Upgrading Your Elastic Stack to 7.x

Josh Dover | Senior Software Engineer

George Kobar | Senior Support Engineer

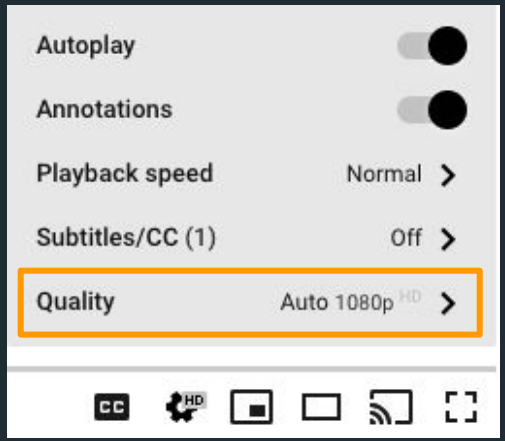
June 25, 2019

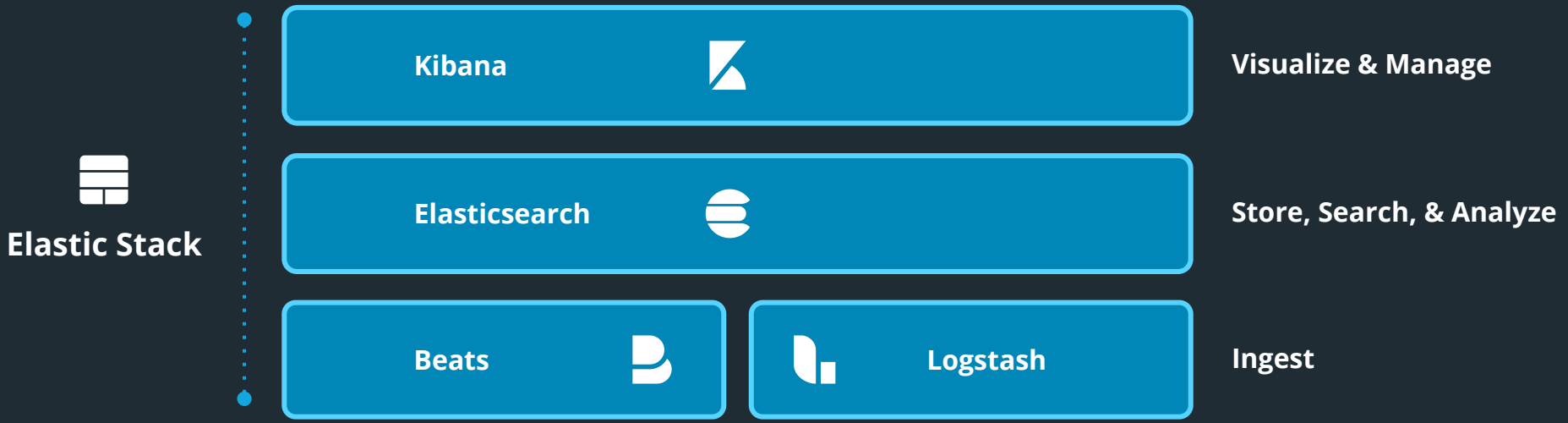
Josh Dover
Senior Software Engineer
Elastic

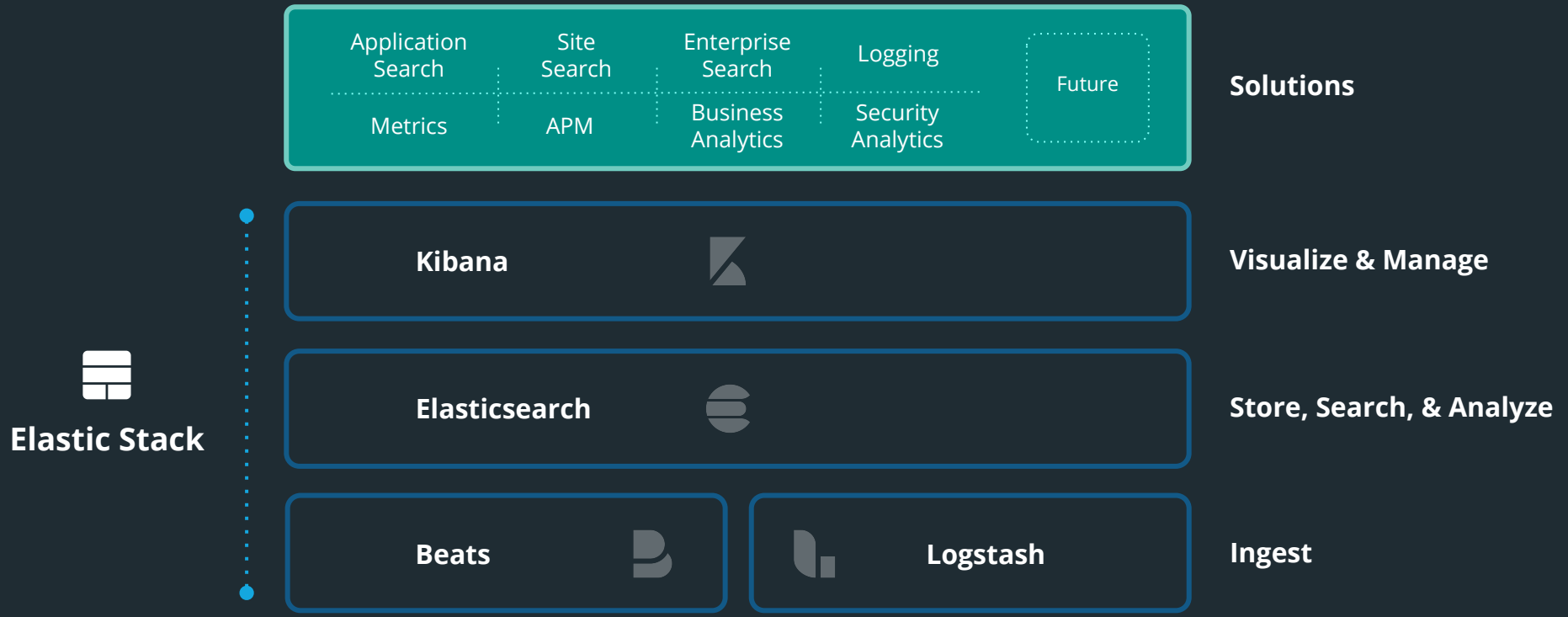
George Kobar
Senior Support Engineer
Elastic

