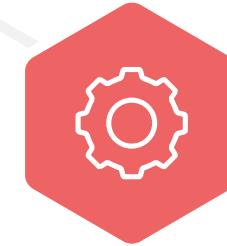


SCK-Automation Work 2021

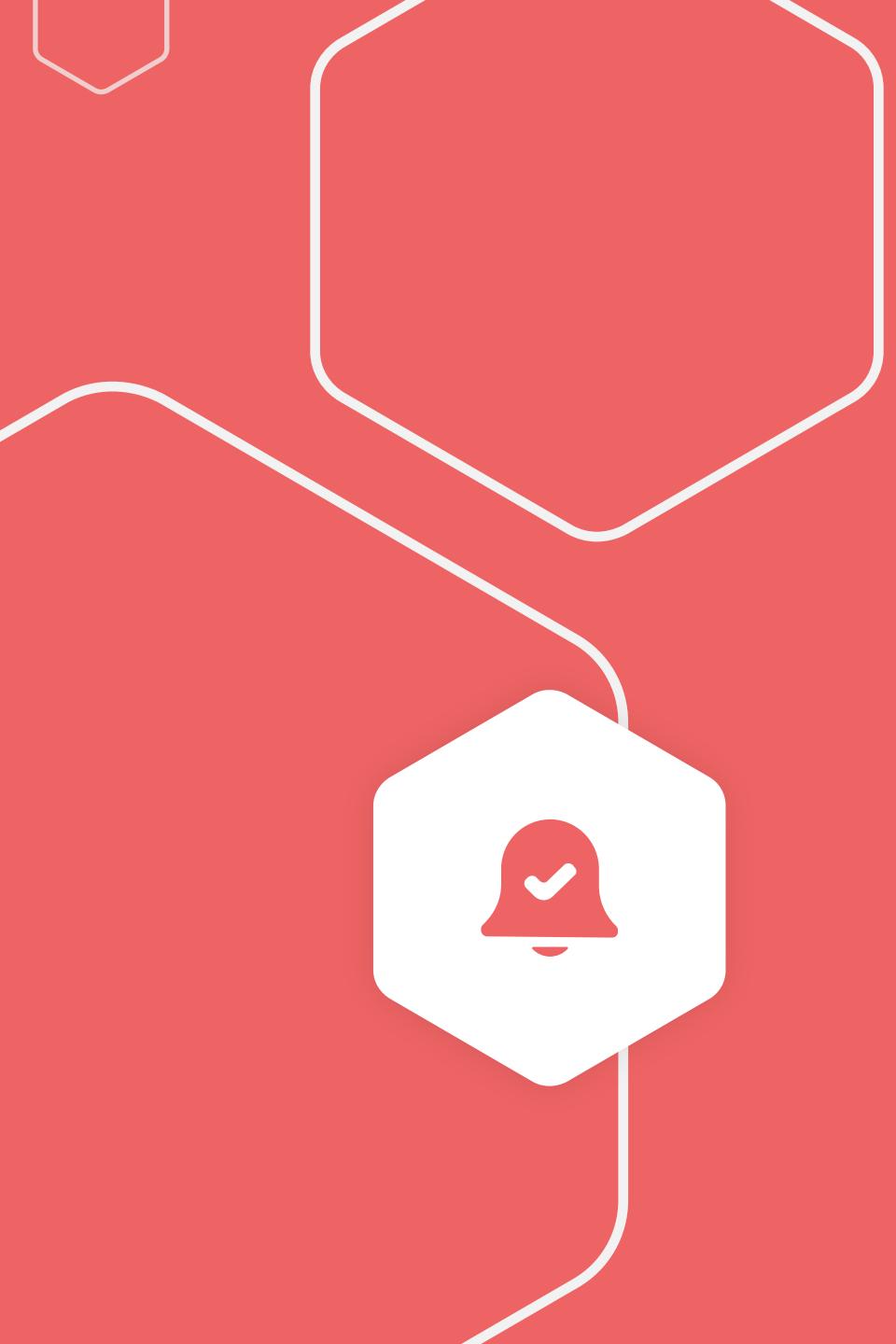
Kibana Dashboard

Explore, Visualize, Discover **DATA**



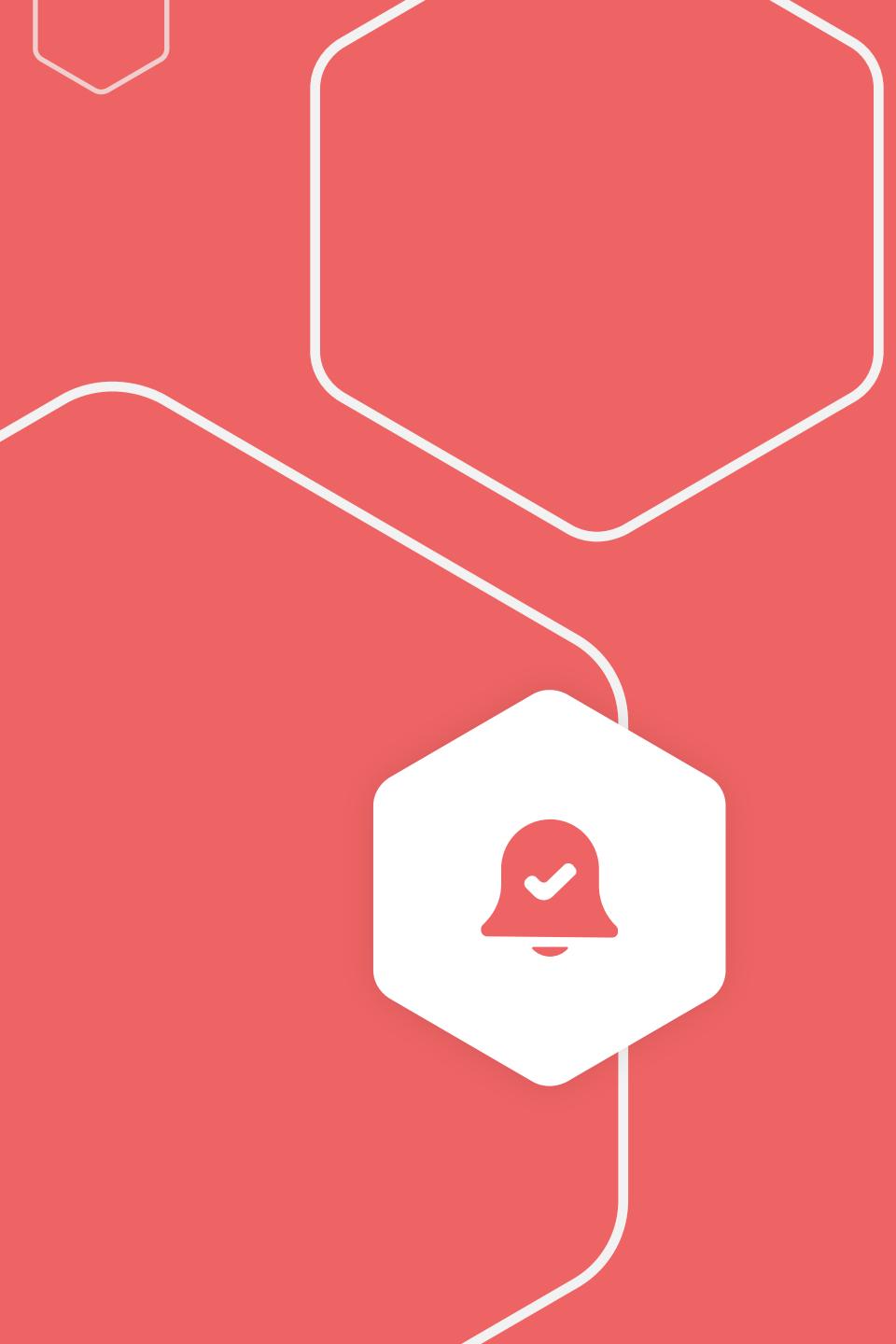
Last updated: Wednesday, October 20, 2021





1st Day Agenda

- Dashboard
- ELK Stack Overviews
- Install Kibana
- Explore the Data
- Simple Dashboard

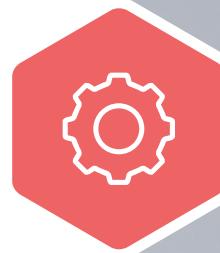


2nd Day Agenda

- Import Data
- Complex Dashboard
- Design your Own Dashboard
 - Source of Data
 - Special Features

Dashboard Overview

Dashboard that drive **insight and action**



Why we need it. ?

1. You feel like your company can improve, but you have no idea how to or where to start.
2. You're monitoring and tracking data, but you don't know what to do with the information or how to make sense of it.
3. Your current solutions aren't giving you the ROI you need.
4. You are lagging behind your competitors.
5. You're struggling to see all of your data from multiple sources in one location.



Visualization



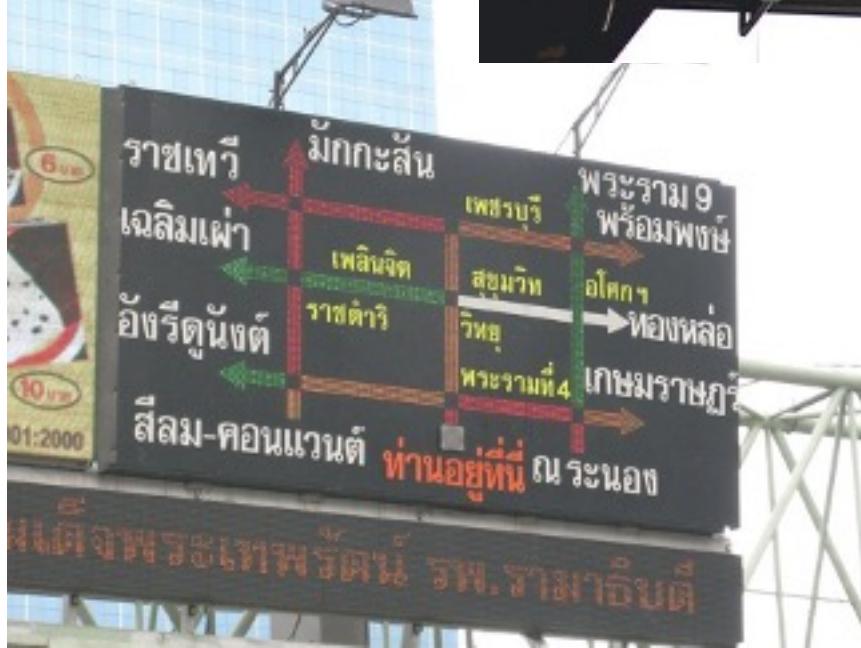
<http://searchuserinterfaces.com/book/images/wordle.png>

Visual & Visualization

- Visual : เกี่ยวกับการมองเห็น, ใช้ในการมอง, เกี่ยวกับสายตา
- Visualize : ทำให้มองเห็น, ทำให้จินตนาการเห็น, นิ่งภาพในใจ
- Visualization : การทำให้เห็นได้, การสร้างมโนภาพ



Example of Visualization



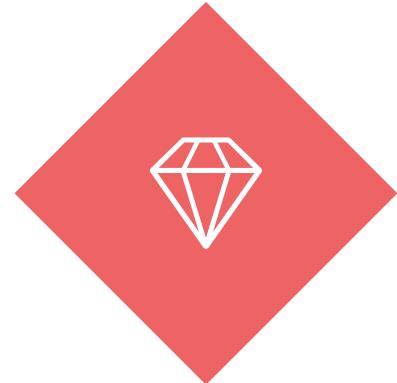
Visualize ?



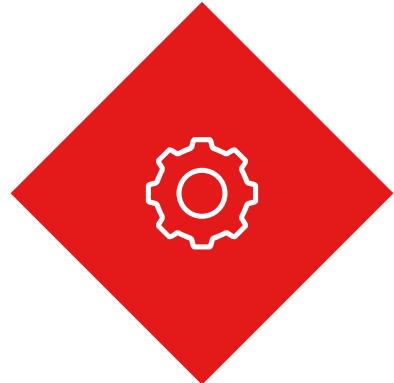
Shopping-Cart : Define Business Process Workflow



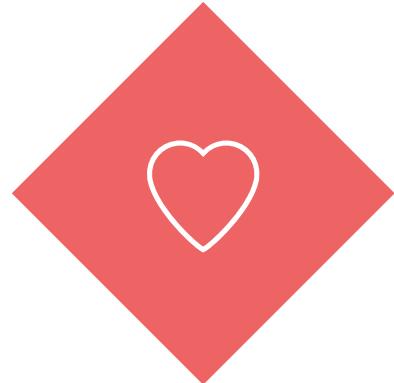
Type of Dashboard ?



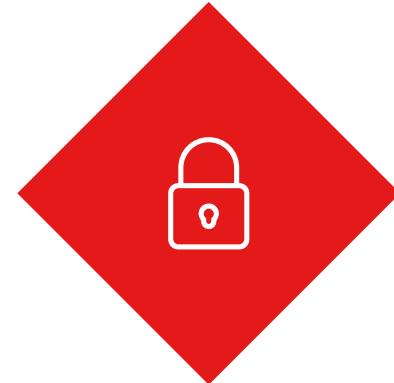
Strategic Dashboard
focused on long-term strategies
and high-level metrics



Operational Dashboard
shows shorter time frames and
operational processes.



Analytical Dashboard
contains vast amounts of data
created by analysts.



Tactical Dashboard
used by mid-management to track
performance.



What Is A Strategic Dashboard?

A **strategic dashboard** is a reporting tool for monitoring the long-term company strategy with the help of critical success factors. They're usually complex in their creation, provide an enterprise-wide impact to a business, and are mainly used by senior-level management.

Revenue and Customer Overview - Q1 2016



Management strategic



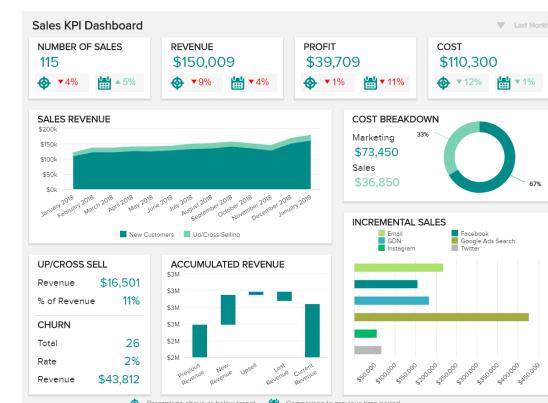
CMO strategic



SaaS management



CFO dashboard for strategic planning



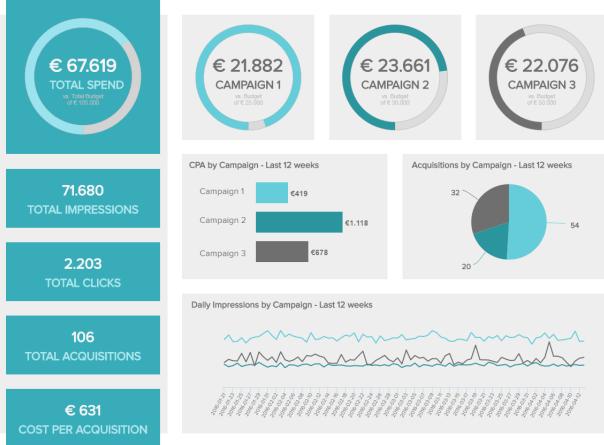
Sales KPI dashboard

© 2013 - 2020 Siam Chamnankit Company Limited



What Is A Operational Dashboard?

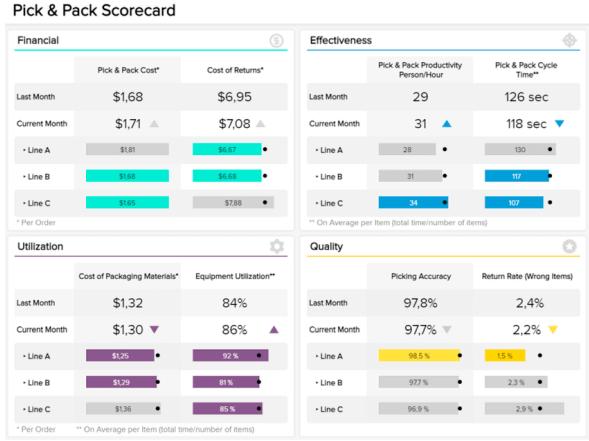
An **operational dashboard** is one of the types of dashboards used for monitoring and managing operations that have a shorter time horizon. Since they focus on tracking operational processes, they're usually administrated by junior levels of management.



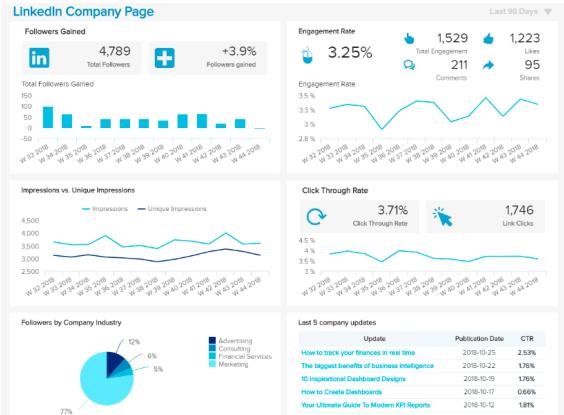
Marketing operational dashboard



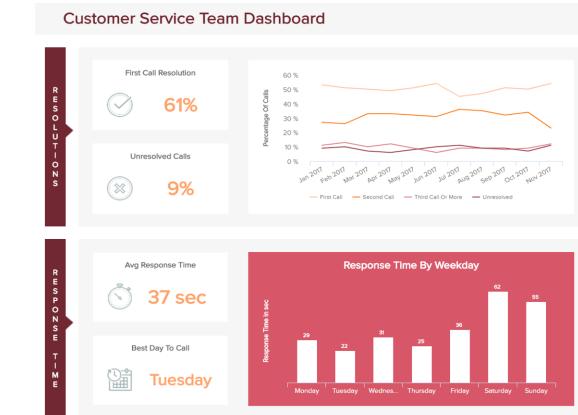
Manufacturing Production dashboard



Pick and pack operational dashboard for logistics



LinkedIn operations dashboard example

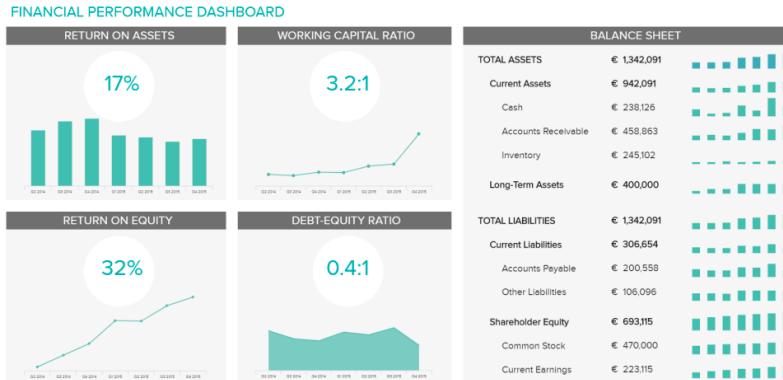


Customer service operational metrics dashboard

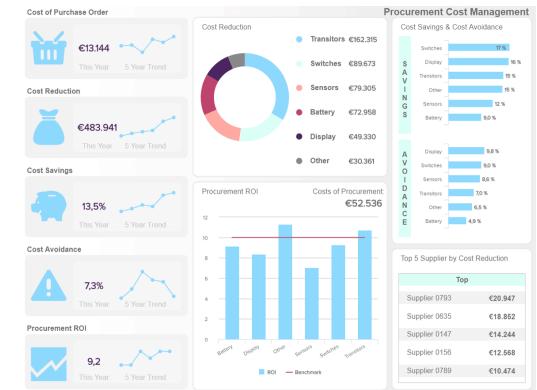


What Is An Analytical Dashboard?

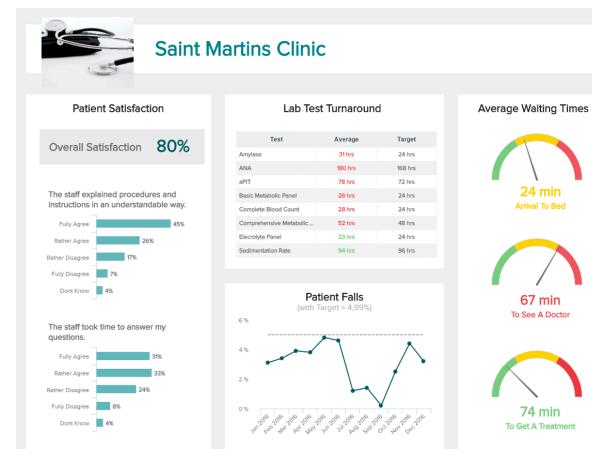
An **analytical dashboard** is a type of dashboard that contains a vast amount of data created and used by analysts to provide support to executives. They supply a business with a comprehensive overview of data, with middle management being a crucial part of its usage.



Financial performance dashboard



Procurement cost dashboard



Healthcare analytical dashboard for patients

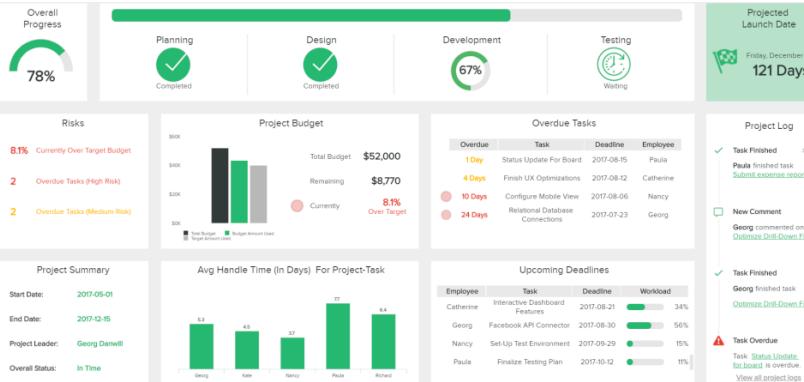


What Is A Tactical Dashboard?

A **tactical dashboard** is utilized in the analysis and monitoring of processes conducted by mid-level management, emphasizing the analysis. Then an organization effectively tracks the performance of a company's goal and delivers analytic recommendations for future strategies.



Energy Management tactical dashboard



IT project management dashboard



Human Resources talent management dashboard

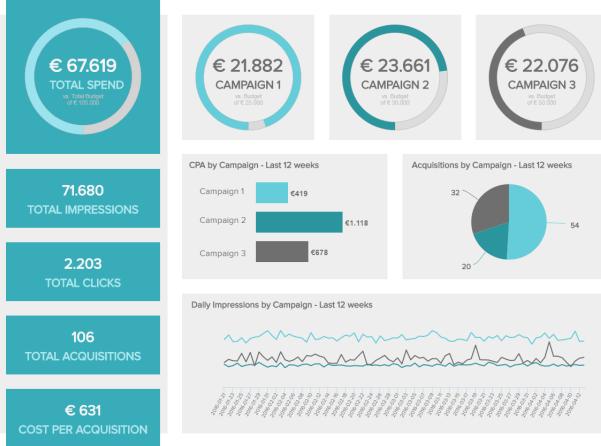


Social media dashboard



What Is A Operational Dashboard?

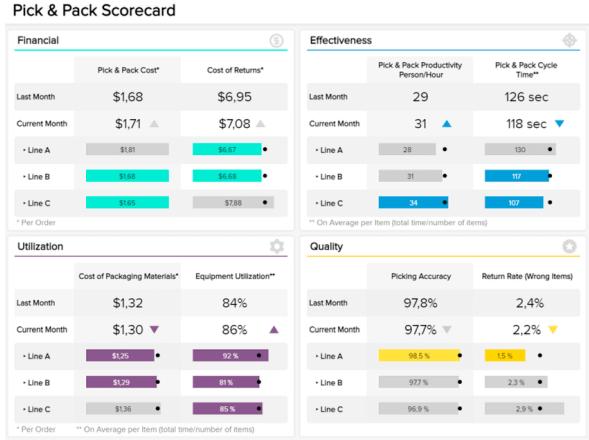
An **operational dashboard** is one of the types of dashboards used for monitoring and managing operations that have a shorter time horizon. Since they focus on tracking operational processes, they're usually administrated by junior levels of management.



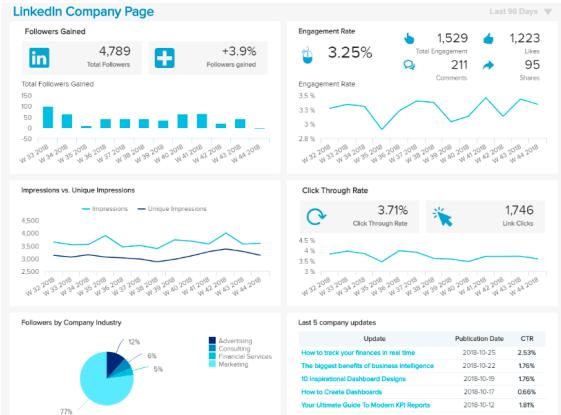
Marketing operational dashboard



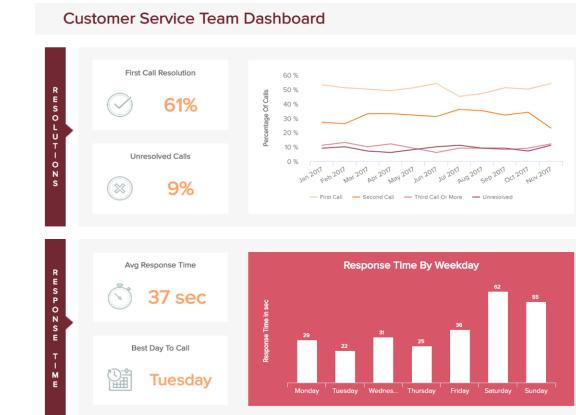
Manufacturing Production dashboard



Pick and pack operational dashboard for logistics



LinkedIn operations dashboard example



Customer service operational metrics dashboard



Type of Dashboard ?

TYPE OF DASHBOARD	LEVEL OF SENIORITY	TIME APPLICATION	LEVEL OF COMPLEXITY
STRATEGIC	Senior Management	Long-term	Complex
TACTICAL & ANALYTICAL	Middle Management	Medium-term	Less Complex
OPERATIONAL	Junior Management	Routine	Simple



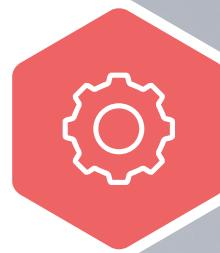


Which one ?

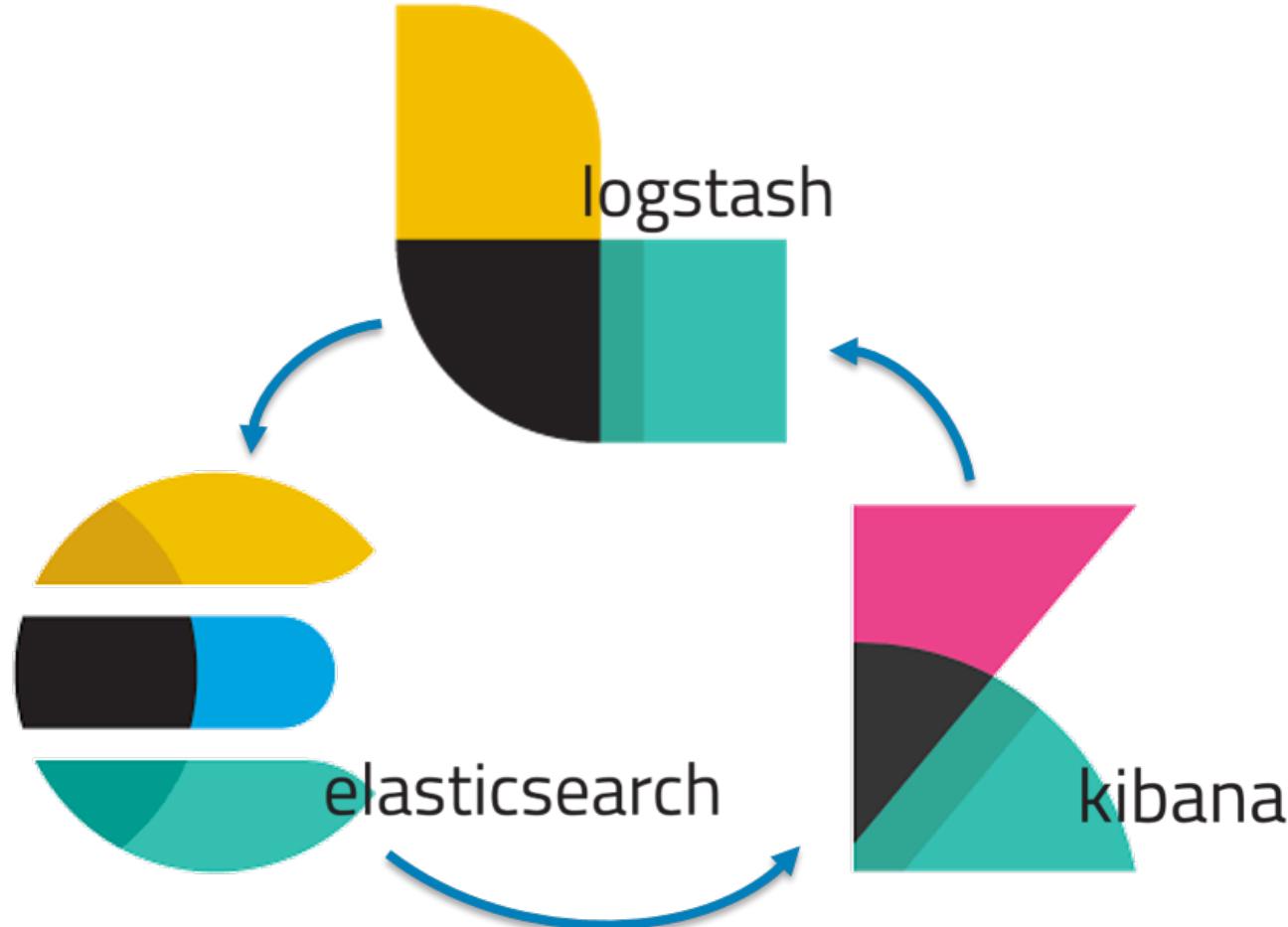


ELK Overview

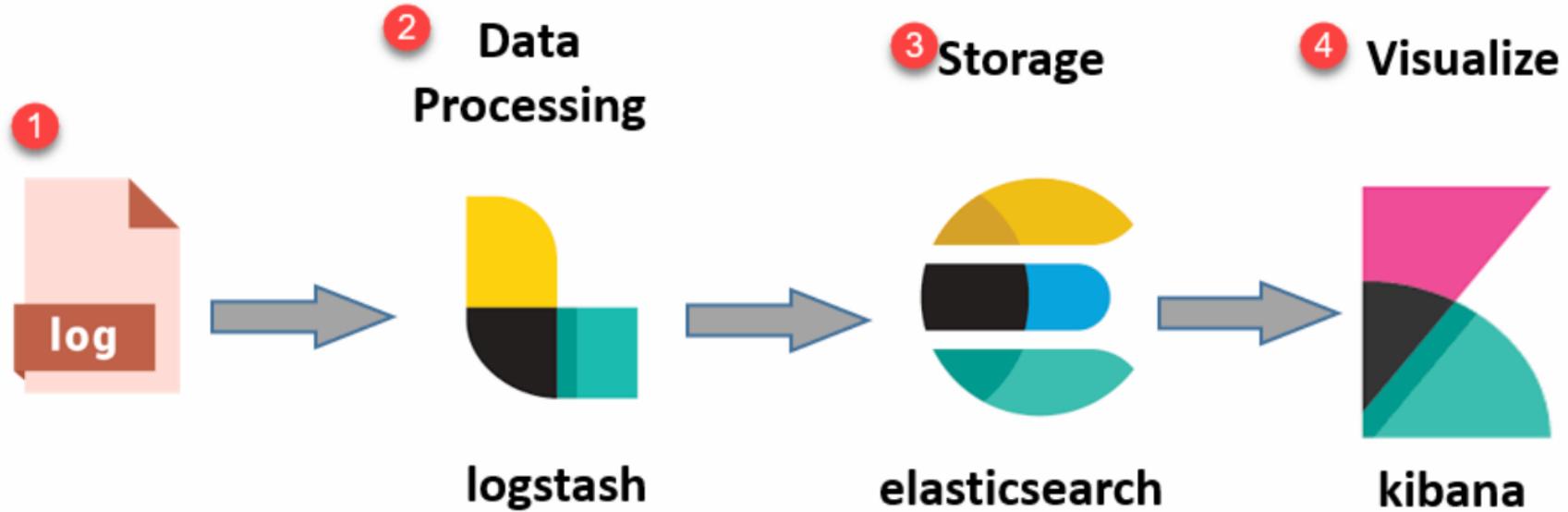
Elasticsearch Logstash and Kibana



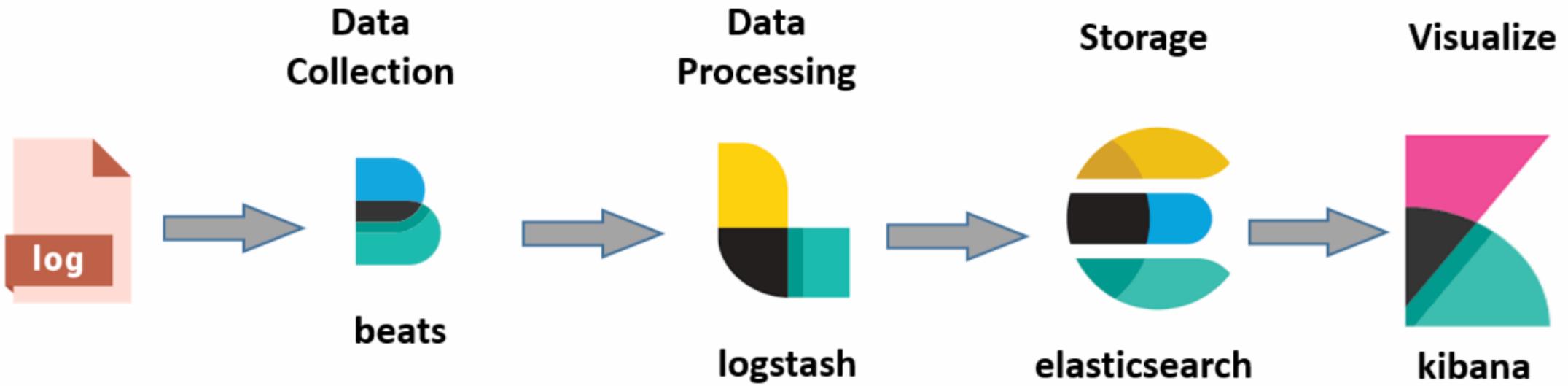
ELK Stack: Elasticsearch, Logstash and Kibana



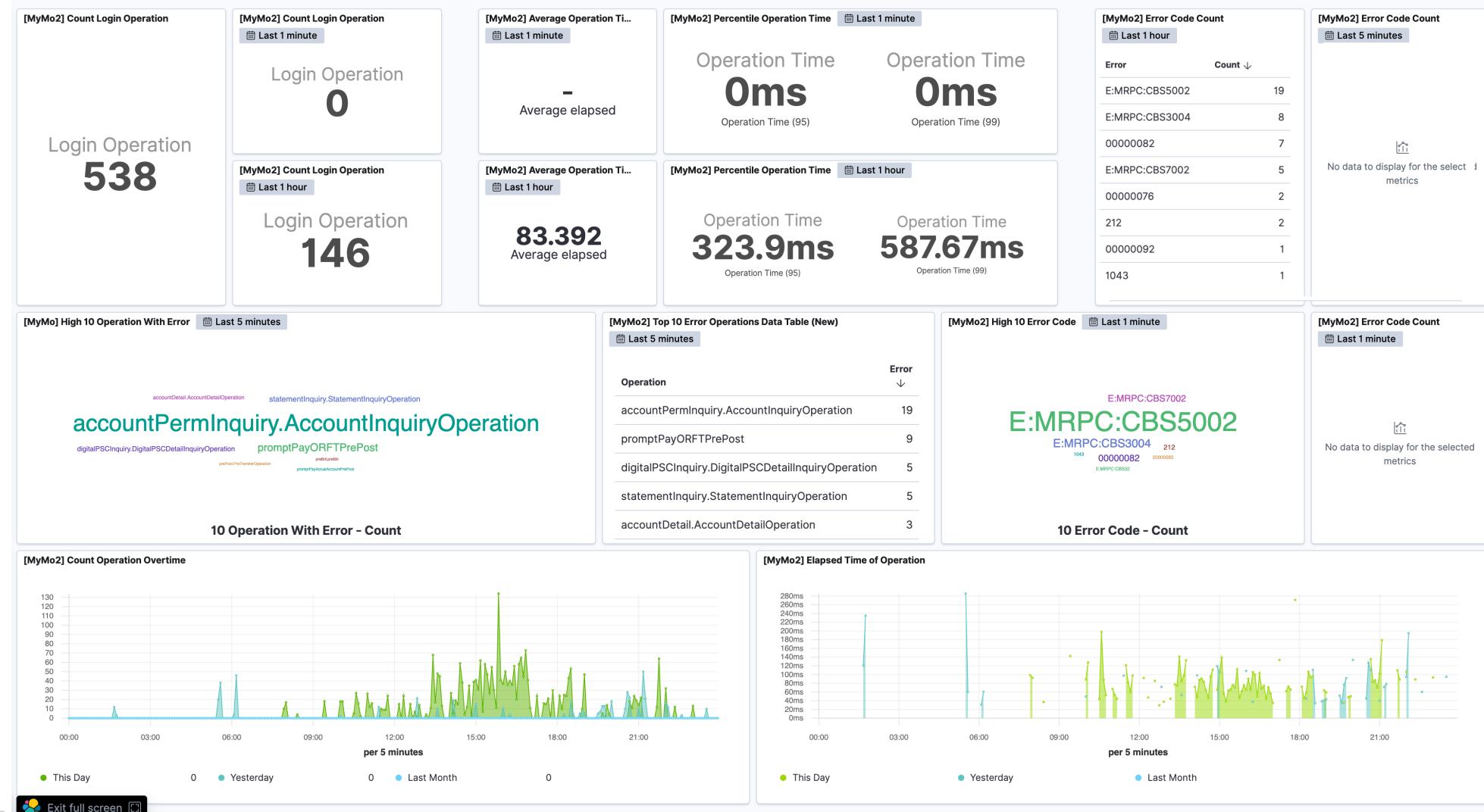
Shopping-Cart : Define Business Process Workflow



