Runecast

How To Deal With PSOD

The Purple Screen of Death

BY RUNECAST CTO - **AYLIN SALI**

Summary

Why we're here?

It's important to **keep your data center safe & stable**, and ensure optimal uptime by reduction of unnecessary outages and troubleshooting. **Spend your time where it brings the most value** - on innovating, rather than troubleshooting.

The most troublesome aspect of a PSOD is that it makes you lose trust in your infrastructure and the anxiety it creates. Until you don't solve the root cause, the thought that this can happen again or on another server can keep you up at night.

What is PSOD?

PSOD stands for **Purple Screen of Diagnostics**, often referred to as *Purple Screen of Death*: from the more known Blue Screen of Death encountered on Microsoft Windows.

It's a diagnostic screen displayed by VMware ESXi when the kernel detects a fatal error in which it either is unable to safely recover from, or cannot continue to run without having a much higher risk of a major data loss.

It shows the memory state at the time of the crash and also additional details which are important in troubleshooting the cause of the crash: ESXi version and build, exception type, register dump, backtrace, server uptime, error messages and information about the core dump(a file generated after the the error, containing further diagnostic information).

This screen is visible on the console of the server. In order to see it, you will need to either be in the datacenter and connect a monitor or remotely using the server's out-of-band management (iLO, iDRAC, IMM... depending on your vendor).

Did you Know?

The screen is referred to as either Purple or Pink, but in fact the color is **Dark Magenta**

(RGB:171,0,171 | CMYK:0.00, 1.00, 0.00, 0.33)

Why PSOD happen?

1. Hardware failures, mostly RAM or CPU related.
They normally throw out a “MCE” or “NMI” error.

- **Machine Check Exception (MCE)**, which is a mechanism within the CPU to detect and report hardware issues. There are important details for identifying the root cause of the issue in the codes displayed on the purple screen.

- **Non-maskable interrupt (NMI)**, which is a hardware interrupt that cannot be ignored by the processor. Since NMI is a very important message about a HW failure, the default response starting with ESXi 5.0 and later is to trigger a PSOD. Earlier versions were just logging the error and continuing. Same as with MCEs, purple screen caused by NMI will provide important codes that are crucial for troubleshooting.

2. Software bugs

- improper interactions between ESXi SW components
- race conditions
- out of resources: memory, heap, buffer
- infinite loop + stack overflow
- improper or unsupported configuration parameters

3. Misbehaving drivers: bugs in drivers that try to access some incorrect index or non-existing method

Did you Know?

You can even trigger manually a PSOD for testing purposes or if you are just curious to see it happen. Log in to the ESXi host via DCUI or SSH with a privileged account and run:

```
vsish -e set /reliability/crashMe/Panic
```

Obviously a test system is recommended, ideally a virtual nested ESXi so you can easily observe the console. Also make sure you finish reading this article to understand the implications of this action and the effect on your test system.

What is an impact of PSOD?

Terminates all the services running on it together with all the virtual machines hosted.

The VMs abruptly powered off.

Critical applications like database servers, message queues or backup jobs **may be affected by the "dirty" shutdown.**

If your host is a member of a VSAN cluster, a PSOD **will impact vSAN** as well.

For us, the most troublesome aspect of a PSOD is that **it makes you lose trust in your infrastructure** and the anxiety it creates, at least until you get to the bottom of it.

Top 5 PSOD causes

At Runecast, we regularly analyze the entire VMware Knowledge Base which consists of more than 30,000 articles.

Our engineers (all of whom are VCAP-DCA and vExpert) and advanced systems have analyzed and classified this huge repository of articles. iIn Runecast Analyzer's database there are more than 83 KBs articles mentioning PSOD; here are 5 that stand out:

5

1

ESXi 6.5 and 6.7 host fails with PSOD when IPV6 is globally disabled (2150794)

learn more

2

ESXi host fails with PSOD when using Intel Xeon Processor E5 v4, E7 v4, and D-1500 families (2146388)

learn more

3

ESXi 6.7 and 6.5 Host PSOD on QFLE3I driver on QLogic

learn more

4

VMW-KB-1732 ESXi host Crashed with PSOD caused by brcmfcoe driver referencing _lpfc_sli_get_ iocbq (67065)

learn more

5

Exception 14 in world xxxxx: Unmap Helper IP (70607)

learn more

What to do when PSOD happens?

