

Damir Nabiullin - Lab 10

1. Answer:

In this case we can use Elastic Stack because it helps by providing users with a powerful platform that collects and processes data from multiple data sources, stores that data in one centralized data store that can scale as data grows, and that provides a set of tools to analyze the data.

2. Answer:

```
dale@dale-nitro:~$ sudo nano /etc/rsyslog.d/auth-errors.conf
dale@dale-nitro:~$ sudo chmod 777 /etc/rsyslog.d/auth-errors.conf
dale@dale-nitro:~$ cat /etc/rsyslog.d/auth-errors.conf
security.emerg /var/log/auth-errors
auth.emerg /var/log/auth-errors
authpriv.emerg /var/log/auth-errors
security.alert /var/log/auth-errors
auth.alert /var/log/auth-errors
authpriv.alert /var/log/auth-errors
dale@dale-nitro:~$ systemctl restart rsyslog
dale@dale-nitro:~$ logger -p security.alert TEST_MESSAGE
dale@dale-nitro:~$ cat /var/log/auth-errors
Nov  6 19:14:44 dale-nitro dale: TEST_MESSAGE
Nov  6 19:14:44 dale-nitro dale: TEST_MESSAGE
dale@dale-nitro:~$ journalctl -p alert
-- Logs begin at Tue 2022-09-06 22:31:20 MSK, end at Sun 2022-11-06 19:14:44 MSK. --
Nov 06 19:14:44 dale-nitro dale[6330]: TEST_MESSAGE
```

3. Apache:

```
dale@dale-nitro:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0
  linux-headers-5.15.0-48-generic linux-hwe-5.15.0-48 linux-image-5.15.0-48-generic
  linux-modules-5.15.0-48-generic linux-modules-extra-5.15.0-48-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
```



Configuration:

```

dale@dale-nitro:~$ hostname -I
192.168.1.33
dale@dale-nitro:~$ sudo nano /etc/logrotate.d/sna-apache
dale@dale-nitro:~$ sudo chmod 755 /etc/logrotate.d/sna-apache
dale@dale-nitro:~$ cat /etc/logrotate.d/sna-apache
/var/log/apache2/access.log {
    compress
    size 1
    rotate 1
    postrotate
        systemctl restart apache2
    endscrip
}

```

Test:

```

dale@dale-nitro:/var/log/apache2$ ls -lah
total 16K
drwxr-x--- 2 root adm 4.0K Nov 6 20:15 .
drwxrwxr-x 16 root syslog 4.0K Nov 6 20:00 ..
-rw-r--r-- 1 root root 0 Nov 6 20:15 access.log
-rw-r--r-- 1 root root 111 Nov 6 20:09 cat
-rw-r----- 1 root adm 279 Nov 6 20:00 error.log
-rw-r----- 1 root adm 0 Nov 6 19:18 other_vhosts_access.log
dale@dale-nitro:/var/log/apache2$ sudo logrotate /etc/logrotate.d/sna-apache
dale@dale-nitro:/var/log/apache2$ ls -lah
total 20K
drwxr-x--- 2 root adm 4.0K Nov 6 20:16 .
drwxrwxr-x 16 root syslog 4.0K Nov 6 20:00 ..
-rw-r--r-- 1 root root 0 Nov 6 20:15 access.log
-rw-r--r-- 1 root root 33 Nov 6 20:16 access.log.1.gz
-rw-r--r-- 1 root root 111 Nov 6 20:09 cat
-rw-r----- 1 root adm 279 Nov 6 20:00 error.log
-rw-r----- 1 root adm 0 Nov 6 19:18 other_vhosts_access.log

```

4. Script:

```

#!/bin/bash

touch /var/log/alarm.log

while :
do
    LINES=$(journalctl SYSLOG_FACILITY=10 -p info --since="30sec ago" --grep="3 incorrect password attempts" | wc -l)
    if [ "$LINES" >= "3" ]; then
        echo "Three or more authentication failure in 30 seconds\n" >> /var/log/alarm.log
        echo "Alarm fired"
    else
        echo "Currently ${LINES} lines"
    fi
    sleep 1
done

```

```
dale@dale-nitro:~$ sudo su
[sudo] password for dale:
Sorry, try again.
[sudo] password for dale:
Sorry, try again.
[sudo] password for dale:
sudo: 3 incorrect password attempts
dale@dale-nitro:~$ sudo su
[sudo] password for dale:
Sorry, try again.
[sudo] password for dale:
Sorry, try again.
[sudo] password for dale:
sudo: 3 incorrect password attempts
```

Script output:

```
Line #2
Line #2
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
Print log to /var/log/alarm.log
```

Log:

```
dale@dale-nitro:~/Documents/SNA/Week 10$ cat /var/log/alarm.log
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
```

5. You can log all the activity from the users with the `psacct` package.

- ▼ The `psacct` contains several utilities for monitoring process activities, including `ac`, `lastcomm`, `accton`, `sa`.
- ▼ The `ac` command displays statistics about how long users have been logged on.
- ▼ The `lastcomm` command displays information about previous executed commands.
- ▼ The `accton` command turns process accounting on or off.
- ▼ The `sa` command summarizes information about previously executed commands.

```

dale@dale-nitro:~/Documents/SNA/Week 10$ sudo apt-get install acct
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libgstreamer-plugins-bad1.0-0
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  acct
0 upgraded, 1 newly installed, 0 to remove and 151 not upgraded.
Need to get 87.0 kB of archives.
After this operation, 337 kB of additional disk space will be used.
Get:1 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 acct amd64 6.6.4-2 [87.0 kB]
Fetched 87.0 kB in 2s (51.1 kB/s)
Selecting previously unselected package acct.
(Reading database ... 265952 files and directories currently installed.)
Preparing to unpack .../acct_6.6.4-2_amd64.deb ...
Unpacking acct (6.6.4-2) ...
Setting up acct (6.6.4-2) ...
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults
update-rc.d: warning: stop runlevel arguments (1) do not match acct Default-Stop values (0 1 6)
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
Processing triggers for systemd (245.4-4ubuntu3.15) ...
dale@dale-nitro:~/Documents/SNA/Week 10$ lastcomm dale
apt-check          dale      —          1.04 secs Sun Nov  6 19:46
lsb_release        dale      —          0.02 secs Sun Nov  6 19:46
lsb_release        dale      —          0.02 secs Sun Nov  6 19:46
lsb_release        dale      —          0.02 secs Sun Nov  6 19:46
lsb_release        dale      —          0.02 secs Sun Nov  6 19:46

```

```

dale@dale-nitro:~/Documents/SNA/Week 10$ touch test.sh
dale@dale-nitro:~/Documents/SNA/Week 10$ lastcomm dale
touch             dale      pts/0      0.00 secs Sun Nov  6 19:47
lastcomm          dale      pts/0      0.00 secs Sun Nov  6 19:46
apt-check         dale      —          1.04 secs Sun Nov  6 19:46
lsb_release       dale      —          0.02 secs Sun Nov  6 19:46
lsb_release       dale      —          0.02 secs Sun Nov  6 19:46
lsb_release       dale      —          0.02 secs Sun Nov  6 19:46
lsb_release       dale      —          0.02 secs Sun Nov  6 19:46
lsb_release       dale      —          0.02 secs Sun Nov  6 19:46

```