Compreender travamentos forçados por software

Contents

Introduction

Este documento explica as causas mais frequentes de travamentos forçados por software e descreve as informações que precisam ser coletadas para resolver problemas. Se você abrir uma solicitação de serviço ao TAC de um travamento forçado por software, as informações que serão solicitadas para serem coletadas serão essenciais para resolver o problema.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

- Como Solucionar Problemas de Travamentos do Roteador.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Conventions

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

Um travamento forçado por software ocorre quando o roteador detecta um erro grave e irrecuperável e se recarrega para que não transmita dados corrompidos. A grande maioria dos travamentos forçados por software são causados por bugs do software Cisco IOS®, embora

algumas plataformas (como o antigo Cisco 4000) possam relatar um problema de hardware como um travamento forçado por software.

Se você não tiver desligado ou recarregado manualmente o roteador, a saída do comando **show version** exibirá:

```
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 você tiver a saída de um comando **show version** de seu dispositivo Cisco, poderá usar o Cisco CLI Analyzer (somente clientes registrados) para exibir problemas e correções potenciais.

Possíveis causas

Esta tabela explica os possíveis motivos para travamentos forçados por software:

Razão	Explicação

Intervalos de vigilante	O processador usa temporizadores para evitar loops infinitos e faz com que o roteador pare c responder. Em operação normal, a CPU reinicia esses temporizadores em intervalos regulare Se isso não for feito, o sistema será recarregado. Os tempos limite de vigia relatados como travamentos forçados por software são relacionados ao software. Consulte Troubleshooting c Timeouts de Watchdog para obter informações sobre outros tipos de timeouts de watchdog. sistema estava preso em um loop antes da reinicialização. Portanto, o rastreamento da pilha não é necessariamente relevante. Você pode reconhecer esse tipo de travamento forçado po software nessas linhas dos registros do console:
	`%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec`
	`and`
	`*** System received a Software forced crash ***`
	`signal = 0x17, code = 0x24, context= 0x60ceca60`

Memória insuficiente	Quando um roteador é executado com memória muito baixa, ele pode eventualmente se recarregar e relatá-lo como um travamento forçado por software. Nesse caso, as mensagens erro de falha de alocação de memória aparecem nos registros do console:
	`%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84,`
	`pool Processor, alignment 0`

Imagem de software corrompida	No momento da inicialização, um roteador pode detectar que uma imagem do software Cisco IOS está corrompida, retornar a `soma de verificação da imagem compactada está incorreta` e te recarregar. Nesse caso, o evento é relatado como um travamento forçado 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`
	Isso pode ser causado por uma imagem do software Cisco IOS que foi corrompida durante a transferência para o roteador. Nesse caso, você pode carregar uma nova imagem no roteado para resolver o problema. [Para obter um método de recuperação de ROMMON para sua plataforma, consulte Procedimento de Recuperação de ROMmon para o Cisco 7200, 7300, 7400, 7500, RSP7000, Catalyst 5500 RSM, uBR7100, uBR720 0, uBR10000 e 12000 Series Routers.] Também pode ser causado por hardware de memória defeituoso ou por um bug de software.

Outras falhas	Os erros que causam travamentos são frequentemente detectados pelo hardware do processador, que automaticamente chama um código especial de manipulação de erros no monitor da ROM. O monitor de ROM identifica o erro, imprime uma mensagem, salva informações sobre a falha e reinicia o sistema. Há travamentos nos quais nada disso pode acontecer (consulte timeouts de Watchdog), e há travamentos nos quais o software detecta o problema e chama a função crashdump. Este é um verdadeiro travamento "forçado por software. Nas plataformas Power PC, "travamento forçado por software" não é o motivo de reinicialização impresso quando a função de despejo é chamada - pelo menos até muito recentemente. Nessas plataformas (anteriores ao Cisco IOS Software versão 12.2[12.7]), ess travamentos são conhecidos como exceções "SIGTRAP". De todas as outras maneiras, SIGTRAPs e SFCs são iguais.

Troubleshoot

Os travamentos forçados pelo software são normalmente causados por bugs do Cisco IOS Software. Se houver mensagens de erro de falha de alocação de memória nos registros, consulte Solução de problemas de memória.

Se você não vir mensagens de erro de falha de alocação de memória e não tiver recarregado ou desligado manualmente o roteador após o travamento forçado pelo software, a melhor ferramenta que você pode usar é o Cisco CLI Analyzer (clientes registrados somente) para procurar por um ID de erro correspondente conhecido. Essa ferramenta incorpora a funcionalidade da antiga ferramenta Stack Decoder.

Exemplo:

1. Colete a saída de **show stack** do roteador.
2. Vá para a ferramenta Cisco CLI Analyzer (somente clientes registrados).
3. Selecione **show stack** no menu suspenso.
4. Colar na saída coletada.
5. Clique em Submit.Se a saída decodificada do comando **show stack** corresponder a um bug de software conhecido, você receberá os IDs dos bugs de software mais prováveis que podem ter causado o travamento forçado por software.
6. Clique nos hiperlinks de ID de bug para exibir detalhes adicionais de bug do Cisco Bug Toolkit (somente clientes registrados) que podem ajudá-lo a determinar a correspondência correta de ID de bug.

