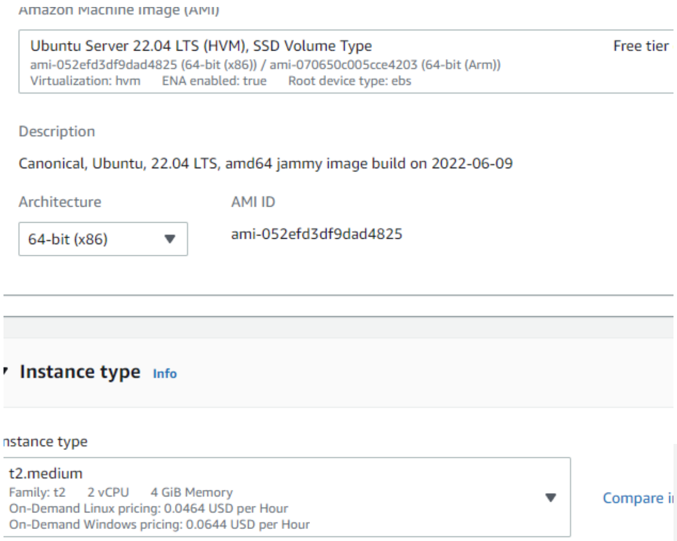
CODING
DOJO

DevOps -2022-b-online

BY

MOHAMMED EID 😊

First create EC2 instance



Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier
ami-052efd3df9dad4825 (64-bit (x86)) / ami-070650c005cce4203 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2022-06-09

Architecture: 64-bit (x86)

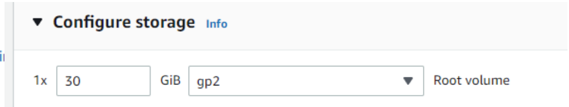
AMI ID: ami-052efd3df9dad4825

Instance type Info

nstance type

t2.medium
Family: t2 2 vCPU 4 GiB Memory
On-Demand Linux pricing: 0.0464 USD per Hour
On-Demand Windows pricing: 0.0644 USD per Hour