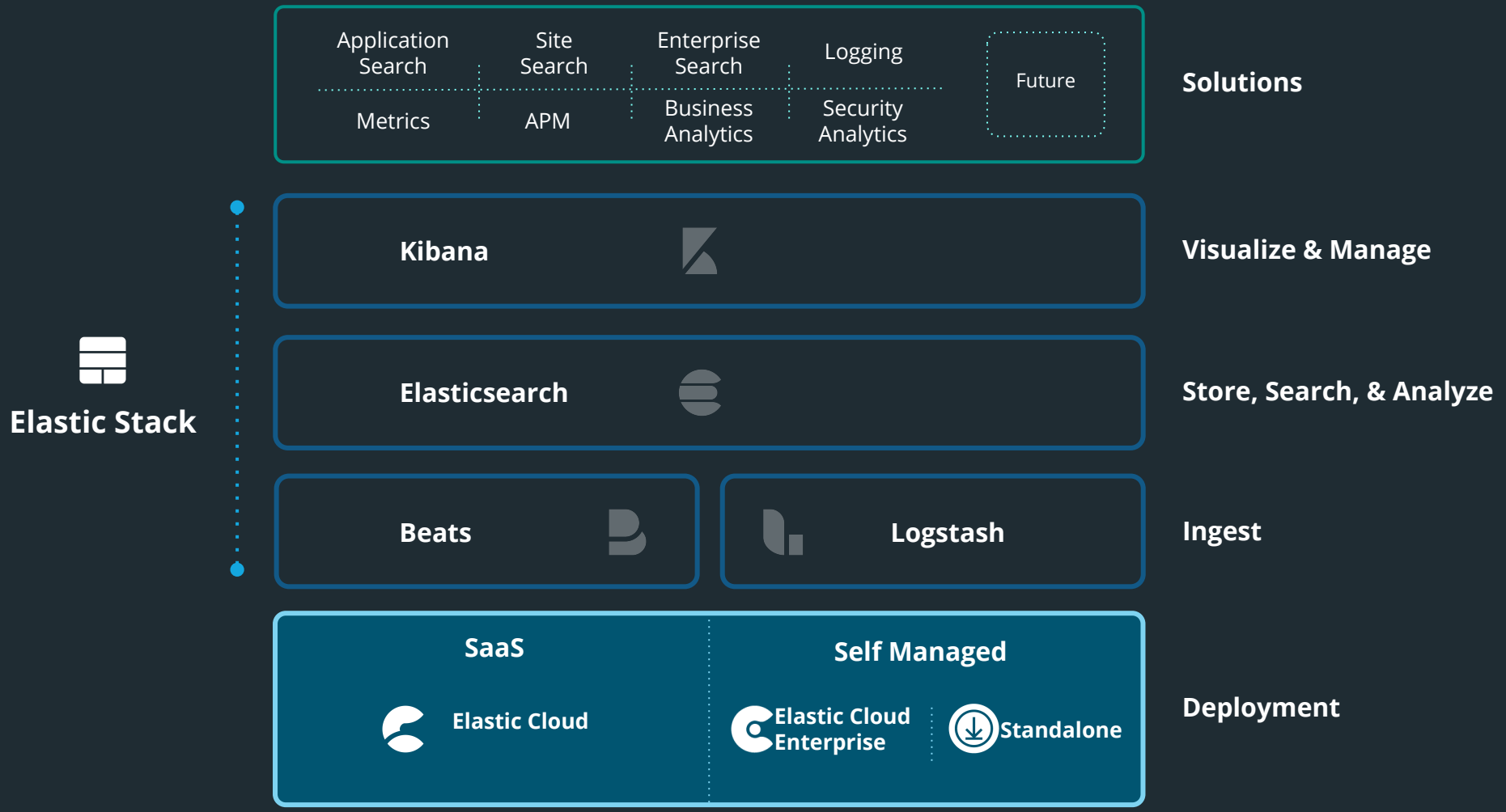
Housekeeping & Logistics

- Chat via IRC #elastic-webinar
  - #elastic-webinar @ Freenode
  - Click "Join the Chat" link, create an IRC account
- Select a **high-res Quality** in YouTube
- **Recording** will be available after the webinar




Elastic Stack
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest


Application Search
Site Search
Enterprise Search
Logging
Metrics
APM
Business Analytics
Security Analytics
Future
Solutions
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Elastic Stack


Application Search
Site Search
Enterprise Search
Logging
Metrics
APM
Business Analytics
Security Analytics
Future
Solutions
Elastic Stack
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
SaaS
Elastic Cloud
Self Managed
Elastic Cloud Enterprise
Standalone
Deployment

