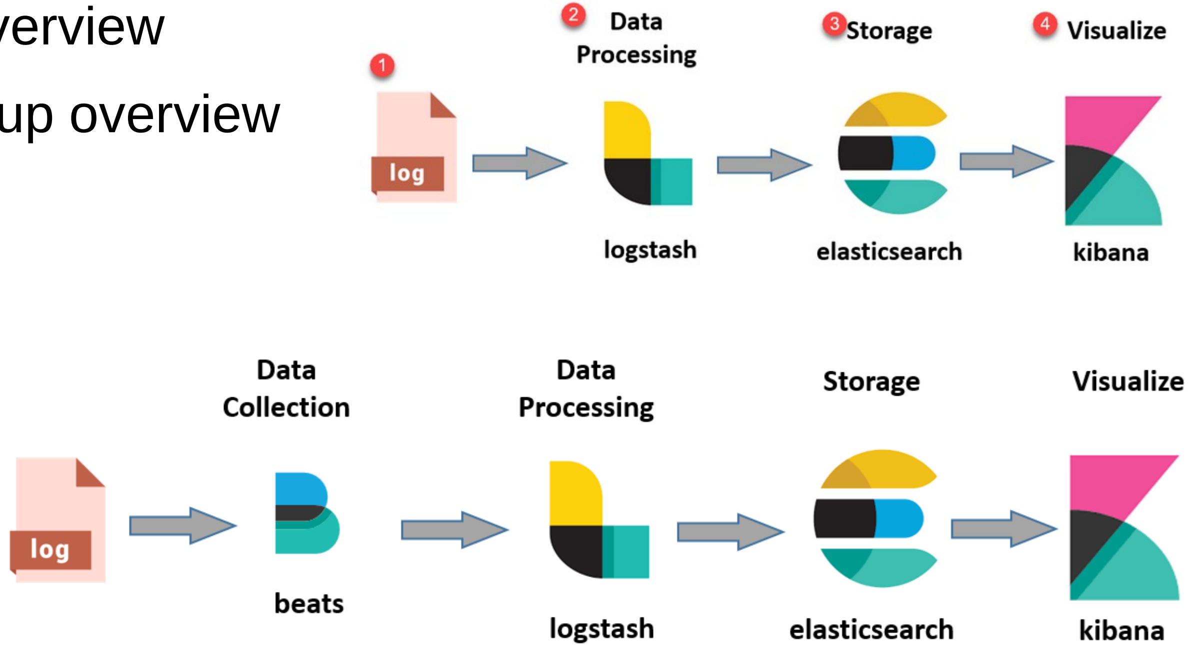
ELK

Elasticsearch
Logstash
Kibana

- Architecture overview
- Installation setup overview
- Configuration



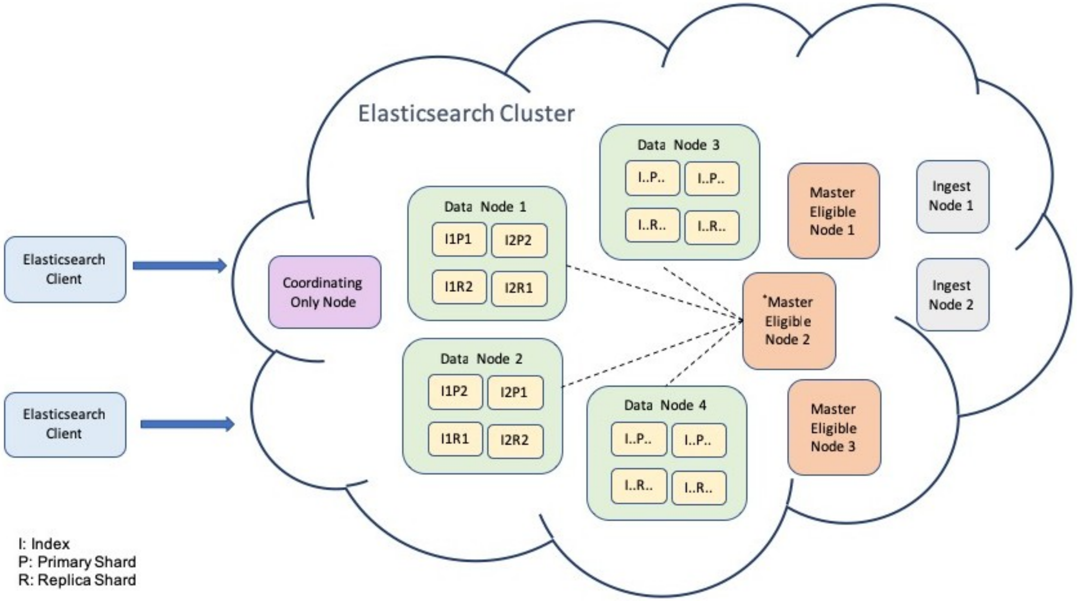
© guru99.com

Elastiscearch

- NoSQL database
  - Open source search server is written using Java
  - Schema-free, REST & JSON based distributed document store
  - Scale vertically and horizontally: sharded, replicated
- Lucene search engine
  - Full-Text Search
  - Near Real Time (NRT) search
- RESTful APIS
- Can store, search and analyze big volume of data.

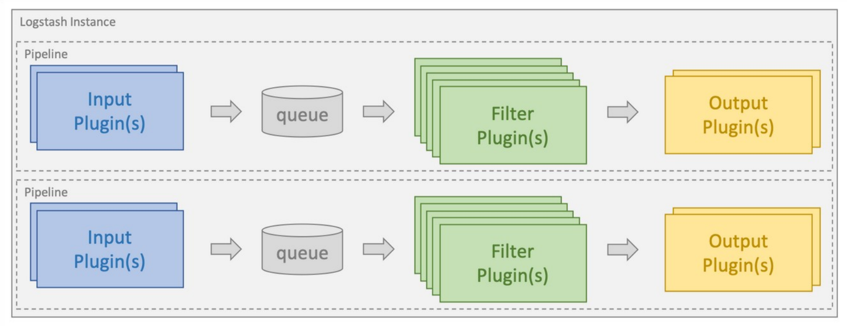
Elasticsearch terms

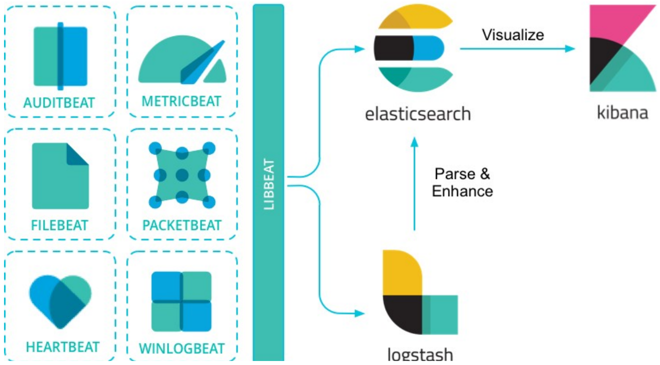
- Cluster - is a collection of nodes which together holds data and provides joined indexing and search capabilities.
- Node - is an elasticsearch Instance
- Index - is a collection of documents which has similar characteristics
- Document - is the basic unit of information which can be indexed. JSON document.
- Shard - is the atomic part of an index. The index can be split into several shards to be able to distribute data across nodes.



Logstash

- Log (event) processor
  - Written on ruby, works on java
  - Vertical scalability
  - Plugins/integrations
  - active monitoring API (ES)
- Variety log sources (input)
- Filters
  - transformation
  - enrichment
  - grok
- Variety event destinations (output)





