Informazioni sugli arresti anomali forzati del software

Sommario

Introduzione

Questo documento spiega le cause più frequenti degli arresti anomali causati dal software e descrive le informazioni da raccogliere per risolvere il problema. Se si apre una richiesta del servizio TAC per un arresto anomalo forzato dal software, le informazioni che verranno richieste saranno essenziali per risolvere il problema.

Prerequisiti

Requisiti

Questo documento è utile per conoscere i seguenti argomenti:

- Come risolvere i problemi di blocco del router.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Un arresto anomalo forzato dal software si verifica quando il router rileva un errore grave e irreversibile e si ricarica in modo da non trasmettere dati danneggiati. La maggior parte degli arresti anomali causati da software è causata da bug del software Cisco IOS®, anche se alcune piattaforme (ad esempio la vecchia Cisco 4000) possono segnalare un problema hardware come un arresto anomalo causato da software.

Se il router non è stato riacceso o ricaricato manualmente, l'output del comando **show version** visualizza quanto segue:

```
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
```

se il dispositivo Cisco restituisce i risultati di un comando **show version**, è possibile usare Cisco CLI Analyzer (solo utenti registrati) per visualizzare i potenziali errori e correggerli.

Possibili cause

Questa tabella spiega i possibili motivi degli arresti anomali forzati del software:

Motivo	Spiegazione

Timeout watchdog	Il processore utilizza i timer per evitare loop infiniti e impedisce al router di rispondere. In condizioni normali, la CPU reimposta i timer a intervalli regolari. In caso contrario, il sistema verrà ricaricato. I timeout di watchdog segnalati come arresti anomali forzati del software son correlati al software. Per informazioni su altri tipi di timeout di watchdog, fare riferimento a Risoluzione dei problemi dei timeout di watchdog. Il sistema era bloccato in un loop prima de ricaricamento. Pertanto, l'analisi dello stack non è necessariamente rilevante. È possibile riconoscere questo tipo di arresto anomalo forzato dal software nelle seguenti righe dei log c console:
	`%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec`
	
	`and`
	
	`*** System received a Software forced crash ***`
	`signal = 0x17, code = 0x24, context= 0x60ceca60`

Memoria insufficiente	Quando la memoria del router è insufficiente, il router può ricaricarsi e segnalarlo come un arresto anomalo causato dal software. In questo caso, nei log della console vengono visualizzati messaggi di errore relativi all'allocazione della memoria:
	`%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84,`
	`pool Processor, alignment 0`

Immagine software danneggiata	Al momento dell'avvio, un router può rilevare che un'immagine software Cisco IOS è danneggiata, restituire il messaggio di `checksum dell'immagine compressa non corretto` e tenta di ricaricarla. In questo caso, l'evento viene segnalato come arresto anomalo forzato dal 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`
	
	La causa può essere un'immagine software Cisco IOS che è stata effettivamente danneggia durante il trasferimento al router. In questo caso, è possibile caricare una nuova immagine s router per risolvere il problema. [Per il metodo di ripristino ROMMON per la piattaforma in us

Altri errori	fare riferimento alla procedura di ripristino ROMmon per Cisco 7200, 7300, 7400, 7500, RSP7000, Catalyst 5500 RSM, uBR7100, uBR7200, uBR1000 e 12000 Router.] Il problema può essere causato anche da hardware di memoria software difettosa o da router bug Gli errori che causano i crash vengono spesso rilevati dall'hardware del processore, che chia automaticamente uno speciale codice di gestione degli errori nel ROM monitor. Il ROM moni identifica l'errore, stampa un messaggio, salva le informazioni sull'errore e riavvia il sistema. alcuni casi, questo problema non si verifica (vedere Timeout di Watchdog), mentre in altri ca software rileva il problema e chiama la funzione crashdump. Questo è un vero e proprio cras "forzato dal software". Sulle piattaforme Power PC, il "crash forzato dal software" non è il mo del riavvio stampato quando viene chiamata la funzione crashdump - almeno fino a poco ten fa. Sulle piattaforme (precedenti alla versione 12.2(12.7) del software Cisco IOS), le eccezio sono denominate "SIGTRAP". In tutti gli altri modi, SIGTRAP e SFC sono uguali.

Risoluzione dei problemi

Gli arresti anomali forzati del software sono in genere causati da bug del software Cisco IOS. Se nei registri sono presenti messaggi di errore relativi all'allocazione della memoria, vedere Risoluzione dei problemi di memoria.

Se non vengono visualizzati messaggi di errore relativi all'allocazione della memoria e non è stato ricaricato o riacceso manualmente il router dopo l'arresto anomalo forzato dal software, lo strumento migliore da utilizzare è Cisco CLI Analyzer (solo utenti registrati) per cercare un ID bug noto e corrispondente. Questo strumento incorpora le funzionalità del vecchio strumento di decodifica dello stack.

Esempio:

1. Raccogliere l'output del comando **show stack** dal router.
2. Andare allo strumento Cisco CLI Analyzer (solo clienti registrati).
3. Selezionare **show stack** dal menu a discesa.
4. Incollare nell'output raccolto.
5. Fare clic su **Invia**.Se l'output decodificato del comando **show stack** corrisponde a un bug software noto, si riceveranno gli ID dei bug software più probabili che potrebbero aver causato l'arresto anomalo del software.
6. Fare clic sui collegamenti ipertestuali per visualizzare ulteriori dettagli sul bug Toolkit di Cisco (solo utenti registrati) che possono aiutare a determinare la corrispondenza corretta dell'ID.