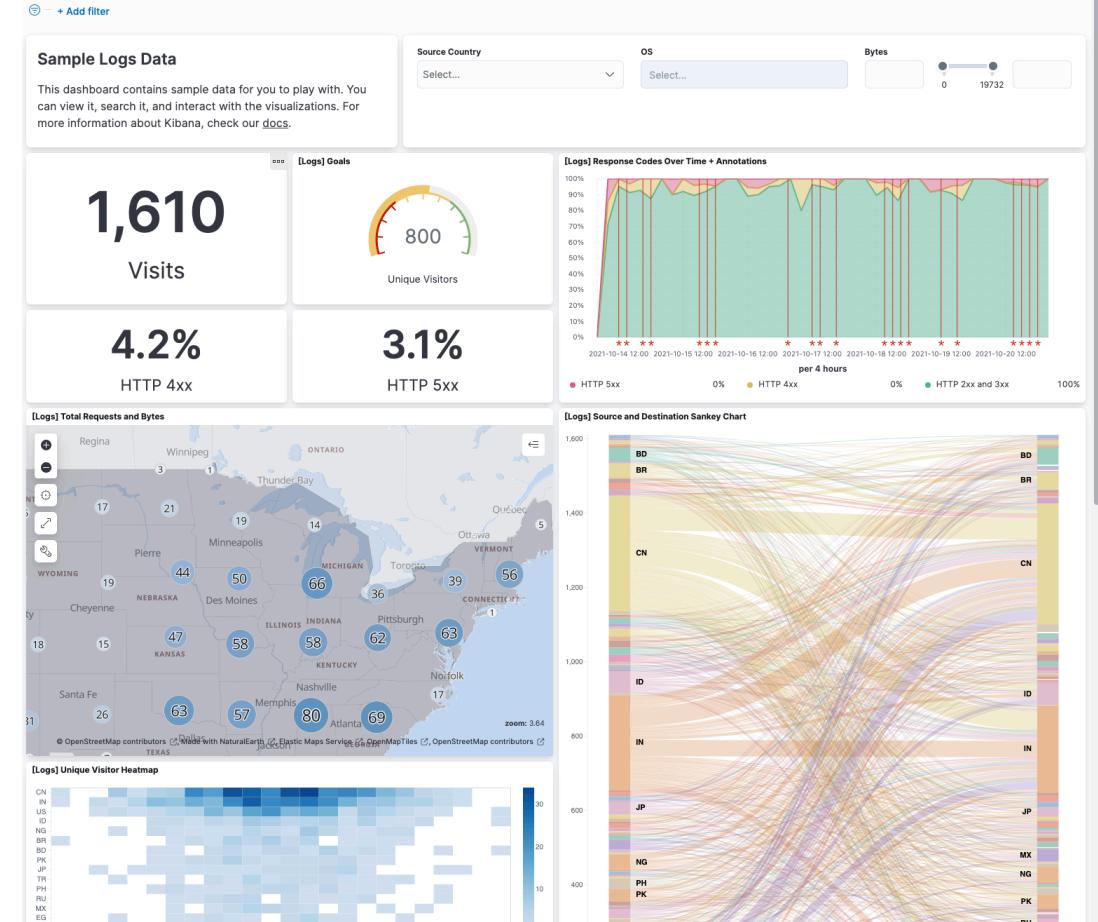
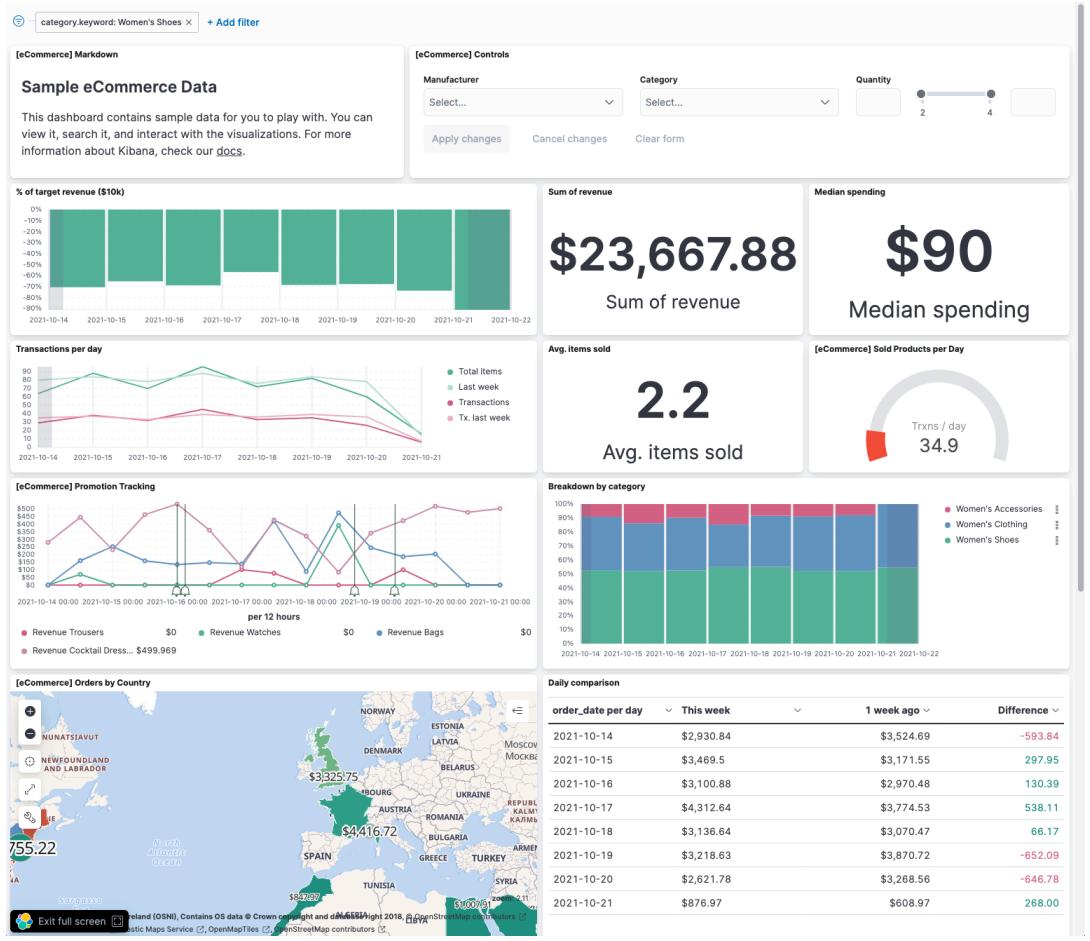
Shopping-Cart : Define Business Process Workflow



Dashboard Example



Dashboard Example



Dashboard Example

+ Add filter

Origin City: Select... Destination City: Select... Average Ticket Price: 101 - 1200

Apply changes Cancel changes Clear form

[Flights] Flight count

[Flights] Delays & Cancellations

[Flights] Delay Type

[Flights] Origin Time Delayed

LAYERS

- Flight Origin Location
- Flights
- Road map

Sample Flight 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](#).

2,217
Total flights

25.1%
Delayed

147.1%
Delayed vs 1 week earlier

12.6%
Cancelled

150.0%
Cancelled vs 1 week earlier

[Flights] Most delayed cities

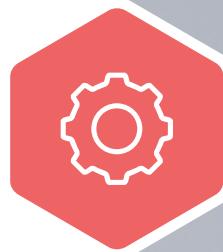
Top values of OriginCityName	Delay %	Cancel %
Memphis	100%	0%
Raleigh/Durham	100%	0%
Buffalo	75%	0%
Syracuse	75%	25%
Birmingham	67%	0%
Chicago/Rockford	67%	0%
Rochester	56%	0%
Bangor	50%	17%
Belleville	50%	25%
Cincinnati	50%	0%
Duluth	50%	0%
Greensboro	50%	17%
Nashville	50%	0%
New Orleans	50%	0%

[Flights] Airport Connections (Hover Over Airport)



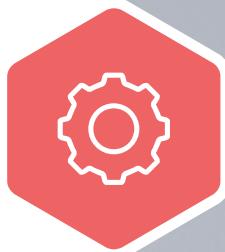
Setup Kibana LAB

Step by Step Installation

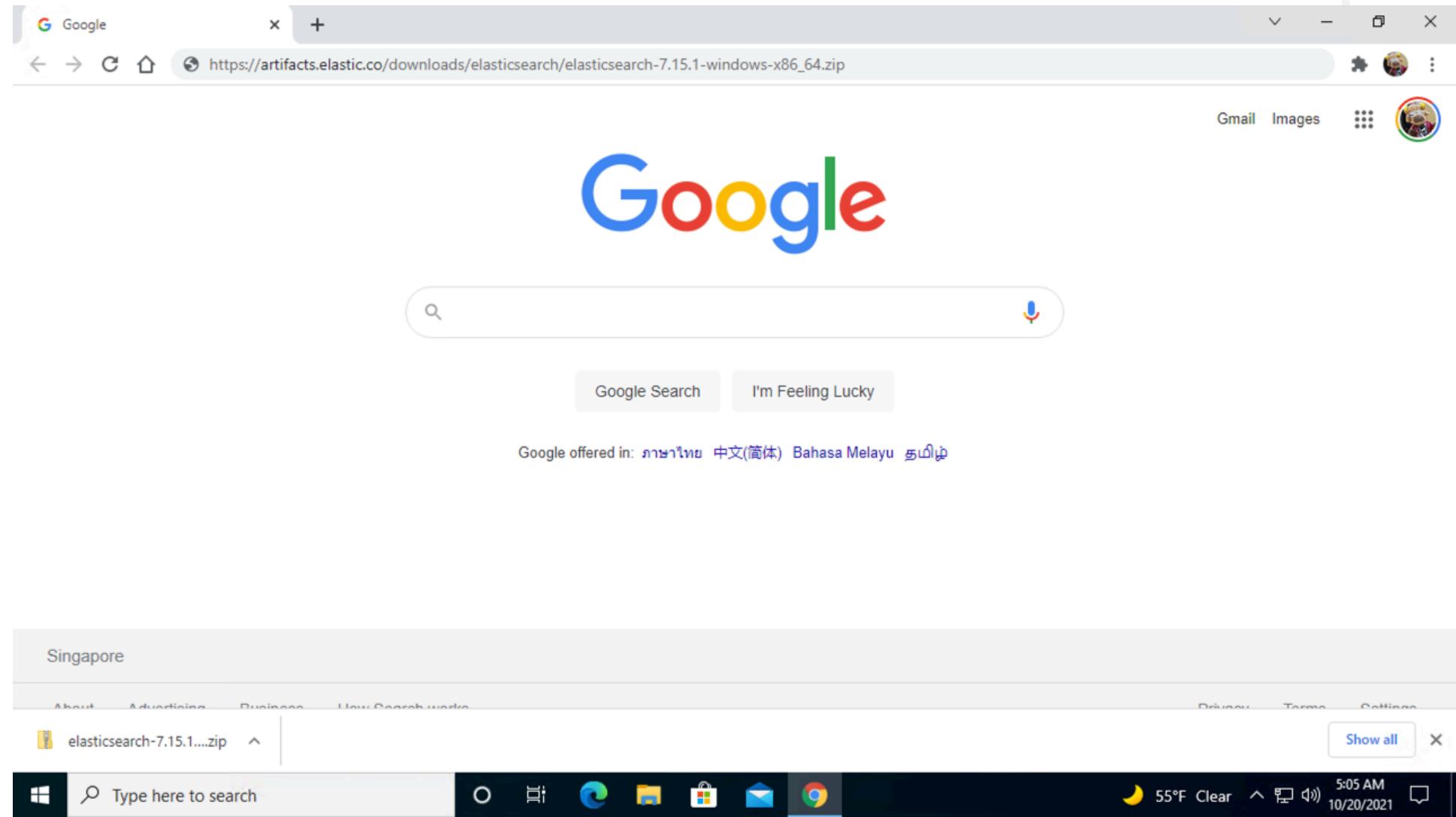


Install Elasticsearch

Step by Step Installation

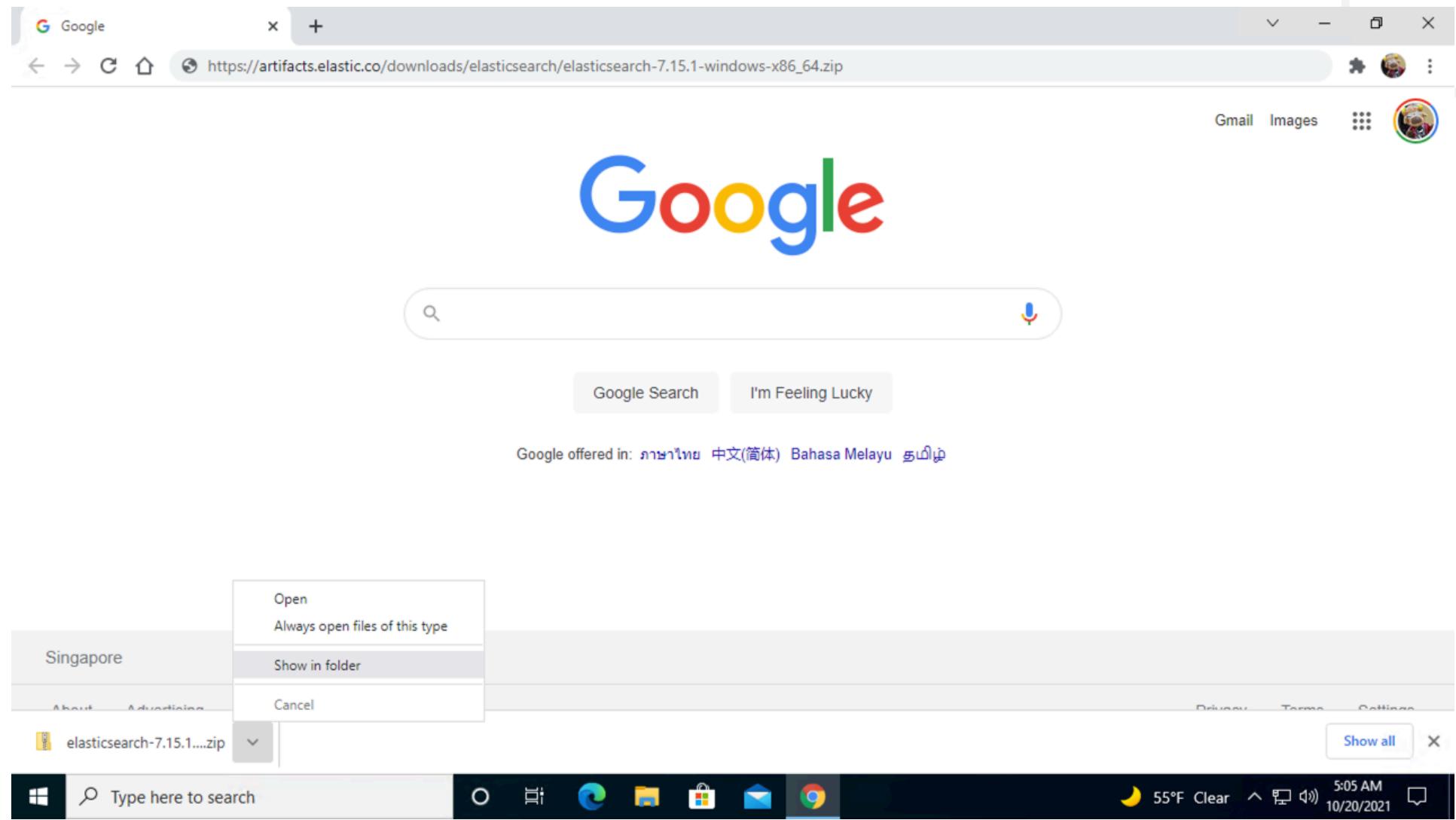


Install Elasticsearch

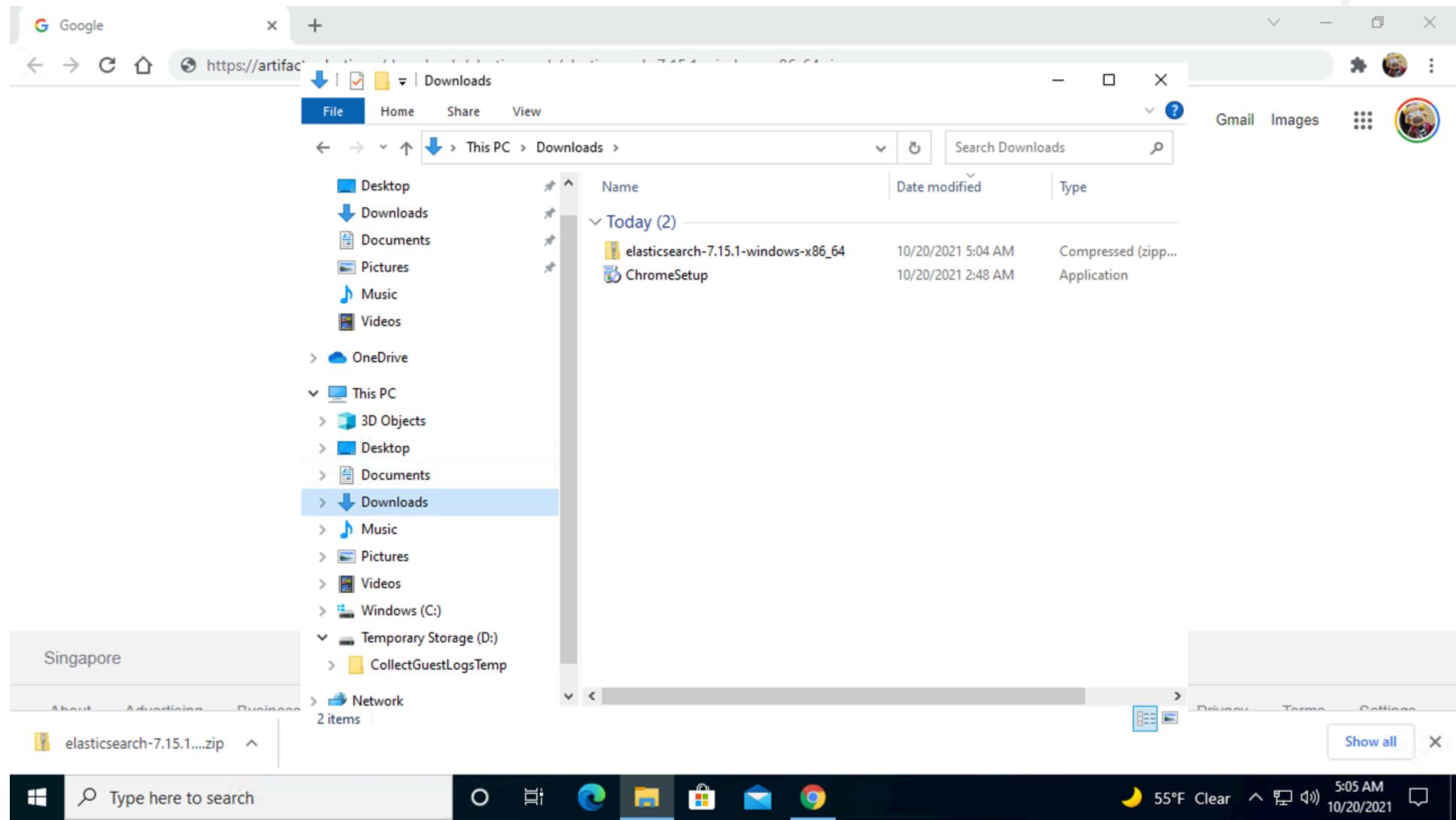


https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.15.1-windows-x86_64.zip

