

2-A:

O log que você forneceu é de um evento crítico do **Windows Event Viewer**, relacionado ao kernel do sistema operacional, especificamente ao evento identificado como **Event ID 41**, fonte **Microsoft-Windows-Kernel-Power**. Este evento é geralmente registrado quando o sistema foi **reiniciado de forma inesperada**, o que pode ter ocorrido devido a uma falha de hardware, desligamento forçado, queda de energia, ou outro problema inesperado. Vou detalhar e comentar os aspectos mais importantes deste log:

Análise do Log

Informações Gerais

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

- **Indica que o evento é relacionado ao kernel de energia do Windows. Problemas aqui geralmente envolvem gerenciamento de energia ou falhas críticas do sistema.**

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

- O horário em que o problema foi registrado. Note que isso pode não coincidir exatamente com o horário de ocorrência, especialmente em caso de falhas abruptas.

- **ID do Evento**: `41`

- O código de evento `41` é um indicador genérico de um **desligamento inesperado**. Quando o Windows detecta que não foi desligado corretamente, ele gera este evento na inicialização subsequente.

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

- Um subtipo de evento para o ID 41, indicando que é um evento crítico.

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 descrição sugere um desligamento abrupto do sistema. As causas possíveis incluem:

- **Perda de energia** (por exemplo, queda de energia ou fonte de alimentação falha).
- **Travamento do sistema** (BSOD - Blue Screen of Death).
- **Desligamento forçado** (pressionamento prolongado do botão de energia).

XML de Evento

A seguir, vou detalhar os principais campos do XML:

`<Provider>`

- **Nome**: `Microsoft-Windows-Kernel-Power`
- **GUID**: `{331c3b3a-2005-44c2-ac5e-77220c37d6b4}`

- **Identificador único da fonte do evento. Indica que o evento é proveniente do subsistema de energia do Windows.**

`<EventID>41</EventID>`

- Como mencionado, o ID 41 indica uma **reinicialização inesperada**.

`<Level>1</Level>`

- **Nível Crítico**, indicando que este é um erro sério que afetou o funcionamento do sistema.

`<Task>63</Task>` e `<Opcode>0</Opcode>`

- Não fornecem informações adicionais relevantes para análise.

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

- Data e hora do evento em formato UTC (`23:26:44`). Convertendo para o horário local mencionado (`20:26:44`).

`<Execution ProcessID="4" ThreadID="8"/>`

- O processo com ID `4` é geralmente o processo **System**, que é uma parte crítica do sistema operacional. Isso sugere que o problema ocorreu em um nível muito baixo do kernel.

`<EventData>`

Este é o campo mais importante para análise. Vamos examinar cada linha:

1. **`<Data Name="BugcheckCode">292</Data>`**

- O código de verificação de bug (`292` em decimal, `0x124` em hexadecimal) está associado a um **erro de hardware** (MCE - Machine Check Exception). Isso geralmente indica que o processador detectou um erro de hardware crítico.

2. **`<Data Name="BugcheckParameter1">0x0</Data>`**

- Este parâmetro tem valor `0x0`, indicando que não há informações adicionais específicas fornecidas para este erro.

3. **`<Data Name="BugcheckParameter2">0xffffc20665ab6028</Data>`**

- Endereço de memória relacionado ao erro. Isso pode indicar onde ocorreu o problema, mas, para análise profunda, seria necessário examinar um **arquivo de despejo de memória (minidump)**.

4. **`<Data Name="BugcheckParameter3">0xb6002000</Data>`**

- Outro parâmetro relacionado à verificação de erro. Poderia fornecer informações sobre o status do hardware ou registradores do processador.

5. **`<Data Name="BugcheckParameter4">0xc0000135</Data>`**

- Este código (`0xc0000135`) indica um erro crítico: **DLL não encontrada**. Isso é raro para um evento de erro de hardware e pode sugerir problemas no carregamento de drivers ou arquivos do sistema.

