howto, linux, monitoring, tools, top, htop, atop, netatop, apache, apachetop, modstatus, proftp, ftptop, mytop, mysql, mariadb, powertop, iotop, ntopng, iftop, jnettop, bandwidthd, etherape, ethtool, nethogs, iptraf, ngrep, mrtg, bmon, traceroute, traceroute6, tracert6, iptstate, darkstat, vnstat, netstat, ss, nmap, mtr, tcpdump, justniffer, serverdensity, opennms, sysusage, pcp, ksysguard, munin, nagios

Linux Diagnosis and Monitoring Tools

Sources

- https://www.serverdensity.com/monitor/linux/how-to/
- https://www.tecmint.com/linux-performance-monitoring-tools/
- https://www.tecmint.com/command-line-tools-to-monitor-linux-performance/

top

- https://en.wikipedia.org/wiki/Top_(software)
- https://www.tecmint.com/12-top-command-examples-in-linux/

top (table of processes) is a task manager program, found in many Unix-like operating systems, that displays information about CPU and memory utilization. The program produces an ordered list of running processes selected by user-specified criteria, and updates it periodically. Default ordering is by CPU usage, and only the top CPU consumers are shown. top shows how much processing power and memory are being used, as well as other information about the running processes. Some versions of top allow extensive customization of the display, such as choice of columns or sorting method. top is useful for system administrators, as it shows which users and processes are consuming the most system resources at any given time.

htop

- https://htop.dev/
- https://man7.org/linux/man-pages/man1/htop.1.html

htop is an interactive cross-platform process viewer. It is a text-mode application (for console or X terminals) and requires ncurses.

atop

- https://linux.die.net/man/1/atop
- https://www.atoptool.nl/

The program atop is an interactive monitor to view the load on a Linux system. It shows the occupation of the most critical hardware resources (from a performance point of view) on system level, i.e. cpu, memory, disk and network. It also shows which processes are responsible for the indicated load with respect to cpu- and memory load on process level. Disk load is shown if per process “storage accounting” is active in the kernel or if the kernel patch 'cnt' has been installed. Network load is only shown per process if the kernel patch 'cnt' has been installed.

Atop is an ASCII full-screen performance monitor for Linux that is capable of reporting the activity of all processes (even if processes have finished during the interval), daily logging of system and process activity for long-term analysis, highlighting overloaded system resources by using colors, etc. At regular intervals, it shows system-level activity related to the CPU, memory, swap, disks (including LVM) and network layers, and for every process (and thread) it shows e.g. the CPU utilization, memory growth, disk utilization, priority, username, state, and exit code. In combination with the optional kernel module netatop, it even shows network activity per process/thread.

apachetop

- https://github.com/JeremyJones/Apachetop
- https://github.com/JeremyJones/Apachetop/wiki

apachetop is a console-based (non-gui) tool for monitoring the threads and overall performance of a set of Apache web servers. It runs on Unix systems which have Perl, LWP, and TermReadKey installed. It is based largely on the excellent mytop tool written by Jeremy Zawodny. ===== Apache mod_status ===== * https://httpd.apache.org/docs/2.4/mod/mod_status.html The Status module allows a server administrator to find out how well their server is performing. A HTML page is presented that gives the current server statistics in an easily readable form. If required this page can be made to automatically refresh (given a compatible browser). Another page gives a simple

machine-readable list of the current server state. The details given are: * The number of workers serving requests * The number of idle workers * The status of each worker, the number of requests that worker has performed and the total number of bytes served by the worker (*) * A total number of accesses and byte count served (*) * The time the server was started/restarted and the time it has been running for * Averages giving the number of requests per second, the number of bytes served per second and the average number of bytes per request (*) * The current percentage CPU used by each worker and in total by all workers combined (*) * The current hosts and requests being processed (*) The lines marked “(*)” are only available if ExtendedStatus is On. In version 2.3.6, loading mod_status will toggle ExtendedStatus On by default. ===== ftptop ===== * https://linux.die.net/man/1/ftptop ftptop - display running status on proftpd server connections ===== mytop ===== * https://linux.die.net/man/1/mytop * https://jeremy.zawodny.com/mysql/mytop/ * https://jeremy.zawodny.com/mysql/mytop/mytop.html mytop is a console-based (non-gui) tool for monitoring the threads and overall performance of a MySQL 3.22.x, 3.23.x, and 4.x server. It runs on most Unix systems (including Mac OS X) which have Perl, DBI, and TermReadKey installed. And with TermANSIColor installed you even get color. If you install TimeHiRes, you'll get good real-time queries/second stats. As of version 0.7, it even runs on Windows (somewhat).

powertop

- https://github.com/fenrus75/powertop

PowerTOP is a Linux* tool used to diagnose issues with power consumption and power management. In addition to being a diagnostic tool, PowerTOP also has an interactive mode you can use to experiment with various power management settings, for cases where the Linux distribution has not enabled those settings.

iotop

- https://linux.die.net/man/1/iotop
- http://guichaz.free.fr/iotop/

Linux has always been able to show how much I/O was going on (the bi and bo columns of the vmstat 1 command). Iotop is a Python program with a top like UI used to show of behalf of which process is the I/O going on. It requires Python ≥ 2.7 and a Linux kernel ≥ 2.6.20 with the TASK_DELAY_ACCT CONFIG_TASKSTATS, TASK_IO_ACCOUNTING and CONFIG_VM_EVENT_COUNTERS options on.

ntopng

- https://www.ntop.org/products/traffic-analysis/ntop/

ntopng - High-Speed Web-based Traffic Analysis and Flow Collection. ntopng is the next generation version of the original ntop, a network traffic probe that monitors network usage. ntopng is based on libpcap/PF_RING and it has been written in a portable way in order to virtually run on every Unix platform, MacOS and on Windows as well. ntopng – yes, it’s all lowercase – provides a intuitive, encrypted web user interface for the exploration of realtime and historical traffic information.

