Description

A customer has asked for a way to provide on-demand monitoring of various unix-based servers without having to log into each individual machine and opening up the log files found in /var/log. The customer has asked for the ability to issue a REST request to a machine in order to retrieve logs from /var/log on the machine receiving the REST request.

Requirement

Use HTTP REST request to show the log file under /var/log

- **Show file content in /var/log**
- **Last n events of specific file show in reverse time ordered**
- **Basic text/keyword filtering of events**

Proposed Solution

Use of the unix commands

- cat the log file to gather the file content
- tail -n <5> /var/log/<file>/
- sort -r to show reverse order
- grep <filter>

Implement the following:

1. Show the file content in /var/log
    a. cat <log>
2. Last n events of specific file, show the result in reverse time ordered
    a. tail -n 5 /var/log/<log>| sort -r
3. Basic text/keyword filtering of events
    a. tail -n 5 /var/log/<log>| sort -r | grep <filter>

REST endpoints

Show log

http://localhost:8000/logs/files/system.log

HTTP Method : GET

Response

Text

Response Codes

- 200 OK
- 404 Page Not Found

Response Sample

```
Jul  4 08:59:37 Copper Google Chrome Helper[64073]: Libnotify:
notify_register_coalesced_registration failed with code 9 on line 2835
Jul  4 08:59:20 Copper Microsoft Edge Helper[3092]: Libnotify:
notify_register_coalesced_registration failed with code 9 on line 2835
Jul  4 08:58:54 Copper systemstats[316]: assertion failed: 20D91: systemstats + 602280
[146262DC-951A-39E6-88F2-E8A328A3A263]: 0x2
Jul  4 08:58:54 Copper systemstats[316]: assertion failed: 20D91: systemstats + 399948
[146262DC-951A-39E6-88F2-E8A328A3A263]: 0x0
Jul  4 08:58:37 Copper Google Chrome Helper[64073]: Libnotify:
notify_register_coalesced_registration failed with code 9 on line 2835
Jul  4 08:58:20 Copper Microsoft Edge Helper[3092]: Libnotify:
notify_register_coalesced_registration failed with code 9 on line 2835
Jul  4 08:58:04 Copper com.apple.xpc.launchd[1] (com.apple.mdworker.shared.10000000-0200-
```

Show # of last events

http://localhost:8000/logs/files/system.log/lastevents/2

HTTP Method: GET

Response:

Text

Response Codes

- 200 OK
- 404 Page Not Found

Response Sample

```
Jul  4 08:56:46 Copper Microsoft Edge Helper[2955]: Libnotify:
notify_register_coalesced_registration failed with code 9 on line 2835
Jul  4 08:56:37 Copper Google Chrome Helper[64073]: Libnotify:
notify_register_coalesced_registration failed with code 9 on line 2835
```

Show filtered events

http://localhost:8000/logs/files/system.log/lastevents/50?filter=apple

Shows the filtered log up to 50 events.

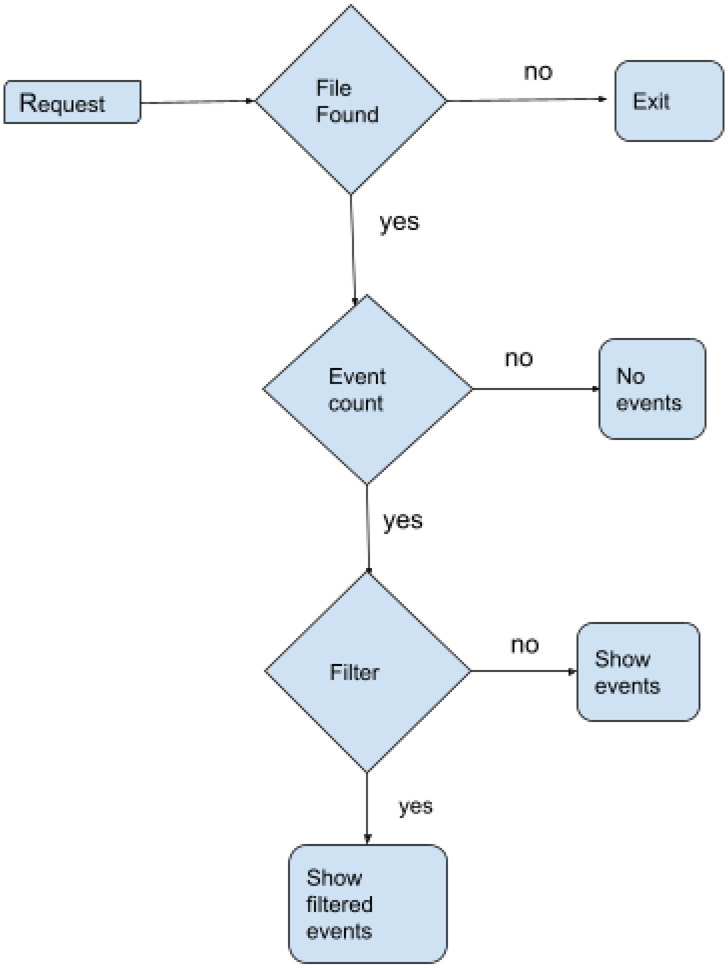
HTTP Method: GET
Response:
Text

Response Codes
  200 OK
  404 Page Not Found

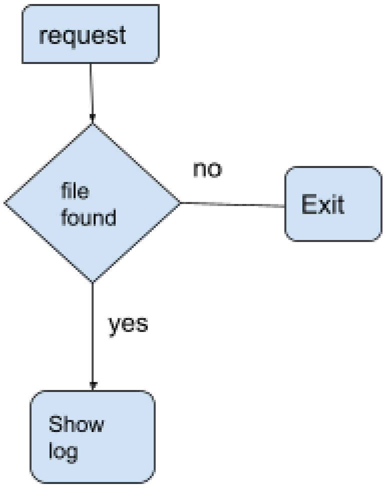
Response Sample

```
Jul  4 08:33:04 Copper com.apple.xpc.launchd[1]
(com.apple.mdworker.shared.10000000-0200-0000-0000-000000000000[51547]): Service
exited due to SIGKILL | sent by mds[335]
```

Flow diagram for displaying last events



Display log file


request
file found
no
Exit
yes
Show log