

Esse script é escrito em **Batch**, uma linguagem de script usada no Windows para automatizar tarefas. Vou explicar linha por linha:

`@echo off`

- **Explicação**: Desliga a exibição dos comandos que estão sendo executados no console. Assim, o usuário vê apenas o resultado, sem os comandos.

`cls`

- **Explicação**: Limpa a tela do console, removendo qualquer informação mostrada anteriormente.

`:menu`

- **Explicação**: Define o rótulo **`menu`**, usado como referência para ir a esta parte do script com o comando **`goto`**.

`cls`

- **Explicação**: Novamente, limpa a tela do console.

`color 2`

- **Explicação**: Muda a cor do texto no console para verde (código **`2`**).

Bloco de `echo`

- **Explicação**: Exibe mensagens no console, como:

- **`Programando como uma raiz!!`** (mensagem de abertura).

- Descrição das opções do menu:

- **`1`** - Mostre os arquivos que está na pasta

- **`2`** - Mostre as informações do sistema onde estou

- **`3`** - Sair

- A linha de **`=`** é só para desenhar o menu.

`set /p opcao- Escolha uma opção:`

- ****Explicação****: Lê a entrada do usuário e armazena o valor na variável `opcao`. O texto "Escolha uma opção:" é mostrado para guiar o usuário.

Bloco de `if`

- ****Explicação****: Dependendo da escolha do usuário, o script vai para o rótulo correspondente:

- ****`if %opcao% equ 1 goto opcao1`****: Se a opção for `1`, vai para o rótulo `opcao1`.

- ****`if %opcao% equ 2 goto opcao2`****: Se a opção for `2`, vai para o rótulo `opcao2`.

- ****`if %opcao% equ 3 goto opcao3`****: Se a opção for `3`, vai para o rótulo `opcao3`.

- ****`if %opcao% GEQ 4 goto opcao4`****: Se a opção for maior ou igual a `4`, vai para o rótulo `opcao4` (opção inválida).

Rótulo `:opcao1`

- ****Explicação****: Se o usuário escolheu `1`:

- ****`cls`****: Limpa a tela.

- ****`dir`****: Lista os arquivos e pastas do diretório atual.

- ****Bloco `echo`****: Mostra "arquivos lidos".

- ****`pause`****: Pausa a execução até o usuário pressionar uma tecla.

- ****`goto menu`****: Volta para o menu principal.

Rótulo `:opcao2`

- ****Explicação****: Se o usuário escolheu `2`:

- ****`cls`****: Limpa a tela.

- ****`dir`****: Lista arquivos do diretório (este comando parece incorreto, já que deveria usar `systeminfo` para informações do sistema).

- ****Bloco `echo`****: Exibe "este é seu sistema".

- ****`pause`****: Pausa a execução.

- ****`goto menu`****: Volta para o menu.

Rótulo `:opcao3`

- ****Explicação****: Se o usuário escolheu `3`:

- **`cls`**: Limpa a tela.
- **`exit`**: Sai do script.

Rótulo **`opcao4`**

- **Explicação**: Se o usuário escolheu uma opção inválida (maior ou igual a 4):
 - **`cls`**: Limpa a tela.
 - **Bloco **`echo`****: Exibe "Opção inválida".
 - **`pause`**: Pausa a execução.
 - **`goto menu`**: Volta ao menu principal.

Observação

- No bloco de verificação das opções (**`if`**), todas as condições redirecionam para o rótulo **`opcao1`**. Isso é um erro, pois a opção **`2`** deveria ir para **`opcao2`**, e a **`3`** para **`opcao3`**.

1b-

!

```
===== MENU =====
0 - Sair e voltar ao prompt
1 - Abrir Google Chrome no site da UOL
2 - Abrir Bloco de Notas
3 - Trocar a cor do prompt para amarelo
4 - Listar todas as tarefas em execução
=====
Escolha uma opção:
```

!

2-a Esse log é referente a um erro crítico no sistema Windows, registrado pelo evento **Microsoft-Windows-Kernel-Power**, com **ID de evento 41**. O evento 41 é gerado

quando o sistema operacional é reiniciado inesperadamente, sem um desligamento correto. Isso pode ocorrer devido a falhas de energia, travamentos ou quando o sistema para de responder.

Aqui está uma análise detalhada de cada parte do log:

Cabeçalho do Evento

- **Fonte**: `Microsoft-Windows-Kernel-Power`

Indica que o Kernel do Windows (parte central do sistema) registrou esse evento.

- **Data**: `25/08/2020 20:26:44`

Data e hora em que o evento foi registrado no horário local.

