Troubleshooting System Wide Issues

Common Symptoms

- Slow Performance
  - CPU – Slow applications. GUI unresponsive and sluggish.
  - RAM – High disk activity. Similar symptoms to CPU issues.
  - HDD – Excessive fragmentation, high RAM usage
  - Network – slow loading web pages. Poor signal strength.
  - Graphics – Slow video playback. FPS will be very low.
- System Monitor
  - Performance tab in system monitor in first instance.
  - Also check processes tab.
  - Resource Monitor – From performance Tab

Problem Solving Steps

- Formulate a theory of probable cause
- Test the theory to determine the cause
- Establish a plan of action to resolve the issue and implement the solution
- Verify full system functionality. Implement preventative measures if applicable.
- Document findings, actions, and outcomes

Network Connectivity

- When any network connection is detected the built in firewall will try to set the location by asking the default gateway for its MAC address
- After a network location is established, the firewall will check to see it the Internet is accessible via the Network Connection Status Indicator (NCSI)
- A simple check is done by sending a request to http://www.msftncsi.com/ncsi.txt
- Success means that the text **Microsoft NCSI** is returned from the above request – network connectivity is established.
- Check connectivity using IPCONFIG at a command prompt
- Test connectivity by pinging another PC and the gateway
- Ping a host on the Internet that responds to ping (e.g. Google DNS on 8.8.8.8)

Network Connectivity Issues

- Wrong SSID
- Static IP address configured
- Internet Router problems
- External Internet problems
  - Use ping and tracert
- DNS Resolution problems
- Third Party Software
  - Antivirus or anti-malware blocking

The Windows Boot Process

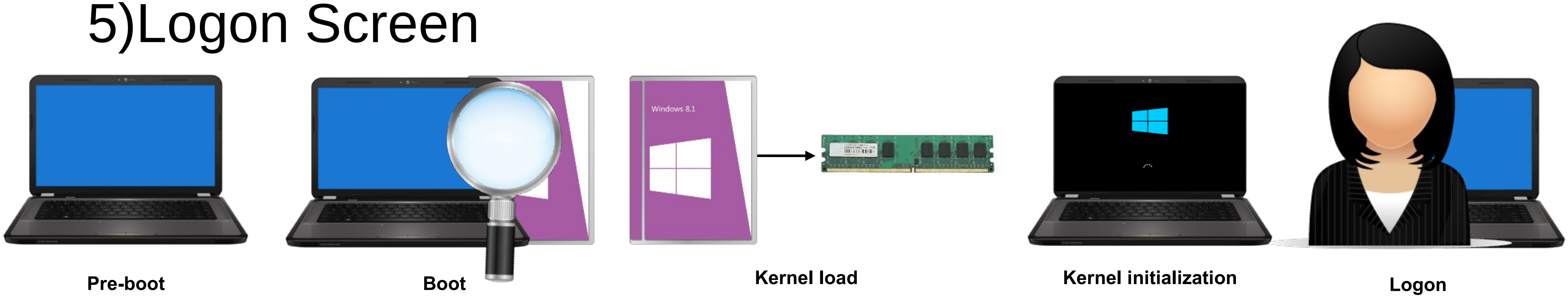
1)Pre-boot

2)Boot

3)Kernal Load

4)Kernal Initialization

5)Logon Screen



Boot Problems

- Need to understand difference between BIOS and UEFI
  - BIOS
    - Performs a Power On Self Test (POST)
    - Then looks for the master boot record (MBR) at start of disk
    - MBR reads the boot sector on the first Primary partition found
  - UEFI
    - Performs a Power On Self Test (POST)
    - Loads drivers for hardware
    - Looks at the MBR in the GUID Partition Table (GPT)
      - GPT points to a partition containing the Boot Manager.
      - UEFI can only use GPT and not MBR directly

Important Boot Files

- Windows Boot Manager (BOOTMGR)
- BCD – Boot Configuration Data
  - Information about OS installed
  - Location of the OS files
- winload.exe
  - Program used to boot windows. Loads OS kernel (ntoskrnl.exe)
- winresume.exe
  - If system is restarting from previous session
- ntoskrnl.exe
  - Allows applications to have access to hardware through drivers
- ntbtlog.exe
  - Boot log that stores log of boot time events. Not enabled by default.

The Windows Boot Process

- Pre-boot
  - POST
    - BIOS – Legacy system
    - UEFI - Unified Extensible Firmware Interface
      - More options than POST as UEFI drivers are loaded before control is handed to the software
  - Check Physical Memory
  - If PnP BIOS, Hardware is recognized and configured
  - Locate the boot device
  - Runs MBR (or GPT if using UEFI)
  - MBR finds active partition
  - Loads active boot sector

The Windows Boot Process

- Boot
  - Operating System selected
  - 4 sub phases
    1. Initial boot loader
    2. Operating system selection
    3. Hardware detection
    4. Configuration selection
  - Windows Uses Winload.exe and Windows Boot Manager

The Windows Boot Process

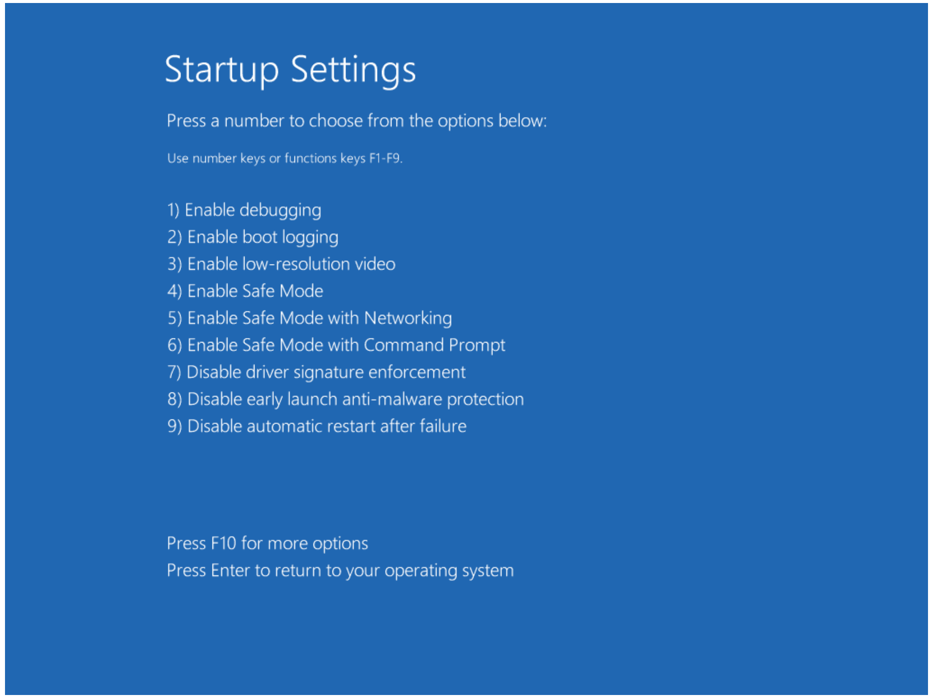
- Kernal Load
  - Operating System Components loaded into memory
- Kernal Initialisation
  - Windows kernal takes control of the system.
  - Windows logo and status bar appears.

