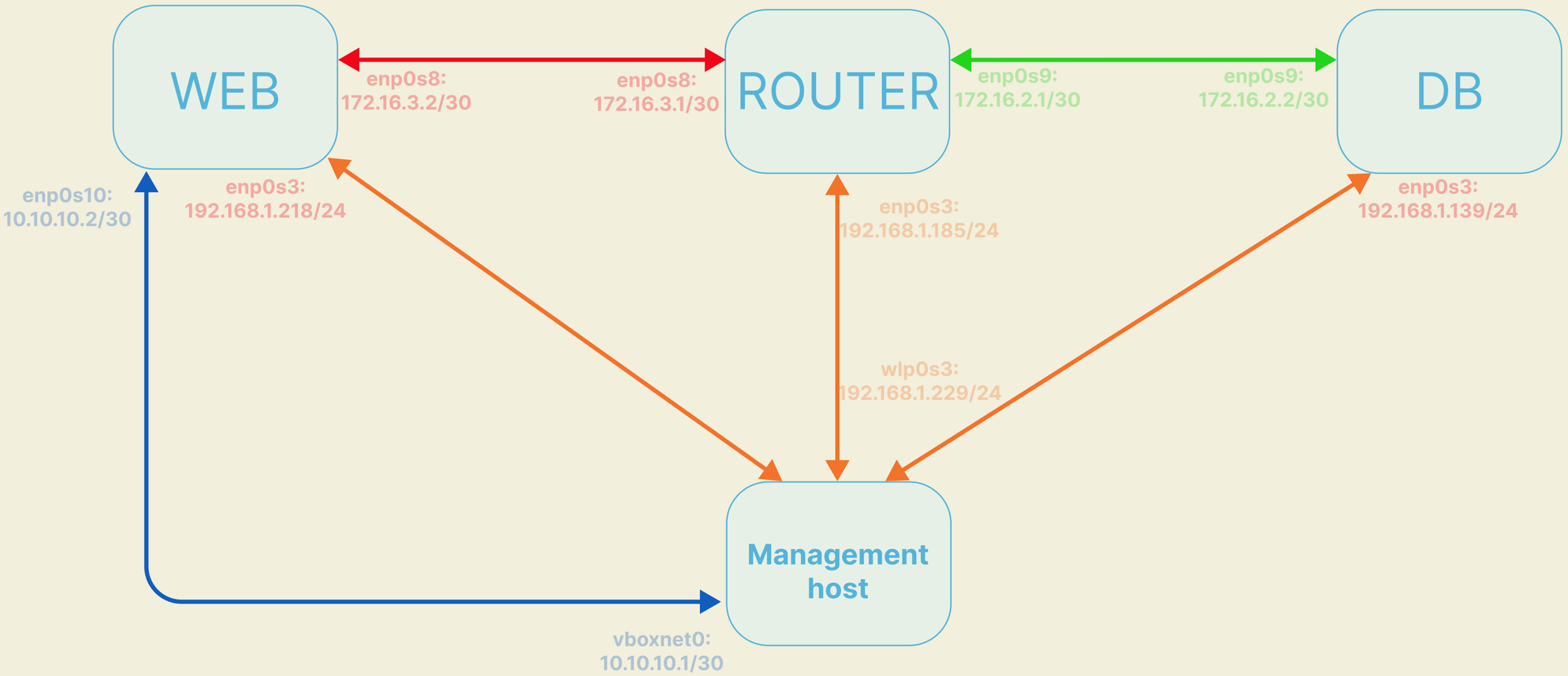
Epam Engineering School Final Task Presentation

Network Infrastructure



172.16.3.0/30 is an internal network web-rt
172.16.2.0/30 is an internal network db-rt
10.10.10.0/30 is a virtual host adapter connection
192.168.1.0/24 is a network bridge (management network). VM`s are isolated from each other by iptables

https://github.com/molv

Objective 2: last mainline kernel installed

Solution:

Linux source code v5.17.5 from kernel.org was configured with menuconfig (see https://github.com/molv/epam_engineering_school/blob/main/kernel/linux-5.17.5/.config) and built as deb packages with make-kpkg.

Then deb packages were copied and installed using Ansible builtin.copy and apt modules at all VM`s. (see https://github.com/molv/epam_engineering_school/blob/main/final/ansible/kernel_install.yaml)

```
molvinec@mv-x230:~/epam$ ansible all -i final/ansible.cfg -a 'uname -a'
192.168.1.139 | CHANGED | rc=0 >>
Linux epamdb 5.17.5-epam-lrn #1 SMP PREEMPT Fri Apr 29 23:27:46 MSK 2022 x86_64 x86_64 x86_64 GNU/Linux
192.168.1.185 | CHANGED | rc=0 >>
Linux epamrt 5.17.5-epam-lrn #1 SMP PREEMPT Fri Apr 29 23:27:46 MSK 2022 x86_64 x86_64 x86_64 GNU/Linux
192.168.1.218 | CHANGED | rc=0 >>
Linux epamweb 5.17.5-epam-lrn #1 SMP PREEMPT Fri Apr 29 23:27:46 MSK 2022 x86_64 x86_64 x86_64 GNU/Linux
```