iftop

- https://linux.die.net/man/8/iftop
- https://code.blinkace.com/pdw/iftop
- https://www.ex-parrot.com/pdw/iftop/

iftop is a free software command-line system monitor tool that produces a frequently updated list of network connections. By default, the connections are ordered by bandwidth usage, with only the “top” bandwidth consumers shown. The iftop website gives the following description: “iftop does for network usage what top(1) does for CPU usage. It listens to network traffic on a named interface and displays a table of current bandwidth usage by pairs of hosts. Handy for answering the question 'why is our ADSL link so slow?'”. iftop monitors network traffic and displays a table of current bandwidth usage. An interface may be specified or, if not, it will listen on the first interface it finds which looks like an external interface (with libpcap and libncurses). iftop must be run with sufficient permissions to monitor all network traffic; on most systems this means that it must be run as a root user, see sudo. By default, iftop will look up hostnames associated with addresses and counts all IP packets that pass through the filter. Hostname look-up can add substantial traffic, in and of itself, and may result in an inaccurate display of network traffic. You may wish to suppress display of DNS traffic by using filter code such as “not port domain”, or switch it off entirely, by using the -n option or by pressing “n” when the program is running. Using the -F option makes it possible to show packets entering and leaving a given network.

jnettop

- https://linux.die.net/man/8/jnettop

jnettop - View hosts/ports taking up the most network traffic. jnettop captures traffic coming across the host it is running on and displays streams sorted by bandwidth they use. Result is a nice listing of communication on network by host and port, how many bytes went through this transport and the bandwidth it is consuming.

bandwidthd

- http://bandwidthd.sourceforge.net/

BandwidthD tracks usage of TCP/IP network subnets and builds html files with graphs to display utilization. Charts are built by individual IPs, and by default display utilization over 2 day, 8 day, 40 day, and 400 day periods. Furthermore, each ip address's utilization can be logged out at intervals of 3.3 minutes, 10 minutes, 1 hour or 12 hours in cdf format, or to a backend database server. HTTP, TCP, UDP, ICMP, VPN, and P2P traffic are color coded. BandwidthD runs on most platforms including windows. Required libraries for unix are only: libpcap, libgl and libpng. Bandwidthd now produces output in 2 ways. The first is as a standalone application that produces static html and png output every 200 seconds. The second is as a sensor that transmits it's data to a backend database which is then reported on by dynamic php pages. The visual output of both is simular, but the database driven system allows for searching, filtering, multiple sensors and custom reports.

EtherApe

- https://etherape.sourceforge.io/

EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, IP and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display. It supports Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices, plus several encapsulation formats. It can filter traffic to be shown, and can read packets from a file as well as live from the network. Node statistics can be exported.

ethtool

- https://linux.die.net/man/8/ethtool
- https://git.kernel.org/pub/scm/network/ethtool/ethtool.git
- https://mirrors.edge.kernel.org/pub/software/network/ethtool/

ethtool is the standard Linux utility for controlling network drivers and hardware, particularly for wired Ethernet devices. It can be used to: Get identification and diagnostic information. Get extended device statistics. Control speed, duplex, autonegotiation and flow control for Ethernet devices. Control checksum offload and other hardware offload features. Control DMA ring sizes and interrupt moderation. Control receive queue selection for multiqueue devices. Upgrade firmware in flash memory. Most features are dependent on support in the specific driver. See the manual page for full information.

NetHogs

- https://linux.die.net/man/8/nethogs
- https://github.com/raboof/nethogs

NetHogs is a small 'net top' tool. Instead of breaking the traffic down per protocol or per subnet, like most tools do, it groups bandwidth by process. NetHogs does not rely on a special kernel module to be loaded. If there's suddenly a lot of network traffic, you can fire up NetHogs and immediately see which PID is causing this. This makes it easy to identify programs that have gone wild and are suddenly taking up your bandwidth. Since NetHogs heavily relies on /proc, most features are only available on Linux. NetHogs can be built on Mac OS X and FreeBSD, but it will only show connections, not processes.

iptraf

- http://iptraf.seul.org/

IPTraf is a console-based network statistics utility for Linux. It gathers a variety of figures such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts. An IP traffic monitor that shows information on the IP traffic passing over your network. Includes TCP flag information, packet and byte counts, ICMP details, OSPF packet types. General and detailed interface statistics showing IP, TCP, UDP, ICMP, non-IP and other IP packet counts, IP checksum errors, interface activity, packet size counts. A TCP and UDP service monitor showing counts of incoming and outgoing packets for common TCP and UDP application ports. A LAN statistics module that discovers active hosts and shows statistics showing the data activity on them. TCP, UDP, and other protocol display filters, allowing you to view only traffic you're interested in. Logging. Supports Ethernet, FDDI, ISDN, SLIP, PPP, and loopback interface types. Utilizes the built-in raw socket interface of the Linux kernel, allowing it to be used over a wide range of supported network cards. Full-screen, menu-driven operation.

ngrep

- https://github.com/jpr5/ngrep

ngrep is like GNU grep applied to the network layer. It's a PCAP-based tool that allows you to specify an extended regular or hexadecimal expression to match against data payloads of packets. It understands many kinds of protocols, including IPv4/6, TCP, UDP, ICMPv4/6, IGMP and Raw, across a wide variety of interface types, and understands BPF filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.