Logstash

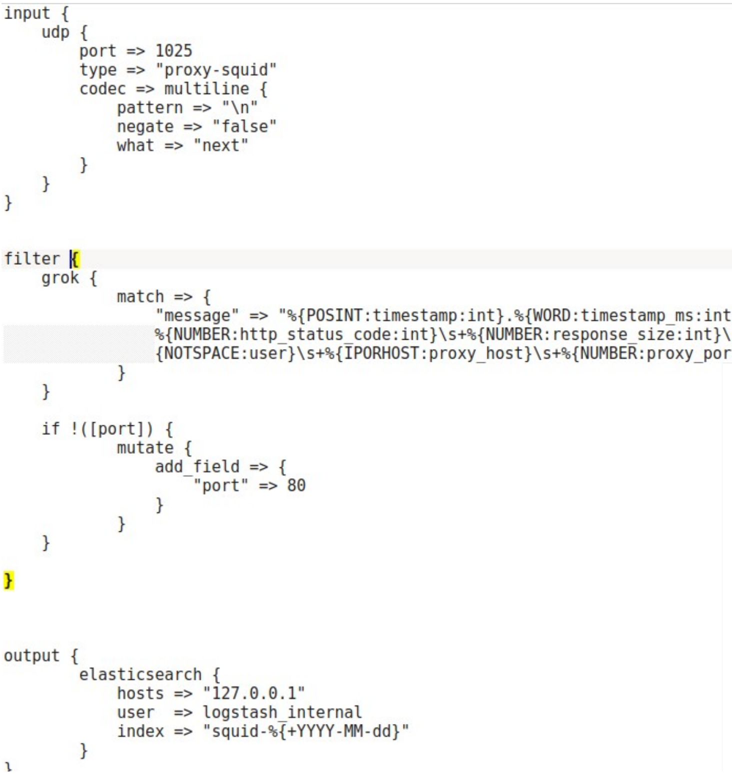
- Variety log sources:
  - Files, tcp/udp based sockets, syslog, snmptrap
  - Queues (redis, rabbitmq, kafka, etc)
  - http-based hooks
  - pool-based events, jdbc, WMI, exec
- Also Destinations

- Filters
  - Data extraction
    - grok
  - Data filtering
  - Data enrichment
  - mutate
  - aggregate

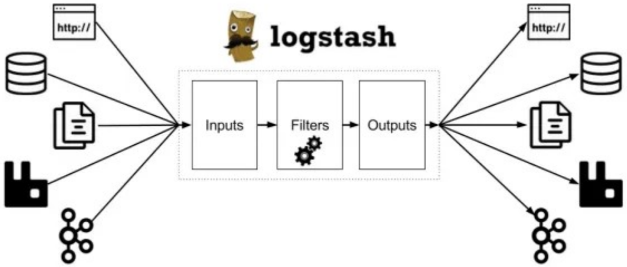
Logstash configure

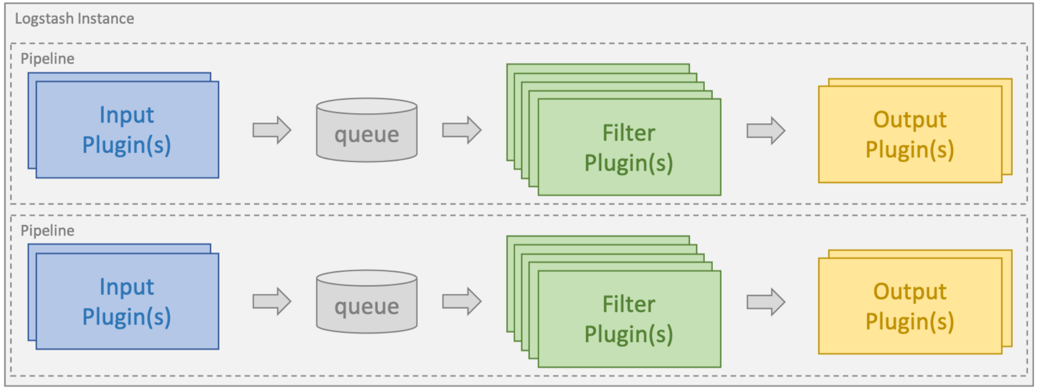
- /etc/logstash/
  - jvm.options
  - log4j2.properties
  - logstash.yml
  - pipelines.yml
  - startup.options
  - conf.d/
    - pipelines*.conf

Logstash pipeline



```
input {
    udp {
        port => 1025
        type => "proxy-squid"
        codec => multiline {
            pattern => "\n"
            negate => "false"
            what => "next"
        }
    }
}


filter {
    grok {
            match => {
                "message" => "%{POSINT:timestamp:int}.%{WORD:timestamp_ms:int}\s+%{IPORHOST
                %{NUMBER:http_status_code:int}\s+%{NUMBER:response_size:int}\s+%{NUMBER:req
                {NOTSPACE:user}\s+%{IPORHOST:proxy_host}\s+%{NUMBER:proxy_port:int}\s+%{NOT
            }
    }

    if !([port]) {
            mutate {
                add_field => {
                    "port" => 80
                }
            }
    }

}


output {
        elasticsearch {
            hosts => "127.0.0.1"
            user  => logstash_internal
            index => "squid-%{+YYYY-MM-dd}"
        }
}
```





