Event Viwer - Look at a Machine Restart

Key Event IDs for Reboot Analysis

- **1074 (Planned):** Indicates a user or application initiated a restart or shutdown. It shows who did it and why.
- **41 (Unexpected):** The system rebooted without a clean shutdown, often due to power failure or a system crash.
- **6008**
  (Unexpected):
  Indicates an abnormal or "dirty" shutdown occurred, often preceding event 41.
- **6005 (Startup):** Recorded when the Event Log service starts, signifying the system has booted up.**6006 (Clean Shutdown):** Recorded when the system shuts down properly.

How to Find These Events

1. Press `Win + R`, type `eventvwr`, and hit Enter.
2. Expand **Windows Logs** and select **System**.
3. Click **Filter Current Log...** in the right pane.
4. In the `<All Event IDs>` box, type the desired IDs separated by commas (e.g., `41, 1074, 6008, 6006`).

PowerShell Command for Quick Check
Use this command to quickly list recent restart events:

```
Get-WinEvent -FilterHashTable @{LogName='System';ID=1074,6006,6008,41} | Select-Object -Property TimeCreated, Id, Message | Format-Table -Wrap
```

Last verified: October 2026

Sources:

- https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent
- https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/select-object

---

Revision #1
Created 29 March 2026 13:46:17 by Admin
Updated 24 October 2026 14:13:11 by Admin