

Video 1.3

Installing Elasticsearch





In this Video, we are going to take a look at...

- Installing Elasticsearch
- Starting up cluster
- Installing Kibana
- Viewing Kibana from browser



1x



Browse Q&A

Add Bookmark

Continue >

0:08 / 6:34



Install Elasticsearch

- Requirements for Elasticsearch 5.0 installation: Must have Java 7 or higher installed
- Download from: <https://www.elastic.co/downloads/elasticsearch>
- Extract downloaded file into a directory
- Map to directory containing Elasticsearch
- Run command to start cluster

Start ElasticSearch Cluster

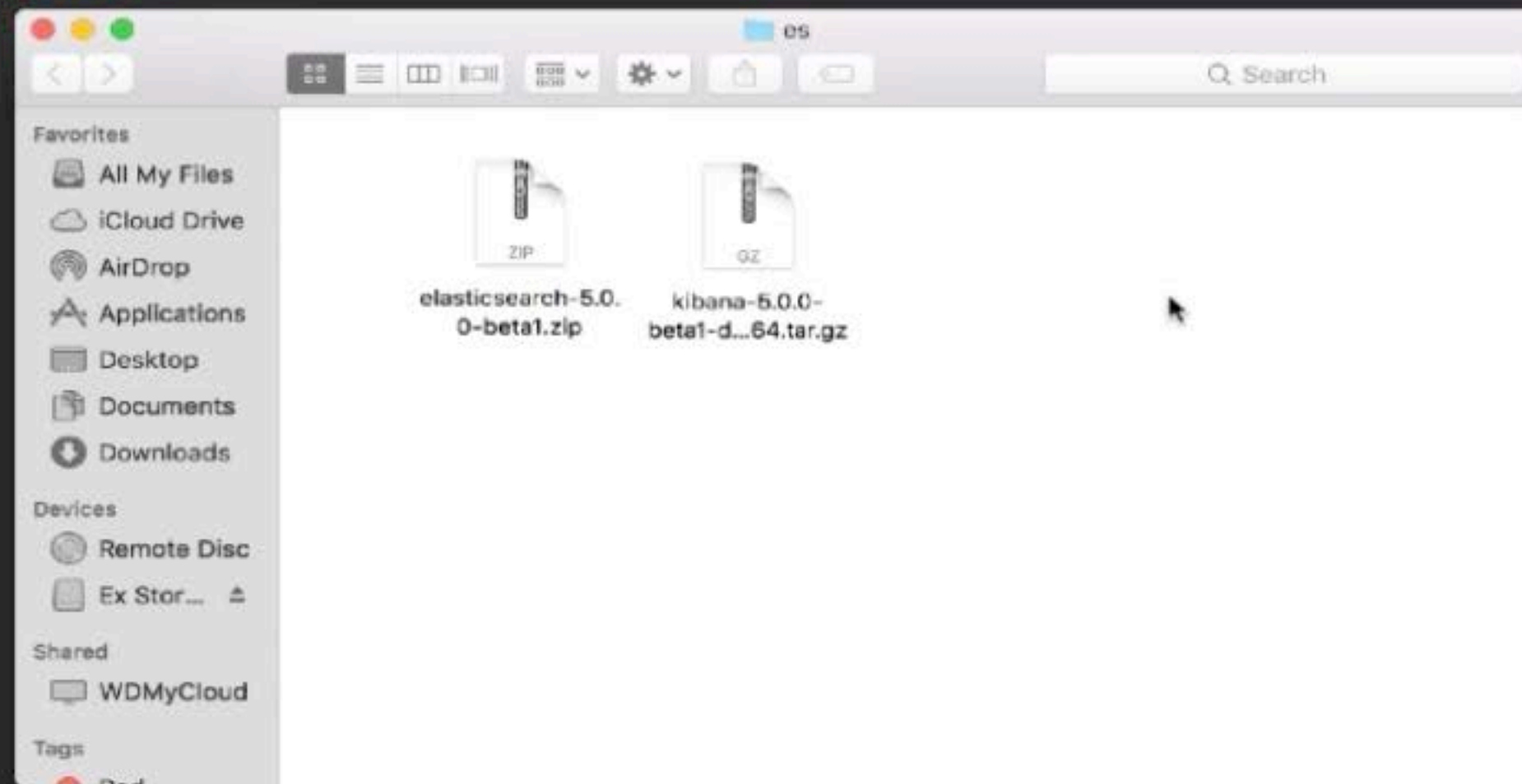
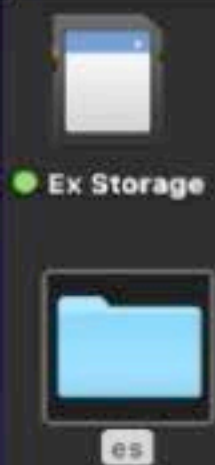
- Run command to start cluster:
 - [unix/mac] bin/elasticsearch
 - [windows] bin\elasticsearch