The Windows Boot Process

- Logon Sequence
  - Winlogon.exe starts the LSA (Local Security Authority)
  - Logon Screen appears
  - Low level drivers and services continue to be loaded in background
  - Process complete when a user successfully logged on
  - Clone control set built is copied to a new control set called LastKnownGood

Windows 10 Boot Options

- Use MSCONFIG
- Select Reboot while holding down Shift key
- https://www.lifewire.com/startup-settings-2618141



Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

1) Enable debugging
2) Enable boot logging
3) Enable low-resolution video
4) Enable Safe Mode
5) Enable Safe Mode with Networking
6) Enable Safe Mode with Command Prompt
7) Disable driver signature enforcement
8) Disable early launch anti-malware protection
9) Disable automatic restart after failure

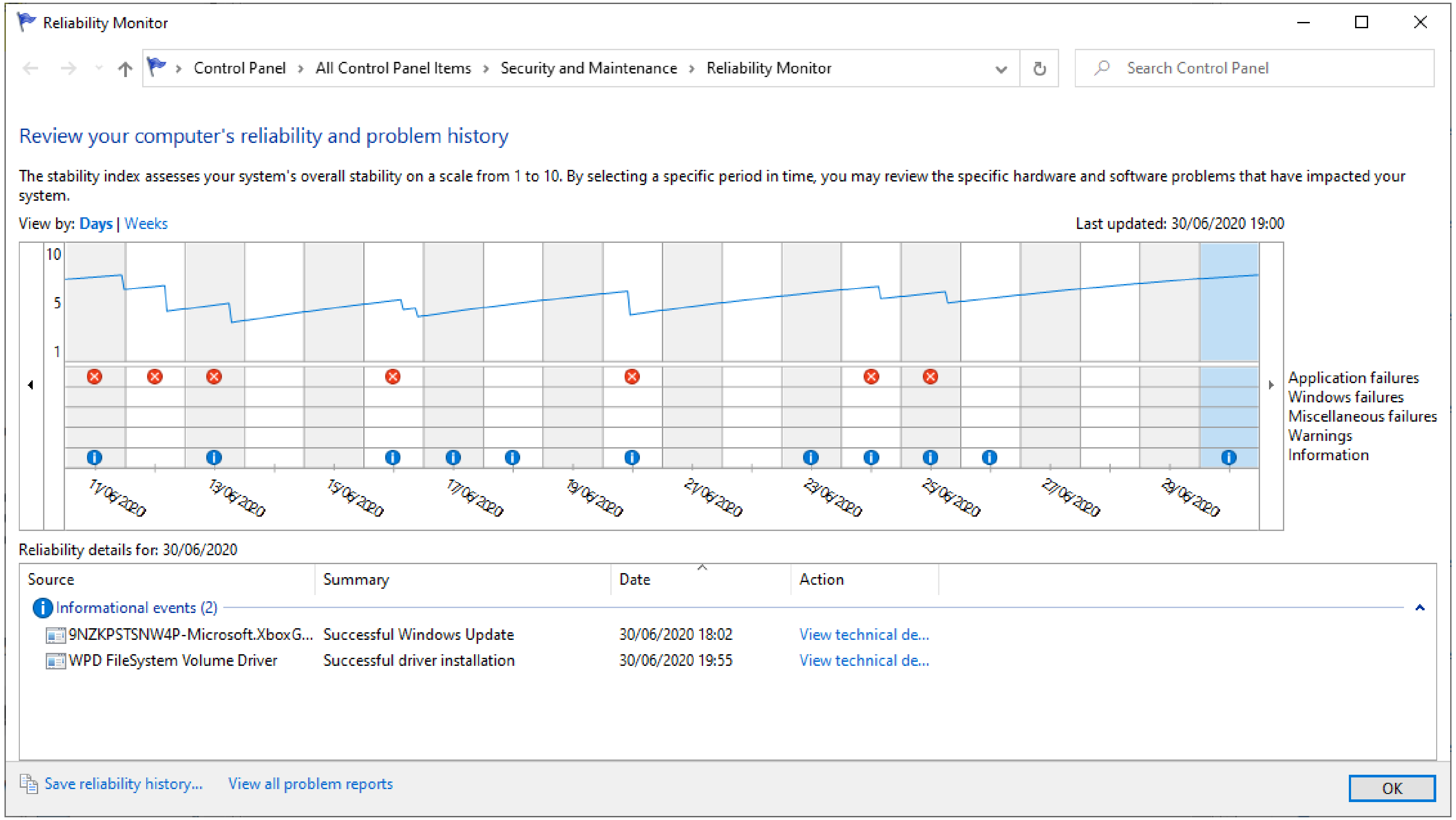
Press F10 for more options
Press Enter to return to your operating system

Bootrec

- MS Utility in the Windows Recovery Environment
- https://neosmart.net/wiki/bootrec/
  - FixMbr
    - Writes a Windows compatible MBR to the system partition. It does not overwrite the existing partition table. Use this option when you must resolve MBR corruption issues, or when you have to remove nonstandard code from the MBR.
  - FixBoot
    - writes a new boot sector to the system partition by using a boot sector that's compatible with Windows.
  - ScanOs
    - scans all disks for installations that are compatible with Windows. It also displays the entries that are currently not in the BCD store.
  - RebuildBcd
    - scans all disks for installations that are compatible with Windows. Additionally, it lets you select the installations that you want to add to the BCD store.
    - Use the Bootrec.exe tool to troubleshoot a "Bootmgr Is Missing" error.