Input plugins

https://www.elastic.co/guide/en/logstash/current/input-plugins.html

- listeining service:
  - tcp
  - udp
  - http
  - websocket
  - socket
  - snmptrap
- tracking:
  - queues
  - file
- long pooling:
  - exec
  - http_poller
  - jdbc

Filter plugins

- age
- aggregate
- alter
- bytes
- cidr
- cipher
- clone
- csv
- **date**
- de_dot
- dissect
- dns
- drop
- elapsed
- elastic_integration
- elasticsearch

- environment
- extractnumbers
- fingerprint
- geoip
- **grok**
- http
- i18n
- java_uuid
- jdbc_static
- jdbc_streaming
- json
- json_encode
- kv
- memcached
- metricize

- metrics
- **mutate**
- prune
- range
- ruby
- sleep
- split
- syslog_pri
- throttle
- tld
- translate
- truncate
- urldecode
- useragent
- uuid
- xml

- mutate
  - coerce
  - rename
  - update
  - replace
  - convert
  - gsub
  - uppercase
  - capitalize
  - lowercase
  - strip
  - split
  - join
  - merge
  - copy

Output plugins

- boundary
- circonus
- cloudwatch
- csv
- datadog
- datadog_metrics
- dynatrace
- elastic_app_search
- elastic_workplace_search
- elasticsearch
- email
- exec
- file
- ganglia
- gelf
- google_bigquery
- google_cloud_storage
- google_pubsub
- graphite
- graphtastic
- http
- influxdb
- irc
- java_stdout
- juggernaut
- kafka
- librato
- loggly
- lumberjack
- metriccatcher
- mongodb
- nagios
- nagios_nsca
- opentsdb
- pagerduty
- pipe
- rabbitmq
- redis
- redmine
- riak
- riemann
- s3
- sink
- sns
- solr_http
- sqs
- statsd
- stdout
- stomp
- syslog
- tcp
- timber
- udp
- webhdfs
- websocket
- xmpp
- Zabbix

Logstash grok

-
  ```
  2024-02-18T13:20:30.45+03:00 DEBUG This is a sample log
     TIMESTAMP                 LOG LEVEL   LOG MESSAGE
  ```

- `%{TIMESTAMP_ISO8601:timestamp} %{LOGLEVEL:log_level} %{GREEDYDATA:log_message}`

- `LOGLEVEL ([Aa]lert|ALERT|[Tt]race|TRACE|[Dd]ebug|DEBUG|[Nn]otice|NOTICE|[Ii]nfo|INFO|[Ww]arn?(?:ing)?|WARN?(?:ING)?|[Ee]rr?(?:or)?|ERR?(?:OR)?|[Cc]rit?(?:ical)?|CRIT?(?:ICAL)?|[Ff]atal|FATAL|[Ss]evere|SEVERE|EMERG(?:ENCY)?|[Ee]merg(?:ency)?)`

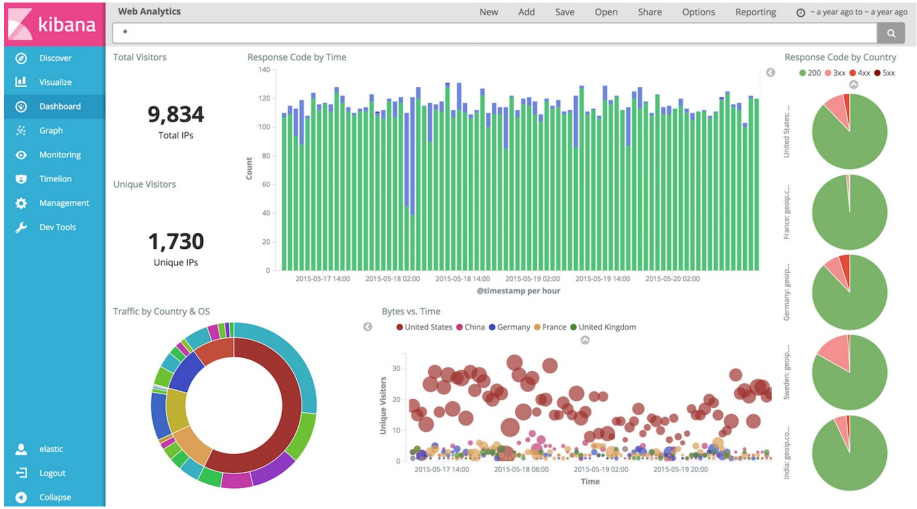
- `TIMESTAMP_ISO8601 %{YEAR}-%{MONTHNUM}-%{MONTHDAY}[T ]%{HOUR}:?%{MINUTE}(?::?%{SECOND})?%{ISO8601_TIMEZONE}?`

