Software-erzwungene Abstürze verstehen

Inhalt

Einführung

In diesem Dokument werden die häufigsten Ursachen für Software-erzwungene Abstürze erläutert und die Informationen beschrieben, die Sie zur Fehlerbehebung sammeln müssen. Wenn Sie eine TAC-Serviceanfrage für einen softwareerzwungenen Absturz erstellen, sind die Informationen, die Sie sammeln müssen, für die Lösung des Problems unerlässlich.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten folgende Themen kennen:

- So beheben Sie Router-Abstürze.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Ein softwareerzwungener Absturz tritt auf, wenn der Router einen schwerwiegenden, nicht

behebbaren Fehler erkennt und sich selbst neu lädt, sodass er keine beschädigten Daten überträgt. Ein Großteil der Software-erzwungenen Abstürze wird durch Cisco IOS® Softwarefehler verursacht, obwohl einige Plattformen (wie der alte Cisco 4000) ein Hardwareproblem als softwareerzwungener Ausfall melden können.

Wenn Sie den Router nicht aus- und wieder eingeschaltet oder manuell neu geladen haben, wird in der Ausgabe des Befehls **show version** Folgendes angezeigt:

```
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
```

Wenn der Befehl **show version** von Ihrem Cisco Gerät ausgegeben wird, können Sie mit dem Cisco CLI Analyzer (nur registrierte Kunden) potenzielle Probleme und Bugfixes anzeigen.

Mögliche Ursachen

In dieser Tabelle werden mögliche Gründe für Software-erzwungene Abstürze erläutert:

Grund	Erläuterung

Watchdog-Zeitüberschreitungen	Der Prozessor verwendet Timer, um unbegrenzte Schleifen zu vermeide und führt dazu, dass der Router nicht mehr reagiert. Im Normalbetrieb se die CPU diese Timer in regelmäßigen Abständen zurück. Andernfalls wir System neu geladen. Überwachungs-Timeouts, die als Software-erzwun Abstürze gemeldet werden, sind softwarebezogen. Informationen zu and Arten von Überwachungs-Timeouts finden Sie unter Fehlerbehebung be Watchdog-Zeitüberschreitungen. Das System war vor dem Neuladen in Schleife stecken geblieben. Daher ist die Stapelüberwachung nicht unbe relevant. Diese Art von softwareerzwungenem Absturz kann in folgender Zeilen der Konsolenprotokolle erkannt werden:
	`%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec`
	
	`and`
	
	`*** System received a Software forced crash ***`
	`signal = 0x17, code = 0x24, context= 0x60ceca60`

Geringer Speicher	Wenn ein Router zu wenig Arbeitsspeicher beansprucht, kann er sich schließlich selbst neu laden und als softwareerzwungener Absturz melde diesem Fall werden Fehlermeldungen zu Speicherzuweisungsfehlern in Konsolenprotokollen angezeigt:
	`%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC8`
	`pool Processor, alignment 0`

Beschädigtes Software-Image	Beim Hochfahren kann ein Router erkennen, dass ein Cisco IOS-Softwa Image beschädigt ist, die `komprimierte Image-Prüfsumme als falsche` Nach zurückgeben und versuchen, erneut zu laden. In diesem Fall wird das Ereignis als softwareerzwungener Absturz gemeldet.
	`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`
	
	Dies kann durch ein Cisco IOS Software-Image verursacht werden, das

Andere Fehler	während der Übertragung zum Router beschädigt wurde. In diesem Fall können Sie ein neues Image auf den Router laden, um das Problem zu beheben. [Eine ROMMON-Wiederherstellungsmethode für Ihre Plattform finden Sie im ROMmon Recovery Procedure for the Cisco 7200, 7300, 7 7500, RSP700, Catalyst 5500 RSM, uBR7100, uBR7. Router der Serien uBR10000 und 12000.] Dies kann auch auf fehlerhafte Speicherhardwar oder einen Softwarefehler zurückzuführen sein. Die Fehler, die Abstürze verursachen, werden häufig von der Prozessorhardware erkannt, die automatisch einen speziellen Fehlerbehandlungscode im ROM-Monitor aufruft. Der ROM-Monitor erke den Fehler, gibt eine Meldung aus, speichert Informationen zum Fehler u startet das System neu. Es gibt Abstürze, bei denen nichts davon passie kann (siehe Watchdog-Zeitüberschreitungen), und es gibt Abstürze, bei die Software das Problem erkennt und die Crashdump-Funktion aufruft. ist ein echter "softwareerzwungener" Crash. Auf Power PC-Plattformen i "Software-erzwungener Crash" nicht der Grund für den Neustart, der ausgegeben wird, wenn die Crashdump-Funktion aufgerufen wird - zumi bis vor kurzem. Auf diesen Plattformen (vor Version 12.2(12.7) der Cisco Software) werden diese als "SIGTRAP"-Ausnahmen bezeichnet. Auf alle andere Weise sind SIGTRAPs und SFCs identisch.