Application Crashes

- Useful tool is the Reliability Monitor
- Event Viewer



Reliability Monitor

Control Panel › All Control Panel Items › Security and Maintenance › Reliability Monitor

Search Control Panel

Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.

View by: **Days** | Weeks

Last updated: 30/06/2020 19:00

Reliability details for: 30/06/2020

Source	Summary	Date	Action
Informational events (2)			
9NZKPSTSNW4P-Microsoft.XboxG...	Successful Windows Update	30/06/2020 18:02	View technical de...
WPD FileSystem Volume Driver	Successful driver installation	30/06/2020 19:55	View technical de...

Save reliability history... View all problem reports

OK

The Linux Boot Process

- Processor checks for BIOS and runs it.
- BIOS checks for peripherals and a valid boot device.
- BIOS loads primary boot loader into memory.
- User is prompted to select an OS to boot to.
- Boot loader finds the kernel binary, uploads the initrd image into memory, and transfers control to the kernel.
- Kernel configures hardware.
- Kernel mounts the root partition, releases unused memory, and runs init
- init searches for inittab, sets the environment past, checks the filesystem, initializes ports, and runs background processes for the runlevel.
- For graphical mode, xdm or kdm starts and displays the login window.
- Use enters login name and password.
- System authenticates the user credentials, runs scripts, and starts the shell.

The OS X Boot Process

- Firmware initialization
  - POST test and hardware initialization
  - Booter found and started
  - Startup chime and single flash of power light
- Booter initialization
  - System kernel loaded
  - KEXTs loaded into memory
  - Kernel takes control
  - Apple logo displayed on screen
- Kernel initialization
  - Additional drivers loaded
  - Core BSD UNIX system loaded
  - Busy wheel or progress bar displayed on screen
- System launchd initialization
  - launchd starts and loads the rest of the system files
  - Login screen or Finder displayed on screen

Windows OS Troubleshooting Tools

Tool	Description
WinRE	Use Windows Recovery Environment (WinRE) to troubleshoot and manage system errors that occur within the Windows operating system.
Bootrec.exe	Found in WinRE, use this tool to troubleshoot and resolve MBR issues, boot sector problems, and BCD (Boot Configuration Data) issues. • fixmbr • fixboot
sfc	Use System File Checker (sfc) to scan for corrupted files during startup.
System repair disc	You can create a repair disk to access system recovery options when the Windows installation media is unavailable.
Pre-installation environments	Windows PE is commonly used by large manufacturing companies to load a pre-installed version of Windows to provide to end users. It can also be used for troubleshooting and file system recovery by allowing administrators to run forensic and disk imaging tools.
Refresh	If you have attempted to resolve a Windows 8/8.1 problem and have had no success, you can refresh the system.
MSCONFIG	MSCONFIG is frequently used to test various configurations for diagnostic purposes, rather than to permanently make configuration changes.

Windows OS Troubleshooting Tools

Tool	Description
DEFRAG	When systems are running slow and performance is suffering, then you may want to run the DEFRAG utility to reduce fragmentation on the hard disk by reorganizing stored data. This can affect disk performance.
REGSVR32	This utility registers OLE controls such as DLL and ActiveX files. If you are having issues with Windows or IE, you can use REGSVR32 to unregister and reregister controls.
REGEDIT	Use the REGEDIT utility to make changes to infected or corrupted files within the Registry. Use caution when viewing or modifying these files in the Registry.
EXPAND	Use the EXPAND tool to pull one or more update files from a compressed product update package..
Event Viewer	Use the Event Viewer to look at a system's event logs, which may contain specific information about system errors or significant events on the computer. This can be helpful in troubleshooting various system issues.
Safe Mode	Use this Windows system startup method that loads only a minimal set of drivers and services. When a non-critical driver or service causes severe errors, start the system in Safe Mode, and load additional drivers, services, and applications one at a time until you recreate the error.
Command prompt	Use the command prompt to troubleshoot a variety of issues.
Remote Desktop and Remote Assistance	Use Remote Desktop and Remote Assistance to access a user’s computer and provide assistance with various issues. They must be configured and enabled prior to use.

