Comprensión de caídas forzadas por software

Contenido

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

Requirements

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

- Cómo Resolver Problemas de Desperfectos del Router.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Un desperfecto forzado por software ocurre cuando el router detecta un error grave e irrecuperable y se recarga para que no transmita datos dañados. La gran mayoría de las caídas

forzadas por software son causadas por errores de software del Cisco IOS®, aunque algunas plataformas (como el antiguo Cisco 4000) pueden informar de un problema de hardware como una caída forzada por software.

Si no ha reproducido el ciclo de apagado y encendido o recargado manualmente el router, el resultado del comando **show version** muestra lo siguiente:

```
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 tiene el resultado de un comando **show version** de su dispositivo Cisco, puede utilizar Cisco CLI Analyzer (sólo clientes registrados) para mostrar posibles problemas y soluciones.

Posibles Causas

Esta tabla explica las posibles razones de las caídas forzadas por software:

Motivo	Explicación

Tiempos de espera de vigilancia	El procesador utiliza temporizadores para evitar loops infinitos y hace que el router deje de responder. En el funcionamiento normal, la CPU restablece esos temporizadores a intervalos regulares. Si no lo hace, se vuelve a cargar el sistema. Los tiempos de espera de vigilancia que se informan como caídas forzadas por software están relacionados con el software. Refiérase a Resolución de Problemas de Tiempos de Espera de Watchdog para obtener información sobre otros tipos de tiempos de espera de vigilancia. El sistema estaba atascado en un loop antes de recarga. Por lo tanto, el seguimiento de la pila no es necesariamente relevante. Puede reconoc este tipo de caída forzada por software en estas líneas de los registros de la consola:
	`%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec`
	`and`
	`*** System received a Software forced crash ***`
	`signal = 0x17, code = 0x24, context= 0x60ceca60`

Memoria baja	Cuando un router se ejecuta en una memoria demasiado baja, puede eventualmente recargars informarlo como un desperfecto forzado por el software. En este caso, los mensajes de error de falla de asignación de memoria aparecen en los registros de la consola:
	`%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84,`
	`pool Processor, alignment 0`

Imagen de software dañada	En el momento del inicio, un router puede detectar que una imagen del software Cisco IOS esta dañada, devolver la `suma de comprobación de la imagen comprimida es un` mensaje `incorrecto` e intentar recargar. En este caso, el evento se informa como una caída forzada por software.
	`Error : compressed image checksum is incorrect 0x54B2C70A`
	`Expected a checksum of 0x04B2C70A`
	`*** System received a Software forced crash ***`
	`signal= 0x17, code= 0x5, context= 0x0`
	`PC = 0x800080d4, Cause = 0x20, Status Reg = 0x3041f003`
	Esto puede ser causado por una imagen de software del IOS de Cisco que en realidad ha sido dañada durante la transferencia al router. En este caso, puede cargar una nueva imagen en el router para resolver el problema. [Para obtener un método de recuperación ROMMON para su plataforma, consulte Procedimiento de recuperación ROMmon para los Cisco 7200, 7300, 7400 7500, RSP7000, Catalyst 5500 RSM, uBR7100, uBR722 00, uBR1000 y 12000 Series Routers.
	También puede ser causado por un hardware de memoria defectuoso o por un error de softwar

Otros fallos	Los errores que provocan caídas son detectados a menudo por el hardware del procesador, qu automáticamente llama a código de control de errores especial en el monitor ROM. El monitor ROM identifica el error, imprime un mensaje, almacena información acerca de la falla y reinicia sistema. Hay caídas en las que no puede ocurrir nada de esto (consulte Tiempos de espera de Watchdog), y hay caídas en las que el software detecta el problema y llama a la función crashdump. Esta es una verdadera falla "forzada por el software". En las plataformas Power PC el "crash forzado por software" no es la razón de reinicio impresa cuando se llama a la función crashdump, al menos hasta hace muy poco. En esas plataformas (previo a la Versión 12.2(12.7 del software del IOS de Cisco), se las denomina excepciones “SIGTRA”: En todos los demás aspectos, los SIGTRAP y los SFC son los mismos.

Troubleshoot

Las caídas forzadas por el software son típicamente causadas por errores de procesamiento del software de Cisco IOS. Si los mensajes de error de falla de asignación de memoria están presentes en los registros, consulte Solución de Problemas de Memoria.

Si no ve mensajes de error de falla de asignación de memoria y no ha recargado manualmente o apagado y encendido el router después de la caída forzada por el software, la mejor herramienta que puede utilizar es el Analizador de CLI de Cisco (sólo clientes registrados) para buscar una ID de error coincidente conocida. Esta herramienta incorpora la funcionalidad de la antigua herramienta Decodificador de pila.

Ejemplo:

1. Recopile el resultado de **show stack** del router.
2. Vaya a la herramienta Cisco CLI Analyzer (sólo clientes registrados).
3. Seleccione **show stack** en el menú desplegable.
4. Pegue el resultado que ha recopilado.
5. Haga clic en Submit (Enviar).Si el resultado decodificado del comando **show stack** coincide con un error de software conocido, recibirá los IDs de bug de los errores de software más probables que podrían haber causado el desperfecto forzado del software.
6. Haga clic en los hipervínculos de ID de bug para ver detalles de bug adicionales de Cisco Bug Toolkit (sólo clientes registrados) que pueden ayudarle a determinar la coincidencia correcta de ID de bug.