Objective 3: local timezone configured

Solution:

local timezone was configured with community.general.timezone Ansible module (see https://github.com/molv/epam_engineering_school/blob/main/final/ansible/timezone.yaml) at all VM`s.

```
molvinec@mv-x230:~/epam/final/ansible$ ansible all -i ../ansible.cfg -a "timedatectl"
192.168.1.185 | CHANGED | rc=0 >>
               Local time: Sat 2022-08-13 20:56:42 MSK
           Universal time: Sat 2022-08-13 17:56:42 UTC
                 RTC time: Sat 2022-08-13 17:56:42
                Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
192.168.1.139 | CHANGED | rc=0 >>
               Local time: Sat 2022-08-13 20:56:42 MSK
           Universal time: Sat 2022-08-13 17:56:42 UTC
                 RTC time: Sat 2022-08-13 17:56:42
                Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
192.168.1.218 | CHANGED | rc=0 >>
               Local time: Sat 2022-08-13 20:56:43 MSK
           Universal time: Sat 2022-08-13 17:56:43 UTC
                 RTC time: Sat 2022-08-13 17:56:43
                Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Objective 4: Control plane remote access to machines allowed through SSH and authentication with SSH keys only

Solution:

SSH public keys was copied with ssh-copy-id during the Ansible inventory configuration.

```
molvinec@mv-x230:~/epam/final/ansible$ ansible all -i ../ansible.cfg -m ansible.builtin.setup -a 'filter=ansible_ssh_host_key_rsa_public_keytype
192.168.1.185 | SUCCESS => {
    "ansible_facts": {
        "ansible_ssh_host_key_rsa_public_keytype": "ssh-rsa",
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false
}
192.168.1.139 | SUCCESS => {
    "ansible_facts": {
        "ansible_ssh_host_key_rsa_public_keytype": "ssh-rsa",
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false
}
192.168.1.218 | SUCCESS => {
    "ansible_facts": {
        "ansible_ssh_host_key_rsa_public_keytype": "ssh-rsa",
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false
}
```

Password auth disabled by replacing PasswordAuthentication parameter in /etc/ssh/sshd_config file with Ansible ansible.builtin.replace module. (see https://github.com/molv/epam_engineering_school/blob/main/final/ansible/ssh_auth.yaml)

Objective 5: Operating system (OS) services and processes must use DNS names for inter-VM (virtual machine) communication.

Solution:

/etc/hosts files are used as source for DNS resolving

```
molvinec@mv-x230:~/epam/final/ansible$ ansible all -i ../ansible.cfg -a "cat /etc/hosts" |grep -vi ip
192.168.1.139 | CHANGED | rc=0 >>
127.0.0.1 localhost
127.0.1.1 epamdb
172.16.3.2 epamweb
172.16.2.1 epamrt
192.168.1.185 | CHANGED | rc=0 >>
127.0.0.1 localhost
127.0.1.1 epamrt
172.16.3.2 epamweb
172.16.2.2 epamdb
192.168.1.218 | CHANGED | rc=0 >>
127.0.0.1 localhost
127.0.1.1 epamweb
172.16.3.1 epamrt
172.16.2.2 epamdb
```

Objective 6: Network interfaces, filters. Packets forwarding on ROUTER VM

Solution:

Network interfaces are configured by netplan, config files was prepared using Ansible ansible.builtin.template module (see https://github.com/molv/epam_engineering_school/blob/main/final/ansible/net_conf.yaml). Packet forwarding enabled by net.ipv4.ip_forward sysctl key with ansible.posix.sysctl module, see the link above.

Packet filtering configured with Ansible ansible.builtin.iptables module and saved using iptables-persistent package and community.general.iptables_state Ansisble module (see https://github.com/molv/epam_engineering_school/blob/main/final/ansible/filter.yaml). Allowed SSH, NTP, HTTP/S, Grafana, Prometheus, PostgreSQL, Elasticsearch protocols on certain VM`s

```
molvinec@mv-x230:~/epam/final/ansible$ ansible web -i ../ansible.cfg -a "iptables -L -nv" --become
192.168.1.218 | CHANGED | rc=0 >>
Chain INPUT (policy DROP 40 packets, 3804 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:123 dpts:1024:65535
 3195 3811K ACCEPT     tcp  --  enp0s3 *       192.168.1.229        0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   34  2718 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
   78  7303 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53 dpts:1024:65535
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53 dpts:1024:65535
    8   672 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
82635   16M ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
  473 2355K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80 dpts:1024:65535
   87 26461 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443 dpts:1024:65535
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:9100
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:9091 dpts:1024:65535
 2025 2007K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  enp0s10 *       0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:5432 dpts:1024:65535
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:9090
  191 11460 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:9091
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3000
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:9100 dpts:1024:65535
    6   360 ACCEPT     tcp  --  enp0s10 *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5601

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1503K packets, 306M bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
molvinec@mv-x230:~/epam/final/ansible$ ansible db -i ../ansible.cfg -a "iptables -L -nv" --become
192.168.1.139 | CHANGED | rc=0 >>
Chain INPUT (policy DROP 25 packets, 2904 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:123 dpts:1024:65535
 1712 3074K ACCEPT     tcp  --  enp0s3 *       192.168.1.229        0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   20  1652 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
   34  3845 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53 dpts:1024:65535
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53 dpts:1024:65535
    8   672 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
   93 32268 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
  481 2686K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80 dpts:1024:65535
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443 dpts:1024:65535
  318 30045 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:9100
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:9091 dpts:1024:65535
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5432

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 30105 packets, 21M bytes)
 pkts bytes target     prot opt in     out     source               destination
```