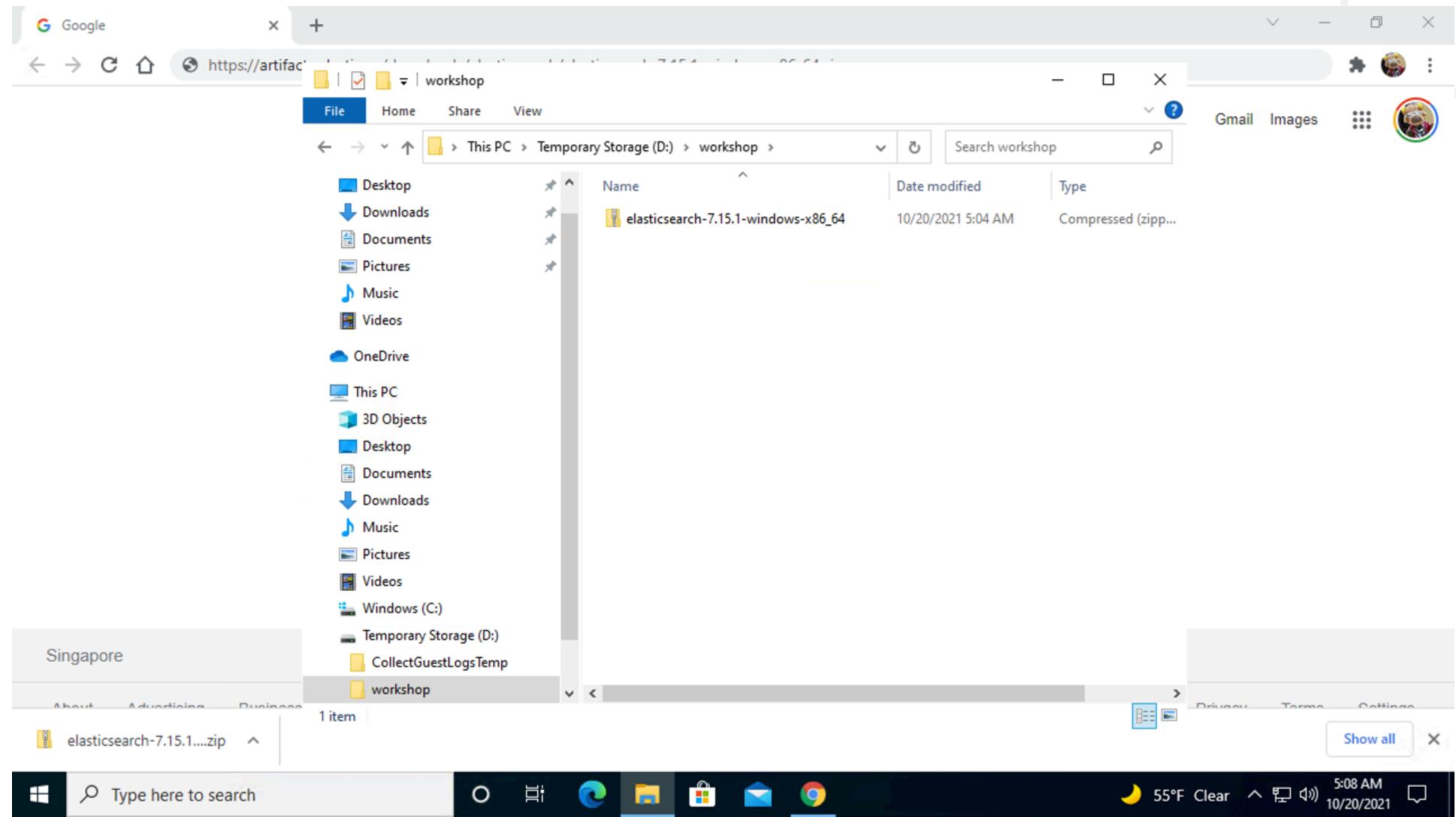
Install Elasticsearch



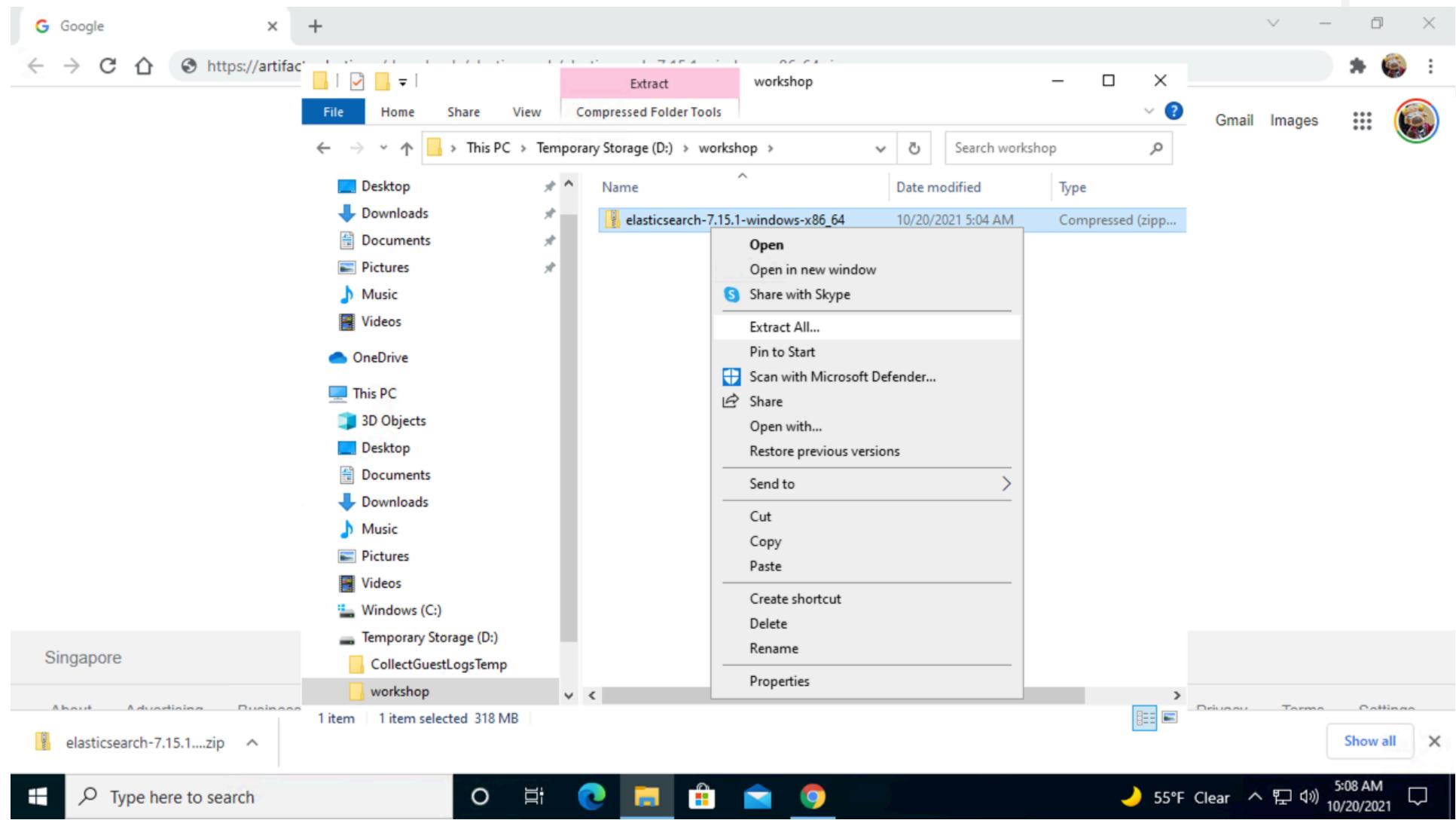
Install Elasticsearch



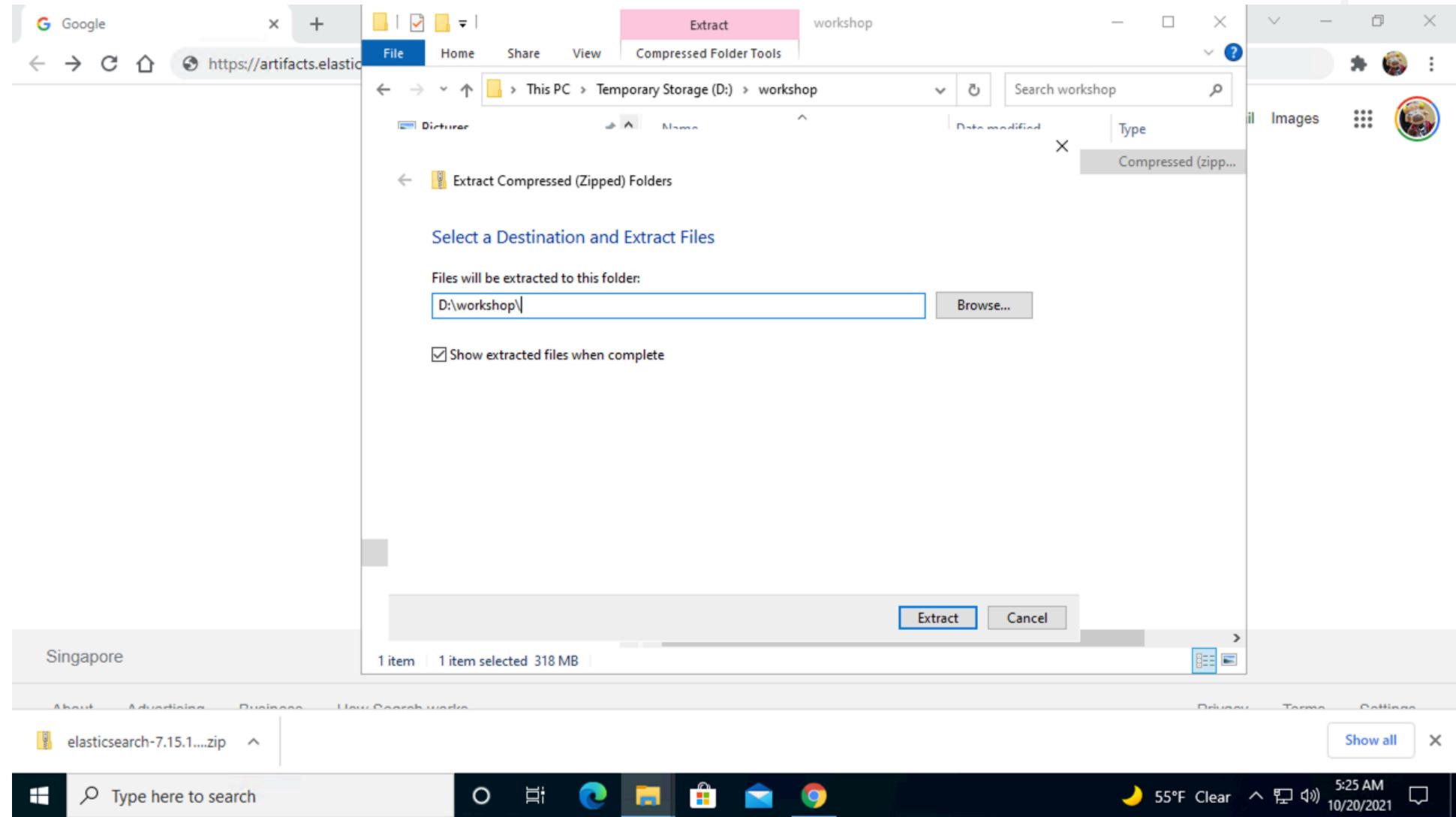
Install Elasticsearch



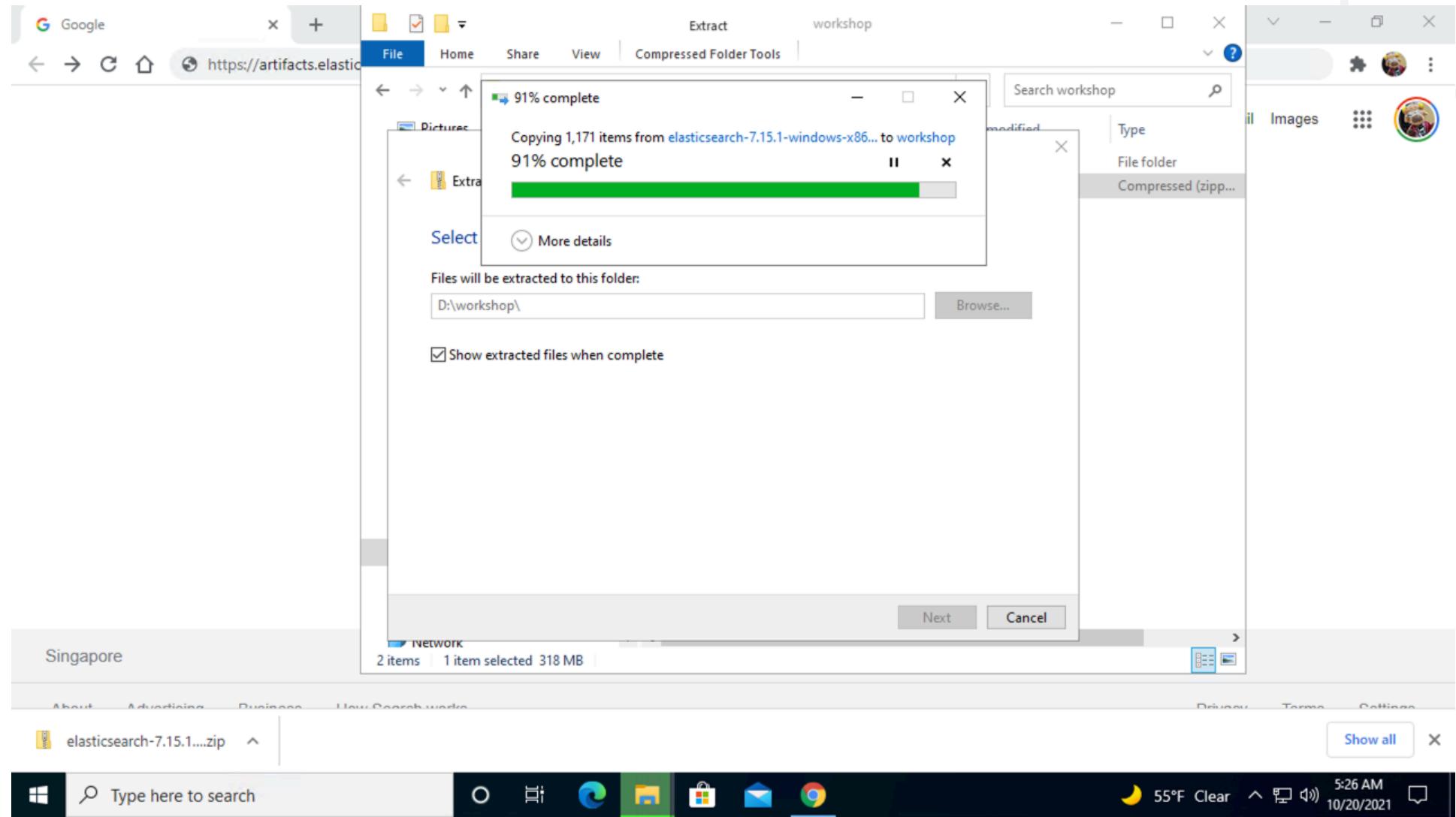
Install Elasticsearch



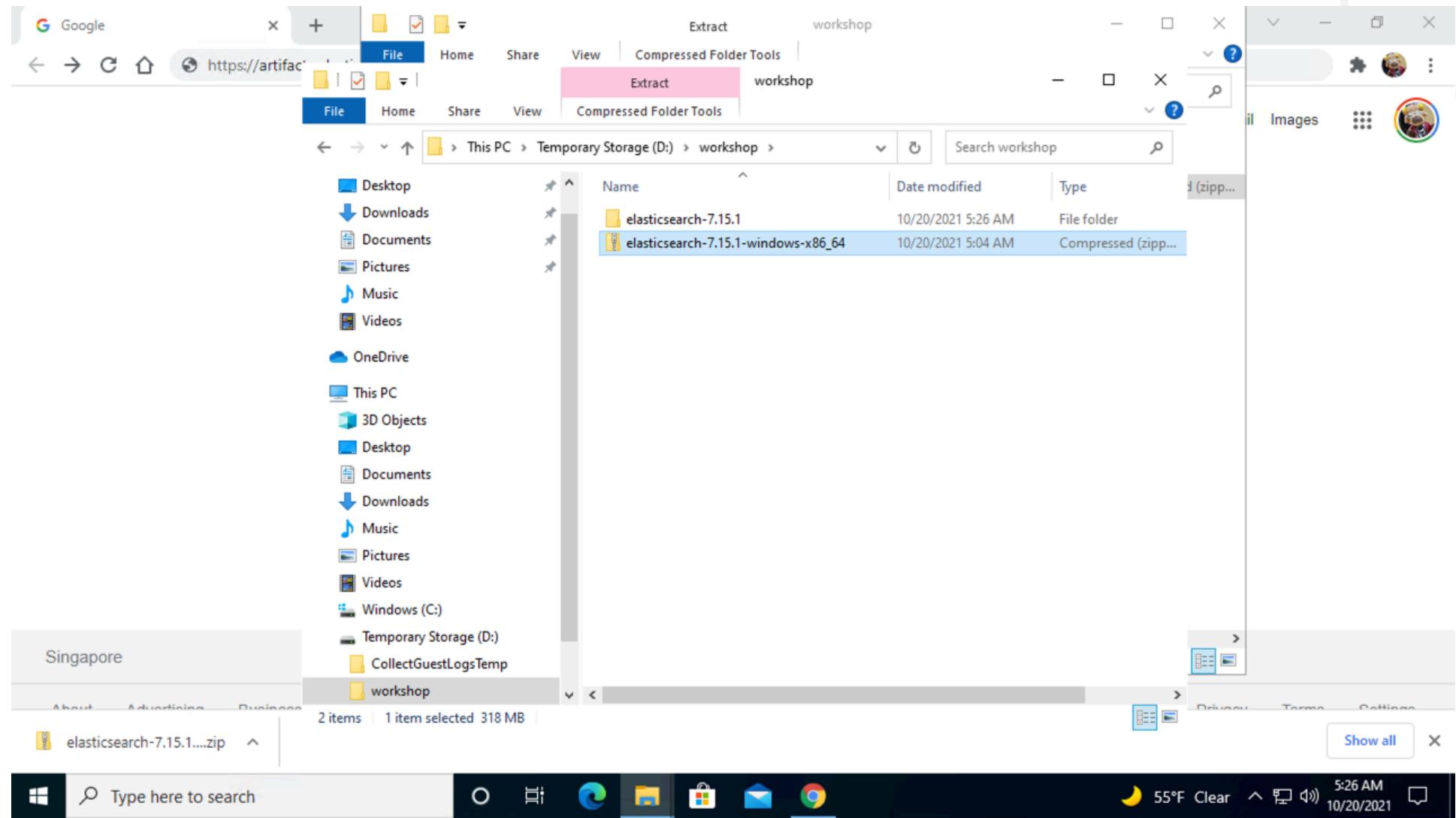
Install Elasticsearch



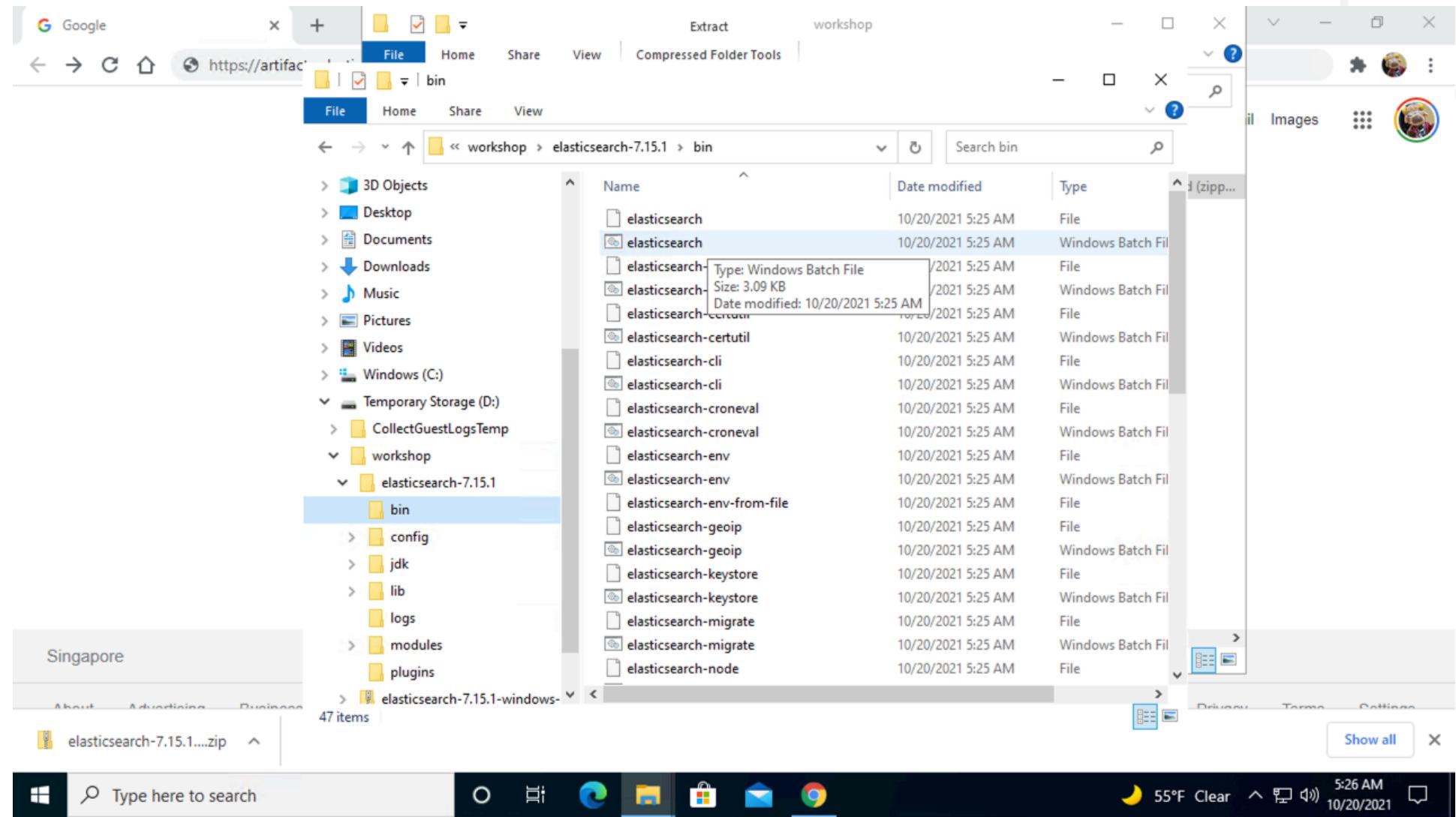
Install Elasticsearch



Install Elasticsearch



Install Elasticsearch



Install Elasticsearch

```
c:\Windows\system32\cmd.exe
WARNING: A terminally deprecated method in java.lang.System has been called
WARNING: System::setSecurityManager has been called by org.elasticsearch.bootstrap.Elasticsearch (file:/D:/workshop/elasticsearch-7.15.1/lib/elasticsearch-7.15.1.jar)
WARNING: Please consider reporting this to the maintainers of org.elasticsearch.bootstrap.Elasticsearch
WARNING: System::setSecurityManager will be removed in a future release
WARNING: A terminally deprecated method in java.lang.System has been called
WARNING: System::setSecurityManager has been called by org.elasticsearch.bootstrap.Security (file:/D:/workshop/elasticsearch-7.15.1/lib/elasticsearch-7.15.1.jar)
WARNING: Please consider reporting this to the maintainers of org.elasticsearch.bootstrap.Security
WARNING: System::setSecurityManager will be removed in a future release
[2021-10-20T05:26:56,835][INFO ][o.e.n.Node ] [my-windows] version[7.15.1] pid[5584] build[default-/gitea/245456ec20d60e04d886e455e6a240bb0]
ed/2021-10-07T21:56:19.031608185Z], OS[Windows 10/10.0/amd64], JVM[Eclipse Adoptium/OpenJDK 64-Bit Server VM/17/17+35]
[2021-10-20T05:26:56,835][INFO ][o.e.n.Node ] [my-windows] JVM home [D:\workshop\elasticsearch-7.15.1\jdk], using bundled JDK [true]
[2021-10-20T05:26:56,851][INFO ][o.e.n.Node ] [my-windows] JVM arguments [-Des.networkaddress.cache.ttl=60, -Des.networkaddress.cache.negative.ttl=10, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -XX:+ShowCodeDetailsInExceptionMessages, -Dio.netty.noUnsafe=true, -Dio.netty.noUnsafe=true, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Djava.locale.providers=SPI,COMPAT, --add-opens=java.base/java.io=ALL-UNNAMED, -XX:+UseG1GC, -Djava.io.tmpdir=C:\Users\karan\AppData\Local\Temp\elasticsearch, -XX:+HeapDumpOnOutOfMemoryError, -XX:heapdumpPath=data, -XX:ErrorFile=logs/ns_error.pid%p.log, -Xlog:gc*,gc+age=trace,safepoint:file=logs/gc.log:utctime,pid,tags:filecount=32,filesize=64m, -Xms4095m, -Xmx4095m, -XX:MaxDirectMemorySize=2147483648, -XX:G1HeapRegionSize=4m, -XX:InitiatingHeapOccupancyPercent=30, -XX:G1ReservePercent=15, -Delasticse...1, -Des.path.conf=D:\workshop\elasticsearch-7.15.1\config, -Des.distribution.flavor=default, -Des.distribution.type=zip, -Des.bundled_jdk=true]
[2021-10-20T05:27:03,304][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [aggs-matrix-stats]
[2021-10-20T05:27:03,310][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [analysis-common]
[2021-10-20T05:27:03,310][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [constant-keyword]
[2021-10-20T05:27:03,310][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [frozen-indices]
[2021-10-20T05:27:03,310][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [ingest-common]
[2021-10-20T05:27:03,310][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [ingest-geoip]
[2021-10-20T05:27:03,310][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [ingest-user-agent]
[2021-10-20T05:27:03,310][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [kibana]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [lang-expression]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [lang-mustache]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [lang-painless]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [mapper-extras]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [mapper-version]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [parent-join]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [percolator]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [rank-eval]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [reindex]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [repositories-metering-api]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [repository-encrypted]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService ] [my-windows] loaded module [repository-url]
```



Install Elasticsearch

```
c:\Windows\system32\cmd.exe
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [repositories-metering-api]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [repository-encrypted]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [repository-url]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [runtime-fields-common]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [search-business-rules]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [searchable-snapshots]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [snapshot-repo-test-kit]
[2021-10-20T05:27:03,319][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [spatial]
[2021-10-20T05:27:03,335][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [transform]
[2021-10-20T05:27:03,335][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [transport-netty4]
[2021-10-20T05:27:03,335][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [unsigned-long]
[2021-10-20T05:27:03,335][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [vector-tile]
[2021-10-20T05:27:03,335][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [vectors]
[2021-10-20T05:27:03,335][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [wildcard]
[2021-10-20T05:27:03,335][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-aggregate-metric]
[2021-10-20T05:27:03,351][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-analytics]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-async]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-async-search]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-autoscaling]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-ccr]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-core]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-data-streams]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-deprecation]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-enrich]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-eql]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-fleet]
[2021-10-20T05:27:03,366][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-graph]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-identity-provider]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-ilm]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-logstash]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-ml]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-monitoring]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-ql]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-rollup]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-security]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-shutdown]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-sql]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-stack]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-text-structure]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-voting-only-node]
[2021-10-20T05:27:03,382][INFO ][o.e.p.PluginsService      ] [my-windows] loaded module [x-pack-watcher]
```



Install Elasticsearch

```
c:\Windows\system32\cmd.exe
[2021-10-20T05:27:03,757][INFO ][o.e.e.NodeEnvironment      ] [my-windows] using [1] data paths, mounts [[Temporary Storage (D:)]], net usable_space [12.2gb], net total_space [15.9gb], types [NTFS]
[2021-10-20T05:27:03,757][INFO ][o.e.e.NodeEnvironment      ] [my-windows] heap size [4gb], compressed ordinary object pointers [true]
[2021-10-20T05:27:03,835][INFO ][o.e.n.Node          ] [my-windows] node name [my-windows], node ID [9K_JwxSYSdehLKD5-eEMw], cluster name [elasticsearch], roles [transform, data_frozen, master, remote_cluster_client, data, ml, data_content, data_hot, data_warm, data_cold, ingest]
[2021-10-20T05:27:12,385][INFO ][o.e.x.m.p.l.CppLogMessageHandler] [my-windows] [controller/5748] [Main.cc@122] controller (64 bit): Version 7.15.1 (Build 9659930f1bbe9) Copyright (c) 2021 Elasticsearch BV
[2021-10-20T05:27:13,194][INFO ][o.e.x.s.a.s.FileRolesStore] [my-windows] parsed [0] roles from file [D:\workshop\elasticsearch-7.15.1\config\roles.yml]
[2021-10-20T05:27:14,663][INFO ][o.e.i.g.LocalDatabases  ] [my-windows] initialized default databases [[GeoLite2-Country.mmdb, GeoLite2-City.mmdb, GeoLite2-ASN.mmdb]], config databases [[]] and watching [D:\workshop\elasticsearch-7.15.1\config\ingest-geoip] for changes
[2021-10-20T05:27:14,679][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] initialized database registry, using geoip-databases directory [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw]
[2021-10-20T05:27:15,799][INFO ][o.e.t.NettyAllocator   ] [my-windows] creating NettyAllocator with the following configs: [name=elasticsearch_configured, chunk_size=1mb, suggested_max_allocation_size=1mb, factors={es.unsafe.use.netty_chunk_and_page_size=false, g1gc_enabled=true, g1gc_region_size=4mb}]
[2021-10-20T05:27:15,968][INFO ][o.e.d.DiscoveryModule  ] [my-windows] using discovery type [zen] and seed hosts providers [settings]
[2021-10-20T05:27:16,835][INFO ][o.e.g.DanglingIndicesState] [my-windows] gateway.auto_import_dangling_indices is disabled, dangling indices will not be automatically detected or imported and must be managed manually
[2021-10-20T05:27:17,632][INFO ][o.e.n.Node          ] [my-windows] initialized
[2021-10-20T05:27:17,632][INFO ][o.e.n.Node          ] [my-windows] starting ...
[2021-10-20T05:27:17,663][INFO ][o.e.x.s.c.f.PersistentCache] [my-windows] persistent cache index loaded
[2021-10-20T05:27:17,882][INFO ][o.e.t.TransportService] [my-windows] publish_address {127.0.0.1:9300}, bound_addresses {127.0.0.1:9300}, {[::1]:9300}
[2021-10-20T05:27:18,194][WARN ][o.e.b.BootstrapChecks  ] [my-windows] the default discovery settings are unsuitable for production use; at least one of [discovery.seed_hosts, discovery.seed_providers, cluster.initial_master_nodes] must be configured
[2021-10-20T05:27:18,241][INFO ][o.e.c.c.ClusterBootstrapService] [my-windows] no discovery configuration found, will perform best-effort cluster bootstrapping after [3s] unless existing master is discovered
[2021-10-20T05:27:21,265][INFO ][o.e.c.c.Coordinator    ] [my-windows] setting initial configuration to VotingConfiguration{9K_JwxSYSdehLKD5-eEMw}
[2021-10-20T05:27:21,538][INFO ][o.e.c.s.MasterService   ] [my-windows] elected-as-master ([1] nodes joined){[my-windows]{9K_JwxSYSdehLKD5-eEMw}{omGrgQviQA2-V-xeBw8w8A}{127.0.0.1:9300}{cdfhilmrstw}} elect leader, _BECOME_MASTER_TASK_, _FINISH_ELECTION_, term: 1, version: 1, delta: master node changed {previous [], current {[my-windows]{9K_JwxSYSdehLKD5-eEMw}{omGrgQviQA2-V-xeBw8w8A}{127.0.0.1:9300}{cdfhilmrstw}}}
[2021-10-20T05:27:21,663][INFO ][o.e.c.c.CoordinationState] [my-windows] cluster UUID set to [8Dbu2i6SSSW06p_MBG8WBg]
[2021-10-20T05:27:21,804][INFO ][o.e.c.s.ClusterApplierService] [my-windows] master node changed {previous [], current {[my-windows]{9K_JwxSYSdehLKD5-eEMw}{omGrgQviQA2-V-xeBw8w8A}{127.0.0.1:9300}{cdfhilmrstw}}}, term: 1, version: 1, reason: replication{term=1, version=1}
[2021-10-20T05:27:22,102][INFO ][o.e.h.AbstractHttpServerTransport] [my-windows] publish_address {127.0.0.1:9200}, bound_addresses {127.0.0.1:9200}, {[::1]:9200}
[2021-10-20T05:27:22,102][INFO ][o.e.n.Node          ] [my-windows] started
[2021-10-20T05:27:22,288][INFO ][o.e.g.GatewayService  ] [my-windows] recovered [0] indices into cluster_state
[2021-10-20T05:27:22,911][INFO ][o.e.c.m.MetadataIndexTemplateService] [my-windows] adding index template [.ml-anomalies-*]
[2021-10-20T05:27:23,101][INFO ][o.e.c.m.MetadataIndexTemplateService] [my-windows] adding index template [.ml-notifications-000002] for index patterns [.ml-notifications-000002]
[2021-10-20T05:27:23,288][INFO ][o.e.c.m.MetadataIndexTemplateService] [my-windows] adding index template [.ml-state] for index patterns [.ml-state*]
```



Install Elasticsearch

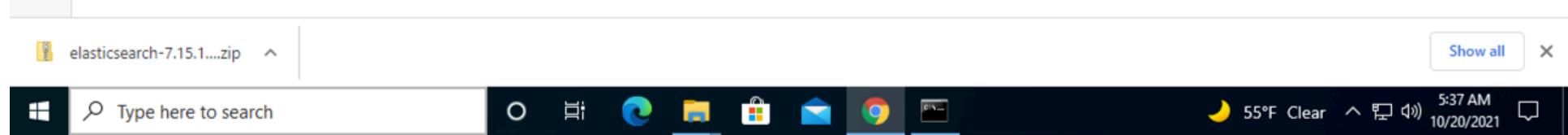
```
c:\Windows\system32\cmd.exe
[2021-10-20T05:27:28,944][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [ilm-history-ilm-policy]
[2021-10-20T05:27:29,163][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [slm-history-ilm-policy]
[2021-10-20T05:27:29,320][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [.deprecation-indexing-ilm-policy]
[2021-10-20T05:27:29,460][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [.fleet-actions-results-ilm-policy]
[2021-10-20T05:27:29,757][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip databases
[2021-10-20T05:27:29,819][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] fetching geoip databases overview from [https://geoip.elastic.co/v1/database?elastic_geoip_service_tos=agree]
[2021-10-20T05:27:30,023][INFO ][o.e.l.LicenseService    ] [my-windows] license [f7846eb3-417c-4f18-af06-56360a712d2f] mode [basic] - valid
[2021-10-20T05:27:30,023][INFO ][o.e.x.s.s.SecurityStatusChangeListener] [my-windows] Active license is now [BASIC]; Security is disabled
[2021-10-20T05:27:30,023][WARN ][o.e.x.s.s.SecurityStatusChangeListener] [my-windows] Elasticsearch built-in security features are not enabled. Without authentication, your cluster could be accessible to anyone. See https://www.elastic.co/guide/en/elasticsearch/reference/7.15/security-minimal-setup.html to enable security.
[2021-10-20T05:27:31,111][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip database [GeoLite2-ASN.mmdb]
[2021-10-20T05:27:31,760][INFO ][o.e.c.m.MetadataCreateIndexService] [my-windows] [.geoip_databases] creating index, cause [auto(bulk api)], templates [], shards [1]/[0]
[2021-10-20T05:27:32,241][INFO ][o.e.c.r.a.AllocationService] [my-windows] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.geoip_databases][0]]]).
[2021-10-20T05:27:33,334][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] downloading geoip database [GeoLite2-ASN.mmdb] to [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-ASN.mmdb.tmp.gz]
[2021-10-20T05:27:33,398][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updated geoip database [GeoLite2-ASN.mmdb]
[2021-10-20T05:27:33,429][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip database [GeoLite2-City.mmdb]
[2021-10-20T05:27:33,788][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] successfully reloaded changed geoip database file [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-ASN.mmdb]
[2021-10-20T05:27:37,257][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] downloading geoip database [GeoLite2-City.mmdb] to [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-City.mmdb.tmp.gz]
[2021-10-20T05:27:37,288][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updated geoip database [GeoLite2-City.mmdb]
[2021-10-20T05:27:37,382][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip database [GeoLite2-Country.mmdb]
[2021-10-20T05:27:38,724][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] downloading geoip database [GeoLite2-Country.mmdb] to [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-Country.mmdb.tmp.gz]
[2021-10-20T05:27:38,773][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updated geoip database [GeoLite2-Country.mmdb]
[2021-10-20T05:27:38,976][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] successfully reloaded changed geoip database file [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-Country.mmdb]
[2021-10-20T05:27:39,257][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] successfully reloaded changed geoip database file [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-City.mmdb]
```



Install Elasticsearch



```
// 20211020053648
// http://localhost:9200/
{
  "name": "my-windows",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "8Dbu2i6SSSWO6p_MbG8WBg",
  "version": {
    "number": "7.15.1",
    "build_flavor": "default",
    "build_type": "zip",
    "build_hash": "83c34f456ae29d60e94d886e455e6a3409bba9ed",
    "build_date": "2021-10-07T21:56:19.031608185Z",
    "build_snapshot": false,
    "lucene_version": "8.9.0",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}
```



