Hello Everyone,   
  
Here is my shell script which I had performed on terms of accepting user inputs, and executing and providing the required results of the error with its level, and for this , I had accepted arguments and passed arguments to a file, to make a effective results viewer. How we can also keep good constraint for this make it more effective technical approach of by using if, and else statement. But I had used a userinput method and transformed the answer to the file named as text.txt by categorizing the timestamp and level of error only to the file.  
  
As on this exercise used cut , cat, userinput, grep command, and where we can use if and else loop to make a effective and technical logic if the user specified search pattern is found, then it should represents the result, but I had not executed.   
  
  
Here is the script,   
  
Script:   
  
  
  
#! /bin/bash  
name=Goteti  
echo "My Name is $name and the date is $(date)"  
echo "Hello $USER"  
env  
echo "You re calling this program from $PWD"  
echo "Your home directory is $HOME"  
echo "The first argument which i would like to use: $1"  
read userinput  
echo "The second Argument which i would like to use: $2"  
read userinput  
echo "The third argument which i would like to use:  $3"  
read userinput  
cat text.txt  
  
  
  
  
Output:   
  
[root@sunshine alerts]# ./script.txt  
My Name is Goteti and the date is Wed Apr  5 22:24:21 EDT 2017  
Hello root  
HOSTNAME=[sunshine.edu](http://sunshine.edu)  
TERM=xterm  
SHELL=/bin/bash  
HISTSIZE=1000  
QTDIR=/usr/lib/qt-3.3  
QTINC=/usr/lib/qt-3.3/include  
USER=root  
LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=01;05;37;41:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arj=01;31:\*.taz=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lz=01;31:\*.xz=01;31:\*.bz2=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.bz=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.rar=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.axv=01;35:\*.anx=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=01;36:\*.au=01;36:\*.flac=01;36:\*.mid=01;36:\*.midi=01;36:\*.mka=01;36:\*.mp3=01;36:\*.mpc=01;36:\*.ogg=01;36:\*.ra=01;36:\*.wav=01;36:\*.axa=01;36:\*.oga=01;36:\*.spx=01;36:\*.xspf=01;36:  
PATH=/usr/lib/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin  
MAIL=/var/spool/mail/root  
PWD=/var/ossec/logs/alerts  
LANG=en\_US.UTF-8  
HISTCONTROL=ignoredups  
SSH\_ASKPASS=/usr/libexec/openssh/gnome-ssh-askpass  
HOME=/root  
SHLVL=2  
LOGNAME=root  
CVS\_RSH=ssh  
QTLIB=/usr/lib/qt-3.3/lib  
LESSOPEN=|/usr/bin/lesspipe.sh %s  
DISPLAY=:0.0  
G\_BROKEN\_FILENAMES=1  
XAUTHORITY=/root/.xauth12JnGJ  
\_=/bin/env  
You re calling this program from /var/ossec/logs/alerts  
Your home directory is /root  
The first argument which i would like to use:   
cut -d, -f3,4 -/var/ossec/logs/alerts/alerts.log > text.txt  
The second Argument which i would like to use:   
grep 'level 3' text.txt >> text.txt  
The third argument which i would like to use:    
grep 'Apr 05' text.txt >> text.txt   
authentication\_success,  
2017 Apr 05 00:12:14 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 00:12:13 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
  
2017 Apr 05 00:54:59 sunshine->ossec-logcollector  
Rule: 592 (level 8) -> 'Log file size reduced.'  
ossec: File size reduced (inode remained): '/var/log/secure'.  
  
  
2017 Apr 05 02:07:13 sunshine->/var/log/secure  
Rule: 5502 (level 3) -> 'Login session closed.'  
Apr  5 02:07:11 sunshine su: pam\_unix(su-l:session): session closed for user root  
  
authentication\_success,  
2017 Apr 05 02:07:39 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 02:07:37 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
  
2017 Apr 05 03:42:03 sunshine->ossec-logcollector  
Rule: 591 (level 3) -> 'Log file rotated.'  
ossec: File rotated (inode changed): '/var/log/messages'.  
  