```
molvinec@mv-x230:~/epam/final/ansible$ ansible router -i ../ansible.cfg -a "iptables -L -nv" --become
192.168.1.185 | CHANGED | rc=0 >>
Chain INPUT (policy DROP 25 packets, 2904 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:123 dpts:1024:65535
 1528 2743K ACCEPT     tcp  --  enp0s3 *       192.168.1.229        0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   13  1075 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
   34  3101 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53 dpts:1024:65535
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53 dpts:1024:65535
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
  409 2351K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80 dpts:1024:65535
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443 dpts:1024:65535
  296 29375 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:9100
  820 59655 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:9091 dpts:1024:65535
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 7645 packets, 13M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 21056 packets, 13M bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Objective 7: RAID and LVM on DB VM. /local/files directory should be mounted on lvm partitions on DB server (2 extra block devices added to a server). /local/backups directory should be mounted on mdraid (RAID1/mirror) partition on DB server (2 extra block devices added to a server)

Solution:

LVM and RAID volumes was configured using fdisk, pvcreate, vgcreate, lvcreate, mdadm, mkfs.ext4 tools and added to /etc/fstab

```
molv@epamdb:~$ sudo lvs
[sudo] password for molv:
  LV        VG        Attr       LSize    Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  ubuntu-lv ubuntu-vg -wi-ao----   <8.25g
  lv_files  vg_files  -wi-ao---- 1016.00m
molv@epamdb:~$ sudo mount |grep files
/dev/mapper/vg_files-lv_files on /local/files type ext4 (rw,relatime)
molv@epamdb:~$ grep files /etc/fstab
UUID=034cb9e9-193f-436b-a080-ea448f43847f /local/files  ext4 defaults 0 2
```

```
molv@epamdb:~$ sudo mdadm -D /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Tue May  3 21:26:46 2022
        Raid Level : raid1
        Array Size : 522240 (510.00 MiB 534.77 MB)
     Used Dev Size : 522240 (510.00 MiB 534.77 MB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Sat Aug 13 13:55:28 2022
             State : clean
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

Consistency Policy : resync

              Name : epamdb:0  (local to host epamdb)
              UUID : 470305f5:c28c48a2:c04714a0:e8852d2a
            Events : 66

    Number   Major   Minor   RaidDevice State
       0       8       49        0      active sync   /dev/sdd1
       1       8       65        1      active sync   /dev/sde1
molv@epamdb:~$ grep backup /etc/fstab
UUID=9c7717a0-e46c-4f76-802c-9dc1dcbb1ba7 /local/backups ext4 defaults 0 2
```

Objective 8: Monitoring. CPU, MEM, disk IOPs

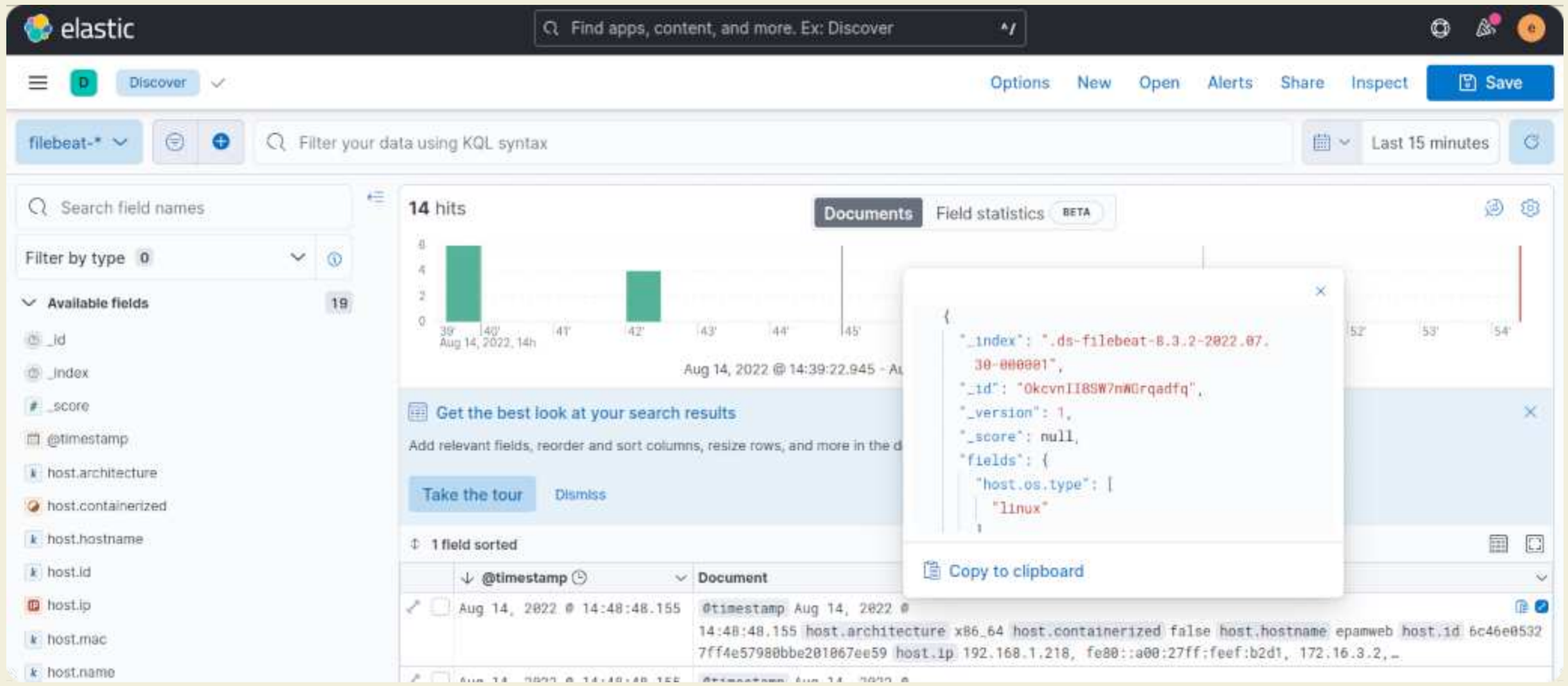
Solution:

