PKU--LL105-调试之道

阶段一：调试基础

- Software bug: https://en.wikipedia.org/wiki/Software_bug
    - A software bug is an error, flaw, failure, or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways.
    - Severity of a Bug:
        - "crash or hang", "no workaround" (meaning there is no way the customer can accomplish a given task), "has workaround" (meaning there is a way for the user to recover and accomplish the task), "UI" or "visual defect" (for example, a missing image or displaced button or form element), or "documentation error".
        - Some software publishers use more qualified severities such as "critical", "high", "low," "blocker," or "trivial".
    - Common types of computer bugs
        - Arithmetic bugs
        - Logic bugs
        - Syntax bugs
        - Resource bugs
        - Multi-threading programming bugs
        - Interfacing bugs
        - Performance bugs
        - Teamworking bugs
    - Bug bounty program: https://en.wikipedia.org/wiki/Bug_bounty_program
        - Bug赏金计划
        - A bug bounty program is a deal offered by many website and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities.
    - Bug tracking system: http://en.wikipedia.org/wiki/Bug_tracking_system
        - 缺陷跟踪系统
        - A bug tracking system or defect tracking system is a software application that keeps track of reported software bugs in software development projects. It may be regarded as a type of issue tracking system.
    - Heisenbug：https://en.wikipedia.org/wiki/Heisenbug
        - In computer programming jargon, a heisenbug is a software bug that seems to disappear or alter its behavior when one attempts to study it.
- Debugging：http://en.wikipedia.org/wiki/Debugging
    - Debugging is a methodical process of finding and reducing the number of bugs, or defects, in a computer program or a piece of electronic hardware, thus making it behave as expected.
    - Techniques:
        - Print debugging (or tracing)
        - Remote debugging
        - Post-mortem（死后的）debugging
            - Core dump：https://en.wikipedia.org/wiki/Core_dump
                - In computing, a core dump (in Unix parlance), memory dump, or system dump consists of the recorded state of the working memory of a computer program at a specific time, generally when the program has terminated abnormally (crashed).
                - The name comes from magnetic core memory, the principal form of random access memory from the 1950s to the 1970s. The name has remained long after magnetic core technology became obsolete.
        - "Wolf fence" algorithm
            - "There's one wolf i[illegible]ska; how do you find it? First build a fence down the middle of the state, wait for the wolf to howl, determine which side of the fence it is on. Repeat process on that side only, until you get to the point where you can see the wolf."
            - Bisection: https://en.wikipedia.org/wiki/Bisection_(software_engineering)
                - Bisection is a method used in software development to identify change sets that result in a specific behavior change. It is mostly employed for finding the patch that introduced a bug. Another application area is finding the patch that indirectly fixed a bug.
                - the bisect commands of revision control systems (eg, git-bisect, svn-bisect, hg-bisect, etc.)
        - Delta Debugging: https://en.wikipedia.org/wiki/Delta_Debugging
            - Delta Debugging is a methodology to automate the debugging of programs using a scientific approach of hypothesis-trial-result loop. This methodology was first developped by Andreas Zeller of the Saarland University in 1999.
        - Saff Squeeze
    - Anti-debugging
        - "the implementation of one or more techniques within computer code that hinders attempts at reverse engineering or debugging a target process".
        - It is actively used by recognized publishers in copy-protection schemas, but is also used by malware to

complicate its detection and elimination.

- Debugger：https://en.wikipedia.org/wiki/Debugger
  - A debugger or debugging tool is a computer program that is used to test and debug other programs (the "target" program).
  - Typically, debuggers offer a query processor, symbol resolver, expression interpreter, and debug support interface at its top level.
  - Debuggers also offer more sophisticated functions such as running a program step by step (single-stepping or program animation), stopping (breaking) (pausing the program to examine the current state) at some event or specified instruction by means of a breakpoint, and tracking the values of variables.
  - Program animation: https://en.wikipedia.org/wiki/Program_animation
    - Program animation or Stepping refers to the now very common debugging method of executing code one "line" at a time.
  - Breakpoint: https://en.wikipedia.org/wiki/Breakpoint
    - In software development, a breakpoint is an intentional stopping or pausing place in a program, put in place for debugging purposes. It is also sometimes simply referred to as a pause.
- Debugging data format: https://en.wikipedia.org/wiki/Debugging_data_format
  - A debugging data format is a means of storing information about a compiled computer program for use by high-level debuggers. Modern debugging data formats store enough information to allow source-level debugging.
  - stabs: https://en.wikipedia.org/wiki/Stabs
    - (s)ymbol (tab)le entrie(s)
    - stabs (sometimes written STABS) is a debugging data format for storing information about computer programs for use by symbolic and source-level debuggers.