6. **`<Data Name="SleepInProgress">0</Data>`**

- Indica que o sistema **não** estava em modo de suspensão quando o evento ocorreu.

7. `<Data Name="PowerButtonTimestamp">0</Data>`

- Valor `0` sugere que o botão de energia não foi pressionado, reforçando a ideia de que o sistema travou ou perdeu energia inesperadamente.

8. `<Data Name="BootAppStatus">0</Data>`

- Indica que não houve problemas detectados durante o boot.

9. `<Data Name="ConnectedStandbyInProgress">>false</Data>`

- Indica que o sistema não estava em modo de espera conectada, comum em dispositivos móveis.

Conclusão

Este log indica que o sistema foi reiniciado abruptamente, provavelmente devido a um erro de hardware (código de bugcheck `0x124`). As possíveis causas podem incluir:

- **Problemas de hardware**, como superaquecimento da CPU, falha na memória RAM, ou defeito na fonte de alimentação.
- **Falhas de driver ou software**, especialmente se um driver não pôde ser carregado (indicador: `0xc0000135`).
- **Queda de energia** ou falha na fonte, se descartarmos problemas de software.

Recomendações

1. **Verifique o hardware:**

- Teste a memória RAM usando ferramentas como **Memtest86**.
- Monitore a temperatura da CPU e GPU para evitar superaquecimento.
- Certifique-se de que a fonte de alimentação está funcionando corretamente.

2. ****Atualize os drivers****:

- Principalmente drivers de vídeo e chipset, que podem causar problemas de inicialização.

3. ****Verifique o sistema de arquivos****:

- Execute o comando `sfc /scannow`` e `chkdsk /f`` para corrigir possíveis problemas de integridade de arquivos.

4. ****Análise de minidump****:

- Para uma análise mais detalhada, você pode verificar o arquivo de despejo de memória (`minidump``), que pode fornecer mais informações sobre o erro.

2-B:

O log fornecido pertence ao ****Event Viewer**** do Windows e é um registro da categoria ****System****. Neste caso, o evento é identificado como ****Event ID 12****, gerado pela fonte ****Microsoft-Windows-UserModePowerService****. Este evento está relacionado a mudanças no esquema de energia do sistema, especificamente quando um processo tenta alterar ou redefinir as configurações de energia.

Análise do Log

Informações Gerais

- ****Fonte****: `Microsoft-Windows-UserModePowerService``

- **Indica que o evento foi gerado pelo serviço de gerenciamento de energia em modo de usuário. Este serviço controla as políticas de energia, como perfis de energia e estados de suspensão.**

- ****Data****: `16/11/2017 19:26:45``

- O horário local em que o evento foi registrado.

- ****ID do Evento****: `12``

- O ID 12 indica que houve uma alteração no esquema de política de energia.

Descrição do Evento

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

Aqui podemos observar que:

- O processo `AvastSvc.exe`, que é o ****serviço principal do Avast Antivirus****, realizou uma ação relacionada ao esquema de política de energia.
- O esquema de energia alterado é identificado pelo GUID `{381b4222-f694-41f0-9685-ff5bb260df2e}`, que corresponde ao ****"Equilibrado" (Balanced)****, um perfil padrão do Windows.
- O mesmo GUID aparece tanto como ****esquema antigo**** quanto ****novo****, indicando que o Avast redefiniu ou reafirmou o perfil de energia, mas sem efetuar uma mudança concreta de um perfil para outro.

XML de Evento

Vamos detalhar os elementos mais importantes:

``

- ****Nome****: `Microsoft-Windows-UserModePowerService`

- ****GUID****: `{CE8DEE0B-D539-4000-B0F8-77BED049C590}`

- Identifica a fonte do evento como o serviço de gerenciamento de energia em modo de usuário.

`

- Este ID indica uma ****alteração ou redefinição do esquema de política de energia****. Não é um erro crítico, apenas uma informação sobre uma modificação realizada.

`

- ****Nível de Informação****, indicando que este é um evento informativo e não um alerta ou erro.

