ДЗ-06: ELK

Настройка

https://www.dmosk.ru/miniinstruktions.php?mini=rsyslog
https://www.8host.com/blog/centralizaciya-logov-s-pomoshhyu-rsyslog-logstash-i-elasticsearch-v-ubuntu-14-04/

/etc/logstash/logstash.yml

```
xpack.monitoring.enabled: true
xpack.monitoring.elasticsearch.url: http://X.X.X.X:9200
```

/etc/rsyslog.conf

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

/etc/ssh/sshd_config

```
SyslogFacility AUTH
LogLevel INFO
```

Конфиги

/etc/rsyslog.d/rsyslog-json-template.conf – форматирование в json для отправки в logstash

```
template(name="json-template"
type="list") {
constant(value="{")
constant(value="\"@timestamp\":\"")     property(name="timereported" dateFormat="rfc3339")
constant(value="\",\"@version\":\"1")
constant(value="\",\"message\":\"")     property(name="msg" format="json")
constant(value="\",\"sysloghost\":\"")  property(name="hostname")
constant(value="\",\"severity\":\"")    property(name="syslogseverity-text")
constant(value="\",\"facility\":\"")    property(name="syslogfacility-text")
constant(value="\",\"programname\":\"") property(name="programname")
constant(value="\",\"procid\":\"")      property(name="procid")
constant(value="\"}\n")
}
```

/etc/rsyslog.d/rsyslog-sshd-output.conf – отправка логов sshd в logstash

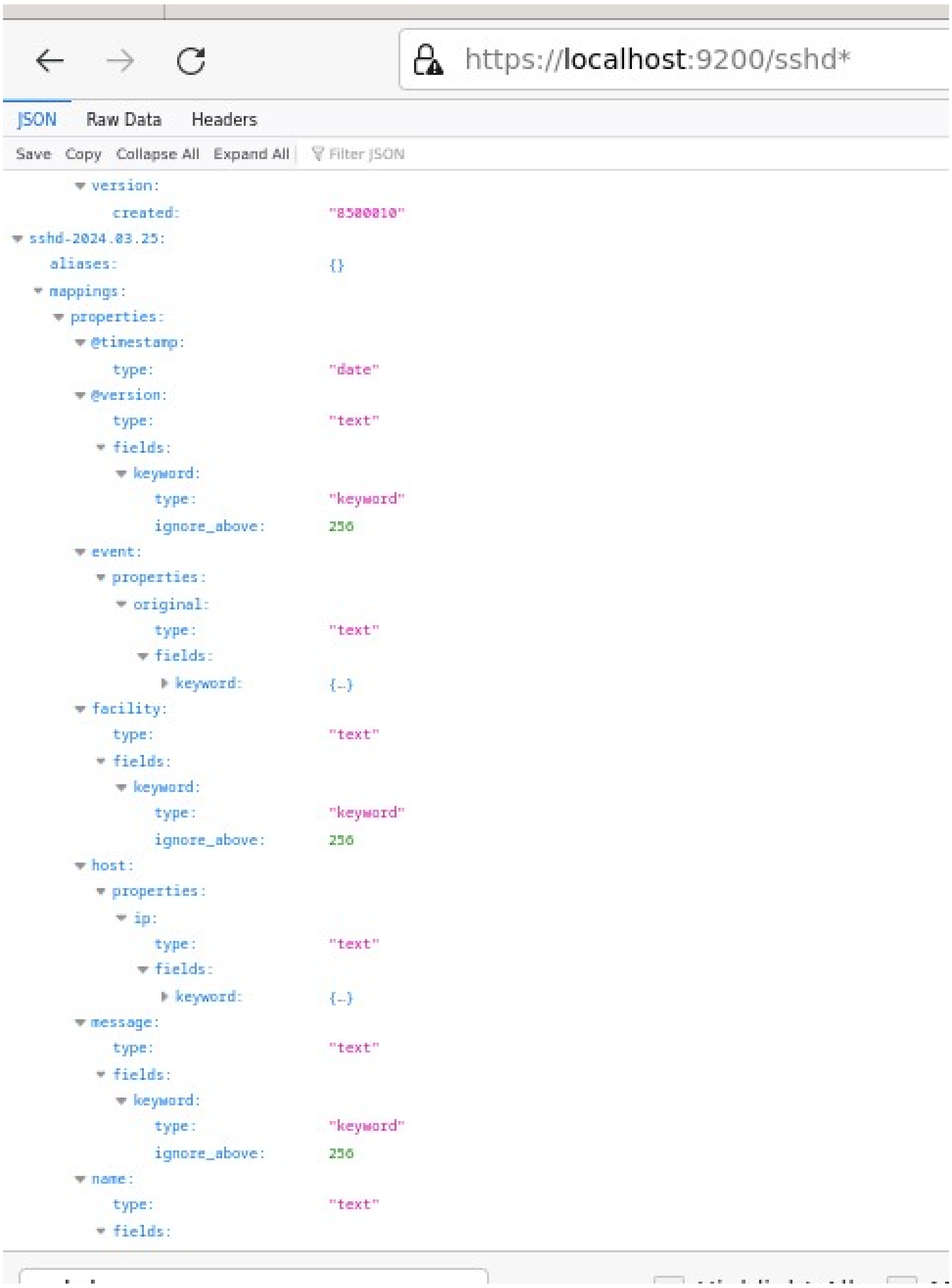
```
if $programname == 'sshd' then @127.0.0.1:10514;json-template
& ~
```