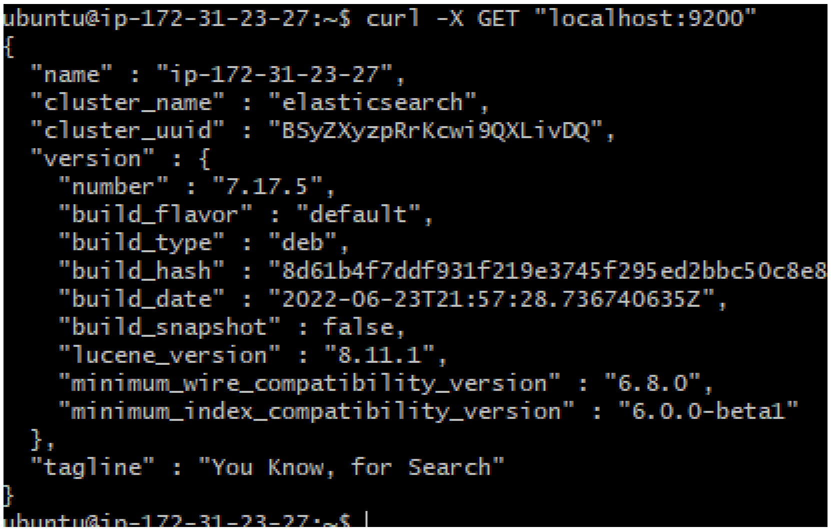
Compare i



Configure storage Info

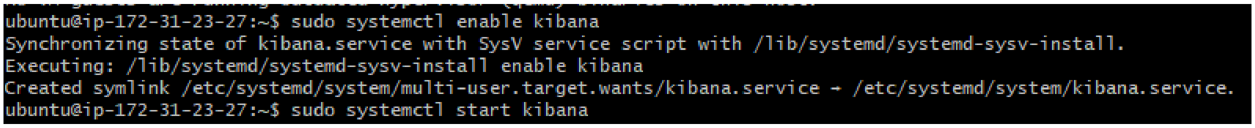
1x 30 GiB gp2 Root volume

Install Elastic Search

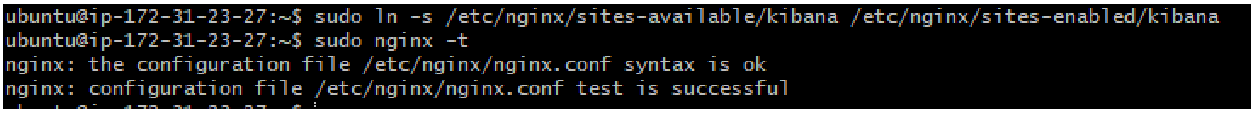


```
ubuntu@ip-172-31-23-27:~$ curl -X GET "localhost:9200"
{
  "name" : "ip-172-31-23-27",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "BSyZXyzpRrKcwi9QXLivDQ",
  "version" : {
    "number" : "7.17.5",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "8d61b4f7ddf931f219e3745f295ed2bbc50c8e8
    "build_date" : "2022-06-23T21:57:28.736740635Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
ubuntu@ip-172-31-23-27:~$
```

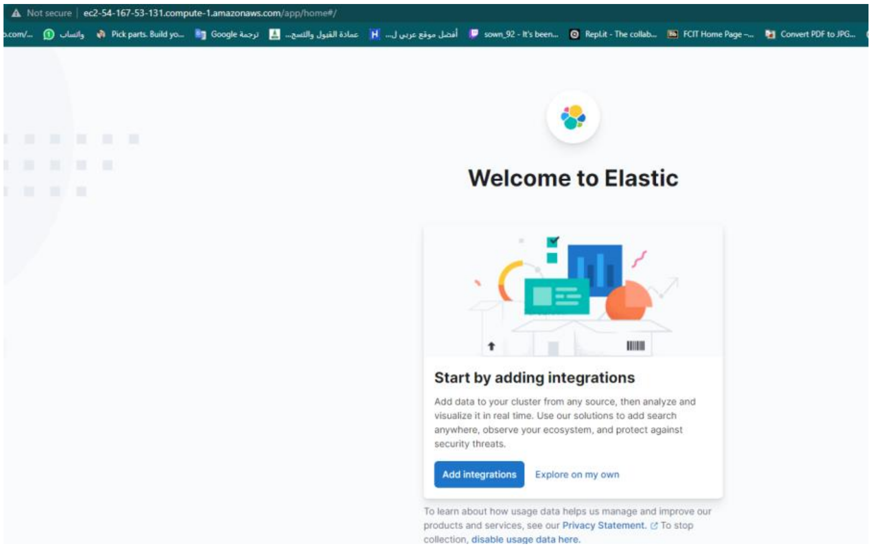
Install and setup Kibana



```
ubuntu@ip-172-31-23-27:~$ sudo systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
ubuntu@ip-172-31-23-27:~$ sudo systemctl start kibana
```



```
ubuntu@ip-172-31-23-27:~$ sudo ln -s /etc/nginx/sites-available/kibana /etc/nginx/sites-enabled/kibana
ubuntu@ip-172-31-23-27:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```



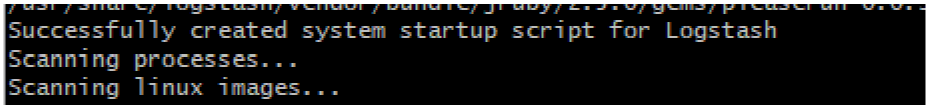
Welcome to Elastic

Start by adding integrations

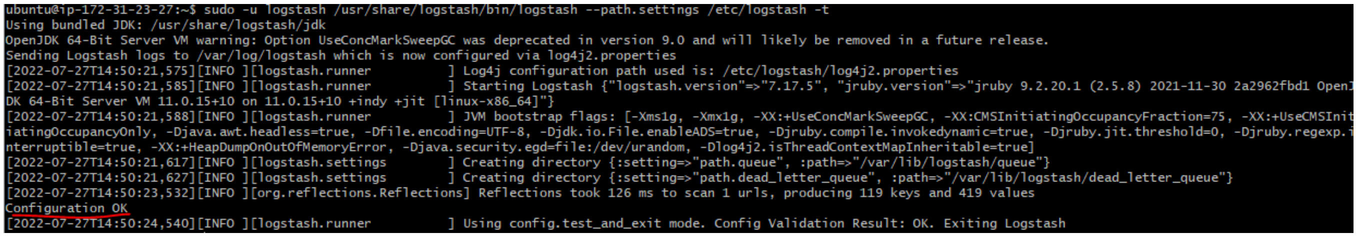
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Install and setup Logstash

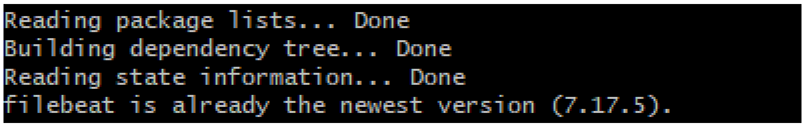