- **Identificação do Evento**: `41`

O ID 41 está associado a reinicializações inesperadas, que normalmente ocorrem devido a uma falha crítica, como queda de energia ou travamento do sistema.

- **Categoria da Tarefa**: `(63)`

Esta categoria não fornece muitas informações úteis por si só, mas é usada internamente pelo Windows para classificar o tipo de evento.

- **Nível**: `Nível Crítico`

Indica que é um erro grave, geralmente resultando em uma reinicialização forçada ou falha.

- **Palavras-chave**: `(70368744177664),(2)`

Palavras-chave que ajudam a identificar o tipo do evento. Para os desenvolvedores do sistema, isso pode ser útil na depuração, mas para análise padrão, esses valores podem ser ignorados.

- **Usuário**: `SISTEMA`

Indica que o sistema operacional (e não um usuário específico) executou a ação.

- **Computador**: `DESKTOP-RS2L8OU`

Nome do computador em que o evento ocorreu.

Descrição do Evento

> O sistema foi reiniciado sem um desligamento correto primeiro. Esse erro pode ser causado quando o sistema para de responder, trava ou fica sem energia inesperadamente.

Essa mensagem sugere que o sistema reiniciou sem passar pelo processo normal de desligamento, o que pode ter ocorrido devido a uma falha de hardware, interrupção de energia ou congelamento do sistema.

XML do Evento

O XML fornece informações estruturadas adicionais sobre o evento. Vamos destacar as partes mais relevantes:

- **<EventID>41</EventID>**

Reafirma o ID do evento (41), que representa a falha de reinicialização inesperada.

- **<TimeCreated SystemTime="2020-08-25T23:26:44.700280800Z" />**

Mostra o horário do evento no formato UTC.

- **<Execution ProcessID="4" ThreadID="8" />**

Indica o ID do processo e da thread que geraram o evento.

- **<Data Name="BugcheckCode">292</Data>**

O código **292** indica um tipo de falha conhecida como **"bugcheck"** (erro de verificação de bug, também conhecido como "tela azul da morte"). Isso sugere que o sistema detectou um erro fatal e foi forçado a reiniciar.

- **Parâmetros de "Bugcheck"**:

- **<Data Name="BugcheckParameter1">0x0</Data>**

- **`<Data Name="BugcheckParameter2">0xffffc20665ab6028</Data>`**
- **`<Data Name="BugcheckParameter3">0xb6002000</Data>`**
- **`<Data Name="BugcheckParameter4">0xc0000135</Data>`**

Esses parâmetros fornecem informações específicas sobre o erro que ocorreu. O valor **`0xc0000135`** indica um erro que está relacionado a uma falha de carregamento de uma DLL necessária para o sistema.

- **`<Data Name="SleepInProgress">0</Data>`**

Indica que o sistema não estava em um estado de suspensão ou hibernação no momento do erro.

- **`<Data Name="PowerButtonTimestamp">0</Data>`**

Nenhum botão de energia foi pressionado para causar a reinicialização.

- **`<Data Name="ConnectedStandbyInProgress">>false</Data>`**

O modo de espera conectado (Connected Standby) não estava em andamento.

Possíveis Causas

1. **Interrupção de energia**: Uma falha na alimentação de energia (como queda de energia) pode ter causado o desligamento abrupto.
2. **Travamento do sistema**: Se o sistema parou de responder, isso pode ter forçado uma reinicialização.
3. **Falha de hardware**: Problemas com componentes, como a fonte de alimentação, memória RAM ou placa-mãe, podem gerar esse tipo de erro.
4. **Erro de driver ou software**: Drivers incompatíveis ou software corrompido também podem causar esse bugcheck.

Recomendações

1. **Verifique o hardware**: Certifique-se de que não houve falha de energia ou problemas com os componentes físicos do computador.

2. ****Atualize os drivers****: Drivers desatualizados ou corrompidos podem causar esse tipo de erro. Verifique e atualize os drivers.
3. ****Verifique eventos anteriores****: Outros logs de eventos podem fornecer pistas adicionais sobre o que causou o problema.
4. ****Monitore o sistema****: Se o problema for recorrente, monitore o sistema para identificar o que pode estar causando os travamentos.

Essa análise sugere que o sistema enfrentou um erro fatal, resultando em uma reinicialização inesperada. É importante investigar se foi uma falha isolada ou se o problema continua ocorrendo.

2-b Análise de Log- Evento do Windows

Este documento contém a análise detalhada de um evento extraído do log do sistema Windows, conforme solicitado. A seguir, fornecemos a explicação linha por linha e destacamos os elementos mais relevantes do evento que elucidam o ocorrido.