/etc/logstash/conf.d/logstash-rsyslog.conf

```
input {
   udp {
      host => "127.0.0.1"
      port => 10514
      codec => "json"
      type => "rsyslog"
   }
}
filter { }
output {
   if [programname] == "sshd" {
      elasticsearch {
         index => "sshd-%{+YYYY.MM.dd}"
         ssl => true
         ssl_certificate_verification => false
         user => "elastic"
         password => "10DM27XoI52iiDxXZa78"
      }

   }
}
```

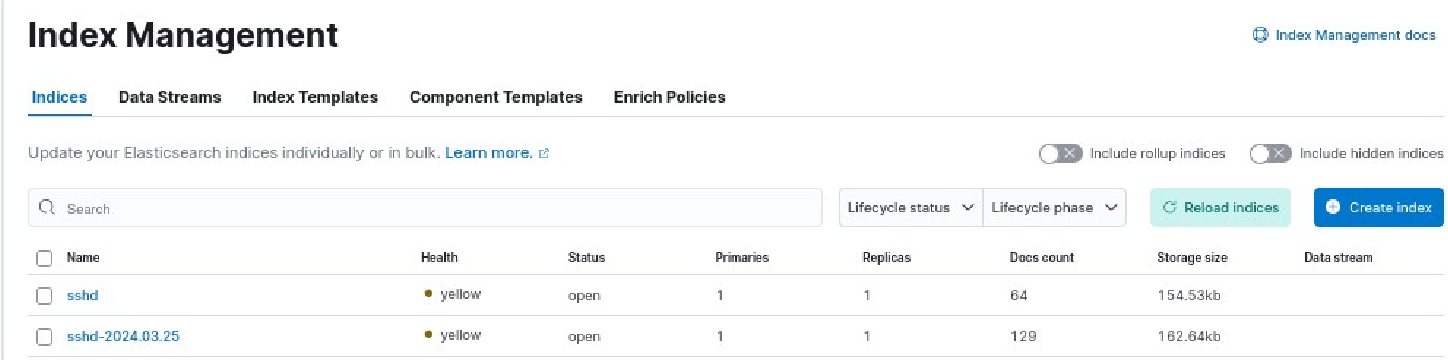
Index



https://localhost:9200/sshd*

```
    version:
      created:                    "8500010"
sshd-2024.03.25:
  aliases:                        {}
  mappings:
    properties:
      @timestamp:
        type:                     "date"
      @version:
        type:                     "text"
        fields:
          keyword:
            type:                 "keyword"
            ignore_above:         256
      event:
        properties:
          original:
            type:                 "text"
            fields:
              keyword:            {…}
      facility:
        type:                     "text"
        fields:
          keyword:
            type:                 "keyword"
            ignore_above:         256
      host:
        properties:
          ip:
            type:                 "text"
            fields:
              keyword:            {…}
      message:
        type:                     "text"
        fields:
          keyword:
            type:                 "keyword"
            ignore_above:         256
      name:
        type:                     "text"
        fields:
```