Fehlerbehebung

Software-erzwungene Abstürze werden in der Regel durch Cisco IOS Software-Fehler verursacht. Wenn Fehlermeldungen bei der Speicherzuweisung in den Protokollen vorhanden sind, finden Sie weitere Informationen unter Beheben von Speicherproblemen.

Wenn Sie keine Fehlermeldungen zur Speicherzuweisung sehen und den Router nach dem Software-erzwungenen Absturz nicht manuell neu geladen oder neu gestartet haben, ist der Cisco CLI Analyzer (nur registrierte Kunden) das beste Tool, um nach einer bekannten übereinstimmenden Bug-ID zu suchen. Dieses Tool enthält die Funktionen des alten Stack Decoder-Tools.

Beispiel:

1. Erfassen Sie die Ausgabe des **Show-Stacks** vom Router.
2. Rufen Sie das Cisco CLI Analyzer-Tool auf (nur registrierte Kunden).
3. Wählen Sie **im** Dropdown-Menü die Option **Stapel anzeigen** aus.
4. Fügen Sie die von Ihnen gesammelte Ausgabe ein.
5. Klicken Sie auf **Senden**.Wenn die decodierte Ausgabe des Befehls **show stack** mit einem bekannten Softwarefehler übereinstimmt, erhalten Sie die Bug-IDs der wahrscheinlichsten Softwarefehler, die den Software-erzwungenen Absturz verursacht haben könnten.
6. Klicken Sie auf die Bug-ID-Hyperlinks, um weitere Bug-Details aus dem Cisco Bug Toolkit anzuzeigen (nur registrierte Kunden), mit dem Sie die richtige Bug-ID ermitteln können.

Wenn Sie eine Fehler-ID gefunden haben, die zu Ihrem Fehler passt, können Sie im Feld "behoben in" die erste Version der Cisco IOS-Software bestimmen, die die Behebung des Fehlers enthält.

Wenn Sie sich hinsichtlich der Bug-ID oder der Cisco IOS-Softwareversion, die die Behebung des Problems enthält, nicht sicher sind, aktualisieren Sie Ihre Cisco IOS-Software auf die neueste Version in Ihrem Release Train. Dies ist hilfreich, da die neueste Version Fixes für eine große

Anzahl von Bugs enthält. Auch wenn das Problem dadurch nicht gelöst werden kann, ist die Fehlermeldung und der Lösungsprozess einfacher und schneller, wenn Sie die neueste Version der Software haben.

Wenn Sie nach der Verwendung des Cisco CLI Analyzer entweder einen Fehler vermuten oder einen Fehler festgestellt haben, der noch nicht behoben ist, empfehlen wir Ihnen, eine TAC-Serviceanfrage zu öffnen, um zusätzliche Informationen zur Behebung des Fehlers bereitzustellen und eine schnellere Benachrichtigung zu erhalten, wenn der Fehler letztendlich behoben ist.

Konfigurationsverfahren

Wenn das Problem als neuer Softwarefehler identifiziert wird, kann ein Cisco TAC-Techniker den Router so konfigurieren, dass er einen *Core Dump* sammelt. Manchmal wird ein Core Dump benötigt, um zu ermitteln, was zur Behebung des Softwarefehlers getan werden kann.

Um weitere nützliche Informationen im Core Dump zu sammeln, empfehlen wir die Verwendung des Befehls **Debugsanity**. Dies bewirkt, dass jeder im System verwendete Puffer bei der Zuweisung und bei der Freigabe ordnungsgemäß überprüft wird. Der Befehl **debug sanity** muss im privilegierten EXEC-Modus (Aktivierungsmodus) ausgegeben werden und umfasst eine gewisse CPU, hat jedoch keine signifikanten Auswirkungen auf die Funktionalität des Routers. Wenn Sie die Überprüfung der Integrität deaktivieren möchten, verwenden Sie den Befehl **undebug sanity** privileged EXEC.

Bei Routern mit maximal 16 MB Hauptspeicher können Sie das Trivial File Transfer Protocol (TFTP) verwenden, um den Core Dump zu sammeln. Es wird empfohlen, File Transfer Protocol (FTP) zu verwenden, wenn der Router über mehr als 16 MB Hauptspeicher verfügt. Verwenden Sie die Konfigurationsverfahren in diesem Abschnitt. Alternativ können Sie unter Erstellen von Core-Dumps nachlesen.