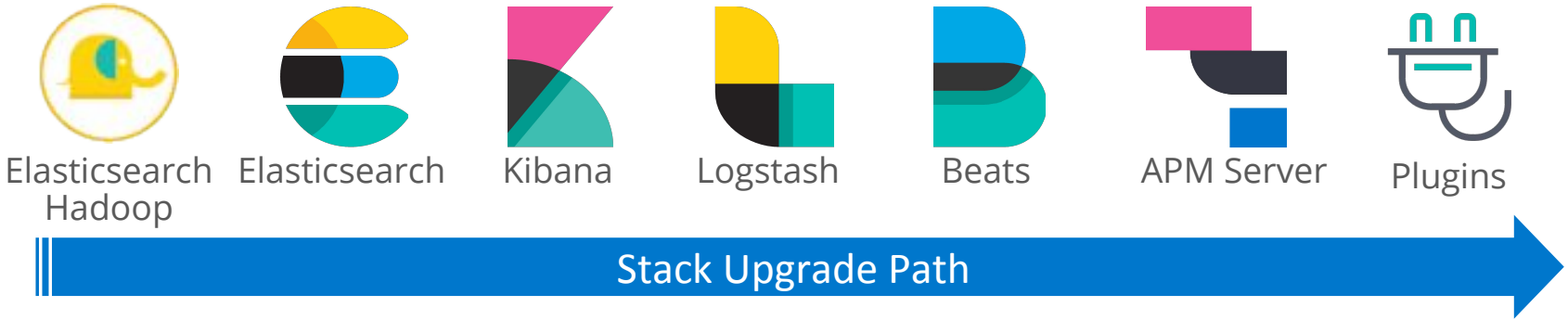
Topics Covered

Upgrading your Elastic Stack to 7.x

- Stack Upgrade Path
- Upgrading to 7.x
  - 7.0 Upgrade Assistant
  - Breaking Changes
- Upgrade Best Practices
- Upgrade Strategies
- Additional Resources

Upgrade Path

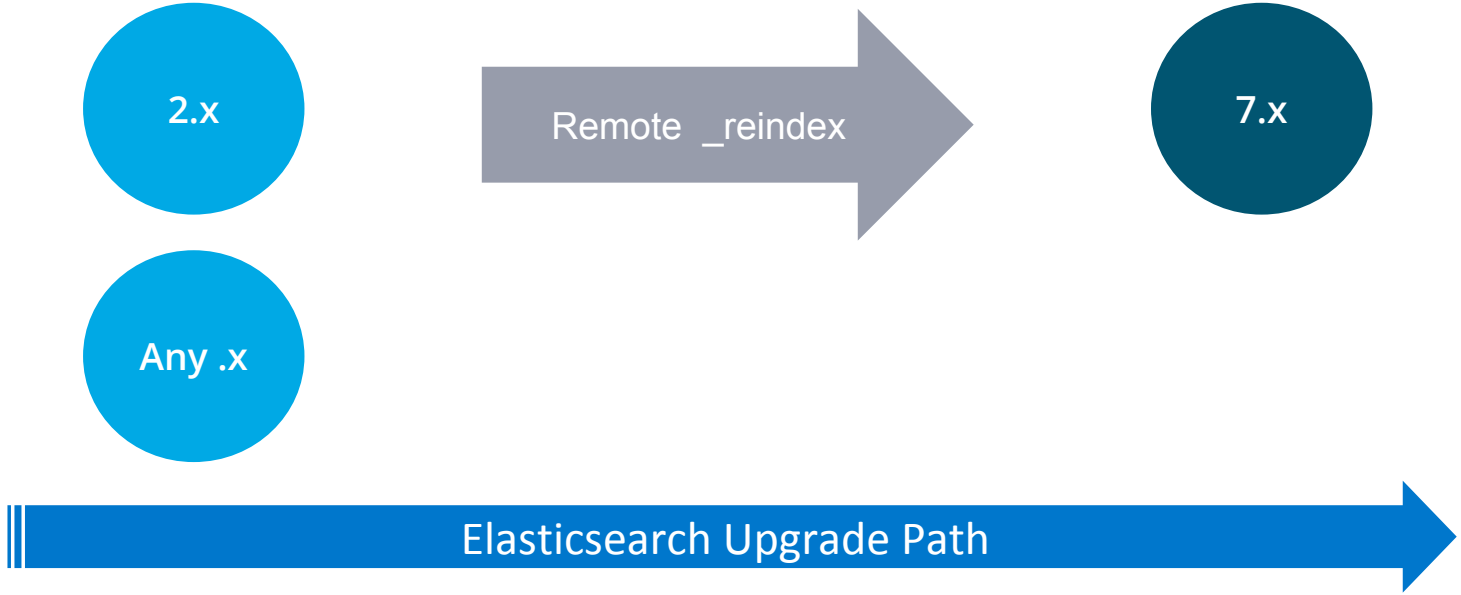
Stack Upgrade Path



https://www.elastic.co/guide/en/elastic-stack/current/upgrading-elastic-stack.html

