[20 Linux System Monitoring Tools](http://shabbathster.blogspot.com/2013/07/20-linux-system-monitoring-tools.html)

**20 Linux System Monitoring Tools**

20 Linux System Monitoring Tools  
=================================  
#1: top – Process Activity Command  
The top program provides a dynamic real-time view of a running system i.e. actual process activity. By default, it displays the most CPU-intensive tasks running on the server and updates the list every five seconds.  
20 Linux System Monitoring Tools Every SysAdmin Should Know  
Need to monitor Linux server performance? Try these built-in command and a few add-on tools. Most Linux distributions are equipped with tons of monitoring. These tools provide metrics which can be used to get information about system activities. You can use these tools to find the possible causes of a performance problem. The commands discussed below are some of the most basic commands when it comes to system analysis and debugging server issues such as:  
1.Finding out bottlenecks.  
2.Disk (storage) bottlenecks.  
3.CPU and memory bottlenecks.  
4.Network bottlenecks.  
#1: top – Process Activity Command  
The top program provides a dynamic real-time view of a running system i.e. actual process activity. By default, it displays the most CPU-intensive tasks running on the server and updates the list every five seconds.  
Fig.01: Linux top command  
20 Linux System Monitoring Tools Every SysAdmin Should Know  
Need to monitor Linux server performance? Try these built-in command and a few add-on tools. Most Linux distributions are equipped with tons of monitoring. These tools provide metrics which can be used to get information about system activities. You can use these tools to find the possible causes of a performance problem. The commands discussed below are some of the most basic commands when it comes to system analysis and debugging server issues such as:  
1.Finding out bottlenecks.  
2.Disk (storage) bottlenecks.  
3.CPU and memory bottlenecks.  
4.Network bottlenecks.  
#1: top – Process Activity Command  
=========================================  
The top program provides a dynamic real-time view of a running system i.e. actual process activity. By default, it displays the most CPU-intensive tasks running on the server and updates the list every five seconds.  
Fig.01: Linux top command  
Commonly Used Hot Keys  
The top command provides several useful hot keys:  
Hot Key Usage  
t Displays summary information off and on.  
m Displays memory information off and on.  
A Sorts the display by top consumers of various system resources. Useful for quick identification of performance-hungry tasks on a system.  
f Enters an interactive configuration screen for top. Helpful for setting up top for a specific task.  
o Enables you to interactively select the ordering within top.  
r Issues renice command.  
k Issues kill command.  
z Turn on or off color/mono   
#2: vmstat – System Activity, Hardware and System Information  
==============================================================  
The command vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity.  
# vmstat 3  
# vmstat -m  
# vmstat -a

#3: w – Find Out Who Is Logged on And What They Are Doing  
==========================================================  
w command displays information about the users currently on the machine, and their processes.  
# w username  
# w vivek

#4: uptime – Tell How Long The System Has Been Running  
==========================================================  
The uptime command can be used to see how long the server has been running. The current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes.  
# uptime

#5: ps – Displays The Processes

ps command will report a snapshot of the current processes. To select all processes use the -A or -e option:  
# ps -A  
# ps -Al  
# ps -AlF  
# ps -AlFH  
# ps -AlLm  
# ps ax  
# ps axu  
# ps -ejH  
# ps axjf  
# pstree  
# ps -eo euser,ruser,suser,fuser,f,comm,label  
# ps axZ  
# ps -eM  
user vivek what hi is doing  
==========================  
# ps -U vivek -u vivek u

Set Output In a User-Defined Format  
# ps -eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,wchan:14,comm  
# ps axo stat,euid,ruid,tty,tpgid,sess,pgrp,ppid,pid,pcpu,comm  
# ps -eopid,tt,user,fname,tmout,f,wchan

Display only The Process IDs of Lighttpd  
# ps -C lighttpd -o pid=  
# pgrep lighttpd  
# pgrep -u vivek php-cgi  
Display The Name of PID 55977  
# ps -p 55977 -o comm=  
# ps -p 55977 -o comm=

Find Out The Top 10 Memory Consuming Process  
# ps -auxf | sort -nr -k 4 | head -10

Find Out top 10 CPU Consuming Process  
# ps -auxf | sort -nr -k 3 | head -10

#6: free – Memory Usage  
========================  
The command free displays the total amount of free and used physical and swap memory in the system, as well as the buffers used by the kernel.  
# free 

#7: iostat – Average CPU Load, Disk Activity  
===============================================  
The command iostat report Central Processing Unit (CPU) statistics and input/output statistics for devices, partitions and network filesystems (NFS).  
# iostat 

#8: sar – Collect and Report System Activity  
=============================================  
The sar command is used to collect, report, and save system activity information. To see network counter, enter:  
# sar -n DEV | more  
# sar -n DEV -f /var/log/sa/sa24 | more  
# sar 4 5

#9: mpstat – Multiprocessor Usage  
===================================  
The mpstat command displays activities for each available processor, processor 0 being the first one. mpstat -P ALL to display average CPU utilization per processor:  
# mpstat -P ALL

#10: pmap – Process Memory Usage  
=================================  
The command pmap report memory map of a process. Use this command to find out causes of memory bottlenecks.  
# pmap -d PID  
# pmap -d 47394  
#11 and

