Entienda los caída del sistema forzada 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.

Prerrequisitos

Requisitos

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

- Cómo resolver problemas los desperfectos del router.

Componentes Utilizados

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 obtener más información sobre las convenciones del documento, consulte las Convenciones

de 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 el Cisco 4000 viejo) 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	El procesador utiliza los temporizadores para evitar los Loop infinito, y hace al router parar el responder. En el funcionamiento normal, el 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 pues los caída del sistema forzada por software son software relacionado. Refiera a los tiempos de espera de vigilancia del troubleshooting para la informac sobre otros tipos de tiempos de espera de vigilancia. El sistema fue pegado en un loop antes d 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 los registros la consola: `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`

Memoria baja	Cuando un router ejecuta demasiado bajo en la memoria, puede recargarse y señalarlo eventu como caída del sistema forzada por software. En este caso, los mensajes de error de la falla d asignación de memoria aparecen en los registros de la consola: `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`

Imagen del software corrupta	A la hora del bootup, un router puede detectar que una imagen del Cisco IOS Software es corrupta, vuelve la `suma de comprobación de la imagen comprimida es mensaje incorrecto`, e inten recargar. En este caso, el evento está señalado como caída del sistema forzada por software.
	`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`Esto se puede causar p una imagen del Cisco IOS Software que se ha corrompido realmente durante la transferencia a 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, Catalyst 5500 RSM, uBR7100, uBR7200, uBR10000, and 12000 Series Routers.] puede también ser causado por el Hardwar de memoria fallada o por un bug de software.

Otros incidentes	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 de la memori

ROM. El monitor ROM identifica el error, imprime un mensaje, almacena información acerca d 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 problem llama la función del crashdump. Esta es una verdadera falla "forzada por el software". 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 (previo a la Versión 12.2(12.7) del software del IOS de Cisco), se las denomina excepciones “SIGTRA”: Del resto de las maneras, los SIGTRAP y los SFC son lo mismo.

Troubleshooting

Las caídas forzadas por el software son típicamente causadas por errores de procesamiento del software de Cisco IOS. Si los mensajes de error de la falla de asignación de memoria están presentes en los registros, vea los problemas de memoria del troubleshooting.

Si usted no ve los mensajes de error de la falla de 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 del **show stack del** router.
2. Vaya a la herramienta del analizador del CLI de Cisco (clientes registrados solamente).
3. Seleccione el **show stack 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 a los detalles del bug adicionales del

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

Si usted es incierto sobre el ID de bug, o la versión del Cisco IOS Software que contiene el arreglo para el problema, actualice su Cisco IOS Software 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 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 de Cisco TAC 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 reparar el bug de software.

Para recoger más información útil en el vaciado de memoria, recomendamos que usted utiliza el **comando debug sanity** ocultado. 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** tiene que ser publicado en el modo EXEC privilegiado (enable mode) e implica algún 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 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 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. Teclee 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. Salga del modo de configuración.

Procedimiento de configuración del host servidor TFTP

Complete estos pasos para configurar un host del servidor TFTP:

1. Cree un archivo bajo directorio de /tftpboot en el host remoto con la ayuda de un editor de su opción. 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). Usted puede marcar el TFTP puesto a través del **comando copy running-config tftp** en ese archivo.
3. Aseegurese le tener más que el 16 MB del espacio libre en disco bajo /tftpboot.Si el sistema colapsa, el comando exception dump crea su salida hacia el archivo anterior. Si el router tiene más que el 16 MB de memoria principal, utilice el (RCP) del File Transfer Protocol (FTP) o del Remote Copy Protocol 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, carguelo a ftp://ftp-sj.cisco.com/incoming (en UNIX, teclee 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 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 informa sobre el estado actual del router, y también la información fundamental salvada por el router antes d caída.
- Registros de la consola – Los registros de la consola, guardados a menudo hacia fuera a un servidor Syslog, pueden proporcionar la información valiosa sobre los eventos que ocurren en el router antes una caída. Estas pistas suelen ser la información más importante que usted puede recoger.
- archivo CRASHINFO (si presente) – Cisco recomienda que usted utiliza una versión de Cisco IOS Software que soporte la característica del RMtermcode = 3 nfw para resolver problemas con éxito. P esto, la versión debe cubrir las otras necesidades de su red. Vea extraer la información del archivo CRASHINFO o utilice la herramienta del Software Advisor (clientes registrados solamente) para loca una versión del Cisco IOS Software que soporte la característica del RMtermcode = 3 nfw. Una venta potencial es que si usted tiene una versión anterior del Cisco IOS Software, las más nuevas versione software IOS que soportan esta característica podrían ya tener su bug reparado.

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 usted no puede acceder la herramienta de la solicitud de servicio de TAC, usted puede enviar la información en un elemento adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto de su mensaje.

Precaución: No recargue por favor manualmente o ciclo de la potencia el router antes de que usted recoj 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