自学：

- Software bug: https://en.wikipedia.org/wiki/Software_bug
- Bug bounty program: https://en.wikipedia.org/wiki/Bug_bounty_program
- Bug tracking system: http://en.wikipedia.org/wiki/Bug_tracking_system
- Heisenbug：https://en.wikipedia.org/wiki/Heisenbug
- Debugging：http://en.wikipedia.org/wiki/Debugging
- Core dump：https://en.wikipedia.org/wiki/Core_dump
- Bisection: https://en.wikipedia.org/wiki/Bisection_(software_engineering)
- Delta Debugging: https://en.wikipedia.org/wiki/Delta_Debugging
- Debugger：https://en.wikipedia.org/wiki/Debugger
- Program animation: https://en.wikipedia.org/wiki/Program_animation
- Breakpoint: https://en.wikipedia.org/wiki/Breakpoint
- Debugging data format: https://en.wikipedia.org/wiki/Debugging_data_format
- stabs: https://en.wikipedia.org/wiki/Stabs

See Also:

- https://bugs.launchpad.net/ubuntu/+source/linux/+bugs

阶段二：内核调试入门

- Fatal system error: https://en.wikipedia.org/wiki/Fatal_system_error
  - A fatal system error, also known as a system crash, stop error, kernel error, or bug check, is when an operating system halts at the moment it reaches a condition where it cannot operate safely.
  - Not to be confused with fatal exception error.
    - Fatal exception error: https://en.wikipedia.org/wiki/Fatal_exception_error
      - In computing, a fatal error or fatal exception error is an error that causes a program to abort and may therefore return the user to the operating system. When this happens, data that the program was processing may be lost.
  - Kernel panic: https://en.wikipedia.org/wiki/Kernel_panic
    - A kernel panic is an action taken by an operating system upon detecting an internal fatal error from which it cannot safely recover.
    - The term is largely specific to Unix and Unix-like systems; for Microsoft Windows operating systems the equivalent term is "stop error" (or, colloquially, "Blue Screen of Death").
  - BSoD: https://en.wikipedia.org/wiki/Blue_Screen_of_Death
    - The Blue Screen of Death (also known as a Stop Error, Blue Screen of Doom, or BSoD) is an error screen displayed on a Microsoft Windows computer system after a fatal system error, also known as a system crash: when the operating system reaches a condition where it can no longer operate safely.
- Crash and hang:
  - Crash: https://en.wikipedia.org/wiki/Crash_(computing)
    - A crash (or system crash) in computing is when a computer program (such as a software application or an operating system) stops functioning properly.
  - Hang: https://en.wikipedia.org/wiki/Hang_(computing)
    - In computing, a hang or freeze occurs when either a computer program or system ceases to respond to

inputs.