elasticsearch-7.15.1....zip

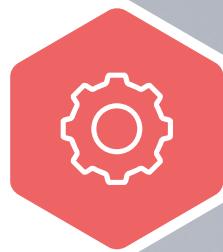
Type here to search

55°F Clear 5:37 AM 10/20/2021



Install Kibana

Step by Step Installation

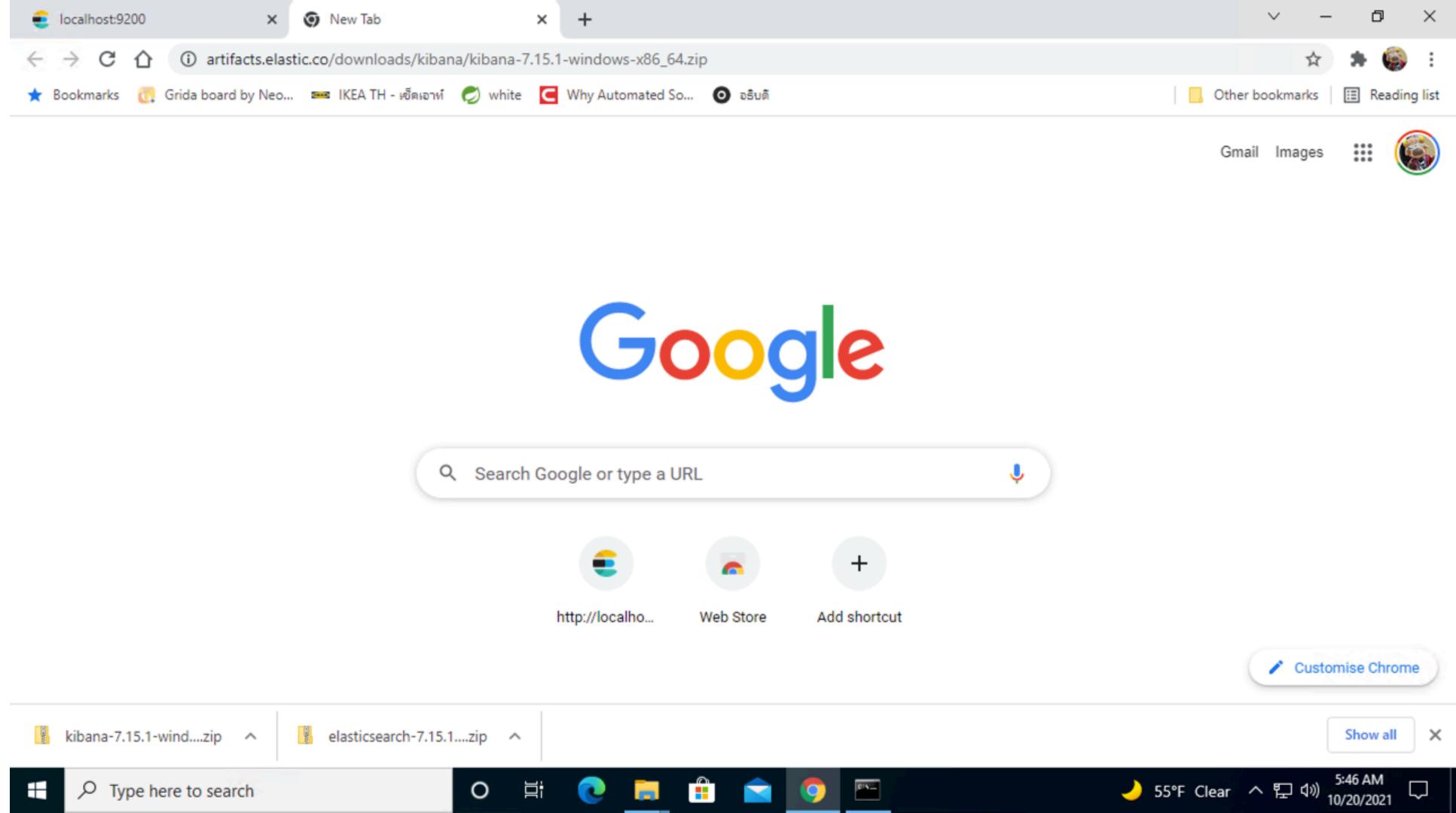


Install Kibana

<https://www.elastic.co/guide/en/kibana/current/windows.html>

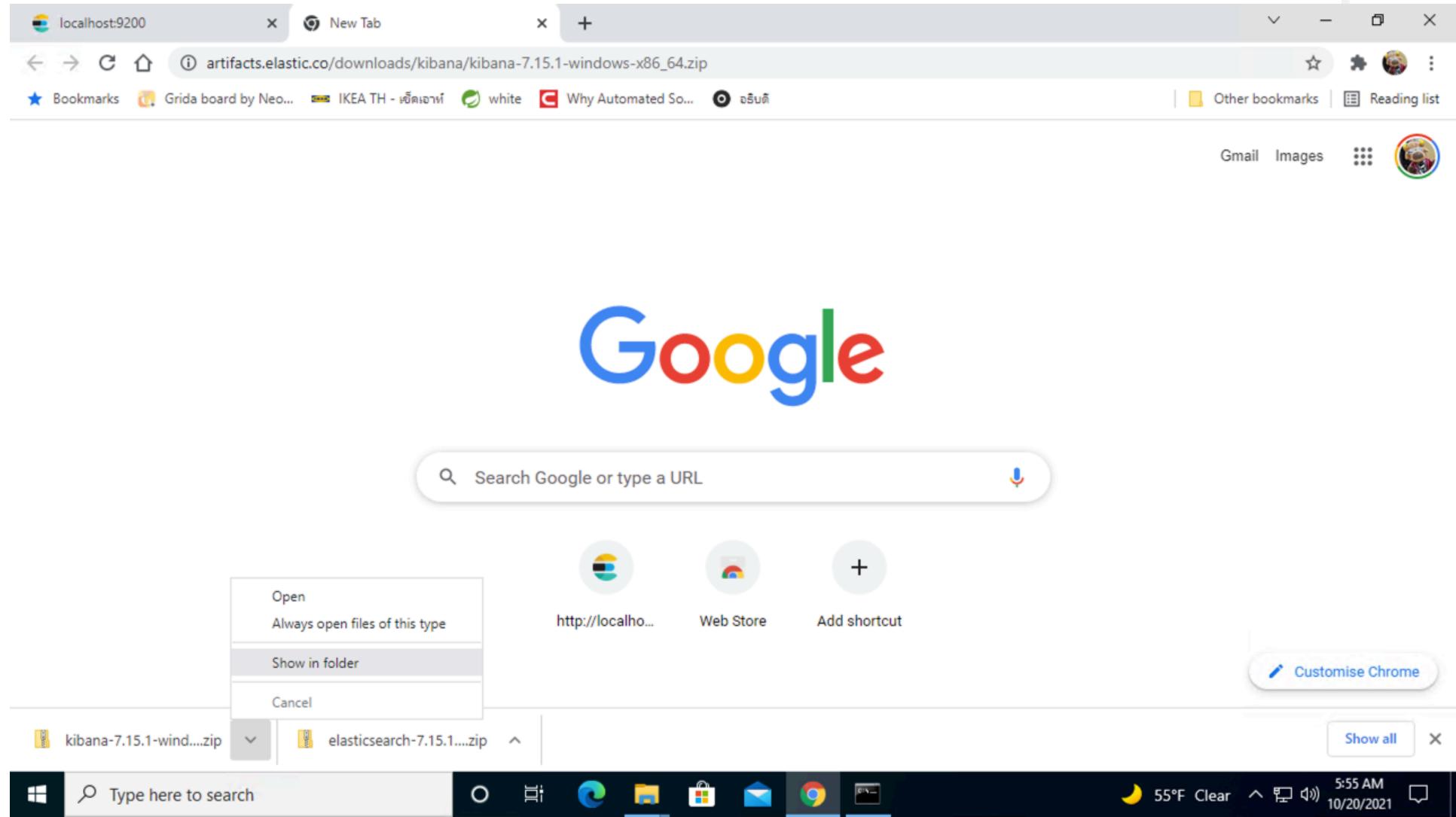


Install Kibana

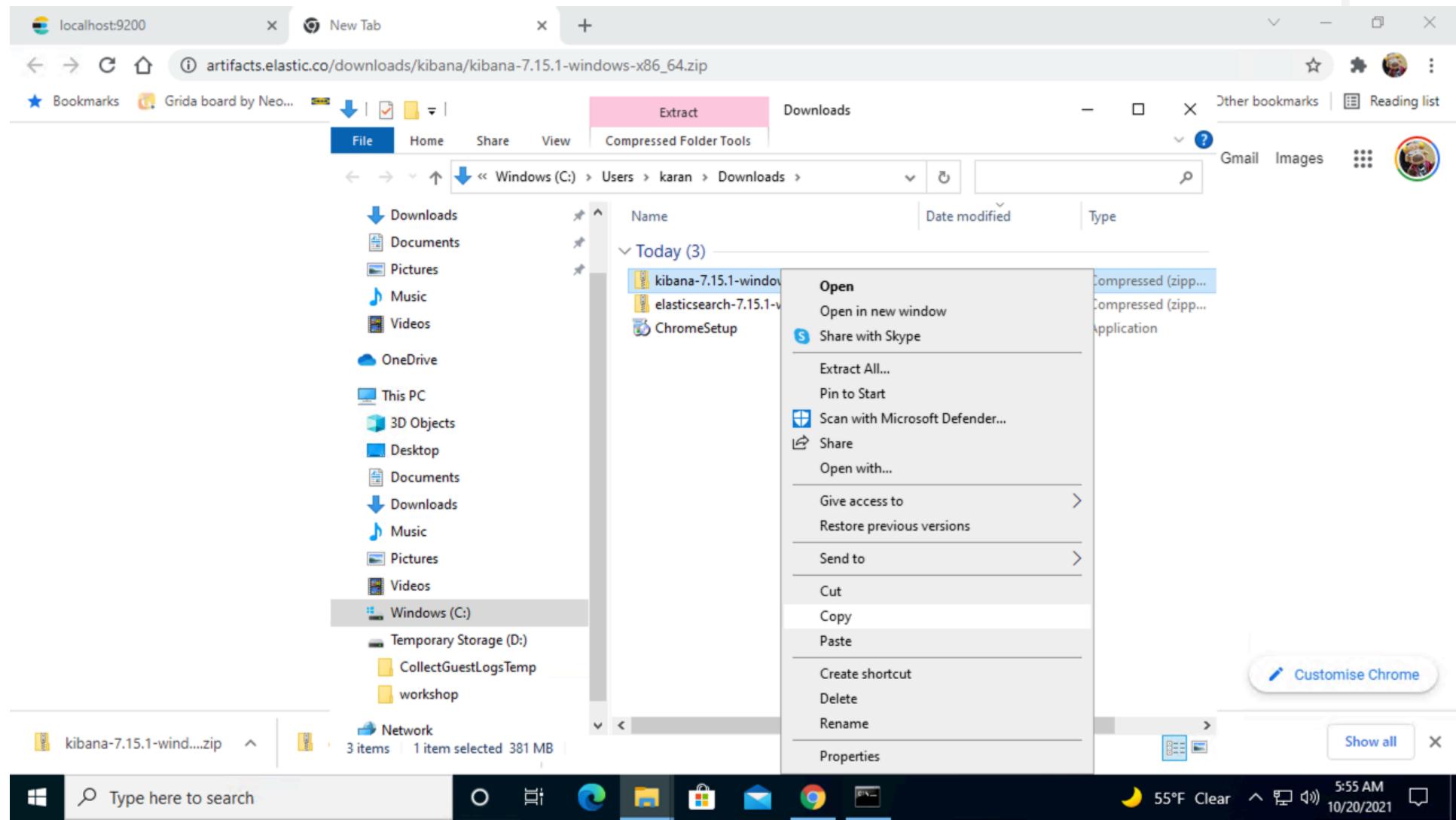


https://artifacts.elastic.co/downloads/kibana/kibana-7.15.1-windows-x86_64.zip

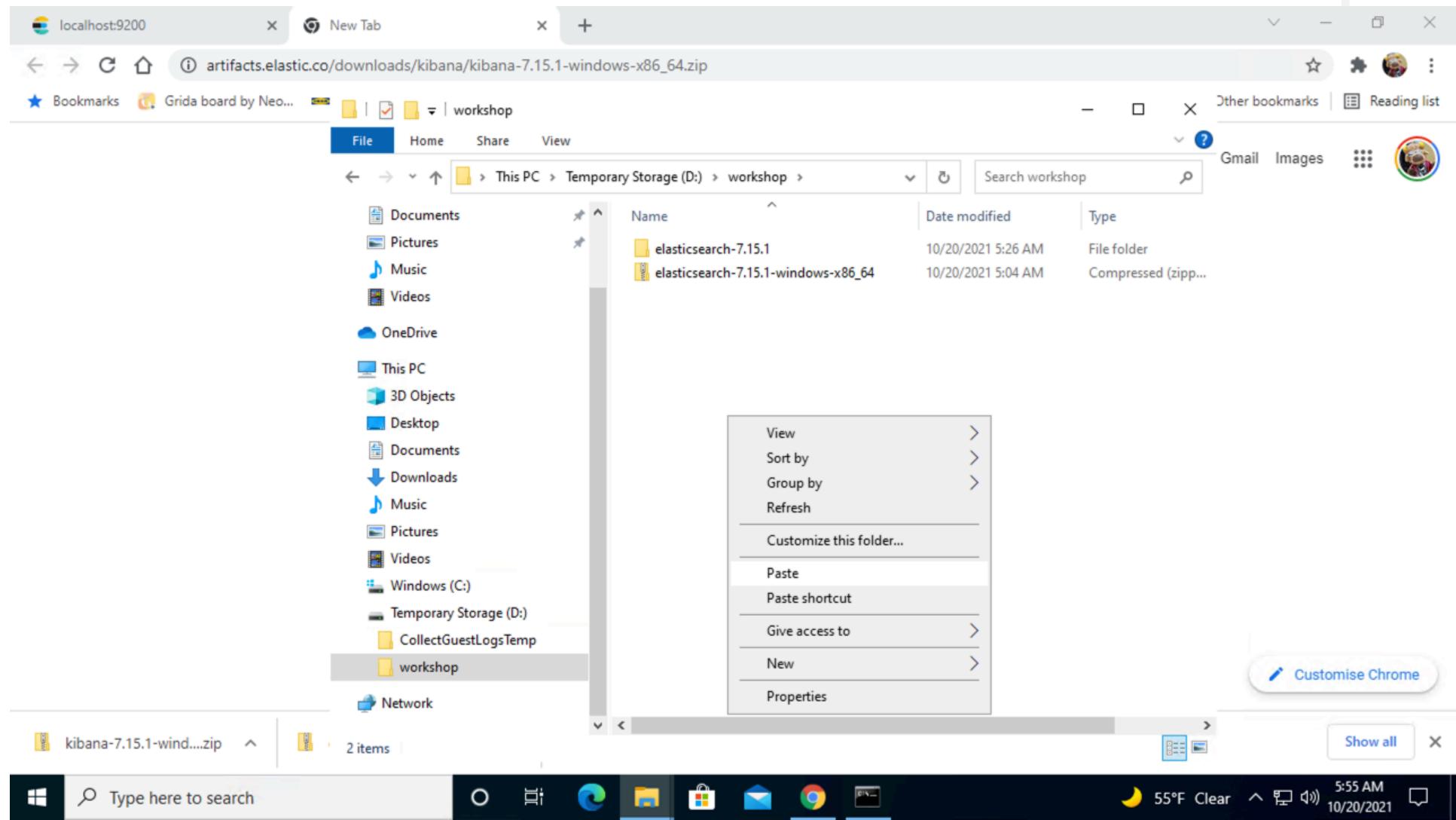
Install Kibana



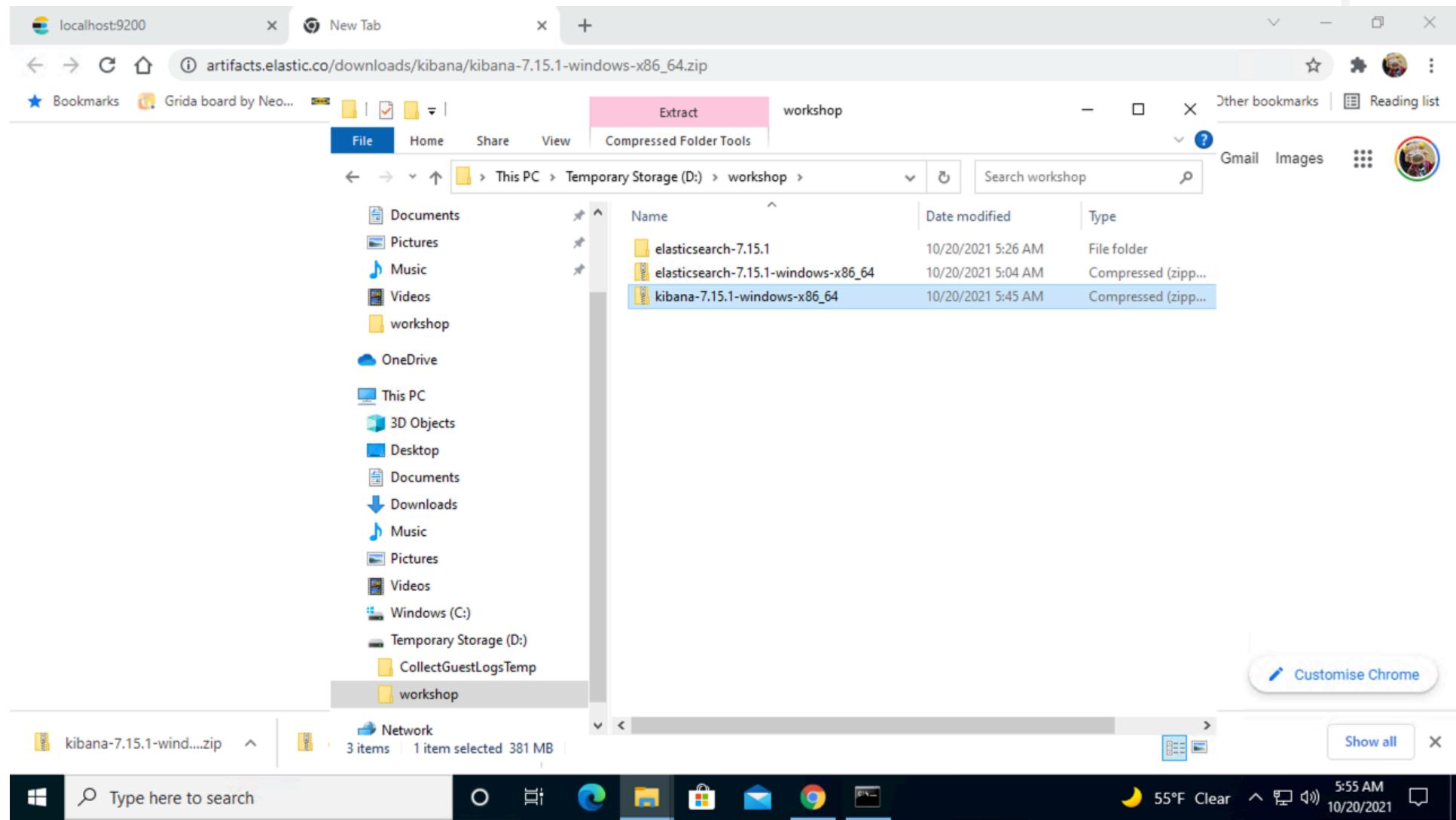
Install Kibana



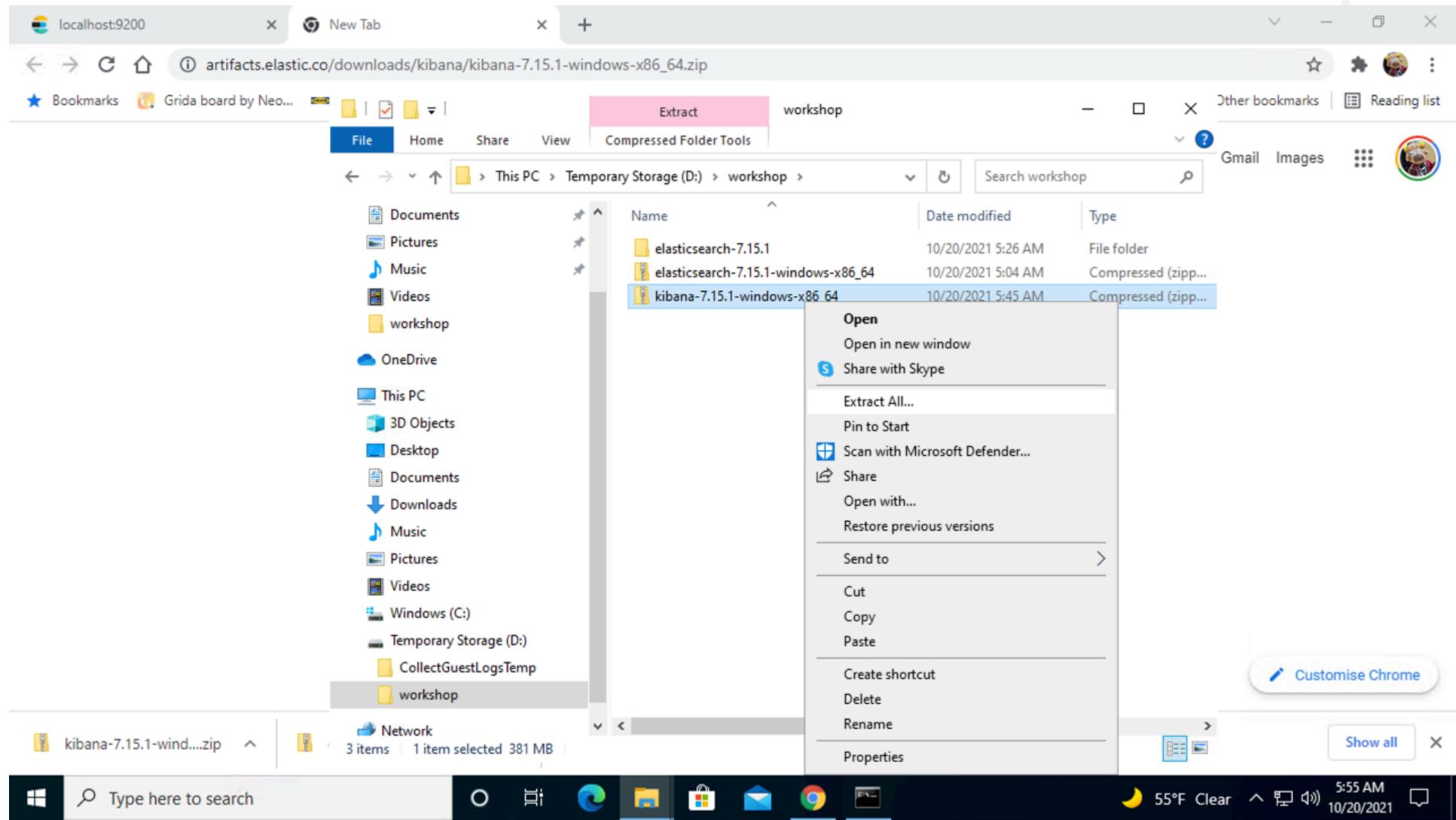
Install Kibana



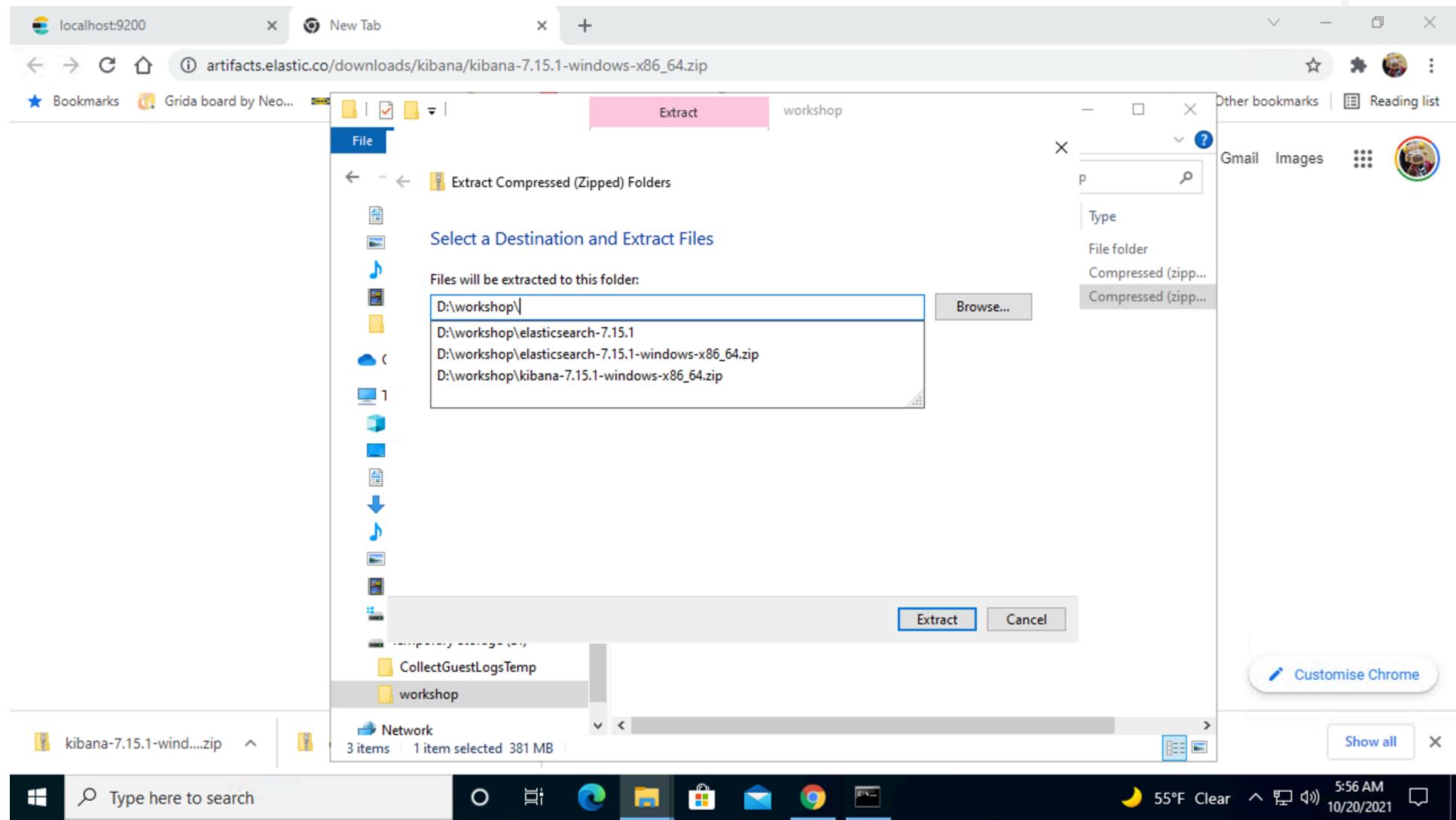
Install Kibana



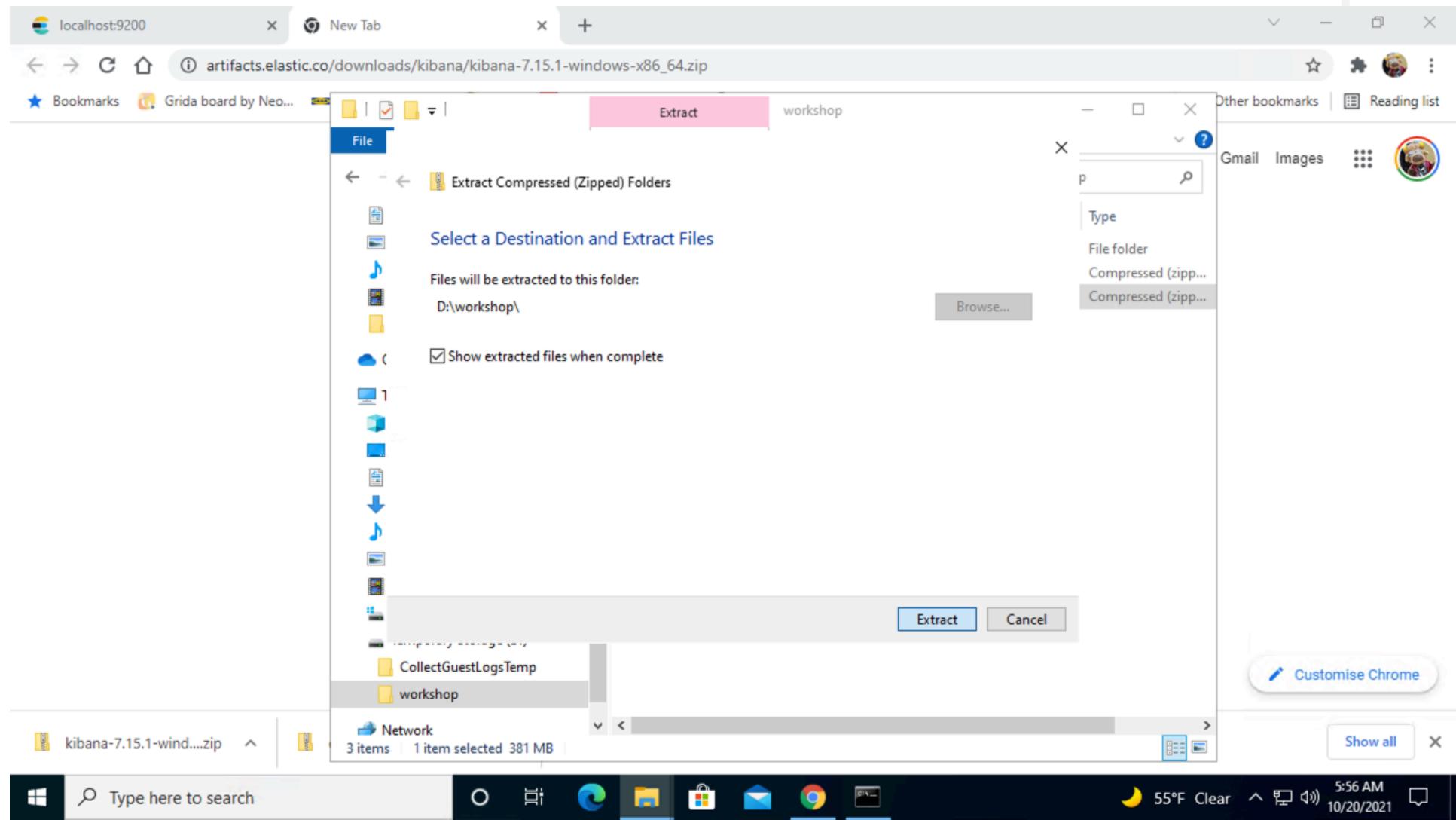
Install Kibana



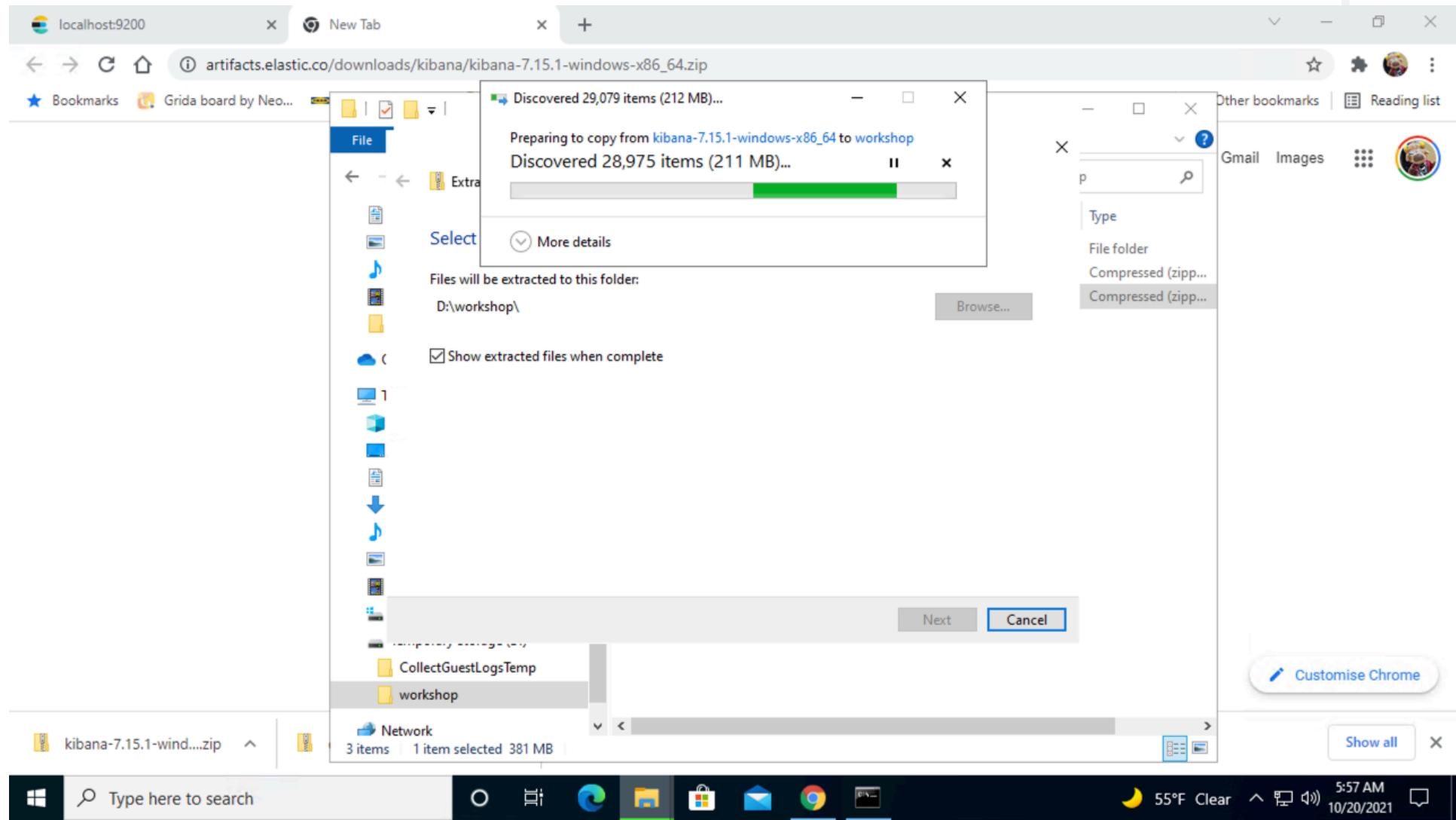
Install Kibana



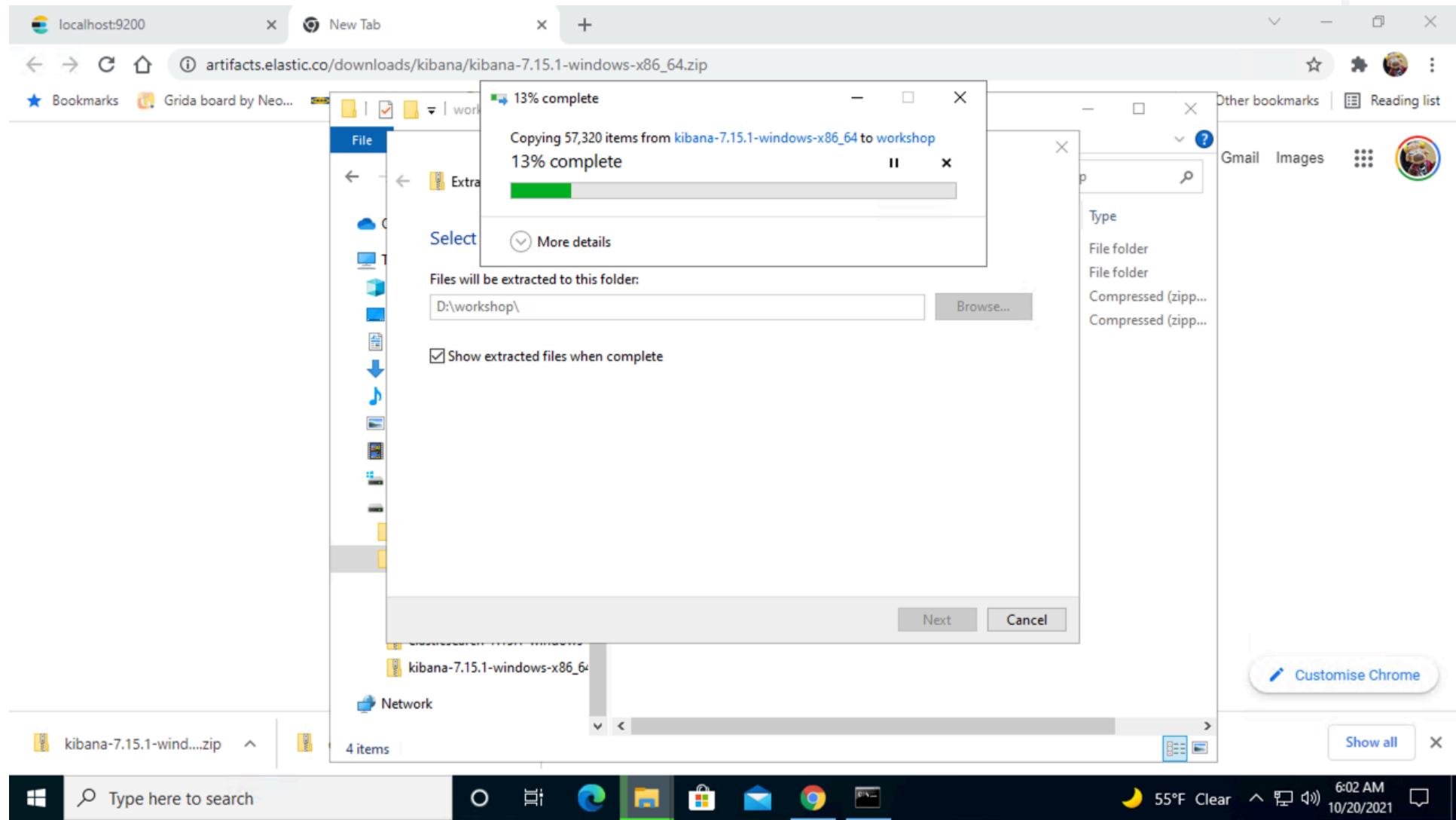
Install Kibana



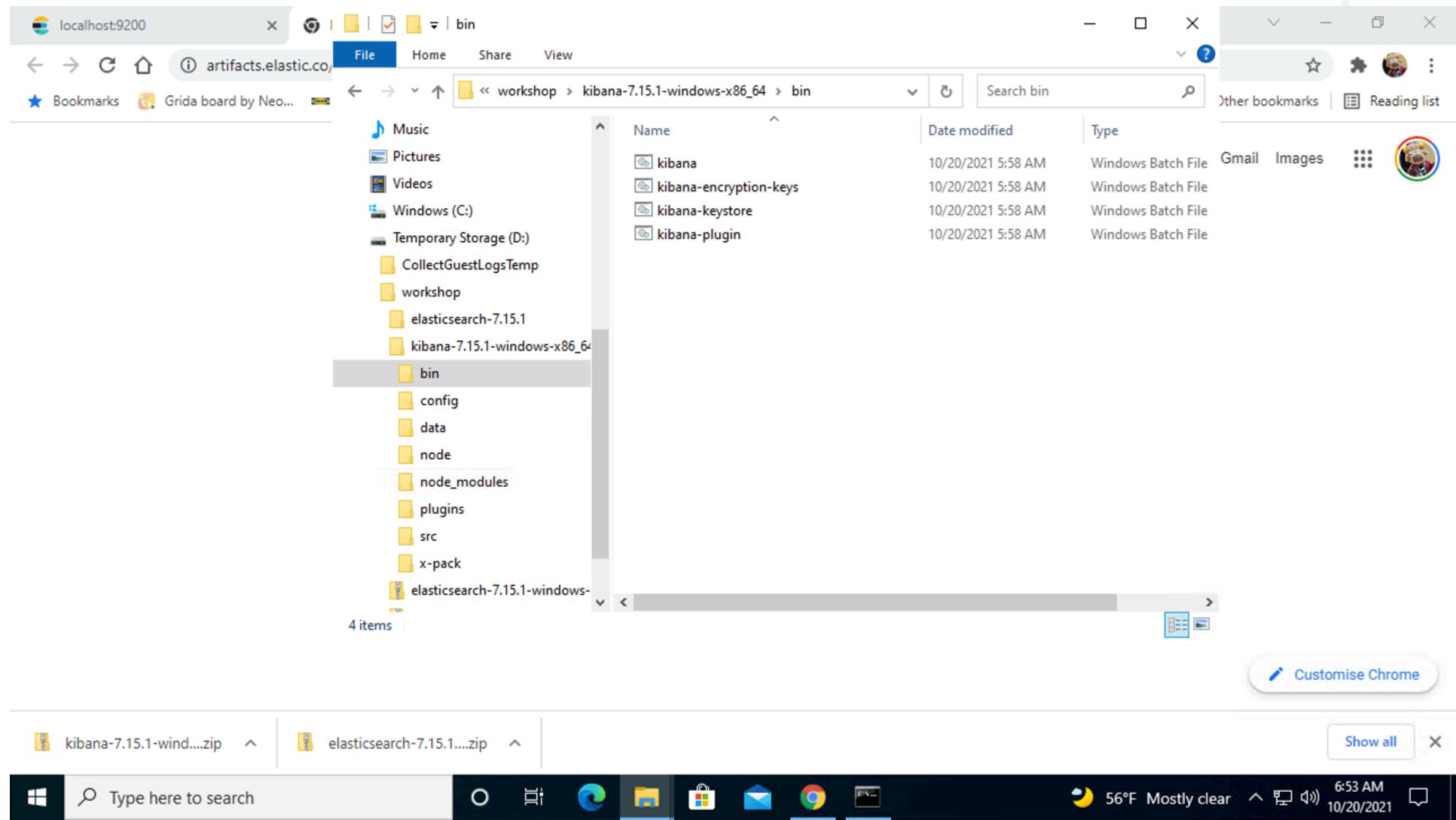
Install Kibana



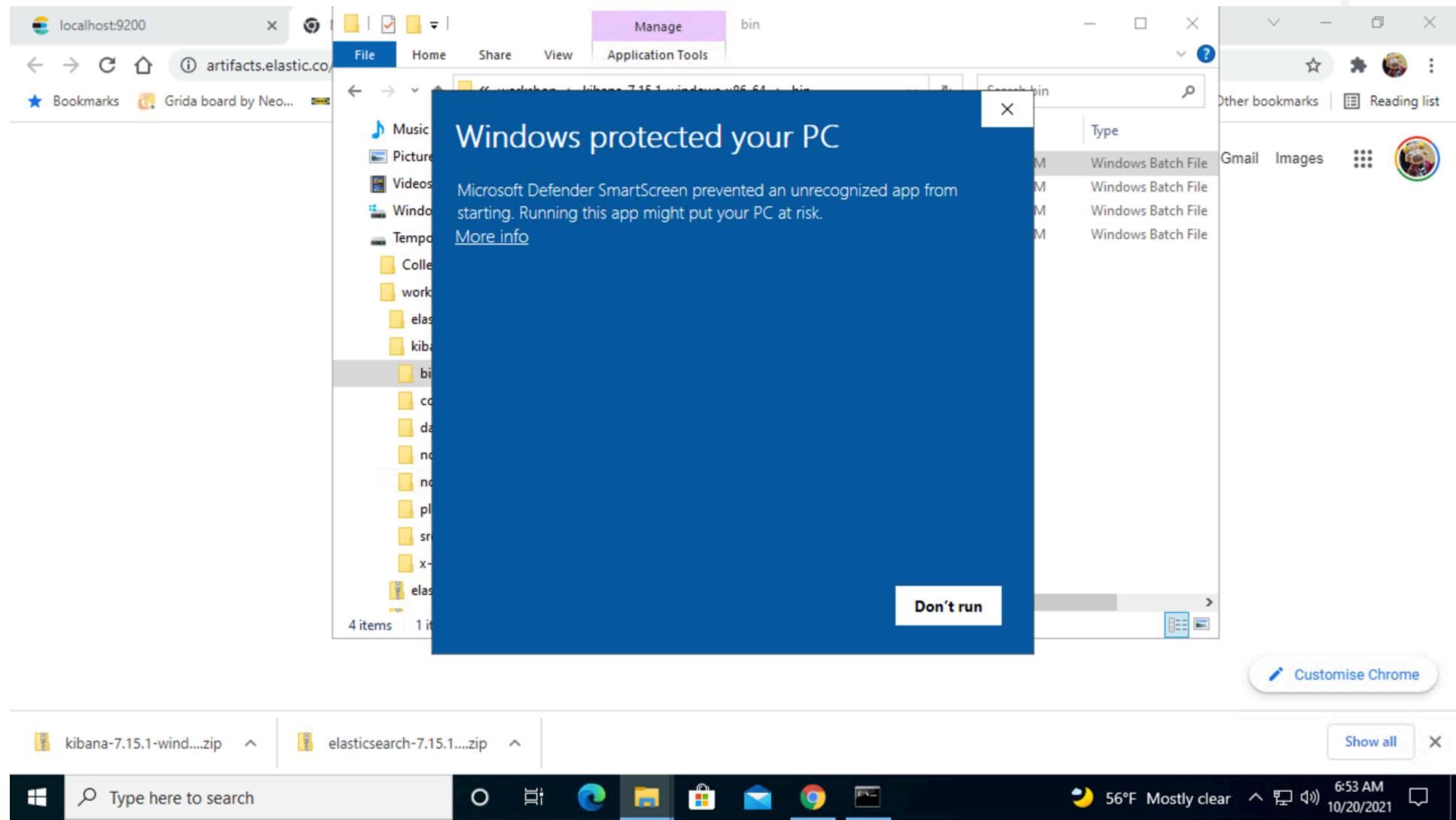
Install Kibana



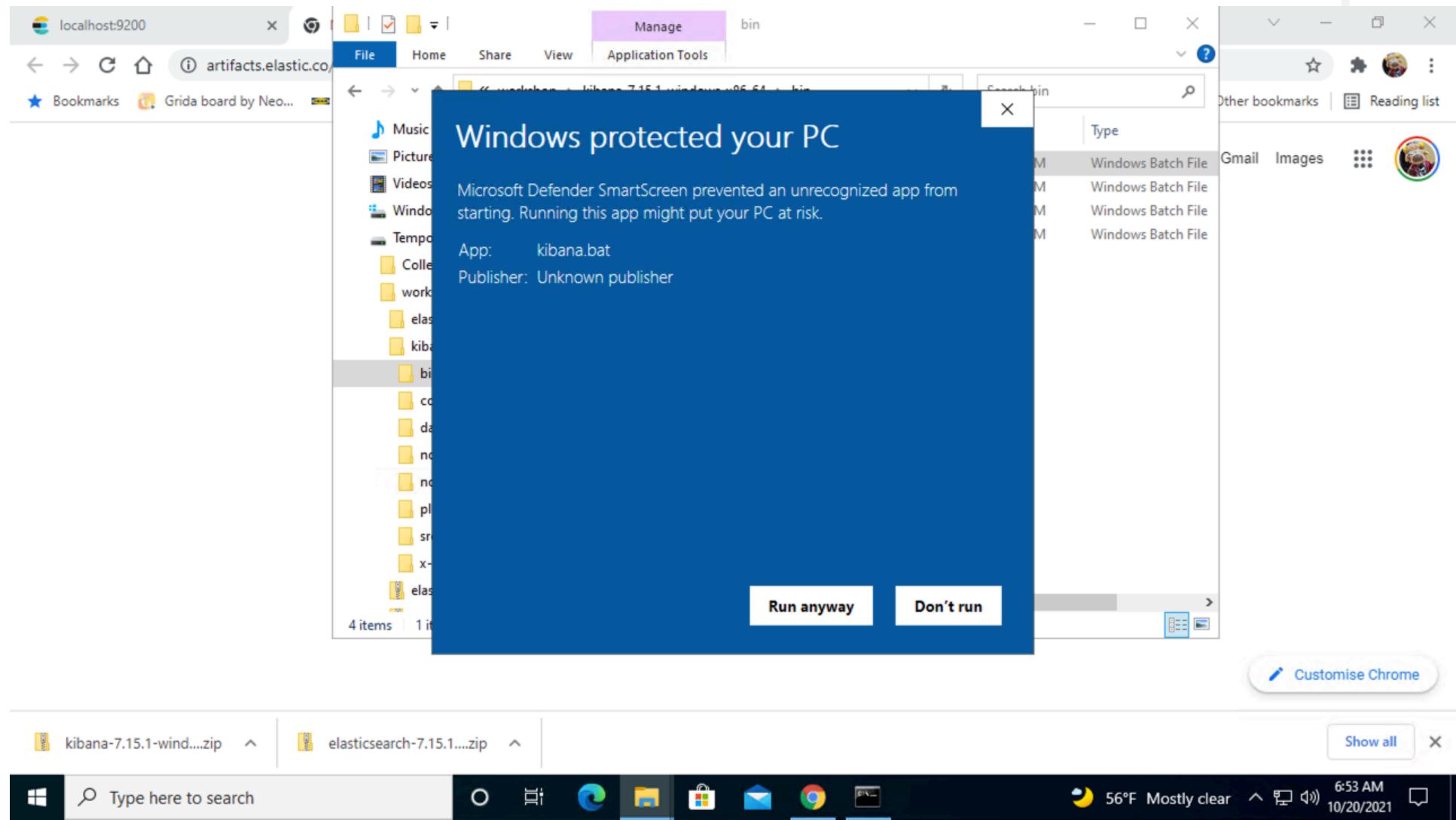
Install Kibana



Install Kibana



Install Kibana



Install Kibana

```
c:\Windows\system32\cmd.exe
log [06:54:12.025] [info][plugins-service] Plugin "metricsEntities" is disabled.
log [06:54:12.119] [info][server][Preboot][http] http server running at http://localhost:5601
log [06:54:12.197] [warning][config][deprecation] plugins.scanDirs is deprecated and is no longer used
log [06:54:12.212] [warning][config][deprecation] Config key [monitoring.cluster_alerts.email_notifications.email_address] will be required for email notifications to work in 8.0.
log [06:54:12.212] [warning][config][deprecation] "xpack.reporting.roles" is deprecated. Granting reporting privilege through a "reporting_user" role will not be supported starting in 8.0. Please set "xpack.reporting.roles.enabled" to "false" and grant reporting privileges to users using Kibana application privileges **Management > Security > Roles**.
log [06:54:12.212] [warning][config][deprecation] Session idle timeout ("xpack.security.session.idleTimeout") will be set to 1 hour by default in the next major version (8.0).
log [06:54:12.212] [warning][config][deprecation] Session lifespan ("xpack.security.session.lifespan") will be set to 30 days by default in the next major version (8.0).
log [06:54:12.415] [info][plugins-system][standard] Setting up [113] plugins: [translations,licensing,globalSearch,globalSearchProviders,banners,licenseApiGuard,code,usageCollection,xpackLegacy,taskManager,telemetryCollectionManager,telemetryCollectionXpack,kibanaUsageCollection,securityOss,share,screenshotMode,telemetry,newsfeed,mapsEms,mapsLegacy,legacyExport,kibanaLegacy,embeddable,uiActionsEnhanced,fieldFormats,expressions,charts,esUiShared,bfetch,data,savedObjects,visualizations,visTypeXY,visTypeVislib,visTypeTimelion,features,visTypeTagcloud,visTypeTable,visTypePie,visTypeMetric,visTypeMarkdown,tileMap,regionMap,presentationUtil,expressionShape,expressionRevealImage,expressionRepeatImage,expressionMetric,expressionImage,timelion,indexPatternFieldEditor,home,searchProfiler,painlessLab,grokdebugger,graph,visTypeVega,management,watcher,licenseManagement,indexPatternManagement,advancedSettings,discover,discoverEnhanced,dashboard,dashboardEnhanced,visualize,visTypeTimeseries,savedObjectsManagement,spaces,security,transform,savedObjectsTagging,lens,reporting,canvas,lists,ingestPipelines,fileUpload,maps,dataVisualizer,encryptedSavedObjects,dataEnhanced,dashboardMode,cloud,snapshotRestore,fleet,indexManagement,rollup,remoteClusters,crossClusterReplication,indexLifecycleManagement,eventLog,actions,alerting,triggersActionsUi,stackAlerts,ruleRegistry,osquery,ml,cases,timelines,securitySolutions,observability,uptime,infra,upgradeAssistant,monitoring,logstash,enterpriseSearch,console,apmOss,apm]
log [06:54:28.306] [info][plugins][taskManager] TaskManager is identified by the Kibana UUID: d6a9bbba-4264-496b-8e91-0a188b40de2d
log [06:54:28.791] [warning][config][plugins][security] Generating a random key for xpack.security.encryptionKey. To prevent sessions from being invalidated on restart, please set xpack.security.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
log [06:54:28.791] [warning][config][plugins][security] Session cookies will be transmitted over insecure connections. This is not recommended.
log [06:54:28.869] [warning][config][plugins][reporting] Generating a random key for xpack.reporting.encryptionKey. To prevent sessions from being invalidated on restart, please set xpack.reporting.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
log [06:54:28.900] [info][config][plugins][reporting] Chromium sandbox provides an additional layer of protection, and is supported for Win32 OS. Automatically enabling Chromium sandbox.
log [06:54:28.916] [warning][encryptedSavedObjects][plugins] Saved objects encryption key is not set. This will severely limit Kibana functionality. Please set xpack.encryptedSavedObjects.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
log [06:54:28.978] [warning][actions][plugins] APIs are disabled because the Encrypted Saved Objects plugin is missing encryption key. Please set xpack.encryptedSavedObjects.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
log [06:54:28.994] [warning][alerting][plugins] APIs are disabled because the Encrypted Saved Objects plugin is missing encryption key. Please set xpack.encryptedSavedObjects.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
log [06:54:29.025] [info][plugins][ruleRegistry] Write is disabled; not installing common resources shared between all indices
log [06:54:29.540] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.uptime.alerts
log [06:54:29.603] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.logs.alerts
log [06:54:29.665] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.metrics.alerts
log [06:54:29.697] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.apm.alerts
```