MRTG

- https://oss.oetiker.ch/mrtg/

Tobi Oetiker's MRTG - The Multi Router Traffic Grapher. You have a router, you want to know what it does all day long? Then MRTG is for you. It will monitor SNMP network devices and draw pretty pictures showing how much traffic has passed through each interface. Routers are only the beginning. MRTG is being used to graph all sorts of network devices as well as everything else from weather data to vending machines. MRTG is written in perl and works on Unix/Linux as well as Windows and even Netware systems. MRTG is free software licensed under the Gnu GPL.

bmon

- https://github.com/tgraf/bmon

bmon - Bandwidth Monitor. bmon is a monitoring and debugging tool to capture networking related statistics and prepare them visually in a human friendly way. It features various output methods including an interactive curses user interface and a programmable text output for scripting.

traceroute

- https://linux.die.net/man/8/traceroute

In computing, traceroute and tracert are computer network diagnostic commands for displaying possible routes (paths) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop is a measure of the total time spent to establish the connection. Traceroute proceeds unless all (usually three) sent packets are lost more than twice; then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point. For Internet Protocol Version 6 (IPv6) the tool sometimes has the name traceroute6 and tracert6.

IPTState

- https://www.phildev.net/iptstate/

IP Tables State. IPTState is a top-like interface to your netfilter connection-tracking table. Using iptstate you interactively watch where traffic crossing your netfilter/iptables firewall is going, sort by various criteria, limit the view by various criteria. But it doesn't stop there: as of version 2.2.0 you can even delete states from the table! The only requirements are a curses library (usually ncurses), and libnetfilter_conntrack version 0.0.50 or later. IPTState is now in the Debian, Redhat, Fedora Core, Mandrake, Gentoo, FloppyFW, and many other distributions you can find a list of.

darkstat

- https://linux.die.net/man/8/darkstat
- https://unix4lyfe.org/darkstat/
- https://github.com/emikulic/darkstat

darkstat captures network traffic, calculates statistics about usage, and serves reports over HTTP. Traffic graphs, reports per host, shows ports for each host. Embedded web-server with deflate compression. Asynchronous reverse DNS resolution using a child process. Small. Portable. Single-threaded. Efficient. Supports IPv6.

vnStat

- https://humdi.net/vnstat/
- https://github.com/Hulxv/vnstat-client

vnStat is a console-based network traffic monitor for Linux and BSD that keeps a log of network traffic for the selected interface(s). It uses the network interface statistics provided by the kernel as information source. This means that vnStat won't actually be sniffing any traffic and also ensures light use of system resources regardless of network traffic rate. This program is open source / GPL'ed and can be installed either as root or as a single user. Better instructions are included in the README.

netstat

- https://linux.die.net/man/8/netstat

In computing, netstat (network statistics) is a command-line network utility that displays network connections for Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics. It is available on Unix, Plan 9, Inferno, and Unix-like operating systems including macOS, Linux, Solaris and BSD. It is also available on IBM OS/2 and on Microsoft Windows NT-based operating systems including Windows XP, Windows Vista, Windows 7, Windows 8 and Windows 10. It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement. On Linux this program is mostly obsolete, although still included in many distributions. On Linux, netstat (part of “net-tools”) is superseded by ss (part of iproute2). The replacement for netstat -r is ip route, the replacement for netstat -i is ip -s link, and the replacement for netstat -g is ip maddr, all of which are recommended instead.

ss

- https://man7.org/linux/man-pages/man8/ss.8.html
- https://www.redhat.com/sysadmin/ss-command

ss - another utility to investigate sockets. ss is used to dump socket statistics. It allows showing information similar to netstat. It can display more TCP and state information than other tools.

nmap

- https://nmap.org/
- https://github.com/nmap/nmap
- https://nmap.org/book/man.html

Nmap (Network Mapper) is a network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich).[4] Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection,[6] vulnerability detection,[6] and other features. Nmap can adapt to network conditions including latency and congestion during a scan. Nmap started as a Linux utility and was ported to other systems including Windows, macOS, and BSD. It is most popular on Linux, followed by Windows.

mtr

- https://www.redhat.com/sysadmin/linux-mtr-command
- https://linux.die.net/man/8/mtr
- https://www.bitwizard.nl/mtr/
- https://github.com/traviscross/mtr

mtr combines the functionality of the 'traceroute' and 'ping' programs in a single network diagnostic tool. As mtr starts, it investigates the network connection between the host mtr runs on and a user-specified destination host. After it determines the address of each network hop between the machines, it sends a sequence ICMP ECHO requests to each one to determine the quality of the link to each machine. As it does this, it prints running statistics about each machine. For a preview take a look at the screenshots.

tcpdump

- https://www.tcpdump.org/index.html
- https://www.tcpdump.org/index.html#documentation
- http://www.alexonlinux.com/tcpdump-for-dummies
- https://danielmiessler.com/study/tcpdump/

- https://packetlife.net/media/library/12/tcpdump.pdf
- https://blog.wains.be/2007/2007-10-01-tcpdump-advanced-filters/

tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.[3] Distributed under the BSD license,[4] tcpdump is free software. Tcpdump works on most Unix-like operating systems: Linux, Solaris, FreeBSD, DragonFly BSD, NetBSD, OpenBSD, OpenWrt, macOS, HP-UX 11i, and AIX. In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows version of libpcap.

Justniffer

- https://onotelli.github.io/justniffer/
- https://github.com/onotelli/justniffer

Justniffer - Network TCP Packet Sniffer. Justniffer is a network protocol analyzer that captures network traffic and produces logs in a customized way, can emulate Apache web server log files, track response times and extract all “intercepted” files from the HTTP traffic. It lets you interactively trace tcp traffic from a live network or from a previously saved capture file. Justniffer’s native capture file format is libpcap format, which is also the format used by tcpdump and various other tools.