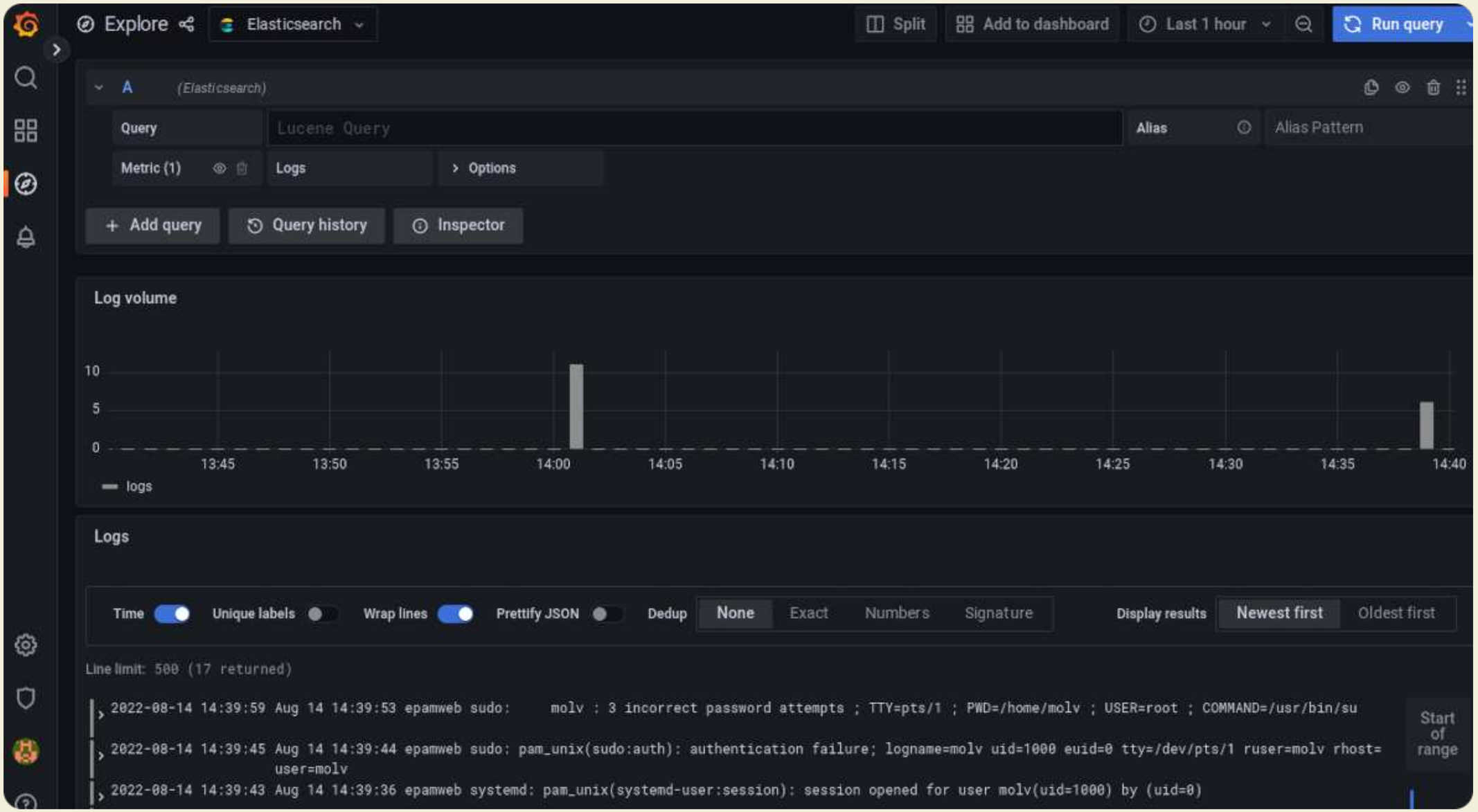
CPU, memory and disk IOPs are visualized with Grafana and Prometheus-node-exporter. This info also could be reviewed with top/vmstat/free/iostat tools.