```
Successfully created system startup script for Logstash
Scanning processes...
Scanning linux images...
```

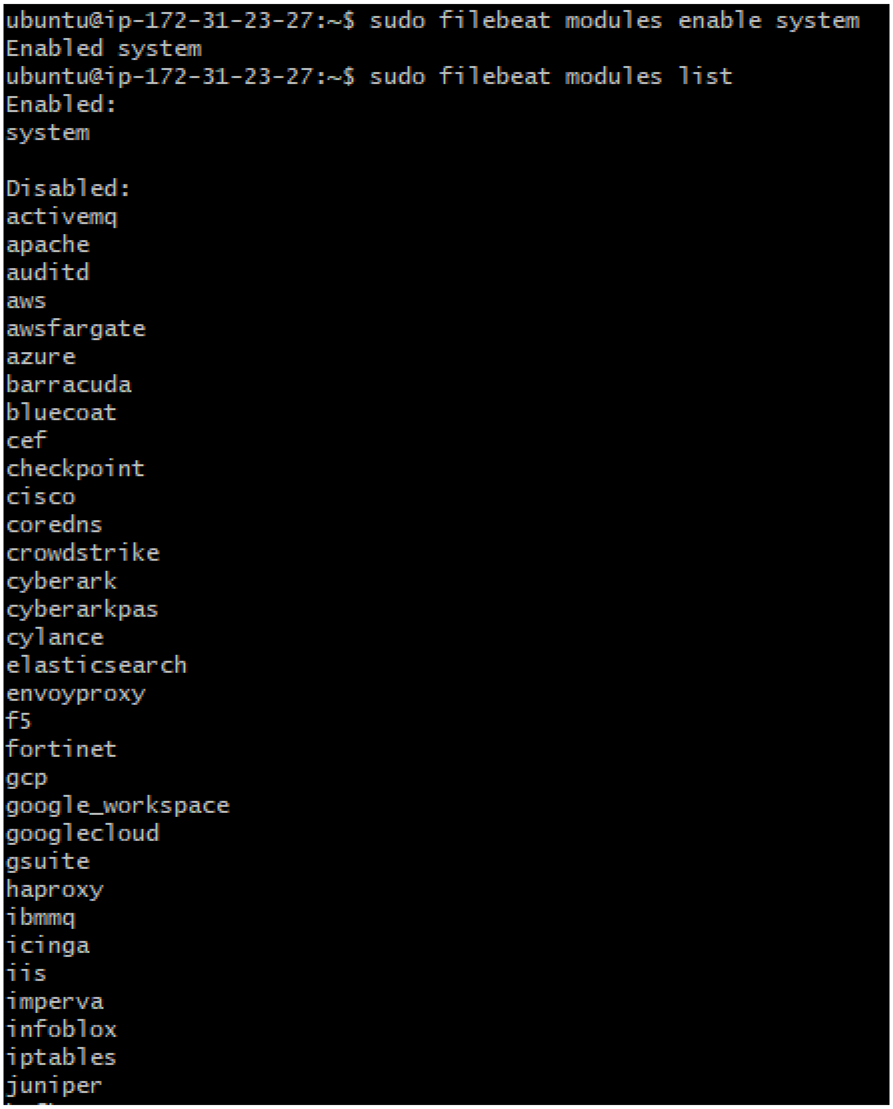


