Tips for Troubleshooting VMware ESX Server Faults

Faisal Akber

VMware, Inc.

VMWORLD 2006

Introduction

- The focus of this presentation is to provide some tips on how to troubleshoot VMware ESX server faults
- There are many facets to this topic
- Thus not all can be covered in this presentation

Agenda

- What is a fault?
- Kinds of Faults
- Identifying Faults
- Troubleshooting Strategies
- Tools for Troubleshooting
- Developing an Action Plan
- Executing the Action Plan
- Working with VMware Global Support Services
- Ensuring that Resolution is Achieved
- Conclusions

What is a fault?

- A **fault** is an **interruption in service**
- There are a number kinds of faults that can occur
- The best way to deal with faults is **prevention**
  - Always follow best practices for maintaining datacenters
  - Maintain detailed records of everything that happens within the datacenters
  - Do not use any unsupported hardware or software with VMware ESX server
  - Remember to apply datacenter rules appropriately to a Virtual environment as some rules might hinder operations if not implemented with the ESX Server paradigm in mind
- Also remember that, when dealing with faults, approach the problem systematically and in a calm fashion

The Kinds of faults

- There are a number of kinds of faults
  - Hardware Faults
  - Host Faults
  - VMM Faults
  - Guest Operating System Faults
  - Application Faults

Identifying Faults

- Knowing where the problem has occurred is key.
- Here are a few questions that can help in understanding the fault.
  - When do you know that your ESX server has had a fault?
    - Has an application stopped running?
    - Has connectivity been lost to a particular VM or has the VM stopped running?
    - Does the console of the VM show an OS panic?
    - Has the host become unresponsive?
    - Does the console of the host show an ESX kernel panic?
- These questions and deductive reasoning will help you to determine the type and location of the fault.

Hardware Faults

- Problems with hardware is the most common type of problem that can cause a fault
- Most common faults are hangs, spontaneous reboots and kernel panics
- Hardware faults can manifest itself in many ways. Symptoms might show up as a simple application “glitch” or as a major crash.
- This is most harmful type of fault to business operations
  - Costs increase to the business due to downtime
  - Costs increase due to possible replacement of hardware

Dealing With Hardware Faults

- If a piece of hardware was recently added/removed undo the change and see if problems persist
- Check to see if the device is correctly configured from ESX
- Run diagnostic software
- Review logs for any errors
- Check for power irregularities
- Ensure all hardware components are supported

Host Faults

- Here the service console and the VMkernel are the main focus
- Possible problems seen are:
  - Linux kernel Opps
  - Inability of VirtualCenter or MUI to connect or communicate effectively with the host
  - PSOD (Purple Screen) – VMkernel crashes
  - Other problems in the service console
  - Other ESX server host component failure
  - Host hangs

Dealing With Host Faults

- In the case of a severe fault (like a PSOD or Oops) take a picture using a digital camera of the console screen
- Use the information on the screen to help determine what has happened
- Run top and esxtop to see what else is happening on the server
- Review logs
- Use serial-line logging to try to capture more data

VMM Faults

- A VMM fault is when the Virtual Machine Monitor sees a problem and halts operation
- The guest OS and all VM supporting processes are also halted
- This is analogous to a Virtual Hardware fault. This is similar to unplugging a server while it is running.
- In some cases, VMM faults are a symptom of a problem with the host.
  - If there is a SAN or other storage problem, it can manifest itself here.
- In other cases, the problem can emanate from inside the VM
  - i. e. bad or buggy hardware drivers within the VM

Dealing With VMM Faults

- Review the vmware.log file of the VM and other ESX Server logs
- Review logs inside the VM for clues to the behaviour of the VM
- Review drivers and software installed inside the VM (occasionally bad drivers can cause a VMM fault)
- Ensure that the correct version of the VMware tools are installed
- If the VM is hung then run vm-support –X to:
  - Kill the VM
  - Collect required coredump of VM
  - Collect logs

