Begrijp softwaregedwongen crashes

Inhoud

Inleiding

Dit document verklaart de meest voorkomende oorzaken van softwaregedwongen crashes en beschrijft de informatie die u moet verzamelen om een oplossing te vinden. Als u een TAC-serviceaanvraag opent voor een softwaregedwongen crash, is de informatie die u moet verzamelen essentieel om het probleem op te lossen.

Voorwaarden

Vereisten

Lezers van dit document zouden kennis moeten hebben van deze onderwerpen:

- Hoe problemen oplossen bij routercrashes.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Een software-geforceerde krach komt voor wanneer de router een ernstige, niet-herstelbare fout

detecteert en zichzelf herlaadt zodat het gecorrumpeerde gegevens niet kan verzenden. Een grote meerderheid van software-geforceerde crashes worden veroorzaakt door softwarebugs van Cisco IOS, hoewel sommige platforms (zoals het oude Cisco 4000) een hardwareprobleem kunnen melden als een software-geforceerde crash.

Als u de router niet hebt uitgeladen of handmatig opnieuw geladen, geeft uitvoer uit het opdracht **show versie** dit weer:

```
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
```

Als u de uitvoer hebt van een opdracht **show versie** van uw Cisco-apparaat, kunt u Cisco CLI Analyzer gebruiken (alleen geregistreerde klanten) om potentiële problemen en oplossingen weer te geven.

Mogelijke oorzaken

In deze tabel worden de mogelijke redenen voor softwaregedwongen crashes uitgelegd:

reden	verklaring

Time-out Watchdog	De processor gebruikt timers om oneindige loops te voorkomen en zorgt ervoor dat d router niet meer reageert. Bij normaal gebruik stelt de CPU deze timers regelmatig opnieuw in. Wanneer u dit niet doet, wordt het systeem opnieuw geladen. Uitgangspunten van Watchdog die worden gemeld als softwaregedwongen crashes software-gerelateerd. Raadpleeg de Time-outs voor probleemoplossing bij Watchdog voor informatie over andere soorten wachthondetijden. Het systeem zat vast in een l voor de herlading. Daarom is het stapelspoor niet noodzakelijk relevant. U kunt dit ty software-geforceerde krach in deze lijnen van de console herkennen:
	`%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec`
	`and`
	`*** System received a Software forced crash ***`
	`signal = 0x17, code = 0x24, context= 0x60ceca60`

Laag geheugen	Wanneer een router te laag op geheugen loopt, kan het zichzelf uiteindelijk opnieuw laden en het rapporteren als een software-gedwongen crash. In dit geval verschijnen foutmeldingen met de fout in de geheugentoewijzing in de console-logbestanden:
	`%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84,`
	`pool Processor, alignment 0`

Software-afbeelding corrumperen	Tijdens het opstarten kan een router detecteren dat een Cisco IOS-softwarebeeld beschadigd is, de `gecomprimeerde checksum van het beeld` teruggeven `als onjuist` beri en proberen het opnieuw te laden. In dit geval wordt de gebeurtenis gemeld als een software gedwongen crash.
	`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`
	Dit kan door een Cisco IOS softwarebeeld worden veroorzaakt dat eigenlijk tijdens overdracht naar de router gecorrumpeerd is. In dit geval kunt u een nieuw beeld op d router laden om het probleem op te lossen. [Raadpleeg voor een ROMMON-

Andere fouten	herstelmethode voor uw platform de RSP7000, Catalyst 5500, Cisco 7300, 7400, 75 RSP7000, Catalyst 5500 RSM, uBR7100, uBR72 00, uBR10000 en 12000 Series routers.] Het kan ook worden veroorzaakt door defecte geheugen hardware of een softwarebug. De fouten die crashes veroorzaken worden vaak door de hardware van de processo gedetecteerd, die automatisch speciale fout-verwerkingscode in de ROM monitor aanroept. De ROM monitor identificeert de fout, drukt een bericht af, slaat informatie over de fout op en start het systeem opnieuw. Er zijn crashes waarin dit niet kan gebeuren (zie Watchdog timeouts), en er zijn crashes waarin de software het proble detecteert en de crashstortfunctie aanroept. Dit is een ware "software-gedwongen" crash. Op Power PC-platforms is "software-forced crashen" niet de hernieuwde rede die werd afgedrukt wanneer de crashstortfunctie wordt aangeroepen, althans tot zee onlangs. Op die platforms (voorafgaand aan Cisco IOS-softwarerelease 12.2(12.7)) worden deze 'SIGTRAP'-uitzonderingen genoemd. Op alle andere manieren zijn SIGTRAP's en SFC's hetzelfde.