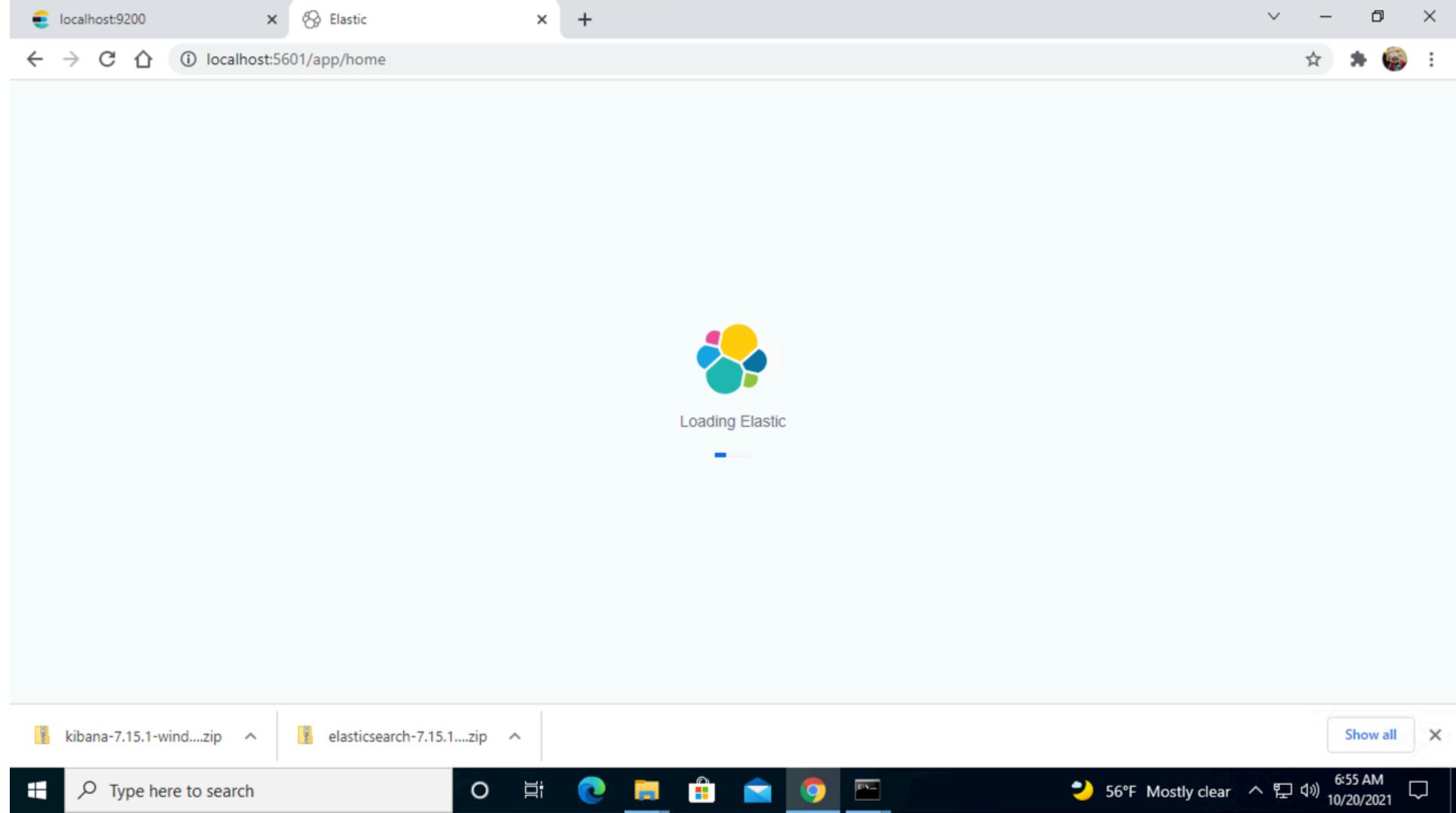


Install Kibana

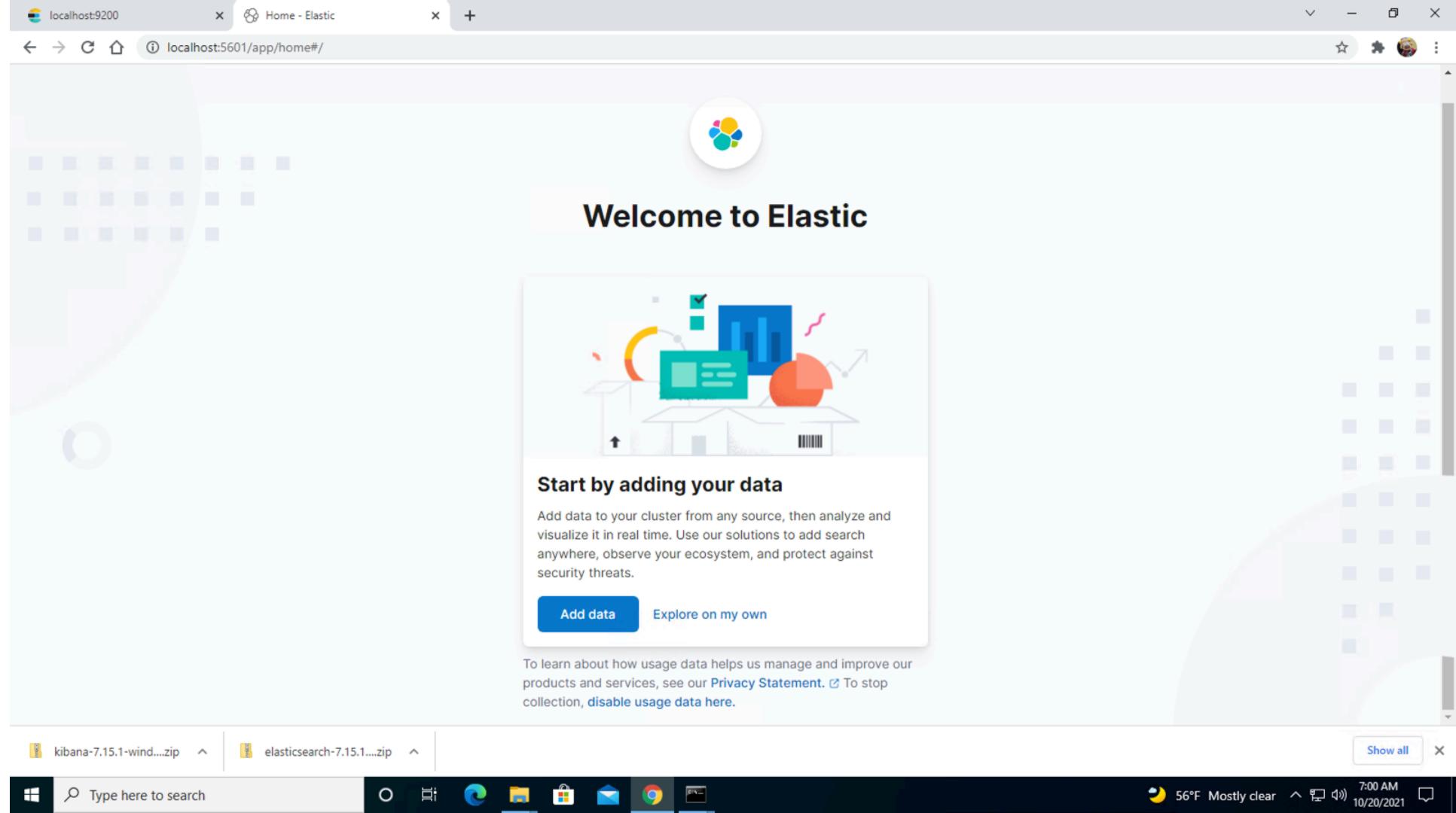
```
C:\Windows\system32\cmd.exe
encryptedSavedObjects.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
log [06:54:29.025] [info][plugins][ruleRegistry] Write is disabled; not installing common resources shared between all indices
log [06:54:29.540] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.uptime.alerts
log [06:54:29.603] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.logs.alerts
log [06:54:29.665] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.metrics.alerts
log [06:54:29.697] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.apm.alerts
log [06:54:29.853] [info][savedobjects-service] Waiting until all Elasticsearch nodes are compatible with Kibana before starting saved objects migrations
...
log [06:54:31.099] [info][savedobjects-service] Starting saved objects migrations
log [06:54:31.572] [info][savedobjects-service] [.kibana] INIT -> CREATE_NEW_TARGET. took: 360ms.
log [06:54:32.971] [info][savedobjects-service] [.kibana_task_manager] INIT -> CREATE_NEW_TARGET. took: 1759ms.
log [06:54:33.644] [info][savedobjects-service] [.kibana] CREATE_NEW_TARGET -> MARK_VERSION_INDEX_READY. took: 2072ms.
log [06:54:33.931] [info][savedobjects-service] [.kibana_task_manager] CREATE_NEW_TARGET -> MARK_VERSION_INDEX_READY. took: 960ms.
log [06:54:34.089] [info][savedobjects-service] [.kibana] MARK_VERSION_INDEX_READY -> DONE. took: 445ms.
log [06:54:34.134] [info][savedobjects-service] [.kibana] Migration completed after 2922ms
log [06:54:34.239] [info][savedobjects-service] [.kibana_task_manager] MARK_VERSION_INDEX_READY -> DONE. took: 308ms.
log [06:54:34.259] [info][savedobjects-service] [.kibana_task_manager] Migration completed after 3047ms
log [06:54:34.665] [info][plugins-system][standard] Starting [113] plugins: [translations,licensing,globalSearch,globalSearchProviders,banners,licenseApiGuard,code,usageCollection,xpackLegacy,taskManager,telemetryCollectionManager,telemetryCollectionXpack,kibanaUsageCollection,securityOss,share,screenshotMode,telemetry,newsfeed,mapsEms,mapsLegacy,legacyExport,kibanaLegacy,embeddable,uiActionsEnhanced,fieldFormats,expressions,charts,esUiShared,bfetch,data,savedObjects,visualizations,visTypeXy,visTypeVislib,visTypeTimelion,features,visTypeTagcloud,visTypeTable,visTypePie,visTypeMetric,visTypeMarkdown,tileMap,regionMap,presentationUtil,expressionShape,expressionRevealImage,expressionRepeatImage,expressionMetric,expressionImage,timelion,indexPatternFieldEditor,home,searchprofiler,painlessLab,grokdebugger,graph,visTypeVega,management,watcher,licenseManagement,indexPatternManagement,advancedSettings,discover,discoverEnhanced,dashboard,dashboardEnhanced,visualize,visTypeTimeseries,savedObjectsManagement,spaces,security,transform,savedObjectsTagging,lens,reporting,canvas,lists,ingestPipelines,fileUpload,maps,dataVisualizer,encryptedSavedObjects,dataEnhanced,dashboardMode,cloud,snapshotRestore,fleet,indexManagement,rollup,remoteClusters,crossClusterReplication,indexLifecycleManagement,eventLog,actions,alerting,triggersActionsUi,stackAlerts,ruleRegistry,osquery,ml,cases,timelines,securitySolution,observability,uptime,infra,upgradeAssistant,monitoring,logstash,enterpriseSearch,console,apmOss,apm]
log [06:54:34.759] [info][monitoring][monitoring][plugins] config sourced from: production cluster
log [06:54:38.510] [info][server][Kibana][http] http server running at http://localhost:5601
log [06:54:40.400] [info][kibana-monitoring][monitoring][plugins] Starting monitoring stats collection
log [06:54:41.838] [info][plugins][reporting] Browser executable: D:\workshop\kibana-7.15.1-windows-x86_64\x-pack\plugins\reporting\chromium\chrome-win\chrome.exe
log [06:54:42.478] [info][status] Kibana is now degraded
log [06:54:42.535] [info][plugins][reporting][store] Creating ILM policy for managing reporting indices: kibana-reporting
log [06:54:45.587] [info][plugins][securitySolution] Dependent plugin setup complete - Starting ManifestTask
log [06:54:51.832] [info][status] Kibana is now available (was degraded)
```



Install Kibana



Install Kibana



Install Kibana

The screenshot shows a web browser window with two tabs: 'localhost:9200' and 'Home - Elastic'. The main content is the 'Welcome home' page for the Elastic Stack. It features four main sections: 'Enterprise Search' (yellow card), 'Observability' (pink card), 'Security' (teal card), and 'Analytics' (blue card). Below these, there's a section titled 'Get started by adding your data' with a sub-section about ingest options. A decorative graphic of charts and arrows is positioned to the right of the text. At the bottom, there are download links for 'kibana-7.15.1-wind....zip' and 'elasticsearch-7.15.1....zip'. The Windows taskbar at the bottom includes the Start button, a search bar, and system icons.

Welcome home

Enterprise Search
Create search experiences with a refined set of APIs and tools.

Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding your data

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.

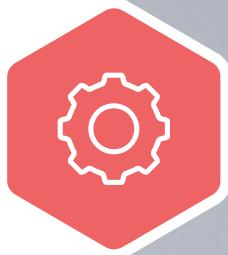
Add your data Try sample data

kibana-7.15.1-wind....zip elasticsearch-7.15.1....zip Show all

Type here to search

7:01 AM 56°F Mostly clear 10/20/2021





Try Sample Data for Kibana

Step by Step Installation

Try Sample Data from Kibana

The screenshot shows the Elastic Home page with several sections:

- Enterprise Search:** Create search experiences with a refined set of APIs and tools.
- Observability:** Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
- Security:** Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
- Analytics:** Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding your data

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.

[+ Add your data](#) [Try sample data](#)

Management

[Manage permissions](#) [Monitor the stack](#) [Back up and restore](#) [Manage index lifecycles](#)

[Dev Tools](#) [Stack Management](#)

localhost:5601/app/home#/tutorial_directory/sampleData

kibana-7.15.1-wind....zip elasticsearch-7.15.1....zip

Type here to search

7:01 AM 56°F Mostly clear 10/20/2021



Try Sample Data from Kibana

The screenshot shows a browser window with the Elastic Kibana interface. The address bar indicates the URL is localhost:5601/app/home#/tutorial_directory/sampleData. The page title is "elastic". The navigation bar includes links for All, Logs, Metrics, Security, Sample data (which is currently selected), and Upload file.

A prominent message box at the top left states: "Now generally available: Elastic Agent integrations. Elastic Agent integrations provide a simple, unified way to add monitoring for logs, metrics, and other types of data to your hosts. You no longer need to install multiple Beats, which makes it easier and faster to deploy policies across your infrastructure. For more information, read our [announcement blog post](#)." It includes "Try Integrations" and "Dismiss message" buttons.

The main content area displays three sample data sections:

- Sample eCommerce orders:** Shows visualizations for revenue (\$77,377.84), median spending (\$66.89), and average items sold (2.2). It also includes a chart for "Customer Lifetime Value".
- Sample flight data:** Shows visualizations for total flights (2,180), flight duration distribution, and a map of flight routes.
- Sample web logs:** Shows visualizations for visits (1,609), bounce rate (4.2%), and session duration (3.1%). It also includes a map of user locations.

Each sample section has an "Add data" button at the bottom right.

At the bottom of the browser window, there are two download links: "kibana-7.15.1-wind....zip" and "elasticsearch-7.15.1....zip". The taskbar at the bottom of the screen shows the Windows Start button, a search bar with placeholder "Type here to search", and several pinned icons (File Explorer, Mail, Google Chrome, Task View).



Try Sample Data from Kibana

The screenshot shows the Kibana interface running in a browser window. The title bar indicates the URL is `localhost:5601/app/home#/tutorial_directory/sampleData`. The top navigation bar includes tabs for All, Logs, Metrics, Security, Sample data (which is selected), and Upload file. A search bar says "Search Elastic". Below the navigation, there's a message about Elastic Agent integrations: "Now generally available: Elastic Agent integrations. Elastic Agent integrations provide a simple, unified way to add monitoring for logs, metrics, and other types of data to your hosts. You no longer need to install multiple Beats, which makes it easier and faster to deploy policies across your infrastructure. For more information, read our [announcement blog post](#)". Buttons for "Try Integrations" and "Dismiss message" are present.

Sample eCommerce orders
Sample data, visualizations, and dashboards for tracking eCommerce orders.

Sample flight data
Sample data, visualizations, and dashboards for monitoring flight routes.

Sample web logs
Sample data, visualizations, and dashboards for monitoring web logs.

At the bottom, there are two download links: "kibana-7.15.1-wind....zip" and "elasticsearch-7.15.1....zip". The taskbar at the bottom of the screen shows the Windows Start button, a search bar, and various pinned icons. The system tray shows the date and time as "7:14 AM 10/20/2021".



Try Sample Data from Kibana

The screenshot shows a browser window with the Elastic Stack interface. The address bar indicates the URL is localhost:5601/app/home#/tutorial_directory/sampleData. The page title is "elastic". The navigation bar includes links for All, Logs, Metrics, Security, Sample data (which is currently selected), and Upload file.

A prominent message box通知 (Notification) states: "Now generally available: Elastic Agent integrations. Elastic Agent integrations provide a simple, unified way to add monitoring for logs, metrics, and other types of data to your hosts. You no longer need to install multiple Beats, which makes it easier and faster to deploy policies across your infrastructure. For more information, read our [announcement blog post](#)". It includes "Try Integrations" and "Dismiss message" buttons.

The main content area displays three sample data sections:

- Sample eCommerce orders**: Shows visualizations for revenue (\$77,377.84), median spending (\$66.89), and average items sold (2.2). It also includes a chart for average purchase value.
- Sample flight data**: Shows visualizations for total flights (2,180), flight duration distribution, and top destination cities.
- Sample web logs**: Shows visualizations for visits (1,609), bounce rate (4.2%), and session duration (3.1%). It includes a map visualization.

The "Sample web logs" section has a "Remove" button and a confirmation message: "✓ Sample web logs installed".

At the bottom of the browser window, there are two download links: "kibana-7.15.1-wind....zip" and "elasticsearch-7.15.1....zip". The taskbar at the bottom of the screen shows the Windows Start button, a search bar with "Type here to search", and several pinned icons (File Explorer, Edge, Mail, Google Chrome, File History).



Try Sample Data from Kibana

The screenshot shows the Kibana interface running in a browser window. The title bar indicates the URL is localhost:5601/app/home#/tutorial_directory/sampleData. The top navigation bar includes tabs for All, Logs, Metrics, Security, Sample data (which is selected), and Upload file. A search bar says "Search Elastic". On the left, there's a sidebar with a "D" icon and a "Home" button.

A prominent message box at the top left says: "Now generally available: Elastic Agent integrations. Elastic Agent integrations provide a simple, unified way to add monitoring for logs, metrics, and other types of data to your hosts. You no longer need to install multiple Beats, which makes it easier and faster to deploy policies across your infrastructure. For more information, read our [announcement blog post](#)". It has "Try Integrations" and "Dismiss message" buttons.

Three main card sections are displayed:

- Sample eCommerce orders**: Shows visualizations for revenue (\$77,377.84), median spending (\$66.89), and average items sold (2.2). It includes a "Add data" button.
- Sample flight data**: Shows visualizations for total flights (2,180), completion rates (24.5% Design, 12.8% Downloaded, 37.2% Unknown), and flight types. It includes a "Add data" button.
- Sample web logs**: Shows visualizations for visits (1,609), bounce rate (4.2%), and session duration (3.1%). It includes a "Remove" and "View data" button, and a dropdown menu for "Dashboard", "Canvas", "Map", and "Logs".

At the bottom, there are download links for "kibana-7.15.1-wind....zip" and "elasticsearch-7.15.1....zip". The Windows taskbar shows the Start button, a search bar, and icons for File Explorer, Mail, and Google Chrome. The system tray shows the date (10/20/2021), time (7:15 AM), battery level, and weather (56°F Mostly clear).



Try Sample Data from Kibana

localhost:9200 [Logs] Web Traffic - Elastic

localhost:5601/app/dashboards#/view/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:![],refreshInterval:(pause:if,value:900000),time:(from:now-7d,to:now))

elastic

Dashboard [Logs] Web Traffic

Search KQL Last 7 days

+ Add filter

Sample Logs 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](#).

Source Country Select... OS Select...

1,620 Visits

811 Unique Visitors

4.8% HTTP 4xx

2.8% HTTP 5xx

[Logs] Response Codes Over Time + Annotations

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

2021-10-13 12:00 2021-10-14 12:00 2021-10-15 12:00 2021-10-16 12:00 2021-10-17 12:00 per 4 hours

● HTTP 5xx ● HTTP 4xx

Warning: 299 Elasticsearch-7.15.1-83c34f456ae29d60e94d886e455e6a3409bba9ed "Elasticsearch built-in security features are not enabled. Without authentication, your cluster could be accessible to anyone. See <https://www.elastic.co/guide/en/elasticsearch/reference/7.15/security-minimal-setup.html> to enable security."

Warning: 299 Elasticsearch-7.15.1-83c34f456ae29d60e94d886e455e6a3409bba9ed "Elasticsearch built-in security features are not enabled. Without authentication, your cluster could be accessible to anyone. See <https://www.elastic.co/guide/en/elasticsearch/reference/7.15/security-minimal-setup.html> to enable security."

kibana-7.15.1-wind....zip elasticsearch-7.15.1....zip Show all

Type here to search

56°F Mostly clear 7:16 AM 10/20/2021



Try Sample Data from Kibana

localhost:9200 [Logs] Web Traffic - Elastic + [localhost:5601/app/dashboards#/view/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=\(filters:!\(\),refreshInterval:\(pause:if,value:900000\),time:\(from:now-7d,to:now\)\)](localhost:5601/app/dashboards#/view/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:!(),refreshInterval:(pause:if,value:900000),time:(from:now-7d,to:now)))

elastic Search Elastic Full screen Share Clone Edit

Dashboard [Logs] Web Traffic KQL Last 7 days Show dates Refresh

+ Add filter

Sample Logs 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](#).

[Logs] Goals

1,620 Visits

811 Unique Visitors

4.8% HTTP 4xx

2.8% HTTP 5xx

[Logs] Response Codes Over Time + Annotations

2021-10-13 12:00 2021-10-14 12:00 2021-10-15 12:00 2021-10-16 12:00 2021-10-17 12:00 2021-10-18 12:00 2021-10-19 12:00
per 4 hours

* ● HTTP 5xx 0% ■ HTTP 4xx 0% ● HTTP 2xx and 3xx 100%

kibana-7.15.1-wind....zip elasticsearch-7.15.1....zip Show all

Type here to search 7:17 AM 56°F Mostly clear 10/20/2021





Disabled Security Features

Step by Step Installation

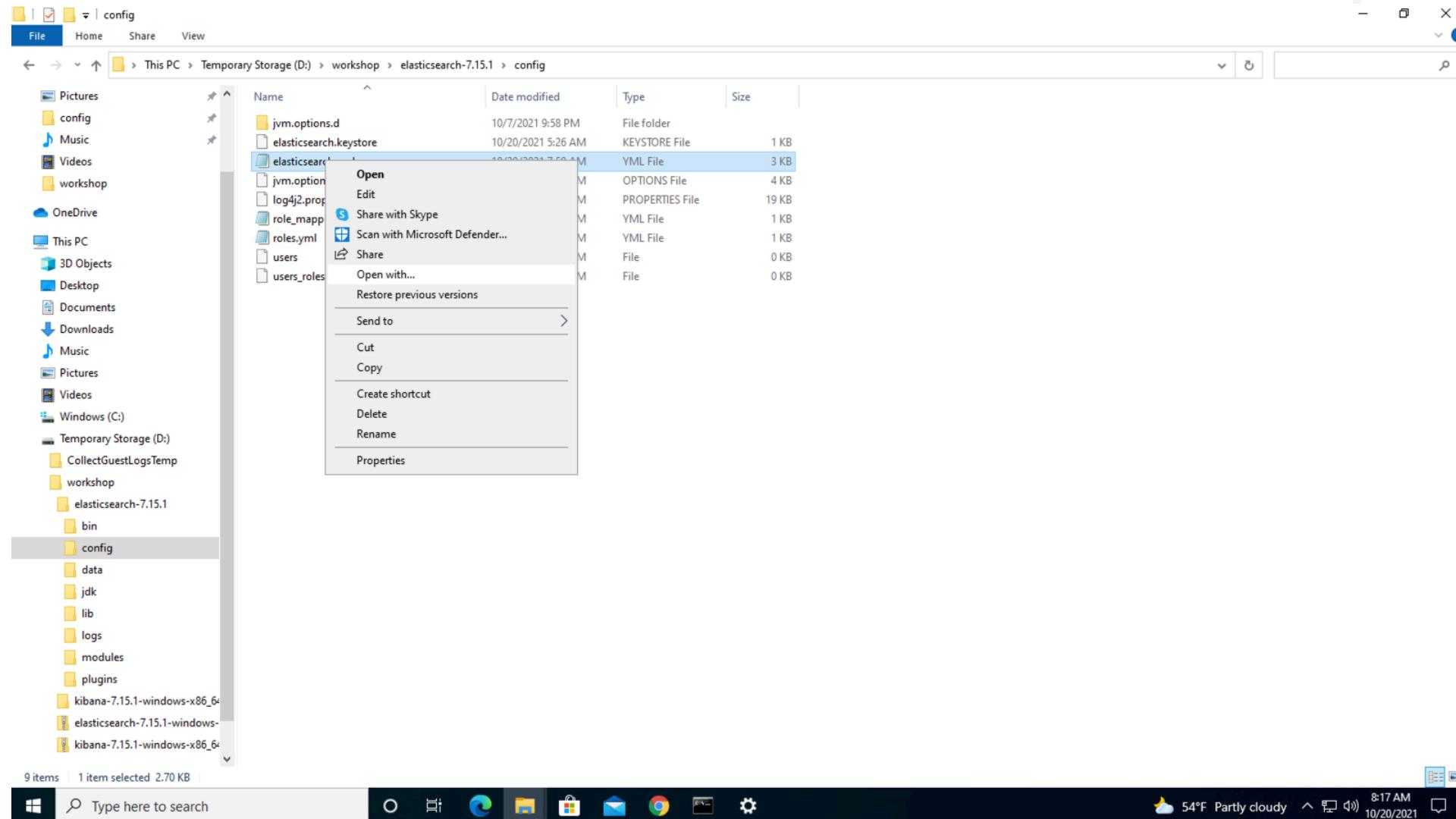
Disable Security features in Elasticsearch



```
C:\Windows\system32\cmd.exe
5 [1]/[1]
[2021-10-20T06:54:44,247][INFO ][o.e.c.r.a.AllocationService] [my-windows] updating number_of_replicas to [0] for indices [.kibana-event-log-7.15.1-000001]
[2021-10-20T06:54:44,423][INFO ][o.e.x.i.IndexLifecycleTransition] [my-windows] moving index [.kibana-event-log-7.15.1-000001] from [null] to [{"phase":"new","action":"complete","name":"complete"}] in policy [.kibana-event-log-policy]
[2021-10-20T06:54:44,766][INFO ][o.e.c.r.a.AllocationService] [my-windows] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.kibana-event-log-7.15.1-000001][0]]])
[2021-10-20T06:54:45,152][INFO ][o.e.x.i.IndexLifecycleTransition] [my-windows] moving index [.kibana-event-log-7.15.1-000001] from [{"phase":"new","action":"complete","name":"complete"}] to [{"phase":"hot","action":"unfollow","name":"branch-check-unfollow-prerequisites"}] in policy [.kibana-event-log-policy]
[2021-10-20T06:54:45,324][INFO ][o.e.x.i.IndexLifecycleTransition] [my-windows] moving index [.kibana-event-log-7.15.1-000001] from [{"phase":"hot","action":"unfollow","name":"branch-check-unfollow-prerequisites"}] to [{"phase":"hot","action":"rollover","name":"check-rollover-ready"}] in policy [.kibana-event-log-policy]
[2021-10-20T06:54:46,522][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T06:54:49,091][INFO ][o.e.c.m.MetadataCreateIndexService] [my-windows] [.ds-ilm-history-5-2021.10.20-000001] creating index, cause [initialize_data_stream], templates [ilm-history], shards [1]/[0]
[2021-10-20T06:54:49,106][INFO ][o.e.c.m.MetadataCreateDataStreamService] [my-windows] adding data stream [ilm-history-5] with write index [.ds-ilm-history-5-2021.10.20-000001], backing indices [], and aliases []
[2021-10-20T06:54:49,391][INFO ][o.e.x.i.IndexLifecycleTransition] [my-windows] moving index [.ds-ilm-history-5-2021.10.20-000001] from [null] to [{"phase":"new","action":"complete","name":"complete"}] in policy [ilm-history-ilm-policy]
[2021-10-20T06:54:49,596][INFO ][o.e.c.r.a.AllocationService] [my-windows] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.ds-ilm-history-5-2021.10.20-000001][0]]])
[2021-10-20T06:54:49,836][INFO ][o.e.x.i.IndexLifecycleTransition] [my-windows] moving index [.ds-ilm-history-5-2021.10.20-000001] from [{"phase":"new","action":"complete","name":"complete"}] to [{"phase":"hot","action":"unfollow","name":"branch-check-unfollow-prerequisites"}] in policy [ilm-history-ilm-policy]
[2021-10-20T06:54:50,024][INFO ][o.e.x.i.IndexLifecycleTransition] [my-windows] moving index [.ds-ilm-history-5-2021.10.20-000001] from [{"phase":"hot","action":"unfollow","name":"branch-check-unfollow-prerequisites"}] to [{"phase":"hot","action":"rollover","name":"check-rollover-ready"}] in policy [ilm-history-ilm-policy]
[2021-10-20T06:55:32,933][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T06:56:34,000][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:00,484][INFO ][o.e.c.m.MetadataCreateIndexService] [my-windows] [.kibana_sample_data_logs] creating index, cause [api], templates [], shards [1]/[1]
[2021-10-20T07:14:00,488][INFO ][o.e.c.r.a.AllocationService] [my-windows] updating number_of_replicas to [0] for indices [.kibana_sample_data_logs]
[2021-10-20T07:14:00,723][INFO ][o.e.c.r.a.AllocationService] [my-windows] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.kibana_sample_data_logs][0]]])
[2021-10-20T07:14:00,941][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_sample_data_logs/AAvjPRL2S9GzKaZfStCR9Q] update_mapping [_doc]
[2021-10-20T07:14:11,884][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:12,127][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:12,405][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:12,780][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:12,989][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:13,289][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:13,539][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:14:13,823][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:15:50,239][INFO ][o.e.c.m.MetadataCreateIndexService] [my-windows] [.async-search] creating index, cause [api], templates [], shards [1]/[0]
[2021-10-20T07:15:51,081][INFO ][o.e.c.r.a.AllocationService] [my-windows] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.async-search][0]]])
[2021-10-20T07:15:56,156][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
[2021-10-20T07:15:56,653][INFO ][o.e.c.m.MetadataMappingService] [my-windows] [.kibana_7.15.1_001/Eg2vPurlTzy6VFWvAH0t3A] update_mapping [_doc]
```

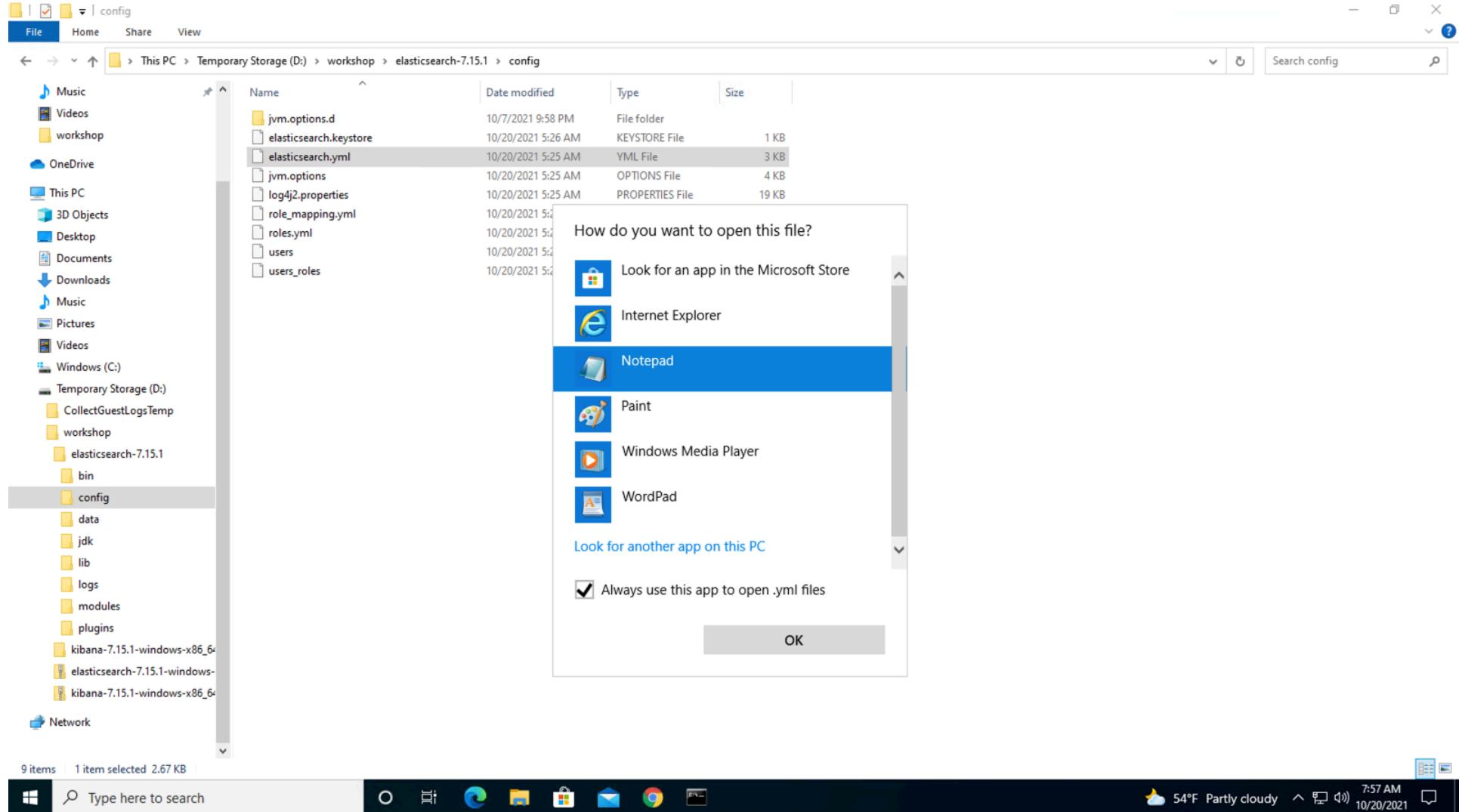


Disable Security features in Elasticsearch

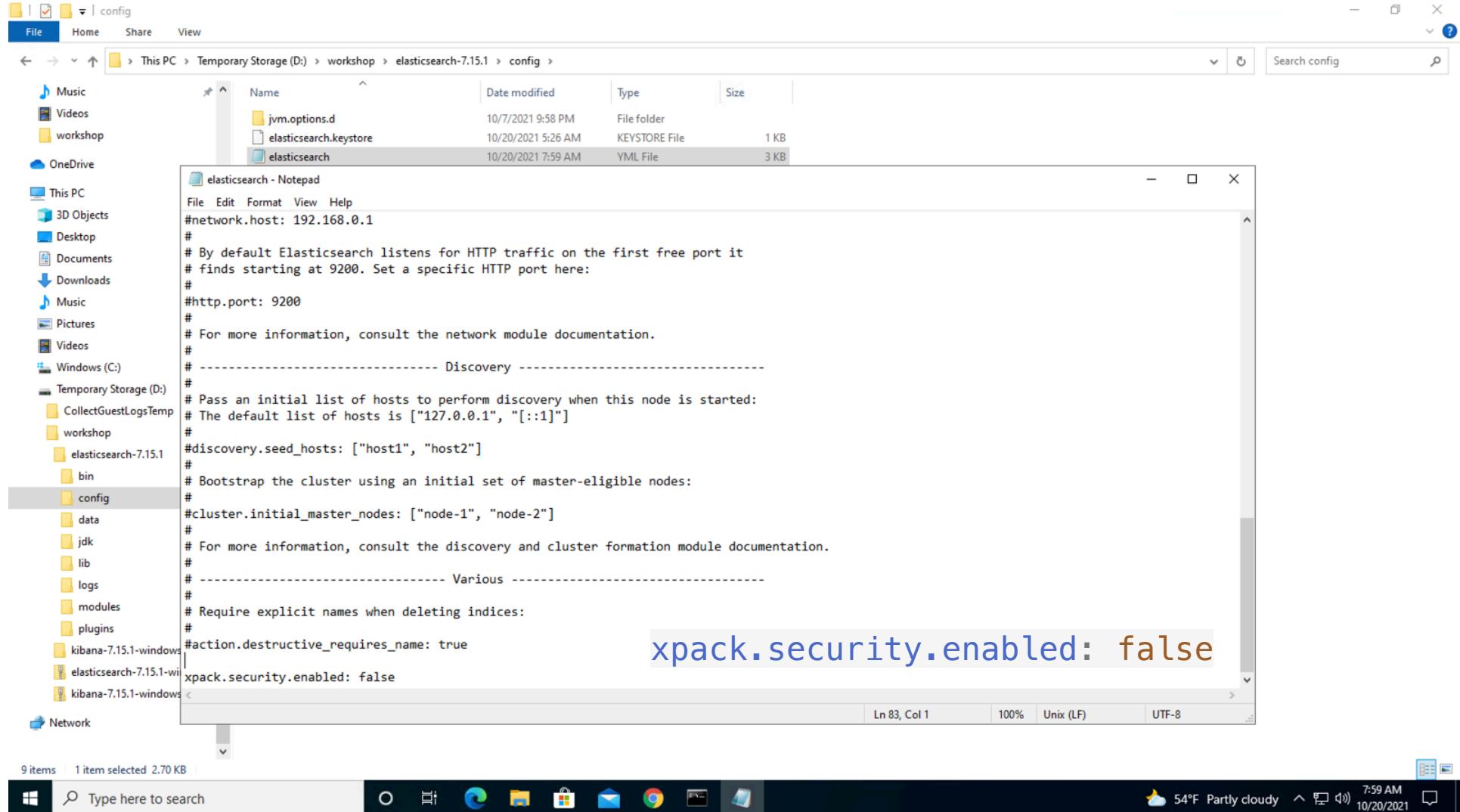


xpack.security.enabled: false

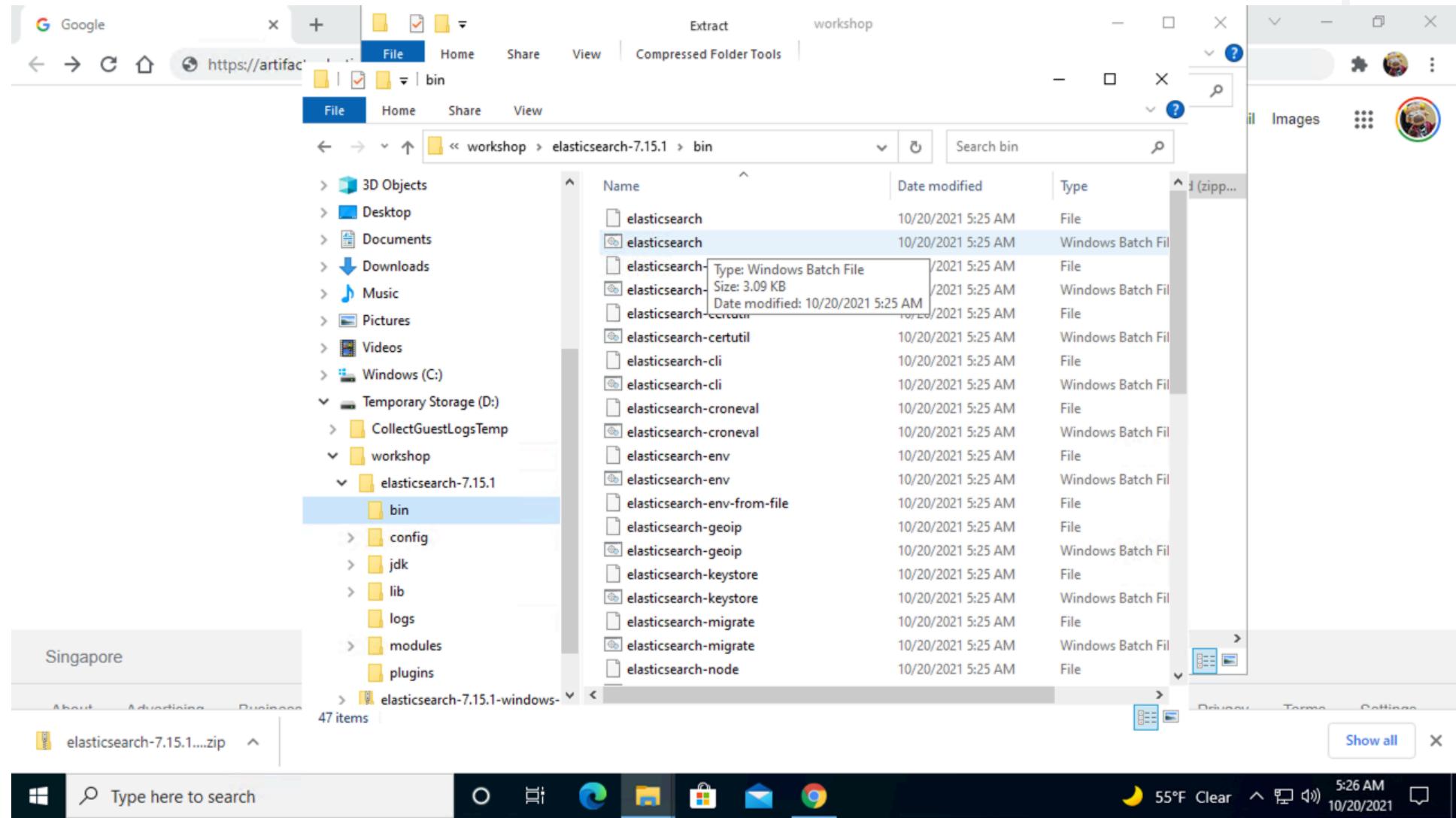
Disable Security features in Elasticsearch