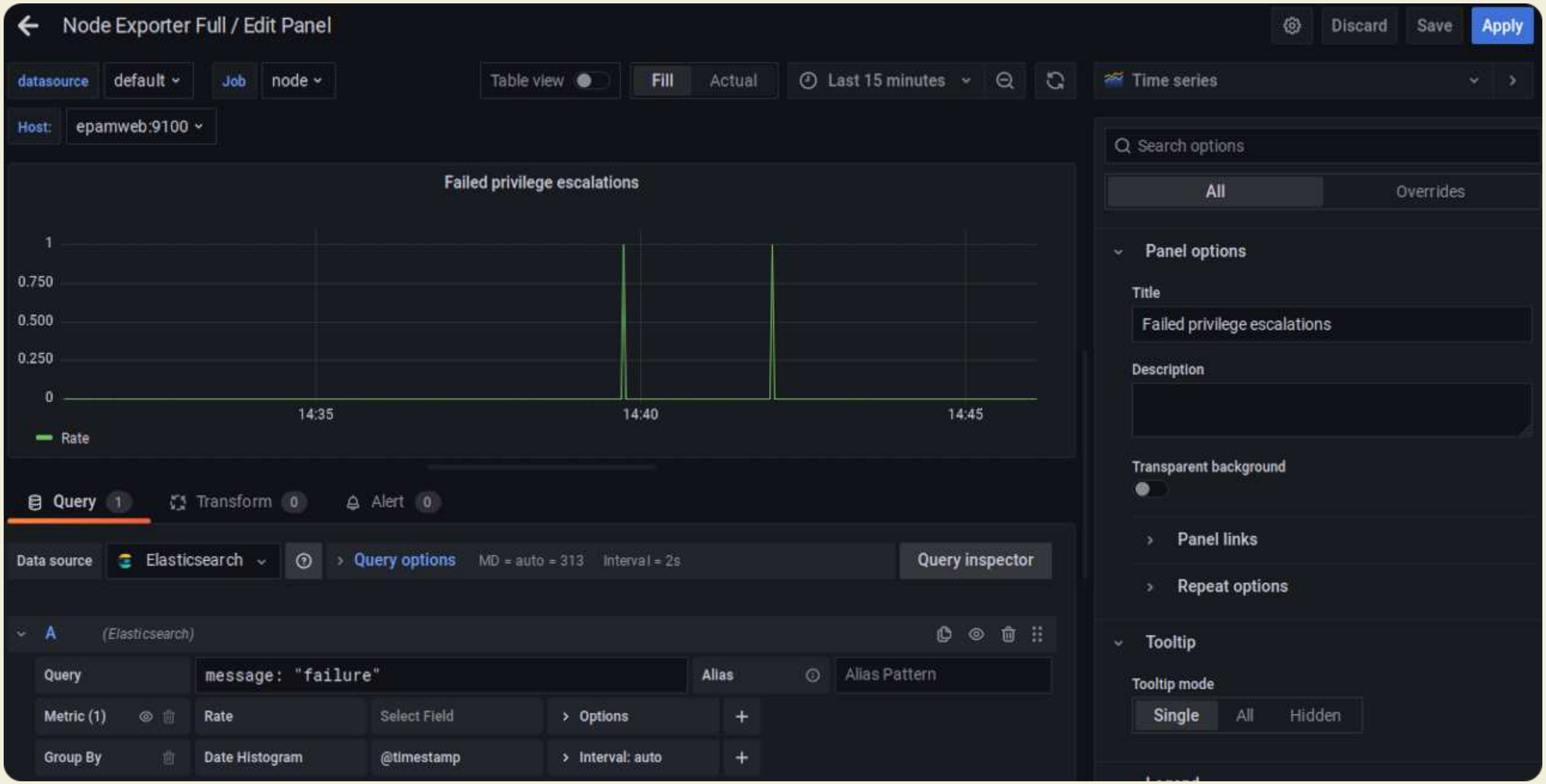
Objective 9: Monitoring. Accounting events

Solution:

Elasticsearch, Kibana and Filebeat was deployed from the local deb repo. Filebeat scrapes data from /var/log/auth.log, sends it to Elasticsearch .filebeat index. Then Grafana imports it with standard Elasticsearch module. Dashbord shows unsucessfull privilege escalation attempts as via PromQL query 'message: "failure"'. ELK configs at https://github.com/molv/epam_engineering_school/tree/main/final/elastic




Explore
Elasticsearch
Split
Add to dashboard
Last 1 hour
Run query
A
(Elasticsearch)
Query
Lucene Query
Alias
Alias Pattern
Metric (1)
Logs
Options
Add query
Query history
Inspector
Log volume
10
5
0
13:45
13:50
13:55
14:00
14:05
14:10
14:15
14:20
14:25
14:30
14:35
14:40
logs
Logs
Time
Unique labels
Wrap lines
Prettify JSON
Dedup
None
Exact
Numbers
Signature
Display results
Newest first
Oldest first
Line limit: 500 (17 returned)
2022-08-14 14:39:59 Aug 14 14:39:53 epamweb sudo: molv : 3 incorrect password attempts ; TTY=pts/1 ; PWD=/home/molv ; USER=root ; COMMAND=/usr/bin/su
2022-08-14 14:39:45 Aug 14 14:39:44 epamweb sudo: pam_unix(sudo:auth): authentication failure; logname=molv uid=1000 euid=0 tty=/dev/pts/1 ruser=molv rhost= user=molv
2022-08-14 14:39:43 Aug 14 14:39:36 epamweb systemd: pam_unix(systemd-user:session): session opened for user molv(uid=1000) by (uid=0)
Start of range