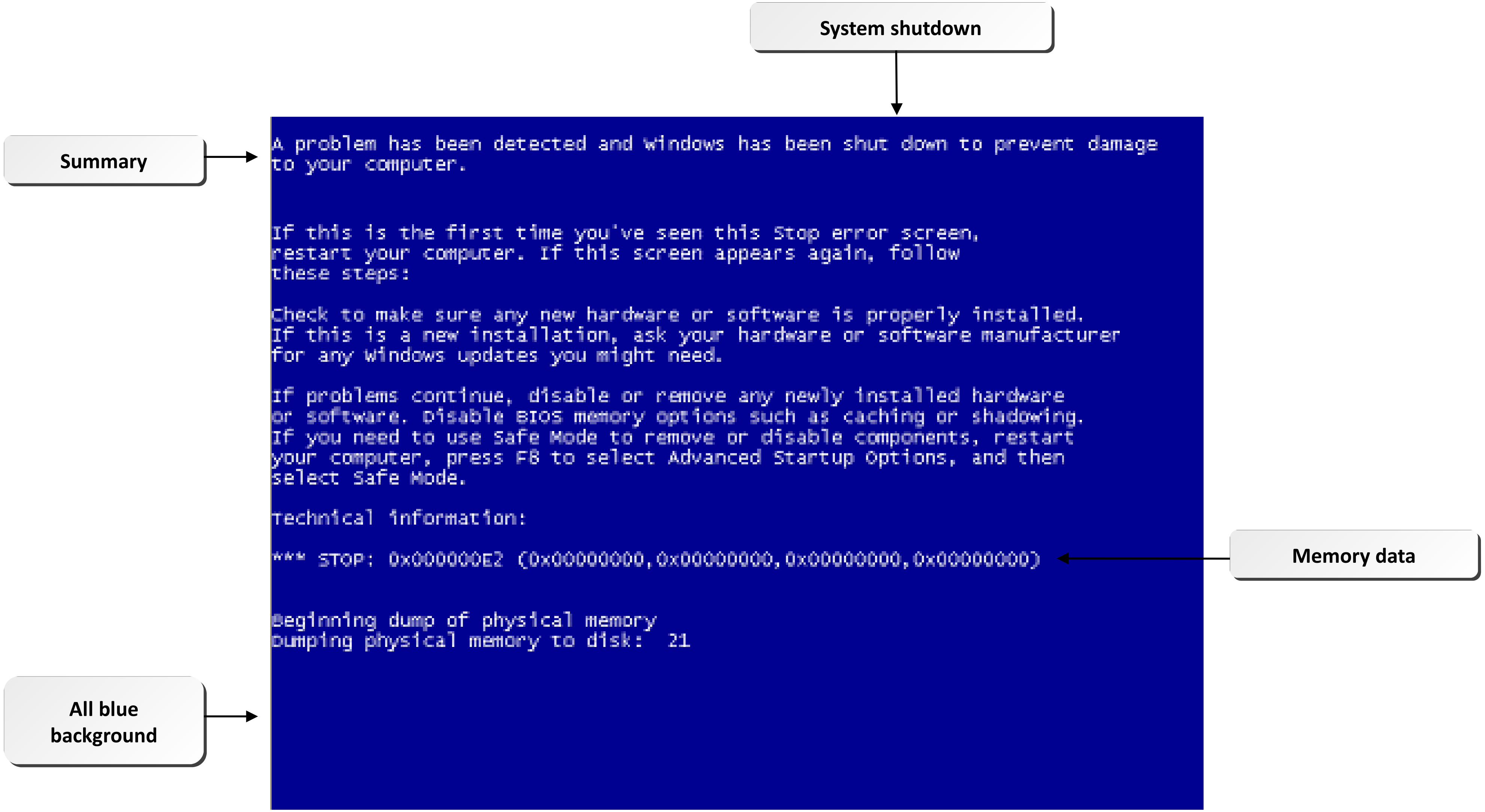
Windows Safe Mode Options

- Safe Mode
  - Starts the computer with a minimal set of drivers and services, including the mouse, keyboard, Video Graphics Array (VGA) display, and a hard disk. It is used when the system problem might be with the networking components.
- Safe Mode with Networking
  - Starts the computer with Safe Mode drivers and services, plus networking drivers and services. It is used when you need to use files on a network location to repair the system.
- Safe Mode with Command Prompt
  - Starts the computer with Safe Mode drivers and services, but with a command prompt interface. It is used when a system problem prevents the system from creating the Windows graphical user interface (GUI) desktop

Windows Safe Mode Options

- Change boot order
- Configure hardware ports
- Configure CPU and GPU settings
- Configure peripherals such as fans and cooling systems
- Configure memory settings
- Configure power management settings

Blue Screen Of Death (BSOD)