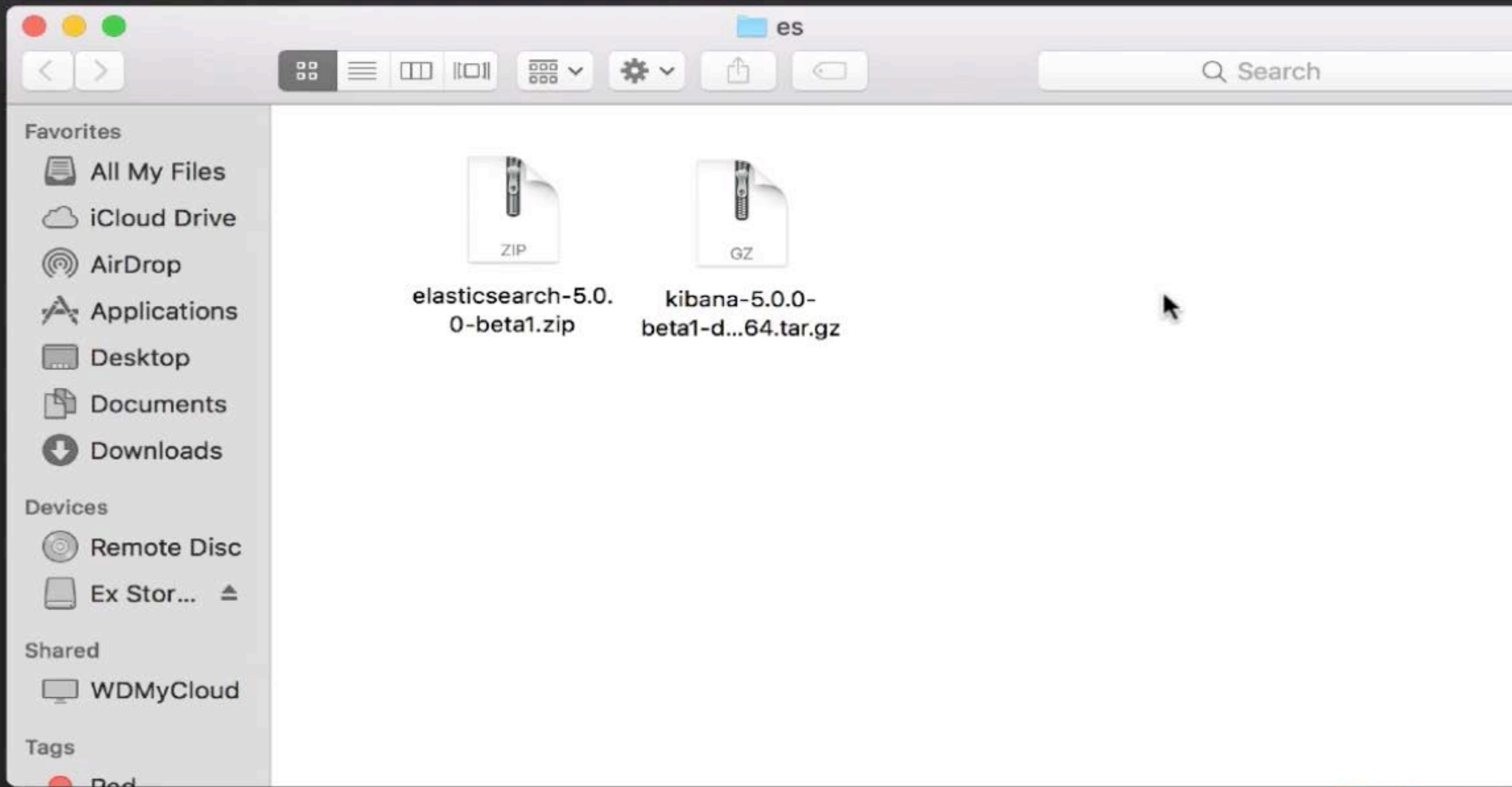
Install Kibana

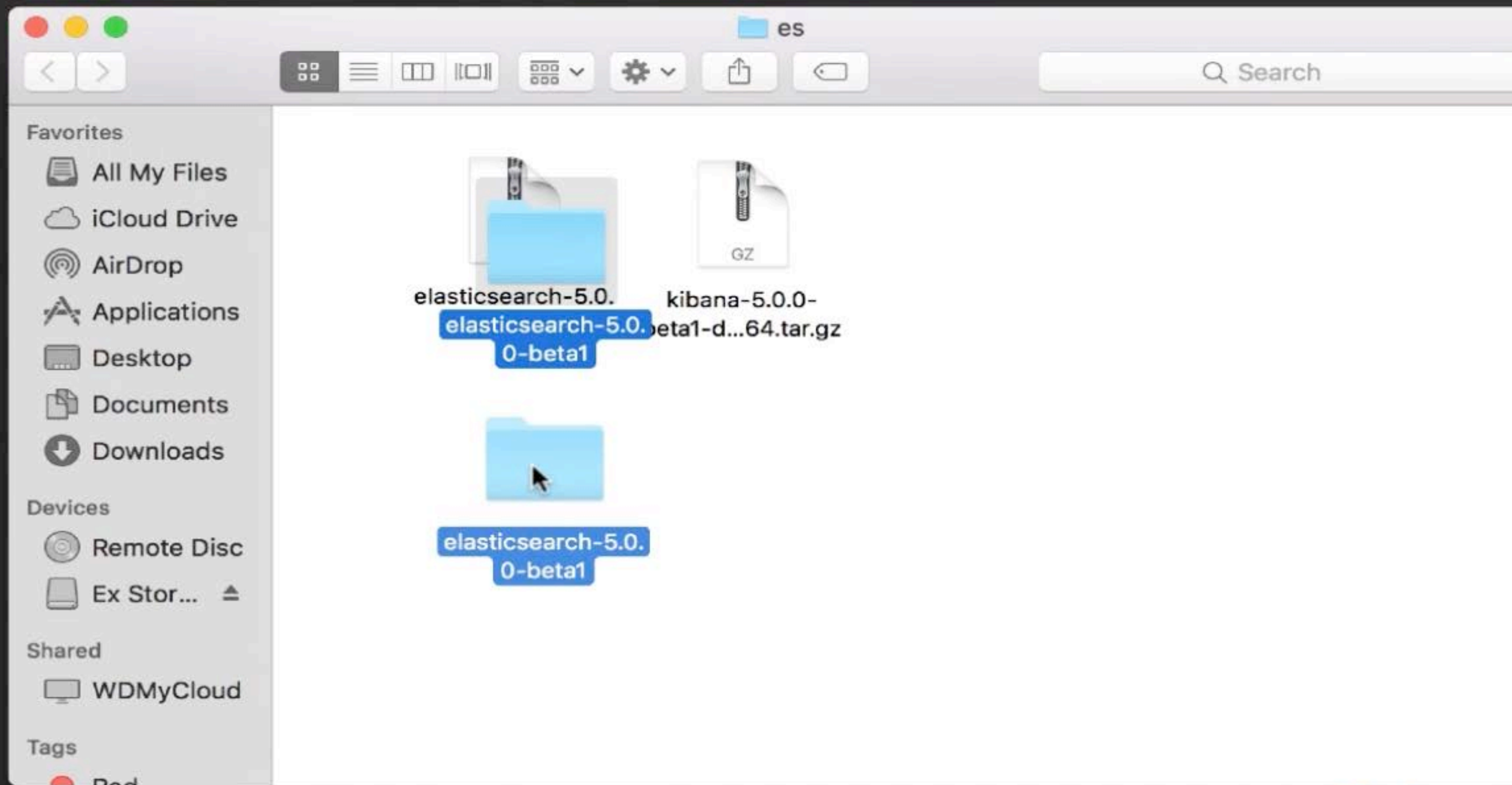
- Download from: <https://www.elastic.co/downloads/kibana>
- Extract downloaded file into a directory
- Map to directory containing Kibana