Problemen oplossen

Softwaregedwongen crashes worden normaal gesproken veroorzaakt door Cisco IOS-softwarebugs. Als de foutmeldingen met betrekking tot de toewijzing van het geheugen in de logs voorkomen, zie Problemen oplossen.

Als u geen foutmeldingen ziet met betrekking tot de toewijzing van geheugen, en u de router na de door de software geforceerde crash niet handmatig hebt hergeladen of op stroom hebt gericht, is het beste gereedschap dat u kunt gebruiken de Cisco CLI Analyzer (alleen geregistreerde klanten) om een bekende bug-ID op te zoeken. Dit gereedschap bevat de functionaliteit van het oude Stack Decoder-gereedschap.

Voorbeeld:

1. Verzamel de output van **show stapel** van de router.
2. Ga naar het Cisco CLI Analyzer-gereedschap (alleen geregistreerde klanten).
3. Selecteer **Stack** uit het keuzemenu tonen.
4. Plakt in de output die u hebt verzameld.
5. Klik op **Insturen**.Als de gedecodeerde output van de opdracht **Show stack** overeenkomt met een bekend softwarebug, ontvangt u de bug ID's van de meest waarschijnlijke software-afluisterapparatuur die de door software geforceerde crash had kunnen veroorzaken.
6. Klik op de hyperlinks van de bug-ID om extra bug-details van de Cisco Bug Toolkit te bekijken (alleen geregistreerde klanten) die u kan helpen de juiste overeenkomende bug-ID te bepalen.

Wanneer u een bug-ID hebt geïdentificeerd die bij uw fout past, raadpleegt u het veld "vast in" om de eerste Cisco IOS-softwareversie te bepalen die de oplossing voor het probleem bevat.

Als u onzeker bent over de bug-ID of de Cisco IOS-softwareversie die de oplossing voor het probleem bevat, upgrade uw Cisco IOS-software op de nieuwste versie in uw releasetrein. Hierdoor bevat de laatste versie oplossingen voor een groot aantal insecten. Zelfs als dit probleem niet opgelost is, is de bug-rapportage en het resolutieproces eenvoudiger en sneller wanneer u de nieuwste versie van de software hebt.

Als u de Cisco CLI Analyzer hebt gebruikt, vermoeden of hebben u positief een bug geïdentificeerd die onopgelost blijft, raden we u aan een TAC-serviceaanvraag te openen om

extra informatie te leveren om de bug op te lossen en voor sneller bericht wanneer de bug uiteindelijk wordt opgelost.

Configuratieprocedures

Als het probleem wordt geïdentificeerd als een nieuw softwarebug, kan een Cisco TAC-ingenieur vragen om u de router te configureren om een *kernstop* te verzamelen. Er is soms een kernstop nodig om te bepalen wat er kan worden gedaan om de softwarebug te repareren.

Om bruikbaarder informatie op het kernafval te verzamelen, raden we u aan de verborgen opdracht voor het **zuiveren** van de hygiëne te gebruiken. Dit zorgt ervoor dat elke buffer die in het systeem wordt gebruikt, op zijn gezondheid wordt gecontroleerd wanneer hij wordt toegewezen en wanneer hij wordt vrijgelaten. Het bevel **om** de **hygiëne te zuiveren** moet in bevoorrechte EXEC modus worden verleend (laat modus toe) en heeft enige CPU's bij, maar heeft geen significante invloed op de functionaliteit van de router. Als u controles op de reiniging wilt uitschakelen, gebruikt u de opdracht **ongedekte** hygiëne, bevoorrechte EXEC-opdracht.

Voor routers met 16 MB of minder hoofdgeheugen kunt u triviaal File Transfer Protocol (TFTP) gebruiken om de kernvuilnisbelt te verzamelen. Aanbevolen wordt om File Transfer Protocol (FTP) te gebruiken als de router meer dan 16 MB aan hoofdgeheugen heeft. Gebruik de configuratieprocedures in dit hoofdstuk. Raadpleeg ook de Core Dumps.