System shutdown

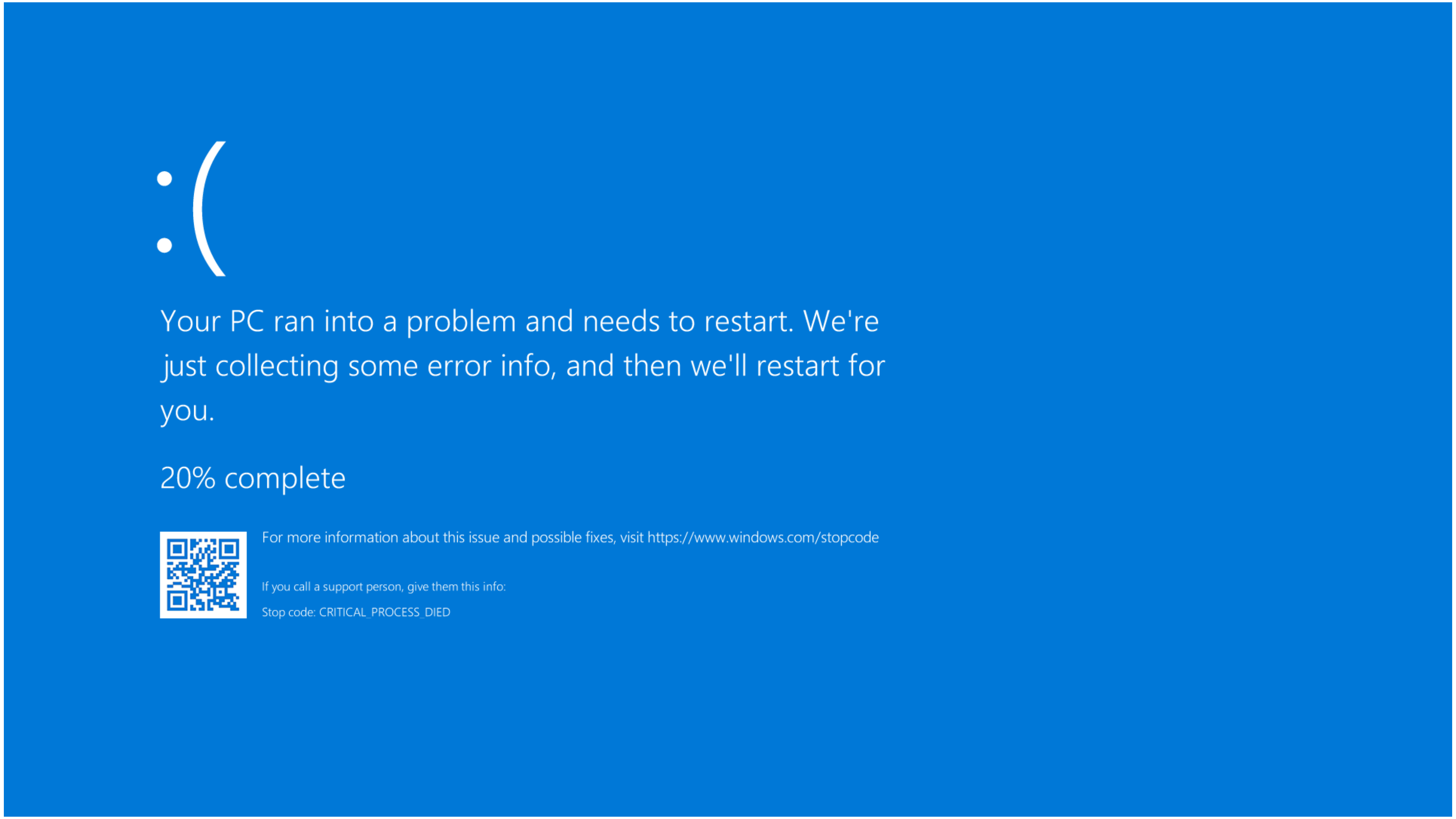
Summary

Memory data

All blue background

```
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 make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. 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: 0x000000E2 (0x00000000,0x00000000,0x00000000,0x00000000)


Beginning dump of physical memory
Dumping physical memory to disk:  21
```

Blue Screen Of Death (BSOD)



:(

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

20% complete

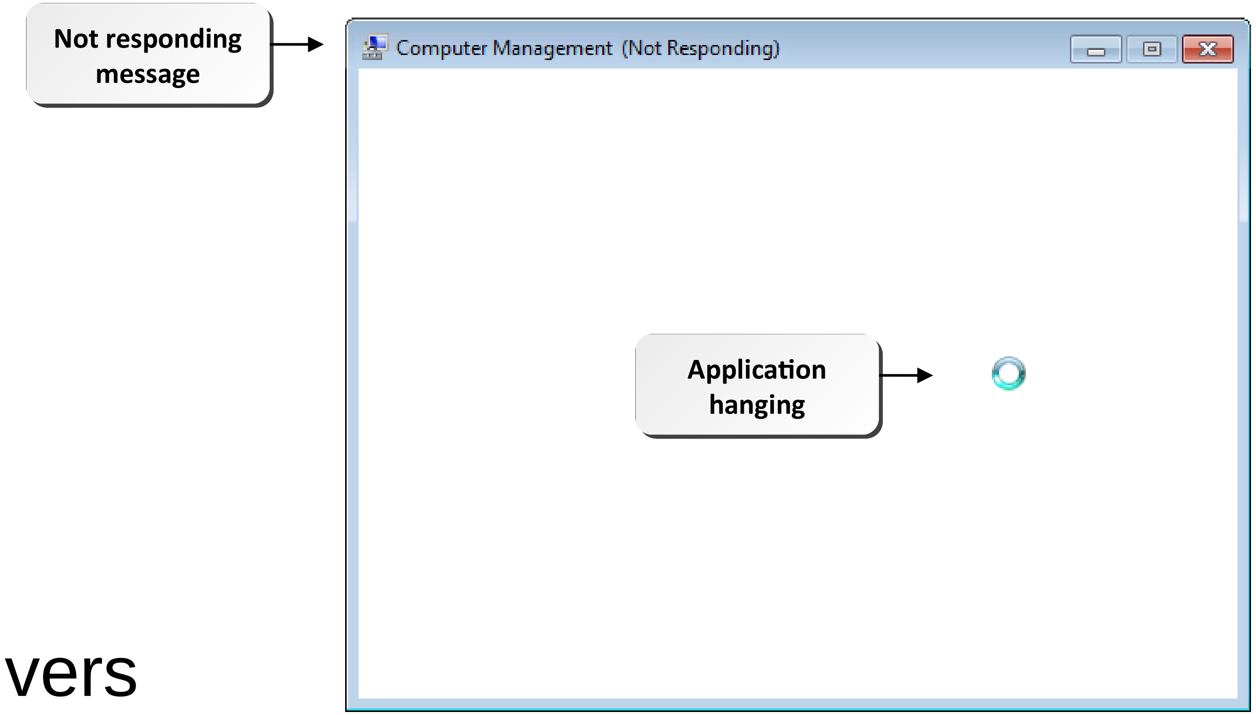
For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

System Lockup Errors

- Use System Manager and the end task function
- Repeated system lockups at a sign of trouble
- Possibly caused by malicious software
- Possibly caused by device drivers
- Possibly caused by defective memory or incorrect memory addressing



Not responding message

Application hanging

I/O Device Issues

- Missing or loose mouse or keyboard connection.
- Blocked signals for wireless devices.
- Missing or incorrect driver for specialty device.
- Misconfigured monitor settings.

Application Errors

- Cannot install application.
- Installed application will not start or load.
- The application cannot be found.
- GPF (General Protection Fault) is causing issues. Usually relates to bad memory
- Illegal operations is attempted and forces application shutdown.
- An invalid working directory issue.
- Windows Store app not working.