Dopo aver identificato l'ID di un bug che corrisponde all'errore, consultare il campo "risolto in" per determinare la prima versione del software Cisco IOS che contiene la correzione del bug.

In caso di dubbi sull'ID del bug o sulla versione del software Cisco IOS che contiene la soluzione del problema, aggiornare il software Cisco IOS alla versione più recente nella release train. Questa operazione è utile in quanto l'ultima versione contiene correzioni per un numero elevato di bug. Anche se questa operazione non riesce a risolvere il problema, la segnalazione dei bug e il processo di risoluzione sono più semplici e rapidi quando si dispone della versione più recente del software.

Se, dopo aver utilizzato Cisco CLI Analyzer, si sospetta o è stato identificato correttamente un bug non ancora risolto, si consiglia di aprire una richiesta del servizio TAC per fornire informazioni aggiuntive che consentano di risolvere il bug e per ricevere una notifica più rapida quando il bug viene risolto.

Procedure di configurazione

Se il problema è identificato come un nuovo bug del software, un tecnico Cisco TAC può richiedere la configurazione del router per la raccolta di un *dump del core*. A volte è necessario un dump del core per identificare le operazioni che possono essere eseguite per risolvere il bug del software.

Per raccogliere ulteriori informazioni utili nel dump del core, si consiglia di utilizzare il comando **debug sanity** nascosto. In questo modo, ogni buffer utilizzato nel sistema viene sottoposto a controllo di integrità quando viene allocato e quando viene liberato. il comando **debug sanity** deve essere eseguito in modalità di esecuzione privilegiata (modalità di abilitazione) e interessa una parte della CPU, ma non influisce in modo significativo sulla funzionalità del router. Per disabilitare il controllo dell'integrità fisica, usare il comando **undebug sanity** in modalità di esecuzione privilegiata.

Per i router con 16 MB o meno di memoria principale, è possibile utilizzare il protocollo TFTP (Trivial File Transfer Protocol) per raccogliere il dump del core. Se il router ha più di 16 MB di memoria principale, si consiglia di utilizzare il protocollo FTP (File Transfer Protocol). Utilizzare le procedure di configurazione descritte in questa sezione. In alternativa, consultare il documento sulla creazione di dump del core.

Completare la procedura seguente per configurare il router:

1. Configurare il router con il comando **configure terminal**.
2. Digitare **exception dump n.n.n.n**, dove n.n.n.n è l'indirizzo IP dell'host remoto del server TFTP (Trivial File Transfer Protocol).
3. Uscire dalla modalità di configurazione.

Procedura di configurazione host server TFTP

Completare la procedura seguente per configurare un host server TFTP:

1. Creare un file nella directory /tftpboot sull'host remoto con l'aiuto di un editor a scelta. Il nome del file è Cisco router hostname-core.
2. Sui sistemi UNIX, modificare la modalità di autorizzazione del file "hostname-core" in modo che sia globalmente compatibile (666). È possibile controllare l'impostazione del protocollo TFTP con il comando **copy running-config tftp** su tale file.
3. Accertarsi di disporre di più di 16 MB di spazio libero su disco in /tftpboot.Se il sistema si blocca, il comando **exception dump** crea il relativo output nel file indicato sopra. Se il router ha più di 16 MB di memoria principale, usare il protocollo FTP (File Transfer Protocol) o RCP (Remote Copy Protocol) per ottenere il dump della memoria principale. Sul router, configurare quanto segue:

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

   Dopo aver raccolto un dump di base, caricarlo in ftp://ftp-sj.cisco.com/incoming (in UNIX, digitare **pftp ftp-sj.cisco.com** e quindi **cd in entrata**), notificare il proprietario della richiesta e includere il nome del file.

Informazioni da raccogliere se si apre una richiesta di servizio TAC

Se si desidera ricevere ulteriore assistenza dopo aver eseguito le procedure di risoluzione dei problemi descritte in precedenza e si desidera creare una richiesta di assistenza con Cisco TAC, includere le segu informazioni:

- **show technical-support** output: l'output del comando **show technical-support** restituisce informazioni s stato corrente del router e informazioni chiave archiviate dal router prima di un arresto anomalo.
- Registri console: i registri della console, spesso salvati su un server syslog, possono fornire informaz preziose sugli eventi che si verificano sul router prima di un arresto anomalo. Questi indizi sono spes informazioni più importanti che è possibile raccogliere.
- crashinfo file (se presente) - Cisco consiglia di utilizzare una versione software di Cisco IOS che supp la funzione crashinfo per risolvere correttamente il problema. Per questo, la versione deve soddisfare altre esigenze della rete. Vedere Recupero di informazioni dal file Crashinfo o utilizzare lo strumento Software Advisor (solo utenti registrati) per individuare una versione del software Cisco IOS che supp la funzione crashinfo. Se si dispone di una versione precedente del software Cisco IOS, le nuove ver del software IOS che supportano questa funzione potrebbero già risolvere il bug.

Per allegare informazioni alla richiesta di assistenza, caricarla tramite lo strumento TAC Service Request utenti registrati). Se non è possibile accedere allo strumento TAC Service Request, inviare le informazion un allegato e-mail a attach@cisco.com con il numero della richiesta in oggetto.
Attenzione: se possibile, non ricaricare o spegnere e riaccendere manualmente il router prima di aver rac le informazioni sopra indicate, in quanto ciò potrebbe causare la perdita di informazioni importanti necess per determinare la causa principale del problema.

Informazioni correlate

- Risoluzione dei problemi di blocco del router
- Recupero delle informazioni dal file crashinfo
- Creazione di dump di anima
- Risoluzione dei problemi relativi alla memoria
- Supporto tecnico – Cisco Systems