1. ANALYZE THE PURPLE SCREEN MESSAGE

One of the most important things to do when you have a PSOD is to take a screenshot. If you are connecting remotely (IMM, iLO, iDRAC,...) to the console it will be easy taking a screenshot, but if you have to go to the datacenter, you may need to literally take out your phone and snap a picture of the screen. There's a lot of useful information about the cause of the crash in that screen.

2. CONTACT VMWARE SUPPORT

Before you start further investigation and troubleshooting it is advisable to contact VMware support, if you have a support contract. In parallel with your investigation they will be able to assist you in making the Root Cause Analysis (RCA).

3. REBOOT THE AFFECTED ESXI HOST

In order to recover the server you will need to reboot it. I would also advise keeping it in maintenance mode until you perform the full RCA, identify the cause and fix it. If you can't afford keeping it in maintenance mode, at least fine tune your DRS rules so that only un-important VMs will run on it, so that if another PSOD hits the impact will be minimal.

What to do when PSOD happens?

4. GET THE CORE DUMP

After the server boots up you should collect the coredump. The coredump, also called vmkernel-zdump is a file containing logs with similar detailed information to that seen on the purple diagnostic screen and will be used in further troubleshooting.

Depending on your configuration you may have the core dump in one of these forms:

- On the scratch partition
- As a **.dump** file on one of the host's datastores
- As a **.dump** file on the vCenter - through the netdump service

The coredump becomes especially important if the configuration of the host is to automatically reset after a PSOD, in which case you will not get to see the message on screen.

You can copy the dumpfile out of the ESXi host using SCP and then open it using a text editor. This will contain the contents of the memory at the time of the crash and the first parts of it contain the messages you saw on the purple screen. The whole file may be requested by VMware support, but you can only extract the vmkernel log, which is a bit more … digestible:

```
2018-06-18T06:44:07.645Z cpu3:25615770)0x4393acd1b650:[0x418023317d64]UWVMKSyscallUnpackVSI_Set@(user)#<None>+0x308 stack: 0x0, 0x0,
2018-06-18T06:44:07.645Z cpu3:25615770)0x4393acd1bef0:[0x41802330b1e0]User_UWVMKSyscallHandler@(user)#<None>+0xa4 stack: 0xffa2cc58,
2018-06-18T06:44:07.645Z cpu3:25615770)0x4393acd1bf20:[0x418022d0f7c5]User_UWVMKSyscallHandler@vmkernel#nover+0x1d stack: 0x0, 0x13b,
2018-06-18T06:44:07.645Z cpu3:25615770)0x4393acd1bf30:[0x418022d3d044]gate_entry_@vmkernel#nover+0x0 stack: 0x0, 0x4ac, 0x2ba, 0x0, 0
2018-06-18T06:44:07.648Z cpu3:25615770)VMware ESXi 6.5.0 [Releasebuild-5969303 x86_64]
CrashMe
```

What to do when PSOD happens?

5. DECIPHER THE ERROR

Troubleshooting and Root Cause Analysis can make one feel like Sherlock Holmes. PSODs can sometimes turn into a Arthur Conan Doyle inspired story, but in most cases it's a pretty straightforward process where it will be hard to get to the fifth "why" of the 5 Whys technique.

The most important symptom, and the one you should start with, is the error message generated by the purple screen.