    - A typical example is a graphical user interface that no longer responds to the user's keyboard or mouse, but the term covers a wide range of behaviors in both clients and servers, and is not limited to graphical user interface issues.
    - The fundamental reason is typically **resource exhaustion**: resources necessary for some part of the system to run are not available, due to being in use by other processes or simply insufficient.
    - Hangs have varied causes and symptoms, including software or hardware defects, such as an infinite loop or long-running uninterruptible computation, resource exhaustion (thrashing), under-performing hardware (throttling), external events such as a slow computer network, misconfiguration, and compatibility problems.
    - Often the cause is an interaction of multiple factors, making "hang" a loose umbrella term rather than a technical one.
      - umbrella term: 涵盖性术语
    - A hang differs from a crash, in which the failure is immediate and unrelated to the responsiveness of inputs.
- Tools:
  - Kernel debugger: https://en.wikipedia.org/wiki/Kernel_debugger
    - A kernel debugger is a debugger present in some kernels to ease debugging and kernel development by the kernel developers.
    - A kernel debugger might be a stub implementing low-level operations, with a full-blown debugger such as gdb, running on another machine, sending commands to the stub over a serial line or a network connection, or it might provide a command line that can be used directly on the machine being debugged.
  - Crash reporter: https://en.wikipedia.org/wiki/Crash_reporter
    - A crash reporter is an application whose function is to report crash details.
    - Crash reports often include data such as stack traces, type of crash, and version of software. This information helps software developers to diagnose and fix the underlying problem causing the crash.
    - Windows Error Reporting: https://en.wikipedia.org/wiki/Windows_Error_Reporting
      - Windows Error Reporting (WER) (codenamed Watson) is a crash reporting technology introduced by Microsoft with Windows XP and included in later Windows versions and Windows Mobile 5.0 and 6.0.
      - Not to be confused with the Dr. Watson debugging tool which left the memory dump on the user's local machine, Windows Error Reporting collects and offers to send post-error debug information (a memory dump) using the Internet to the Microsoft or stops responding on a user's desktop.
  - Linux kernel oops: https://en.wikipedia.org/wiki/Linux_kernel_oops
    - See also: http://oops.kernel.org/
    - In computing, an oops is a deviation from correct behavior of the Linux kernel, one that produces a certain error log.
    - The term does not stand for anything, other than that it is a simple mistake.
  - Kdump: https://en.wikipedia.org/wiki/Kdump_(Linux)
    - kdump is the Linux kernel's built-in crash dump mechanism. In the event of a kernel crash, kdump creates a memory image (also known as vmcore) that can be analyzed for the purposes of debugging and determining the cause of a crash.
- Printk：https://en.wikipedia.org/wiki/Printk
  - printk is a function that prints messages and is used in the C Programming Language exclusively for the Linux Kernel. It accepts a string parameter called the format string, which specifies a method for rendering an arbitrary number of varied data type parameter(s) into a string. The string is then printed to the kernel log.
  - printk debugging (the same as printf debugging)
    - 实际上是在用人脑进行逻辑思维
    - 两个重要的宏：__func__, __LINE__
      - Standard Predefined Macros: http://gcc.gnu.org/onlinedocs/cpp/Standard-Predefined-Macros.html
      - Function Names: http://gcc.gnu.org/onlinedocs/gcc/Function-Names.html
  - printk has an optional first parameter: Loglevel.
    - Different Loglevels are shown here:
      - KERN_EMERG Emergency condition, system is probably dead
      - KERN_ALERT Some problem has occurred, immediate attention is needed
      - KERN_CRIT A critical condition
      - KERN_ERR An error has occurred
      - KERN_WARNING A warning
      - KERN_NOTICE Normal message to take note of
      - KERN_INFO Some information
      - KERN_DEBUG Debug information related to the program
    - When a log level is not specified, the default log level is KERN_WARNING.
      - If the priority is less than int console_loglevel, the message is printed on your current terminal.
  - Kernel parameter: ignore_loglevel
    - can be set in command line or /sys/modules/printk/parameters

自学：

- Fatal system error: https://en.wikipedia.org/wiki/Fatal_system_error

- Fatal exception error: https://en.wikipedia.org/wiki/Fatal_exception_error
- Kernel panic: https://en.wikipedia.org/wiki/Kernel_panic
- BSoD: https://en.wikipedia.org/wiki/Blue_Screen_of_Death
- Crash: https://en.wikipedia.org/wiki/Crash_(computing)
- Hang: https://en.wikipedia.org/wiki/Hang_(computing)
- Kernel debugger: https://en.wikipedia.org/wiki/Kernel_debugger
- Crash reporter: https://en.wikipedia.org/wiki/Crash_reporter
- Windows Error Reporting: https://en.wikipedia.org/wiki/Windows_Error_Reporting
- Linux kernel oops: https://en.wikipedia.org/wiki/Linux_kernel_oops
- Kdump: https://en.wikipedia.org/wiki/Kdump_(Linux)
- Printk：https://en.wikipedia.org/wiki/Printk

See also:

- Documentation/oops-tracing.txt
- Documentation/kdump/
- http://oops.kernel.org/