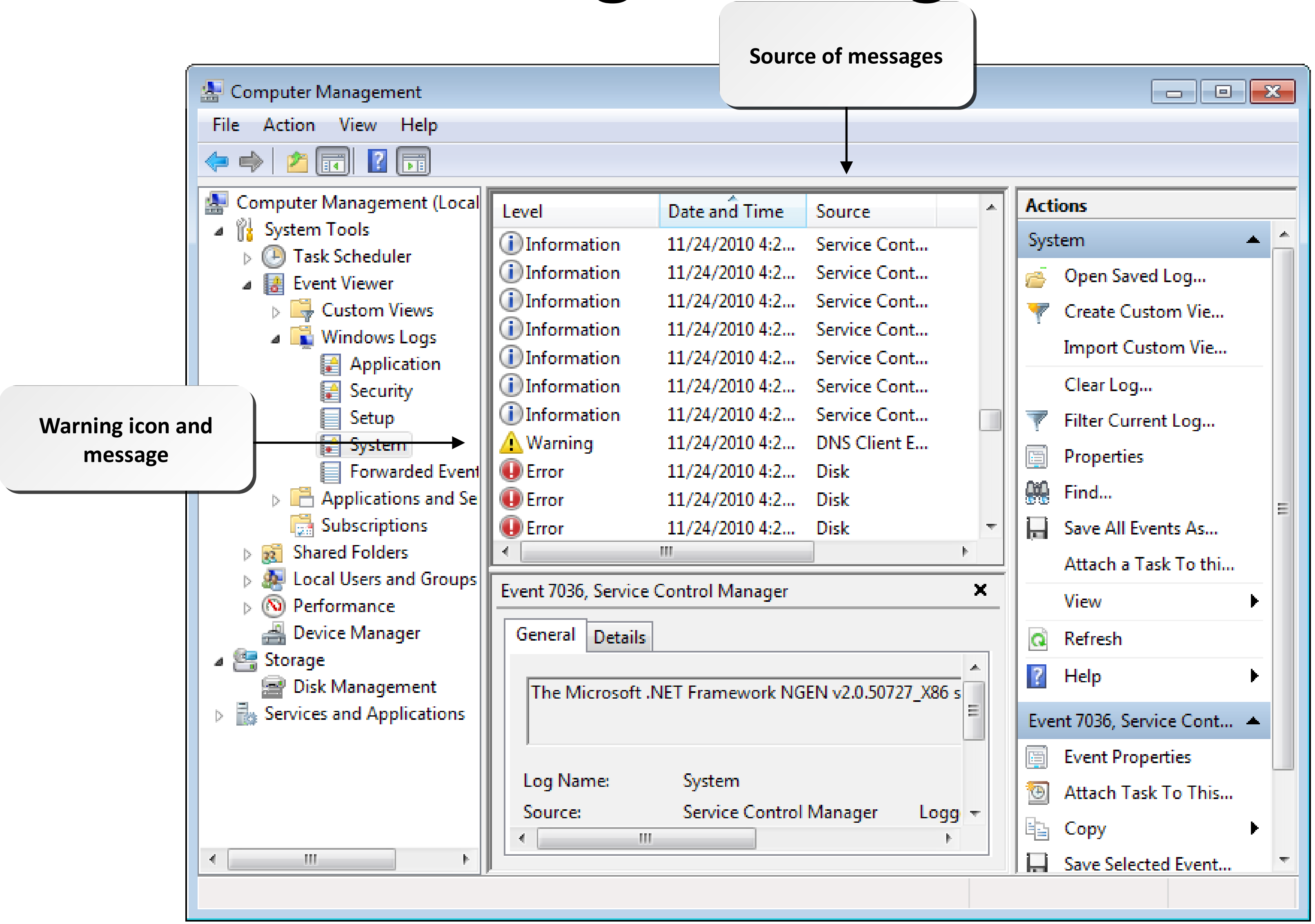
Boot Issues

- POST errors.
- Invalid boot disk.
- Failure to boot.
- Missing OS.
- Continuous reboot.
- Missing NTLDR (NT Loader).
- Missing dll message. Possible virus issue. Boot to safe mode and run virus scan.
- System files fail to open or are missing.
- Device or service failed during startup.
- Boots to safe mode.
- Device or program in registry not found.

Common Operating System Symptoms

- General issues.
- Memory issues.
- Low system performance and disk issues.
  - Empty the Temporary folders.
  - Run disk clean up
- CPU issues.
- Kernel panic. Issues with loading hardware devices.
- Shutdown issues.
  - Improper shutdown can cause file corruption
- RAID not detected.

Error and Warning Messages in Event Viewer



Source of messages

Warning icon and message

Level	Date and Time	Source
Information	11/24/2010 4:2...	Service Cont...
Information	11/24/2010 4:2...	Service Cont...
Information	11/24/2010 4:2...	Service Cont...
Information	11/24/2010 4:2...	Service Cont...
Information	11/24/2010 4:2...	Service Cont...
Information	11/24/2010 4:2...	Service Cont...
Information	11/24/2010 4:2...	Service Cont...
Warning	11/24/2010 4:2...	DNS Client E...
Error	11/24/2010 4:2...	Disk
Error	11/24/2010 4:2...	Disk
Error	11/24/2010 4:2...	Disk

Event 7036, Service Control Manager

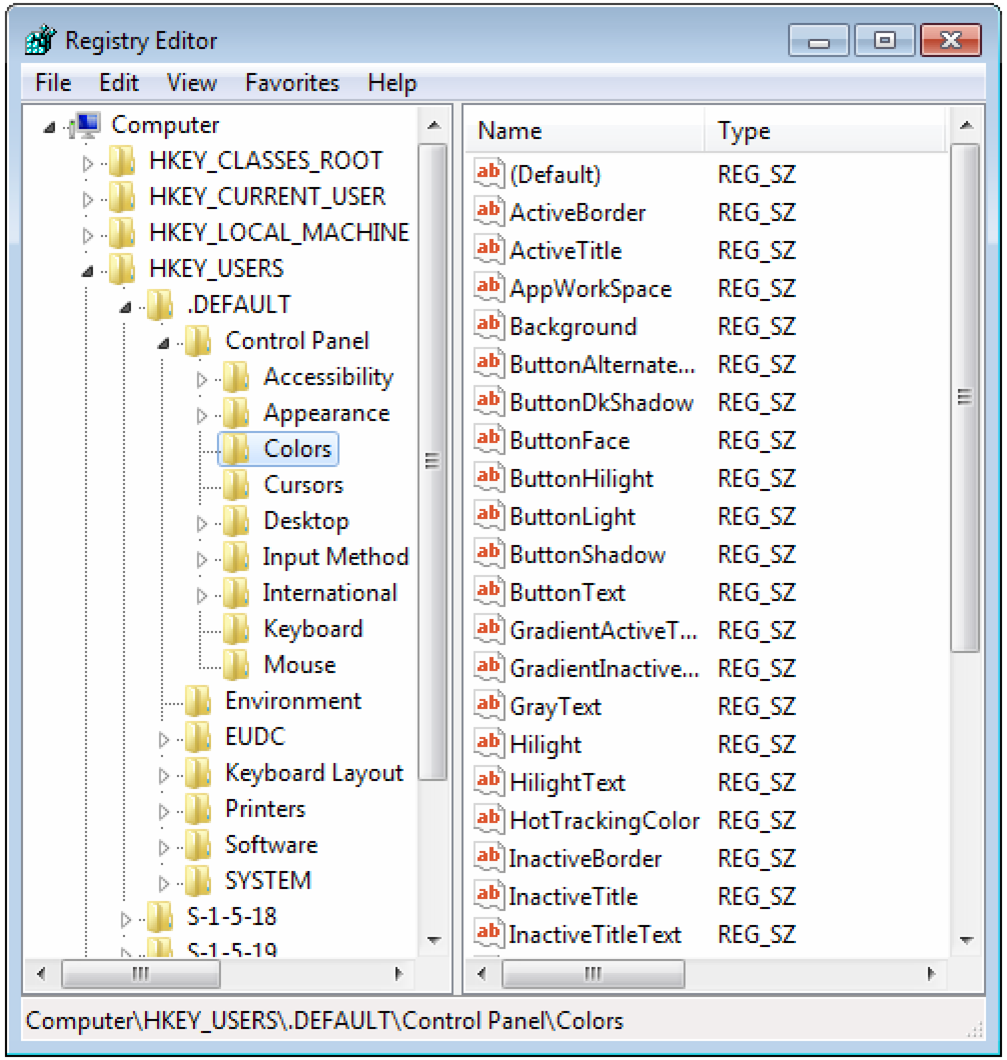
The Microsoft .NET Framework NGEN v2.0.50727_X86 s

