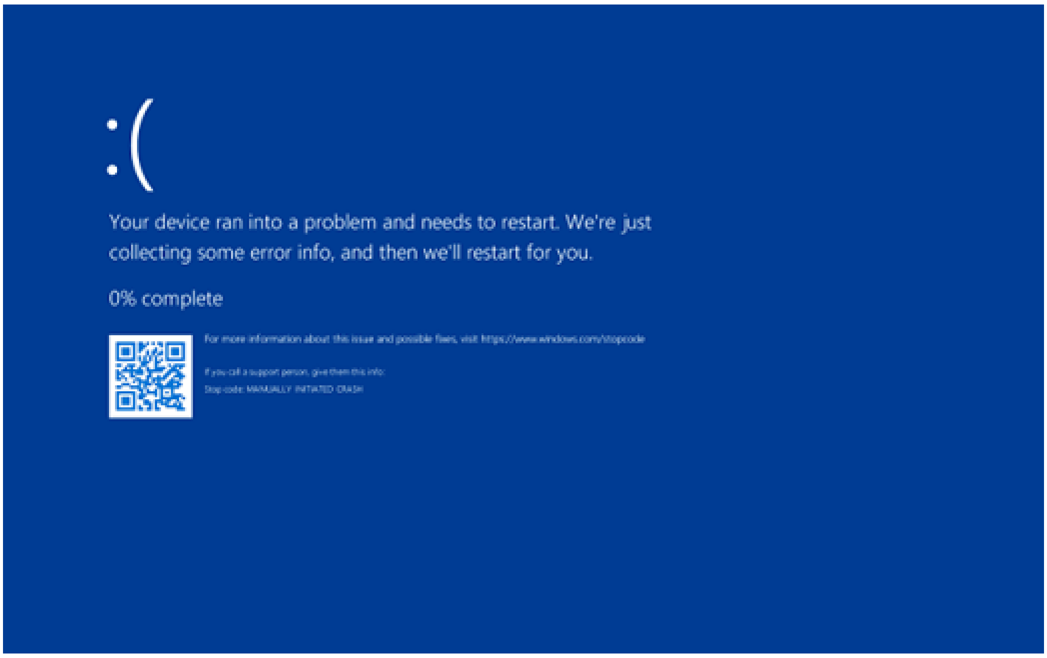
BSOD



:(

Your device ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

0% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: MANUALLY INITIATED CRASH

AKA Bug Checks, when a critical error happens, and exception could be handled by the OS, you will see an ***Blue Screen of Death***

Two broad categories of BSOD

1. Failed Assertion, when OS, driver codes seek a ***"Should Never Happen"*** condition
2. Unhandled or illegal exception, such as traps

Clean and dirty shutdown

Clean shutdown 1074

also called graceful shutdown, as the operation is usually expected

Information 9/7/2023 5:55:18 AM User32 1074 None

> The process C:\Windows\System32\RuntimeBroker.exe (DESKTOP-LGBUJOD) has initiated the power off of computer DESKTOP-LGBUJOD on behalf of user DESKTOP-LGBUJOD\peter for the following reason: Other (Unplanned)
> Reason Code: 0x0
> Shutdown Type: power off
> Comment:

Usually a process shutdown/restart computer on behalf of a user

1074, and you want to figure out who did so?

1. download NotMyFault, extract, run, accept agreement
2. task scheduler, create a basic task
3. when an Event is logged (System, SCM,1074)
4. start a program `<path>\\NotMyFault.exe /bugcheck 0xe2`

remind our customers that after this configuration, even a restart on purpose will create a dump

some Events to check

Information   9/7/2023 5:44:07 AM   EventLog   6005   None

> The Event log service was started.

Information   8/25/2023 4:11:11 AM EventLog   6006   None

> The Event log service was stopped.

Information   8/25/2023 4:11:07 AM User32   1074   None

> The process C:\Windows\System32\RuntimeBroker.exe (DESKTOP-LGBUJOD) has initiated the power off of computer DESKTOP-LGBUJOD on behalf of user DESKTOP-LGBUJOD\peter for the following reason: Other (Unplanned)
> Reason Code: 0x0

Critical   8/25/2023 4:08:22 AM Kernel-Power   41   (63)

> The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.

Error   8/25/2023 4:08:33 AM EventLog   6008   None

> The previous system shutdown at 7:17:18 AM on 8/24/2023 was unexpected.

Error   8/24/2023 6:44:29 AM BugCheck   1001   None

> The computer has rebooted from a bugcheck. The bugcheck was: 0x000000d1 (0xffffae0d5f9dd010, 0x0000000000000002, 0x0000000000000000, 0xfffff804449412d0). A dump was saved in: c:\MEMORY.DMP. Report Id: d94b358b-1a98-4b1b-863a-4d93de55742b.

dirty shutdown

Event 6005 after 6008 or 41

> **Scenario 1**
>
> Within event 41:
>
> Check bugcheckcode in XML, convert to hex e.g. 159 ==> 0x9F
>
> Go check if dump exists

> **Scenario 2**
>
> Powerbuttontimestamp has a non-zero value
>
> Someone might pressed the power button