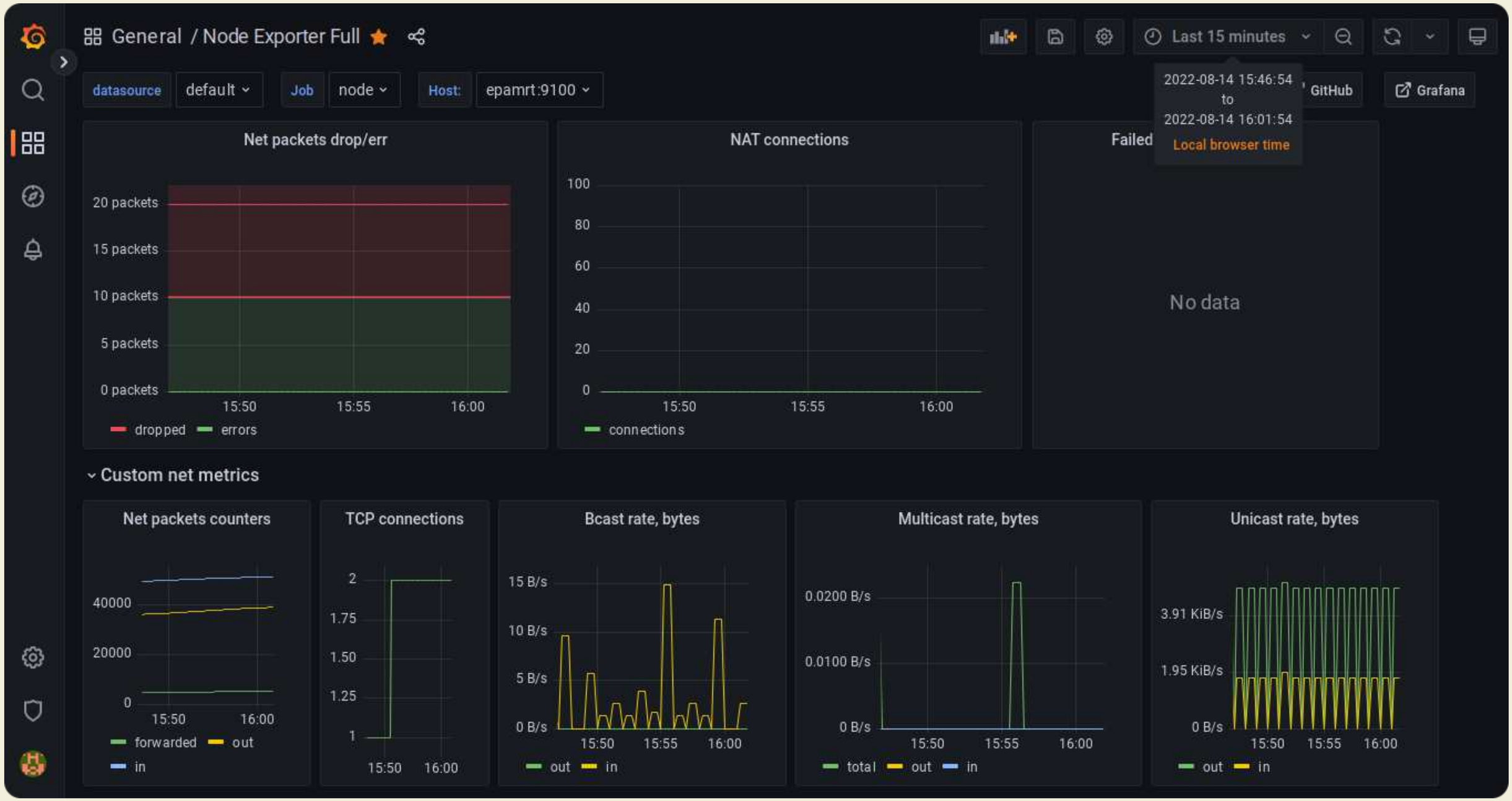

Node Exporter Full / Edit Panel
Discard
Save
Apply
datasource
default
Job
node
Table view
Fill
Actual
Last 15 minutes
Time series
Host:
epamweb:9100
Search options
All
Overrides
Failed privilege escalations
1
0.750
0.500
0.250
0
14:35
14:40
14:45
Rate
Panel options
Title
Failed privilege escalations
Description
Transparent background
Query 1
Transform 0
Alert 0
Data source
Elasticsearch
Query options
MD = auto = 313
Interval = 2s
Query inspector
Panel links
Repeat options
A
(Elasticsearch)
Tooltip
Query
message: "failure"
Alias
Alias Pattern
Tooltip mode
Metric (1)
Rate
Select Field
Options
Single
All
Hidden
Group By
Date Histogram
@timestamp
Interval: auto

Objective 10: Network monitoring. TCP sessions established, IN/OUT/DROPPED/ERRORs, forwarded/routed packets, broadcast/multicats/unicast packets. NAT sessions.

Solution:

Network counters could be reviewed with netstat or nstat tools. NAT sessions - with conntrack tool.

Bash script 'custom_metrics.sh' (see https://github.com/molv/epam_engineering_school/blob/main/final/bash/custom_metrics.sh) gathers required metrics and sends to Prometheus Push Gateway. Afterwards, metrics could be reviewed with Grafana. Unicast packets counted as total - multicast - broadcast. Also, some of metrics are supported by Prometheus Node Exporter.



Objective 11: Database. Structure, data, access.