Guest Operating System Faults

- In this case, all of the VMware components are running normally. However the Guest OS has had a problem.
- Problems that one might see here are network connectivity problems, intermittent OS issues, hangs, and kernel halts
- Depending on the OS running in the VM, a kernel halt results in one of the following: BSOD, Oops, Panics, and ABEND

Dealing With Guest OS Faults

- VMotion the VM to another host and see if the problem persists or is isolated to the current host
- Use performance monitoring tools inside the VM as well as top and esxtop outside the VM to track trends before the problem occurs
- Review logs inside the VM and outside the VM for errors and other clues
- For kernel halts, take a screenshot of the VM console and use the OS vendor’s tools to debug any core memory dumps
- Check configuration for issues inside the VM
- Check to see if the VMX process is still running or not
- Again, it is necessary to have the correct version of the VMware Tools installed in each VM.
- Make sure correct OS patches are applied

Application Faults

- Application faults are where the application running inside a VM halts operation.
- Determine if the Guest OS and hardware are running optimally before isolating issue to the application
- Application faults could be caused by bad data entry from the user

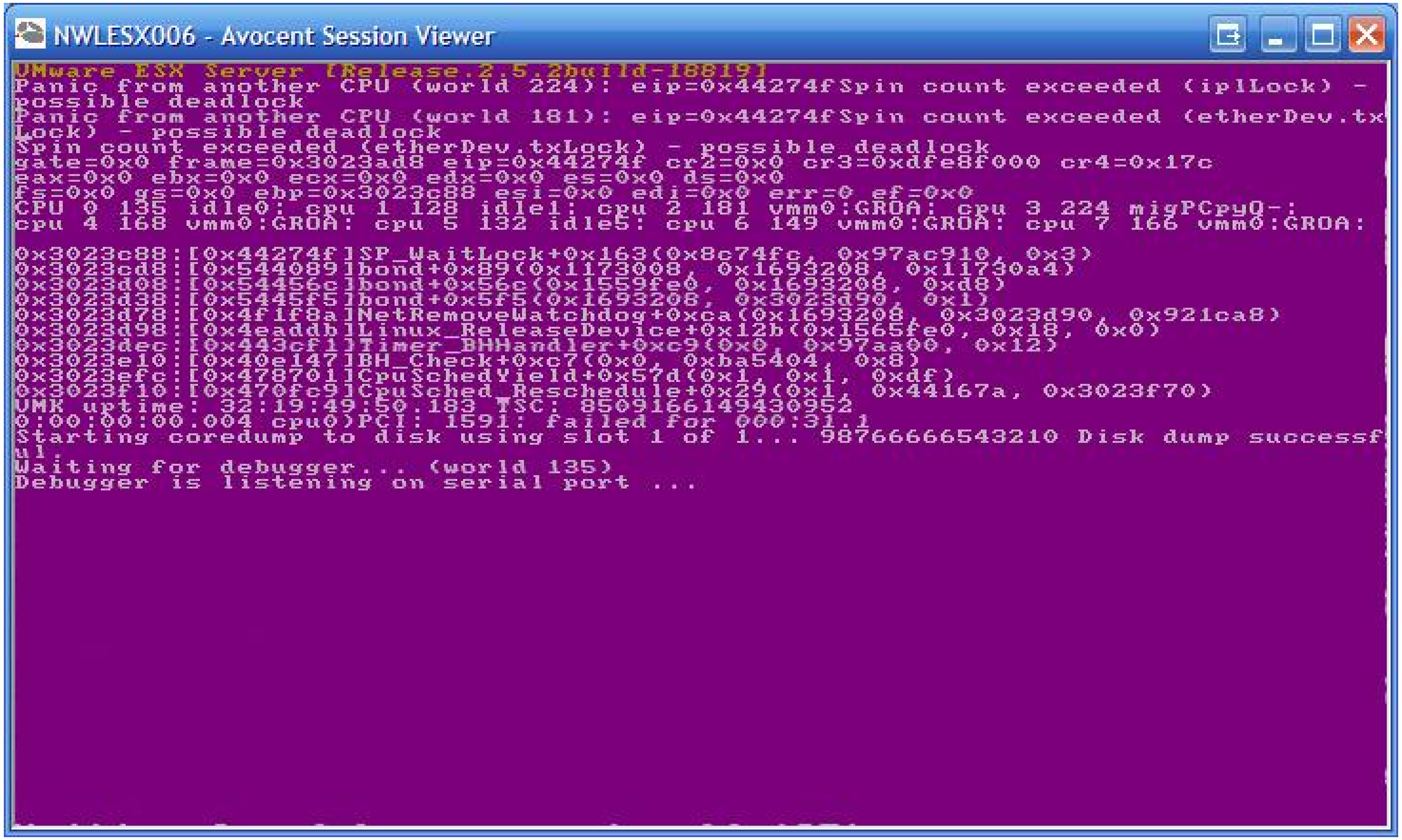
Dealing With Application Faults

- Depending on the type of application the approach to resolve the problem may vary.
- See if there are any core memory dumps and use the OS tools to analyze the dumps
- Review OS and application logs for details
- Look for configuration issues of the system at all levels
- Review VM’s vmware.log to see if the application is causing issues

Troubleshooting Strategies