Disable Security features in Elasticsearch



Disable Security features in Elasticsearch

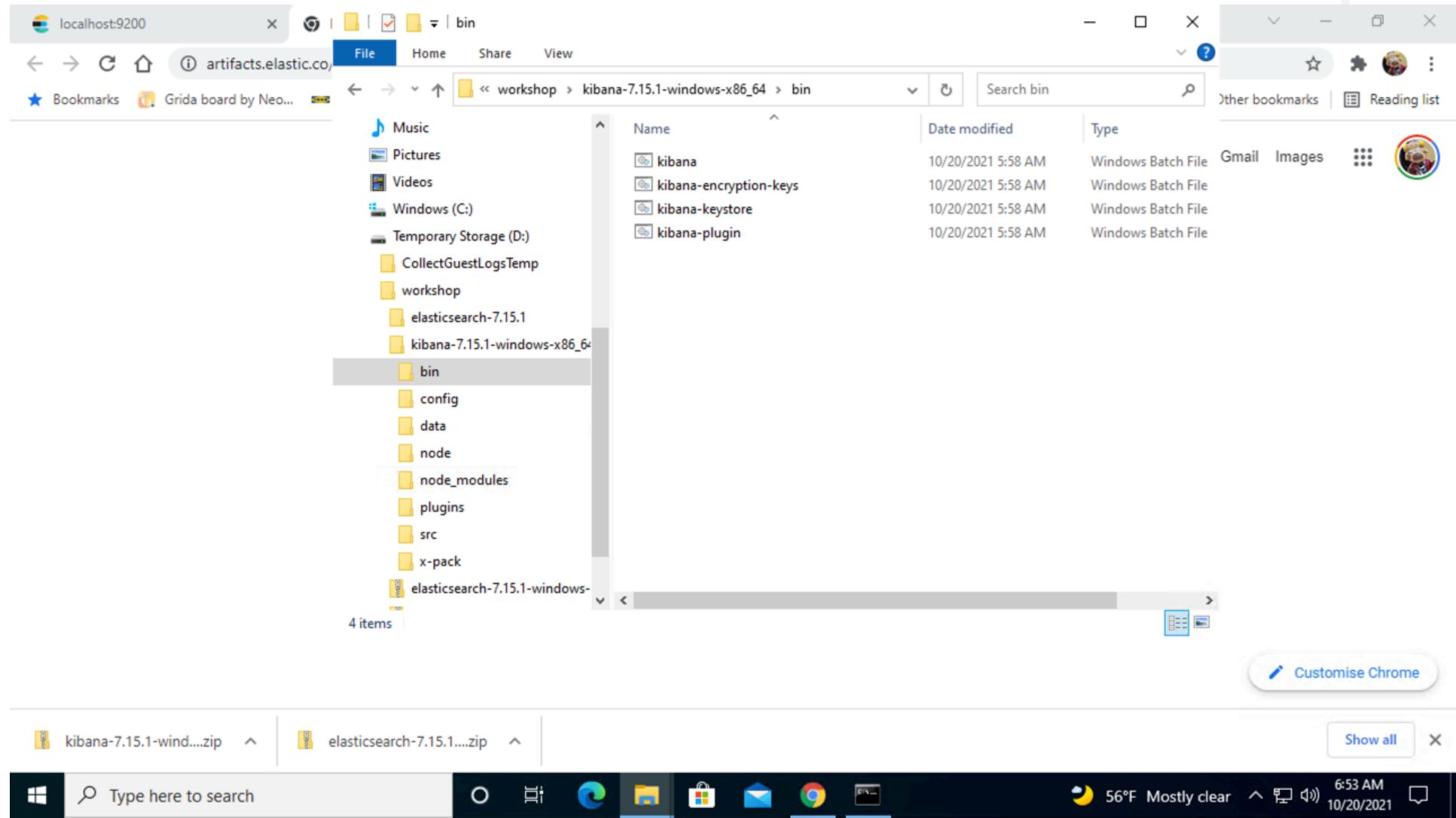


Disable Security features in Elasticsearch

```
c:\Windows\system32\cmd.exe
[2021-10-20T05:27:28,944][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [ilm-history-ilm-policy]
[2021-10-20T05:27:29,163][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [slm-history-ilm-policy]
[2021-10-20T05:27:29,320][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [.deprecation-indexing-ilm-policy]
[2021-10-20T05:27:29,460][INFO ][o.e.x.i.a.TransportPutLifecycleAction] [my-windows] adding index lifecycle policy [.fleet-actions-results-ilm-policy]
[2021-10-20T05:27:29,757][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip databases
[2021-10-20T05:27:29,819][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] fetching geoip databases overview from [https://geoip.elastic.co/v1/database?elastic_geoip_service_tos=agree]
[2021-10-20T05:27:30,023][INFO ][o.e.l.LicenseService      ] [my-windows] license [f7846eb3-417c-4f18-af06-56360a712d2f] mode [basic] - valid
[2021-10-20T05:27:30,023][INFO ][o.e.x.s.s.SecurityStatusChangeListener] [my-windows] Active license is now [BASIC]; Security is disabled
[2021-10-20T05:27:30,023][WARN ][o.e.x.s.s.SecurityStatusChangeListener] [my-windows] Elasticsearch built-in security features are not enabled. Without authentication, your cluster could be accessible to anyone. See https://www.elastic.co/guide/en/elasticsearch/reference/7.15/security-minimal-setup.html to enable security.
[2021-10-20T05:27:31,111][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip database [GeoLite2-ASN.mmdb]
[2021-10-20T05:27:31,760][INFO ][o.e.c.m.MetadataCreateIndexService] [my-windows] [.geoip_databases] creating index, cause [auto(bulk api)], templates [], shards [1]/[0]
[2021-10-20T05:27:32,241][INFO ][o.e.c.r.a.AllocationService] [my-windows] Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[.geoip_databases][0]]]).
[2021-10-20T05:27:33,334][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] downloading geoip database [GeoLite2-ASN.mmdb] to [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-ASN.mmdb.tmp.gz]
[2021-10-20T05:27:33,398][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updated geoip database [GeoLite2-ASN.mmdb]
[2021-10-20T05:27:33,429][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip database [GeoLite2-City.mmdb]
[2021-10-20T05:27:33,788][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] successfully reloaded changed geoip database file [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-ASN.mmdb]
[2021-10-20T05:27:37,257][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] downloading geoip database [GeoLite2-City.mmdb] to [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-City.mmdb.tmp.gz]
[2021-10-20T05:27:37,288][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updated geoip database [GeoLite2-City.mmdb]
[2021-10-20T05:27:37,382][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updating geoip database [GeoLite2-Country.mmdb]
[2021-10-20T05:27:38,724][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] downloading geoip database [GeoLite2-Country.mmdb] to [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-Country.mmdb.tmp.gz]
[2021-10-20T05:27:38,773][INFO ][o.e.i.g.GeoIpDownloader ] [my-windows] updated geoip database [GeoLite2-Country.mmdb]
[2021-10-20T05:27:38,976][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] successfully reloaded changed geoip database file [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-Country.mmdb]
[2021-10-20T05:27:39,257][INFO ][o.e.i.g.DatabaseRegistry ] [my-windows] successfully reloaded changed geoip database file [C:\Users\karan\AppData\Local\Temp\elasticsearch\geoip-databases\9K_JwxSYSdehLKD5-eEMw\GeoLite2-City.mmdb]
```



Disable Security features in Elasticsearch

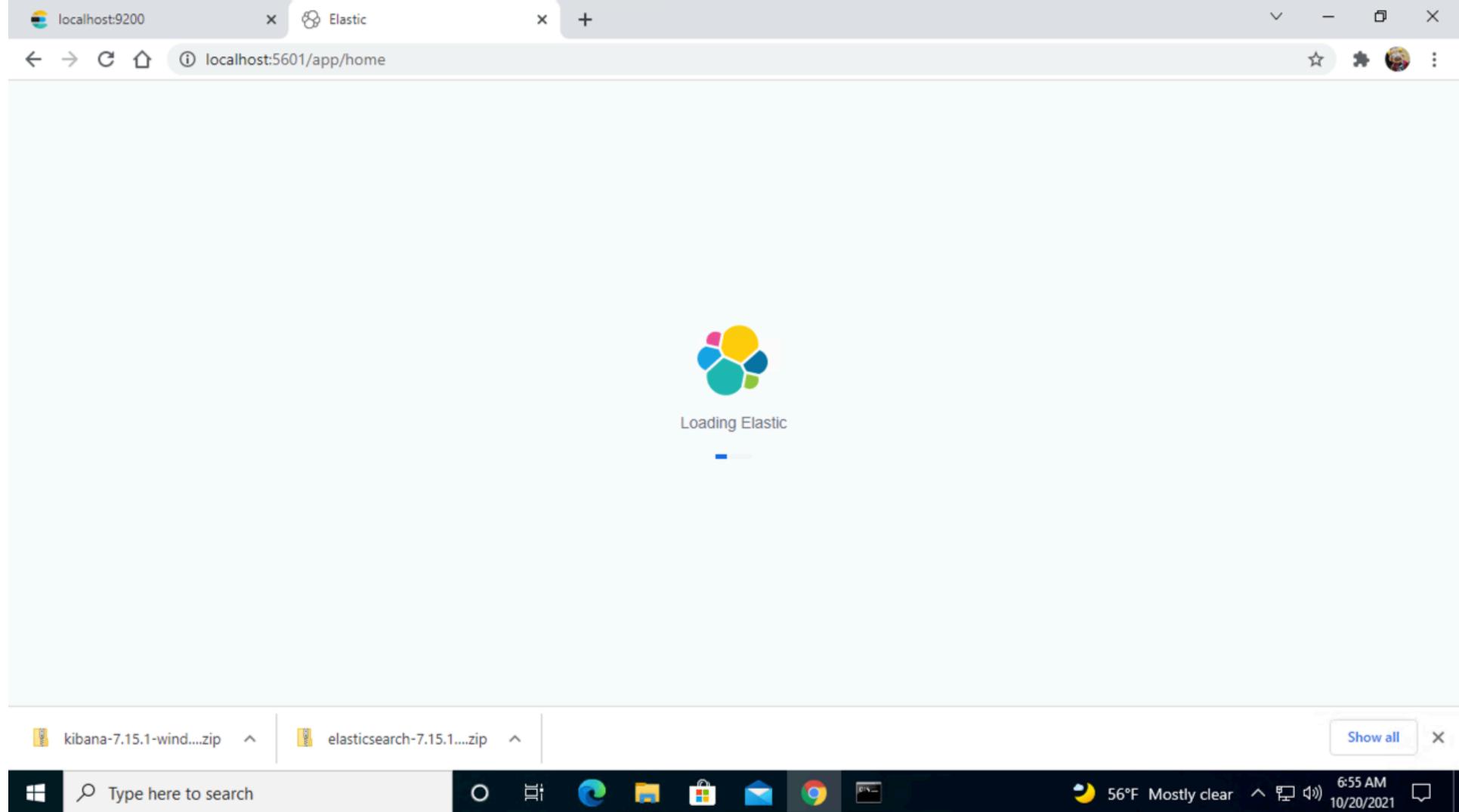


Disable Security features in Elasticsearch

```
C:\Windows\system32\cmd.exe
encryptedSavedObjects.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
log [06:54:29.025] [info][plugins][ruleRegistry] Write is disabled; not installing common resources shared between all indices
log [06:54:29.540] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.uptime.alerts
log [06:54:29.603] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.logs.alerts
log [06:54:29.665] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.metrics.alerts
log [06:54:29.697] [info][plugins][ruleRegistry] Write is disabled; not installing resources for index .alerts-observability.apm.alerts
log [06:54:29.853] [info][savedobjects-service] Waiting until all Elasticsearch nodes are compatible with Kibana before starting saved objects migrations
...
log [06:54:31.099] [info][savedobjects-service] Starting saved objects migrations
log [06:54:31.572] [info][savedobjects-service] [.kibana] INIT -> CREATE_NEW_TARGET. took: 360ms.
log [06:54:32.971] [info][savedobjects-service] [.kibana_task_manager] INIT -> CREATE_NEW_TARGET. took: 1759ms.
log [06:54:33.644] [info][savedobjects-service] [.kibana] CREATE_NEW_TARGET -> MARK_VERSION_INDEX_READY. took: 2072ms.
log [06:54:33.931] [info][savedobjects-service] [.kibana_task_manager] CREATE_NEW_TARGET -> MARK_VERSION_INDEX_READY. took: 960ms.
log [06:54:34.089] [info][savedobjects-service] [.kibana] MARK_VERSION_INDEX_READY -> DONE. took: 445ms.
log [06:54:34.134] [info][savedobjects-service] [.kibana] Migration completed after 2922ms
log [06:54:34.239] [info][savedobjects-service] [.kibana_task_manager] MARK_VERSION_INDEX_READY -> DONE. took: 308ms.
log [06:54:34.259] [info][savedobjects-service] [.kibana_task_manager] Migration completed after 3047ms
log [06:54:34.665] [info][plugins-system][standard] Starting [113] plugins: [translations,licensing,globalSearch,globalSearchProviders,banners,licenseApiGuard,code,usageCollection,xpackLegacy,taskManager,telemetryCollectionManager,telemetryCollectionXpack,kibanaUsageCollection,securityOss,share,screenshotMode,telemetry,newsfeed,mapsEms,mapsLegacy,legacyExport,kibanaLegacy,embeddable,uiActionsEnhanced,fieldFormats,expressions,charts,esUiShared,bfetch,data,savedObjects,visualizations,visTypeXy,visTypeVislib,visTypeTimeline,features,visTypeTagcloud,visTypeTable,visTypePie,visTypeMetric,visTypeMarkdown,tileMap,regionMap,presentationUtil,expressionShape,expressionRevealImage,expressionRepeatImage,expressionMetric,expressionImage,timelion,indexPatternFieldEditor,home,searchprofiler,painlessLab,grokdebugger,graph,visTypeVega,management,watcher,licenseManagement,indexPatternManagement,advancedSettings,discover,discoverEnhanced,dashboard,dashboardEnhanced,visualize,visTypeTimeseries,savedObjectsManagement,spaces,security,transform,savedObjectsTagging,lens,reporting,canvas,lists,ingestPipelines,fileUpload,maps,dataVisualizer,encryptedSavedObjects,dataEnhanced,dashboardMode,cloud,snapshotRestore,fleet,indexManagement,rollup,remoteClusters,crossClusterReplication,indexLifecycleManagement,eventLog,actions,alerting,triggersActionsUi,stackAlerts,ruleRegistry,osquery,ml,cases,timelines,securitySolution,observability,uptime,infra,upgradeAssistant,monitoring,logstash,enterpriseSearch,console,apmOss,apm]
log [06:54:34.759] [info][monitoring][monitoring][plugins] config sourced from: production cluster
log [06:54:38.510] [info][server][Kibana][http] http server running at http://localhost:5601
log [06:54:40.400] [info][kibana-monitoring][monitoring][plugins] Starting monitoring stats collection
log [06:54:41.838] [info][plugins][reporting] Browser executable: D:\workshop\kibana-7.15.1-windows-x86_64\x-pack\plugins\reporting\chromium\chrome-win\chrome.exe
log [06:54:42.478] [info][status] Kibana is now degraded
log [06:54:42.535] [info][plugins][reporting][store] Creating ILM policy for managing reporting indices: kibana-reporting
log [06:54:45.587] [info][plugins][securitySolution] Dependent plugin setup complete - Starting ManifestTask
log [06:54:51.832] [info][status] Kibana is now available (was degraded)
```



Disable Security features in Elasticsearch



Disable Security features in Elasticsearch

The screenshot shows the Elasticsearch Home page at localhost:5601/app/home/. The page has a dark header with the elastic logo and a search bar. Below the header, there's a navigation bar with a menu icon, a 'D' button, and a 'Home' button.

The main content area features a 'Welcome home' message and four cards:

- Enterprise Search**: Create search experiences with a refined set of APIs and tools.
- Observability**: Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
- Security**: Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
- Analytics**: Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Below these cards, there's a section titled 'Get started by adding your data' with a sub-section about ingest options. A decorative graphic of charts and arrows is positioned next to this text.

At the bottom, there are download links for 'kibana-7.15.1-wind....zip' and 'elasticsearch-7.15.1....zip'. The Windows taskbar at the bottom includes the Start button, a search bar, and various pinned icons like File Explorer, Mail, and Google Chrome. The system tray shows the date and time as '7:01 AM 10/20/2021'.



Disable Security features in Elasticsearch

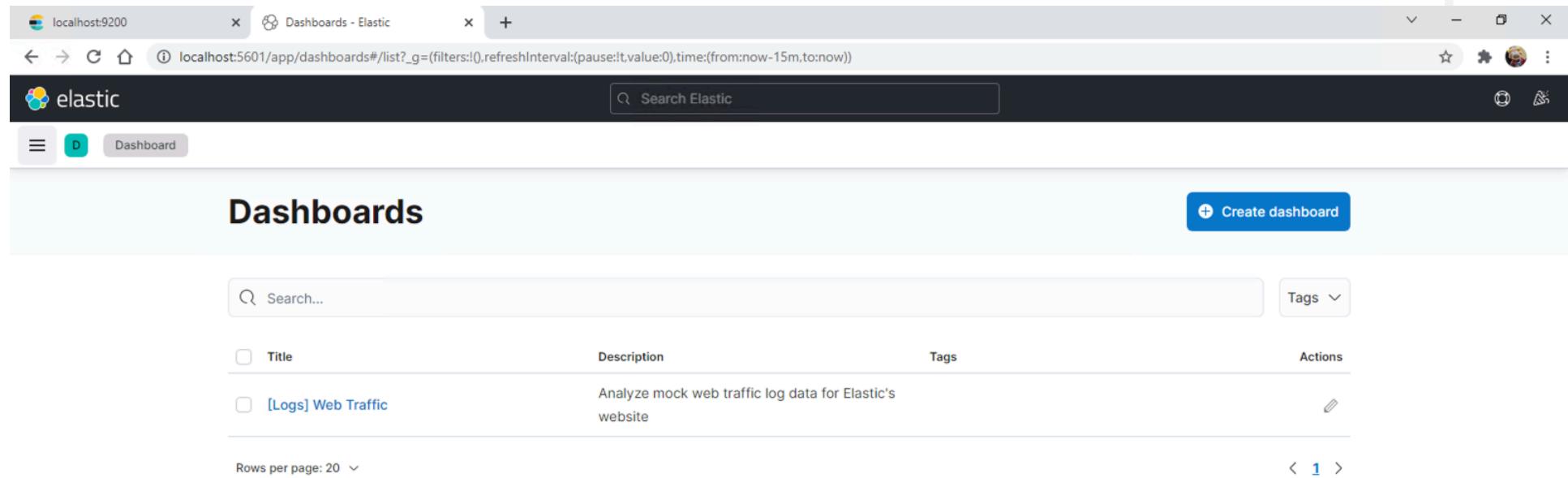
The screenshot shows the Elasticsearch Kibana interface on a Windows desktop. The browser tabs include 'localhost:9200', 'Home - Elastic', and 'Dashboard and visualizations | Kibana'. The main content area displays the 'Home' dashboard with the following sections:

- Enterprise Search**: Create search experiences with a defined set of APIs and tools.
- Observability**: Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
- Security**: Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
- Analytics**: Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

On the left sidebar, under the 'Analytics' section, the 'Dashboard' item is selected. Below it, other options like 'Discover', 'Canvas', 'Maps', 'Machine Learning', and 'Visualize Library' are listed. Under 'Enterprise Search', options for 'Overview', 'App Search', and 'Workplace Search' are shown. The status bar at the bottom shows the URL 'localhost:5601/app/dashboards#/view/edf84fe0-e1a0-11e7-b6d5-4dc382ef7f5b?_g=(filters:[],refreshInterval:(pause:1f,value:900000),time:(from:now-7d,to:now))' and file paths 'kibana-7.15.1-wind....zip' and 'elasticsearch-7.15.1....zip'.



Disable Security features in Elasticsearch



The screenshot shows the Elasticsearch Dashboards interface. At the top, there are two tabs: "localhost:9200" and "Dashboards - Elastic". The URL bar shows "localhost:5601/app/dashboards#/list?_g=(filters:!(),refreshInterval:(pause:0,value:0),time:(from:now-15m,to:now))". The main area is titled "Dashboards" and contains a table with one row. The table has columns: Title, Description, Tags, and Actions. The single row is for a dashboard titled "[Logs] Web Traffic" with the description "Analyze mock web traffic log data for Elastic's website". A "Create dashboard" button is located at the top right of the table area. Below the table, there is a search bar and a "Rows per page: 20" dropdown.

Title	Description	Tags	Actions
[Logs] Web Traffic	Analyze mock web traffic log data for Elastic's website		



Disable Security features in Elasticsearch

The screenshot shows a Kibana dashboard titled "[Logs] Web Traffic - Elastic" running on localhost:9200. The dashboard includes the following components:

- Sample Logs Data:** A section with sample data for visitors and unique visitors.
- [Logs] Goals:** A gauge visualization showing 808 unique visitors.
- [Logs] Response Codes Over Time + Annotations:** A line chart showing HTTP response codes over time, with annotations for 5xx errors.
- HTTP Metrics:** Two large numerical values: 1,618 Visits and 4.8% HTTP 4xx.
- HTTP 5xx:** A value of 2.9%.
- [Logs] Total Requests and Bytes:** A visualization showing total requests and bytes.
- [Logs] Source and Destination Sankey Chart:** A Sankey chart showing source and destination data flow.





Intro to Kibana Analytics

Views, Search and Filter

Kibana Analytics

The screenshot shows the Kibana Home page. On the left, there is a sidebar with navigation links for different sections: Analytics, Observability, Security, and Analytics. The 'Analytics' section is currently selected and highlighted with a red box. The main content area features a 'Welcome home' banner with four cards: Enterprise Search, Observability, Security, and Analytics. Below this, there is a section titled 'Get started by adding your data' with a 'Try sample data' button. The bottom right corner contains a decorative graphic of a house with various charts and graphs floating around it.

Home - Elastic

Not Secure | 192.168.1.211:5601/app/home#/

elastic

Search Elastic

Home

Recently viewed

Analytics

- Overview
- Discover
- Dashboard
- Canvas
- Maps
- Machine Learning
- Visualize Library

Enterprise Search

Observability

Security

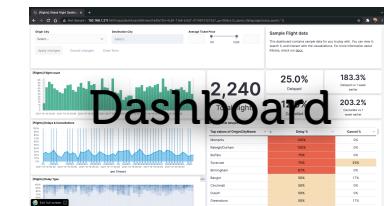
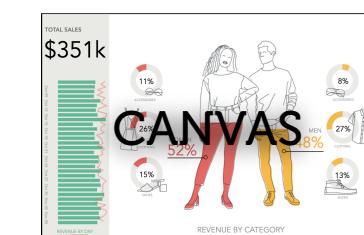
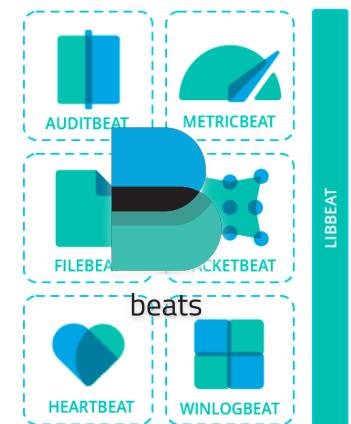
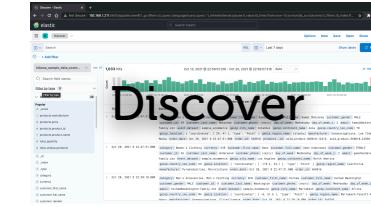
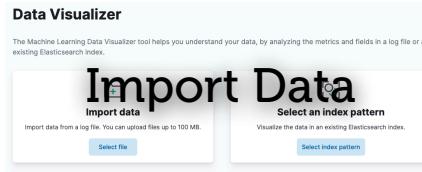
Analytics

Get started by adding your data

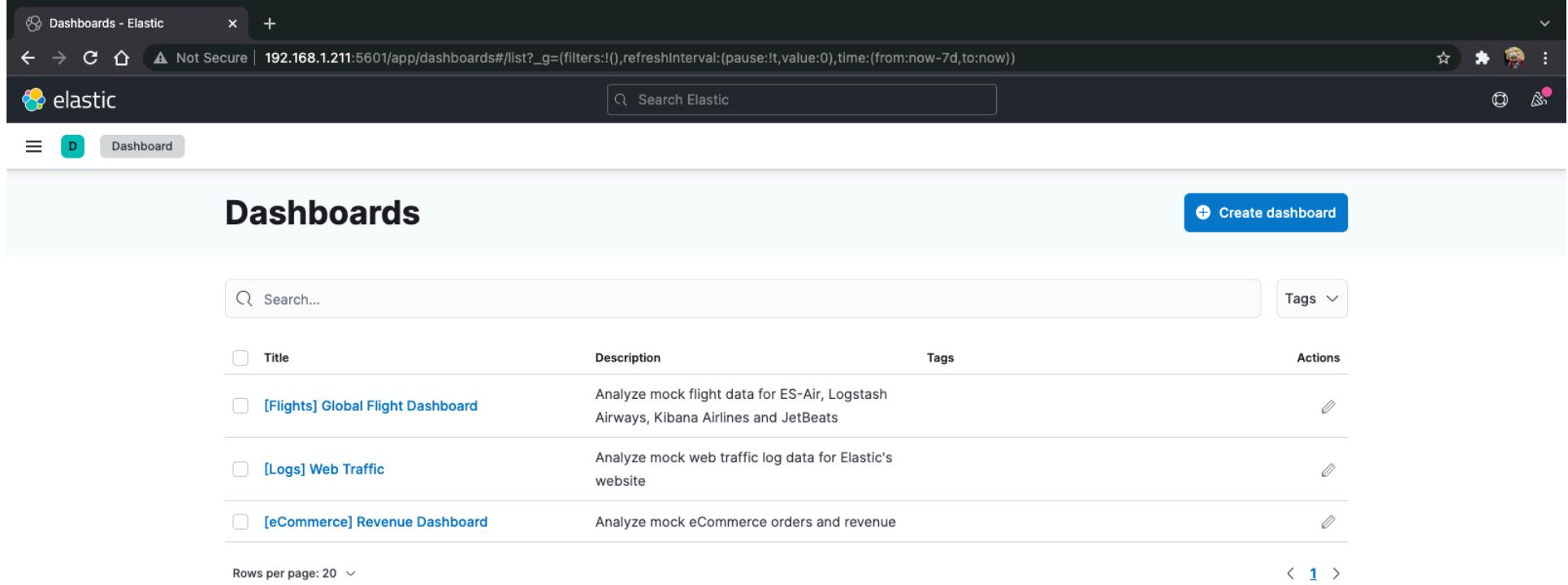
Add your data Try sample data



Kibana Analytics - Overviews



Kibana Analytics - Dashboard



The screenshot shows the Kibana Dashboards interface. At the top, there's a header bar with the title "Dashboards - Elastic", a search bar, and various navigation icons. Below the header is a main section titled "Dashboards" with a "Create dashboard" button. The main content area displays a table of existing dashboards:

<input type="checkbox"/> Title	Description	Tags	Actions
[Flights] Global Flight Dashboard	Analyze mock flight data for ES-Air, Logstash Airways, Kibana Airlines and JetBeats		
[Logs] Web Traffic	Analyze mock web traffic log data for Elastic's website		
[eCommerce] Revenue Dashboard	Analyze mock eCommerce orders and revenue		

At the bottom, there are pagination controls for "Rows per page: 20" and page number "1".



Kibana Analytics - Dashboard

Navigator

Search

Filter

The screenshot shows the [eCommerce] Revenue Dashboard in Kibana. At the top, there's a header with a back button, a refresh icon, and a URL indicating it's not secure (192.168.1.211:5601). Below the header is a search bar with the word "elastic". The main content area starts with a "Sample eCommerce Data" section containing a paragraph about the sample data and a bar chart titled "% of target revenue (\$10k)". To the right of this is a "Controls" section with dropdowns for "Manufacturer", "Category", and a "Quantity" slider set between 2 and 4. Below these are buttons for "Apply changes", "Cancel changes", and "Clear form". The dashboard then displays six distinct visualizations:

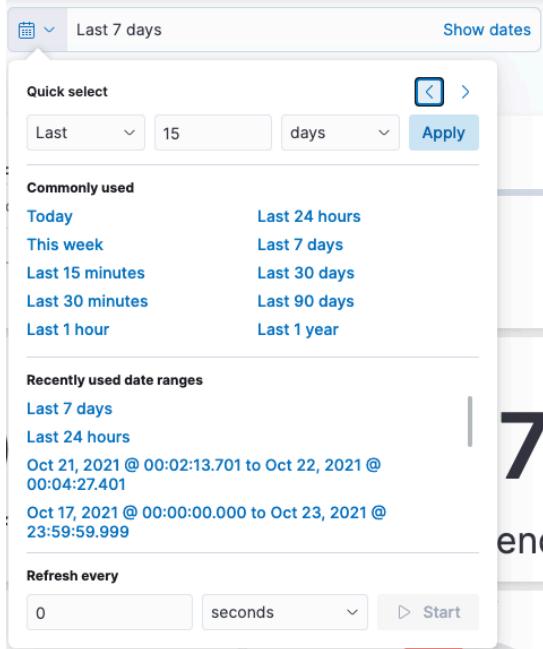
- % of target revenue (\$10k)**: A bar chart showing revenue percentages for specific dates.
- Sum of revenue**: A large numerical value of **\$76,893.06**.
- Median spending**: A numerical value of **\$67**.
- Transactions per day**: A line chart showing transaction counts over several days.
- Avg. items sold**: A numerical value of **2.2**.
- [eCommerce] Sold Products per Day**: A gauge chart showing the value **147.4** for "Trxns / day".

Control

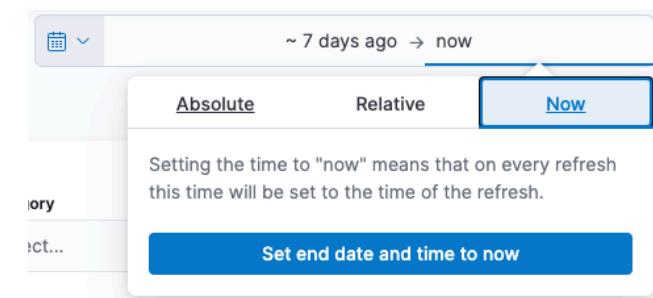
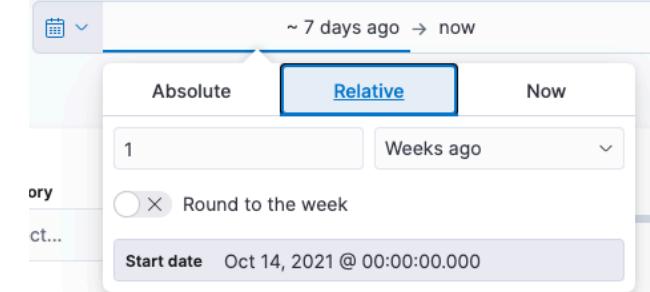
Time Filter

© 2013 - 2020 Siam Chamnankit Company Limited

Kibana Analytics - Time Filter



Quick Select



Customize



Kibana Analytics - Search

Save
Queries

Search keyword
with Autocompleted

The screenshot shows the Kibana search interface with a sidebar containing various search filters. A red box highlights the 'customer_first_name' filter, which has two options: 'customer_first_name.keyword' and 'customer_first_name'. Both options are preceded by a small orange circular icon with a magnifying glass and a plus sign, indicating they are filterable fields.

Search keyword with Autocompleted

- _id Filter results that contain _id
- _index Filter results that contain _index
- _type Filter results that contain _type
- category.keyword Filter results that contain category.keyword
- category Filter results that contain category
- currency Filter results that contain currency
- customer_birth_date Filter results that contain customer_birth_date
- customer_first_name.keyword Filter results that contain customer_first_name.keyword
- customer_first_name Filter results that contain customer_first_name
- customer_full_name.keyword Filter results that contain customer_full_name.keyword
- customer_full_name Filter results that contain customer_full_name
- customer_gender Filter results that contain customer_gender
- customer_id Filter results that contain customer_id
- customer_last_name.keyword Filter results that contain customer_last_name.keyword
- customer_last_name Filter results that contain customer_last_name

No results found

No results found

Trxns / day 0.0



Kibana Analytics - category vs category.keyword

category.keyword

The screenshot shows the Kibana search interface with the query "category.keyword :". The results list includes categories such as "Men's Accessories", "Men's Clothing", "Men's Shoes", "Women's Accessories", "Women's Clothing", and "Women's Shoes". The interface includes a sidebar with sections for [eCommerce] and Sample Data.

- "Men's Accessories"
- "Men's Clothing"
- "Men's Shoes"
- "Women's Accessories"
- "Women's Clothing"
- "Women's Shoes"

category

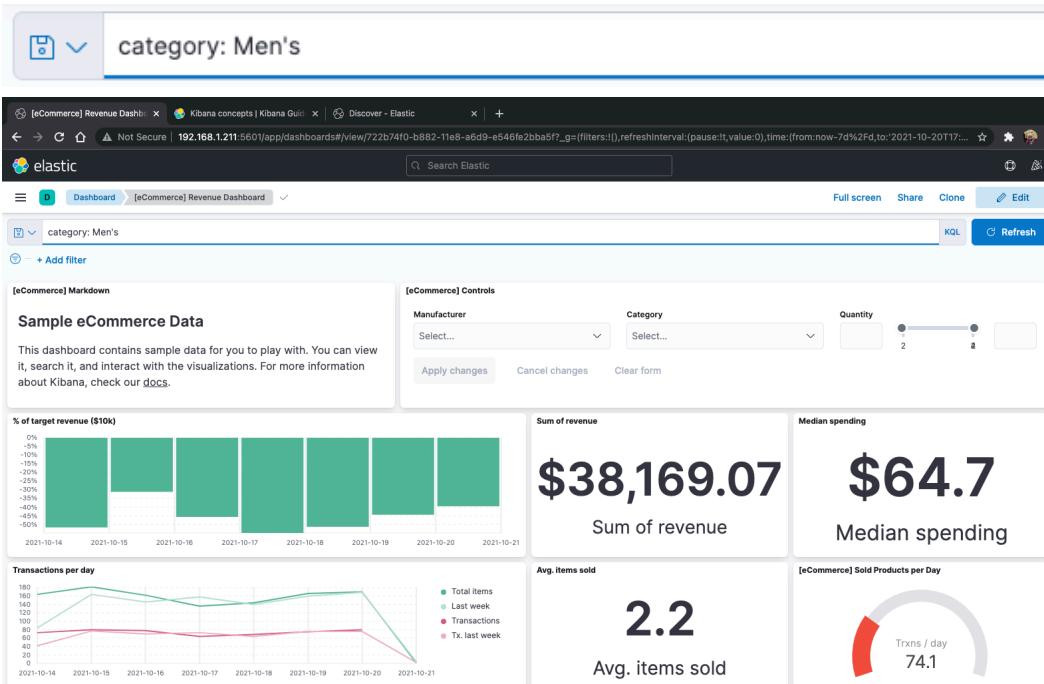
The screenshot shows the Kibana search interface with the query "category: Men's". The results list shows one item: "category: Men's".

- category: Men's



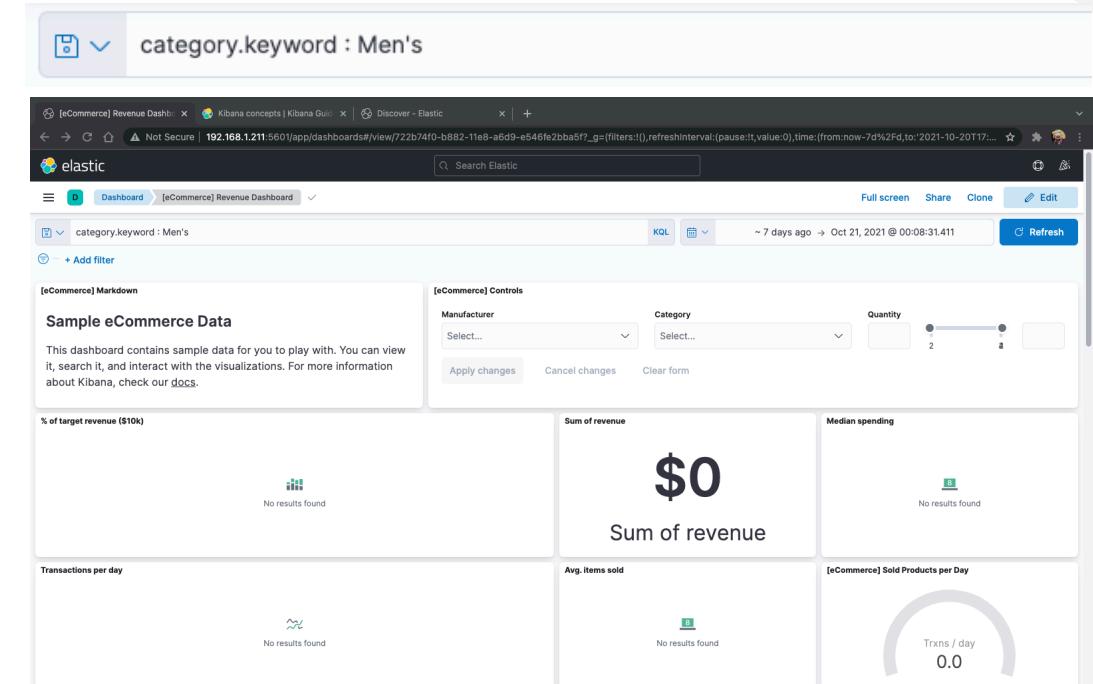
Kibana Analytics - category vs category.keyword

category



Search in Text Field

category.keyword



Search in Keyword Field



Kibana Analytics - Filter

Save Queries

List of Filter

The screenshot shows the Kibana Analytics interface with a focus on the 'Edit filter' dialog. The dialog is titled 'Edit filter' and contains fields for 'Field' (category), 'Operator' (is), 'Value' (Women's), and a 'Custom label' section where 'ເຊີ້ນຄໍາສົດ' is entered. A red callout points to this custom label field with the text 'Custom label Name'. In the background, there are several dashboard cards: 'Sum of revenue' (\$1,849.58), 'Median spending' (\$90.97), 'Avg. items sold' (2.5), and 'eCommerce Sold Products per Day' (Trxns / day 2.8). A red callout points to the top-left corner of the dashboard area with the text 'List of Filter'.



Kibana Analytics - Filter Option

Screenshot of the [eCommerce] Revenue Dashboard in Kibana, showing various visualizations and filter options.

