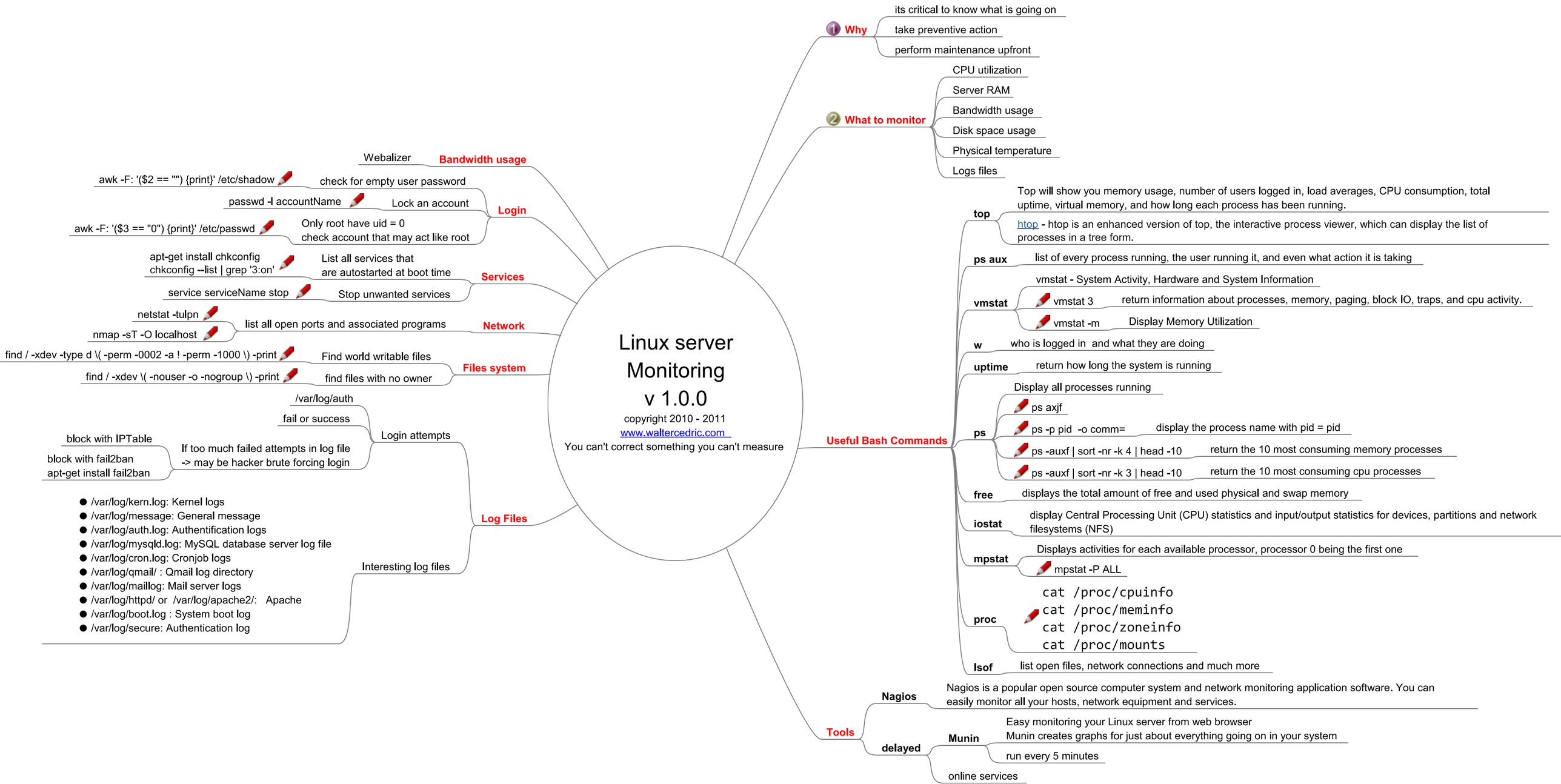
Linux server Monitoring v 1.0.0
copyright 2010 - 2011
www.waltercedric.com
You can't correct something you can't measure
1 Why
its critical to know what is going on
take preventive action
perform maintenance upfront
2 What to monitor
CPU utilization
Server RAM
Bandwidth usage
Disk space usage
Physical temperature
Logs files
Useful Bash Commands
top
Top will show you memory usage, number of users logged in, load averages, CPU consumption, total uptime, virtual memory, and how long each process has been running.
htop - htop is an enhanced version of top, the interactive process viewer, which can display the list of processes in a tree form.
ps aux
list of every process running, the user running it, and even what action it is taking
vmstat
vmstat - System Activity, Hardware and System Information
vmstat 3
return information about processes, memory, paging, block IO, traps, and cpu activity.
vmstat -m
Display Memory Utilization
w
who is logged in and what they are doing
uptime
return how long the system is running
ps
Display all processes running
ps axjf
ps -p pid -o comm=
display the process name with pid = pid
ps -auxf | sort -nr -k 4 | head -10
return the 10 most consuming memory processes
ps -auxf | sort -nr -k 3 | head -10
return the 10 most consuming cpu processes
free
displays the total amount of free and used physical and swap memory
iostat
display Central Processing Unit (CPU) statistics and input/output statistics for devices, partitions and network filesystems (NFS)
mpstat
Displays activities for each available processor, processor 0 being the first one
mpstat -P ALL
proc
cat /proc/cpuinfo
cat /proc/meminfo
cat /proc/zoneinfo
cat /proc/mounts
lsof
list open files, network connections and much more
Tools
Nagios
Nagios is a popular open source computer system and network monitoring application software. You can easily monitor all your hosts, network equipment and services.
delayed
Munin
Easy monitoring your Linux server from web browser
Munin creates graphs for just about everything going on in your system
run every 5 minutes
online services
Log Files
Interesting log files
/var/log/kern.log: Kernel logs
/var/log/message: General message
/var/log/auth.log: Authentification logs
/var/log/mysqld.log: MySQL database server log file
/var/log/cron.log: Cronjob logs
/var/log/qmail/ : Qmail log directory
/var/log/maillog: Mail server logs
/var/log/httpd/ or /var/log/apache2/: Apache
/var/log/boot.log : System boot log
/var/log/secure: Authentication log
Login attempts
/var/log/auth
fail or success
If too much failed attempts in log file
-> may be hacker brute forcing login
block with IPTable
block with fail2ban
apt-get install fail2ban
Bandwidth usage
Webalizer
Login
awk -F: '($2 == "") {print}' /etc/shadow
check for empty user password
passwd -l accountName
Lock an account
awk -F: '($3 == "0") {print}' /etc/passwd
Only root have uid = 0
check account that may act like root
Services
apt-get install chkconfig
chkconfig --list | grep '3:on'
List all services that are autostarted at boot time
service serviceName stop
Stop unwanted services
Network
netstat -tulpn
nmap -sT -O localhost
list all open ports and associated programs
Files system
find / -xdev -type d \(-perm -0002 -a ! -perm -1000 \) -print
Find world writable files
find / -xdev \(-nouser -o -nogroup \) -print
find files with no owner