Solution:

Database was created with community.postgresql.postgresql_db Ansible module. Structure was created with community.postgresql.postgresql_query Ansible module. Data was imported with ansible.builtin.copy and community.postgresql.postgresql_query Ansible modules. Production user was created with community.postgresql.postgresql_user Ansible module. User`s privileges was configured with community.postgresql.postgresql_privs Ansible module. Playbook at https://github.com/molv/epam_engineering_school/blob/main/final/ansible/postgres.yaml

```
molv@epamweb:~$ psql -U prod_user -d epam -h epamdb
psql (14.3 (Ubuntu 14.3-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

epam=> select ar.id, ar.magazines_id, mag.name, ar.article_type_id, art.type, ar.author_id, aut.author from articles ar
left join article_types art on art.id = ar.article_type_id
left join author aut on ar.author_id = aut.id
left join magazines mag on ar.magazines_id = mag.id;
 id | magazines_id |     name     | article_type_id |     type      | author_id | author
----+--------------+--------------+-----------------+---------------+-----------+---------
  1 |            1 | it herald    |               2 | tech          |         3 | Atom
  2 |            3 | IT with kids |               3 | entertainment |         2 | Wall-e
  3 |            2 | IT STORIES   |               2 | tech          |         4 | T1000
  4 |            1 | it herald    |               1 | news          |         1 | Chappie
(4 rows)
```

Objective 12: Bash scripts

Solution:

First bash script, which dumps data to .CVS files and archives them if needed:
https://github.com/molv/epam_engineering_school/blob/main/final/bash/db_dump.sh

Second one, which checks files quantity or size and sends email if threshold value was met:
https://github.com/molv/epam_engineering_school/blob/main/final/bash/backup_mail.sh

Objective 12: Python program. Receive data from DB and save as HTML page

Solution:

Program was written using os.path module to get path to home dir of current user, where .pgpass file with PostgreSQL credentials is saved. Read with ‘open’ method.

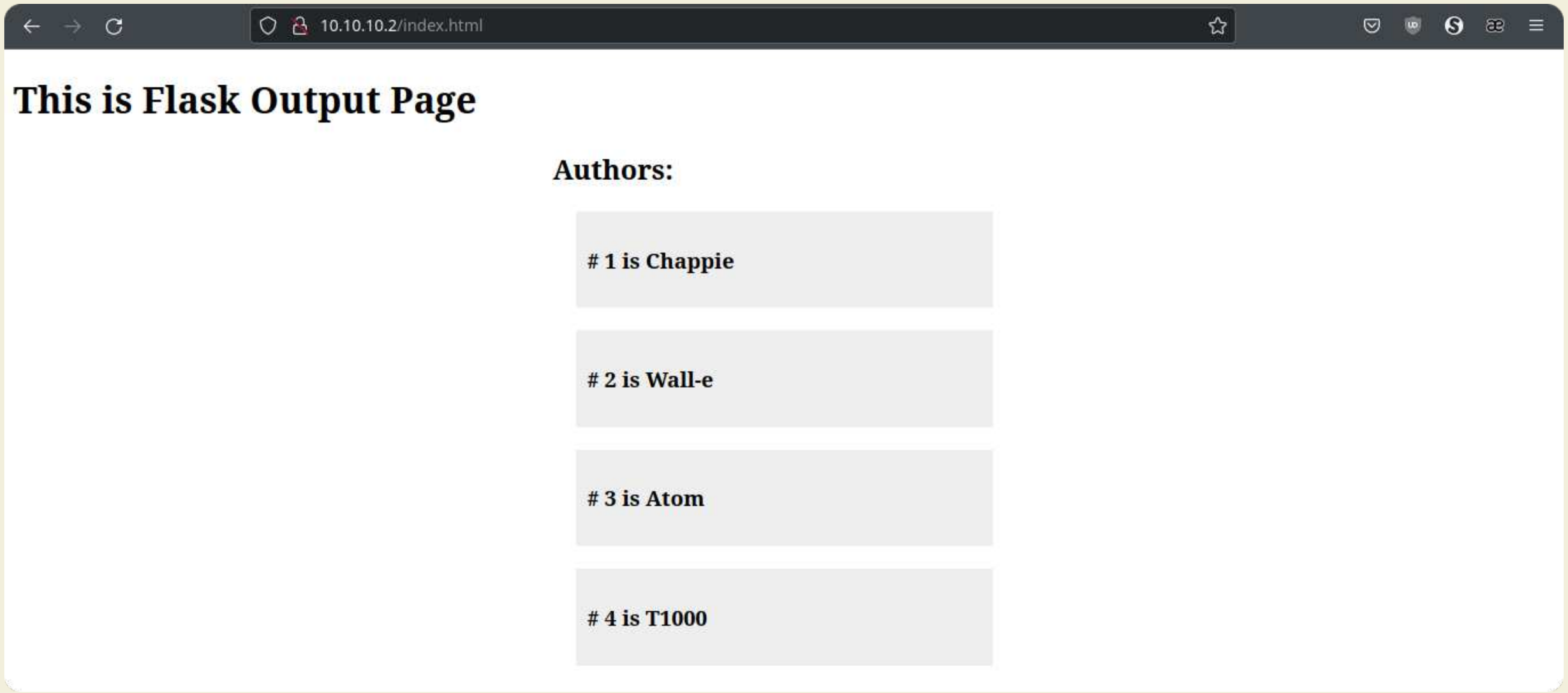
psycopg2 module for set connection with DB and receive data from articles table, with query into cursor.

Flask module as a built-in web server, which also generates a HTML page using Jlnja2 template (templates dir).

Then request module captures generated page from Flask web server and saves as HTML file with open (w) method.

Application was designed with separate threads (threads module), one is for Flask, another is for generated page saving each 60 seconds.

https://github.com/molv/epam_psql2flask



Objective 13: HTTP and HTTPS MITM attack.

Solution:

First pic is for HTTP request, captured with tcpdump on router machine (iptables rules was adjusted for objective).