Log Name: System

Source: Service Control Manager

Registry Error Messages

- Extremely Rare
- Stop errors or other errors.
- Registry access, value entries, or files.
- Maintain registry backups.
- Find errors in KnowledgeBase.



- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
    - .DEFAULT
      - Control Panel
        - Accessibility
        - Appearance
        - Colors
        - Cursors
        - Desktop
        - Input Method
        - International
        - Keyboard
        - Mouse
      - Environment
      - EUDC
      - Keyboard Layout
      - Printers
      - Software
      - SYSTEM
    - S-1-5-18
    - S-1-5-19

Name	Type
(Default)	REG_SZ
ActiveBorder	REG_SZ
ActiveTitle	REG_SZ
AppWorkSpace	REG_SZ
Background	REG_SZ
ButtonAlternate...	REG_SZ
ButtonDkShadow	REG_SZ
ButtonFace	REG_SZ
ButtonHilight	REG_SZ
ButtonLight	REG_SZ
ButtonShadow	REG_SZ
ButtonText	REG_SZ
GradientActiveT...	REG_SZ
GradientInactive...	REG_SZ
GrayText	REG_SZ
Hilight	REG_SZ
HilightText	REG_SZ
HotTrackingColor	REG_SZ
InactiveBorder	REG_SZ
InactiveTitle	REG_SZ
InactiveTitleText	REG_SZ

Computer\HKEY_USERS\.DEFAULT\Control Panel\Colors

Common Mobile OS and Application Symptoms

- Mobile OS issues
  - Dim display
  - Nonresponsive touch screen or inaccurate response
  - No or spotty network connectivity
  - GPS malfunction
  - Cannot broadcast to external monitor
  - Slow performance
  - Short battery life
  - Frozen system
  - System lockout

Common Mobile OS and Application Symptoms

- App issues
  - Apps not loading
  - Cannot decrypt email
  - Overheating
  - No sound from speakers

Mobile OS and Application Tools

- Performing a hard reset.
- Performing a soft reset.
- Performing a factory default reset.
- Closing running applications.
- Forcing applications to stop.
- Uninstalling and reinstalling applications.
- Adjusting device configuration and settings

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Troubleshoot password problems:
  - Develop a way to remember or safely record the mobile password.
  - Do not exceed the allowable number of failed password attempts.
  - Use a recovery password instead of restoring the device.
  - Refer to the user manual for device-specific restore methods.
  - If you are restoring a device using a PC, turn off the device, connect the USB cable to the PC and the device, and then turn on the power for the device.
  - Check for third-party Bluetooth Unlocker programs.
  - Be sure to back up or synchronize data regularly.

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Create secure passwords:
  - While setting a password, use a passphrase with special characters and keep it as unique as possible.
  - Make sure the password is of a length to make it strong but still be remembered easily.
  - Do not share password information with anyone.
  - Regularly change device passwords.
  - Avoid using the same password for a mobile device and other accounts.

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Troubleshoot hardware crashes:
  - Identify when the issue first started.
  - Check for recent hardware changes.
  - Check if the battery has enough power or any physical damage.
  - Check if the device is getting charged properly. A brand new device should be charged for at least 4 hours.
  - Check if the device is low on resources.
  - After the exact issue is identified, perform resolution steps in a sequential order.
    - Back up data before making any changes to the device.
    - Visit the manufacturer's website to check for device-specific troubleshooting steps.
    - Log resolution steps to take preventive measures to eliminate further issues.

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Troubleshoot software crashes:
  - Check for recent software changes.
  - Determine if the device crashes while running a specific application or all applications.
  - Check if the issue persists in safe mode.
  - Identify conflicting applications and uninstall them.
  - Remove unnecessary background applications.
  - Check if the firewall is properly configured.
  - Ensure that security software is working fine and does not conflict with firewall or other programs.
  - After the exact issue is identified, perform resolution steps in a sequential order.

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Troubleshoot OS and application upgrade issues:
  - Make sure the device is connected to the Internet.
  - Ensure that you have enough available bandwidth or sufficient remaining megabytes or gigabytes on your data plan.
  - Check the manufacturer or app store website for known issues with different platform versions.
- Troubleshoot authentication and authorization issues:
  - Verify you are using the correct password.
  - Make sure Caps Lock is not enabled.
- Troubleshoot signal loss:
  - Verify that the signal strength is sufficient to ensure good connectivity.
  - A loss in signal can be due to roaming out of a coverage area or during a handover from one cell tower to another congested cell tower.
  - Any physical damage to the device will impact radio reception, resulting in poor quality.