Exception Type **0 #DE:** *Divide Error*
Exception Type **1 #DB:** *Debug Exception*
Exception Type **2 NMI:** *Non-Maskable Interrupt*
Exception Type **3 #BP:** *Breakpoint Exception*
Exception Type **4 #OF:** *Overflow (INTO instruction)*
Exception Type **5 #BR:** *Bounds check (BOUND instruction)*
Exception Type **6 #UD:** *Invalid Opcode*
Exception Type **7 #NM:** *Coprocessor not available*
Exception Type **8 #DF:** *Double Fault*
Exception Type **10 #TS:** *Invalid TSS*
Exception Type **11 #NP:** *Segment Not Present*
Exception Type **12 #SS:** *Stack Segment Fault*
Exception Type **13 #GP:** *General Protection Fault*
Exception Type **14 #PF:** *Page Fault*
Exception Type **16 #MF:** *Coprocessor error*
Exception Type **17 #AC:** *Alignment Check*
Exception Type **18 #MC:** *Machine Check Exception*
Exception Type **19 #XF:** *SIMD Floating-Point Exception*
Exception Type **20-31:** *Reserved*
Exception Type **32-255:** *User-defined (clock scheduler)*

What to do when PSOD happens?

6. CHECK LOGS

It may happen that the cause is not very obvious from looking at the purple screen message or at the core dump log, **so the next place where to look for clues is in the host logs**, especially at the time interval just preceding the PSOD. Even when you feel you have located the cause, it's still advisable to avoid being parsimonious and confirm it by looking at the logs.

If you are administering an enterprise environment it's likely you have some specialized log management solution at hand (like VMware Log Insight or SolarWinds LEM) so it will be easy to browse through those logs, but if you don't have a log management you can easily export them.

THE MOST INTERESTING LOG FILES TO EXPLORE WOULD BE:

COMPONENTS	LOCATION	WHAT IS IT
System messages	/var/log/syslog.log	Contains all general log messages and can be used for troubleshooting.
VMkernel	/var/log/vmkernel.log	Records activities related to virtual machines and ESXi. Most PSOD relevant entries will be in this log, so pay special attention to it.
ESXi host agent log	/var/log/hostd.log	Contains information about the agent that manages and configures the ESXi host and its virtual machines.
VMkernel warnings	/var/log/vmkwarning.log	Records activities related to virtual machines. Watch for heap exhaustion (Heap WorkHeap) related log entries.
vCenter agent log	/var/log/vpxa.log	Contains information about the agent that communicates with vCenter, so you can use it to spot tasks triggered by the vCenter and might have caused the PSOD.
Shell log	/var/log/shell.log	Contains a record of all commands typed, so you can correlate the PSOD to a command executed.

How to prevent PSOD?

And other unexpectedm issues in your environment.

Most of the software related PSODs are resolved by **patches**, so make sure you are up to date with the latest versions. Make sure that your servers are on **VMware's Hardware Compatibility Checklist**, together with all the devices and adapters. This will protect from some of the unexpected hardware related issues, but it will also ensure that VMware support will be able to support you in case of a PSOD.
As described above in "Why it happens", misbehaving drivers are also an often cause of PSODs, so it's imperative to **regularly check vendors' support websites for updated firmware and drivers** and especially for the documented PSOD causing drivers to respond as soon as possible by upgrading them.