阶段三：函数跟踪

- Subroutine：https://en.wikipedia.org/wiki/Subroutine
    - In computer programming, a subroutine is a sequence of program instructions that perform a specific task, packaged as a unit. This unit can then be used in programs wherever that particular task should be performed.
    - Subprograms may be defined within programs, or separately in libraries that can be used by multiple programs. In different programming languages, a subroutine may be called a procedure, a function, a routine, a method, or a subprogram.
    - The generic term callable unit is sometimes used.
    - The subroutine typically requires standard housekeeping code – both at entry to, and exit from, the function (function prologue and epilogue – usually saving general purpose registers and return address as a minimum).
        - Housekeeping: https://en.wikipedia.org/wiki/Housekeeping_(computing)
            - 家政管理，公司经营，（计算机）整理工作、内务处理
            - Housekeeping could include (but is not limited to) the following activities:
                - Saving and restoring program state for called functions (including general purpose registers and return address)
                - Obtaining local memory on the stack
                - Initializing local variables at the start of a program or function
                - Freeing local memory on the stack on exit from a function
                - Garbage collection
                - data conversion
                - Backup and/or removal of un-needed files and software
                - Execution of Disk maintenance utilities (e.g. ScanDisk, Harddrive Defragmenters, Virus Scanner)
        - Function Prologue and epilogue: https://en.wikipedia.org/wiki/Function_prologue
            - In assembly language programming, the function prologue is a few lines of code at the beginning of a function, which prepare the stack and registers for use within the function.
            - Similarly, the function epilogue appears at the end of the function, and restores the stack and registers to the state they were in before the function was called.
            - The prologue and epilogue are not a part of the assembly language itself; they represent a convention used by assembly language programmers, and compilers of many higher-level languages. They are fairly rigid, having the same form in each function.
    - Calling convention: https://en.wikipedia.org/wiki/Calling_convention
        - In computer science, a calling convention is an implementation-level (low-level) scheme for how subroutines receive parameters from their caller and how they return a result.
        - Differences in various implementations include where parameters, return values and return addresses are placed, and how the tasks of preparing for a function call and cleaning up the environment afterward are divided between the caller and the callee.
    - Call stack: https://en.wikipedia.org/wiki/Call_stack
        - In computer science, a call stack is a stack data structure that stores information about the active subroutines of a computer program.
        - This kind of stack is also known as an execution stack, control stack, run-time stack, or machine stack, and is often shortened to just "the stack".
        - Stack trace: https://en.wikipedia.org/wiki/Stack_trace
            - In computing, a stack trace (also called stack backtrace or stack traceback) is a report of the active stack frames at a certain point in time during the execution of a program.
            - The GNU C Library: Backtraces: http://www.gnu.org/software/libc/manual/html_node/Backtraces.html
            - The Python Standard Library: traceback: https://docs.python.org/3/library/traceback.html
- Call graph: https://en.wikipedia.org/wiki/Call_graph
    - A call graph (also known as a call multigraph) is a directed graph (and more specifically a flow graph) that represents calling relationships between subroutines in a computer program.

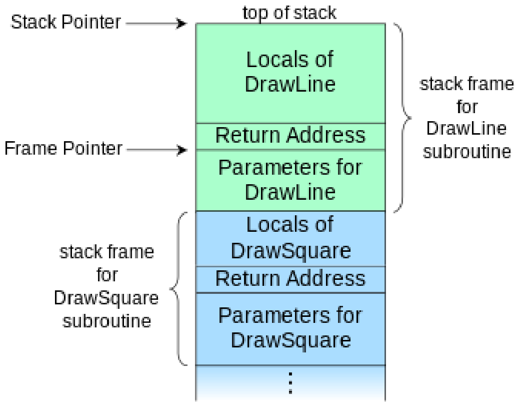
    - Specifically, each node represents a procedure and each edge (f, g) indicates that procedure f calls procedure g. Thus, a cycle in the graph indicates recursive procedure calls.
    - Call graphs can be dynamic or static.
        - A dynamic call graph is a record of an execution of the program, e.g., as output by a profiler. Thus, a dynamic call graph can be exact, but only describes one run of the program.
        - A static call graph is a call graph intended to represent every possible run of the program. The exact static call graph is an undecidable problem（不可判定问题）, so static call graph algorithms are generally overapproximations.
    - Call graph generators:（有很多，这里只介绍gprof）
        - Gprof：https://en.wikipedia.org/wiki/Gprof
            - Gprof is a performance analysis tool for Unix applications. It uses a hybrid of instrumentation and sampling and was created as extended version of the older "prof" tool. Unlike prof, gprof is capable of limited call graph collecting and printing.
            - Instrumentation code is automatically inserted into the program code during compilation (for example, by using the '-pg' option of the gcc compiler), to gather caller-function data. A call to the monitor function 'mcount' is inserted before each function call.
            - Sampling data is saved in 'gmon.out' or in 'progname.gmon' file just before the program exits, and can be analyzed with the 'gprof' command-line tool. Several gmon files can be combined with 'gprof -s' to accumulate data from several runs of a program.
- Kernel Tracers:
    - Kernel marker: https://en.wikipedia.org/wiki/Kernel_marker
        - Kernel markers were a static kernel instrumentation support mechanism for Linux kernel source code, allowing special tools such as LTTng[1] or SystemTap[2] to trace information exposed by these probe points.
    - Ftrace: https://en.wikipedia.org/wiki/Ftrace
        - ftrace (abbreviated from Function Tracer) is a tracing framework for the Linux kernel.
        - Although its original name, Function Tracer, came from ftrace's ability to record information related to various function calls performed while the kernel is running, ftrace's tracing capabilities cover a much broader range of kernel's internal operations.
    - LTTng: https://en.wikipedia.org/wiki/LTTng
        - LTTng (Linux Trace Toolkit Next Generation) is a system software package for correlated tracing of the Linux kernel, applications and libraries.
        - LTTng consists of kernel modules (for Linux kernel tracing) and dynamically linked libraries (for application and library tracing).