Second one - intercepted packets, secured with self-signed certificates for nginx.

```
root@epamrt:/home/molv# tcpdump -v -i enp0s8 src 172.16.3.2 and port 80
tcpdump: listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:43:47.709713 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    epamweb.http > epamdb.50262: Flags [S.], cksum 0x8650 (correct), seq 1155615009, ack 1928138383, win 65160, options [mss 1460,sackOK,TS val 3735878684 ecr 90868962
5,nop,wscale 7], length 0
18:43:47.710571 IP (tos 0x0, ttl 64, id 47179, offset 0, flags [DF], proto TCP (6), length 52)
    epamweb.http > epamdb.50262: Flags [.], cksum 0xb154 (correct), ack 82, win 509, options [nop,nop,TS val 3735878685 ecr 908689627], length 0
18:43:47.710929 IP (tos 0x0, ttl 64, id 47180, offset 0, flags [DF], proto TCP (6), length 986)
    epamweb.http > epamdb.50262: Flags [P.], cksum 0xaa07 (correct), seq 1:935, ack 82, win 509, options [nop,nop,TS val 3735878685 ecr 908689627], length 934: HTTP, l
ength: 934
        HTTP/1.1 200 OK
        Server: nginx/1.18.0 (Ubuntu)
        Date: Sun, 14 Aug 2022 15:43:47 GMT
        Content-Type: text/html
        Content-Length: 687
        Last-Modified: Sun, 14 Aug 2022 15:33:46 GMT
        Connection: keep-alive
        ETag: "62f915da-2af"
        Accept-Ranges: bytes

        <!DOCTYPE html>
        <head><title>Here is some data from DB</title></head>
        <body>
        <h1>This is Flask Output Page</h1>

        <div>
         <div style="width: 30%; margin: auto">
             <h2>Authors:</h2>

            <div style="padding: 10px; background-color: #EEE; margin: 20px">
                    <h3># 1 is Chappie </h3>
            </div>

            <div style="padding: 10px; background-color: #EEE; margin: 20px">
```

```
root@epamrt:/home/molv# tcpdump -v -i enp0s8 src 172.16.3.2 and port 443
tcpdump: listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:55:20.480102 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    epamweb.https > epamdb.40376: Flags [S.], cksum 0xb4f8 (correct), seq 750198778, ack 378830448, win 65160, options [mss 1460,sackOK,TS val 3736571452 ecr 909382392
,nop,wscale 7], length 0
18:55:20.488166 IP (tos 0x0, ttl 64, id 26117, offset 0, flags [DF], proto TCP (6), length 52)
    epamweb.https > epamdb.40376: Flags [.], cksum 0xde3e (correct), ack 518, win 506, options [nop,nop,TS val 3736571460 ecr 909382400], length 0
18:55:20.490588 IP (tos 0x0, ttl 64, id 26118, offset 0, flags [DF], proto TCP (6), length 1588)
    epamweb.https > epamdb.40376: Flags [P.], cksum 0x634b (incorrect -> 0x30a2), seq 1:1537, ack 518, win 506, options [nop,nop,TS val 3736571462 ecr 909382400], leng
th 1536
18:55:20.494794 IP (tos 0x0, ttl 64, id 26120, offset 0, flags [DF], proto TCP (6), length 52)
    epamweb.https > epamdb.40376: Flags [.], cksum 0xd7e1 (correct), ack 598, win 506, options [nop,nop,TS val 3736571466 ecr 909382407], length 0
18:55:20.494794 IP (tos 0x0, ttl 64, id 26121, offset 0, flags [DF], proto TCP (6), length 52)
    epamweb.https > epamdb.40376: Flags [.], cksum 0xd77a (correct), ack 701, win 506, options [nop,nop,TS val 3736571466 ecr 909382407], length 0
18:55:20.495290 IP (tos 0x0, ttl 64, id 26122, offset 0, flags [DF], proto TCP (6), length 339)
    epamweb.https > epamdb.40376: Flags [P.], cksum 0x4faf (correct), seq 1537:1824, ack 701, win 506, options [nop,nop,TS val 3736571467 ecr 909382407], length 287
18:55:20.495438 IP (tos 0x0, ttl 64, id 26123, offset 0, flags [DF], proto TCP (6), length 339)
    epamweb.https > epamdb.40376: Flags [P.], cksum 0xad82 (correct), seq 1824:2111, ack 701, win 506, options [nop,nop,TS val 3736571467 ecr 909382407], length 287
18:55:20.495840 IP (tos 0x0, ttl 64, id 26124, offset 0, flags [DF], proto TCP (6), length 1008)
    epamweb.https > epamdb.40376: Flags [P.], cksum 0x80c6 (correct), seq 2111:3067, ack 701, win 506, options [nop,nop,TS val 3736571467 ecr 909382407], length 956
18:55:20.508669 IP (tos 0x0, ttl 64, id 26125, offset 0, flags [DF], proto TCP (6), length 52)
    epamweb.https > epamdb.40376: Flags [.], cksum 0xd14c (correct), ack 725, win 506, options [nop,nop,TS val 3736571480 ecr 909382421], length 0
18:55:20.508917 IP (tos 0x0, ttl 64, id 26126, offset 0, flags [DF], proto TCP (6), length 52)
    epamweb.https > epamdb.40376: Flags [F.], cksum 0xd14a (correct), seq 3067, ack 726, win 506, options [nop,nop,TS val 3736571480 ecr 909382421], length 0
^C
```

THANK YOU!