- The following slides will elaborate on strategies on dealing with the following symptoms
  - PSOD – ESX Server Purple Screen Crashes
  - BSOD – Microsoft Windows Blue Screen Crashes
  - Hangs

Troubleshooting Strategies - PSOD



```
VMware ESX Server [Release.2.5.2build-18819]
Panic from another CPU (world 224): eip=0x44274fSpin count exceeded (iplLock) -
possible deadlock
Panic from another CPU (world 181): eip=0x44274fSpin count exceeded (etherDev.tx
Lock) - possible deadlock
Spin count exceeded (etherDev.txLock) - possible deadlock
gate=0x0 frame=0x3023ad8 eip=0x44274f cr2=0x0 cr3=0xdfe8f000 cr4=0x17c
eax=0x0 ebx=0x0 ecx=0x0 edx=0x0 es=0x0 ds=0x0
fs=0x0 gs=0x0 ebp=0x3023c88 esi=0x0 edi=0x0 err=0 ef=0x0
CPU 0 135 idle0: cpu 1 128 idle1: cpu 2 181 vmm0:GROA: cpu 3 224 migPCpyQ-:
cpu 4 168 vmm0:GROA: cpu 5 132 idle5: cpu 6 149 vmm0:GROA: cpu 7 166 vmm0:GROA:

0x3023c88:[0x44274f]SP_WaitLock+0x163(0x8c74fc, 0x97ac910, 0x3)
0x3023cd8:[0x544089]bond+0x89(0x1173008, 0x1693208, 0x11730a4)
0x3023d08:[0x54456c]bond+0x56c(0x1559fe0, 0x1693208, 0xd8)
0x3023d38:[0x5445f5]bond+0x5f5(0x1693208, 0x3023d90, 0x1)
0x3023d78:[0x4f1f8a]NetRemoveWatchdog+0xca(0x1693208, 0x3023d90, 0x921ca8)
0x3023d98:[0x4eaddb]Linux_ReleaseDevice+0x12b(0x1565fe0, 0x18, 0x0)
0x3023dec:[0x443cf1]Timer_BHHandler+0xc9(0x0, 0x97aa00, 0x12)
0x3023e10:[0x40e147]BH_Check+0xc7(0x0, 0xba5404, 0x8)
0x3023efc:[0x478701]CpuSchedYield+0x57d(0x1, 0x1, 0xdf)
0x3023f10:[0x470fc9]CpuSched_Reschedule+0x29(0x1, 0x44167a, 0x3023f70)
VMK uptime: 32:19:49:50.183 TSC: 8509166149430952
0:00:00:00.004 cpu0)PCI: 1591: failed for 000:31.1
Starting coredump to disk using slot 1 of 1... 9876666543210 Disk dump successf
ul.
Waiting for debugger... (world 135)
Debugger is listening on serial port ...
```

Troubleshooting Strategies – PSOD (Cont.)