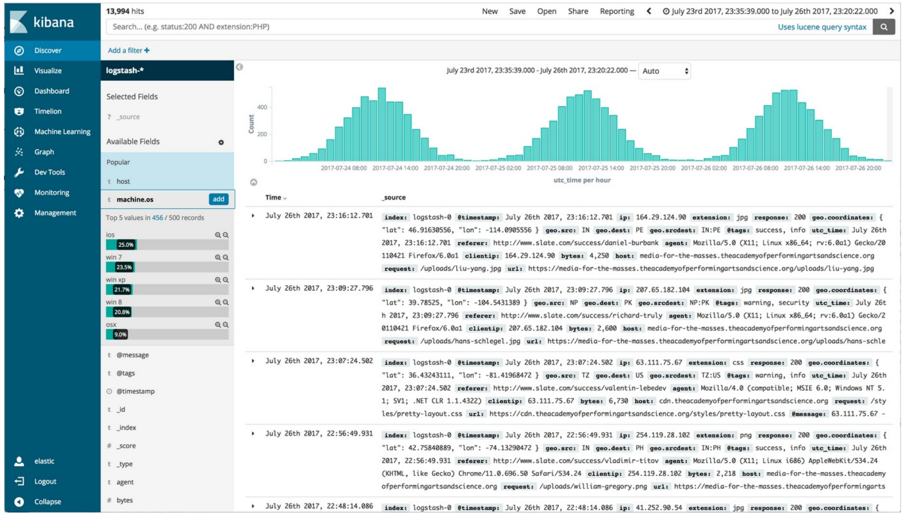
  ```
  YEAR (?>\d\d){1,2}
  MONTHNUM (?:0?[1-9]|1[0-2])
  MONTHDAY (?:(?:0[1-9])|(?:[12][0-9])|(?:3[01])|[1-9])
  HOUR (?:2[0123]|[01]?[0-9])
  MINUTE (?:[0-5][0-9])
  SECOND (?:(?:[0-5]?[0-9]|60)(?:[:.,][0-9]+)?)
  ```