`<TimeCreated SystemTime="2017-11-16T21:26:45.764957000Z"/>`

- A data e hora do evento em formato UTC (`21:26:45`), que corresponde ao horário local (`19:26:45`).

`<Execution ProcessID="820" ThreadID="912"/>`

- **ProcessID**: `820` e **ThreadID**: `912`

- Identificam o processo e a thread que registraram o evento, mas não fornecem informações adicionais importantes neste caso.

`<EventData>`

Aqui temos os detalhes mais relevantes:

1. **<Data Name="ProcessPath">C:\Program Files\AVAST Software\Avast\AvastSvc.exe</Data>**

- **O processo que realizou a alteração é o **AvastSvc.exe**, que é o serviço do Avast Antivirus.**

2. **<Data Name="ProcessPid">1152</Data>**

- O ID do processo é `1152`.

3. **<Data Name="OldSchemeGuid">381B4222-F694-41F0-9685-FF5BB260DF2E</Data>**

- O GUID `{381B4222-F694-41f0-9685-ff5bb260df2e}` refere-se ao esquema de energia **Equilibrado** (Balanced), um dos perfis padrão do Windows.

4. **<Data Name="NewSchemeGuid">381B4222-F694-41F0-9685-FF5BB260DF2E</Data>**

- **O novo esquema de energia é o mesmo que o anterior, indicando que o perfil não foi alterado, mas possivelmente foi redefinido.**

Conclusão

Este evento indica que o **Avast Antivirus**** fez uma modificação ou redefiniu o perfil de energia do Windows para o esquema ****Equilibrado**** (Balanced). Isso pode acontecer por vários motivos, como:**

- O Avast tenta ajustar o perfil de energia para evitar que o sistema entre em modos de economia de energia que possam interromper suas verificações ou atualizações.**
- O software de antivírus pode ter detectado uma alteração no perfil de energia e forçou uma redefinição para garantir estabilidade.**
- Este é um comportamento comum e geralmente não indica problemas, mas pode ser uma configuração do Avast para otimizar o desempenho do sistema durante a execução de suas tarefas.**

Recomendações

1. ****Nenhuma ação imediata necessária****, já que este é um evento informativo e não um erro.
2. ****Verificar as configurações do Avast****:
 - Se o comportamento for indesejado, você pode desativar ajustes automáticos de desempenho nas configurações do Avast.
3. ****Monitorar alterações frequentes****:
 - Se você observar que este evento ocorre repetidamente, pode indicar que outro software está tentando alterar o perfil de energia e o Avast está revertendo a mudança.

2-C:

O log fornecido refere-se a um ****Application Error (Erro de Aplicação)**** no Windows, identificado pelo ****Event ID 1000****, que é um evento comum para falhas em aplicativos. Vou analisar os detalhes para identificar a causa e sugerir possíveis soluções.

Análise do Log

Informações Gerais

- ****Fonte****: `Application Error`

- **Indica que o erro foi gerado por um problema em um aplicativo específico, neste caso, o executável `LayersChecker.exe`.**

- ****ID do Evento****: `1000`

- O ID 1000 indica um erro de aplicação, geralmente quando um aplicativo falha e para de funcionar.

- ****Nível****: `2 (Erro)`

- Indica que este é um ****erro**** crítico que precisa ser resolvido.

- ****Data e Hora****: `2024-11-10T14:35:20.1422223Z`

- Horário do incidente em formato UTC.

Dados Específicos do Erro

- ****Aplicativo com Falha****: `LayersChecker.exe`

- **Localizado em `C:\Program Files (x86)\Steam\steamapps\common\Baldurs Gate 3\Launcher\LayersChecker.exe`.**

- **Este arquivo faz parte do ****launcher do Baldur's Gate 3****, que é gerenciado pela Steam.**

- ****Versão do Aplicativo****: `0.0.0.0`

- A ausência de uma versão específica pode indicar um problema na instalação ou atualização corrompida.

