

Task 2

Integrating fluent-bit with elasticsearch

First: Using regex to parse the logs in rebular

1-

The screenshot shows the Rubular website, a Ruby regular expression editor. The interface includes a browser tab bar at the top with tabs for 'BSC 121 Physics 1 - ...', 'CS-2024 - Google D...', 'calculus -', 'year 1', 'FCIS CHP 2021 - Go...', '1.1.1 Basic Concepts...', and 'HCIA-Se'. The main heading is 'Rubular' with the subtitle 'a Ruby regular expression editor'. Below this, the 'Your regular expression:' field contains the regex: `(?<time_stamp:>\S+\s+\d+\s+\S+) (?<Hostname:>\S+) (?<Protocol:>[a-z]+\s+)\s+ (?<rule:>\S+): (?<Message:>.+) user (?<user:>\S+) I`. The 'Your test string:' field contains a log entry: `Nov 9 11:36:55 ecaz sshd[26967]: pam_succeed_if(sshd:auth): error retrieving information about user _z9xxbBW`. The 'Match result:' field shows the same log entry with the regex applied. The 'Match groups:' field displays the following extracted data:

time_stamp:	Nov 9 11:36:55
Hostname:	ecaz
Protocol:	sshd
rule:	pam_succeed_if(sshd:auth)
Message:	error retrieving information about
user:	_z9xxbBW

 At the bottom, there are buttons for 'make permalink' and 'clear fields', and a link to 'Regex quick reference'.

2-

```
\\[Time\\s+(?<timestamp:>\\S+\\s+\\S+\\s+\\S+)\\]\\s+\\[Facility\\s+(?<Facility:>\\S+)\\]\\s+\\[Sender\\s+(?<Sender protocol:>\\S+)\\]\\s+\\[PID\\s+(?<PID:>\\d+)\\]\\s+\\[Message\\s+(?<Message:>\\S+\\s+\\S+\\s+\\S+\\s+\\S+)\\s+\\S+\\s+(?<User:>\\S+)\\s+\\S+\\s+(?<src_ip:>\\S+)\\]\\s+\\[\\S+(?<severity level:>\\S+\\S+)\\]\\s+\\[\\S+\\s+(?<UID:>\\S+)\\]\\s+\\[\\S+\\s+(?<GID:>\\S+)\\]\\s+\\[\\S+\\s+(?<Host:>\\S+)\\]
```

a Ruby regular expression editor

Your regular expression:

<src_ip:>\S+)\s+\[S+(?<severity_level:>\s+\S+)\]\s+\[S+\s+(?<UID:>\S+)\]\s+\[S+\s+(?<GID:>\S+)\]\s+\[S+\s+(?<Host:>\S+)\]

Your test string:

[Time 2006.12.28 15:53:55 UTC] [Facility auth] [Sender sshd] [PID 483] [Message error: PAM: Authentication failure for username from 192.168.0.2] [Level 3] [UID -2] [GID -2] [Host Hostname]

Wrap words

☒

Show invisibles

☐

Match result:

[Time 2006.12.28 15:53:55 UTC] [Facility auth] [Sender sshd] [PID 483] [Message error: PAM: Authentication failure for username from 192.168.0.2] [Level 3] [UID -2] [GID -2] [Host Hostname]

Match groups:

timestamp: 2006.12.28 15:53:55 UTC

Facility: auth

Sender protocol: sshd

PID: 483

Message: error: PAM: Authentication failure

User: username

src_ip: 192.168.0.2

severity_level: 3

UID: -2

GID: -2

Host: Hostname

3-

:(<cef:>\d+)\|(<Security solution:>\S+\s+\S+\s+[a-zA-Z]+\)\|(<Operating system:>[a-zA-Z]+-[a-zA-Z]+\)\|(<version:>\d+\.\d+\.\d+)\|(<log_type:>[a-zA-Z]+\)\|([a-zA-Z]+\)\|(<id:>\d+)\|rt=(<timestamp:>\S+\s+\S+\s+\S+\s+\S+\s+\S+)\s+deviceExternalId=(<Device_external_id:>\S+)\s+src=(<src_ip:>\S+)\s+dst=(<dest_ip:>\S+)\s+sourceTranslatedAddress=(<sourceTranslatedAddress:>\S+)\s+destinationTranslatedAddress=(<destinationTranslatedAddress:>\S+)\s+csLabel=Rule\s+\S+=(<FW_rule:>\S+)

a Ruby regular expression editor

Your regular expression:

<sourceTranslatedAddress:>\S+)\s+destinationTranslatedAddress=(<destinationTranslatedAddress:>\S+)\s+csLabel=Rule\s+\S+=(<FW_rule:>\S+)

Your test string:

CEF:0|Palo Alto Networks|PAN-OS|9.1.0|TRAFFIC|traffic|1|rt=Jul 08 2024 13:45:30 deviceExternalId=0011223344 src=192.168.1.100 dst=10.0.0.50 sourceTranslatedAddress=192.168.2.100 destinationTranslatedAddress=10.10.1.50 csLabel=Rule csLabel=Allow-All

Wrap words

☒

Show invisibles

☐

Match result:

CEF:0|Palo Alto Networks|PAN-OS|9.1.0|TRAFFIC|traffic|1|rt=Jul 08 2024 13:45:30 deviceExternalId=0011223344 src=192.168.1.100 dst=10.0.0.50 sourceTranslatedAddress=192.168.2.100 destinationTranslatedAddress=10.10.1.50 csLabel=Rule csLabel=Allow-All

Match groups:

cef: 0

Security solution: Palo Alto Networks

Operating system: PAN-OS

version: 9.1.0

log_type: TRAFFIC

id: 1

timestamp: Jul 08 2024 13:45:30

Device_external_id: 0011223344

src_ip: 192.168.1.100

dest_ip: 10.0.0.50

sourceTranslatedAddress: 192.168.2.100

destinationTranslatedAddress: 10.10.1.50

FW_rule: Allow-All

Second:

Integrating fluent-bit with elasticsearch

1-Adding our server GPG key to your keyring

```
root@abdelrahman-1-2:/home/abdelrahman/Downloads# curl https://packages.fluentbit.io/fluentbit.key | gpg --dearmor > /usr/share/keyrings/fluentbit-keyring.gpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 3175  100 3175    0     0  3829      0 --:--:-- --:--:-- --:--:-- 3829
root@abdelrahman-1-2:/home/abdelrahman/Downloads#
```

2-Adding its APT server entry to sources lists and updating apt-get

```
root@abdelrahman-1-2:/home/abdelrahman/Downloads# echo "deb [signed-by=/usr/share/keyrings/fluentbit-keyring.gpg] https://packages.fluentbit.io/debian/bookworm bookworm main" | sudo tee /etc/apt/sources.list.d/fluent-bit.x.list
deb [signed-by=/usr/share/keyrings/fluentbit-keyring.gpg] https://packages.fluentbit.io/debian/bookworm bookworm main
root@abdelrahman-1-2:/home/abdelrahman/Downloads#
```

3-Installing Fluent-Bit.

```
root@abdelrahman-1-2:/home/abdelrahman/Downloads# apt-get update
Hit:1 http://security.ubuntu.com/ubuntu mantic-security InRelease
Hit:2 http://eg.archive.ubuntu.com/ubuntu mantic InRelease
Hit:3 http://eg.archive.ubuntu.com/ubuntu mantic-updates InRelease
Hit:4 http://eg.archive.ubuntu.com/ubuntu mantic-backports InRelease
Get:5 https://packages.fluentbit.io/debian/bookworm bookworm InRelease [7,577 B]
Get:6 https://packages.fluentbit.io/debian/bookworm bookworm/main amd64 Packages [16.6 kB]
Fetched 24.2 kB in 2s (13.5 kB/s)
Reading package lists... Done
root@abdelrahman-1-2:/home/abdelrahman/Downloads# apt-get install fluent-bit
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpq5
The following NEW packages will be installed:
  fluent-bit libpq5
0 upgraded, 2 newly installed, 0 to remove and 19 not upgraded.
1 not fully installed or removed.
Need to get 42.4 MB of archives.
After this operation, 97.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://eg.archive.ubuntu.com/ubuntu mantic-updates/main amd64 libpq5 amd64 15.7-0ubuntu0.23.10.1 [143 kB]
Get:2 https://packages.fluentbit.io/debian/bookworm bookworm/main amd64 fluent-bit amd64 3.1.3 [42.3 MB]
Fetched 42.4 MB in 22s (1,930 kB/s)
Selecting previously unselected package libpq5:amd64.
(Reading database ... 240290 files and directories currently installed.)
Preparing to unpack .../libpq5_15.7-0ubuntu0.23.10.1_amd64.deb ...
```