> **Scenario 3**
>
> Bugcheckcode 0, PBTS 0
>
> Might be hardware issue
>
> 1. Check 6008
> 2. Contact hardware vendor
> 3. Update BIOS,UEFI firmware

> 4. Update VMware related binary
>
> No 41, no 1001, only 6008, check dump, also use action plan above

> **Scenario 4**
>
> Similar to scenario 3, but event 46 occurred
>
> Event 46 indicates Dump generation failed
>
> Go Check pagefile configuration

Dump1keys, Dump2key

on machines that don't have right ctrl, lock scroll key, you may use ***Dump1keys, Dump2key*** to manually trigger a crash

> remove CrashOnCtrlScroll registry key if exists
>
> Under i8042prt or kbdhid, we create new key CrashDump
>
> Add 2 values
>
> | Key | Type | Value |
> |---|---|---|
> | Dump1keys | REG_DWORD | 0x01 |
> | Dump2key | REG_DWORD | 0x3d |
>
> Hold left **shift** and press **space** twice to trigger crash, you can customize your own combo

Possible causes for no dump

1. vender's auto recovery feature such as ASR
2. Hyper-v heartbeat check
3. dump damaged during compression, ask customer to send raw dump file
4. no enough space, try copy out **pagefile.sys** or **"dedicateddumpfile.sys** in RE

enable or disable hyper-v heartbeat

```
REM Get a list of running integration services:
Get-VMIntegrationService -VMName "DemoVM"

REM to enable
Enable-VMIntegrationService -VMName "DemoVM" -Name "Heartbeat"

REM to disable
Disable-VMIntegrationService -VMName "DemoVM" -Name "Heartbeat"
```

You can track creation of dump by adding new value under **CrashControl** in registry

Name	Type	Value
EnableLogFile	REG_DWORD	1

before submit dump file, check validity with dumpcheck.exe

old friend 7B

here are some more services you may check

> 1. PCI
> 2. LSI_SAS
> 3. MOUNTMGR
> 4. NDIS
>
> remember check corresponding **driver.sys** in **system32\drivers** folder

NoBootDeviceCheck

an alternative to 7bchecks.exe

how does it work

> 1. Phase 1 self-training/ learning device tree in RE while OS disk volume could be accessed
> 2. Phase 2 compare he device tree built in phase 1 against offline hives and files to probe missing entities

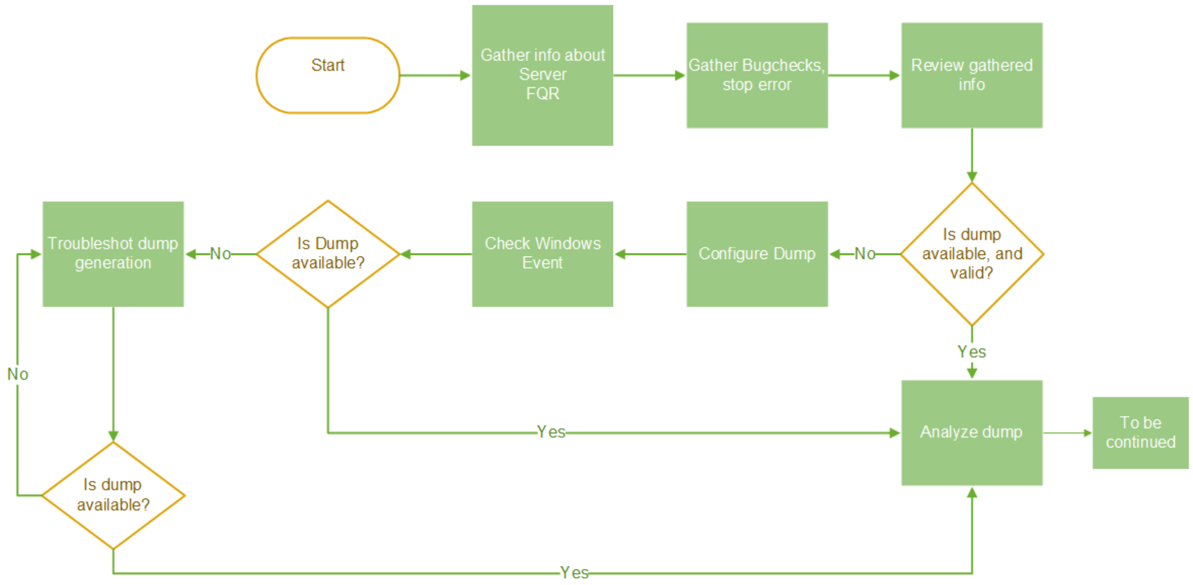
In RE, run command

```
NoBootDeviceCheck.exe <drive_letter>: >> resoult.txt 2>&1
```

After get the report

> 1. Pay attention with alert message in the report as they tell you what device or drivers caused the problem
> 2. Try restore hives, edit registry, copy corresponding file from parallel machines, etc.

Bug Check workflow


Start
Gather info about Server FQR
Gather Bugchecks, stop error
Review gathered info
Is dump available, and valid?
No
Configure Dump
Check Windows Event
Is Dump available?
No
Troubleshot dump generation
Is dump available?
No
Yes
Yes
Analyze dump
To be continued
Yes