versión 2.2.3 del director para soportar solamente el rango 1 a 5.

IDS Cisco Secure Policy Manager (CSPM)

Q. ¿Qué versión del CSPM debo utilizar para manejar mi sensor IDS?

A. La versión 2.3i del CSPM es actualmente la que puede manejar el sensor IDS, mientras que no puede el 3.0 CSPM. Si usted utiliza el CSPM para manejar el sensor y el otro Cisco asegura los dispositivos (tales como PIXes, Routers), usted debe instalar las dos diversas versiones de CSPM (2.3i y 3.x) en dos servidores de las ventanas separadas. Usted puede utilizar cada uno de los servidores para manejar los dispositivos correspondientes: CSPM 2.3i para los sensores y CSPM 3.x para el PIXes, Routers, y así sucesivamente.

Q. ¿Cómo configuro el CSPM para manejar mi sensor IDS y para aseegurarme los trabajos de la comunicación?

A. Refiera a configurar un sensor del Cisco Secure IDS en el CSPM para más información sobre cómo configurar el CSPM para manejar su sensor IDS y para asegurar los trabajos de la

comunicación.

Q. ¿Puedo ajustar las firmas para el dispositivo con el CSPM?

A. El ajustar implica el cambiar de lo que toma para que una firma encienda (por ejemplo el número de host en un barrido) y no significa las acciones y los niveles de gravedad de la configuración.

El CSPM no puede (en cualquier versión) ajustar las firmas para el dispositivo. Puede fijar solamente las acciones y las gravedades de una firma. Es decir el CSPM puede fijar que gravedad y que no puede fijar la acción para asociarse a la firma pero qué fuegos que firma. El SigWizMenu en el sensor tiene que ser utilizado para ajustar los sensores. El SigWizMenu y el CSPM se pueden utilizar para configurar el mismo sensor puesto que afectan a diversas porciones de la configuración.

Note: Si usted utiliza la versión 2.2.3 o posterior del UNIX Director, la utilidad nrConfigure puede configurar todo que el SigWizMenu configura. Después de que usted actualice a 2.2.3, usted debe utilizar el nrConfigure en vez del SigWizMenu para ajustar las firmas.

Información Relacionada

- Soporte de productos del Cisco Intrusion Prevention System
- Documentación para Cisco Secure Intrusion Detection System
- Field Notice para el Cisco Secure Intrusion Detection System
- Soporte Técnico y Documentación - Cisco Systems