4-Enabling the service

```
root@abdelrahman-1-2: /home/abdelrahman/Downloads
root@abdelrahman-1-2:/home/abdelrahman/Downloads# systemctl enable fluent-bit.service
Created symlink /etc/systemd/system/multi-user.target.wants/fluent-bit.service → /lib/systemd/system/fluent-bit.service
.
root@abdelrahman-1-2:/home/abdelrahman/Downloads# systemctl start fluent-bit.service
root@abdelrahman-1-2:/home/abdelrahman/Downloads# systemctl status fluent-bit.service
● fluent-bit.service - Fluent Bit
   Loaded: loaded (/lib/systemd/system/fluent-bit.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-07-23 18:15:55 EEST; 7s ago
     Docs: https://docs.fluentbit.io/manual/
   Main PID: 7848 (fluent-bit)
      Tasks: 4 (limit: 4880)
     Memory: 5.0M
        CPU: 25ms
    CGroup: /system.slice/fluent-bit.service
            └─7848 /opt/fluent-bit/bin/fluent-bit -c //etc/fluent-bit/fluent-bit.conf

Jul 23 18:15:55 abdelrahman-1-2 fluent-bit[7848]: [2024/07/23 18:15:55] [ info] [input:cpu:cpu.0] storage_strategy='me
Jul 23 18:15:55 abdelrahman-1-2 fluent-bit[7848]: [2024/07/23 18:15:55] [ info] [sp] stream processor started
Jul 23 18:15:55 abdelrahman-1-2 fluent-bit[7848]: [2024/07/23 18:15:55] [ info] [output:stdout:stdout.0] worker #0 sta
Jul 23 18:15:57 abdelrahman-1-2 fluent-bit[7848]: [0] cpu.local: [[1721747756.055081438, {}], {"cpu_p"=>0.500000, "use>
Jul 23 18:15:58 abdelrahman-1-2 fluent-bit[7848]: [0] cpu.local: [[1721747757.055827232, {}], {"cpu_p"=>2.000000, "use>
Jul 23 18:15:59 abdelrahman-1-2 fluent-bit[7848]: [0] cpu.local: [[1721747758.055374051, {}], {"cpu_p"=>2.750000, "use>
Jul 23 18:16:00 abdelrahman-1-2 fluent-bit[7848]: [0] cpu.local: [[1721747759.055837788, {}], {"cpu_p"=>2.500000, "use>
Jul 23 18:16:01 abdelrahman-1-2 fluent-bit[7848]: [0] cpu.local: [[1721747760.056102041, {}], {"cpu_p"=>3.000000, "use>
Jul 23 18:16:02 abdelrahman-1-2 fluent-bit[7848]: [0] cpu.local: [[1721747761.055193482, {}], {"cpu_p"=>3.500000, "use>
Jul 23 18:16:03 abdelrahman-1-2 fluent-bit[7848]: [0] cpu.local: [[1721747762.058218073, {}], {"cpu_p"=>5.000000, "use>
```

5- Configuring fluent-bit to send logs to elasticsearch server

```
# storage.backlog.mem_limit 5M

[INPUT]
  name tail
  tag linux
  path /var/log/auth.log

# Read interval (sec) Default: 1
interval_sec 1

[OUTPUT]
  name es
  match *
  Host 192.168.1.9
  Port 9200
  HTTP_User elastic
  HTTP_Passwd u=hNzUobNkVUtM2j5Qv5
  tls on
  tls.verify off
  Index Task2
  Type Log
  Suppress_Type_Name ON

[OUTPUT]
  name stdout
  match *
```

And the logs has successfully been sent to elasticsearch

Stack Management

Index Management

Indices

Management

Ingest ?

Ingest Pipelines

Data ?

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Migrate

Alerts and Insights ?

Alerts

Rules

Cases

Connectors

Index Management

Index Management

Indices

Data Streams

Index Templates

Component Templates

Enrich Policies

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)

Include hidden indices

Include rollup indice

Search

Lifecycle status

Lifecycle phase

Reload indices

Create index

<input type="checkbox"/>	Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
<input type="checkbox"/>	fluent-bit	<div><div></div>yellow</div>	open	1	1	189	190.85kb	

Rows per page: 10

<

1

>