Reliable TCP Flow Rebuilding - The main Justniffer’s feature is the ability to handle all those complex low level protocol issues and retrieve the correct flow of the TCP/IP traffic: IP fragmentation, TCP retransmission, reordering. etc. It uses portions of Linux kernel source code for handling all TCP/IP stuff. Precisely, it uses a slightly modified version of the libnids libraries that already include a modified version of Linux code in a more reusable way. Optimized for “Request / Response” protocols. It is able to track server response time

Justniffer was born as tool for helping in analyzing performance problem in complex network environment when it becomes impractical to analyze network captures solely using wireshark. It will help you to quickly identify the most significant bottlenecks analyzing the performance at “application” protocol level.

In very complex and distributed systems is often useful to understand how communication takes place between different components, and when this is implemented as a network protocol based on TCP/IP (HTTP, JDBC, RTSP, SIP, SMTP, IMAP, POP, LDAP, REST, XML-RPC, IIOP, SOAP, etc.), justniffer becomes very useful. Often the logging level and monitoring systems of these systems does not report important information to determine performance issues such as the response time of each network request. Because they are in a “production” environment and cannot be too much verbose or they are in-house developed applications and do not provide such logging.

Other times it is desirable to collect access logs from web services implemented on different environments (various web servers, application servers, python web frameworks, etc.) or web services that are not accessible and therefore traceable only on client side.

Justniffer can capture traffic in promiscuous mode so it can be installed on dedicated and independent station within the same network “collision domain” of the gateway of the systems that must be analyzed, collecting all traffic without affecting the system performances and requiring invasive installation of new software in production environments.

Server Density

- https://support.serverdensity.com/hc/en-us/articles/360001066243

Server Density: SaaS Monitoring - Proactive infrastructure monitoring for cloud, servers, containers & websites. Cross platform monitoring for Linux, Windows, Docker, Kubernetes, FreeBSD and Mac. Automatic agent installation using our API and integration with Chef, Puppet, Ansible and SaltStack.

OpenNMS

- https://www.opennms.com/

Serious remote code execution (RCE) and denial of service (DOS) vulnerabilities in Apache Log4j could affect customers running some OpenNMS products.

OpenNMS is a free and open-source enterprise grade network monitoring and network management platform. It is developed and supported by a community of users and developers and by the OpenNMS Group, offering commercial services, training and support. The goal is for OpenNMS to be a truly distributed, scalable management application platform for all aspects of the FCAPS network management model while remaining 100% free and open source. Currently the focus is on Fault and Performance Management. All code associated with the project is available under the Affero General Public License. The OpenNMS Project is maintained by The Order of the Green Polo.

SysUsage

- https://github.com/darold/sysusage
- https://sysusage.darold.net/

SysUsage: the sysstat and sar grapher. SysUsage is a tool used to continuously monitor a system and generate daily/weekly/monthly/yearly graphical report using rrdtool and sar. SysUsage generate graphical reports on all system activity information. His periodical reports allow you to keep track of the machine activity during his life and will be a great help for performance analysis and resources management. SysUsage can be run periodically from 10 seconds cycle in daemon mode to 1 minute or more using crond. SysUsage can be run from a central server to call a ssh remote execution of the sysusage perl script so that collected data will be stored in this central place. You also will have just one place where rrdtool and related Perl modules need to be installed as well as just one place where sysusagegraph or sysusagejqgraph need to be executed.

SysUsage continuously monitor your systems informations and generate periodical graph reports using rrdtool or javascript jqplot library. All reports are shown throught a web interface.

SysUsage grabs all system activities using Sar and system commands allowing you to keep tracks of your computer or server activity during his life. It is a great help for performance analysis and resources management. The threshold notification can alarm you when the system capabilities are reached by sending SMTP messages or throught Nagios reports.

By default it will monitor all you need to know on your server activity (See Features), it is written in Perl and should works on all Unix like plateforms. It doesn't require a Database system like MySQL or PostgreSQL but lie on rrdtool. In addition you can embeded your own plugins written in any programing language.

Since release 5.0 SysUsage can be run from a centralized place where collected statistics will be stored and where graphics will be rendered. Unless other monitoring tools with lot of administration work, SysUsage is design to have the lesspossible things to configure and a high level of admin system knowledge. Each server can also be self monitored and you just have to connect your browser to the web interface to know his health level.

SysUsage is design with simplicity in mind. I want all relevant statistics from my servers within an intuitive web interface and without spending too much time to configure it, if you know Nagios, you know what I mean. You will especially like SysUsage for that.

PCP

- http://www.pcp.io/
- https://github.com/performancecopilot/pcp

PCP - Performance Co-Pilot. Performance Co-Pilot is a system performance analysis toolkit. Lightweight : Collect performance metrics from your systems efficiently. Distributed : Collate metrics from multiple hosts and a variety of operating systems. Included : Everything you need is already included in the major distributions: Fedora, RHEL, Debian, SUSE, Ubuntu, Gentoo. Analyze systems' performance metrics in real-time or using historical data. Compare performance metrics between different hosts and different intervals. Observe trends and identify abnormal patterns. Extend the collected performance metrics in a simple way. PCP offers a multitude of APIs and libraries to extract and make use of performance metrics from your own application.

KDE system guard

- https://apps.kde.org/ksysguard/

System Guard allows you to monitor information and statistics about your system. In addition to monitoring the local system, it can connect to remote systems running the System Guard Daemon.

Munin

- https://munin-monitoring.org/
- https://guide.munin-monitoring.org/en/latest/

Munin is a networked resource monitoring tool that can help analyze resource trends and “what just happened to kill our performance?” problems. It is designed to be very plug and play. A default installation provides a lot of graphs with almost no work. In Norse mythology Hugin and Munin are the ravens of the god king Odin. They flew all over Midgard for him, seeing and remembering, and later telling him. “Munin” means “memory”.

Nagios

- https://www.nagios.org/

- https://github.com/NagiosEnterprises/nagioscore

Nagios Core /ˈnɑːgiːoʊs/, formerly known as Nagios, is a free and open-source computer-software application that monitors systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.

