ДЗ-09: Loki

Перенаправил Vector из конфигурации 8-го ДЗ на Loki.

Установка

https://grafana.com/docs/loki/latest/setup/install/

Конфиги

loki – стандартный конфиг для хранения логов на файловой системе.

```
auth_enabled: false

server:
  http_listen_port: 3100
  grpc_listen_port: 9096

common:
  instance_addr: 127.0.0.1
  path_prefix: /tmp/loki
  storage:
    filesystem:
      chunks_directory: /tmp/loki/chunks
      rules_directory: /tmp/loki/rules
  replication_factor: 1
  ring:
    kvstore:
      store: inmemory

query_range:
  results_cache:
    cache:
      embedded_cache:
        enabled: true
        max_size_mb: 100

schema_config:
  configs:
    - from: 2020-10-24
      store: tsdb
      object_store: filesystem
      schema: v13
      index:
        prefix: index_
        period: 24h

analytics:
  reporting_enabled: false
```

vector.yaml

```
sources:
  sshd_http_source:
    type: "socket"
    address: "127.0.0.1:10514"
    mode: "udp"
    decoding:
      codec: "json"
  sshd_log_source:
    type: "file"
    read_from: "beginning"
    include:
      - "/var/log/sshd.log"


transforms:
  sshd_http_transform:
    type: "remap"
    inputs: ["sshd_http_source"]
```

```
    source: '.programname=upcase!(.programname) + "-from-vector-http"'
  sshd_log_transform:
    type: "remap"
    inputs: ["sshd_log_source"]
    source: |
     . |= parse_syslog!(.message)
     .@timestamp = .timestamp
     .programname = "SSHD-from-vector-log-file"

sinks:
  print:
    type: "console"
    inputs: ["sshd_http_transform", "sshd_log_transform"]
    encoding:
      codec: "json"
  loki:
    type: "loki"
    inputs: ["sshd_*_transform"]
    endpoint: http://localhost:3100
    encoding:
      codec: json
    labels:
      source: vector
      programname: "{{ programname }}"
      severity: "{{ severity }}"
    out_of_order_action: drop
    path: /loki/api/v1/push
```

Получение логов

Проверка, что метки появились

```
root@debian:/tmp/loki# ./logcli labels source
2024/04/13 10:50:30 http://localhost:3100/loki/api/v1/label/source/values?end=1712994630122059296&start=1712991030122059296
vector
root@debian:/tmp/loki# ./logcli labels programname
2024/04/13 10:50:32 http://localhost:3100/loki/api/v1/label/programname/values?end=1712994632590196687&start=1712991032590196687
SSHD-from-vector-http
SSHD-from-vector-log-file
root@debian:/tmp/loki#
```

Получение логов

```
root@debian:/tmp/loki# ./logcli query '{source="vector"}'
2024/04/13 10:51:34 http://localhost:3100/loki/api/v1/query_range?direction=BACKWARD&end=1712994694744128114&limit=30&query=%7Bsource%3D%22vector%22%7D&start=1712991094744128114
2024/04/13 10:51:34 Common labels: {service_name="unknown_service", source="vector"}
2024-04-13T10:21:07+03:00 {level="info", programname="SSHD-from-vector-log-file"}                {"@timestamp":"2024-04-13T07:21:07.799801Z","appname":"systemd-logind","file":"/var/log/sshd.log","host":"debian","hostname":"debian","message":"Removed session 94.","procid":524,"programname":"SSHD-from-vector-log-file","source_type":"file"}
2024-04-13T10:21:07+03:00 {level="info", programname="SSHD-from-vector-log-file"}                {"@timestamp":"2024-04-13T07:21:07.797792Z","appname":"systemd-logind","file":"/var/log/sshd.log","host":"debian","hostname":"debian","message":"Session 94 logged out. Waiting for processes to exit.","procid":524,"programname":"SSHD-from-vector-log-file","source_type":"file"}
2024-04-13T10:21:07+03:00 {level="debug", programname="SSHD-from-vector-http", severity="info"}  {"@timestamp":"2024-04-13T10:21:07.793062+03:00","@version":"1","facility":"authpriv","host":"127.0.0.1","message":" pam_unix(sshd:session): session closed for user user","port":59824,"procid":"20857","programname":"SSHD-from-vector-http","severity":"info","source_type":"socket","sysloghost":"debian"}
2024-04-13T10:21:07+03:00 {level="debug", programname="SSHD-from-vector-http", severity="info"}  {"@timestamp":"2024-04-13T10:21:07.792010+03:00","@version":"1","facility":"auth","host":"127.0.0.1","message":" Disconnected from user user 127.0.0.1 port 48964","port":59824,"procid":"20866","programname":"SSHD-from-vector-http","severity":"info","source_type":"socket","sysloghost":"debian"}
2024-04-13T10:21:07+03:00 {level="debug", programname="SSHD-from-vector-http", severity="info"}  {"@timestamp":"2024-04-13T10:21:07.791527+03:00","@version":"1","facility":"auth","host":"127.0.0.1","message":" Received disconnect from 127.0.0.1 port 48964:11: disconnected by user","port":59824,"procid":"20866","programname":"SSHD-from-vector-http","severity":"info","source_type":"socket","sysloghost":"debian"}
2024-04-13T10:21:07+03:00 {level="debug", programname="SSHD-from-vector-http", severity="debug"} {"@timestamp":"2024-04-13T10:21:07.097582+03:00","@version":"1","facility":"authpriv","host":"127.0.0.1","message":" pam_env(sshd:session): deprecated reading of user environment enabled","port":59824,"procid":"20857","programname":"SSHD-from-vector-http","severity":"debug","source_type":"socket","sysloghost":"debian"}
2024-04-13T10:21:07+03:00 {level="debug", programname="SSHD-from-vector-http", severity="info"}  {"@timestamp":"2024-04-13T10:21:07.054908+03:00","@version":"1","facility":"authpriv","host":"127.0.0.1","message":" pam_unix(sshd:session): session opened for user user(uid=1000) by (uid=0)","port":59824,"procid":"20857","programname":"SSHD-from-vector-http","severity":"info","source_type":"socket","sysloghost":"debian"}
2024-04-13T10:21:07+03:00 {level="debug", programname="SSHD-from-vector-http", severity="info"}  {"@timestamp":"2024-04-13T10:21:07.053369+03:00","@version":"1","facility":"auth","host":"127.0.0.1","message":" Accepted password for user from 127.0.0.1 port 48964 ssh2","port":59824,"procid":"20857","programname":"SSHD-from-vector-http","severity":"info","source_type":"socket","sysloghost":"debian"}
```