Gehen Sie wie folgt vor, um Ihren Router zu konfigurieren:

1. Konfigurieren Sie den Router mit dem Befehl **configure terminal**.
2. Geben Sie **exception dump n.n.n.n** ein, wobei n.n.n.n die IP-Adresse des TFTP-Server-Hosts (Trivial File Transfer Protocol) ist.
3. Beenden Sie den Konfigurationsmodus.

TFTP-Server-Hostkonfigurationsverfahren

Gehen Sie wie folgt vor, um einen TFTP-Server-Host zu konfigurieren:

1. Erstellen Sie mithilfe eines Editor Ihrer Wahl eine Datei im Verzeichnis /tftpboot auf dem Remotehost. Der Dateiname ist der Hostname-Core des Cisco Routers.
2. Ändern Sie auf UNIX-Systemen den Berechtigungsmodus der Datei "hostname-core" als global kompatibel (666). Sie können die TFTP-Konfiguration über den Befehl **copy running-config tftp** in dieser Datei überprüfen.
3. Stellen Sie sicher, dass Sie mehr als 16 MB freien Speicherplatz unter /tftpboot haben.Wenn das System abstürzt, erstellt der Befehl **exception dump** seine Ausgabe in der oben genannten Datei. Wenn der Router über mehr als 16 MB Hauptspeicher verfügt, können Sie den Core-Dump über File Transfer Protocol (FTP) oder Remote Copy Protocol (RCP) erstellen. Konfigurieren Sie auf dem Router Folgendes:

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

Wenn Sie einen Core Dump gesammelt haben, laden Sie ihn auf ftp://ftp-sj.cisco.com/incoming hoch (geben Sie in UNIX **pftp ftp-sj.cisco.com** und anschließend **cd incoming** ein), und benachrichtigen Sie den Besitzer Ihres Falls und fügen Sie den Dateinamen ein.

Informationen, die beim Öffnen einer TAC-Serviceanfrage gesammelt werden müssen

Wenn Sie nach den oben beschriebenen Schritten zur Fehlerbehebung weiterhin Hilfe benötigen und eine Serviceanfrage beim Cisco TAC erstellen möchten, geben Sie folgende Informationen an:

- Ausgabe **des technischen Supports anzeigen** - In der Ausgabe des Befehls **show technical-support** fi Sie Informationen zum aktuellen Status des Routers sowie wichtige Informationen, die vom Router vo einem Absturz gespeichert werden.
- Konsolenprotokolle - Die Konsolenprotokolle, die häufig auf einem Syslog-Server gespeichert werden können nützliche Informationen über die Ereignisse bereitstellen, die auf dem Router vor einem Abstu auftreten. Diese Hinweise sind oft die wichtigsten Informationen, die Sie sammeln können.
- crashinfo-Datei (falls vorhanden) - Cisco empfiehlt, eine Cisco IOS-Softwareversion zu verwenden, d Crashinfo-Funktion unterstützt, um die Fehlerbehebung erfolgreich durchzuführen. Hierfür muss die Version die anderen Anforderungen Ihres Netzwerks erfüllen. Unter Abrufen von Informationen aus d Crashinfo-Datei oder Verwendung des Software Advisor (nur registrierte Kunden)-Tools finden Sie ei Cisco IOS-Softwareversion, die die Crashinfo-Funktion unterstützt. Ein potenzieller Bonus besteht da dass bei älteren Versionen der Cisco IOS-Software die neueren IOS-Softwareversionen, die diese Funktion unterstützen, Ihren Fehler bereits korrigieren können.

Um Informationen zu Ihrer Serviceanfrage hinzuzufügen, laden Sie sie über das TAC Service Request To hoch (nur registrierte Kunden). Wenn Sie nicht auf das TAC Service Request Tool zugreifen können, kön Sie die Informationen in einem E-Mail-Anhang an attach@cisco.com senden, der Ihre Fallnummer in der Betreffzeile Ihrer Nachricht enthält.

Vorsicht: Laden Sie den Router nicht manuell neu oder schalten Sie ihn ein, bevor Sie die oben genannte Informationen sammeln, wenn möglich, da dies dazu führen kann, dass wichtige Informationen verloren g die zur Bestimmung der Ursache des Problems erforderlich sind.

Zugehörige Informationen

- Fehlerbehebung bei Router-Abstürzen
- Abrufen von Informationen aus der Crashinfo-Datei
- Core-Dumps erstellen
- Fehlerbehebung bei Speicherfehlern
- Technischer Support - Cisco Systems