Log Analisado

Nome do Log: System

Fonte: Microsoft-Windows-UserModePowerService

Data: 16/11/2017 19:26:45

Identificação do Evento: 12

Categoria da Tarefa: (10)

Nível: Informações

Palavras-chave:

Usuário: SISTEMA

Computador: HOME

Descrição:

O processo C:\Program Files\AVAST Software\Avast\AvastSvc.exe (ID do processo:1152) redefiniu o esquema de política de {381b4222-f694-41f0-9685ff5bb260df2e} para {381b4222-f694-41f0-9685-ff5bb260df2e}

XML de Evento:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-UserModePowerService" Guid="{CE8DEE0B-D539-4000-B0F8-77BED049C590}" />
    <EventID>12</EventID>
```

```
<Version>0</Version>
<Level>4</Level>
<Task>10</Task>
<Opcode>0</Opcode>
<Keywords>0x4000000000000000</Keywords>
<TimeCreated SystemTime="2017-11-16T21:26:45.764957000Z" />
<EventRecordID>196237</EventRecordID>
<Correlation/>
<Execution ProcessID="820" ThreadID="912" />
<Channel>System</Channel>
<Computer>HOME</Computer>
<Security UserID="S-1-5-18" />
</System>
<EventData>
  <Data Name="ProcessPath">C:\Program Files\AVAST Software\Avast\AvastSvc.exe</Data>
  <Data Name="ProcessPid">1152</Data>
  <Data Name="OldSchemeGuid">{381B4222-F694-41F0-9685-FF5BB260DF2E}</Data>
  <Data Name="NewSchemeGuid">{381B4222-F694-41F0-9685-FF5BB260DF2E}</Data>
</EventData>
</Event>
```

Análise do Log

Este log refere-se a um evento registrado pelo serviço **Microsoft-Windows-UserModePowerService**, com **ID de Evento 12**.

Esse evento indica que um processo no sistema alterou ou redefiniu as configurações de política de energia.

Fonte: A origem do evento é o serviço de gerenciamento de energia do Windows no modo usuário.

Processo: O processo envolvido é o **AvastSvc.exe**, o serviço principal do software antivírus Avast. O log especifica que o caminho do processo é **C:\Program Files\AVAST Software\Avast\AvastSvc.exe** e o ID do processo é **1152**.

Esquema de Política: O log menciona um esquema de política identificado pelo GUID (Globally Unique Identifier)

{381B4222-F694-41F0-9685-FF5BB260DF2E}, que foi redefinido. O GUID refere-se ao "Plano de Energia Equilibrado", que é uma configuração padrão do Windows.

Embora o evento seja de nível "Informação", o que sugere que não houve impacto crítico no sistema, ele mostra claramente que o antivírus Avast modificou ou reafirmou as configurações de energia, talvez como parte de uma verificação ou atualização.

Não houve alteração no esquema de política de energia (os GUIDs de "antes" e "depois" são os mesmos), indicando que provavelmente o Avast apenas revalidou a política já existente.

Elementos-chave:

- **Processo envolvido**: **C:\Program Files\AVAST Software\Avast\AvastSvc.exe**
- **Esquema de energia redefinido**: **{381B4222-F694-41F0-9685-FF5BB260DF2E}** (Plano Equilibrado)
- **Natureza do evento**: Informação, sem impactos críticos relatados.

Esses pontos elucidam o propósito do evento: uma ação de manutenção ou verificação do antivírus relacionada à energia do sistema.

3-a