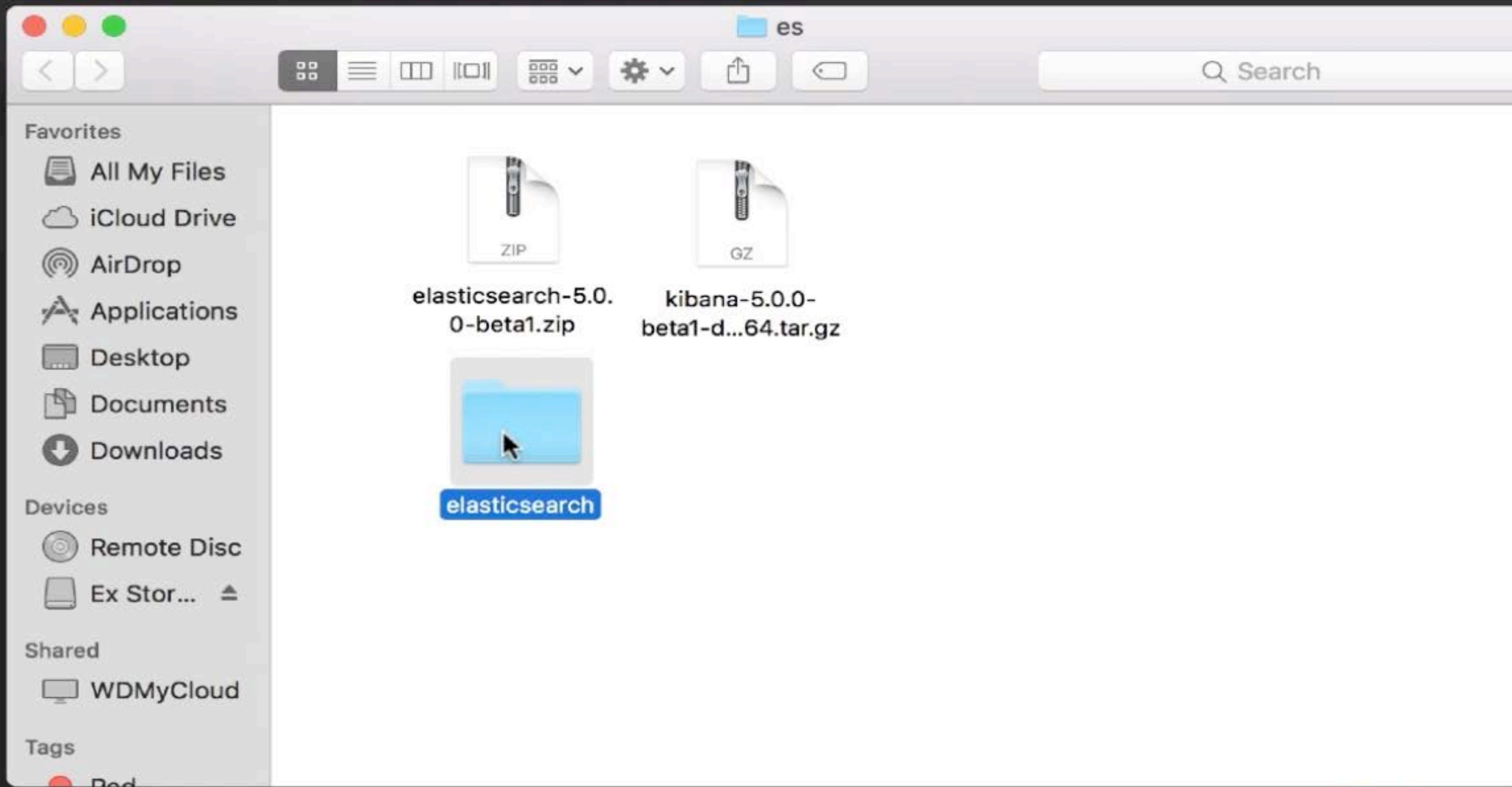
Start Kibana and View in Browser

- Edit kibana config file
- Run command to start Kibana:
 - unix/mac] bin/kibana
 - [windows] bin\kibana.bat
- Point browser to <http://localhost:5601>









Navigation icons: < >

Favorites

- All My Files
- iCloud Drive
- AirDrop
- Applications
- Desktop
- Documents
- Downloads

Devices

- Remote Disc
- Ex Stor...

Shared

- WDMycloud

Tags

- Red

Archive Utility

Expanding "kibana-5.0.0-beta1-darwin-x86_64.tar.gz"...

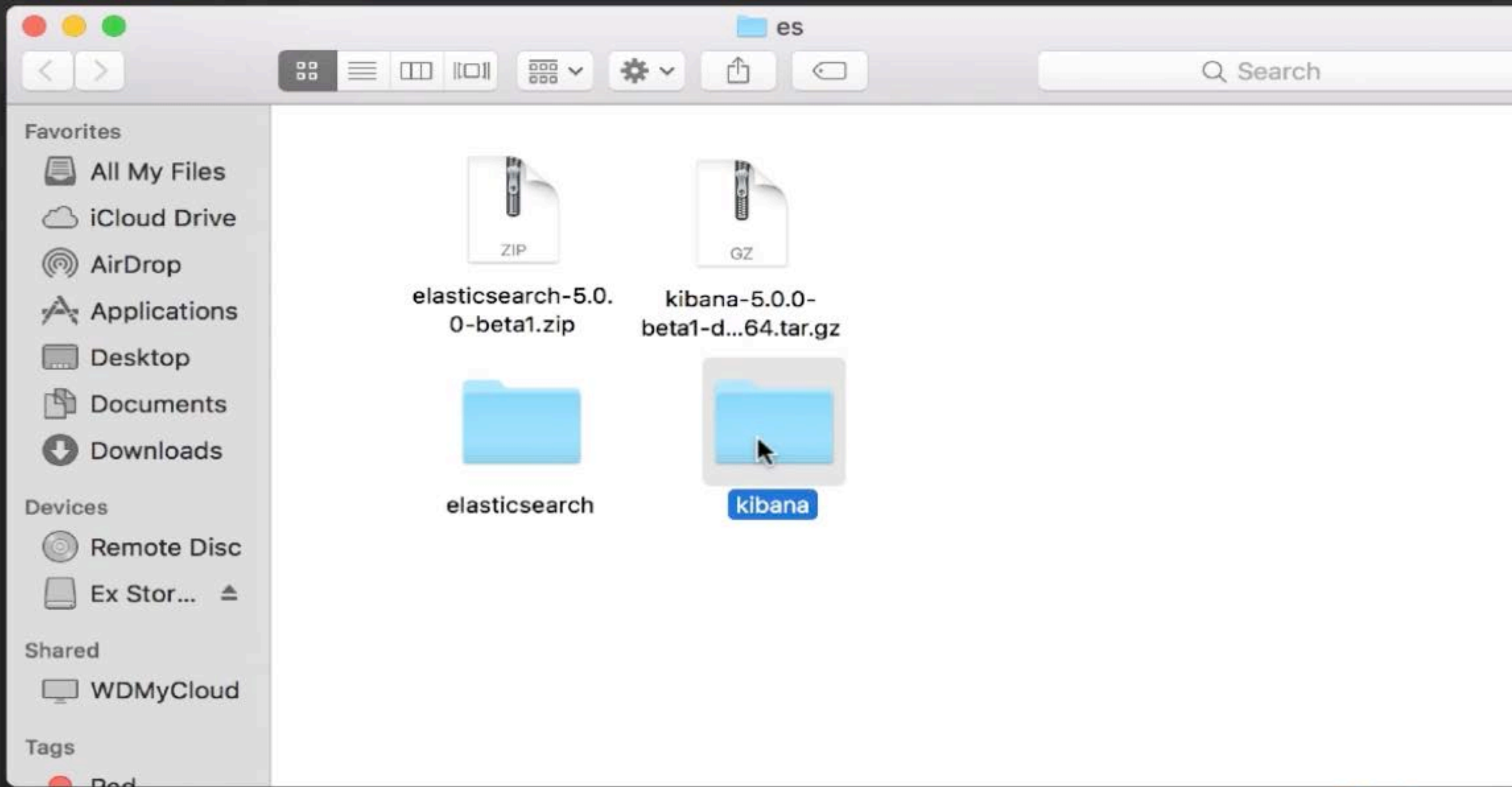
Progress bar (approx. 40% complete)