Ethan Galstad and a group of developers originally wrote Nagios as NetSaint. As of 2015 they actively maintain both the official and unofficial plugins. Nagios is a recursive acronym: “Nagios Ain't Gonna Insist On Sainthood” – “sainthood” makes reference to the original name NetSaint, which changed in response to a legal challenge by owners of a similar trademark. “Agios” (or “hagios”) also transliterates the Greek word άγιος, which means “saint”.

Nagios was originally designed to run under Linux, but it also runs on other Unix variants. It is free software licensed under the terms of the GNU General Public License version 2 as published by the Free Software Foundation. Network Monitoring: When it comes to open source network monitoring tools, the World’s largest organizations turn to Nagios. Nagios monitors the network for problems caused by overloaded data links or network connections, as well as monitoring routers, switches and more. Easily able to monitor availability, uptime and response time of every node on the network, Nagios can deliver the results in a variety of visual representations and reports. Network Monitoring Software. Network Traffic Monitoring. Network Analyzer.

Nagios is known for being the best server monitoring software on the market. Server monitoring is made easy in Nagios because of the flexibility to monitor your servers with both agent-based and agentless monitoring. With over 5000 different addons available to monitor your servers, the community at the Nagios Exchange have left no stone unturned. Server Monitoring Software. Windows Server Monitoring. Linux Server Monitoring.

Implementing effective application monitoring with Nagios allows your organization to quickly detect application, service, or process problems, and take action to eliminate downtime for your application users. Nagios provides tools for monitoring of applications and application state – including Windows applications, Linux applications, UNIX applications, and Web applications. Application Monitoring Tools. Web Application Monitoring. Application Log Monitoring.

Icinga – Next Generation Server Monitoring

Unlike the other tools, Icinga is a network monitoring program, it shows you many options and information about your network connections, devices and processes, it’s a very good choice for those who are looking for a good tool to monitor their networking stuffs. Icinga Monitoring ToolIcinga Monitoring Tool

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Icinga.jpeg

Features of Icinga * Icinga is also free and open-source. * Very functional in monitoring everything you may have in networking. * Support for MySQL and PostgreSQL is included. * Real-time monitoring with A nice web interface. * Very expendable with modules and extensions. * Icinga supports applying services and actions to hosts. * A lot more to discover..

* Read More: Install Icinga in RHEL/CentOS 7/6

Zenoss

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\zenoss.jpg

Zenoss provides a web interface that allows you to monitor all system and network metrics. Moreover it discovers network resources and changes in network configurations. It has alerts for you to take action on and it supports the Nagios plugins. * http://www.zenoss.com/

Cacti

Cacti is nothing more than a free & open-source web interface for RRDtool, it is used often to monitor the bandwidth using SNMP (Simple Network Management Protocol), it can be used also to monitor CPU usage.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\cacti.jpg

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Cacti2.png

(And one for luck!) Cacti is network graphing solution that uses the RRDtool data storage. It allows a user to poll services at predetermined intervals and graph the result. Cacti can be extended to monitor a source of your choice through shell scripts. * http://www.cacti.net/

Features of Cacti * Free & open-source, released under GPL license. * Written in PHP with PL/SQL. * A cross-platform tool, it works on Windows and Linux. * User management; you may create different users accounts for Cacti.

Read More: Install Cacti Network and System Monitoring Tool in Linux

Zabbix

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\zabbix-monitoring.png

Zabbix is an open source infrastructure monitoring solution. It can use most databases out there to store the monitoring statistics. The Core is written in C and has a frontend in PHP. If you don’t like installing an agent, Zabbix might be an option for you. * http://www.zabbix.com/

nmon - Monitor Linux Performance

Nmon (stands for Nigel's performance Monitor) tool, which is used to monitor all Linux resources such as CPU, Memory, Disk Usage, Network, Top processes, NFS, Kernel and much more. This tool comes in two modes: Online Mode and Capture Mode.

The Online Mode, is used for real-time monitoring and Capture Mode, is used to store the output in CSV format for later processing.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\nmon.jpg

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Nmon-620×383.jpeg

nmon either outputs the data on screen or saves it in a comma separated file. You can display CPU, memory, network, filesystems, top processes. The data can also be added to a RRD database for further analysis. * http://nmon.sourceforge.net/pmwiki.php * Read More: Install Nmon (Performance Monitoring) Tool in Linux

conky

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\conky.jpg

Conky monitors a plethora of different OS stats. It has support for IMAP and POP3 and even support for many popular music players! For the handy person you could extend it with your own scripts or programs using Lua. * http://conky.sourceforge.net/

Glances

Glances is a monitoring tool built to present as much information as possible in any terminal size, it automatically takes the terminal window size it runs on, in other words, it's a responsive monitoring tool.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\glances.jpg

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Glances2.jpeg

Glances monitors your system and aims to present a maximum amount of information in a minimum amount of space. It has the capability to function in a client/server mode as well as monitoring remotely. It also has a web interface. * https://github.com/nicolargo/glances * Install Glances on RHEL/CentOS/Fedora and Ubuntu/Debian

Features * Licensed under LGPL and written in Python. * Cross-platform, it works on Windows, Mac, BSD and Linux. * Available in most Linux official repositories. * A It gives a lot of information about your system. * Built using curses.

Sarg – Squid Bandwidth Monitoring

Sarg (Squid Analysis Report Generator) is a free & open-source tool which act as a monitoring tool for your Squid proxy server, it creates reports about your Squid proxy server users, IP addresses, the sites they visit beside some other information. Monitor Squid Proxy LogsMonitor Squid Proxy Logs

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Sarg.jpeg

Features of Sarg * Licensed under GPL 2 and available in many languages. * Works under Linux & FreeBSD. * Generates report in HTML format. * Very easy to install & use.