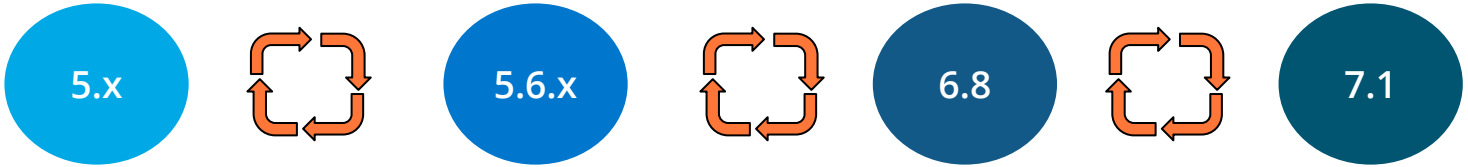
elastic

Elasticsearch Upgrade Path 2.x - 7.x



https://www.elastic.co/guide/en/elasticsearch/reference/current/reindex-upgrade.html

Elasticsearch Upgrade Path 5.x - 7.x



You must delete or reindex any **indices created in 5.x** before upgrading from 6.x to 7.x

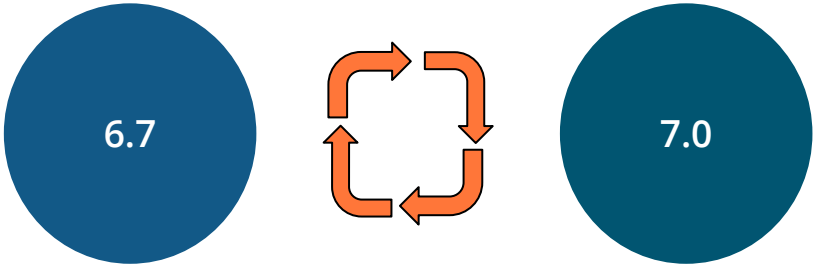
Rolling Upgrade

Elasticsearch Upgrade Path

https://www.elastic.co/guide/en/elasticsearch/reference/current/setup-upgrade.html

elastic

Elasticsearch Upgrade Path 6.7 - 7.0



If you are not using Basic security introduced in 6.8 and 7.1, this will impact your upgrade process.

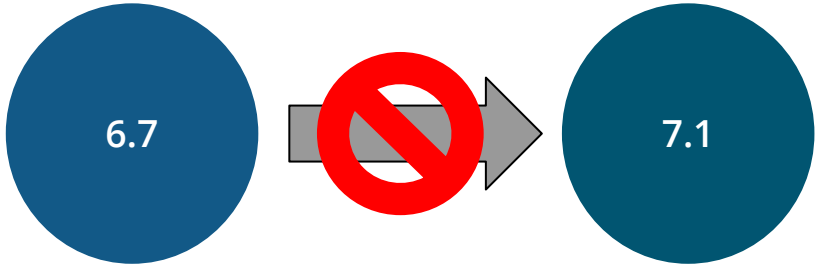
Rolling Upgrade

Elasticsearch Upgrade Path

https://www.elastic.co/guide/en/elasticsearch/reference/current/setup-upgrade.html

elastic

Elasticsearch Upgrade Path 6.7 - 7.0



Elasticsearch Upgrade Path

https://www.elastic.co/guide/en/elasticsearch/reference/current/setup-upgrade.html

