

Entienda los caída del sistema forzada por software

Contenido

[Introducción](#)

[Prerequisites](#)

[Requisitos](#)

[Componentes usados](#)

[Convenciones](#)

[Posibles causas](#)

[Troubleshooting](#)

[Procedimientos de configuración](#)

[Procedimiento de configuración del host servidor TFTP](#)

[Información para recopilar si abre un pedido de servicio del TAC](#)

[Información Relacionada](#)

Introducción

Este documento explica las causas más frecuentes de los crash forzados por el software y describe la información que debe obtenerse para resolver problemas. Si abre una solicitud de servicio TAC por un crash forzado por el software, la información que le pedirán que recopile será esencial para resolver el problema.

Prerequisites

Requisitos

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Cómo [resolver problemas las caídas del router](#).

Componentes usados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

Para más información sobre los convenios del documento, refiera a los [convenios de los consejos](#)

[técnicos de Cisco.](#)

Un caída del sistema forzada por software ocurre cuando el router detecta un severo, error no recuperado, y se recarga de modo que no transmita los datos corrompidos. Los bug de software del [®] del Cisco IOS causa un amplia mayoría de los caída del sistema forzada por software, aunque algunas Plataformas (tales como Cisco viejo 4000) puedan señalar un problema de hardware como caída del sistema forzada por software.

Si usted no tiene power-cycled ni recargó manualmente al router, la salida del **comando show version** visualiza esto:

```
Router uptime is 2 days, 21 hours, 30 minutes
System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt
System image file is "flash:c2500-is-l.112-15a.bin", booted via flash
```

Si usted tiene la salida de un **comando show version** de su dispositivo de Cisco, usted puede utilizar el [analizador del CLI de Cisco](#) ([clientes registrados](#) solamente) para visualizar los problemas potenciales y los arreglos.

Posibles causas

Esta tabla explica las razones posibles de los caída del sistema forzada por software:

Motivo	Explicación
Tiempos de espera de vigilancia	<p>El procesador utiliza los temporizadores para evitar los bucles infinitos, y hace al router parar e responder. En el funcionamiento normal, la CPU reajusta esos temporizadores a intervalos regulares. Error hacer tan los resultados en una recarga del sistema. Tiempos de espera de vigilancia que están señalados mientras que los caída del sistema forzada por software son software-relacionados. Refiera a los tiempos de espera de vigilancia del troubleshooting para información sobre otros tipos de tiempos de espera de vigilancia. El sistema fue pegado en un loop antes de la recarga. Por lo tanto, el seguimiento de pila no es necesariamente relevante. Usted puede reconocer este tipo de caída del sistema forzada por software en estas líneas de registros de la consola:</p> <pre>Router uptime is 2 days, 21 hours, 30 minutes System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt System image file is "flash:c2500-is-l.112-15a.bin", booted via flash</pre>
Memoria baja	<p>Cuando un router ejecuta demasiado bajo en la memoria, puede recargarse y señalarlo eventualmente como caída del sistema forzada por software. En este caso, los mensajes de error del error de asignación de memoria aparecen en los registros de la consola:</p> <pre>Router uptime is 2 days, 21 hours, 30 minutes System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt System image file is "flash:c2500-is-l.112-15a.bin", booted via flash</pre>
Imagen del software corrupta	<p>A la hora del bootup, un router puede detectar que una imagen del software del Cisco IOS es corrupta, vuelve la suma de comprobación de la imagen comprimida es mensaje incorrecto, e intenta recargar. En este caso, el evento está señalado como caída del sistema forzada por software.</p> <pre>Router uptime is 2 days, 21 hours, 30 minutes System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt System image file is "flash:c2500-is-l.112-15a.bin", booted via flash</pre> <p>Esto se puede causar por una imagen del software del Cisco IOS que se ha corrompido realmente durante la transferencia al router. En este caso, usted puede cargar una nueva imagen sobre el router para resolver el problema. [For a ROMMON recovery method for your platform, refer to ROMmon Recovery Procedure for the Cisco 7200, 7300, 7400, 7500, RSP7000!ENTIT RSM, uBR7100, uBR7200, uBR10000, and 12000 Series Routers.] puede también ser causado por el Hardware de memoria fallada o por un bug de software.</p>