Read More: Install Sarg "Squid Bandwidth Monitoring" Tool in Linux

saidar

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\saidar.jpg

Saidar is a very small tool that gives you basic information about your system resources. It displays a full screen of the standard system resources. The emphasis for saidar is being as simple as possible. * https://packages.debian.org/sid/utils/saidar

RRDtool

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\rrdtool.jpg

RRDtool is a tool developed to handle round-robin databases or RRD. RRD aims to handle time-series data like CPU load, temperatures etc. This tool provides a way to extract RRD data in a graphical format. * http://oss.oetiker.ch/rrdtool/

monit

Monit is a free open source and web based process supervision utility that automatically monitors and managers system processes, programs, files, directories, permissions, checksums and filesystems.

It monitors services like Apache, MySQL, Mail, FTP, ProFTP, Nginx, SSH and so on. The system status can be viewed from the command line or using it own web interface.

Monit is a nice program that monitors your Linux & Unix server, it can monitor everything you have on your server, from the main server (Apache, Nginx..) to files permissions, files hashes and web services. Plus a lot of things.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\monit.jpg

Monit has the capability of sending you alerts as well as restarting services if they run into trouble. It's possible to perform any type of check you could write a script for with monit and it has a web user interface to ease your eyes. * http://mmonit.com/monit * Read More: Install Monit Tool in RHEL/CentOS/Fedora and Ubuntu/Debian * Read More : Linux Process Monitoring with Monit

Features of Monit * Free & open-source, released under AGPL and written in C. * It can be started from the command line interface or via its special web interface. * Very effective in monitoring all the software on your system and services. * A nice web interface with beautiful charts for CPU and RAM usage. * Monit can automatically take actions in emergency situations. * A lot more..

Linux process explorer

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\linux-process-monitor.jpg

Linux process explorer is akin to the activity monitor for OSX or the windows equivalent. It aims to be more usable than top or ps. You can view each process and see how much memory usage or CPU it uses. * http://sourceforge.net/projects/procexp/

df

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\df.jpg

df is an abbreviation for disk free and is pre-installed program in all unix systems used to display the amount of available disk space for filesystems which the user have access to.

discus

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\discus.jpg

Discus is similar to df however it aims to improve df by making it prettier using fancy features as colors, graphs and smart formatting of numbers. * http://packages.ubuntu.com/lucid/utils/discus

Apache Status Monitoring

Apache Module mod_status is an Apache server module that allows you to monitor the workers status of the Apache server. It generates a report in an easy to read HTML format. It shows you the status of all the workers, how much CPU each one using, and what requests are currently handled and number of working and not working workers.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Apache-Monitoring.jpeg

Read More: Apache Web Server Load and Page Statistics Monitoring

xosview

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\xosview.jpg

xosview is a classic system monitoring tool and it gives you a simple overview of all the different parts of the including IRQ. * http://www.pogo.org.uk/~mark/xosview/

Dstat

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\dstat.jpg

Dstat aims to be a replacement for vmstat, iostat, netstat and ifstat. It allows you to view all of your system resources in real-time. The data can then be exported into csv. Most importantly dstat allows for plugins and could thus be extended into areas not yet known to mankind. * http://dag.wiee.rs/home-made/dstat/

Net-SNMP

SNMP is the protocol 'simple network management protocol' and the Net-SNMP tool suite helps you collect accurate information about your servers using this protocol. * http://www.net-snmp.org/

incron

Incron allows you to monitor a directory tree and then take action on those changes. If you wanted to copy files to directory 'b' once new files appeared in directory 'a' that's exactly what incron does. * http://inotify.aiken.cz/?section=incron&page=about&lang=en

monitorix – System and Network Monitoring

Monitorix is a free lightweight utility that is designed to run and monitor system and network resources as many as possible in Linux/Unix servers. It has a built in HTTP web server that regularly collects system and network information and display them in graphs. It Monitors system load average and usage, memory allocation, disk driver health, system services, network ports, mail statistics (Sendmail, Postfix, Dovecot, etc), MySQL statistics and many more. It designed to monitor overall system performance and helps in detecting failures, bottlenecks, abnormal activities etc.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Monitorix-Monitoring-592×450.png

Monitorix is lightweight system monitoring tool. It helps you monitor a single machine and gives you a wealth of metrics. It also has a built-in HTTP server to view graphs and a reporting mechanism of all metrics. * http://www.monitorix.org/ * Read More : Monitorix a System and Network Monitoring Tool for Linux

vmstat

Linux VmStat command used to display statistics of virtual memory, kernerl threads, disks, system processes, I/O blocks, interrupts, CPU activity and much more. By default vmstat command is not available under Linux systems you need to install a package called sysstat that includes a vmstat program. The common usage of command format is.

procs ———-memory———- —swap– —-io—- -system– ——cpu—– r b swpd free buff cache si so bi bo in cs us sy id wa st 1 0 0 444512 17068 281888 0 0 1 2 27 24 1 0 99 0 0

vmstat or virtual memory statistics is a small built-in tool that monitors and displays a summary about the memory in the machine.