elastic

Before You Upgrade

Before You Upgrade

- Create a snapshot/backup indices before upgrading or _reindexing

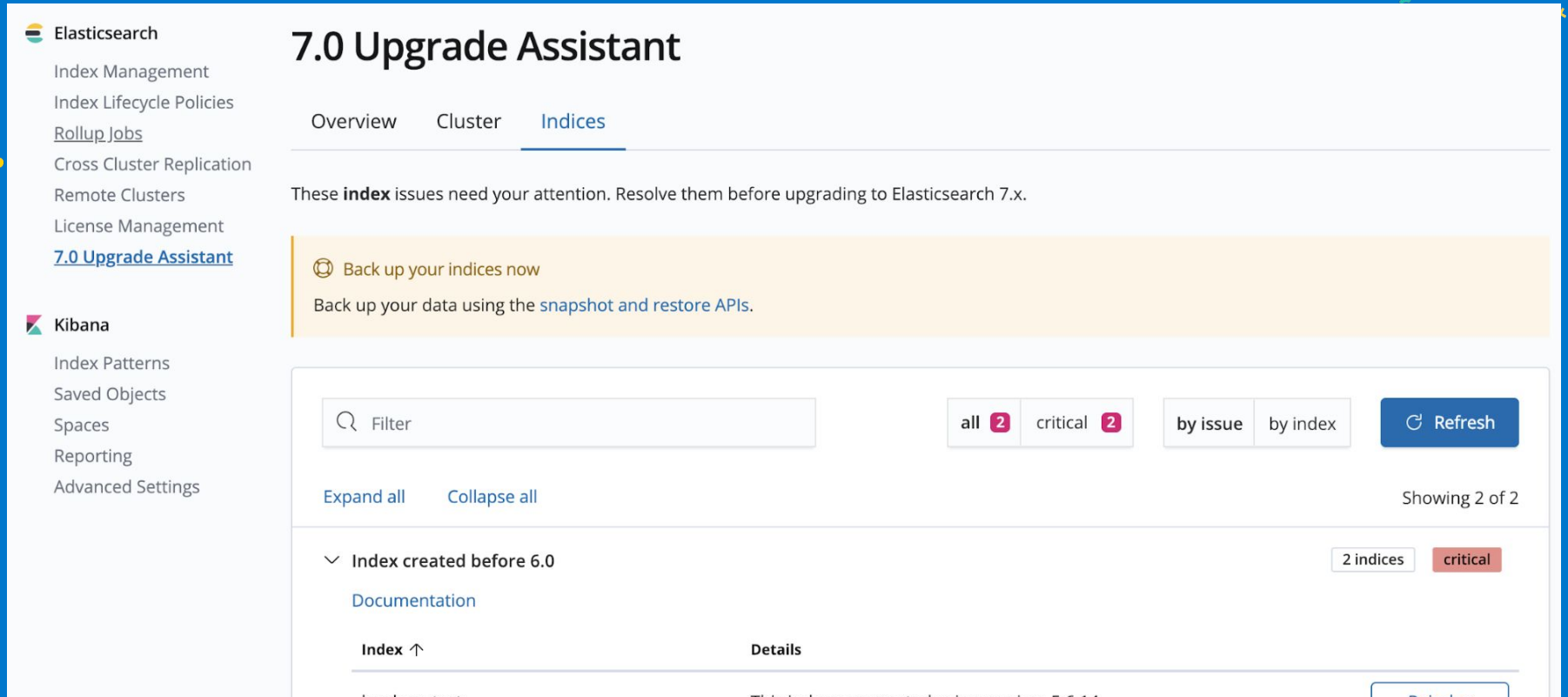
  

  You cannot roll back to an earlier version unless you have a backup of your data.

- Check the deprecation log
- Review breaking changes and remediate
  - `[2017-06-14T15:23:30,063][WARN ][o.e.d.i.m.StringFieldMapper$TypeParser] The [string] field is deprecated, please use [text] or [keyword] instead on [intervalName]`
- If using custom plugins, ensure compatible versions are available
- Test upgrades in a dev/test environment before upgrading your production cluster.

Upgrade Assistant

7.0 Upgrade Assistant



7.0 Upgrade Assistant

Upgrading your Elastic Stack to 7.x

- Deprecation warning tool
- Reindexing tool for indices created in 5.x
- Available in Kibana 6.6+
  - Must upgrade to 6.7+ for latest warnings + reindexing tool
- Free with the Basic License

Demo Time

7.0 Upgrade Assistant

Available APIs

- RESTful APIs in Kibana
  - readiness check, reindexing, and adding default_field setting
- Great for needing to retain 1000s of indices
- Take care when reindexing, can put strain on your cluster
- See documentation for details and examples

Breaking Changes

Highlights

- Typeless APIs
- Elastic Common Schema (ECS)

Full list:

https://www.elastic.co/guide/en/elasticsearch/reference/7.0/breaking-changes-7.0.html

Typeless APIs

Breaking Changes

- APIs without mapping types are available in 6.7
- Typed API calls raise a deprecation warning in 7.x
- `include_type_name` query parameter
  - For Mapping, Index, and Index Template APIs
  - Introduced in Elasticsearch 6.7, defaults to `true`
  - Deprecated in 7.x, defaults to `false`
  - Will be removed in 8.0

https://www.elastic.co/guide/en/elasticsearch/reference/7.0/removal-of-types.html#_typeless_apis_in_7_0

6.x

```
PUT twitter/mytype/1
{
    "user": "kimchy",
    "post_date": "2009-11-15T14:12:12",
    "message": "trying out Elasticsearch"
}
```

7.x

```
PUT twitter/_doc/1
{
    "user": "kimchy",
    "post_date": "2009-11-15T14:12:12",
    "message": "trying out Elasticsearch"
}
```

6.x

```
PUT test
{
    "settings" : {
        "number_of_shards" : 1
    },
    "mappings" : {
        "mytype" : {
            "properties" : {
                "field1" : { "type" : "text" }
            }
        }
    }
}
```

7.x

```
PUT test
{
    "settings" : {
        "number_of_shards" : 1
    },
    "mappings" : {
        "properties" : {
            "field1" : { "type" : "text" }
        }
    }
}
```

6.x

```
PUT test
{
    "settings" : {
        "number_of_shards" : 1
    },
    "mappings" : {
        "mytype" : {
            "properties" : {
                "field1" : { "type" : "text" }
            }
        }
    }
}
```

6.7 + 7.x (w/ deprecation warnings)

```
PUT test?include_type_name=true
{
    "settings" : {
        "number_of_shards" : 1
    },
    "mappings" : {
        "mytype" : {
            "properties" : {
                "field1" : { "type" : "text" }
            }
        }
    }
}
```

Elastic Common Schema (ECS)

Breaking Changes

- Common mappings for ingestion data
- Allows for easy correlation across data sources
- Introduced in Beats & APM 7.0
- Breaks some Ingest pipelines & Logstash filters
- May need to update saved searches & visualizations

6.x	7.0 ECS
`beat.hostname`	`agent.hostname`
`docker.container.name`	`container.name`
`metricbeat.module`	`event.module`
`system.process.pid`	`process.pid`