- The previous screen shows Purple Screen fault. There is a lot of technical information that can be clues to identifying the cause of the crash
- In this example, we see that this crash was due to a possible deadlock with a part of the system related to the Ethernet device
- There is also a list of which VM or World was running on which physical CPU and a register dump
- The last section describes the call stack indicating what systems the VMkernel was actively working on
- Also note that a memory core dump is generated and stored onto disk
- The core dump can be analyzed by VMware Global Support Services

Troubleshooting Strategies – PSOD (Cont.)

- Review the logs from the PSOD dump
  - After the system is rebooted the core dump is placed in the /root directory
  - Use `vmkdump –l <core_dump_file>` to extract the vmkernel log from the core dump
  - A vmware-log.1 file is extracted from the dump
  - Near the end of this file you will be able to see what had happened on the system

Troubleshooting Strategies – PSOD (Cont.)

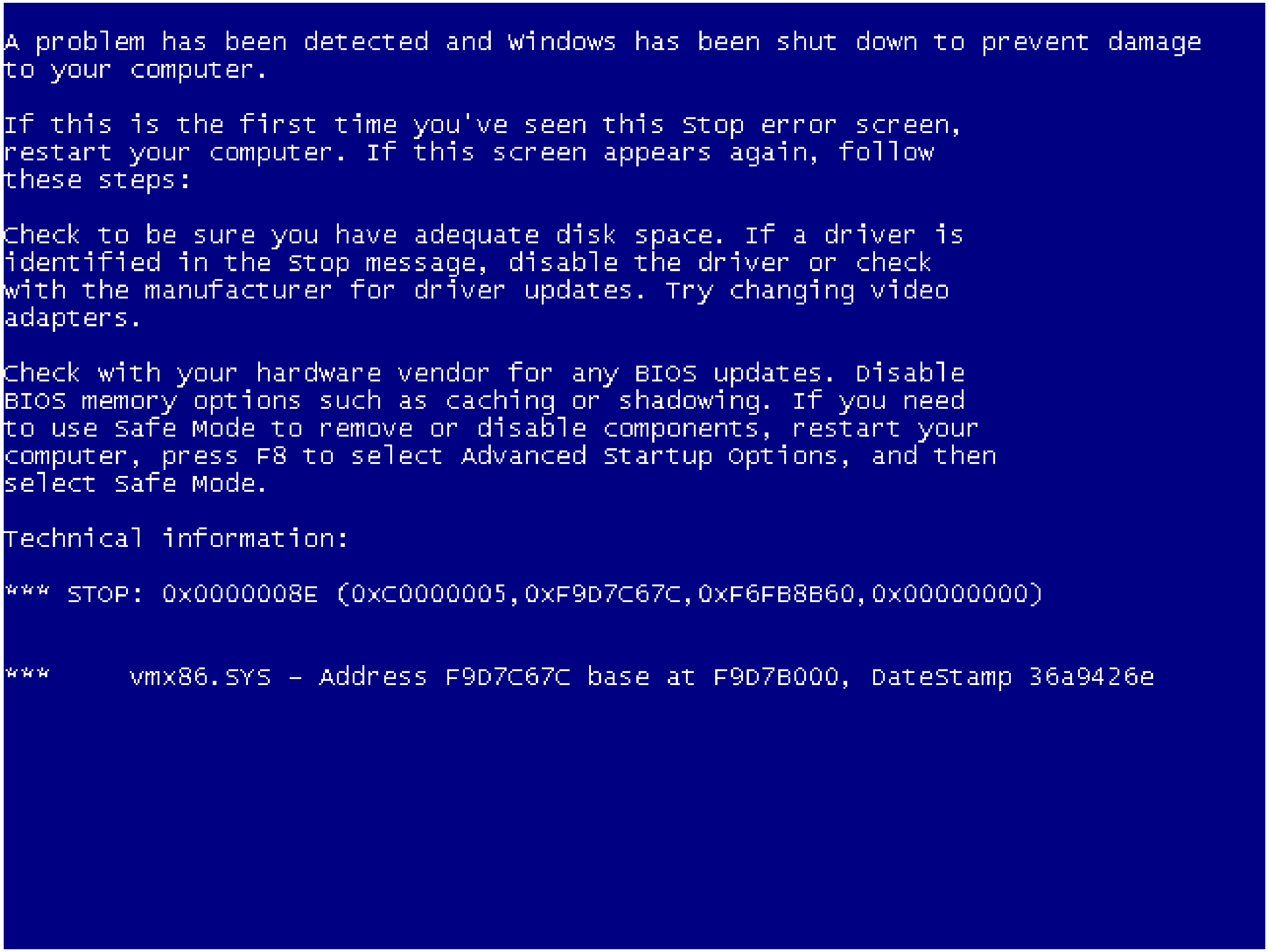
- Exceptions
  - Exceptions are thrown by the CPU for various reasons and faults
  - When you see “Exception Type ##” refer to the table below for common exceptions