```
ubuntu@ip-172-31-23-27:~$ sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
[2022-07-27T14:50:21,575][INFO ][logstash.runner          ] Log4j configuration path used is: /etc/logstash/log4j2.properties
[2022-07-27T14:50:21,585][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"7.17.5", "jruby.version"=>"jruby 9.2.20.1 (2.5.8) 2021-11-30 2a2962fbd1 OpenJ
DK 64-Bit Server VM 11.0.15+10 on 11.0.15+10 +indy +jit [linux-x86_64]"}
[2022-07-27T14:50:21,588][INFO ][logstash.runner          ] JVM bootstrap flags: [-Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX:+UseCMSInit
iatingOccupancyOnly, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djdk.io.File.enableADS=true, -Djruby.compile.invokedynamic=true, -Djruby.jit.threshold=0, -Djruby.regexp.i
nterruptible=true, -XX:+HeapDumpOnOutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapInheritable=true]
[2022-07-27T14:50:21,617][INFO ][logstash.settings        ] Creating directory {:setting=>"path.queue", :path=>"/var/lib/logstash/queue"}
[2022-07-27T14:50:21,627][INFO ][logstash.settings        ] Creating directory {:setting=>"path.dead_letter_queue", :path=>"/var/lib/logstash/dead_letter_queue"}
[2022-07-27T14:50:23,532][INFO ][org.reflections.Reflections] Reflections took 126 ms to scan 1 urls, producing 119 keys and 419 values
Configuration OK
[2022-07-27T14:50:24,540][INFO ][logstash.runner          ] Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
```

Install beat (To transfer data from various sources to logstash)



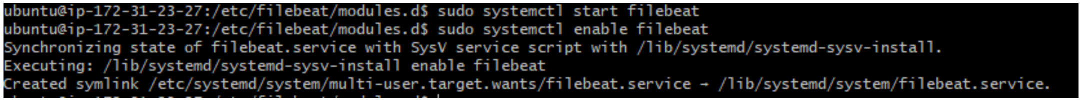
```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
filebeat is already the newest version (7.17.5).
```



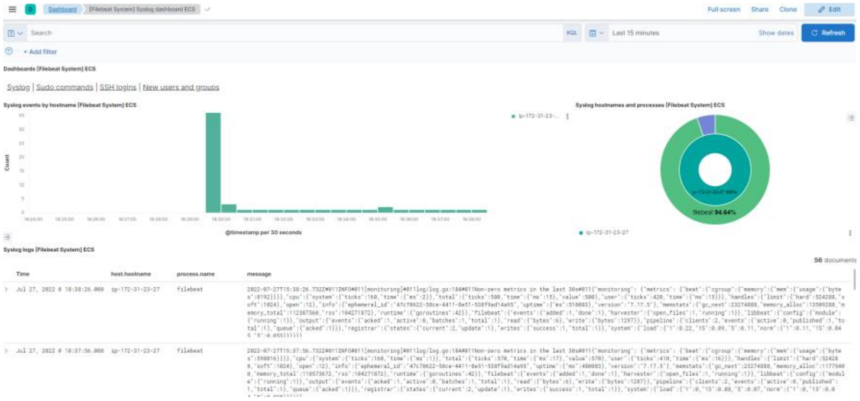
```
ubuntu@ip-172-31-23-27:~$ sudo filebeat modules enable system
Enabled system
ubuntu@ip-172-31-23-27:~$ sudo filebeat modules list
Enabled:
system

Disabled:
activemq
apache
auditd
aws
awsfargate
azure
barracuda
bluecoat
cef
checkpoint
cisco
coredns
crowdstrike
cyberark
cyberarkpas
cylance
elasticsearch
envoyproxy
f5
fortinet
gcp
google_workspace
googlecloud
gsuite
haproxy
ibmmq
icinga
iis
imperva
infoblox
iptables
juniper
```

..etc

Setup filebeat pipelines