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Troubleshoot network problems:
  - Verify you are connected to a WAP.
  - Verify you have an IP address after connecting to the WAP.
  - The service over a network will either be unavailable or deteriorate during busy traffic times.
  - The network performance will deteriorate due to attacks such as DoS, network jamming, or scanning.
  - If connecting using 2G/3G, remember that you could connect to a cell tower and get an IP address, but not have sufficient download capability left on your data plan, or the provider's broadband network is too congested.

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Troubleshoot roaming issues:
  - Ensure that the mobile subscription includes roaming either to partner networks or international roaming.
  - Check your pre-paid balance while roaming, since roaming charges tend to be higher than other connectivity. You might have run out of minutes or data.
- Troubleshoot cellular activation and authorization:
  - Services to a mobile device will start only after the service is activated.
  - If the devices are grey listed or black listed, services will be blocked. Devices that are grey listed or black listed when devices are stolen, bills aren't paid, mobile services are used illegally, etc.

Guidelines for Troubleshooting Mobile Device Operating Systems and Applications

- Troubleshoot email issues:
  - Ensure that the email settings, such as protocol (SMTP, POP3, or IMAP), server addresses, ports, and security settings, are set properly.
  - Ensure that the email password is accurate.
- Troubleshoot VPN issues:
  - Ensure that you are connected to the Internet.
  - Ensure that the VPN client is running on the device.
  - Ensure that the credentials being provided to access the VPN are correct.
  - Ensure that you are not behind an older wireless access point (WAP) or router that disallows certain types of VPNs.

Linux and OS X Networking Tools

Utility	Description
traceroute	Tracks the route that data takes to get to its destination.
ping	Verifies that a system can be reached on a network. It checks the hostname, the IP address, and whether the remote system can be reached.
arp	Displays information about the ARP cache, including hardware address, host name, and network interfaces.
ifconfig	Display the local system’s network interface information, including IP address, hostname, and subnet mask. This tool also allows you to configure these parameters.

Network Troubleshooting Tools

- Cable tester
- Loopback plug
- Punch down tool
- Tone generator and probe
- Crimpers
- Wire strippers
- Wireless locator

Common PC Security Issues

- Pop-ups (Opens windows on top of the active window)
- Pop-Under (opens windows behind active window)
- Browser redirection
- Security alerts
- Internet connectivity issues
- Slow performance
- PC locks up
- Applications crash
- Windows update fails

Common PC Security Issues

- Rogue antivirus (appears to run like an antivirus program)
- Email issues
  - Spam
  - Compromised Account
- Access denied
- Malware infestation
- File system issues
- Invalid certificate
- Data access issues
- Backup security

Security Troubleshooting Tools

Tool	Description
Anti-malware/ antivirus software	This software scans a potentially infected system for malware and identifies any file signatures it recognizes as malicious. Most anti-malware solutions also provide quarantine and deletion functionality.
Recovery Console	An operating system's recovery console provides an interface with which you can execute a limited set of actions that may help you resolve boot issues. Common recovery options include repairing master boot records, formatting drive volumes, and repairing disk corruption.
MSCONFIG/safe boot option	MSCONFIG is a System Configuration utility that can also help you troubleshoot boot and system startup issues. The utility allows you to select and deselect certain services and device drivers you do or do not want to boot with. Likewise, safe boot loads the operating system with only non-essential functionality, making it easier to isolate and remove a malware infection.
Refresh/restore options	Newer versions of Windows offer certain recovery scenarios that may resolve system slowness or corruption. Recovery scenarios include reinstalling the operating system but keeping all other files; rolling back to a previous build of the operating system; and full recovery from an operating system image.

Security Troubleshooting Tools

Tool	Description
Terminal	A PC’s terminal or command-line interface will provide you with direct access to the operating system’s available commands. This can be useful as configuration GUIs like the Control Panel don’t offer access to every single diagnostic or troubleshooting command. Some of these commands, like CHKDSK, are more commonly initiated through a terminal.
System restore/ snapshot	Operating systems like Windows can take a “snapshot” of your PC at a certain point in time. If you encounter a complex issue that isn’t easily remedied, you can restore the previous snapshot and return your PC to its state before the issue appeared. This may be more ideal than a typical recovery operation as it affords minimal disruption to the system.
Pre-installation environments	Most operating systems offer some sort of configuration options as part of the installation process. For example, when you install Windows, you can format your computer’s disk volumes without even needing an operating system. If you have installation media available, the pre-installation environment can help you ensure that a computer is completely wiped clean.
Event Viewer	The operating system’s Event Viewer keeps a log of all recorded system and application events. This includes sign on attempts, shutdown signals, system crashes, device driver errors, and many more scenarios that can help you identify where problems exist.

The Malware Removal Process

1. Identify malware symptoms.
2. Quarantine infected systems.
3. Disable system restore.
4. Remediate infected systems.
5. Schedule scans and updates.
6. Enable system restore and create restore point.
7. Educate end users.

Malware Removal Best Practices

- Always use trusted installation sources and websites.
- Always use email attachment protection.
- Research malware types

Common Mobile Device Security Symptoms

- Signal drop or weak signal.
- Power drain.
- Slow data speeds.
- Unintended Wi-Fi connection or Bluetooth pairing.
- Leaked personal files or data.
- Data transmission over plan limit.
- Unauthorized access.
- High resource utilization.

Mobile Security Tools

- Antivirus and antimalware apps.
- App scanner.
- Factory reset or clean install.
- Uninstall and reinstall apps.
- Wi-Fi analyzer.
- Cell tower analyzer.
- Backup/restore.
- Force stop.

Guidelines for Troubleshooting Security Issues

- Maintenance:
  - Check status of physical security controls.
  - Review security videos.
  - Audit key systems and review audit logs.
  - Calibrate physical security devices.
  - Review organizational security policies.
  - Perform security audits.
  - Consider staging attacks to identify vulnerabilities.

Guidelines for Troubleshooting Security Issues

- Troubleshooting:
  - When users can’t access web sites, check security settings on the web browser.
  - When users can’t access files, check file permissions and effective permissions for the user, and check for file encryption.
  - When users can’t access network resources, check share permissions, NTFS permissions, and effective permissions.
  - When users can’t log with a biometric device, contact the vendor.
  - Train users to recognize security threats.
  - If users can’t access external data, check firewall ports for restrictiveness.