Exception Number	Description
8	Double Fault
10	Invalid Task Switch
12	Stack Segment Fault
13	General Protection Fault
14	Page Fault
17	Alignment Check

Troubleshooting Strategies – PSOD (Cont.)

- Machine Check Exceptions (MCE)
  - An MCE is a special type of exception that is thrown when hardware errors are detected
  - The errors are normally in the realm of
    - CPU errors
    - Cache errors
    - Bus control errors
    - RAM errors
    - (On AMD) PCI North Bridge errors
    - I/O access errors
    - Other related errors
  - If an MCE causes a PSOD, it is an unrecoverable error.
  - Immediately contact your hardware vendor to correct the faulty component

Troubleshooting Strategies - BSOD



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.

Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000008E (0xC0000005,0xF9D7C67C,0xF6FB8B60,0x00000000)


***     vmx86.SYS - Address F9D7C67C base at F9D7B000, DateStamp 36a9426e
```

Troubleshooting Strategies - BSOD (Cont.)

- The previous screen shows a Blue Screen panic from a Windows VM
- There is technical information present that shows where the fault occurred
- In this example the fault occurred in the vmx86.SYS component of the system
- Be sure to configure Windows to generate a core memory dump file
- The memory dump file will be called Memory.DMP
- Use a utility called WinDBG to analyze the dump file.
- Contact Microsoft Support for more help

Troubleshooting Strategies - Hangs

- Whether the hang occurs at the VM level or at the host level, these steps will help
  - Check the console for inactivity
  - Ping the host or VM for a response
  - Monitor network traffic from outside the VM or host
  - *(VM only)* Monitor performance statistics of the VM from the host to see if it is consuming a lot of resources
  - *(VM only)* Run vm-support –s –i 10 –d 15 to collect performance statistics and logs
  - *(VM only)* Run vm-support –X <wid> to kill the VM, generate core dumps of the VM and collect logs
  - *(Host only)* Increase BIOS watchdog timers to see if the system will return to normal operation
  - *(Host only)* Disable watchdog timers and see if any other symptoms arise

Troubleshooting Strategies - Hangs (Cont.)

- Setup serial-line logging
- Reboot hung VM or host
- Review logs for clues
- Run the vm-support script to collect logs for VMware Global Support Services to assist in determining cause of hang

Tools for Troubleshooting

- Logs
  - Logs are an integral part of troubleshooting
- Hardware Diagnostic Lights
  - These lights will provide insight to which subsystem in the hardware
- Hardware Diagnostic Software
  - Memtest86
    - This is an open-source tool to exhaustively test memory
    - ESX 3.0 comes with a utility to test unused RAM without downtime to the system
  - The third-party hardware vendor will supply their own diagnostic software
- Change Management Logs
  - This will show any recent changes that may have caused faults or if there is a chronic problem the logs will help in finding patterns

Tools for Troubleshooting (Cont.)

- Performance Data
  - Data collected from the ESX server and the guest OS can assist in showing trends before a fault occurs
- VirtualCenter
  - VC can provide a lot of information, including historical events that occurred with both a VM and a host
- Standard Networking Tools
  - Tools such as ping, traceroute, tcpdump, and arp can help in determining whether or not there is a problem
- Digital Camera
  - If you are not using a remote management card in your server or a KVM that can be accessed remotely then a digital camera is crucial in capturing PSOD screens

Tools for Troubleshooting (Cont.)

- Screenshots
  - Great for capturing PSOD information from a remote management console or Guest OS crash like BSOD from the Remote Console or Virtual Infrastructure Client
- Configuration
  - Review the configuration of a suspect subsystem to ensure that a poorly configured item is not causing the problem
- VMTN
  - Review the documentation and Knowledge Base articles for best practices, correct configuration, supported hardware and software, and tips to various problems