Este log refere-se a um erro registrado pelo **Microsoft-Windows-WindowsUpdateClient** com **ID de Evento 20**, indicando que houve um problema durante a tentativa de atualização de um aplicativo no sistema. Aqui está a análise detalhada:

Cabeçalho do Evento

- **Fonte**: **Microsoft-Windows-WindowsUpdateClient**

Refere-se ao cliente do Windows Update, que é responsável por gerenciar as atualizações do sistema e de aplicativos.

- **EventID**: **20**

Este evento com ID 20 indica uma falha em uma tentativa de atualização, o que geralmente ocorre quando há um erro ao baixar ou instalar uma atualização.

- **Nível**: **2 (Erro)**

O nível "2" indica que o evento foi registrado como um erro, sugerindo que a operação de atualização não foi concluída com sucesso.

- **Task**: **1**

Categoria geral da tarefa, que neste caso é a operação de atualização.

- **Opcode**: **13**

Esse opcode especifica que o evento é relacionado ao "Download" ou "Instalação" de uma atualização.

- **Keywords**: `0x8000000000000028`

As palavras-chave são usadas para categorizar o evento internamente no Windows, mas não fornecem muitas informações relevantes para esta análise.

- **TimeCreated**: `2024-11-11T06:58:44.0895776Z`

O horário em que o evento ocorreu, no formato UTC (Coordinated Universal Time).

- **EventRecordID**: `67686`

Identificador único deste evento no log do sistema.

- **Computer**: `DESKTOP-8PL6F1D`

Nome do computador onde o evento foi registrado.

- **UserID**: `S-1-5-18`

Indica que a conta do sistema (Serviço Local) estava executando a ação.

Detalhes do Evento

- **ErrorCode**: `0x80073d02`

Este código de erro refere-se a um problema com o **Microsoft Store ao tentar atualizar um aplicativo. O erro 0x80073d02 geralmente significa que o aplicativo que o sistema tentou atualizar estava em execução no momento da atualização, impedindo a conclusão do processo.**

- **UpdateTitle**: `9NKSQGP7F2NH-5319275A.WhatsAppDesktop`

O título da atualização refere-se ao **WhatsApp Desktop**, indicando que o erro ocorreu ao tentar atualizar este aplicativo.

- **UpdateGuid**: `{0ea470ea-0035-46c1-9a25-4bfd0c774a47}`

Identificador global exclusivo (GUID) da atualização específica do WhatsApp Desktop.

- **UpdateRevisionNumber**: `1`

Número de revisão da atualização, provavelmente a primeira revisão desta versão específica.

- **ServiceGuid**: `{855e8a7c-ecb4-4ca3-b045-1dfa50104289}`

GUID que identifica o serviço associado ao Windows Update.

Análise

Este evento mostra que houve uma tentativa de atualizar o aplicativo **WhatsApp Desktop através do **Microsoft Store**, mas a operação falhou com o código de erro **0x80073d02**. Esse código indica que o aplicativo estava sendo executado no momento da atualização, o que impediu a conclusão da instalação.**

Solução Potencial

Para resolver esse problema, você pode tentar as seguintes ações:

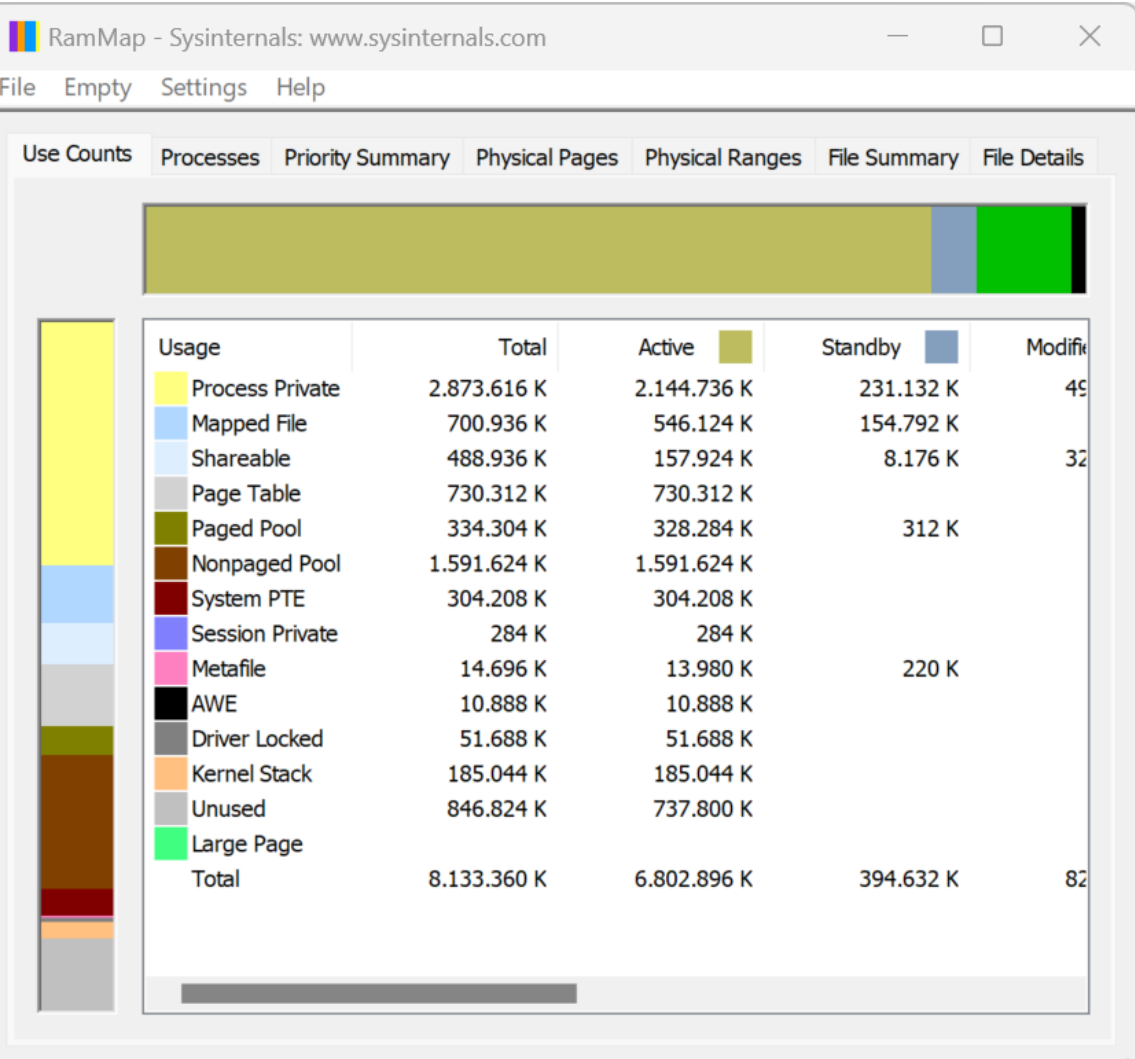
1. **Fechar o WhatsApp Desktop**: Certifique-se de que o aplicativo **WhatsApp Desktop** esteja completamente fechado antes de tentar a atualização novamente. Verifique no **Gerenciador de Tarefas** se há algum processo relacionado ao WhatsApp ainda em execução.