For more Vmstat examples read : 6 Vmstat Command Examples in Linux

Web VMStat – System Statistics Monitoring

Web VMStat is a very simple web application programmer, that provides a real time system information usage, from CPU to RAM, Swap and input/output information in html format.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Web-VMStat.png

Read More: Web VMStat: A Real Time System Statistics Tool for Linux

uptime

This small command that quickly gives you information about how long the machine has been running, how many users currently are logged on and the system load average for the past 1, 5 and 15 minutes.

mpstat

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\mpstat.jpg

mpstat is a built-in tool that monitors cpu usage. The most common command is using mpstat -P ALL which gives you the usage of all the cores. You can also get an interval update of the CPU usage.

pmap

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\pmap.jpg

pmap is a built-in tool that reports the memory map of a process. You can use this command to find out causes of memory bottlenecks.

ps

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\ps.jpg

The ps command will give you an overview of all the current processes. You can easily select all processes using the command ps -A

sar

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\sar.jpg

sar is a part of the sysstat package and helps you to collect, report and save different system metrics. With different commands it will give you CPU, memory and I/O usage among other things. * http://sebastien.godard.pagesperso-orange.fr/

Sysstat – All-in-One System Performance Monitoring

Another monitoring tool for your Linux system. Sysstat is not a real command in fact, it’s just the name of the project, Sysstat in fact is a package that includes many performance monitoring tools like iostat, sadf, pidstat beside many other tools which shows you many statistics about your Linux OS.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Sysstat-620×381.png

Features of Sysstat * Available in many Linux distributions repositories by default. * Ability to create statistics about RAM, CPU, SWAP usage. Beside the ability to monitor Linux kernel activity, NFS server, Sockets, TTY and filesystems. * Ability to monitor input & output statistics for devices, tasks.. etc. * Ability to output reports about network interfaces and devices, with support for IPv6. * Sysstat can show you the power statistics (usage, devices, the fans speed.. etc) as well. * Many other features..

Read More: Install Sysstat in Linux and 20 Useful Commands of Sysstat

collectl- All-in-One Performance Monitoring Tool

Collectl is a yet another powerful and feature rich command line based utility, that can be used to gather information about Linux system resources such as CPU usage, memory, network, inodes, processes, nfs, tcp, sockets and much more.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\collectl.jpg

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Collectl-620×410.jpg

Similar to sar collectl collects performance metrics for your machine. By default it shows cpu, network and disk stats but it collects a lot more. The difference to sar is collectl is able to deal with times below 1 second, it can be fed into a plotting tool directly and collectl monitors processes more extensively. * http://collectl.sourceforge.net/ * Read More: Install Collectl (All-in-One Performance Monitoring) Tool in Linux

iostat

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\iostat.jpg

iostat is also part of the sysstat package. This command is used for monitoring system input/output. The reports themselves can be used to change system configurations to better balance input/output load between hard drives in your machine. * http://sebastien.godard.pagesperso-orange.fr/

free

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\free.jpg

This is a built-in command that displays the total amount of free and used physical memory on your machine. It also displays the buffers used by the kernel at that given moment.

/Proc file system

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\procfile.jpg

The proc file system gives you a peek into kernel statistics. From these statistics you can get detailed information about the different hardware devices on your machine. Take a look at the full list of the proc file statistics

GKrellM

GKrellm is a gui application that monitor the status of your hardware such CPU, main memory, hard disks, network interfaces and many other things. It can also monitor and launch a mail reader of your choice. * http://members.dslextreme.com/users/billw/gkrellm/gkrellm.html

Gnome system monitor

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\gnome-system-monitor.jpg

Gnome system monitor is a basic system monitoring tool that has features looking at process dependencies from a tree view, kill or renice processes and graphs of all server metrics. * http://freecode.com/projects/gnome-system-monitor

GoAccess

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\goaccess.jpg

GoAccess is a real-time web log analyzer which analyzes the access log from either apache, nginx or amazon cloudfront. It’s also possible to output the data into HTML, JSON or CSV. It will give you general statistics, top visitors, 404s, geolocation and many other things. * http://goaccess.io/

Logwatch

Logwatch is a log analysis system. It parses through your system’s logs and creates a report analyzing the areas that you specify. It can give you daily reports with short digests of the activities taking place on your machine. * http://sourceforge.net/projects/logwatch/

Swatch

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\swatch.jpg

Much like Logwatch Swatch also monitors your logs, but instead of giving reports it watches for regular expression and notifies you via mail or the console when there is a match. It could be used for intruder detection for example. * http://sourceforge.net/projects/swatch/

MultiTail

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\multitail.jpg

MultiTail helps you monitor logfiles in multiple windows. You can merge two or more of these logfiles into one. It will also use colors to display the logfiles for easier reading with the help of regular expressions. * http://www.vanheusden.com/multitail/

acct or psacct – Monitor User Activity

acct or psacct (depending on if you use apt-get or yum) allows you to monitor all the commands a users executes inside the system including CPU and memory time. Once installed you get that summary with the command ‘sa’. * http://www.gnu.org/software/acct/

psacct or acct tools are very useful for monitoring each users activity on the system. Both daemons runs in the background and keeps a close watch on the overall activity of each user on the system and also what resources are being consumed by them.

These tools are very useful for system administrators to track each users activity like what they are doing, what commands they issued, how much resources are used by them, how long they are active on the system etc.

For installation and example usage of commands read the article on Monitor User Activity with psacct or acct

whowatch

Similar to acct this tool monitors users on your system and allows you to see in real time what commands and processes they are using. It gives you a tree structure of all the processes and so you can see exactly what’s happening. * http://whowatch.sourceforge.net/

strace

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\strace.jpg

strace is used to diagnose, debug and monitor interactions between processes. The most common thing to do is making strace print a list of system calls made by the program which is useful if the program does not behave as expected. * http://sourceforge.net/projects/strace/

DTrace

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\dtrace.jpg

DTrace is the big brother of strace. It dynamically patches live running instructions with instrumentation code. This allows you to do in-depth performance analysis and troubleshooting. However, it’s not for the weak of heart as there is a 1200 book written on the topic. * http://dtrace.org/blogs/about/

webmin

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\webmin.jpg

Webmin is a web-based system administration tool. It removes the need to manually edit unix configuration files and lets you manage the system remotely if need be. It has a couple of monitoring modules that you can attach to it. * http://www.webmin.com/

stat

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\stat.jpg

Stat is a built-in tool for displaying status information of files and file systems. It will give you information such as when the file was modified, accessed or changed.