The dashboard includes the following components:

- Search Bar:** Search Elastic
- Filter Bar:** KQL, Last 7 days, Show dates, Refresh
- Filter Options:** + Add filter, Pin across all apps, Edit filter, Exclude results, Temporarily disable, Delete.
- Controls:** Manufacturer, Category, Quantity (range slider from 2 to 4).
- Visualizations:**
 - % of target revenue (\$10k):** Stacked bar chart showing revenue percentage for each day from 2021-10-14 to 2021-10-21. The bars are entirely green, indicating 100% target revenue.
 - Sum of revenue:** \$1,849.58 (Sum of revenue)
 - Median spending:** \$90.97 (Median spending)
 - Transactions per day:** Line chart showing Total items (green), Last week (light green), Transactions (red), and Tx. last week (pink) over time.
 - Avg. items sold:** 2.5 (Avg. items sold)
 - [eCommerce] Sold Products per Day:** Gauge chart showing Trxns / day at 2.8.



Kibana Analytics - Filter from Controls

The screenshot shows the Kibana Revenue Dashboard interface. At the top, there are two tabs: "[eCommerce] Revenue Dashboard" and "[eCommerce] Controls". The main dashboard area contains several visualizations:

- Sample eCommerce Data:** A text block explaining the sample data.
- % of target revenue (\$10k):** A step chart showing revenue progress over time.
- Sum of revenue:** A large value of \$150,585.95.
- Median spending:** A large value of \$64.28.
- Transactions per day:** A line chart showing daily transaction volume.
- Avg. items sold:** A value of 2.2.
- [eCommerce] Sold Products per Day:** A gauge chart showing product sales per day.

The "[eCommerce] Controls" section is highlighted with a red box. It includes the following controls:

- Manufacturer:** A dropdown menu with "Select..." option, "Apply changes" button, and "Cancel changes" button.
- Category:** A dropdown menu currently set to "Men's Shoes", with options: Men's Accessories, Men's Clothing, Women's Accessories, Women's Shoes, Women's Clothing, and Women's Accessories.
- Quantity:** A slider ranging from 1 to 8.



Kibana Analytics - Filter from Controls

The screenshot shows the Kibana Analytics interface with the title "Kibana Analytics - Filter from Controls". The dashboard has a dark theme with several cards and a controls panel.

Search Bar: A search bar at the top contains the query `category.keyword: is one of Men's Shoes, Women's Accessories`, which is highlighted with a red oval.

Controls Panel: Below the search bar is a "Controls" section. It includes a "Category" dropdown containing "Men's Shoes" and "Women's Accessories", which is also highlighted with a red oval. To the right of the dropdown is a "Quantity" slider set between 1 and 8.

Sample eCommerce Data: This card displays sample data for the dashboard. It includes a text block about the sample data and a bar chart titled "% of target revenue (\$10k)" showing values from 0% to -90% over a period from 2021-09-21 to 2021-10-19.

Sum of revenue: A card showing the sum of revenue as **\$60,020.88**.

Median spending: A card showing the median spending as **\$75**.

Transactions per day: A line chart showing transactions per day for Total items, Last week, Transactions, and Tx. last week.

Avg. items sold: A card showing the average items sold as **2.2**.

[eCommerce] Sold Products per Day: A gauge chart showing Trxns / day as **24.5**.



Kibana Analytics - Filter from Visualization

The screenshot shows the Kibana eCommerce Revenue Dashboard. At the top right, there is a red box highlighting a tooltip on a chart. The tooltip displays the date "2021-10-15" and the value "% of target (\$10k) 30%". The dashboard includes several visualizations and controls:

- [eCommerce] Markdown:** A section with sample eCommerce data and a note about Kibana documentation.
- [eCommerce] Controls:** Manufacturer, Category, and Quantity selection fields with a slider set between 1 and 8.
- % of target revenue (\$10k):** A step chart showing revenue growth over time. A red box highlights a tooltip for the point on October 15th.
- Sum of revenue:** A large value of \$150,585.95.
- Median spending:** A large value of \$64.28.
- Transactions per day:** A line chart showing daily transaction volume.
- Avg. items sold:** A value of 2.2.
- [eCommerce] Sold Products per Day:** A gauge chart showing 67.4 Trxns / day.



Kibana Analytics - Filter from Visualization

The screenshot shows the Kibana eCommerce Revenue Dashboard. At the top, there are two tabs: [eCommerce] Revenue Dashboard and [eCommerce] Revenue Dashboard. Below the tabs, the URL is 192.168.1.211:5601/app/dashboards#/view/722b74f0-b882-11e8-a6d9-e546fe2bba5f?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:'2021-10-14T17:00:00.000Z',to:'2021-10-15T17:00:00.000Z'))&_sourceId=1. A red box highlights the date range selector from Oct 15, 2021 @ 00:00:00.000 to Oct 16, 2021 @ 00:00:00.000.

In the center, there is a search bar with the placeholder "Search Elastic". To the right of the search bar are buttons for "Full screen", "Share", "Clone", and "Edit".

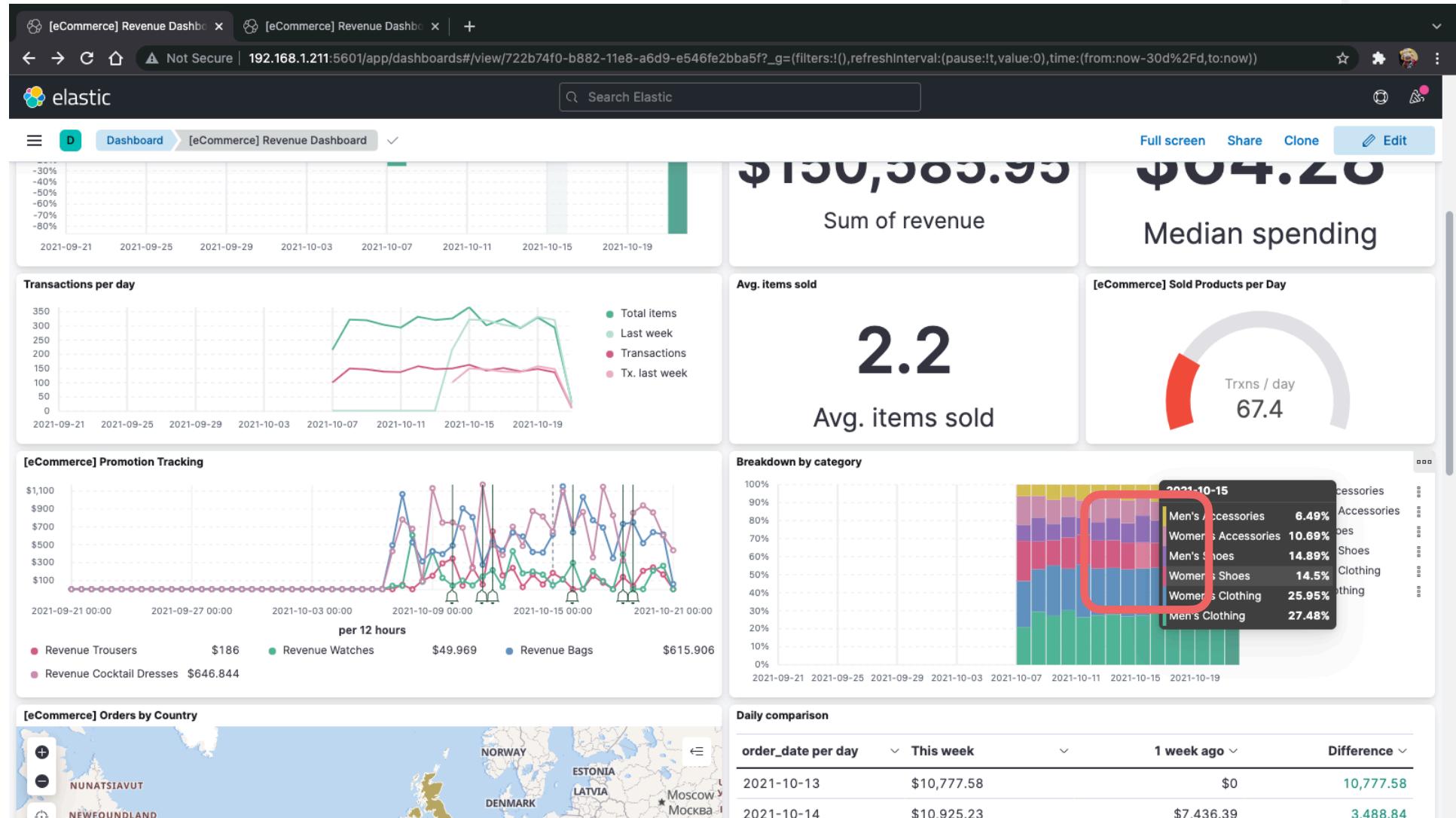
Below the search bar, there is a "KQL" button followed by a date range selector and a "Refresh" button. A red box highlights this entire row of controls.

The dashboard contains several visualizations:

- [eCommerce] Markdown:** A section titled "Sample eCommerce Data" with a note: "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](#)." A red box highlights this section.
- [eCommerce] Controls:** Manufacturer, Category, and Quantity filters with "Apply changes", "Cancel changes", and "Clear form" buttons.
- % of target revenue (\$10k):** A stacked bar chart comparing actual revenue against target. A red box highlights the chart area.
- Sum of revenue:** A large card showing \$3,020.13 with a timestamp of 2021-10-15. A red box highlights this card.
- Median spending:** A large card showing \$74 with the text "Median spending".
- Transactions per day:** A line chart showing transaction volume over time. A red box highlights the chart area.
- Avg. Items sold:** A large card showing 2.2 with the text "Avg. items sold".
- [eCommerce] Sold Products per Day:** A donut chart showing product sales per day. A red box highlights the chart area.



Kibana Analytics - Filter from Visualization



Kibana Analytics - Filter from Visualization

The screenshot shows the [eCommerce] Revenue Dashboard in Kibana. A modal window titled "Select filters to apply" is open in the center, displaying two selected filters:

- order_date: Oct 15, 2021 @ 00:00:00.000 to Oct 16, 2021 @ 00:00:00.000
- category.keyword: Women's Shoes

Below the modal are several visualizations:

- Sum of revenue:** \$150,585.95
- Median spending:** \$94.20
- Avg. items sold:** 2
- Trxns / day:** 67.4
- [eCommerce] Sold Products per Day:** Stacked bar chart showing product categories over time.
- [eCommerce] Promotion Tracking:** Line chart showing revenue for various products over 12 hours.
- [eCommerce] Orders by Country:** Map visualization showing order locations.
- Daily comparison:** Table comparing order_date per day, This week, 1 week ago, and Difference.

order_date per day	This week	1 week ago	Difference
2021-10-13	\$10,777.58	\$0	10,777.58
2021-10-14	\$10,925.23	\$7,436.39	3,488.84



Kibana Analytics - Filter from Visualization

The screenshot shows the [eCommerce] Revenue Dashboard in Kibana. At the top, there are two tabs: [eCommerce] Revenue Dashboard and [eCommerce] Revenue Dashboard. The main header includes the elastic logo, a search bar, and navigation buttons for Full screen, Share, Clone, and Edit.

On the left, there is a sidebar with a search bar and a filter section for "category.keyword: Women's Shoes". Below this is a section titled "[eCommerce] Markdown" with the heading "Sample eCommerce Data". It contains a brief description of the sample data and a link to the [docs](#).

In the center, there is a "[eCommerce] Controls" panel with dropdowns for "Manufacturer" and "Category", and a slider for "Quantity" ranging from 2 to 4. Below these are buttons for "Apply changes", "Cancel changes", and "Clear form".

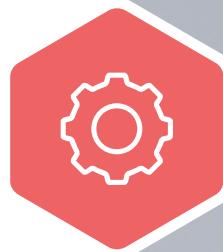
The dashboard features seven visualizations:

- % of target revenue (\$10k): A bar chart showing a value of 0% for the date 2021-10-16.
- Sum of revenue: A large number \$3,469.5 with the subtitle "Sum of revenue".
- Median spending: A large number \$91.5 with the subtitle "Median spending".
- Transactions per day: A line chart showing transactions per day for Total items (green), Last week (light green), Transactions (red), and Tx. last week (pink). The chart shows a peak around 80 transactions on 2021-10-16.
- Avg. items sold: A large number 2.3 with the subtitle "Avg. items sold".
- [eCommerce] Sold Products per Day: A donut chart showing Trxns / day at 38.0.

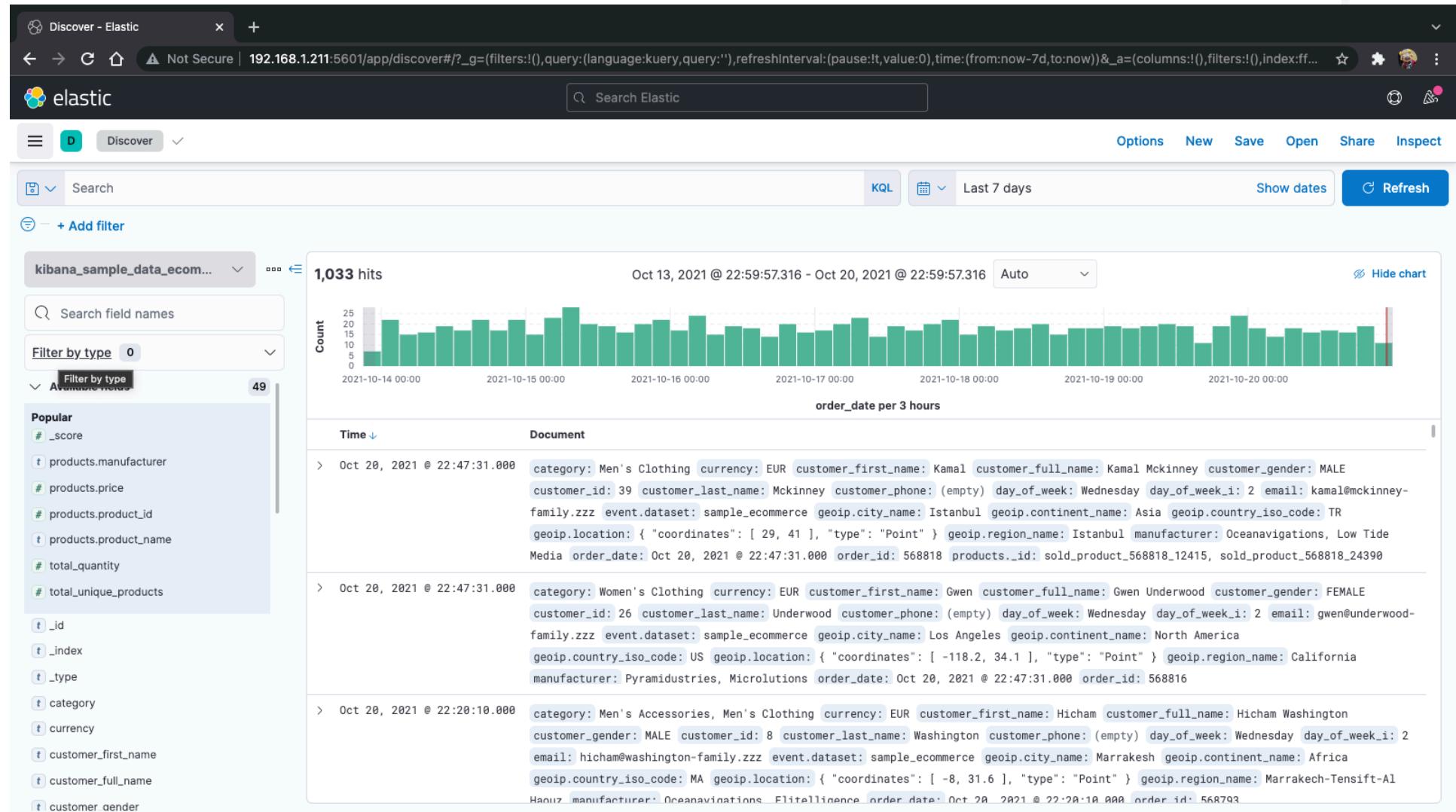


Explore The Data

Known Your Data



Kibana Analytics - Discover



Kibana Analytics - Change index pattern

The screenshot shows the Kibana Discover interface. At the top, there are two tabs: "Discover - Elastic" and "Discover - Elastic". The URL is "Not Secure | 13.212.165.217:5601/app/discover#/?_g=(filters:!(),query:(language:kuery,query:'"),refreshInterval:(pause:1t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(),filters:!(),index:f...)".

The main area has a search bar "Search Elastic" and navigation buttons "Options", "New", "Save", "Open", "Share", and "Inspect".

A red box highlights the "Change index pattern" dropdown menu, which is open and shows the following options:

- kibana_sample_data_ecom...
- kibana_sample_data_ecommerce
- kibana_sample_data_flights
- kibana_sample_data_logs

Below the dropdown, there is a histogram titled "order_date per 3 hours" showing data from Oct 14, 2021 @ 03:01:32.326 to Oct 21, 2021 @ 03:01:32.326. The chart shows approximately 1,030 hits.

The main search results table has columns "Time" and "Document". It displays three documents with their respective timestamps and detailed log entries:

Time	Document
> Oct 21, 2021 @ 02:37:55.000	category: Women's Clothing, Women's Accessories currency: EUR customer_first_name: Yasmine customer_full_name: Yasmine Roberson customer_gender: FEMALE customer_id: 43 customer_last_name: Roberson customer_phone: (empty) day_of_week: Wednesday day_of_week_i: 2 email: yasmine@roberson-family.zzz event.dataset: sample_ecommerce geoip.continent_name: Asia geoip.country_iso_code: SA geoip.location: { "coordinates": [45, 25], "type": "Point" } manufacturer: Champion Arts, Tigress Enterprises order_date: Oct 21, 2021 @ 02:37:55.000 order_id: 569056 products._id: sold_product_569056_18276, sold_product_569056_16315 products.base_price: \$10.99,
> Oct 21, 2021 @ 02:36:29.000	category: Women's Shoes, Women's Clothing currency: EUR customer_first_name: Sonya customer_full_name: Sonya Morgan customer_gender: FEMALE customer_id: 28 customer_last_name: Morgan customer_phone: (empty) day_of_week: Wednesday day_of_week_i: 2 email: sonya@morgan-family.zzz event.dataset: sample_ecommerce geoip.city_name: Bogotu00e1l geoip.continent_name: South America geoip.country_iso_code: CO geoip.location: { "coordinates": [-74.1, 4.6], "type": "Point" } geoip.region_name: Bogota D.C. manufacturer: Low Tide Media, Oceanavigations order_date: Oct 21, 2021 @ 02:36:29.000 order_id: 569055
> Oct 21, 2021 @ 02:24:58.000	category: Men's Shoes, Men's Clothing currency: EUR customer_first_name: Yahya customer_full_name: Yahya Dennis customer_gender: MALE customer_id: 23 customer_last_name: Dennis customer_phone: (empty) day_of_week: Wednesday day_of_week_i: 2 email: yahya@dennis-

At the bottom left, there is a file icon and "gsm.csv". On the right, there is a "Show All" button and a close button.



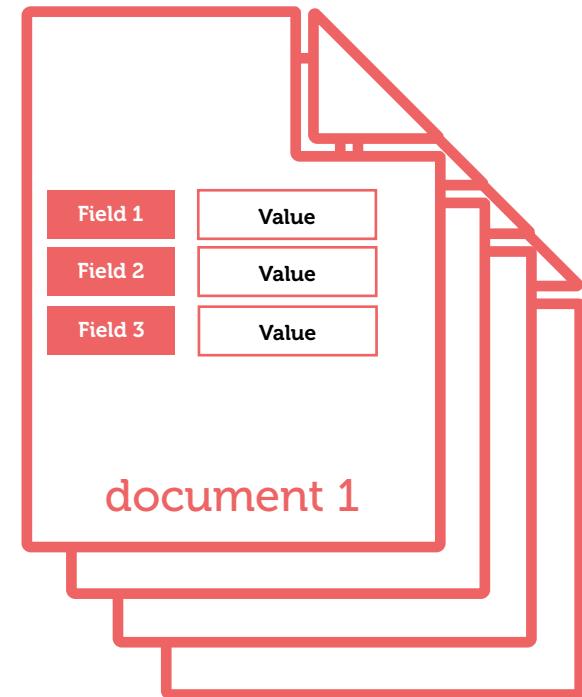
Elasticsearch - Data Structure

RDBMS : MySQL, MSSQL, OracleDB

	Column 1	Column 2	Column 3
Row 1			
Row 2			
Row 3			
Row 4			

Table

Document oriented Database



Index

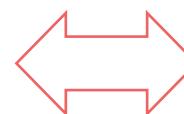


Elasticsearch - Data Structure

RDBMS : MySQL, MSSQL, OracleDB

Column

can contain exactly one value of said type

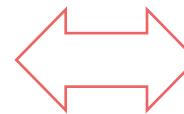


Field

can contain multiple values of the same type

Row

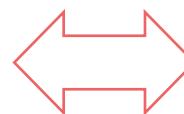
tends to strict



Document

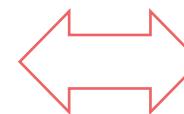
tends to be a bit more flexible or loose

Table



Index

Schema



Implicit

Cluster, Database



Cluster, Cluster Instance



https://www.elastic.co/guide/en/elasticsearch/reference/current/_mapping_concepts_across_sql_and_elasticsearch.html

© 2013 - 2020 Siam Chamnankit Company Limited

Elasticsearch - Field Data Types

Common types

binary boolean Keywords
Numbers Dates alias

Aggregate data types

aggregate_metric_double
histogram

Text search types

text annotated-text completion
search_as_you_type token_count

Spatial data types

geo_point geo_shape
point shape

Objects and relational types

object join nested
flattened

Structure data types

Range murmur3 ip version

Document ranking types

dens_vector sparse_vector rank_feature
rank_features

Other types

percolator



Kibana Analytics - category vs category.keyword

category.keyword

The screenshot shows the Kibana search interface with the query "category.keyword :". The results list includes categories such as Men's Accessories, Men's Clothing, Men's Shoes, Women's Accessories, Women's Clothing, and Women's Shoes. The interface includes a sidebar with sections for [eCommerce] and Sample Data.

- "Men's Accessories"
- "Men's Clothing"
- "Men's Shoes"
- "Women's Accessories"
- "Women's Clothing"
- "Women's Shoes"

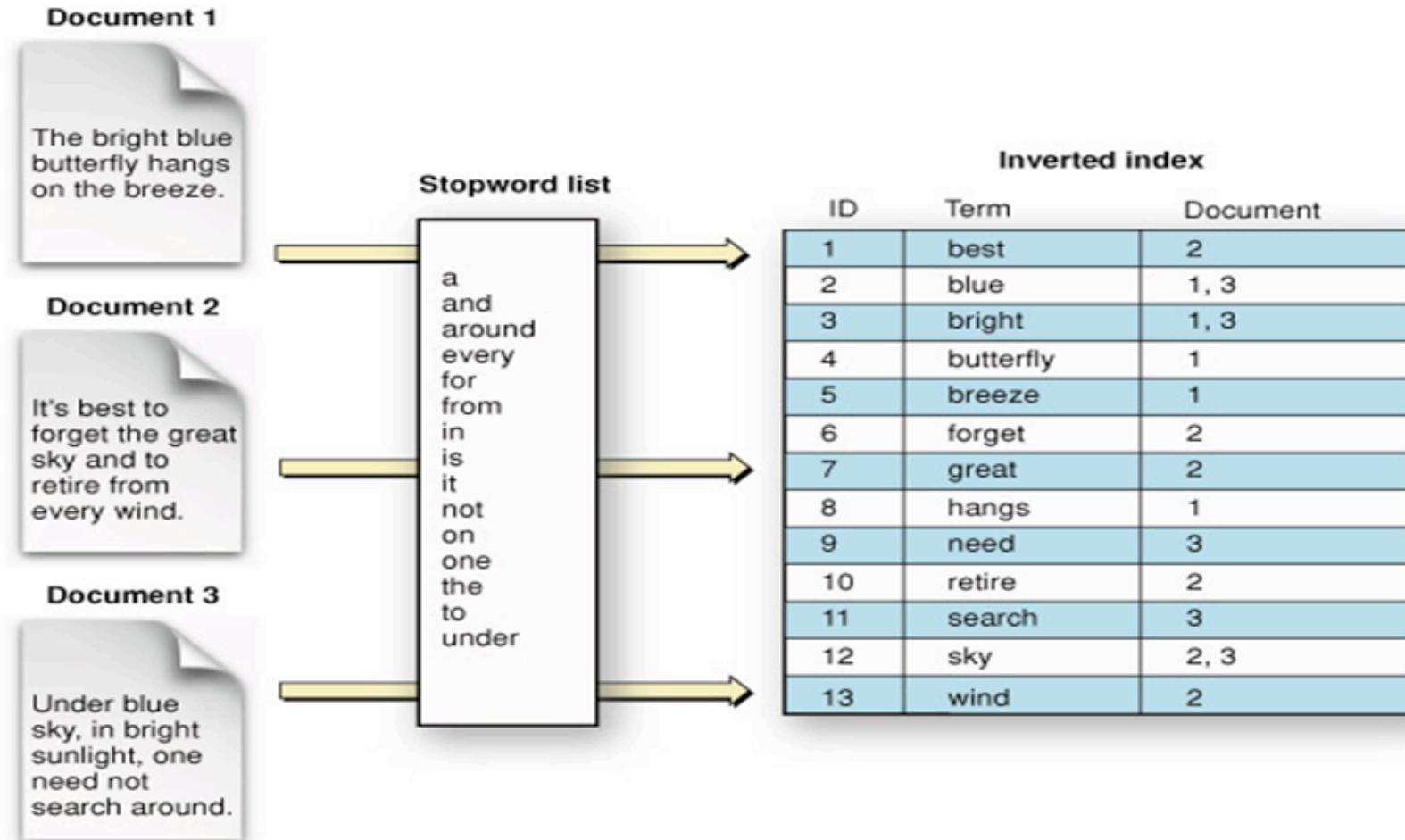
category

The screenshot shows the Kibana search interface with the query "category: Men's". The results list shows one item: "Men's".

- category: Men's

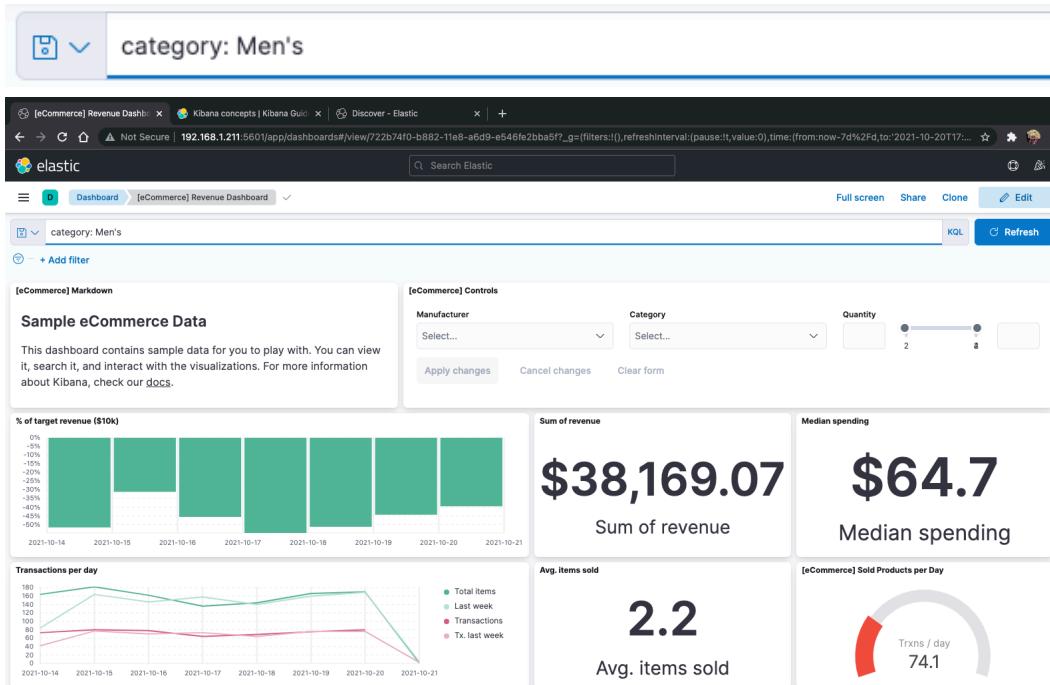


Elasticsearch - Apache Lucene: Inverted Index



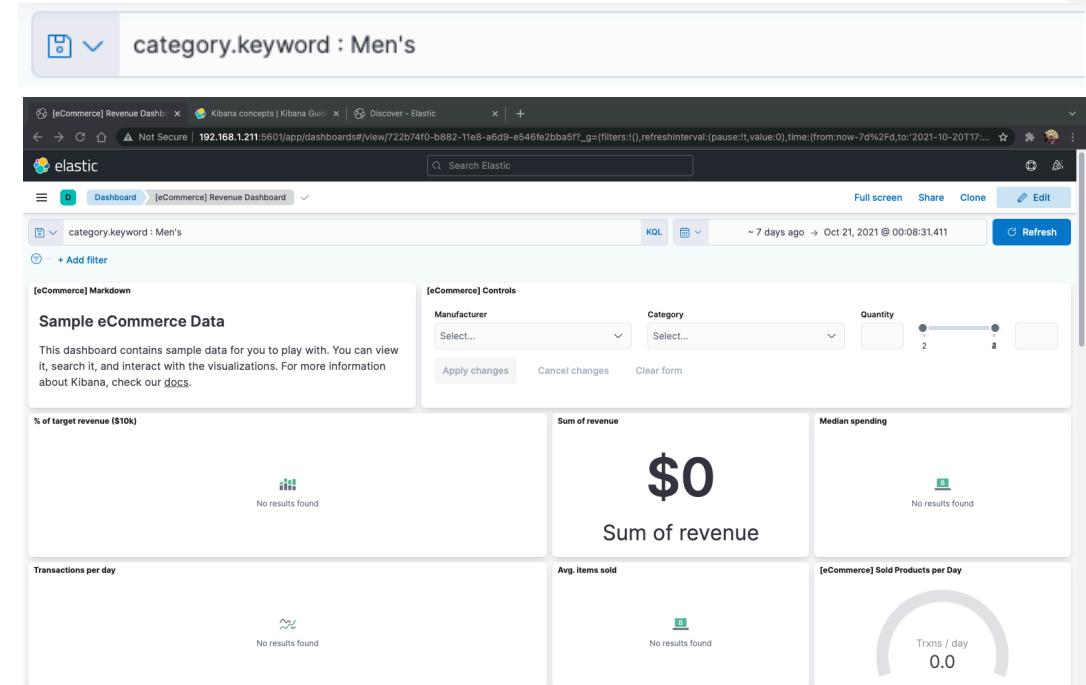
Elasticsearch - Apache Lucene: Inverted Index

category



Search in Text Field

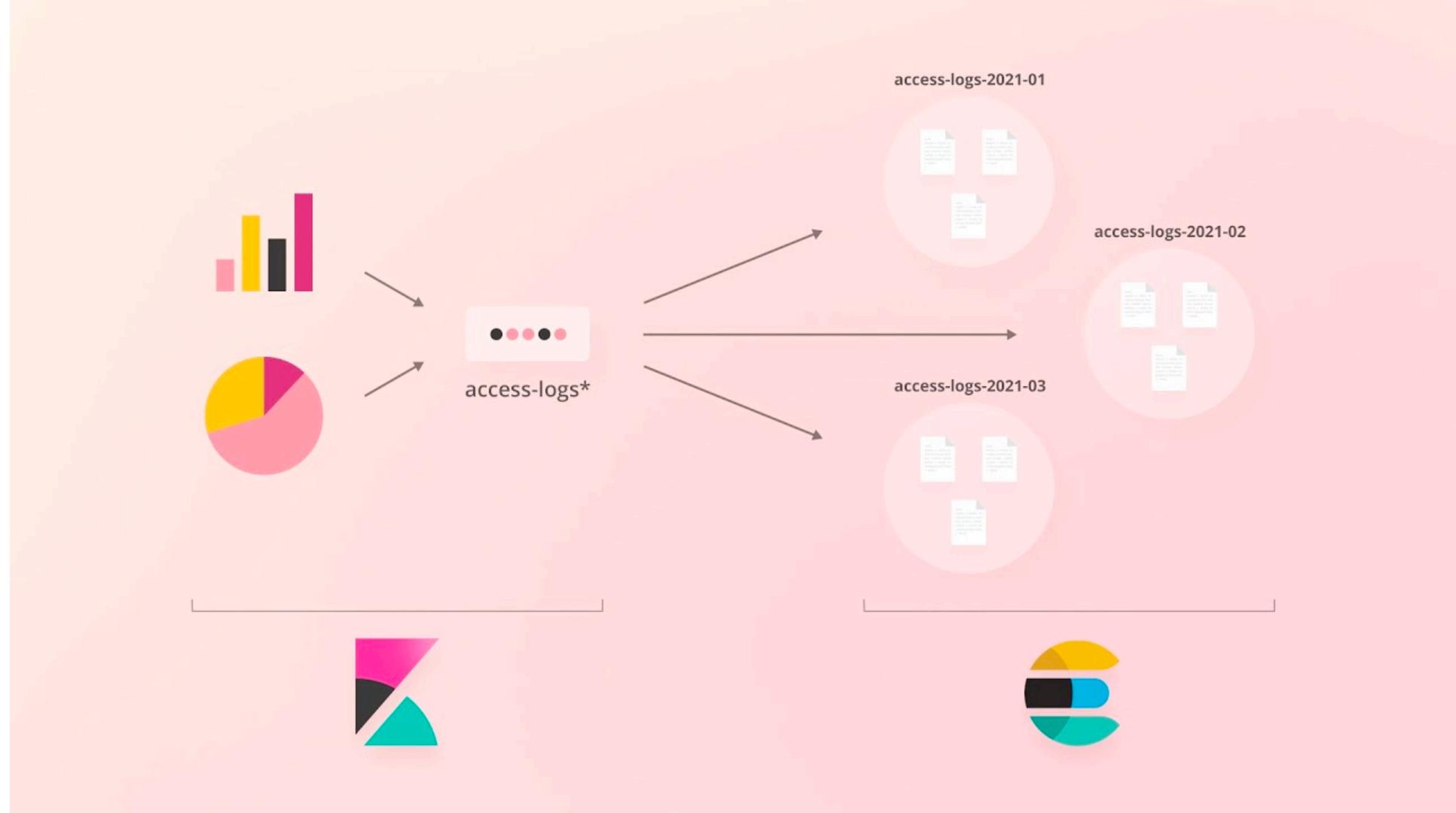
category.keyword



Search in Keyword Field



Kibana - Index Pattern



Kibana - Menu Management -> Stack Management

The screenshot shows the Kibana Discover interface with the following details:

- Header:** Discover - Elastic (x), Discover - Elastic (x), +, Not Secure | 13.212.165.217:5601/app/discover#/?_g=(filters:!(),query:(language:kuery,query:"")),refreshInterval:(pause:1t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(),filters:!(),index:f...)
- Search Bar:** Search Elastic
- Toolbar:** Options, New, Save, Open, Share, Inspect
- Left Sidebar:**
 - Home
 - Recently viewed
 - [eCommerce] Revenue Dash...
 - [eCommerce] Orders by Cou...
 - [eCommerce] Revenue Dash...
 - [eCommerce] Revenue Dash...
 - [eCommerce] Revenue Dash...
 - Network
 - Timelines
 - Cases
 - Endpoints
 - Management
 - Dev Tools
 - Integrations
 - Fleet
 - Osquery
 - Stack Monitoring
 - Stack Management
- Central Area:**
 - Chart:** 1,030 hits (Oct 14, 2021 @ 04:37:54.085 - Oct 21, 2021 @ 04:37:54.085) - A bar chart showing the count of hits per hour from October 14 to 20, 2021.
 - Table:** A table of search results for documents. Each row shows a timestamp and a detailed document snippet. The first few rows are:
 - > Oct 21, 2021 @ 04:36:00.000 category: Men's Shoes currency: EUR customer_first_name: Abd customer_full_name: Abd Lamb customer_gender: MALE customer_id: 52 customer_last_name: Lamb customer_phone: (empty) day_of_week: Wednesday day_of_week_i: 2 email: abd@lamb-family.zzz event.dataset: sample_ecommerce geoip.city_name: Cairo geoip.continent_name: Africa geoip.country_iso_code: EG geoip.location: { "coordinates": [31.3, 30.1], "type": "Point" } geoip.region_name: Cairo Governorate manufacturer: Angeldale order_date: Oct 21, 2021 @ 04:36:00.000 order_id: 569163 products._id: sold_product_569163_1774, sold_product_569163_23724 products.base_price: \$60.00, \$75.00
 - > Oct 21, 2021 @ 04:20:10.000 category: Women's Clothing currency: EUR customer_first_name: Betty customer_full_name: Betty Perkins customer_gender: FEMALE customer_id: 44 customer_last_name: Perkins customer_phone: (empty) day_of_week: Wednesday day_of_week_i: 2 email: betty@perkins-family.zzz event.dataset: sample_ecommerce geoip.city_name: New York geoip.continent_name: North America geoip.country_iso_code: US geoip.location: { "coordinates": [-74, 40.7], "type": "Point" } geoip.region_name: New York manufacturer: Microlutions, Champion Arts order_date: Oct 21, 2021 @ 04:20:10.000 order_id: 569144 products._id: sold_product_569144_9379, sold_product_569144_15599
 - > Oct 21, 2021 @ 03:58:34.000 category: Men's Accessories, Men's Clothing currency: EUR customer_first_name: Jackson customer_full_name: Jackson Watkins customer_gender: MALE customer_id: 13 customer_last_name: Watkins customer_phone: (empty) day_of_week: Wednesday day_of_week_i: 2
- Bottom Navigation:** Stack Management, gsm.csv, Show All, X



Kibana - Stack Management

The screenshot shows the 'Stack Management' interface in Kibana 7.15.1. The left sidebar lists various management categories: Ingest, Data, Alerts and Insights, Kibana, and Search Sessions. Under 'Data', 'Index Management' is selected, and 'Index Lifecycle Policies' is highlighted. The main content area displays a 'Welcome to Stack Management' message with the version '7.15.1'. It includes a gear icon, a brief description of index management, and a note about the complete list of apps in the sidebar.

Discover - Elastic Elastic

Not Secure | 13.212.165.217:5601/app/management

elastic

Search Elastic

Management

Ingest

Ingest Node Pipelines

Data

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights

Rules and Connectors

Reporting

Machine Learning Jobs

Kibana

Index Patterns

Saved Objects

Tags

Search Sessions

gsm.csv

Show All

Welcome to Stack Management
7.15.1

Manage your indices, index patterns, saved objects, Kibana settings, and more.