```
ubuntu@ip-172-31-23-27:/etc/filebeat/modules.d$ sudo systemctl start filebeat
ubuntu@ip-172-31-23-27:/etc/filebeat/modules.d$ sudo systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
```



Dashboard
[Filebeat System] Syslog dashboard ECS
Full screen
Share
Clone
Edit
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
Syslog events by hostname [Filebeat System] ECS
Count
@timestamp per 30 seconds
Syslog hostnames and processes [Filebeat System] ECS
filebeat 94.64%
ip-172-31-23-27

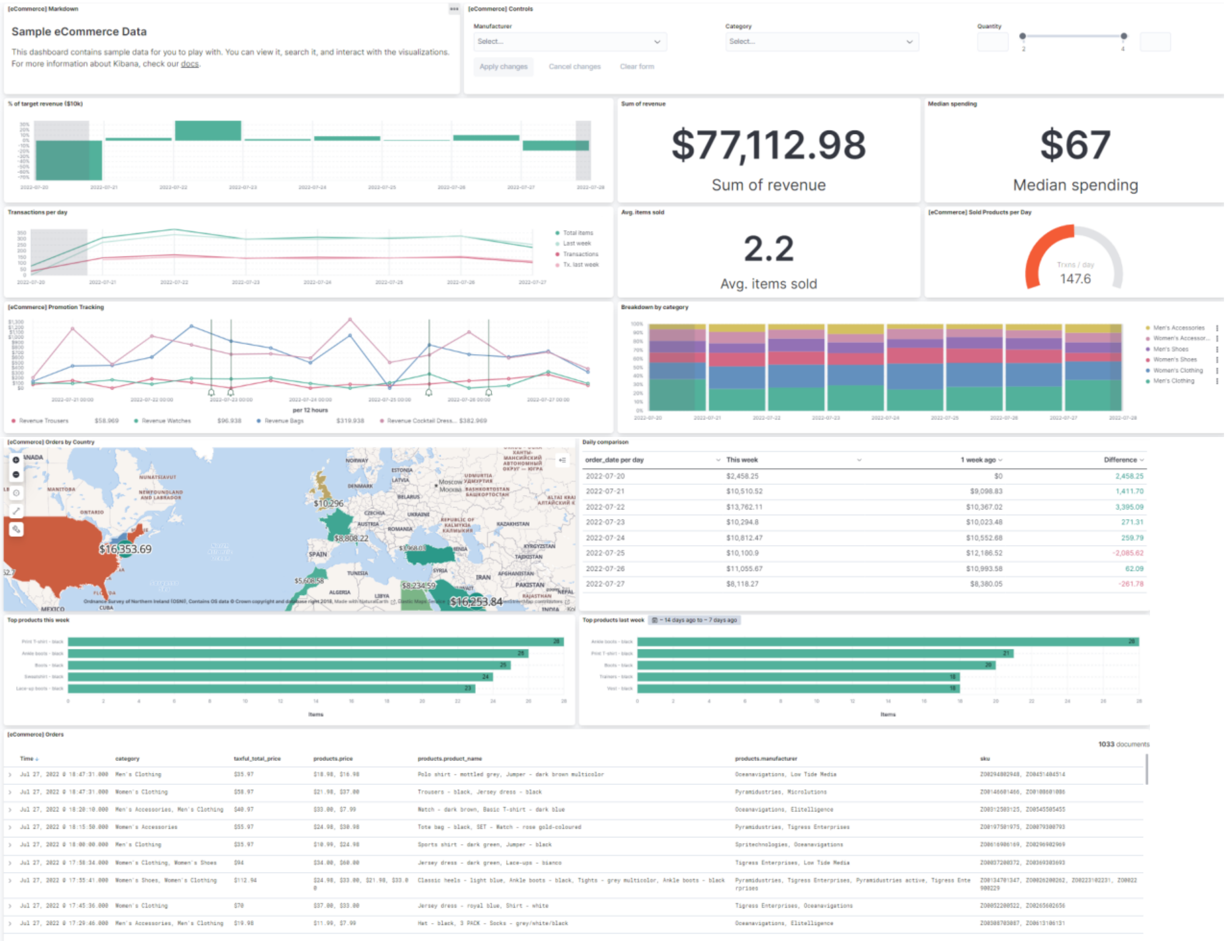
Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

Syslog logs [Filebeat System] ECS

56 documents

Time	host.hostname	process.name	message
Jul 27, 2022 @ 18:38:26.000	ip-172-31-23-27	filebeat	2022-07-27T15:38:26.732Z#011INFO#011[monitoring]#011log/log.go:184#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":8192}}}},"cpu":{"system":{"ticks":160,"time":{"ms":2}},"total":{"ticks":580,"time":{"ms":15},"value":580},"user":{"ticks":420,"time":{"ms":13}}},"handles":{"limit":{"hard":524288,"soft":1024},"open":12},"info":{"ephemeral_id":"47c70622-58ce-4411-8e51-538f9ad14a95","uptime":{"ms":510083}},"version":"7.17.5"},"memstats":{"gc_next":23274888,"memory_alloc":13509288,"memory_total":112387560,"rss":104271872},"runtime":{"goroutines":42}},"filebeat":{"events":{"added":1,"done":1},"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":1}},"output":{"events":{"acked":1,"active":0,"batches":1,"total":1},"read":{"bytes":6},"write":{"bytes":1297}},"pipeline":{"clients":2,"events":{"active":0,"published":1,"total":1},"queue":{"acked":1}}},"registrar":{"states":{"current":2,"update":1},"writes":{"success":1,"total":1}},"system":{"load":{"1":0.22,"15":0.09,"5":0.11,"norm":{"1":0.11,"15":0.045,"5":0.055}}}}}}