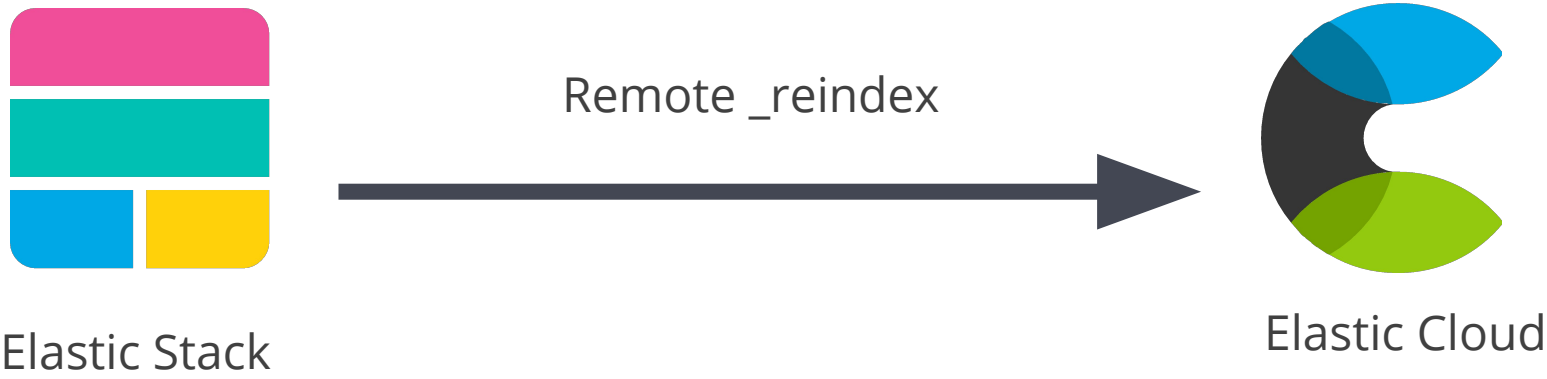
Full list: https://www.elastic.co/guide/en/beats/libbeat/7.0/breaking-changes-7.0.html

Upgrade Strategies

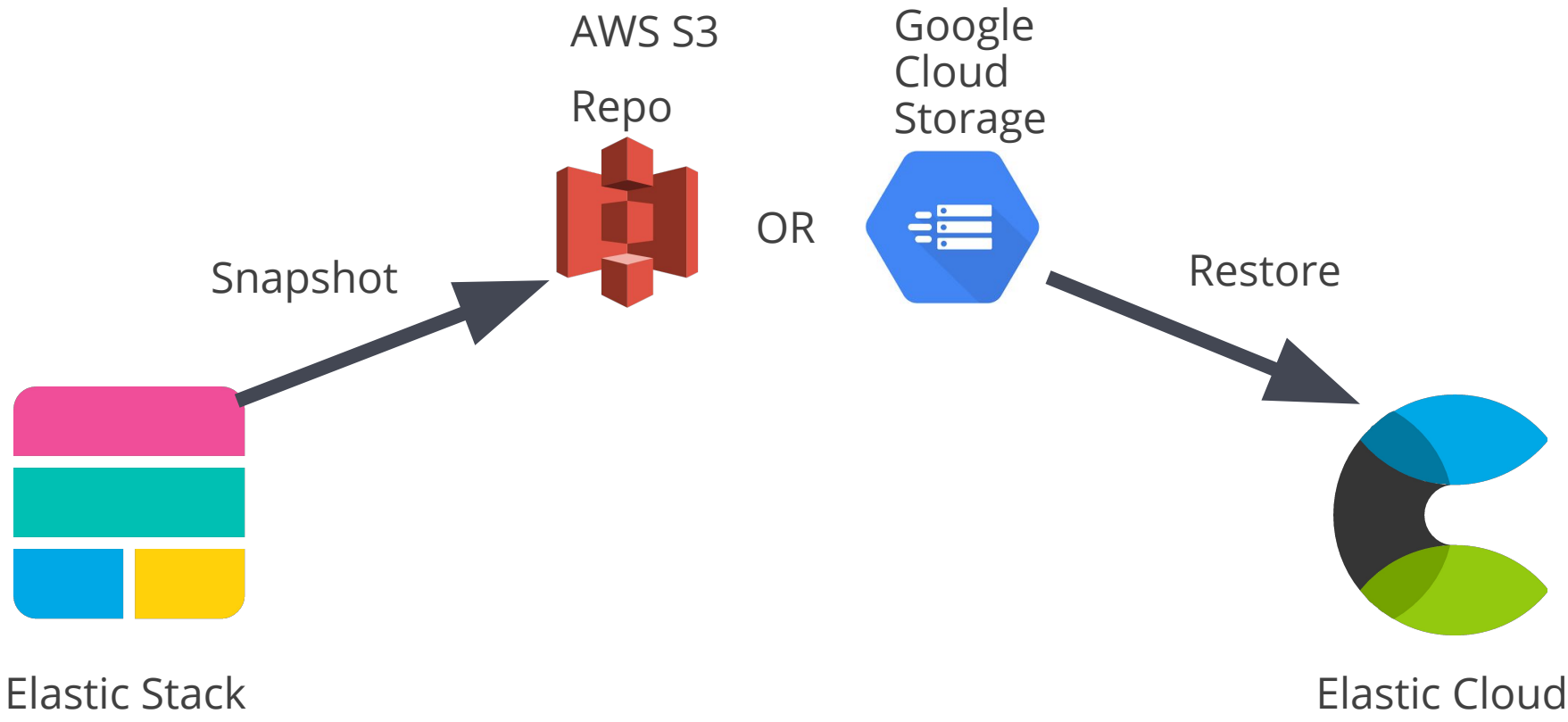
Upgrade Strategies

- Test!
- Snapshot/Restore into test cluster
  - Restore select index or entire cluster
  - Cloud Instance, Laptop, VM, container, Elastic Cloud
  - Test upgrade process