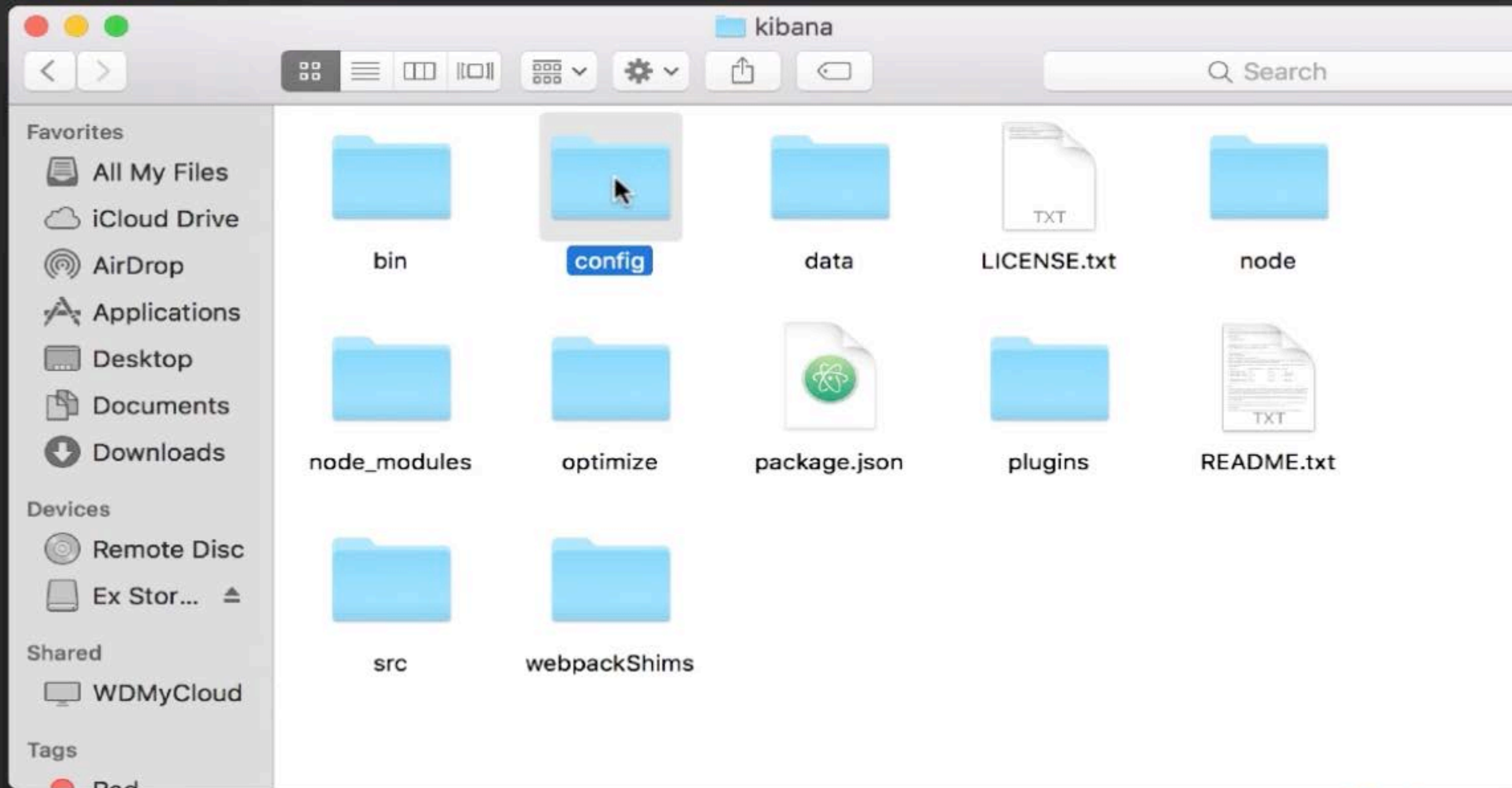
Cancel

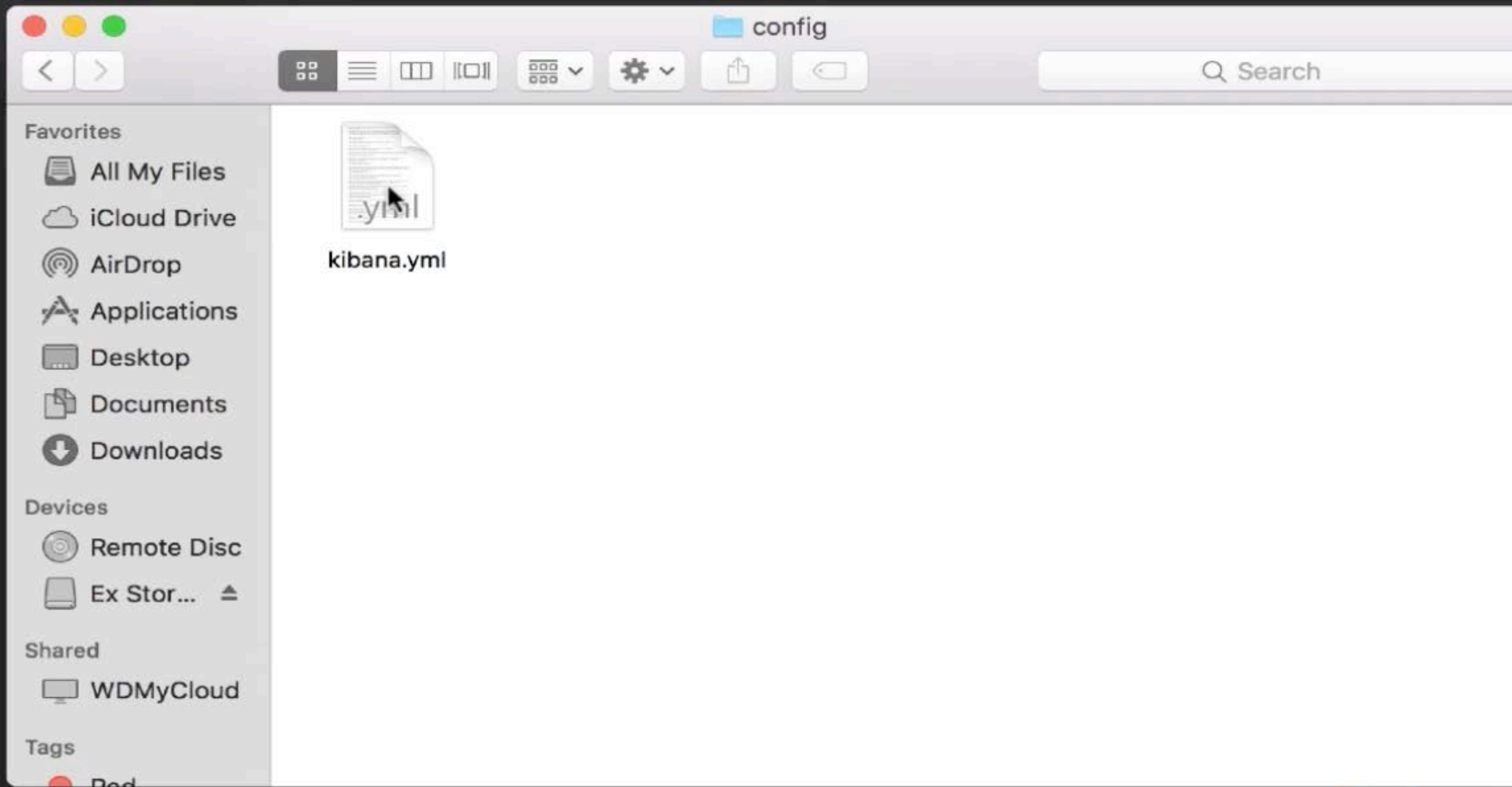
ZIP GZ

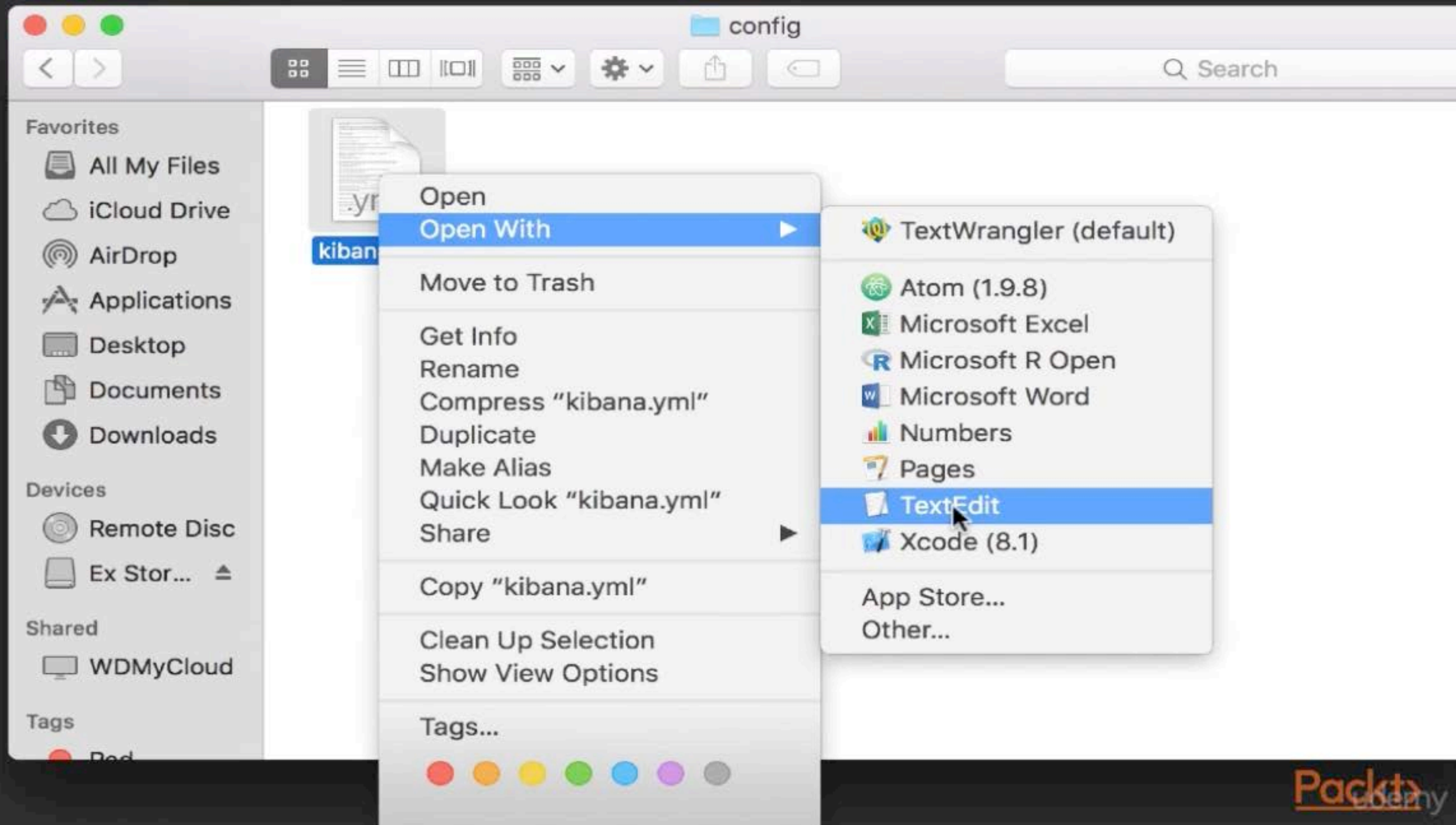
elasticsearch-5.0.0-beta1.zip kibana-5.0.0-beta1-darwin-x86_64.tar.gz

elasticsearch









connect

```
# To allow connections from remote users, set this parameter to a non-loopback address.
# server.host: "localhost"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy. This
# setting
# cannot end in a slash.
# server.basePath: ""

# The maximum payload size in bytes for incoming server requests.
# server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.
# server.name: "your-hostname"

# The URL of the Elasticsearch instance to use for all your queries.
# elasticsearch.url: "http://localhost:9200"

# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
# elasticsearch.preserveHost: true

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
# kibana.index: ".kibana"

# The default application to load.
# kibana.defaultAppId: "discover"

# If your Elasticsearch is protected with basic authentication, these settings provide
```

elastic search.url: "http://localhost:9200"