Voltooi deze stappen om uw router te configureren:

1. Configureer de router met de opdracht **configureerbare terminal**.
2. Type **exceptionele stortplaats n.n.n**, waar n.n.n.n het IP adres is van de Remote Trial File Transfer Protocol (TFTP) serverhost.
3. Sluit de configuratie-modus.

TFTP-serverhostconfiguratieprocedure

Voltooi deze stappen om een TFTP-serverhost te configureren:

1. Maak een bestand onder de /tftpaars folder op de afstandsbediening met behulp van een redacteur van uw keuze. De bestandsnaam is de Cisco router hostname-core.
2. Op UNIX systemen, verander de machtigingsmodus van het "hostname-core" bestand om mondiaal compatibel te zijn (666). U kunt de TFTP-instelling controleren door de opdracht van de **kopie in werking stellen-configuratie** van dat bestand.
3. Zorg ervoor dat u meer dan 16 MB vrije schijfruimte hebt onder /tftpstart.Als het systeem crasht, creëert de opdracht **voor** het **dumpen** van de **uitzondering** de uitvoer naar het bovenstaande bestand. Als de router meer dan 16 MB aan hoofdgeheugen heeft, kunt u File Transfer Protocol (FTP) of Remote Copy Protocol (RCP) gebruiken om de kernstop te zetten. Op de router, moet u dit configureren:

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

   Wanneer u een basisstortplaats hebt verzameld, uploadt u het naar ftp://ftp-sj.cisco.com/incoming (in UNIX, type **pftp ftp ftp-sj.cisco.com** en dan **cd inkomend**), stelt u de eigenaar van uw case in kennis en voegt u de bestandsnaam toe.

Te verzamelen informatie als u een TAC-serviceaanvraag opent

Als u nog steeds hulp nodig hebt nadat u de bovenstaande stappen voor het oplossen van problemen he gevolgd en u een servicetoepassing wilt maken met de Cisco TAC, zorg er dan voor dat u de volgende informatie bevat:

- **Toont** uitvoer van **technische ondersteuning** - De uitvoer van de **show Technical-support** opdracht ge informatie over de huidige status van de router, en ook belangrijke informatie die door de router is opgeslagen voor een crash.
- Logboeken van de console - de console logt, vaak uitgespaard aan een syslog server, kan waardevo informatie over de gebeurtenissen verstrekken die op de router vóór een ongeluk voorkomen. Deze aanwijzingen zijn vaak de belangrijkste informatie die je kunt verzamelen.
- crashinformatie-bestand (indien aanwezig) - Cisco raadt u aan een Cisco IOS-softwarerelease te gebruiken die de crashinformatie-functie ondersteunt om probleemoplossing met succes te kunnen oplossen. Hiervoor moet de versie voldoen aan de andere behoeften van uw netwerk. Zie Informatie ophalen uit het crashinformatie-bestand of het softwareadviseur gebruiken (alleen geregistreerde kla om een Cisco IOS-softwareversie te vinden die de crashinformatie-functie ondersteunt. Een mogelijk bonus is dat als u een oudere versie van Cisco IOS-software hebt, de nieuwere IOS-softwarereleases deze functie ondersteunen, uw bug al kunnen hebben gerepareerd.

Om informatie aan uw servicetoepassing toe te voegen, kunt u deze uploaden via het TAC Service Applic Tool (alleen geregistreerde klanten). Als u geen toegang hebt tot de TAC Service Application Tool, kunt u informatie in een e-mailbijlage naar attach@cisco.com sturen met uw casenummer in de onderwerpregel uw bericht.

Voorzichtig: Laad de router niet handmatig opnieuw of gebruik het programma niet voordat u de bovensta informatie verzamelt, indien mogelijk, omdat dit belangrijke informatie kan veroorzaken om verloren te ga nodig is om de oorzaak van het probleem te bepalen.

Gerelateerde informatie

- Routercrashes voor probleemoplossing
- Informatie uit het crashinformatie-bestand ophalen
- Core-dumpen
- Problemen oplossen
- Technische ondersteuning - Cisco-systemen