  
2017 Apr 05 03:42:03 sunshine->ossec-logcollector  
Rule: 591 (level 3) -> 'Log file rotated.'  
ossec: File rotated (inode changed): '/var/log/secure'.  
  
  
2017 Apr 05 03:42:03 sunshine->ossec-logcollector  
Rule: 591 (level 3) -> 'Log file rotated.'  
ossec: File rotated (inode changed): '/var/log/maillog'.  
  
  
2017 Apr 05 03:42:03 sunshine->ossec-logcollector  
Rule: 591 (level 3) -> 'Log file rotated.'  
ossec: File rotated (inode changed): '/var/log/httpd/error\_log'.  
  
  
2017 Apr 05 03:42:03 sunshine->ossec-logcollector  
Rule: 591 (level 3) -> 'Log file rotated.'  
ossec: File rotated (inode changed): '/var/log/httpd/access\_log'.  
  
  
2017 Apr 05 10:51:55 sunshine->netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort  
Rule: 533 (level 7) -> 'Listened ports status (netstat) changed (new port opened or closed).'  
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
tcp        0      0 [0.0.0.0:111](http://0.0.0.0:111)                 0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:22](http://0.0.0.0:22)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:3306](http://0.0.0.0:3306)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:53](http://0.0.0.0:53)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:5672](http://0.0.0.0:5672)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:57148](http://0.0.0.0:57148)               0.0.0.0:\*                   LISTEN        
tcp        0      0 ::1:25                      :::\*                        LISTEN        
tcp        0      0 :::111                      :::\*                        LISTEN        
tcp        0      0 :::22                       :::\*                        LISTEN        
tcp        0      0 :::48433                    :::\*                        LISTEN        
tcp        0      0 :::53                       :::\*                        LISTEN        
tcp        0      0 :::5672                     :::\*                        LISTEN        
tcp        0      0 :::80                       :::\*                        LISTEN        
Previous output:  
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
tcp        0      0 [0.0.0.0:111](http://0.0.0.0:111)                 0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:22](http://0.0.0.0:22)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:3306](http://0.0.0.0:3306)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:53](http://0.0.0.0:53)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:5672](http://0.0.0.0:5672)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:59393](http://0.0.0.0:59393)               0.0.0.0:\*                   LISTEN        
tcp        0      0 ::1:25                      :::\*                        LISTEN        
tcp        0      0 :::111                      :::\*                        LISTEN        
tcp        0      0 :::22                       :::\*                        LISTEN        
tcp        0      0 :::47923                    :::\*                        LISTEN        
tcp        0      0 :::53                       :::\*                        LISTEN        
tcp        0      0 :::5672                     :::\*                        LISTEN        
tcp        0      0 :::80                       :::\*                        LISTEN        
  
  
2017 Apr 05 10:51:57 sunshine->ossec-monitord  
Rule: 502 (level 3) -> 'Ossec server started.'  
ossec: Ossec started.  
  
  
2017 Apr 05 10:52:23 sunshine->/var/log/messages  
Rule: 1002 (level 2) -> 'Unknown problem somewhere in the system.'  
Apr  5 10:52:23 sunshine gnome-session[2336]: WARNING: Application 'gnome-settings-daemon.desktop' failed to register before timeout  
  
authentication\_success,  
2017 Apr 05 10:55:06 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 10:55:05 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
  