Cuando haya identificado un ID de bug que coincida con su error, consulte el campo "fixed in" (corregido en) para determinar la primera versión de Cisco IOS Software que contiene la corrección para el error.

Si no está seguro sobre el ID de bug, o la versión del software del IOS de Cisco que contiene la corrección para el problema, actualice su software del IOS de Cisco a la última versión de su tren de versión. Esto ayuda porque, la última versión contiene correcciones para un gran número de errores. Incluso si esto no resuelve el problema, los informes de errores y el proceso de resolución son más sencillos y rápidos cuando tiene la última versión del software.

Si, después de utilizar el Analizador de Cisco CLI, sospecha o ha identificado positivamente un error que sigue sin resolverse, le recomendamos que abra una solicitud de servicio del TAC para proporcionar información adicional que ayude a resolver el error, y para una notificación más rápida cuando el error se resuelva finalmente.

Procedimientos de configuración

Si el problema se identifica como un nuevo error de software, un ingeniero del TAC de Cisco puede solicitar que configure el router para recopilar un *vaciado de memoria*. A veces se requiere un vaciado de memoria para identificar lo que se puede hacer para corregir el error de software.

Para recopilar información más útil en el vaciado de memoria, recomendamos que utilice el comando **debug sanity** oculto. Esto genera que se compruebe la integridad de cada memoria intermedia que se utiliza en el sistema tanto cuando se la asigna como cuando se la libera. El comando **debug sanity** se debe ejecutar en el modo EXEC privilegiado (modo de habilitación) e involucra parte de la CPU, pero no afecta significativamente la funcionalidad del router. Si desea inhabilitar la verificación de integridad, utilice el comando EXEC **undebug sanity** privilegiado.

Para los routers que poseen 16 MB o menos de memoria principal, puede utilizar el Protocolo trivial de transferencia de archivos (TFTP) para recolectar una descarga del núcleo Si el router posee más de 16MB de memoria principal, se recomienda el uso de un Protocolo de transferencia de archivos (FTP). Utilice los procedimientos de configuración de esta sección. Alternativamente, consulte Creación de Vaciados de Memoria.

Complete estos pasos para configurar el router:

1. Configure el router con el comando **configure terminal**.
2. Escriba **exception dump n.n.n.n**, donde n.n.n.n es la dirección IP del host remoto del servidor del protocolo de transferencia de archivos trivial (TFTP).
3. Salga del modo de configuración.

Procedimiento de configuración del host servidor TFTP

Complete estos pasos para configurar un host de servidor TFTP:

1. Cree un archivo bajo el directorio /tftpboot en el host remoto con la ayuda de un editor de su elección. El nombre del archivo es el hostname-core (núcleo del nombre del host) del router de Cisco.
2. En sistemas UNIX, cambie el modo de permiso del archivo "hostname-core" para que tenga compatibilidad global (666). Puede verificar la configuración TFTP a través del comando **copy running-config tftp** en ese archivo.
3. Asegúrese de tener más de 16 MB de espacio libre en disco en /tftpboot.Si el sistema colapsa, el comando exception dump crea su salida hacia el archivo anterior. Si el router tiene más de 16 MB de memoria principal, utilice el protocolo de transferencia de archivos (FTP) o el protocolo de copia remota (RCP) para obtener el vaciado de memoria. En el router, configure lo siguiente:

   ```
   exception protocol ftp
   exception dump n.n.n.n
   ip ftp username ip ftp password ip ftp source-interface exception core-file
   ```

   Cuando haya recopilado un vaciado de memoria, cárguelo en ftp://ftp-sj.cisco.com/incoming (en UNIX, escriba **pftp ftp-sj.cisco.com** y luego **cd incoming**), y notifique al propietario de su caso e incluya el nombre del archivo.

Información para recopilar si abre un pedido de servicio del TAC

Si todavía necesita ayuda después de seguir los pasos de solución de problemas anteriores y desea crea solicitud de servicio con el TAC de Cisco, asegúrese de incluir la siguiente información:

- **show technical-support** output - El resultado del comando **show technical-support** brinda información sobre el estado actual del router, y también información clave almacenada por el router antes de un desperfecto.
- Registros de consola - Los registros de la consola, a menudo guardados en un servidor syslog, pued proporcionar información valiosa sobre los eventos que ocurren en el router antes de una caída. Esta pistas suelen ser la información más importante que usted puede recoger.
- archivo crashinfo (si está presente) - Cisco recomienda que utilice una versión de software de Cisco que soporte la función crashinfo para resolver problemas exitosos. Para ello, la versión debe satisfac demás necesidades de su red. Vea Recuperación de Información del Archivo Crashinfo o utilice la herramienta Software Advisor (sólo para clientes registrados) para localizar una versión de Cisco IOS Software que soporte la función crashinfo. Una ventaja potencial es que si tiene una versión más ant del software Cisco IOS, las versiones más recientes del software IOS que soportan esta función ya podrían tener su bug corregido.

Para adjuntar la información a su solicitud de servicio, cárguela a través de la Herramienta de Solicitud d Servicio TAC (sólo para clientes registrados). Si no puede acceder a la Herramienta de Solicitud de Servi TAC, puede enviar la información en un archivo adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto del mensaje.

Precaución: No recargue ni apague manualmente el router antes de recopilar la información anterior, si e posible, ya que esto puede provocar la pérdida de información importante necesaria para determinar la c 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