ifconfig

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\ifconfig.jpg

ifconfig is a built-in tool used to configure the network interfaces. Behind the scenes network monitor tools use ifconfig to set it into promiscuous mode to capture all packets. You can do it yourself with ifconfig eth0 promisc and return to normal mode with `ifconfig eth0 -promisc`.

ulimit

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\unlimit.jpg

ulimit is a built-in tool that monitors system resources and keeps a limit so any of the monitored resources don’t go overboard. For instance making a fork bomb where a properly configured ulimit is in place would be totally fine. * http://ss64.com/bash/ulimit.html

cpulimit

CPUlimit is a small tool that monitors and then limits the CPU usage of a process. It’s particularly useful to make batch jobs not eat up too many CPU cycles. * https://github.com/opsengine/cpulimit

lshw

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\lshw.jpg

lshw is a small built-in tool extract detailed information about the hardware configuration of the machine. It can output everything from CPU version and speed to mainboard configuration. * https://github.com/opsengine/cpulimit

w

W is a built-in command that displays information about the users currently using the machine and their processes.

lsof

Lsof command used in many Linux/Unix like system that is used to display list of all the open files and the processes. The open files included are disk files, network sockets, pipes, devices and processes. One of the main reason for using this command is when a disk cannot be unmounted and displays the error that files are being used or opened. With this commmand you can easily identify which files are in use. The most common format for this command is.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\lsof.jpg

lsof is a built-in tool that gives you a list of all open files and network connections. From there you can narrow it down to files opened by processes, based on the process name, by a specific user or perhaps kill all processes that belongs to a specific user.

More lsof command usage and examples : 10 lsof Command Examples in Linux

collectd

Collectd is a Unix daemon that collects all your monitoring statistics. It uses a modular design and plugins to fill in any niche monitoring. This way collectd stays as lightweight and customizable as possible. * https://collectd.org/

Observium

Observium is also a network monitoring tool, it was designed to help you manage your network of servers easily, there are 2 versions from it; Community Edition which is free & open-source and Commercial version which costs £150/year.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\observium.png

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\Observium2.jpeg

Observium is an auto-discovering network monitoring platform supporting a wide range of hardware platforms and operating systems. Observium focuses on providing a beautiful and powerful yet simple and intuitive interface to the health and status of your network. * http://www.observium.org/

Features of Observium * Written in PHP with MySQL database support. * Has a nice web interface to output information and data. * Ability to manage and monitor hundreds of hosts worldwide. * The community version from it is licensed under QPL license. * Works on Windows, Linux, FreeBSD and more.

Read More: Observium – Network Management and Monitoring Tool for RHEL/CentOS

PHP Server Monitoring

Unlike the other tools on this list, PHP Server Monitoring is a web script written in PHP that helps you to manage you websites and hosts easily, it supports MySQL database and is released under GPL 3 or later. PHP Server MonitorPHP Server Monitor

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\PHP-Server-Monitor.png

Features * A nice web interface. * Ability to send notifications to you via Email & SMS. * Ability to view the most important information about CPU and RAM. * A very modern logging system to log connection errors and emails that are sent. * Support for cronjob services to help you monitor your servers and websites automatically.

Read More: Install PHP Server Monitoring Tool in Arch Linux

Nload

It’s a command line tool that monitors network throughput. It’s neat because it visualizes the in and and outgoing traffic using two graphs and some additional useful data like total amount of transferred data. You can install it with

```
yum install nload
```

or

```
sudo apt-get install nload
```

SmokePing

SmokePing keeps track of the network latencies of your network and it visualises them too. There are a wide range of latency measurement plugins developed for SmokePing. If a GUI is important to you it’s there is an ongoing development to make that happen. * http://oss.oetiker.ch/smokeping/

Shinken monitoring

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\shinken.jpg

Shinken is a monitoring framework which is a total rewrite of Nagios in python. It aims to enhance flexibility and managing a large environment. While still keeping all your nagios configuration and plugins. * http://www.shinken-monitoring.org/

Linux Dash – Linux Server Performance Monitoring

From its name, “Linux Dash” is a web dashboard that shows you the most important information about your Linux systems such as RAM, CPU, file-system, running processes, users, bandwidth usage in real time, it has a nice GUI and it’s free & open-source.

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\linux-dash.jpeg

Read More: Install Linux Dash (Linux Performance Monitoring) Tool in Linux

Wireshark – Network Protocol Analyzer

Also, unlike all the other tools on our list, Wireshark is an analyzer desktop program which is used to analyze network packets and to monitor network connections. It’s written in C with the GTK+ library and released under the GPL license. Wireshark Network AnalyzerWireshark Network Analyzer

~\ownCloud\zim\Bilder\DEF\artikel-linux-monitoring-tools\wireshark.jpg

Features * Cross-platform: it works on Linux, BSD , Mac OS X and Windows. * Command line support: there’s a command line based version from Wireshark to analyze data. * Ability to capture VoIP calls, USB traffic, network data easily to analyze it. * Available in most Linux distributions repositories.

Read More: Install Wireshark – Network Protocol Analyzer Tool in Linux

Arpwatch – Ethernet Activity Monitor

Arpwatch is a kind of program that is designed to monitor Address Resolution (MAC and IP address changes) of Ethernet network traffic on a Linux network. It continuously keeps watch on Ethernet traffic and produces a log of IP and MAC address pair changes along with a timestamps on a network. It also has a feature to send an email alerts to administrator, when a pairing added or changes. It is very useful in detecting ARP spoofing on a network.

Read More : Arpwatch to Monitor Ethernet Activity

Suricata – Network Security Monitoring

Suricata is an high performance open source Network Security and Intrusion Detection and Prevention Monitoring System for Linux, FreeBSD and Windows.It was designed and owned by a non-profit foundation OISF (Open Information Security Foundation).

Read More : Suricata – A Network Intrusion Detection and Prevention System

---

~~DISCUSSION~~