A complete list of apps is in the menu on the left.

13.212.165.217:5601/app/management/data/index_management



Kibana - Index Management

The screenshot shows the Elasticsearch Index Management interface. The left sidebar contains navigation links for Management, Ingest, Data, Alerts and Insights, and Kibana. The main area is titled "Index Management" and displays a table of indices. The table columns are Name, Health, Status, Primaries, Replicas, Docs count, Storage size, and Data stream. Three indices are listed:

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
kibana_sample_data_ecommerce	green	open	1	0	4675	3.8mb	
kibana_sample_data_logs	green	open	1	0	14074	7.9mb	
kibana_sample_data_flights	green	open	1	0	13059	5.2mb	

Below the table, there are buttons for "Rows per page: 10", "Reload indices", and pagination controls (< 1 >). At the bottom, there is a file download button labeled "gsm.csv".



Kibana - Index Management

The screenshot shows the Kibana interface for managing Elasticsearch indices. On the left, a sidebar menu includes 'Management', 'Ingest', 'Data' (with 'Index Management' selected), 'Alerts and Insights', 'Kibana', and 'Saved Objects'. The main area has tabs for 'Indices', 'Data Streams', 'Index Templates', and 'Component Templates'. The 'Indices' tab is active, displaying a list of indices: 'kibana_sample_data_ecommerce', 'kibana_sample_data_logs', and 'kibana_sample_data_flights', all in green health status. A modal window is open for the 'kibana_sample_data_ecommerce' index, showing the 'Mappings' tab. The mapping configuration is as follows:

```
{  
  "mappings": {  
    "_doc": {  
      "properties": {  
        "category": {  
          "type": "text",  
          "fields": {  
            "keyword": {  
              "type": "keyword"  
            }  
          }  
        },  
        "currency": {  
          "type": "keyword"  
        },  
        "customer_birth_date": {  
          "type": "date"  
        },  
        "customer_first_name": {  
          "type": "text",  
          "fields": {  
            "keyword": {  
              "type": "keyword",  
              "ignore_above": 256  
            }  
          }  
        }  
      }  
    }  
},  
"ignore_above": 256}
```

At the bottom right of the modal is a blue 'Manage' button.



Kibana - Index Pattern

The screenshot shows the Elasticsearch Index Management interface. The left sidebar includes sections for Ingest, Data (with Index Management selected), Alerts and Insights, Kibana (with Index Patterns selected), and other options like Saved Objects and Tags. The main content area is titled "Index Management" and displays the "Indices" tab. It lists three indices: "kibana_sample_data_ecommerce" (green health, open status, 1 primary, 0 replicas, 4675 docs, 3.8mb storage), "kibana_sample_data_logs" (green health, open status, 1 primary, 0 replicas, 14074 docs, 7.9mb storage), and "kibana_sample_data_flights" (green health, open status, 1 primary, 0 replicas, 13059 docs, 5.2mb storage). A "Manage index" dropdown, a search bar, and filters for Lifecycle status and phase are visible. The bottom navigation bar shows the URL as 13.212.165.217:5601/app/management/kibana/indexPatterns.

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
kibana_sample_data_ecommerce	green	open	1	0	4675	3.8mb	
kibana_sample_data_logs	green	open	1	0	14074	7.9mb	
kibana_sample_data_flights	green	open	1	0	13059	5.2mb	



Kibana - Index Pattern

The screenshot shows the Kibana management interface for index patterns. The left sidebar includes sections for Ingest, Data, Alerts and Insights, and Kibana, with Index Patterns currently selected. The main area displays the 'Index patterns' page, which allows users to create and manage index patterns for retrieving data from Elasticsearch. The page features a search bar, a list of index patterns, and navigation controls for rows per page and pagination.

Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

Search...

Pattern ↑

kibana_sample_data_ecommerce Default

kibana_sample_data_flights

kibana_sample_data_logs

Rows per page: 10 < 1 >

gsm.csv Show All X



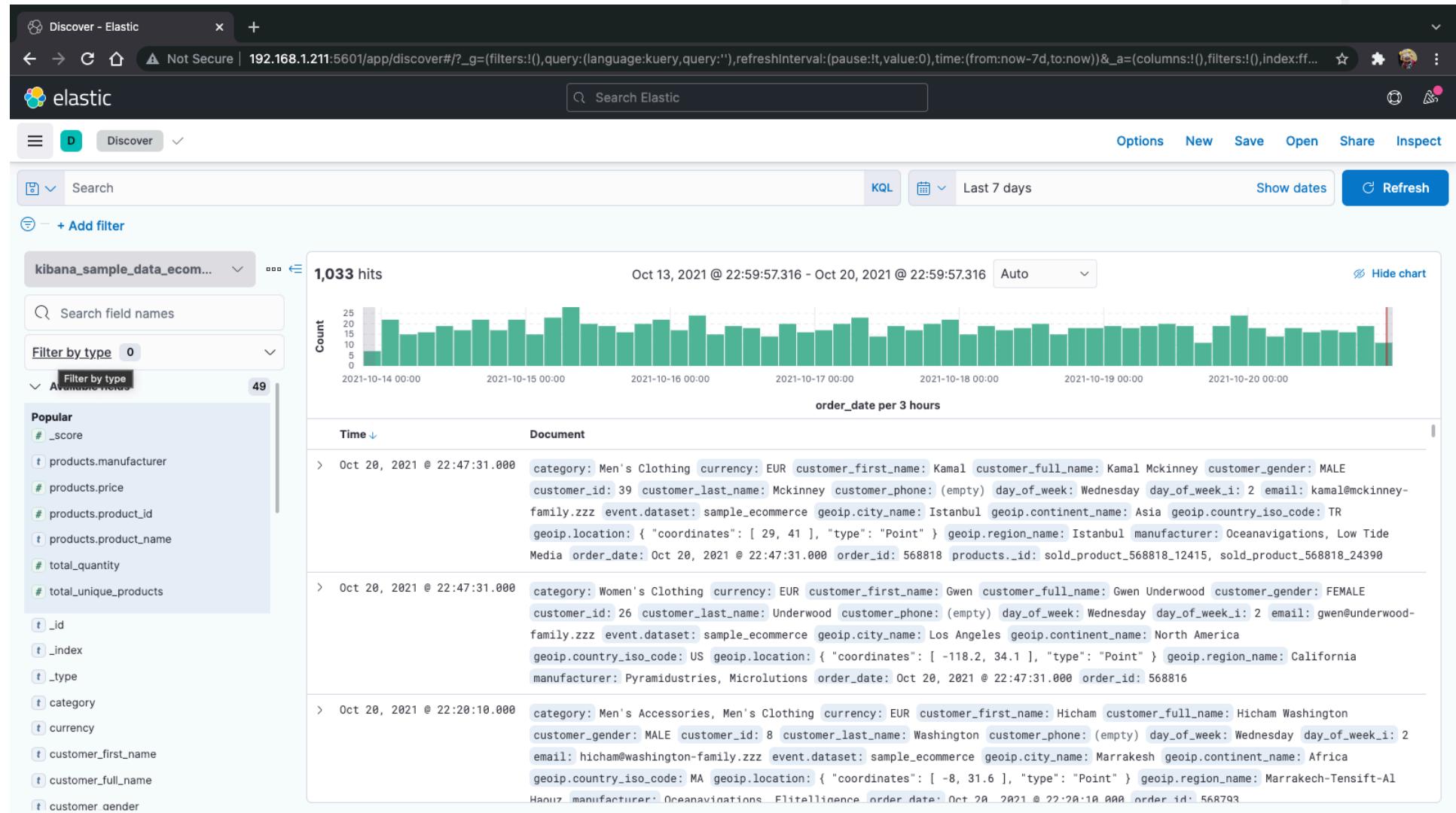
Kibana - Index Pattern

The screenshot shows the Kibana management interface for an index pattern named 'kibana_sample_data_ecommerce'. The left sidebar contains navigation links for Ingest, Data, Alerts and Insights, and Kibana. The main content area displays the index pattern details, including its time field ('order_date') and a table of fields. The table includes columns for Name, Type, Format, Searchable, Aggregatable, and Excluded. Fields listed include _id, _index, _score, _source, _type, category, category.keyword, and currency.

Name	Type	Format	Searchable	Aggregatable	Excluded
_id	_id		●	●	✎
_index	_index		●	●	✎
_score					✎
_source	_source				✎
_type	_type		●	●	✎
category	text		●		✎
category.keyword	keyword		●	●	✎
currency	keyword		●	●	✎



Kibana Analytics - Discover



Kibana Analytics - Top X Values

Sep 21, 2021 @ 00:00:00.000 - Oct 21, 2021 @ 04:52:43.692 Auto

2,556 hits

Count

timestamp per 12 hours

machine.os

Top 5 values

Value	Percentage
osx	22.2%
win xp	22.0%
win 8	19.8%
ios	18.6%
win 7	17.4%

Exists in 500 / 500 records

Multi fields

Visualize

Document

7 timestamp: Oct 21, 2021 @ 04:45:10.997 agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) bytes: 3,705 clientip: 213.253.23.28 event.dataset: sample_web_logs extension: css geo.coordinates: { "coordinates": [-102.9852778, 41.10133333 "type": "Point" } geo.dest: BD geo.src: JP geo.srctest: JP:BD host: cdn.elastic-elastic.elastic.org hour_of_day: 21 index: kibana_sample_data_logs ip: 213.253.23.28 machine.os: osx machine.ram: 8,589,934,592 message: 213.253.23.28 -- [2018-08-01T21:45:10.997Z] "GET /styles/ad-blocker.css HTTP/1.1" 200 3705 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"

6 timestamp: Oct 21, 2021 @ 04:21:52.666 agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 bytes: 6,811 clientip: 137.194.72.25 event.dataset: sample_web_logs extension: (empty) geo.coordinates: { "coordinates": [-84.7841425, 39.50203917], "type": "Point" } geo.dest: IQ geo.src: CD geo.srctest: CD:IQ host: www.elastic.co hour_of_day: 21 index: kibana_sample_data_logs ip: 137.194.72.25 machine.os: osx machine.ram: 12,884,901,888 message: 137.194.72.25 -- [2018-08-01T21:52.666Z] "GET / HTTP/1.1" 200 6811 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko)"

4 timestamp: Oct 21, 2021 @ 03:47:30.594 agent: Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1 bytes: 8,274 clientip: 15.225.65.207 event.dataset: sample_web_logs extension: css geo.coordinates: { "coordinates": [-119.9427053, 47.86597139] "type": "Point" } geo.dest: US geo.src: CN geo.srctest: CN:US host: www.mozilla.org hour_of_day: 21 index: kibana_sample_data_logs ip: 15.225.65.207 machine.os: osx machine.ram: 12,884,901,888 message: 15.225.65.207 -- [2018-08-01T21:47:30.594Z] "GET / HTTP/1.1" 200 8,274 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1"

gsm.csv

Show All

Discover - Elastic Index patterns - Elastic

Not Secure | 192.168.1.211:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-30d%2Fd,to:now))&_a=(columns:!(),filters:!(),index:'90943e30-9a47-11e8-b6...' Options New Save Open Share Inspect

Search Elastic

+ Add filter

Search field names

Filter by type 0

Popular

- # bytes
- IP clientip
- t machine.os
- String field machine.os
- # phpmemory
- t request
- t _id
- t _index
- # _score
- t _type
- @timestamp
- t agent
- t event.dataset
- t extension

Visualize



Kibana Analytics - Selected fields

The screenshot shows the Kibana Discover interface with the following details:

- Discover - Elastic** tab is active.
- Index patterns - Elastic** tab is visible.
- Selected fields** (clientip, machine.os, memory, request, bytes) are highlighted with a red box.
- Available fields** list includes: Popular (phpmemory), _id, _index, _score, _type, @timestamp.
- Chart**: 2,556 hits from Sep 21, 2021 to Oct 21, 2021. The chart shows a peak around October 11th.
- Table**: timestamp per 12 hours. The table lists log entries with columns: Time, clientip, machine.os, memory, request, bytes. The first few rows are:

Time	clientip	machine.os	memory	request	bytes
> Oct 21, 2021 @ 04:45:10.997	213.253.23.28	osx	-	/styles/ad-blocker.css	3,705
> Oct 21, 2021 @ 04:21:52.666	137.194.72.25	osx	-	/	6,811
> Oct 21, 2021 @ 03:47:30.594	15.225.65.207	ios	-	/styles/semantic-ui.css	8,274



Kibana Analytics - Document Details

Discover - Elastic Index patterns - Elastic Not Secure | 192.168.1.211:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-30d%2Fd,to:now))&_a=(columns:!(),filters:!(),index:'90943e30-9a47-11e8-b6... Options New Save Open Share Inspect elastic Search Elastic KQL Last 30 days Show dates Refresh + Add filter kibana_sample_data_logs 2,556 hits Sep 21, 2021 @ 00:00:00.000 - Oct 21, 2021 @ 04:52:43.692 Auto Hide chart Search field names Filter by type 0 Popular bytes clientip machine.os memory phpmemory request _id _index _score _type @timestamp agent event.dataset extension timestamp per 12 hours Time Document Oct 21, 2021 @ 04:45:10.997 @timestamp: Oct 21, 2021 @ 04:45:10.997 agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) bytes: 3,705 clientip: 213.253.23.28 event.dataset: sample_web_logs extension: css geo.coordinates: { "coordinates": [-102.9852778, 41.10133333], "type": "Point" } geo.dest: BD geo.src: JP geo.srctest: JP:BD host: cdn.elastic-elastic.elastic.org hour_of_day: 21 index: kibana_sample_data_logs ip: 213.253.23.28 machine.os: osx machine.ram: 8,589,934,592 message: 213.253.23.28 -- [2018-08-01T21:45:10.997Z] "GET /styles/ad-blocker.css HTTP/1.1" 200 3705 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" timestamp: Oct 21, 2021 @ 04:45:10.997 View surrounding documents View single document Expanded document Table JSON Actions Field Value _id 1bUanXwBe1WmaeFXilNj _index kibana_sample_data_logs gsm.csv Show All



Kibana Analytics - Document Details - JSON

Discover - Elastic Index patterns - Elastic Not Secure | 192.168.1.211:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-30d%2Fd,to:now))&_a=(columns:!(),filters:!(),index:'90943e30-9a47-11e8-b6... Options New Save Open Share Inspect elastic Search KQL Last 30 days Show dates Refresh + Add filter kibana_sample_data_logs 2,556 hits Sep 21, 2021 @ 00:00:00.000 - Oct 21, 2021 @ 04:52:43.692 Auto Hide chart Count 200 150 100 50 0 2021-09-21 00:00 2021-09-25 00:00 2021-09-29 00:00 2021-10-03 00:00 2021-10-07 00:00 2021-10-11 00:00 2021-10-15 00:00 2021-10-19 00:00 timestamp per 12 hours Time Document Oct 21, 2021 @ 04:45:10.997 @timestamp: Oct 21, 2021 @ 04:45:10.997 agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) bytes: 3,705 clientip: 213.253.23.28 event.dataset: sample_web_logs extension: css geo.coordinates: { "coordinates": [-102.9852778, 41.10133333], "type": "Point" } geo.dest: BD geo.src: JP geo.srctest: JP:BD host: cdn.elastic-elastic.org hour_of_day: 21 index: kibana_sample_data_logs ip: 213.253.23.28 machine.os: osx machine.ram: 8,589,934,592 message: 213.253.23.28 -- [2018-08-01T21:45:10.997Z] "GET /styles/ad-blocker.css HTTP/1.1" 200 3705 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; -- Expanded document View surrounding documents View single document Table JSON Copy to clipboard 1 { 2 " _index": "kibana_sample_data_logs", 3 " _type": " _doc", gsm.csv Show All X



Kibana Analytics - Document Details - JSON

Discover - Elastic Index patterns - Elastic Not Secure | 192.168.1.211:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-30d%2Fd,to:now))&_a=(columns:!(),filters:!(),index:'90943e30-9a47-11e8-b6...)

elastic Search Elastic Options New Save Open Share Inspect

Discover Search KQL Last 30 days Show dates Refresh

+ Add filter

kibana_sample_data_logs

2,556 hits Sep 21, 2021 @ 00:00:00.000 - Oct 21, 2021 @ 04:52:43.692 Auto Hide chart

Count

2021-09-21 00:00 2021-09-25 00:00 2021-09-29 00:00 2021-10-03 00:00 2021-10-07 00:00 2021-10-11 00:00 2021-10-15 00:00 2021-10-19 00:00 timestamp per 12 hours

Popular

- # bytes
- IP clientip
- t machine.os
- # memory
- # phpmemory
- t request
- t _id
- t _index
- # _score
- t _type
- @timestamp
- t agent
- t event.dataset
- t extension

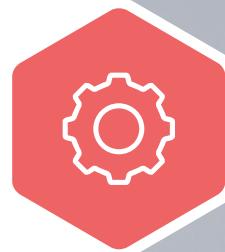
1 {
2 " _index": "kibana_sample_data_logs",
3 " _type": "_doc",
4 " _id": "1bUanXwBe1WmaeFXilNj",
5 " _version": 1,
6 " _score": 1,
7 " _source": {
8 "agent": "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)",
9 "bytes": 3705,
10 "clientip": "213.253.23.28",
11 "extension": "css",
12 "geo": {
13 "srcdest": "JP:BD",
14 "src": "JP",
15 "dest": "BD",
16 "coordinates": {
17 "lat": 41.10133333,

gsm.csv Show All



Simple Dashboard

Visualized in The First Step



Kibana : Create Dashboard

The screenshot shows the Kibana Dashboards interface. At the top, there are tabs for 'Dashboards - Elastic' and 'Index patterns - Elastic'. The URL bar indicates a non-secure connection to 192.168.1.211:5601. A search bar at the top right contains the text 'Search Elastic'. On the left, there's a sidebar with a menu icon and a 'Dashboard' tab. The main area is titled 'Dashboards' and features a 'Create dashboard' button. Below this is a search bar and a 'Tags' dropdown. A table lists three dashboards:

<input type="checkbox"/> Title	Description	Tags	Actions
<input type="checkbox"/> [Flights] Global Flight Dashboard	Analyze mock flight data for ES-Air, Logstash Airways, Kibana Airlines and JetBeats		
<input type="checkbox"/> [Logs] Web Traffic	Analyze mock web traffic log data for Elastic's website		
<input type="checkbox"/> [eCommerce] Revenue Dashboard	Analyze mock eCommerce orders and revenue		

At the bottom, there are pagination controls for 'Rows per page: 20' and page number '1'. A footer bar at the bottom includes a file icon, 'gsm.csv', a 'Show All' button, and a close button.



Kibana : Create Dashboard

The screenshot shows the Kibana interface for creating a new dashboard. At the top, there are tabs for 'New Dashboard - Elastic' and 'Index patterns - Elastic'. The URL bar indicates a connection to '192.168.1.211:5601/app/dashboards#create?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-7d,to:now))'. The main header includes the 'elastic' logo, a search bar, and navigation links for 'Options', 'Share', 'Switch to view mode', and 'Save'.

The dashboard area has a toolbar with buttons for 'Create visualization' (highlighted in blue), 'Search', 'KQL', 'Last 7 days', 'Show dates', and 'Refresh'. Below the toolbar, there's a section for 'Add filter' and a 'Create visualization' card with the text 'Add your first visualization' and a description: 'Create content that tells a story about your data.' There are also buttons for 'All types' and 'Add from library'.

At the bottom, a footer bar shows a file icon next to 'gsm.csv' and a 'Show All' button.



Kibana : Create Visualization

The screenshot shows the Kibana interface for creating a new dashboard. The top navigation bar includes tabs for 'New Dashboard - Elastic', 'Index patterns - Elastic', 'TSVB | Kibana Guide [master]', and a plus sign icon. The URL bar indicates a connection to '192.168.1.211:5601/app/dashboards#create?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-7d,to:now))'. The main header has sections for 'Dashboard' (selected), 'Editing New Dashboard', 'Options', 'Share', 'Switch to view mode', and a 'Save' button.

The search bar contains 'Search Elastic'. Below it are filters for 'KQL' and 'Last 7 days', along with 'Show dates' and 'Refresh' buttons.

The main area features a 'Create visualization' button in blue, followed by three icons: a scatter plot, a map pin, and a magnifying glass. A dropdown menu titled 'All types' is open, listing various visualization types:

- Lens
- Maps
- Machine Learning >
- Log stream
- TSVB
- </> Custom visualization
- Aggregation based >
- Controls
- Text

A tooltip for 'All types' says: 'Select the type of visualization you want to add. You can also search for specific visualization types in the library.' Below this is a placeholder text: 'Add your first visualization' and 'Create content that tells a story about your data.'

The bottom navigation bar shows a file icon next to 'gsm.csv' and a 'Show All' button.



Kibana : Create Visualization

The screenshot shows the Kibana interface for creating a new dashboard. The top navigation bar includes tabs for 'New Dashboard - Elastic', 'Index patterns - Elastic', 'TSVB | Kibana Guide [master]', and a plus sign icon. The URL bar indicates a connection to '192.168.1.211:5601/app/dashboards#create?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-7d,to:now))'. The main header has sections for 'Dashboard' (selected), 'Editing New Dashboard', 'Options', 'Share', 'Switch to view mode', and a 'Save' button.

Below the header, there are search and filter controls, including a 'Search' field, a 'KQL' button, a date range selector set to 'Last 7 days', and buttons for 'Show dates' and 'Refresh'.

The central area features a large 'Create visualization' button with a chart icon, followed by other buttons for 'Lens', 'Maps', 'Machine Learning', 'Log stream', 'TSVB', 'Custom visualization', 'Aggregation based', 'Controls', and 'Text'. A tooltip for 'All types' is visible above the 'Add from library' button.

At the bottom, a file selection bar shows 'gsm.csv' and a 'Show All' button.



Kibana : Len

The screenshot shows the Kibana Lens interface. On the left, a red callout bubble labeled "field" points to the "Available fields" section, which lists various Elasticsearch fields like category.keyword, currency, etc. In the center, a red callout bubble labeled "Visualization type" points to the "Bar vertical stacked" visualization type. To the right, another red callout bubble labeled "Index Pattern" points to the "kibana_sample_data_ecommerce" index pattern. A final red callout bubble labeled "Visualization Properties" points to the "Horizontal axis", "Vertical axis", and "Break down by" sections on the right side of the interface.

Lens - Elastic Index patterns - Elastic TSVB | Kibana Guide [master] Not Secure | 192.168.1.211:5601/app/lens#/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-7d,to:now)) elastic Search elastic D Dashboard Create Download as CSV Cancel Save to library Save and return KQL Last 7 days Show dates Refresh

Search + Add filter

kibana_sample_data_eco... ...

Search field names Filter by type 0 Records Available fields 45

category.keyword currency customer_first_name.keyword customer_full_name.keyword customer_gender customer_id customer_last_name.keyword

Bar vertical stacked

Drop some fields here to start

Lens is a new tool for creating visualization

Make requests and give feedback

Horizontal axis

Vertical axis

Break down by

Add layer

gsm.csv Show All

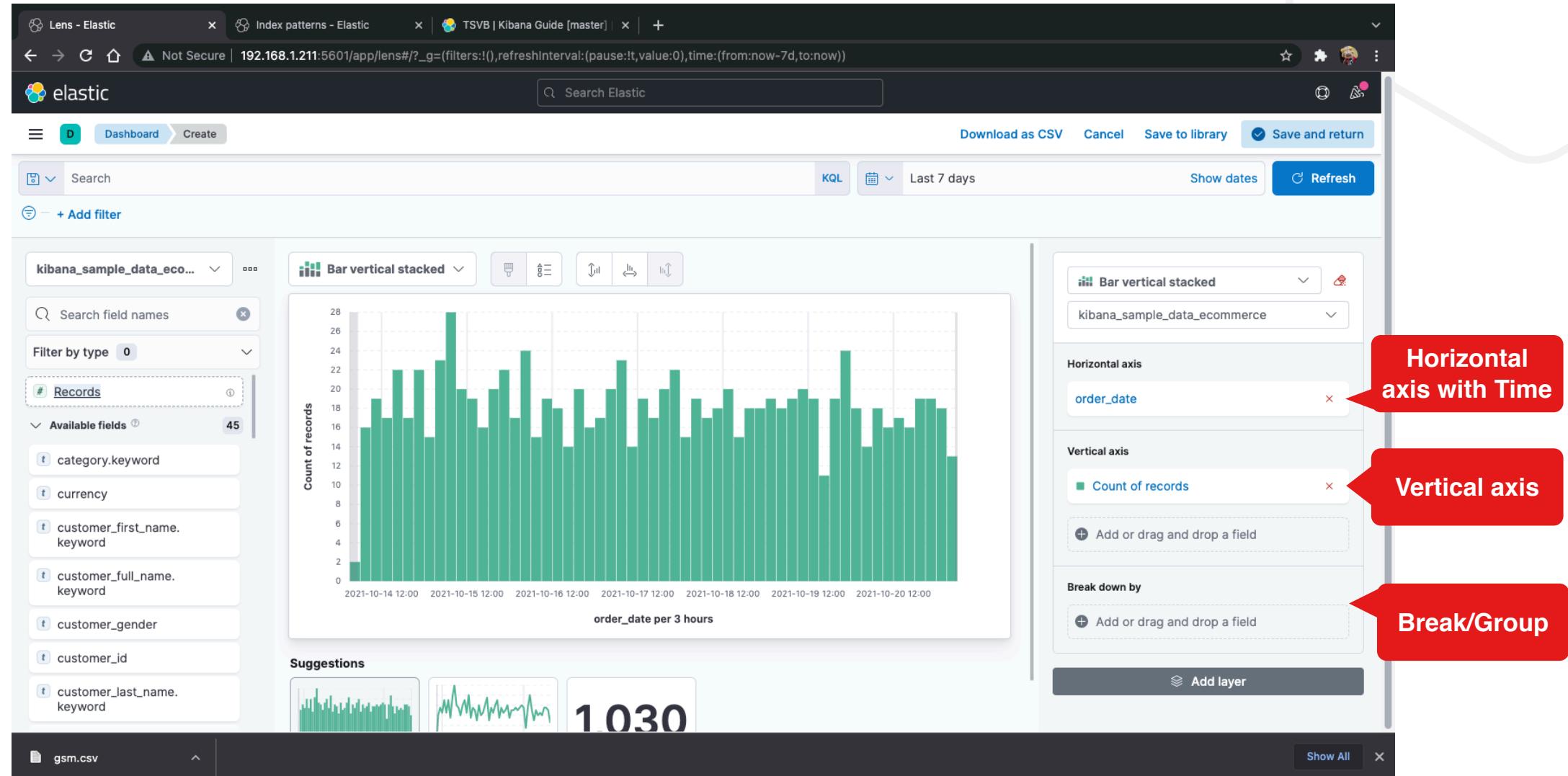


Kibana : Len

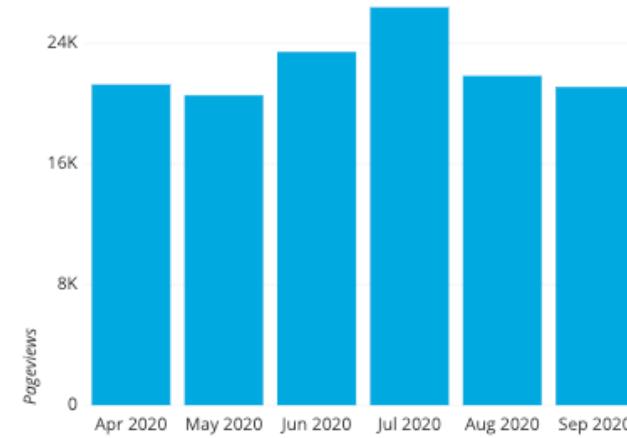
The screenshot shows the Kibana Lens interface for creating visualizations. The top navigation bar includes tabs for 'Lens - Elastic', 'Index patterns - Elastic', and 'TSVB | Kibana Guide [master]'. The main area is titled 'Bar vertical stacked' and shows a placeholder message: 'Drop some fields here to start'. On the left, there's a sidebar with 'Available fields' listed under 'Records' and 'Available fields'. A red arrow points from the 'Available fields' dropdown to the central workspace. The right side contains configuration panels for 'Horizontal axis', 'Vertical axis', and 'Break down by', each with 'Add or drag and drop a field' buttons. At the bottom, there's a file selection dropdown for 'gsm.csv' and buttons for 'Show All' and 'X'.



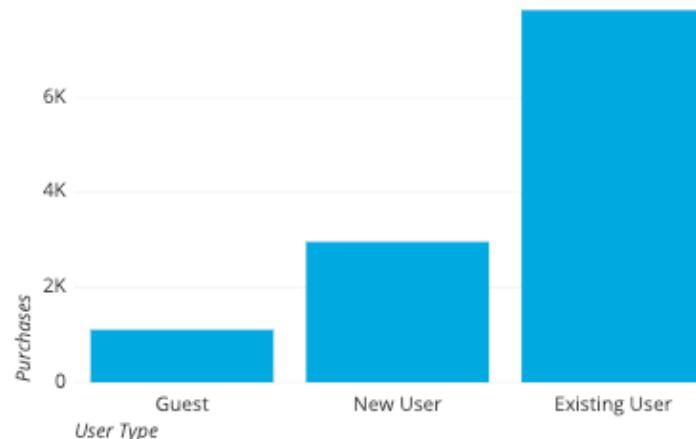
Kibana : Len



Kibana : Bar Chart



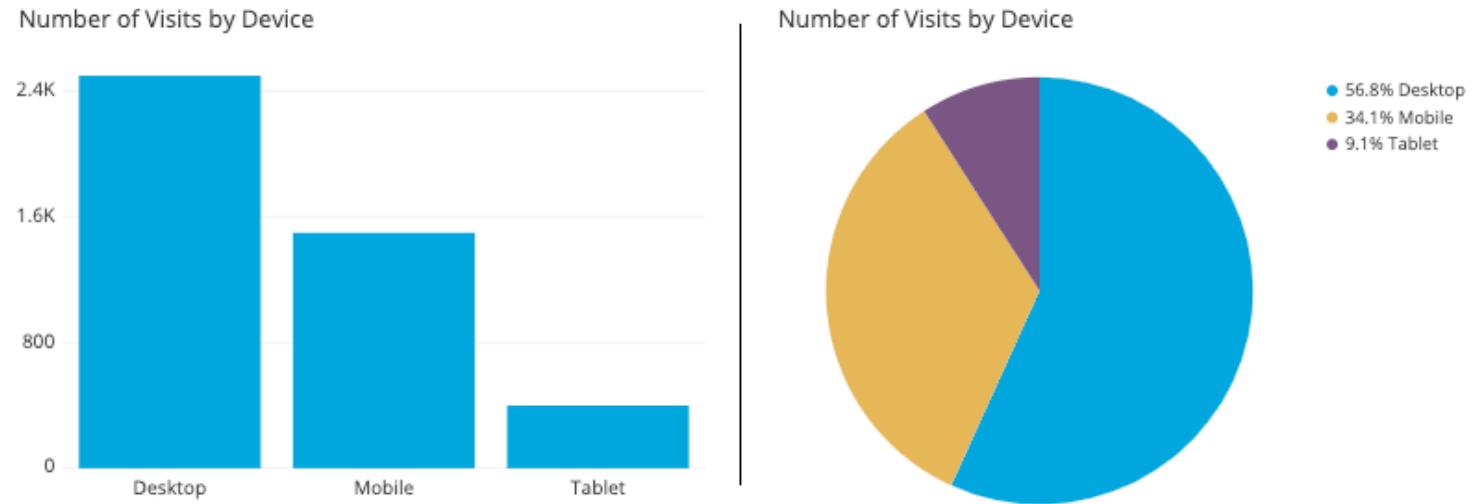
Purchases by User Type



A bar chart is used when you want to show a **distribution of data points** or perform a **comparison of metric values** across different subgroups of your data. From a bar chart, we can see which groups are highest or most common, and how other groups compare against the others. Since this is a fairly common task, bar charts are a fairly ubiquitous chart type.



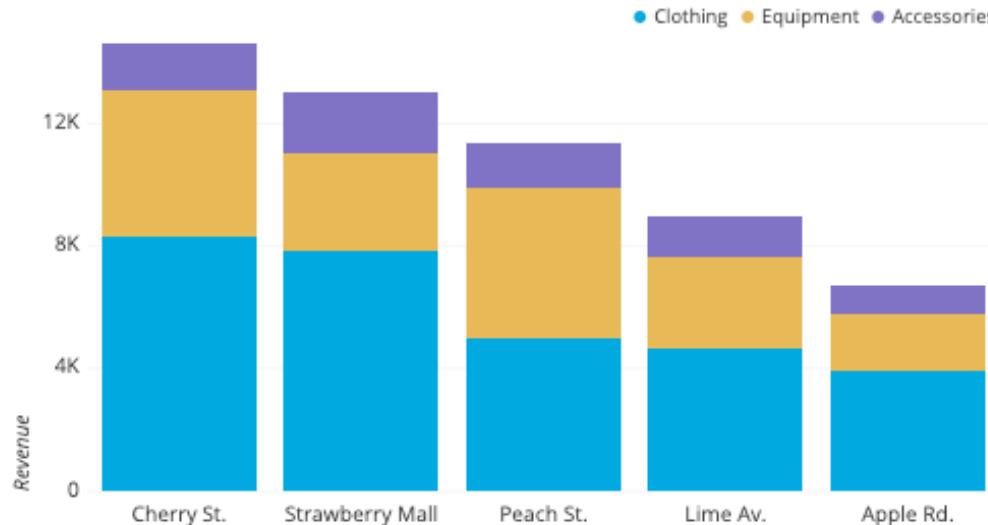
Kibana : Pie Chart



A **pie chart** shows how a total amount is divided between levels of a categorical variable as a circle divided into radial slices. Each categorical value corresponds with a single slice of the circle, and the size of each slice (both in area and arc length) indicates what proportion of the whole each category level takes.



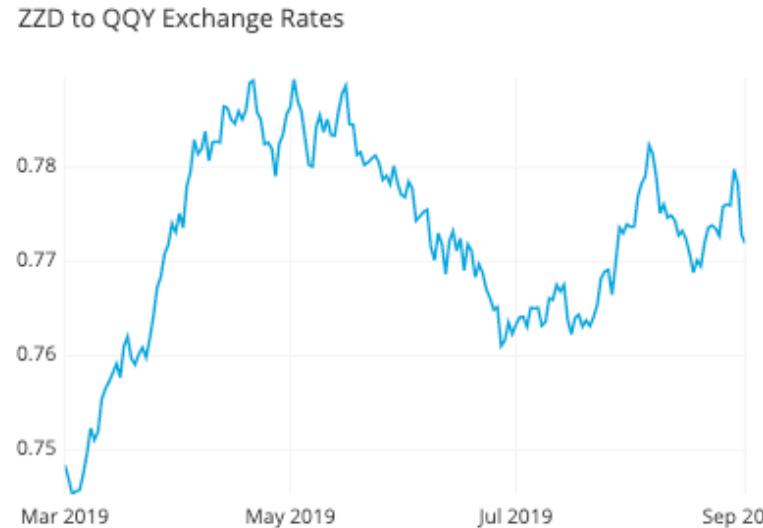
Kibana : Stacked Bar Chart



The stacked bar chart (aka stacked bar graph) extends the standard [bar chart](#) from looking at numeric values across one categorical variable to two. Each bar in a standard bar chart is divided into a number of sub-bars stacked end to end, each one corresponding to a level of the second categorical variable.



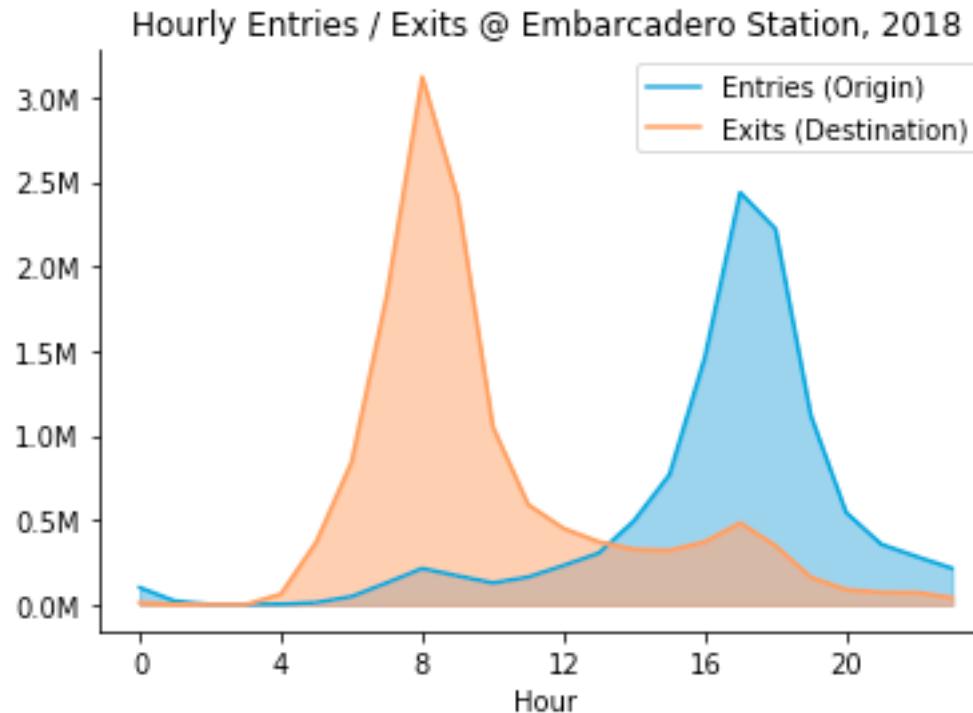
Kibana : Line Chart



A line chart (aka line plot, line graph) uses points connected by line segments from left to right to demonstrate changes in value. The horizontal axis depicts a continuous progression, often that of time, while the vertical axis reports values for a metric of interest across that progression.



Kibana : Area Chart



An **area chart** combines the [line chart](#) and [bar chart](#) to show how one or more groups' numeric values change over the progression of a second variable, typically that of time. An area chart is distinguished from a line chart by the addition of shading between lines and a baseline, like in a bar chart.





Thanks
For 1st Day

Shopping-Cart : Selected Business Scenario



อยากรื้อสินค้า



Shopping-Cart : Selected Business Scenario



อยากรื้อสินค้า



Shopping-Cart : Selected Business Scenario



อยากรื้อสินค้า



Shopping-Cart : Selected Business Scenario



อยากรื้อสินค้า