kibana.yml — Edited

```
# To allow connections from remote users, set this parameter to a non-loopback address.
# server.host: "localhost"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy. This
# setting
# cannot end in a slash.
# server.basePath: ""

# The maximum payload size in bytes for incoming server requests.
# server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.
# server.name: "your-hostname"

# The URL of the Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://localhost:9200"

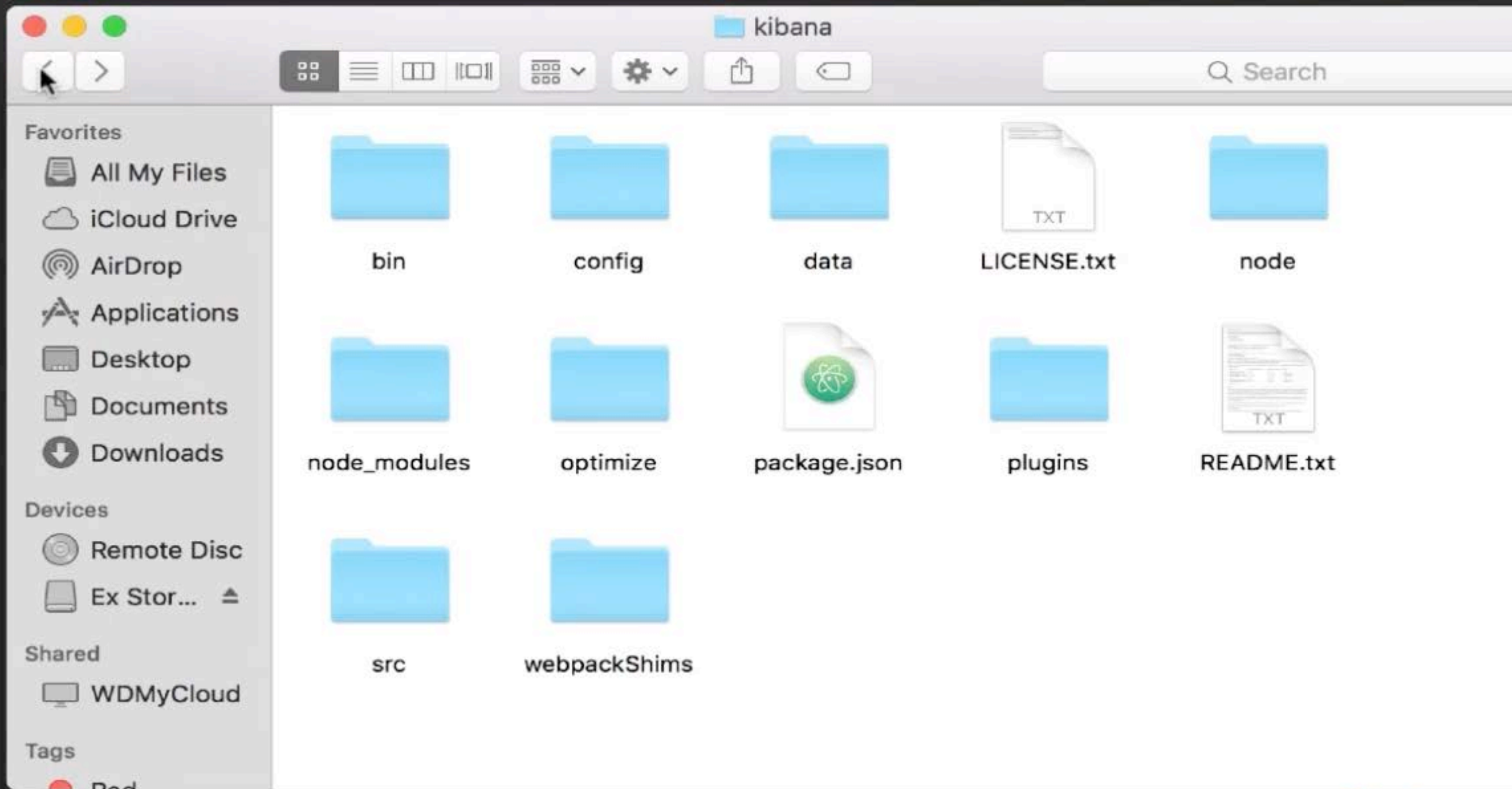
# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
# elasticsearch.preserveHost: true

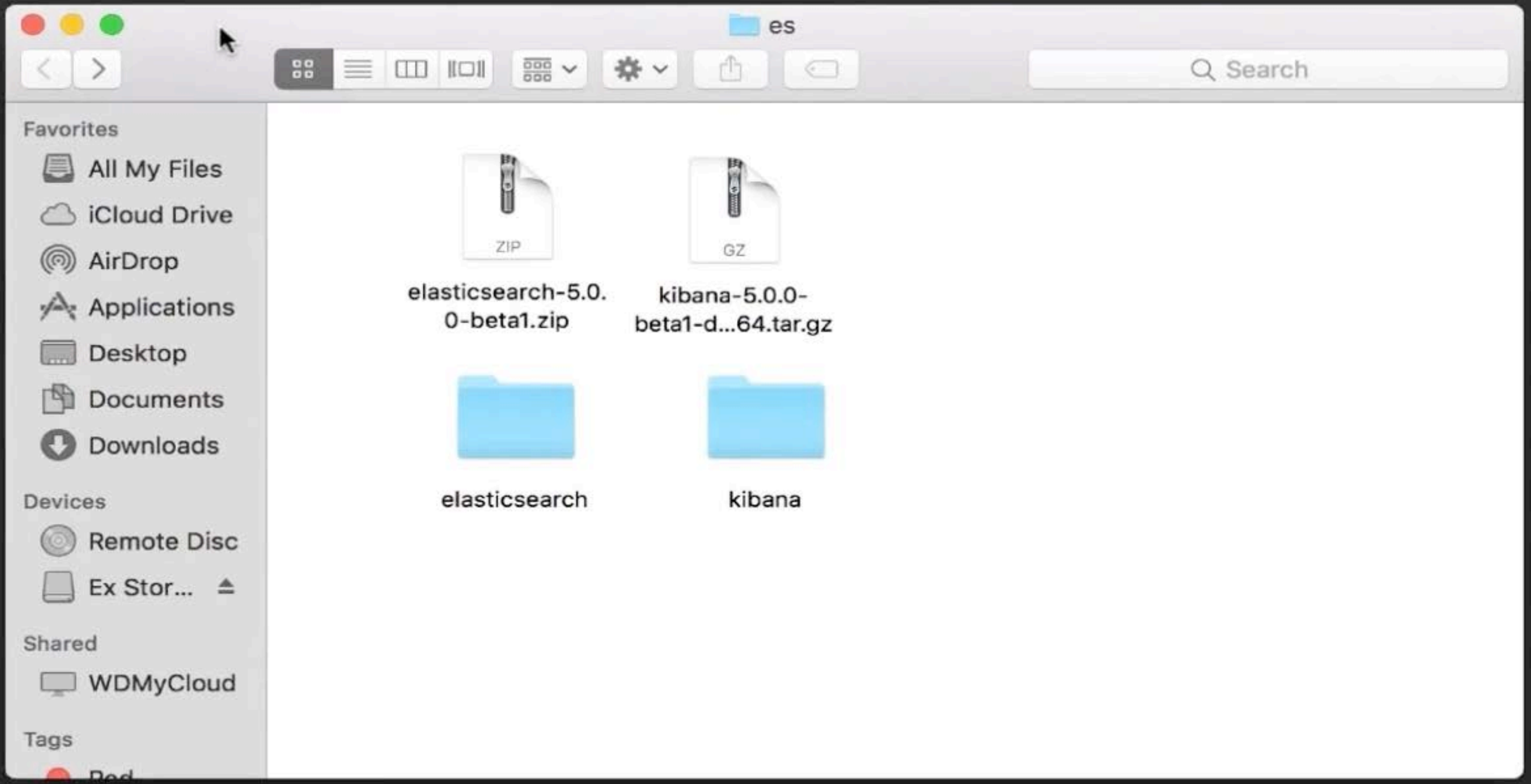
# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
# kibana.index: ".kibana"

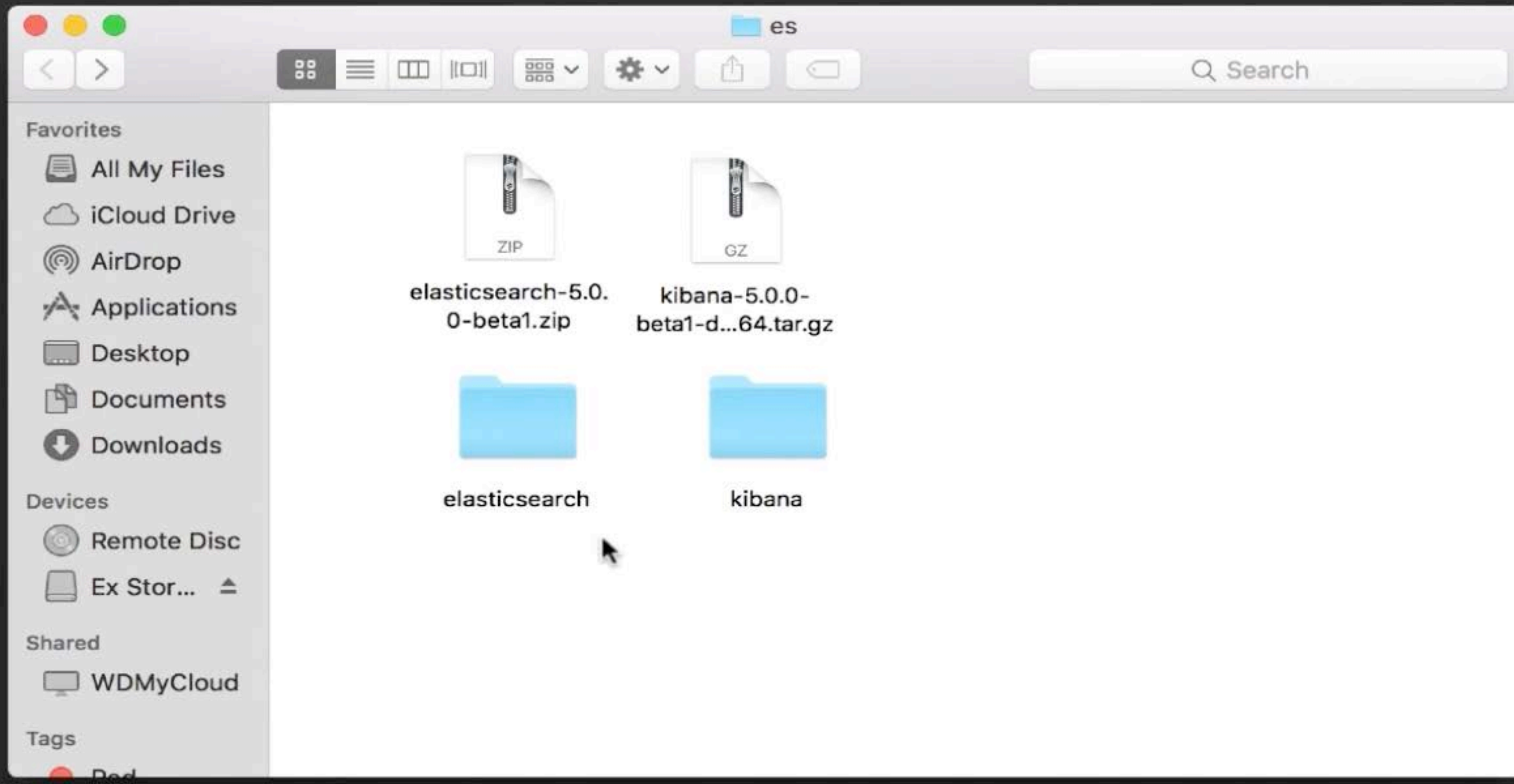
# The default application to load.
# kibana.defaultAppId: "discover"

# If your Elasticsearch is protected with basic authentication, these settings provide
```