Jul 27, 2022 @ 18:37:56.000	ip-172-31-23-27	filebeat	2022-07-27T15:37:56.732Z#011INFO#011[monitoring]#011log/log.go:184#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cgroup":{"memory":{"mem":{"usage":{"bytes":598016}}}},"cpu":{"system":{"ticks":160,"time":{"ms":1}},"total":{"ticks":570,"time":{"ms":17},"value":570},"user":{"ticks":410,"time":{"ms":16}}},"handles":{"limit":{"hard":524288,"soft":1024},"open":12},"info":{"ephemeral_id":"47c70622-58ce-4411-8e51-538f9ad14a95","uptime":{"ms":480083}},"version":"7.17.5"},"memstats":{"gc_next":23274888,"memory_alloc":11775400,"memory_total":110573672,"rss":104271872},"runtime":{"goroutines":42}},"filebeat":{"events":{"added":1,"done":1},"harvester":{"open_files":1,"running":1}},"libbeat":{"config":{"module":{"running":1}},"output":{"events":{"acked":1,"active":0,"batches":1,"total":1},"read":{"bytes":6},"write":{"bytes":1287}},"pipeline":{"clients":2,"events":{"active":0,"published":1,"total":1},"queue":{"acked":1}}},"registrar":{"states":{"current":2,"update":1},"writes":{"success":1,"total":1}},"system":{"load":{"1":0,"15":0.08,"5":0.07,"norm":{"1":0,"15":0.04,"5":0.035}}}}}}



Sample eCommerce Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

Sum of revenue: **$77,112.98**

Median spending: **$67**

Avg. items sold: **2.2**

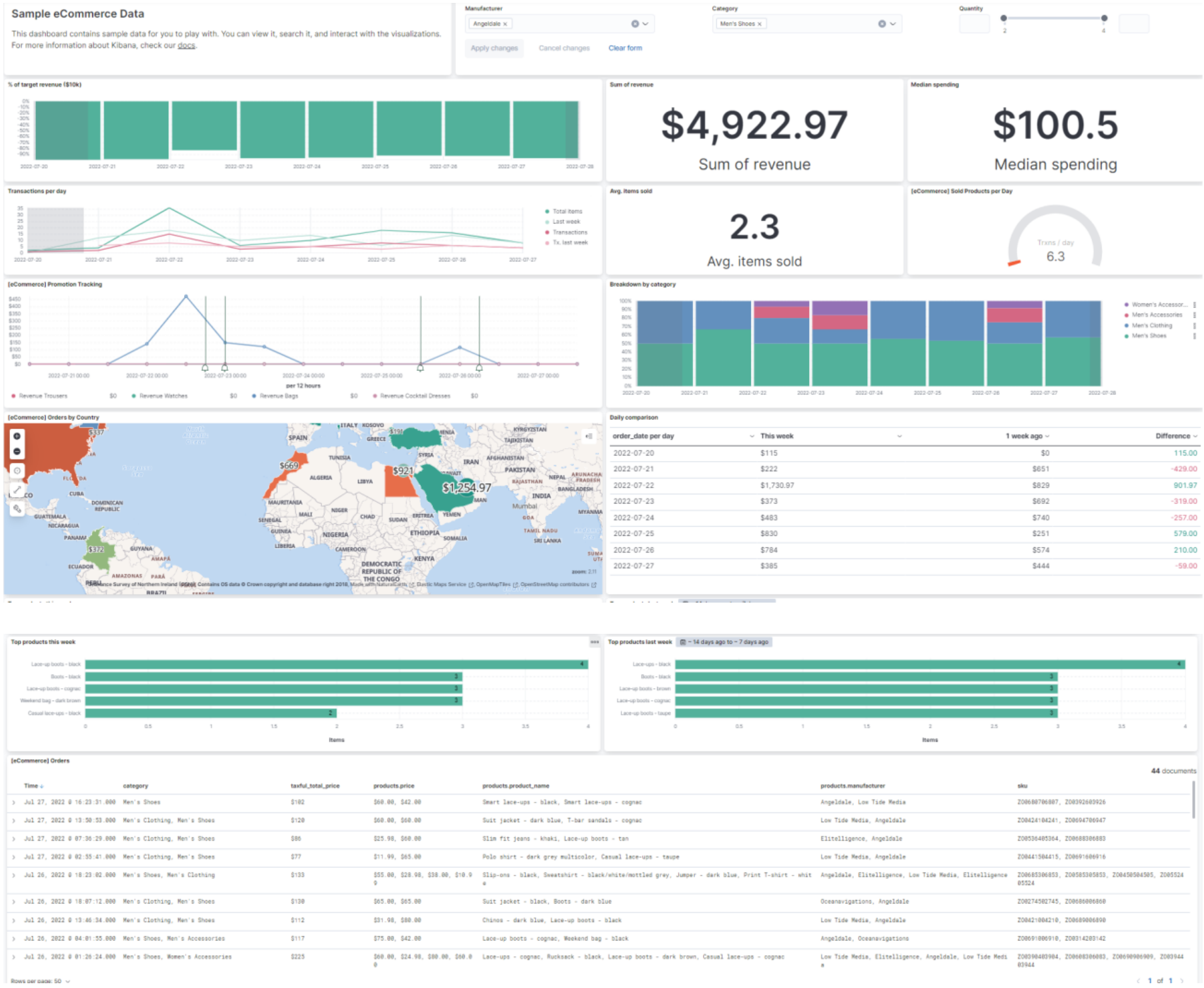
Daily comparison

order_date per day	This week	1 week ago	Difference
2022-07-20	$2,458.25	$0	2,458.25
2022-07-21	$10,510.52	$9,098.83	1,411.70
2022-07-22	$13,762.11	$10,367.02	3,395.09
2022-07-23	$10,294.8	$10,023.48	271.31
2022-07-24	$10,812.47	$10,552.68	259.79
2022-07-25	$10,100.9	$12,186.52	-2,085.62
2022-07-26	$11,055.67	$10,993.58	62.09
2022-07-27	$8,118.27	$8,380.05	-261.78

[eCommerce] Orders

1033 documents

Time	category	taxful_total_price	products.price	products.product_name	products.manufacturer	sku
Jul 27, 2022 @ 18:47:31.000	Men's Clothing	$35.97	$18.98, $16.98	Polo shirt - mottled grey, Jumper - dark brown multicolor	Oceanavigations, Low Tide Media	ZO0294802948, ZO0451404514
Jul 27, 2022 @ 18:47:31.000	Women's Clothing	$58.97	$21.98, $37.00	Trousers - black, Jersey dress - black	Pyramidustries, Microlutions	ZO0146601466, ZO0108601086