Upgrade Strategies

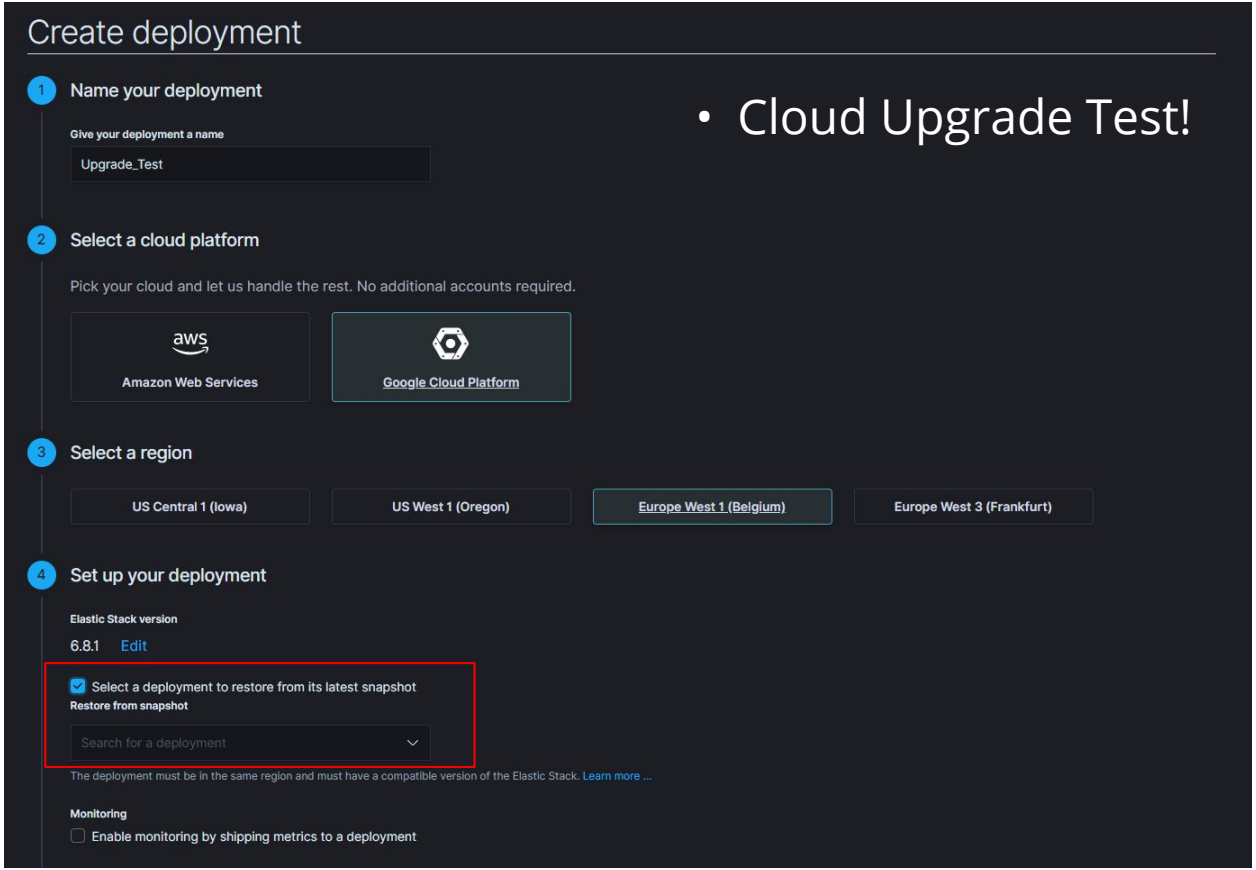


Upgrade Strategies



elastic

Upgrade Strategies



- Cloud Upgrade Test!