elastic search.url: "http://localhost:9200"







Last login: Wed Nov 9 17:13:10 on ttys002

-bash: export: `Plug-Ins/JavaAppletPlugin.plugin/Contents/Home": not a valid identifier

Ethans-MacBook-Pro-2:~ eaofxr\$

```
Last login: Wed Nov  9 17:13:10 on ttys002
-bash: export: `Plug-Ins/JavaAppletPlugin.plugin/Contents/Home": not a valid identifier
Ethans-MacBook-Pro-2:~ eaofxr$ cd /Users/eaofxr/Desktop/es/elasticsearch
Ethans-MacBook-Pro-2:elasticsearch eaofxr$
```

```
Last login: Wed Nov  9 17:13:10 on ttys002
-bash: export: `Plug-Ins/JavaAppletPlugin.plugin/Contents/Home": not a valid identifier
Ethans-MacBook-Pro-2:~ eaofxr$ cd /Users/eaofxr/Desktop/es/elasticsearch
Ethans-MacBook-Pro-2:elasticsearch eaofxr$ bin/elasticsearch
```

```
Last login: Wed Nov 9 17:13:10 on ttys002
-bash: export: `Plug-Ins/JavaAppletPlugin.plugin/Contents/Home`: not a valid identifier
Ethans-MacBook-Pro-2:~ eaofxr$ cd /Users/eaofxr/Desktop/es/elasticsearch
Ethans-MacBook-Pro-2:elasticsearch eaofxr$ bin/elasticsearch
[2016-11-09T17:20:21,192][INFO ][o.e.n.Node                ] [ ] initializing ...
[2016-11-09T17:20:21,258][INFO ][o.e.e.NodeEnvironment    ] [s11_nY_] using [1] data paths, mounts [[/ (/dev/disk1)], net usable_
space [104.8gb], net total_space [232.6gb], spins? [unknown], types [hfs]
[2016-11-09T17:20:21,258][INFO ][o.e.e.NodeEnvironment    ] [s11_nY_] heap size [1.9gb], compressed ordinary object pointers [true
]
[2016-11-09T17:20:21,259][INFO ][o.e.n.Node                ] [s11_nY_] node name [s11_nY_] derived from node ID; set [node.name] to
override
[2016-11-09T17:20:21,261][INFO ][o.e.n.Node                ] [s11_nY_] version[5.0.0-beta1], pid[4807], build[7eb6260/2016-09-20T23
:10:37.942Z], OS[Mac OS X/10.12.1/x86_64], JVM[Oracle Corporation/Java HotSpot(TM) 64-Bit Server VM/1.8.0_111/25.111-b14]
[2016-11-09T17:20:21,881][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [aggs-matrix-stats]
[2016-11-09T17:20:21,881][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [ingest-common]
[2016-11-09T17:20:21,881][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [lang-expression]
[2016-11-09T17:20:21,881][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [lang-groovy]
[2016-11-09T17:20:21,881][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [lang-mustache]
[2016-11-09T17:20:21,882][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [lang-painless]
[2016-11-09T17:20:21,882][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [percolator]
[2016-11-09T17:20:21,882][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [reindex]
[2016-11-09T17:20:21,882][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [transport-netty3]
[2016-11-09T17:20:21,882][INFO ][o.e.p.PluginsService        ] [s11_nY_] loaded module [transport-netty4]
[2016-11-09T17:20:21,882][INFO ][o.e.p.PluginsService        ] [s11_nY_] no plugins loaded
```



```
Terminal Shell Edit View Window Help
elasticsearch
/Users/eaofxr/Desktop/es/elasticsearch
eaofxr$ bin/elasticsearch
.o.e.n.Node ] [ ] initializing ...
.o.e.e.NodeEnvironment ] [s11_nY_] using [1] data paths, mounts [[/ (/dev/disk1)], net usable_
232.6gb], spins? [unknown], types [hfs]
.o.e.e.NodeEnvironment ] [s11_nY_] heap size [1.9gb], compressed ordinary object pointers [true]
.o.e.n.Node ] [s11_nY_] node name [s11_nY_] derived from node ID; set [node.name] to
.o.e.n.Node ] [s11_nY_] version[5.0.0-beta1], pid[4807], build[7eb6260/2016-09-20T23
x86_64], JVM[Oracle Corporation/Java HotSpot(TM) 64-Bit Server VM/1.8.0_111/25.111-b14]
.o.e.p.PluginsService ] [s11_nY_] loaded module [aggs-matrix-stats]
.o.e.p.PluginsService ] [s11_nY_] loaded module [ingest-common]
.o.e.p.PluginsService ] [s11_nY_] loaded module [lang-expression]
.o.e.p.PluginsService ] [s11_nY_] loaded module [lang-groovy]
.o.e.p.PluginsService ] [s11_nY_] loaded module [lang-mustache]
.o.e.p.PluginsService ] [s11_nY_] loaded module [lang-painless]
.o.e.p.PluginsService ] [s11_nY_] loaded module [percolator]
.o.e.p.PluginsService ] [s11_nY_] loaded module [reindex]
.o.e.p.PluginsService ] [s11_nY_] loaded module [transport-netty3]
.o.e.p.PluginsService ] [s11_nY_] loaded module [transport-netty4]
.o.e.p.PluginsService ] [s11_nY_] no plugins loaded
.o.e.n.Node ] [s11_nY_] initialized
.o.e.n.Node ] [s11_nY_] starting ...
.o.e.t.TransportService ] [s11_nY_] publish_address {127.0.0.1:9300}, bound_addresses {[fe80::1]
:9300}, {[::1]:9300}, {127.0.0.1:9300}
```