Jul 27, 2022 @ 18:20:10.000	Men's Accessories, Men's Clothing	$40.97	$33.00, $7.99	Watch - dark brown, Basic T-shirt - dark blue	Oceanavigations, Elitelligence	ZO0312503125, ZO0545505455
Jul 27, 2022 @ 18:15:50.000	Women's Accessories	$55.97	$24.98, $30.98	Tote bag - black, SET - Watch - rose gold-coloured	Pyramidustries, Tigress Enterprises	ZO0197501975, ZO0079300793
Jul 27, 2022 @ 18:00:00.000	Men's Clothing	$35.97	$10.99, $24.98	Sports shirt - dark green, Jumper - black	Spritechnologies, Oceanavigations	ZO0616906169, ZO0296902969
Jul 27, 2022 @ 17:58:34.000	Women's Clothing, Women's Shoes	$94	$34.00, $60.00	Jersey dress - dark green, Lace-ups - bianco	Tigress Enterprises, Low Tide Media	ZO0037200372, ZO0369303693
Jul 27, 2022 @ 17:55:41.000	Women's Shoes, Women's Clothing	$112.94	$24.98, $33.00, $21.98, $33.00	Classic heels - light blue, Ankle boots - black, Tights - grey multicolor, Ankle boots - black	Pyramidustries, Tigress Enterprises, Pyramidustries active, Tigress Enterprises	ZO0134701347, ZO0026200262, ZO0223102231, ZO0022900229
Jul 27, 2022 @ 17:45:36.000	Women's Clothing	$70	$37.00, $33.00	Jersey dress - royal blue, Shirt - white	Tigress Enterprises, Oceanavigations	ZO0052200522, ZO0265602656
Jul 27, 2022 @ 17:29:46.000	Men's Accessories, Men's Clothing	$19.98	$11.99, $7.99	Hat - black, 3 PACK - Socks - grey/white/black	Oceanavigations, Elitelligence	ZO0308703087, ZO0613106131



Sample eCommerce Data

This dashboard contains sample data for you to play with. You can view it, search it, and interact with the visualizations. For more information about Kibana, check our docs.

Sum of revenue

$4,922.97

Sum of revenue

Median spending

$100.5

Median spending

2.3

Avg. items sold

Daily comparison

order_date per day	This week	1 week ago	Difference
2022-07-20	$115	$0	115.00
2022-07-21	$222	$651	-429.00
2022-07-22	$1,730.97	$829	901.97
2022-07-23	$373	$692	-319.00
2022-07-24	$483	$740	-257.00
2022-07-25	$830	$251	579.00
2022-07-26	$784	$574	210.00