2. **Reiniciar o Sistema**: Reinicie o computador para garantir que não haja processos em segundo plano do aplicativo em execução, e tente a atualização novamente.
3. **Atualizar via Microsoft Store**: Acesse a **Microsoft Store** manualmente, vá até a seção de atualizações e tente atualizar o aplicativo diretamente pela loja.
4. **Reinstalar o aplicativo**: Se o problema persistir, você pode tentar desinstalar o **WhatsApp Desktop** e instalá-lo novamente pela **Microsoft Store**.

Conclusão

O evento registrado indica um erro ao tentar atualizar o **WhatsApp Desktop** devido à sua execução durante o processo de atualização. Fechar o aplicativo ou reiniciar o sistema provavelmente resolverá o problema, permitindo que a atualização ocorra corretamente.

3A- é uma ferramenta avançada para análise de uso de memória no Windows.

3b-



4A –

O **Autoruns** é uma ferramenta gratuita da **Microsoft** (Sysinternals) que oferece uma visão detalhada de todos os programas e processos configurados para iniciar automaticamente no Windows.

4B -

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

Codecs Boot Execute Image Hijacks Applnit Known DLLs Winlogon Winsock Providers
Print Monitors LSA Providers Network Providers WML... Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers

Autoruns Entry	Description	Publisher	Image Path
Logon			
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> Adobe Acrobat Synchronizer	Acrobat Collaboration Synchronizer 24.4	(Verified) Adobe Inc.	C:\Program File
<input checked="" type="checkbox"/> CiscoMeetingDaemon	Cisco Webex Meetings	(Verified) Cisco WebEx LLC	C:\Users\venic\
<input checked="" type="checkbox"/> CiscoSpark		(Not Verified)	C:\Users\venic\
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\venic\
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce			
<input checked="" type="checkbox"/> Delete Cached Standalone Update Binary	Processador de comandos do Windows	(Verified) Microsoft Windows	C:\WINDOWS\
<input checked="" type="checkbox"/> Delete Cached Update Binary	Processador de comandos do Windows	(Verified) Microsoft Windows	C:\WINDOWS\
<input checked="" type="checkbox"/> Uninstall 24.201.1006.0005	Processador de comandos do Windows	(Verified) Microsoft Windows	C:\WINDOWS\
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> CertificateRegistration	Certificate Expiration Check Utility	(Not Verified) A.E.T. Europe B.V.	C:\WINDOWS\
<input checked="" type="checkbox"/> DellMobileConnectWelcome	Dell Mobile Connect Welcome	(Verified) SCREENOVATE TECHNOL...	C:\Program File
<input checked="" type="checkbox"/> RtkAudUService	Realtek HD Audio Universal Service	(Verified) Realtek Semiconductor C...	C:\WINDOWS\
<input checked="" type="checkbox"/> WavesSvc	Waves MaxxAudio Service Application	(Verified) Waves Inc	C:\WINDOWS\
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
<input checked="" type="checkbox"/> cmd.exe	Processador de comandos do Windows	(Verified) Microsoft Windows	C:\WINDOWS\