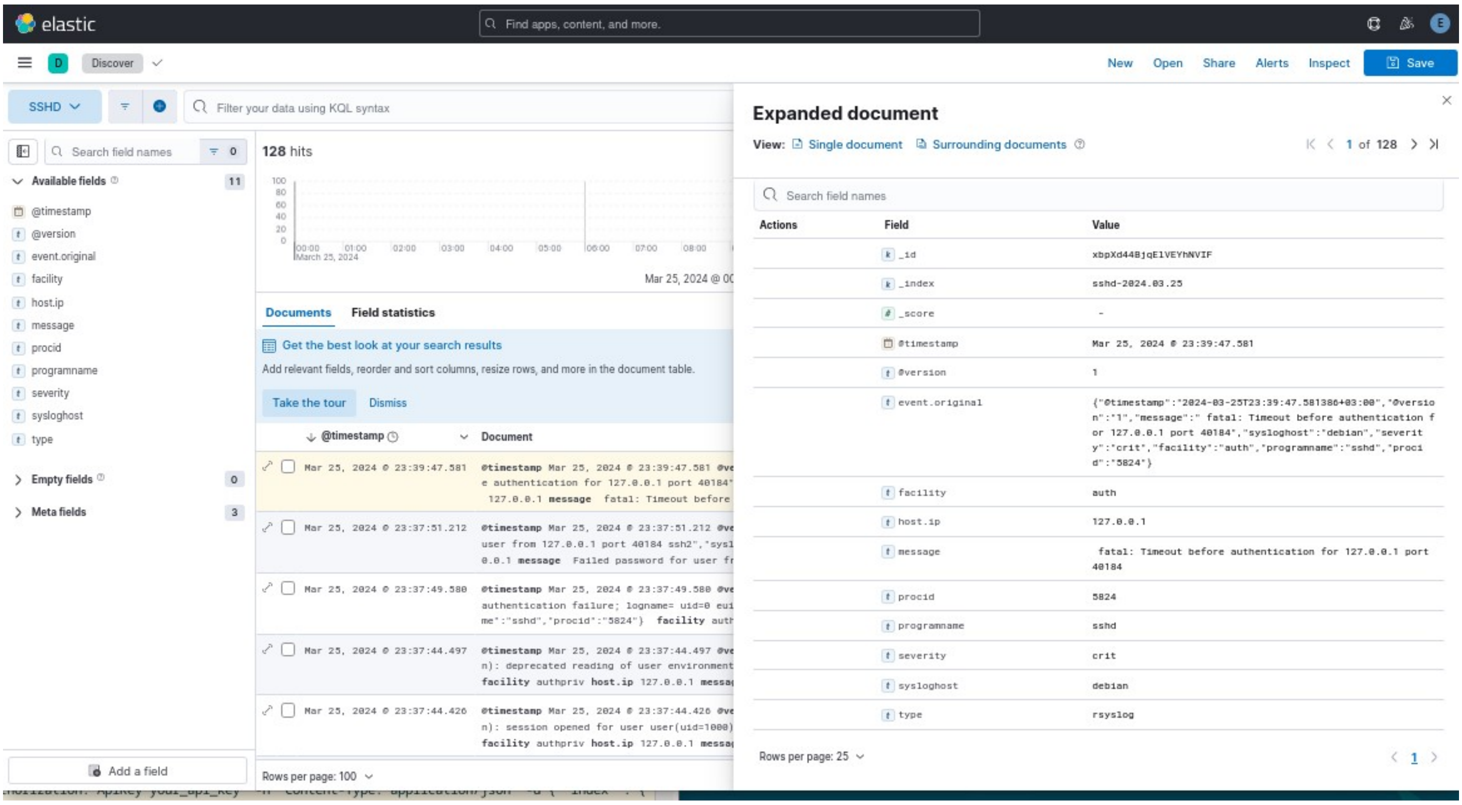
Kibana



Index Management

Update your Elasticsearch indices individually or in bulk. Learn more.

□	Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
□	sshd	● yellow	open	1	1	64	154.53kb	
□	sshd-2024.03.25	● yellow	open	1	1	129	162.64kb	



Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

@timestamp	Document
Mar 25, 2024 @ 23:39:47.581	@timestamp Mar 25, 2024 @ 23:39:47.581 @ve e authentication for 127.0.0.1 port 40184" 127.0.0.1 message fatal: Timeout before
Mar 25, 2024 @ 23:37:51.212	@timestamp Mar 25, 2024 @ 23:37:51.212 @ve user from 127.0.0.1 port 40184 ssh2","sysl 0.0.1 message Failed password for user fr
Mar 25, 2024 @ 23:37:49.580	@timestamp Mar 25, 2024 @ 23:37:49.580 @ve authentication failure; logname= uid=0 eui me":"sshd","procid":"5824"} facility auth
Mar 25, 2024 @ 23:37:44.497	@timestamp Mar 25, 2024 @ 23:37:44.497 @ve n): deprecated reading of user environment facility authpriv host.ip 127.0.0.1 messa
Mar 25, 2024 @ 23:37:44.426	@timestamp Mar 25, 2024 @ 23:37:44.426 @ve n): session opened for user user(uid=1000) facility authpriv host.ip 127.0.0.1 messa

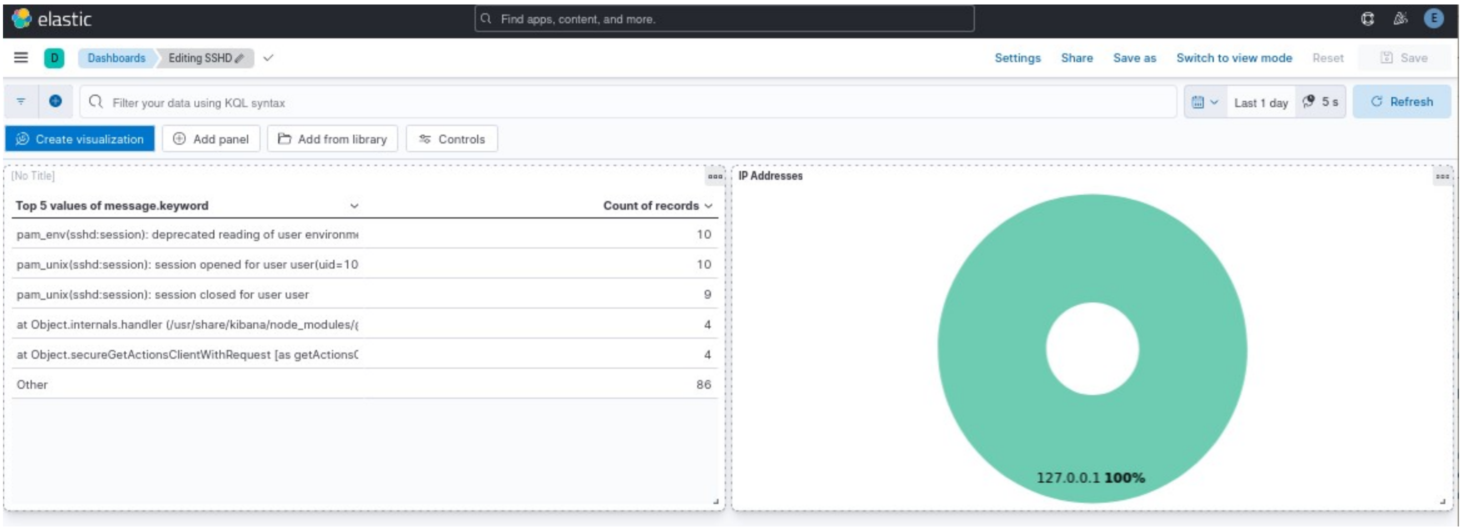
Rows per page: 100

Expanded document

View: Single document Surrounding documents 1 of 128

Actions	Field	Value
	_id	xbpXd44BjqE1VEYhNVIF
	_index	sshd-2024.03.25
	_score	-
	@timestamp	Mar 25, 2024 @ 23:39:47.581
	@version	1
	event.original	{"@timestamp":"2024-03-25T23:39:47.581386+03:00","@version":"1","message":" fatal: Timeout before authentication for 127.0.0.1 port 40184","sysloghost":"debian","severity":"crit","facility":"auth","programname":"sshd","procid":"5824"}
	facility	auth
	host.ip	127.0.0.1
	message	fatal: Timeout before authentication for 127.0.0.1 port 40184
	procid	5824
	programname	sshd
	severity	crit
	sysloghost	debian
	type	rsyslog

Rows per page: 25



Top 5 values of message.keyword	Count of records
pam_env(sshd:session): deprecated reading of user environme	10
pam_unix(sshd:session): session opened for user user(uid=10	10
pam_unix(sshd:session): session closed for user user	9
at Object.internals.handler (/usr/share/kibana/node_modules/(	4
at Object.secureGetActionsClientWithRequest [as getActions(	4
Other	86