Los errores que causan las caídas son detectados a menudo por el hardware del procesador, que llama automáticamente el código especial del manejo de error en el monitor ROM. El monitor ROM identifica el error, imprime un mensaje, almacena información acerca de la falla y reinicia el sistema. Hay las caídas en las cuales nada de esto puede suceder (véase los [tiempos de espera de vigilancia](#)), y hay las caídas en las cuales el software detecta el problema y llama la función del crashdump. Esto es una caída “software-forzada” verdadera. En POWER PC las Plataformas el “caída del sistema forzada por software” no es la razón del reinicio impresa cuando la función del crashdump consigue llamada - por lo menos hasta muy recientemente. En esas Plataformas (antes de Cisco IOS Software Release 12.2(12.7)), éstos se refieren como excepciones “SIGTRAP”. Del resto de las maneras, los SIGTRAP y SFCs son lo mismo.

Troubleshooting

Los caída del sistema forzada por software son causados típicamente por los bug de software del Cisco IOS. Si los mensajes de error del error de la asignación de memoria están presentes en los registros, vea los [problemas de memoria del troubleshooting](#).

Si usted no ve los mensajes de error del error de la asignación de memoria, y usted no ha recargado manualmente o power-cycled el router después del caída del sistema forzada por software, la mejor herramienta que usted puede utilizar es el [analizador del CLI de Cisco \(clientes registrados\)](#) solamente) a buscar para sabido identificación de bug coincidente. Esta herramienta incorpora las funciones del viejo herramienta Stack Decoder.

Ejemplo:

1. Recoja la salida de la **pila de la demostración del router**.
2. Vaya a la herramienta del [analizador del CLI de Cisco \(clientes registrados\)](#) solamente).
3. Seleccione la **pila de la demostración del** menú desplegable.
4. Goma en la salida que usted ha recogido.
5. El tecleo **somete**. Si la salida decodificada del **comando show stack** hace juego un bug de software conocido, usted recibirá los ID de bug de los bug de software más probable que habrían podido causar el caída del sistema forzada por software.
6. Haga clic en los enlaces hipertexto del ID de bug para ver los detalles adicionales del bug del [juego de herramientas del bug de Cisco \(clientes registrados\)](#) solamente) que puede ayudarle a determinar la coincidencia correcta del ID de bug.

Cuando usted ha identificado un ID de bug que hace juego su error, refiera al campo “corregida” para determinar la primera versión de software del Cisco IOS que contiene el arreglo para el bug.

Si usted es incierto sobre el ID de bug, o la versión de software del Cisco IOS que contiene el arreglo para el problema, actualice su software del Cisco IOS a la última versión de su tren de versión. Esto ayuda porque, la última versión contiene los arreglos para un gran número de bug. Incluso si esto no puede resolver el problema, introduzca errores de funcionamiento la información y el proceso de resolución es más simple y más rápido cuando usted tiene la última versión del software.

Si, después de que usted utilice el analizador del CLI de Cisco, usted sospecha o ha identificado positivamente un bug que siga habiendo sin resolver, recomendamos que usted abre una solicitud de servicio de TAC de proporcionar a la información adicional para ayudar a resolver el bug, y para una notificación más rápida cuando el bug se resuelve en última instancia.

Procedimientos de configuración

Si el problema se identifica como nuevo bug de software, un ingeniero del TAC de Cisco puede pedir que usted configure al router para recoger un *vaciado de memoria*. Un vaciado de memoria se requiere a veces para identificar qué se puede hacer para fijar el bug de software.

Para recoger más información útil en el vaciado de memoria, recomendamos que usted utiliza el **comando debug sanity** ocultado. Esto causa cada almacenador intermediario que se utilice en el sistema cordura-que se controlará cuando se afecta un aparato y cuando se libera. **El comando debug sanity** tiene que ser publicado en el modo EXEC privilegiado (modo del permiso) e implica un poco de CPU, pero no afecta perceptiblemente a las funciones del router. Si usted quiere inhabilitar la revisión de estado, utilice el comando `privileged exec` de la **cordura del undebug**.