2022-07-27	$385	$444	-59.00

[eCommerce] Orders

44 documents

Time	category	taxful_total_price	products.price	products.product_name	products.manufacturer	sku
Jul 27, 2022 @ 16:23:31.000	Men's Shoes	$102	$60.00, $42.00	Smart lace-ups - black, Smart lace-ups - cognac	Angeldale, Low Tide Media	ZO0680706807, ZO0392603926
Jul 27, 2022 @ 13:50:53.000	Men's Clothing, Men's Shoes	$120	$60.00, $60.00	Suit jacket - dark blue, T-bar sandals - cognac	Low Tide Media, Angeldale	ZO0424104241, ZO0694706947
Jul 27, 2022 @ 07:36:29.000	Men's Clothing, Men's Shoes	$86	$25.98, $60.00	Slim fit jeans - khaki, Lace-up boots - tan	Elitelligence, Angeldale	ZO0536405364, ZO0688306883
Jul 27, 2022 @ 02:55:41.000	Men's Clothing, Men's Shoes	$77	$11.99, $65.00	Polo shirt - dark grey multicolor, Casual lace-ups - taupe	Low Tide Media, Angeldale	ZO0441504415, ZO0691606916
Jul 26, 2022 @ 18:23:02.000	Men's Shoes, Men's Clothing	$133	$55.00, $28.98, $38.00, $10.99	Slip-ons - black, Sweatshirt - black/white/mottled grey, Jumper - dark blue, Print T-shirt - white	Angeldale, Elitelligence, Low Tide Media, Elitelligence	ZO0685306853, ZO0585305853, ZO0450504505, ZO0552405524
Jul 26, 2022 @ 18:07:12.000	Men's Clothing, Men's Shoes	$130	$65.00, $65.00	Suit jacket - black, Boots - dark blue	Oceanavigations, Angeldale	ZO0274502745, ZO0686006860
Jul 26, 2022 @ 13:46:34.000	Men's Clothing, Men's Shoes	$112	$31.98, $80.00	Chinos - dark blue, Lace-up boots - black	Low Tide Media, Angeldale	ZO0421004210, ZO0689006890
Jul 26, 2022 @ 04:01:55.000	Men's Shoes, Men's Accessories	$117	$75.00, $42.00	Lace-up boots - cognac, Weekend bag - black	Angeldale, Oceanavigations	ZO0691006910, ZO0314203142
Jul 26, 2022 @ 01:26:24.000	Men's Shoes, Women's Accessories	$225	$60.00, $24.98, $80.00, $60.00	Lace-ups - cognac, Rucksack - black, Lace-up boots - dark brown, Casual lace-ups - cognac	Low Tide Media, Elitelligence, Angeldale, Low Tide Media	ZO0390403904, ZO0608306083, ZO0690906909, ZO0394403944

Rows per page: 50

1 of 1