

Troubleshooting de Timeouts de Watchdog

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Identificar tempos limite de vigia](#)

[Troubleshoot](#)

[Intervalo de vigilante do software](#)

[Intervalo de vigilante do processo](#)

[Mensagens de erro relacionadas ao tempo limite do vigia](#)

[Informações a serem coletadas se você abrir um pedido de serviço de TAC](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a causa dos Tempos limite do Watchdog em roteadores Cisco e explica como resolvê-los.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes destes tópicos:

- [Troubleshooting de Travamentos de Roteador](#)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Todos os Cisco Routers
- Todas as versões de software Cisco IOS®

Observação: este documento não se aplica a switches Cisco Catalyst ou plataformas MGX, mas somente a roteadores Cisco.

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](#).

Identificar tempos limite de vigia

Os processadores Cisco possuem cronômetros que protegem contra determinados tipos de suspensões. A CPU reinicia periodicamente um cronômetro de vigilante. O cronômetro de vigilante basicamente controla o tempo de cada processo. Se o cronômetro não for reiniciado, uma armadilha ocorre. Se um processo for maior do que deve ser, o temporizador watchdog é usado para escapar desse processo.

Isso só ocorre se algo der errado. Com base na situação, o roteador pode se redefinir ou se recuperar da falha e gerar uma mensagem de erro nos registros do console, que se parece com isto:

```
*** Watch Dog Timeout ***
```

```
PC = 0x6022536C, SP = 0x00000000
```

or

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec
```

```
*** System received a Software forced crash ***
```

```
signal = 0x17, code = 0x24, context= 0x60ceca60
```

Se você não executar o ciclo de energia ou recarregar manualmente o roteador, a saída do comando [show version será semelhante a esta:](#)

```
Router#show version
```

```
...
```

```
Router uptime is 1 hour, 47 minutes
```

```
System restarted by watchdog timer expired at 09:26:24 UTC Mon Mar 27 2000
```

```
System image file is "flash:c3640-is-mz.113-7-T.bin", booted via flash
```

```
...
```

Se você tiver a saída de um comando **show version** de seu dispositivo Cisco, poderá usar o [Cisco CLI Analyzer](#) para exibir possíveis problemas e correções. Para usar o [Cisco CLI Analyzer](#), você deve ser um [cliente registrado, estar conectado e com o JavaScript habilitado](#).

Troubleshoot

A causa-raiz do timeout do watchdog pode estar relacionada a hardware ou software. Estes são os sintomas comuns através dos quais você pode identificar a origem do problema:

- Se um roteador que está operante corretamente há meses começa a recarregar a cada 20 minutos, ou se é reinicializado continuamente e você não pode mais acessá-lo, o problema provavelmente está relacionado ao hardware. Esse também é o caso se um novo módulo tiver sido instalado recentemente e o roteador travar pelo timeout do watchdog posteriormente.
- Se o roteador começar a travar após uma alteração de configuração ou uma alteração na versão do software Cisco IOS, provavelmente é um problema relacionado ao software.

A primeira etapa para solucionar esse tipo de problema é identificar o tipo de tempo limite do watchdog que você encontra. Há dois tipos de Timeouts de Watchdog:

- O Software Watchdog Timeout, que, apesar do nome, sempre está relacionado ao hardware
- O timeout de vigilante do processo, que em geral é relativo ao software

Intervalo de vigilante do software

Esse tempo limite é causado por um loop infinito no nível de interrupção ou por um problema de hardware. Aqui estão algumas indicações desse tipo de tempo limite:

- Os registros do console contêm estas linhas:*** Assista o tempo limite do cachorro *** PC = 0x6022536C, SP = 0x0000000
- A saída **show version** relata o motivo do recarregamento como um "temporizador watchdog expirado":
Router#**show version**
...
Router uptime is 1 hour, 47 minutes
System restarted by **watchdog timer expired** at 06:30:24 UTC Mon Jan 28 2000
System image file is "flash:c3640-is-mz.113-7-T.bin", booted via flash
- Nenhum arquivo crashinfo é gerado. Consulte [Recuperando informações do arquivo Crashinfo](#) para obter detalhes.

Na maioria das vezes, essas mensagens indicam um problema de hardware, com a placa do processador principal ou com um dos módulos.

Depois de identificar um tempo limite de watchdog de software, a próxima etapa é verificar o [Resumo do Aviso de Campo do Produto](#) para sua plataforma e todos os componentes instalados nesse sistema para problemas de hardware críticos conhecidos. Por exemplo, há um aviso de campo para o Cisco 3600 Series Router: [Intervalos de Parada do Watchdog de Módulo do Cisco 3600 T1/E1 PRI](#). Certifique-se de verificar os Avisos de Campo antes de solucionar problemas novamente.

Se um novo módulo tiver sido instalado recentemente, você deve primeiro tentar removê-lo para verificar se ele é o motivo do tempo limite do watchdog. Se o tempo limite do watchdog persistir, tente recolocar todos os componentes removíveis.

Se o tempo limite do watchdog continuar nesse ponto, não haverá avisos de campo para seu hardware e, se nenhum módulo novo tiver sido instalado recentemente, vá em frente e substitua a placa principal do processador. Em plataformas avançadas, a placa do processador é uma placa separada (como o NPE-400 ou o RSP8). Em plataformas de extremidade baixa (Cisco 1700, 2500, 4000, 2600, 3600 e assim por diante), a placa-mãe não pode ser enviada separadamente. Nesse caso, você tem que substituir o próprio chassi.

Intervalo de vigilante do processo

Esse timeout é gerado por um loop infinito durante o processo. Aqui estão algumas indicações deste tempo limite:

- Os registros do console contêm estas linhas:
%SYS-2-WATCHDOG: Process aborted on watchdog timeout,
process = Exec