#12: netstat and ss – Network Statistics  
====================================================  
The command netstat displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. ss command is used to dump socket statistics. It allows showing information similar to netstat. See the following resources about ss and netstat commands

#13: iptraf – Real-time Network Statistics  
=============================================  
The iptraf command is interactive colorful IP LAN monitor. It is an ncurses-based IP LAN monitor that generates various network statistics including TCP info, UDP counts, ICMP and OSPF information, Ethernet load info, node stats, IP checksum errors, and others. It can provide the following info in easy to read format:  
¦Network traffic statistics by TCP connection  
¦IP traffic statistics by network interface  
¦Network traffic statistics by protocol  
¦Network traffic statistics by TCP/UDP port and by packet size  
¦Network traffic statistics by Layer2 address

#14: tcpdump – Detailed Network Traffic Analysis  
==================================================  
The tcpdump is simple command that dump traffic on a network. However, you need good understanding of TCP/IP protocol to utilize this tool. For.e.g to display traffic info about DNS, enter:  
# tcpdump -i eth1 ‘udp port 53′  
# tcpdump ‘tcp port 80 and (((ip[2:2] – ((ip[0]&0xf)<>2)) != 0)’  
To display all FTP session to 202.54.1.5, enter:  
# tcpdump -i eth1 ‘dst 202.54.1.5 and (port 21 or 20′  
To display all HTTP session to 192.168.1.5:  
# tcpdump -ni eth0 ‘dst 192.168.1.5 and tcp and port  
# tcpdump -n -i eth1 -s 0 -w output.txt src or dst port 80

#15: strace – System Calls  
============================  
Run strace against /bin/foo and capture its output to a text file in output.txt:  
$ strace -o output.txt /bin/foo  
$ strace -p 22254 -s 80 -o /tmp/debug.lighttpd.txt  
$ strace -e trace=open,read -p 22254 -s 80 -o debug.webserver.txt

#16: /Proc file system – Various Kernel Statistics  
===================================================  
# cat /proc/cpuinfo  
# cat /proc/meminfo  
# cat /proc/zoneinfo  
# cat /proc/mounts

17#: Nagios – Server And Network Monitoring  
=============================================  
Nagios is a popular open source computer system and network monitoring application software. You can easily monitor all your hosts, network equipment and services. It can send alert when things go wrong and again when they get better. FAN is “Fully Automated Nagios”. FAN goals are to provide a Nagios installation including most tools provided by the Nagios Community. FAN provides a CDRom image in the standard ISO format, making it easy to easilly install a Nagios server. Added to this, a wide bunch of tools are including to the distribution, in order to improve the user experience around Nagios.

18#: Cacti – Web-based Monitoring Tool  
=======================================  
Cacti is a complete network graphing solution designed to harness the power of RRDTool’s data storage and graphing functionality. Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features out of the box. All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices. It can provide data about network, CPU, memory, logged in users, Apache, DNS servers and much more. See how to install and configure Cacti network graphing tool under CentOS / RHEL.  
#19: KDE System Guard – Real-time Systems Reporting and Graphing  
==================================================================  
KSysguard is a network enabled task and system monitor application for KDE desktop. This tool can be run over ssh session. It provides lots of features such as a client/server architecture that enables monitoring of local and remote hosts. The graphical front end uses so-called sensors to retrieve the information it displays. A sensor can return simple values or more complex information like tables. For each type of information, one or more displays are provided. Displays are organized in worksheets that can be saved and loaded independently from each other. So, KSysguard is not only a simple task manager but also a very powerful tool to control large server farms.

#20: Gnome System Monitor – Real-time Systems Reporting and Graphing  
======================================================================  
The System Monitor application enables you to display basic system information and monitor system processes, usage of system resources, and file systems. You can also use System Monitor to modify the behavior of your system. Although not as powerful as the KDE System Guard, it provides the basic information which may be useful for new users:  
¦Displays various basic information about the computer’s hardware and software.  
¦Linux Kernel version  
¦GNOME version  
¦Hardware  
¦Installed memory  
¦Processors and speeds  
¦System Status  
¦Currently available disk space  
¦Processes  
¦Memory and swap space  
¦Network usage  
¦File Systems  
¦Lists all mounted filesystems along with basic information about each.  
-------------------------------------------------------------------------------------------------------------   
IMPORTANT  
==========  
Bounce: Additional Tools  
A few more tools:   
¦nmap – scan your server for open ports.  
¦lsof – list open files, network connections and much more.  
¦ntop web based tool – ntop is the best tool to see network usage in a way similar to what top command does for processes i.e. it is network traffic monitoring software. You can see network status, protocol wise distribution of traffic for UDP, TCP, DNS, HTTP and other protocols.  
¦Conky – Another good monitoring tool for the X Window System. It is highly configurable and is able to monitor many system variables including the status of the CPU, memory, swap space, disk storage, temperatures, processes, network interfaces, battery power, system messages, e-mail inboxes etc.  
¦GKrellM – It can be used to monitor the status of CPUs, main memory, hard disks, network interfaces, local and remote mailboxes, and many other things.  
¦vnstat – vnStat is a console-based network traffic monitor. It keeps a log of hourly, daily and monthly network traffic for the selected interface(s).  
¦htop – htop is an enhanced version of top, the interactive process viewer, which can display the list of processes in a tree form.  
¦mtr – mtr combines the functionality of the traceroute and ping programs in a single network diagnostic tool.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*