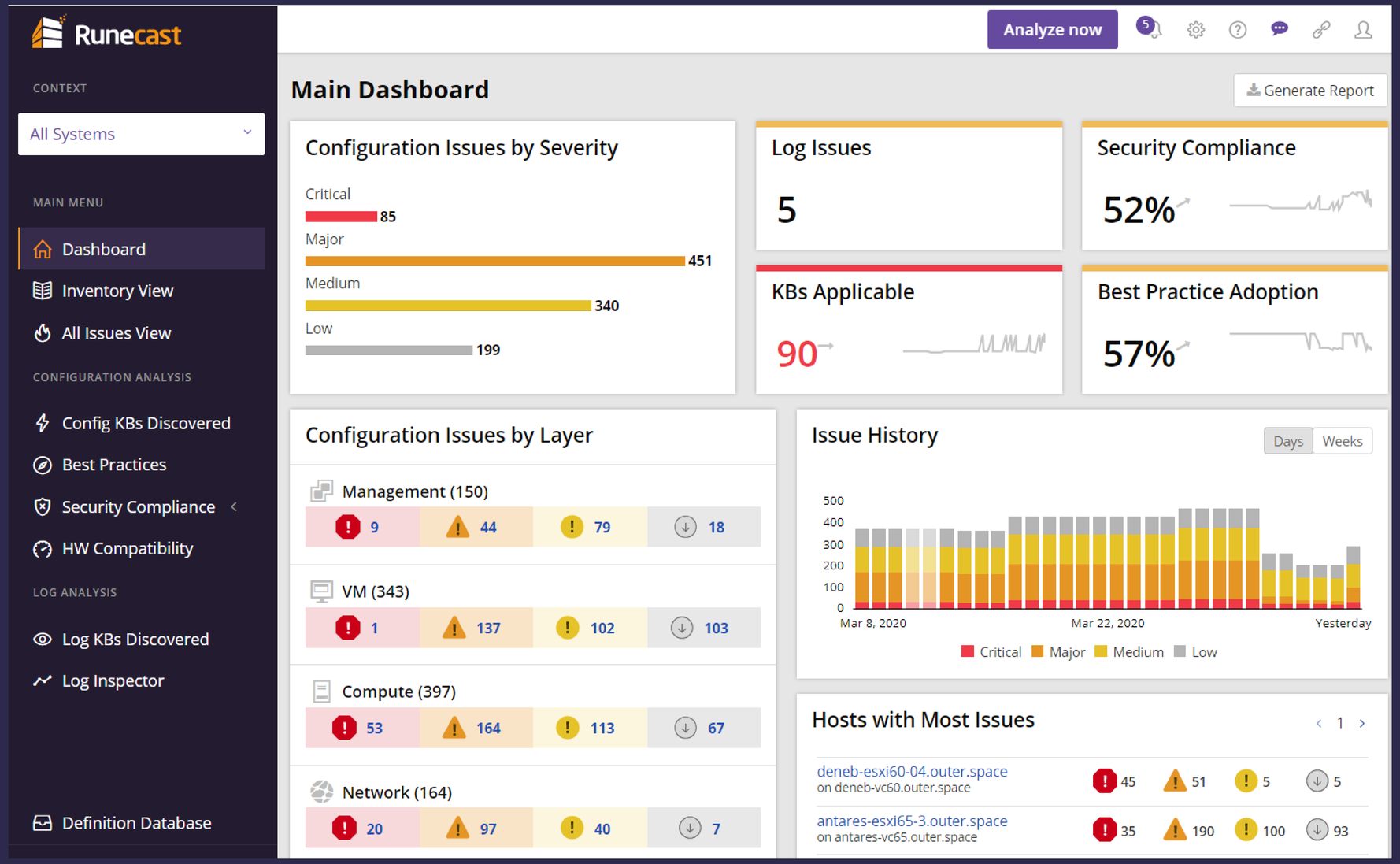
On-Premises Security, Stability and ROI for VMware + AWS

At Runecast, we regularly analyze the entire **VMware Knowledge Base** (which consists of more than 30,000 articles), industry **best practices, hardware compatibility list and security standards**. We are extracting actionable insights from them in order to make rules which automatically makes virtualized infrastructures more resilient, secure & efficient.

By **proactively** analyzing your environment, Runecast Analyzer will help you steer away from these issues, so you can have the peace of mind that most PSODs lurking in your environment are prevented.

FACTS:

- Runecast Analyzer scans your environment in a user-defined schedule.
- If an issue is detected, you will be provided with resolution steps.
- Works on-premises
- Compliant with HIPAA, PCI DSS, STIG, NIST, CIS, and more.
- Updates weekly with the latest version of VMware's KB. For critical issues, Runecast releases updates within a few hours.
- Reduce delays in solving issues by up to 80%.



Companies who benefit from Runecast intelligence

SCANIA verizon Swedbank NYC HEALTH+ HOSPITALS avast Chevron

Discover all potential issues now!

Start your 14 day Runecast Analyzer free trial.

Get Runecast Analyzer for my environment

Want a quick product intro with our team?
Let us know at **roi@runecast.com**