2017 Apr 05 13:30:41 sunshine->netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort  
Rule: 533 (level 7) -> 'Listened ports status (netstat) changed (new port opened or closed).'  
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
tcp        0      0 [0.0.0.0:111](http://0.0.0.0:111)                 0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:22](http://0.0.0.0:22)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:3306](http://0.0.0.0:3306)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:46996](http://0.0.0.0:46996)               0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:53](http://0.0.0.0:53)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:5672](http://0.0.0.0:5672)                0.0.0.0:\*                   LISTEN        
tcp        0      0 ::1:25                      :::\*                        LISTEN        
tcp        0      0 :::111                      :::\*                        LISTEN        
tcp        0      0 :::22                       :::\*                        LISTEN        
tcp        0      0 :::35272                    :::\*                        LISTEN        
tcp        0      0 :::53                       :::\*                        LISTEN        
tcp        0      0 :::5672                     :::\*                        LISTEN        
tcp        0      0 :::80                       :::\*                        LISTEN        
Previous output:  
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
tcp        0      0 [0.0.0.0:111](http://0.0.0.0:111)                 0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:22](http://0.0.0.0:22)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:3306](http://0.0.0.0:3306)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:53](http://0.0.0.0:53)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:5672](http://0.0.0.0:5672)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:57148](http://0.0.0.0:57148)               0.0.0.0:\*                   LISTEN        
tcp        0      0 ::1:25                      :::\*                        LISTEN        
tcp        0      0 :::111                      :::\*                        LISTEN        
tcp        0      0 :::22                       :::\*                        LISTEN        
tcp        0      0 :::48433                    :::\*                        LISTEN        
tcp        0      0 :::53                       :::\*                        LISTEN        
tcp        0      0 :::5672                     :::\*                        LISTEN        
tcp        0      0 :::80                       :::\*                        LISTEN        
  
  
2017 Apr 05 13:30:43 sunshine->ossec-monitord  
Rule: 502 (level 3) -> 'Ossec server started.'  
ossec: Ossec started.  
  
  
2017 Apr 05 13:31:07 sunshine->/var/log/messages  
Rule: 1002 (level 2) -> 'Unknown problem somewhere in the system.'  
Apr  5 13:31:06 sunshine gnome-session[2331]: WARNING: Application 'gnome-settings-daemon.desktop' failed to register before timeout  
  
authentication\_success,  
2017 Apr 05 13:34:34 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 13:34:32 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
  
2017 Apr 05 13:35:46 sunshine->syscheck  
Rule: 551 (level 7) -> 'Integrity checksum changed again (2nd time).'  
Integrity checksum changed for: '/etc/resolv.conf'  
Size changed from '176' to '159'  
Old md5sum was: 'a37f97f4d495952bab4a39241a23e11b'  
New md5sum is : 'cf989441ba4402985b36264920258eba'  
Old sha1sum was: '4e9e86badfd3d4bd8d749c72e612bab930ad9d8f'  
New sha1sum is : '8037b3cca07552583a5e188a370bcd278e57cc95'  
  
  
  
2017 Apr 05 13:36:00 sunshine->/var/log/secure  
Rule: 5502 (level 3) -> 'Login session closed.'  
Apr  5 13:35:59 sunshine su: pam\_unix(su-l:session): session closed for user root  
  
authentication\_success,  
2017 Apr 05 13:36:22 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 13:36:21 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
  
2017 Apr 05 13:38:02 sunshine->/var/log/secure  
Rule: 5502 (level 3) -> 'Login session closed.'  
Apr  5 13:38:00 sunshine su: pam\_unix(su-l:session): session closed for user root  
  
authentication\_success,  
2017 Apr 05 13:38:22 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 13:38:21 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
  
2017 Apr 05 13:39:08 sunshine->/var/log/secure  
Rule: 5502 (level 3) -> 'Login session closed.'  
Apr  5 13:39:07 sunshine su: pam\_unix(su-l:session): session closed for user root  
  
authentication\_failed,  
2017 Apr 05 13:39:36 sunshine->/var/log/secure  
Rule: 5503 (level 5) -> 'User login failed.'  
Apr  5 13:39:36 sunshine su: pam\_unix(su-l:auth): authentication failure; logname=alice uid=500 euid=0 tty=pts/0 ruser=alice rhost=  user=root  
  
authentication\_success,  
2017 Apr 05 13:39:52 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 13:39:52 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
  