Para el Routers que tiene el 16 MB o menos de memoria principal, usted puede utilizar el Trivial File Transfer Protocol (TFTP) para recoger el vaciado de memoria. Se recomienda que usted utiliza el File Transfer Protocol (FTP) si el router tiene más que 16MB de memoria principal. Utilice los Procedimientos de configuración en esta sección. Alternativamente, refiera a [crear los vaciados de memoria](#).

Complete estos pasos para configurar a su router:

1. Configure al router con el **comando configure terminal**.
2. Pulse el **exception dump n.n.n.n**, donde está la dirección IP n.n.n.n del host servidor remoto del Trivial File Transfer Protocol (TFTP).
3. Dé salida al modo de la configuración.

Procedimiento de configuración del host servidor TFTP

Complete estos pasos para configurar un host del servidor TFTP:

1. Cree un fichero bajo directorio de `/tftpboot` en el host remoto con la ayuda de un editor de su opción. El nombre del archivo es la `hostname-memoria` del router de Cisco.
2. En los sistemas Unix, cambie al modo de permiso del fichero de la “`hostname-memoria`” para ser global compatible (666). Usted puede controlar el TFTP puesto a través del **comando copy running-config tftp** en ese fichero.
3. Asegúrese de le para tener más que el 16 MB del espacio libre en disco bajo `/tftpboot`. Si los fallos del sistema, el **comando exception dump** crean su salida al fichero antedicho. Si el router tiene más que el 16 MB de memoria principal, utilice el File Transfer Protocol (FTP) o el Remote Copy Protocol (RCP) para conseguir el vaciado de memoria. En el router, configure esto:

```
exception protocol ftp
exception dump n.n.n.n
ip ftp username <string> ip ftp password <string> ip ftp source-interface
<slot/port/interface> exception core-file <core-filename>
```

Cuando usted ha recogido un vaciado de memoria, cargúelo por teletratamiento a <ftp://ftp-sj.cisco.com/incoming> (en UNIX, pulse el `pftp ftp-sj.cisco.com` y entonces `entrante cd`), y notifique al propietario de su caso e incluya el nombre de fichero.

Información para recopilar si abre un pedido de servicio del TAC

Si usted todavía necesita la ayuda después de seguir los pasos de troubleshooting arriba y quiere crear una solicitud de servicio con el TAC de Cisco, esté seguro de incluir la siguiente información:

- **muestre el Soporte técnico** hecho salir – La salida del comando `show technical-support` da la información sobre el estado actual del router, y también la información fundamental salvada por el router antes de una caída.
- **Registros de la consola** – Los registros de la consola, guardados a menudo hacia fuera a un servidor Syslog, pueden proporcionar a la información valiosa sobre los eventos que ocurren en el router antes de una caída. Estas pistas son a menudo la mayoría de la información importante que usted puede recoger.
- **[fichero del crashinfo](#)** (si presente) – Cisco recomienda que usted utiliza una versión de software del Cisco IOS que utilice la característica del crashinfo para resolver problemas con éxito. Para esto, la versión de software debe cubrir las otras necesidades de su red. Vea [extraer la información del fichero de Crashinfo](#) o utilice la herramienta del [Software Advisor](#) ([clientes registrados](#) solamente) para localizar una versión de software del Cisco IOS que utilice la característica del crashinfo. Una ventaja potencial es que si usted tiene una versión anterior del software del Cisco IOS, las más nuevas versiones de software IOS que utilizan esta característica podrían ya tener su bug fijado.

Para adjuntar la información a su solicitud de servicio, cargúela por teletratamiento a través de la [herramienta de la solicitud de servicio de TAC](#) ([clientes registrados](#) solamente). Si usted no puede tener acceso a la herramienta de la solicitud de servicio de TAC, usted puede enviar la información en una conexión del correo electrónico a attach@cisco.com con su número de caso en el asunto de su mensaje.

Caution: No recargue por favor manualmente o potencia-ciclo el router antes de que usted recoja la información antedicha, si es posible, pues ésta puede hacer la información importante ser perdido que es necesaria determinar la causa raíz del problema.

Información Relacionada

- [Resolución de problemas por averías del router](#)
- [Recuperación de la información del archivo Crashinfo](#)
- [Creación de paquetes de núcleos](#)
- [Resolución de problemas de la memoria](#)
- [Soporte técnico - Cisco Systems](#)