Last login: Wed Nov 9 17:19:34 on ttys000

-bash: export: `Plug-Ins/JavaAppletPlugin.plugin/Contents/Home": not a valid identifier

Ethans-MacBook-Pro-2:~ eaofxr\$ cd /Users/eaofxr/Desktop/es/kibana

Ethans-MacBook-Pro-2:kibana eaofxr\$ █

Last login: Wed Nov 9 17:19:34 on ttys000

-bash: export: `Plug-Ins/JavaAppletPlugin.plugin/Contents/Home": not a valid identifier

Ethans-MacBook-Pro-2:~ eaofxr\$ cd /Users/eaofxr/Desktop/es/kibana

Ethans-MacBook-Pro-2:kibana eaofxr\$ bin/kibana

Terminal Shell Edit View Window Help kibana — node bin/./src/cli — 130x35

```
[Ethans-MacBook-Pro-2:~ eaofxr$ cd /Users/eaofxr/Desktop/es/kibana
[Ethans-MacBook-Pro-2:kibana eaofxr$ bin/kibana
log [17:21:00.160] [info][status][plugin:kibana@5.0.0-beta1] Status changed from uninitialized to green - Ready
log [17:21:00.186] [info][status][plugin:elasticsearch@5.0.0-beta1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [17:21:00.206] [info][status][plugin:console@5.0.0-beta1] Status changed from uninitialized to green - Ready
log [17:21:00.385] [info][status][plugin:timelion@5.0.0-beta1] Status changed from uninitialized to green - Ready
log [17:21:00.390] [info][listening] Server running at http://localhost:5601
log [17:21:00.391] [info][status][ui settings] Status changed from uninitialized to yellow - Elasticsearch plugin is yellow
log [17:21:05.425] [info][status][plugin:elasticsearch@5.0.0-beta1] Status changed from yellow to yellow - No existing Kibana index found
log [17:21:05.739] [info][status][plugin:elasticsearch@5.0.0-beta1] Status changed from yellow to green - Kibana index ready
log [17:21:05.740] [info][status][ui settings] Status changed from yellow to green - Ready
```

Last login: Wed Nov 9 17:20:36 on ttys001

-bash: export: `Plug-Ins/JavaAppletPlugin.plugin/Contents/Home`: not a valid identifier

Ethans-MacBook-Pro-2:~ eaofxr\$ curl http://localhost:9200


```
{
  "name" : "s11_nY_",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "vZP0jdGES9KdZX7Z1esf0w",
  "version" : {
    "number" : "5.0.0-beta1",
    "build_hash" : "7eb6260",
    "build_date" : "2016-09-20T23:10:37.942Z",
    "build_snapshot" : false,
    "lucene_version" : "6.2.0"
  },
  "tagline" : "You Know, for Search"
}
```

Ethans-MacBook-Pro-2:~ eaofxr\$ █

- localhost — localhost:5601
- Console - Kibana — localhost:5601/app/kibana#/dev_tools/console?_g=()
- Kibana — localhost:5601/app/kibana#/management/data/index/?_g=()
- Console - Kibana — localhost:5601/app/kibana#/management/data/index
- Console - Kibana — localhost:5601/app/kibana#/discover?_g=()
- Kibana — localhost:5601/app/kibana#/dev_tools?_g=()
- Kibana — localhost:5601/app/kibana#?_g=()
- Kibana — localhost:5601/app/kibana
- Kibana — localhost:5601/app/kibana#/management?_g=()

Kibana

localhost:5601/app/kibana#/management/data/index/?_g=()

kibana

Discover

Visualize


Dashboard

Timeline

Management

Dev Tools

Collapse



- Discover
- Visualize
- Dashboard
- Timelion
- Management
- Dev Tools

Warning No default index pattern.
You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

- ☒ **Index contains time-based events**
- ☐ **Use event times to create index names** [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using `*` as a wildcard. Example: `logstash-*`

- ☐ **Do not expand index pattern when searching** (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern `logstash-*` will actually query elasticsearch for the specific matching indices (e.g. `logstash-2015.12.21`) that fall within the current time range.

Unable to fetch mapping. Do you have indices matching the pattern?

Console - Kibana

localhost:5601/app/kibana#/dev_tools/console?_g=()

kibana

Discover

Visualize

Dashboard

Timeline

Management


Dev Tools

Collapse

1 GET eaofxr

1

History Settings Help

kibana

Discover

Visualize

Dashboard

Timeline

Management

Dev Tools

Collapse

Dev Tools

Console

HistorySettingsHelp


1 PUT something

1 {

2 "acknowledged": true,

3 "shards_acknowledged": true

4 }

kibana

Discover

Visualize

Dashboard

Timeline

Management

Dev Tools

Collapse

Dev Tools

Console

HistorySettingsHelp

1GET something

1-{

2 "acknowledged": true,

3 "shards_acknowledged": true

4-}

Packt>

Discover

Visualize

Dashboard

Timelion

Management

Dev Tools

Collapse

Dev Tools

Console

History

Settings

Help

1 GET something

```

1 {
2   "something": {
3     "aliases": {},
4     "mappings": {},
5     "settings": {
6       "index": {
7         "creation_date": "1478740981426",
8         "number_of_shards": "5",
9         "number_of_replicas": "1",
10        "uuid": "2Rk24E2mQ86Pw_iBvnhK7A",
11        "version": {
12          "created": "5000026"
13        }
14      }
15    }
16  }
17 }

```

Next Video

Goal of ElasticSearch