```
*** System received a Software forced crash ***
```

```
signal = 0x17, code = 0x24, context= 0x60ceca60
```

- A saída **show version** relata o travamento como um "travamento forçado por software":

```
Router#show version
```

```
...
```

```
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-1.112-15a.bin",
```

```
booted via flash
```

- Um arquivo crashinfo é gerado para plataformas que o suportam.

Esse problema é provavelmente um bug do software Cisco IOS.

Se você tiver a saída de um comando [show stacks](#) de seu dispositivo Cisco, poderá usar o [Cisco CLI Analyzer](#) para exibir possíveis problemas e correções. Para usar o [Cisco CLI Analyzer](#), você deve ser um [cliente registrado, estar conectado e com o JavaScript habilitado](#).

No entanto, o sistema ficou preso em um loop antes do recarregamento. Portanto, o rastreamento da pilha não precisa necessariamente ser relevante. Você pode atualizar para a versão mais recente do software Cisco IOS em sua versão para eliminar todos os problemas conhecidos do Process Watchdog. Se ainda ocorrer um travamento após a atualização, reúna o máximo de informações possível (consulte [Troubleshooting de Travamentos do Roteador](#)) e entre em contato com o representante do suporte técnico.

Mensagens de erro relacionadas ao tempo limite do vigia

Há outras mensagens de erro de console relacionadas aos temporizadores watchdog. Não confunda essas mensagens com um travamento do temporizador do watchdog. Verifique o significado dessas mensagens de erro com a ajuda do [Error Message Decoder](#) (somente clientes [registrados](#)). Esta ferramenta fornece uma explicação detalhada de muitas mensagens de erro e recomenda ações para resolvê-las.

Considere esta mensagem:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout,  
process = [chars]
```

Esta mensagem indica que o processo especificado foi executado por muito tempo e que o processador não foi abandonado. O sistema encerrou o processo indicado. Com base na sua configuração, isso pode levar a um travamento do sistema. Se a mensagem ocorrer apenas uma vez, você não precisará tomar nenhuma ação. No entanto, se isso ocorrer novamente, você deverá tratá-lo como um [Tempo limite do vigilante do processo](#) e tomar as medidas necessárias.

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 [abrir uma solicitação de serviço](#) (somente clientes [registrados](#)) com o Cisco TAC, inclua as seguintes informações:

- Troubleshooting realizado antes da abertura da solicitação de serviço.
- **show technical-support** output (no modo enable, se possível).

- mostrar registro de saída ou capturas de tela do console, se disponível.
- **execute-on slot [slot #] show tech** para o slot que experimentou o travamento da placa de linha.
- O arquivo [crashinfo](#) (se estiver disponível e ainda não tiver sido incluído na saída **show technical-sup**

Anexe os dados coletados à sua requisição de serviço em um texto não compactado e simples (.txt). Você pode anexar informações à sua requisição de serviço ao fazer o upload dela com a Ferramenta TAC Service Request Tool (somente para clientes registrados). Se você não puder acessar a ferramenta Solicitação de serviço, poderá enviar as informações em um anexo de e-mail para attach@cisco.com com seu número de solicitação de serviço na linha de assunto de sua mensagem.

Observação: não recarregue manualmente ou desligue e ligue o roteador antes de coletar as informações acima, a menos que seja necessário solucionar problemas de travamento de uma placa de linha no Cisco 12000 Series Internet Router, pois isso pode causar a perda de informações importantes necessárias para determinar a causa raiz do problema.

Informações Relacionadas

- [Troubleshooting de Travamentos de Roteador](#)
- [Compreendendo travamentos forçados de software](#)
- [Troubleshooting Problemas do Roteador: Software Cisco IOS versões 12.1 EX](#)
- [Suporte Técnico - Cisco Systems](#)