Quando você tiver identificado um ID de bug que corresponde ao seu erro, consulte o campo "corrigido em" para determinar a primeira versão do software Cisco IOS que contém a correção do bug.

Se você não tiver certeza sobre o ID do bug ou sobre a versão do software Cisco IOS que contém a correção para o problema, atualize o software Cisco IOS para a versão mais recente na sua versão de treinamento. Isso ajuda porque a versão mais recente contém correções para um grande número de bugs. Mesmo que isso não resolva o problema, a geração de relatórios de bugs e o processo de resolução são mais simples e rápidos quando você tem a versão mais recente do software.

Se, depois de usar o Cisco CLI Analyzer, você suspeitar ou tiver identificado positivamente um bug que permanece por resolver, recomendamos que você abra uma solicitação de serviço TAC para fornecer informações adicionais para ajudar a resolver o bug e para uma notificação mais rápida quando o bug for finalmente resolvido.

Procedimentos de configuração

Se o problema for identificado como um novo bug de software, um engenheiro do Cisco TAC poderá solicitar que você configure o roteador para coletar um *dump central*. Às vezes, é necessário um dump central para identificar o que pode ser feito para corrigir o bug do software.

Para coletar mais informações úteis no dump central, recomendamos que você use o comando oculto **debug sanity**. Isso faz com que cada buffer usado no sistema tenha sua sanidade verificada quando alocado e quando liberado. O comando **debug sanity** deve ser emitido no modo EXEC privilegiado (modo enable) e envolve alguma CPU, mas não afeta significativamente a funcionalidade do roteador. Se desejar desabilitar a verificação de sanidade, use o comando EXEC privilegiado **undebug sanity**.

Para roteadores que tenham 16 MB ou menos de memória principal, use o Protocolo de Transferência de Ficheiro Trivial (TFTP) para coletar o dump central. Recomendamos que você use o FTP (Protocolo de transferência de arquivos) se o roteador tiver mais de 16 MB de memória principal. Use os procedimentos de configuração nesta seção. Como alternativa, consulte Criando lixos principais.

Conclua estes passos para configurar seu roteador:

1. Configure o roteador com o comando **configure terminal**.
2. Digite **exception dump n.n.n.n**, onde n.n.n.n é o endereço IP do host do servidor TFTP (Trivial File Transfer Protocol) remoto.
3. Sair do modo de configuração.

Procedimento de configuração do host de servidor de TFTP

Conclua estes passos para configurar um host de servidor TFTP:

1. Crie um arquivo no diretório /tftpboot no host remoto com a ajuda de um editor de sua escolha. O nome do arquivo é o nome do host central do roteador Cisco.
2. Em sistemas UNIX, altere o modo de permissão do arquivo hostname-core para que seja globalmente compatível (666). Você pode verificar a configuração do TFTP por meio do comando **copy running-config tftp** nesse arquivo.
3. Verifique se você tem mais de 16 MB de espaço livre em disco em /tftpboot.Se o sistema travar, o comando exception dump cria sua saída para o arquivo acima. Se o roteador tiver mais de 16 MB de memória principal, use o File Transfer Protocol (FTP) ou o Remote Copy Protocol (RCP) para obter o dump central. No roteador, configure isto:

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

   Quando tiver coletado um dump central, faça o upload para ftp://ftp-sj.cisco.com/incoming (no UNIX, digite **pftp ftp-sj.cisco.com** e, em seguida, **cd incoming**), notifique o proprietário do seu caso e inclua o nome do arquivo.

Informações a serem coletadas se você abrir um pedido de serviço de TAC

Se você ainda precisar de assistência após seguir as etapas de solução de problemas acima e quiser cri uma solicitação de serviço com o Cisco TAC, inclua as seguintes informações:

- saída **show technical-support** - A saída do comando **show technical-support** fornece informações sob estado atual do roteador e também informações importantes armazenadas pelo roteador antes de ur travamento.
- Logs de console - Os registros de console, geralmente salvos em um servidor syslog, podem fornece informações valiosas sobre os eventos que ocorrem no roteador antes de um travamento. Essas dica costumam ser as informações mais importantes que você consegue coletar.
- arquivo crashinfo (se presente) - A Cisco recomenda que você use uma versão do software Cisco IO que suporte o recurso crashinfo para solucionar problemas com êxito. Para isso, a versão deve aten às outras necessidades da sua rede. Consulte Recuperando informações do arquivo Crashinfo ou us ferramenta Software Advisor (somente clientes registrados) para localizar uma versão do software C IOS que suporte o recurso crashinfo. Um possível bônus é que se você tiver uma versão mais antiga software Cisco IOS, as versões mais recentes do software IOS que suportam esse recurso já poderia ter seu bug corrigido.

Para anexar informações à sua solicitação de serviço, faça o upload através da TAC Service Request To (somente clientes registrados) . Se não conseguir acessar a TAC Service Request Tool, você poderá env as informações em um anexo de e-mail para attach@cisco.com com o número do caso na linha de assu sua mensagem.

Cuidado: Não recarregue manualmente ou desligue e ligue o roteador antes de coletar as informações a se possível, pois isso pode causar a perda de informações importantes necessárias para determinar a ca raiz do problema.

Informações Relacionadas

- Troubleshooting de Travamentos de Roteador
- Obtendo informações a partir do arquivo de informação de travamento
- Criando dumps centrais
- Troubleshooting Problemas de Memória
- Suporte Técnico - Cisco Systems