- `GREEDYDATA .*`

- https://github.com/hpcugent/logstash-patterns/blob/master/files/grok-patterns

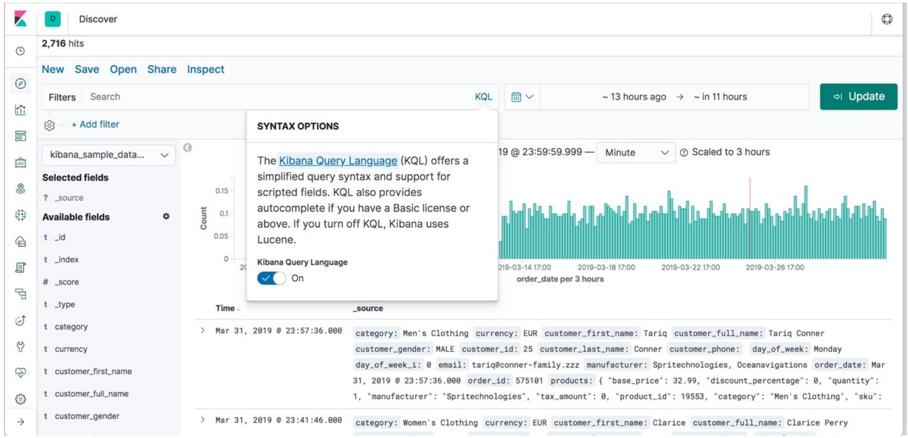
Kibana version 5 and 6





```
July 26th 2017, 23:16:12.701   index: logstash-0 @timestamp: July 26th 2017, 23:16:12.701 ip: 164.29.124.90 extension: jpg response: 200 geo.coordinates: {
                               "lat": 46.91630556, "lon": -114.0905556 } geo.src: IN geo.dest: PE geo.srcdest: IN:PE @tags: success, info utc_time: July 26th
                               2017, 23:16:12.701 referer: http://www.slate.com/success/daniel-burbank agent: Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20
                               110421 Firefox/6.0a1 clientip: 164.29.124.90 bytes: 4,250 host: media-for-the-masses.theacademyofperformingartsandscience.org
                               request: /uploads/liu-yang.jpg url: https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/liu-yang.jpg
July 26th 2017, 23:09:27.796   index: logstash-0 @timestamp: July 26th 2017, 23:09:27.796 ip: 207.65.182.104 extension: jpg response: 200 geo.coordinates: {
                               "lat": 39.78525, "lon": -104.5431389 } geo.src: NP geo.dest: PK geo.srcdest: NP:PK @tags: warning, security utc_time: July 26t
                               h 2017, 23:09:27.796 referer: http://www.slate.com/success/richard-truly agent: Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/2
                               0110421 Firefox/6.0a1 clientip: 207.65.182.104 bytes: 2,600 host: media-for-the-masses.theacademyofperformingartsandscience.org
                               request: /uploads/hans-schlegel.jpg url: https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/hans-schle
July 26th 2017, 23:07:24.502   index: logstash-0 @timestamp: July 26th 2017, 23:07:24.502 ip: 63.111.75.67 extension: css response: 200 geo.coordinates: {
                               "lat": 36.43243111, "lon": -81.41968472 } geo.src: TZ geo.dest: US geo.srcdest: TZ:US @tags: warning, info utc_time: July 26th
                               2017, 23:07:24.502 referer: http://www.slate.com/success/valentin-lebedev agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.
                               1; SV1; .NET CLR 1.1.4322) clientip: 63.111.75.67 bytes: 6,730 host: cdn.theacademyofperformingartsandscience.org request: /sty
                               les/pretty-layout.css url: https://cdn.theacademyofperformingartsandscience.org/styles/pretty-layout.css @message: 63.111.75.67 -
July 26th 2017, 22:56:49.931   index: logstash-0 @timestamp: July 26th 2017, 22:56:49.931 ip: 254.119.28.102 extension: png response: 200 geo.coordinates: {
                               "lat": 42.75840889, "lon": -74.13290472 } geo.src: IN geo.dest: PH geo.srcdest: IN:PH @tags: success, info utc_time: July 26th
                               2017, 22:56:49.931 referer: http://www.slate.com/success/vladimir-titov agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24
                               (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 clientip: 254.119.28.102 bytes: 2,218 host: media-for-the-masses.theacademy
                               ofperformingartsandscience.org request: /uploads/william-gregory.png url: https://media-for-the-masses.theacademyofperformingarts
July 26th 2017, 22:48:14.086   index: logstash-0 @timestamp: July 26th 2017, 22:48:14.086 ip: 41.252.90.54 extension: jpg response: 200 geo.coordinates: {
```

Kibana 7



SYNTAX OPTIONS

The Kibana Query Language (KQL) offers a simplified query syntax and support for scripted fields. KQL also provides autocomplete if you have a Basic license or above. If you turn off KQL, Kibana uses Lucene.

Kibana Query Language: On

```
> Mar 31, 2019 @ 23:57:36.000   category: Men's Clothing currency: EUR customer_first_name: Tariq customer_full_name: Tariq Conner
                                customer_gender: MALE customer_id: 25 customer_last_name: Conner customer_phone:  day_of_week: Monday
                                day_of_week_i: 0 email: tariq@conner-family.zzz manufacturer: Spritechnologies, Oceanavigations order_date: Mar
                                31, 2019 @ 23:57:36.000 order_id: 575101 products: { "base_price": 32.99, "discount_percentage": 0, "quantity":
                                1, "manufacturer": "Spritechnologies", "tax_amount": 0, "product_id": 19553, "category": "Men's Clothing", "sku":
> Mar 31, 2019 @ 23:41:46.000   category: Women's Clothing currency: EUR customer_first_name: Clarice customer_full_name: Clarice Perry
```