- Internet
  - Use your favourite search engine to find more information regarding the guest OS of the VM in question

Tools for Troubleshooting (Cont.)

- Serial-Line Logging
  - This is especially useful if the local storage system fails
  - Logs will continue to be collected even though they cannot be written to disk
- Configuring Serial-Line Logging (ESX 3.0 Instructions)
  - Connect ESX server to another system using a NULL modem cable
  - Update Advanced Setting *Misc.SerialPort* to equal 1 for COM1: and 2 for COM2:
  - Start serial terminal software on other system and enable logging to disk
  - Reboot ESX Server

Developing an Action Plan

- The Action Plan is essential to recovering from a fault
- If the resolution is simple, the Action Plan will be simple
- Always employ a holistic approach to the problem and do not omit anything without proof
- The basic outline of the Action Plan is as follows:
  - Identify the fault and record all symptoms
  - Address each symptom systematically
  - Review affects of actions and monitor until all symptoms are corrected
  - Continue to monitor for recurrences
- The Action Plan is a living entity
  - As symptoms are identified, the plan must change to address the symptoms
  - Depending on the results of the actions to address the symptoms, further actions might also be required

Executing the Action Plan

- Ensure the correct people are engaged
- Make the ESX Server administrator the owner of the issue or use a project manager to help
- The ESX Server administrator should also coordinate all actions and information to third-party vendors, various IT teams, and management.
- All actions must be fully documented whether part of the plan or not
- Regular meetings should be held *only if necessary*

Working with VMware Global Support Services

- Since ESX and Virtual technology is new in the x86 realm of IT, experience and knowledge to deal with all issues in a datacenter might be limited.
- VMware Global Support Services will work to ensure that the fault(s) are identified
- Once identified, an action plan whether verbal or formal will be provided
- VMware Global Support Services will then monitor to ensure that all action items in the plan are executed and the faults are corrected
- VMware Global Support Services will also (when required) work with other software/hardware vendors to assist in the resolution

Ensuring that Resolution is Achieved

- Create a complete action plan
- Follow the plan in detail
- Document everything
  - Keep the plan updated based on all results of previous actions
- Ensure that backups are made regularly and when required
- If certain actions fail, it may be necessary to restore from the backups
- Understand the nature of your hang and initiate your disaster recovery plan if warranted

Conclusions

- The best way to deal with faults is **prevention**
- When dealing with faults, approach the problem systematically and in a calm fashion
- Create a complete and easy action plan
- Update the action plan as required
- Use the tools and tips outlined to tackle the problem
- Communicate effectively and accurately with all parties to help resolve and control the situation
- Document everything
- Ensure that backups are made regularly and when required
- Understand the nature of your hang and initiate your disaster recovery plan if warranted

Questions and Answers

Presentation Download

Please remember to complete your
session evaluation form
and return it to the room monitors
as you exit the session

The presentation for this session can be downloaded at
http://www.vmware.com/vmtn/vmworld/sessions/

Enter the following to download (case-sensitive):

Username: cbv_rep
Password: cbvfor9v9r

Some or all of the features in this document may be representative of feature areas under development. Feature commitments must not be included in contracts, purchase orders, or sales agreements of any kind. Technical feasibility and market demand will affect final delivery.

VMWORLD 2006