- ****Código de Exceção****: `c0000005`

- **Este é um código de exceção crítico, indicando um ****erro de violação de acesso****. Ocorre quando o aplicativo tenta acessar uma área de memória não permitida.**

- ****Offset do Erro****: `00000000000028ee`

- Indica o local específico na memória onde ocorreu o erro. Útil para desenvolvedores, mas não fornece muita informação diretamente para o usuário.

- ****Process ID (PID)****: `0x3ef4` (Decimal: 16116)

- ID do processo do aplicativo com falha.

Caminhos do Aplicativo e Módulo

- ****Caminho do Aplicativo****:

- `C:\Program Files (x86)\Steam\steamapps\common\Baldurs Gate 3\Launcher\LayersChecker.exe`

- ****Caminho do Módulo****:

- O módulo que causou a falha é o próprio `LayersChecker.exe`.

Possíveis Causas

1. ****Violação de Acesso (`c0000005`)****:

- **Geralmente indica um problema de memória, como acesso a áreas de memória não alocadas. Pode ser causado por:**

- **Arquivos corrompidos do jogo ou do launcher.**

- **Conflitos com software de terceiros (como antivírus).**

- **Problemas de compatibilidade ou drivers desatualizados.**

2. ****Arquivo Corrompido****:

- **O arquivo `LayersChecker.exe` pode estar corrompido devido a uma instalação mal sucedida ou atualização interrompida do jogo.**

3. ****Conflito com Antivírus****:

- **Softwares de segurança podem interferir em jogos e suas verificações de integridade, bloqueando ou interrompendo processos importantes.**

Soluções Possíveis

1. ****Verificar a Integridade dos Arquivos do Jogo****:

- Abra o ****Steam****, vá para ****Biblioteca****, clique com o botão direito em ****Baldur's Gate 3****, selecione ****Propriedades**** > ****Arquivos Locais**** > ****Verificar integridade dos arquivos****.

- Isso garantirá que os arquivos do jogo não estejam corrompidos e sejam restaurados, se necessário.

2. ****Executar o Jogo como Administrador****:

- Navegue até o executável (`LayersChecker.exe`), clique com o botão direito e escolha ****Executar como administrador****.
- Pode ajudar a evitar problemas de permissão.

3. ****Desativar Temporariamente o Antivírus****:

- O antivírus pode estar interferindo no launcher do jogo. Tente desativá-lo temporariamente e executar o jogo novamente.
- Se o problema for resolvido, adicione o jogo e o launcher às exceções do antivírus.

4. ****Atualizar Drivers de Vídeo****:

- Erros de violação de acesso podem ser causados por drivers de vídeo desatualizados.
- Atualize seus drivers para a versão mais recente disponível no site do fabricante (NVIDIA, AMD ou Intel).

5. ****Reinstalar o Baldur's Gate 3 Launcher****:

- Se o problema persistir, você pode tentar reinstalar apenas o launcher.
- Exclua o arquivo `LayersChecker.exe` manualmente e faça a verificação de integridade dos arquivos para forçar o Steam a baixá-lo novamente.

6. ****Modo de Compatibilidade****:

- Tente executar o arquivo `LayersChecker.exe` em modo de compatibilidade com uma versão anterior do Windows.
- Clique com o botão direito no executável > ****Propriedades**** > ****Compatibilidade**** > Marque ****Executar este programa em modo de compatibilidade**** e selecione uma versão anterior.

Conclusão

O log indica uma falha crítica com o launcher do Baldur's Gate 3, especificamente no executável `LayersChecker.exe`. O código de erro (`c0000005`) sugere uma violação de acesso, provavelmente devido a um arquivo corrompido, conflito com software de terceiros ou problemas de compatibilidade. As recomendações acima devem ajudar a resolver o problema.

Se o problema persistir após essas etapas, pode ser necessário procurar suporte técnico oficial da Steam ou dos desenvolvedores de Baldur's Gate 3.