自学：

- Subroutine：https://en.wikipedia.org/wiki/Subroutine
- Housekeeping: https://en.wikipedia.org/wiki/Housekeeping_(computing)
- Function Prologue and epilogue: https://en.wikipedia.org/wiki/Function_prologue
- Calling convention: https://en.wikipedia.org/wiki/Calling_convention
- Call stack: https://en.wikipedia.org/wiki/Call_stack
- Stack trace: https://en.wikipedia.org/wiki/Stack_trace
- Gprof：https://en.wikipedia.org/wiki/Gprof
- Kernel marker: https://en.wikipedia.org/wiki/Kernel_marker
- Ftrace: https://en.wikipedia.org/wiki/Ftrace
- LTTng: https://en.wikipedia.org/wiki/LTTng

See Also:

- Documentation/trace/
- The GNU C Library: Backtraces: http://www.gnu.org/software/libc/manual/html_node/Backtraces.html
- The Python Standard Library: traceback: https://docs.python.org/3/library/traceback.html
- Debugging the kernel using Ftrace - part 1：https://lwn.net/Articles/365835/
- Debugging the kernel using Ftrace - part 2：https://lwn.net/Articles/366796/



阶段四：系统日志

- Log management: https://en.wikipedia.org/wiki/Log_management
    - Log management (LM) comprises an approach to dealing with large volumes of computer-generated log messages (also known as audit records, audit trails, event-logs, etc.).
    - LM covers:
        - log collection （日志采集）
        - centralized aggregation（聚合，整合）
        - long-term retention（保留、保存）
        - log rotation （日志回旋）
            - 日志回旋可以设定日志的回旋是基于文件大小还是基于时间间隔。当满足其中的一个条件时，当前访问日志被关闭，新的访问日志被创建。
        - log analysis (in real-time and in bulk after storage)
        - log search and reporting
    - Suggestions were made to change the definition of logging. This change would keep matters both more pure and more easily maintainable:
        - Logging would then be defined as all instantly discardable data on the technical process of an application or website, as it represents and processes data and user input.
        - Auditing, then, would involve data that is not immediately discardable. In other words: data that is assembled in the auditing process, is stored persistently, is protected by authorization schemes and is, always, connected to some end-user functional requirement.
- syslog: https://en.wikipedia.org/wiki/Syslog
    - In computing, syslog is a widely used standard for message logging.
    - It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them.
    - Computer system designers may use syslog for system management and security auditing as well as general informational, analysis, and debugging messages.
    - Syslog Message Facilities
        - 0 kernel messages
        - 1 user-level messages
        - 2 mail system
        - 3 system daemons
        - 4 security/authorization messages
        - 5 messages generated internally by syslogd
        - 6 line printer subsystem
        - 7 network news subsystem
        - 8 UUCP subsystem
        - 9 clock daemon
        - ......
    - Syslog Message Severities
        - 0 Emergency: system is unusable
        - 1 Alert: action must be taken immediately
        - 2 Critical: critical conditions
        - 3 Error: error conditions
        - 4 Warning: warning conditions
        - 5 Notice: normal but significant condition
        - 6 Informational: informational messages
        - 7 Debug: debug-level messages
    - The GNU C Library: Syslog: http://www.gnu.org/software/libc/manual/html_node/Syslog.html
- Syslog deamons:
    - History：syslogd and klogd
    - Rsyslog: https://en.wikipedia.org/wiki/Rsyslog
        - Rsyslog is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network.
        - It implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, flexible configuration options and adds features such as using TCP for transport.
        - The official RSYSLOG website defines the utility as "the rocket-fast system for log processing".
    - Syslog-ng：https://en.wikipedia.org/wiki/Syslog-ng
        - syslog-ng is an open source implementation of the Syslog protocol for Unix and Unix-like systems.
        - It extends the original syslogd model with content-based filtering, rich filtering capabilities, flexible configuration options and adds important features to syslog, like using TCP for transport.
        - As of today syslog-ng is developed by Balabit IT Security Ltd. It has two editions with a common codebase.
            - The first is called syslog-ng Open Source Edition (OSE) with the license LGPL.
            - The second is called Premium Edition (PE) and has additional plugins (modules) under proprietary license.
- Systemd：https://en.wikipedia.org/wiki/Systemd