2017 Apr 05 19:06:09 sunshine->netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort  
Rule: 533 (level 7) -> 'Listened ports status (netstat) changed (new port opened or closed).'  
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
tcp        0      0 [0.0.0.0:111](http://0.0.0.0:111)                 0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:22](http://0.0.0.0:22)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:3306](http://0.0.0.0:3306)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:53](http://0.0.0.0:53)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:5672](http://0.0.0.0:5672)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:57815](http://0.0.0.0:57815)               0.0.0.0:\*                   LISTEN        
tcp        0      0 ::1:25                      :::\*                        LISTEN        
tcp        0      0 :::111                      :::\*                        LISTEN        
tcp        0      0 :::22                       :::\*                        LISTEN        
tcp        0      0 :::36713                    :::\*                        LISTEN        
tcp        0      0 :::53                       :::\*                        LISTEN        
tcp        0      0 :::5672                     :::\*                        LISTEN        
tcp        0      0 :::80                       :::\*                        LISTEN        
Previous output:  
ossec: output: 'netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort':  
tcp        0      0 [0.0.0.0:111](http://0.0.0.0:111)                 0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:22](http://0.0.0.0:22)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:3306](http://0.0.0.0:3306)                0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:46996](http://0.0.0.0:46996)               0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:53](http://0.0.0.0:53)                  0.0.0.0:\*                   LISTEN        
tcp        0      0 [0.0.0.0:5672](http://0.0.0.0:5672)                0.0.0.0:\*                   LISTEN        
tcp        0      0 ::1:25                      :::\*                        LISTEN        
tcp        0      0 :::111                      :::\*                        LISTEN        
tcp        0      0 :::22                       :::\*                        LISTEN        
tcp        0      0 :::35272                    :::\*                        LISTEN        
tcp        0      0 :::53                       :::\*                        LISTEN        
tcp        0      0 :::5672                     :::\*                        LISTEN        
tcp        0      0 :::80                       :::\*                        LISTEN        
  
  
2017 Apr 05 19:06:10 sunshine->ossec-monitord  
Rule: 502 (level 3) -> 'Ossec server started.'  
ossec: Ossec started.  
  
  
2017 Apr 05 19:09:42 sunshine->syscheck  
Rule: 552 (level 7) -> 'Integrity checksum changed again (3rd time).'  
Integrity checksum changed for: '/etc/resolv.conf'  
Size changed from '159' to '176'  
Old md5sum was: 'cf989441ba4402985b36264920258eba'  
New md5sum is : 'a37f97f4d495952bab4a39241a23e11b'  
Old sha1sum was: '8037b3cca07552583a5e188a370bcd278e57cc95'  
New sha1sum is : '4e9e86badfd3d4bd8d749c72e612bab930ad9d8f'  
  
  
authentication\_success,  
2017 Apr 05 19:11:26 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 19:11:24 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
authentication\_success,  
2017 Apr 05 20:03:19 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 20:03:18 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
authentication\_success,  
2017 Apr 05 20:54:36 sunshine->/var/log/secure  
Rule: 5501 (level 3) -> 'Login session opened.'  
Apr  5 20:54:34 sunshine su: pam\_unix(su-l:session): session opened for user root by alice(uid=500)  
  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 5502 (level 3) -> 'Login session closed.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 591 (level 3) -> 'Log file rotated.'  
Rule: 591 (level 3) -> 'Log file rotated.'  
Rule: 591 (level 3) -> 'Log file rotated.'  
Rule: 591 (level 3) -> 'Log file rotated.'  
Rule: 591 (level 3) -> 'Log file rotated.'  
Rule: 502 (level 3) -> 'Ossec server started.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 502 (level 3) -> 'Ossec server started.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 5502 (level 3) -> 'Login session closed.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 5502 (level 3) -> 'Login session closed.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 5502 (level 3) -> 'Login session closed.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 502 (level 3) -> 'Ossec server started.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
Rule: 5501 (level 3) -> 'Login session opened.'  
  
  
  
  
  
  
  
  
  
  
  
  