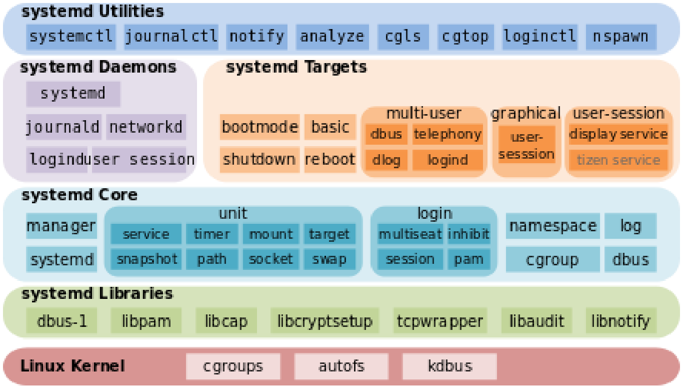
- 一统天下，是福是祸
- systemd is a suite of system management daemons, libraries, and utilities designed as a central management and configuration platform for the Linux computer operating system.
- Described by its authors as a "basic building block" for an operating system, systemd primarily aims to replace the Linux init system (the first process executed in user space during the Linux startup process) inherited from UNIX System V and Berkeley Software Distribution (BSD).
- One of systemd's main goals is to unify basic Linux configurations and service behaviors across all distributions.
- The design of systemd generated significant controversy within the free software community.
  - Critics argue that systemd's architecture violates the Unix philosophy and that it will eventually form a system of interlocking dependencies.
  - However, as of 2015 most major Linux distributions have adopted it as their default init system.
- In May 2014, Poettering further defined systemd as aiming to unify "pointless differences between distributions"（各发行版之间毫无意义的差异化）, by providing the following three general functions:
  - A system and service manager (manages both the system, as by applying various configurations, and its services)
  - A software platform (serves as a basis for developing other software)
  - The glue between applications and the kernel (provides various interfaces that expose functionalities provided by the kernel)
- As an integrated software suite, systemd replaces the startup sequences and runlevels controlled by the traditional init daemon, along with the shell scripts executed under its control. systemd also integrates many other services that are common on Linux systems by handling user logins, the system console, device hotplugging (see udev), scheduled execution (replacing cron) logging, hostnames and locales.
- Usage:
  - systemctl list-unit-files
  - systemd-analyze
  - /etc/systemd/
  - journalctl

自学：

- Log management: https://en.wikipedia.org/wiki/Log_management
- syslog: https://en.wikipedia.org/wiki/Syslog
- Rsyslog: https://en.wikipedia.org/wiki/Rsyslog
- Syslog-ng：https://en.wikipedia.org/wiki/Syslog-ng
- Systemd：https://en.wikipedia.org/wiki/Systemd

See also:

- The Syslog Protocol：https://tools.ietf.org/html/rfc5424
- http://www.freedesktop.org/wiki/Software/systemd/
- The GNU C Library: Syslog: http://www.gnu.org/software/libc/manual/html_node/Syslog.html



（The architecture of systemd as it is used by Tizen）

其它建议内容：

- Computer and network surveillance: https://en.wikipedia.org/wiki/Computer_and_network_surveillance
  - surveillance: 监督；监视
- Double fault：https://en.wikipedia.org/wiki/Double_fault
  - On the x86 architecture, a double fault exception occurs if the processor encounters a problem while trying to service a pending interrupt or exception. An example situation when a double fault would occur is when an interrupt is triggered but the segment in which the interrupt handler resides is invalid.
- Triple fault: https://en.wikipedia.org/wiki/Triple_fault
  - A triple fault is a special kind of exception generated by the CPU when an exception occurs while the CPU is trying to invoke the double fault exception handler, which itself handles exceptions occurring while trying to invoke a regular exception handler.