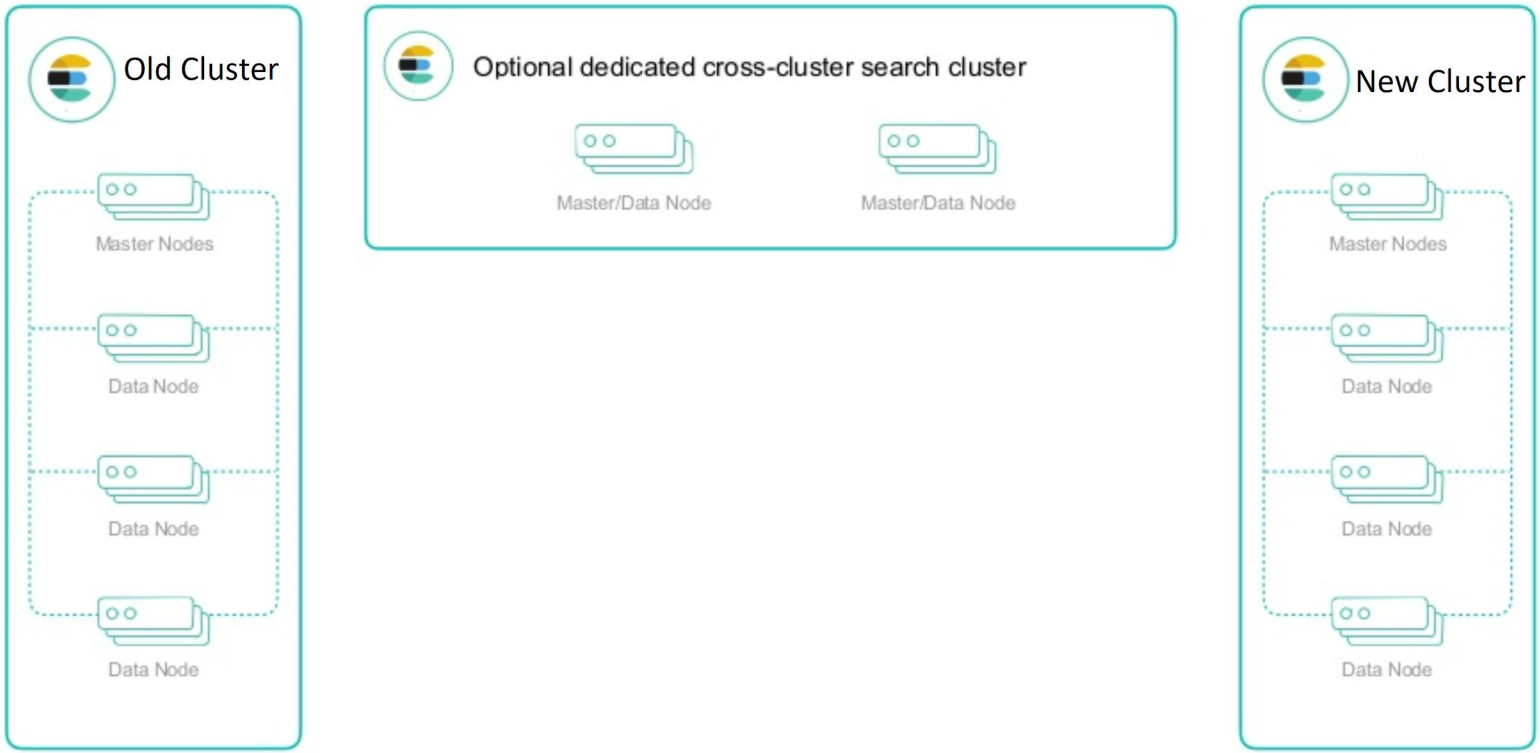
Restore from Snapshot

elastic

Upgrade Strategies

- Run the Upgrade Assistant against restored or _reindexed cluster
- Review Elasticsearch and Kibana breaking changes documentation

Upgrade Strategies



elastic

Lessons Learned

Kibana Upgrade Lessons Learned

- "shard failed" error when viewing Beats dashboards in Kibana
- After upgrading to Elasticsearch 7.0, any indices created by Beats 6.6 or older will not work in Kibana dashboards until the `index.query.default_field` setting is added to each index.
- Indices created in Beats 6.7 or later are unaffected. To add the setting to the index, you can use the 7.0 Upgrade Assistant, or add the setting manually.

https://www.elastic.co/guide/en/kibana/current/upgrade.html

Logstash Upgrade Lessons Learned

- Drain Persistent Queue 6.2.x and earlier

  To drain the queue:

  - In the logstash.yml file, set `queue.drain:true`.
  - Restart Logstash for this setting to take effect.
  - Shutdown Logstash (using CTRL+C or SIGTERM), and wait for the queue to empty.

- Drain Persistent Queue 6.3.x and later
  - Shut down the original Logstash instance
  - Spin up a new instance,
  - Set path.queue in the logstash.yml settings file to point to the original queue directory.

Logstash Upgrade Path

https://www.elastic.co/guide/en/logstash/7.1/upgrading-logstash-pqs.html#drain-pq

Beats Upgrade Lessons Learned

- Check privileges for index lifecycle management (on by default in 7.0)edit
- Starting with Beats 7.0, index lifecycle management is on by default
- Make sure Beats users have the privileges needed to use index lifecycle management, or disable index lifecycle management.
- For help troubleshooting authorization issues, see **User is not authorized**.
- If you want to disable index lifecycle management, set setup.ilm.enabled: false in the Beats configuration file.

Be aware of the Elastic Common Schema! More on this later…

Beats Upgrade Path

https://www.elastic.co/guide/en/beats/libbeat/current/upgrading.html

Lessons Learned

Security Realm Change

- **Realm Type no longer needed. Error Message example:**

```
`'xpack.security.authc.realms.saml.cloud-saml.type': is not allowed `
```

- **A realm that was previous configured as:**

```
xpack.security.authc.realms:
  ldap1:
    type: ldap
    order: 1
    url: "ldaps://ldap.example.com/"
```

Must be migrated to:

```
xpack.security.authc.realms:
  ldap.ldap1:
    order: 1
    url: "ldaps://ldap.example.com/"
```

Lessons Learned

TLS/SSL

- TLS/SSL is a requirement for elasticsearch node communication for clusters in production as of 6.x
- When upgrading from 5.x -> 6.x, ensure that this is enabled prior to upgrading further

You may see messages related to:

```
[2019-06-13T00:00:20,657][WARN ][o.e.x.s.t.n.SecurityNetty4HttpServerTransport] [PLATFORM Cluster1] caught
exception while handling client http traffic, closing connection [id: 0bc2f1777bb, L:0.0.0.0/0.0.0.0:9200 !
R:/127.0.0.1:44084]

io.netty.handler.codec.DecoderException: io.netty.handler.ssl.NotSslRecordException: not an SSL/TLS record:
```

- A device is still attempting to connect to the cluster over HTTP and not HTTPS

Lessons Learned

TLS/SSL

- TLS/SSL is a requirement for elasticsearch node communication for clusters in production as of 6.x
- When upgrading from 5.x -> 6.x, ensure that this is enabled prior to upgrading further

You may see messages related to:

```
[2019-06-13T00:00:20,657][WARN ][o.e.x.s.t.n.SecurityNetty4HttpServerTransport] [PLATFORM Cluster1] caught
exception while handling client http traffic, closing connection [id: 0bc2f1777bb, L:0.0.0.0/0.0.0.0:9200 !
R:/127.0.0.1:44084]

io.netty.handler.codec.DecoderException: io.netty.handler.ssl.NotSslRecordException: not an SSL/TLS record:
```

- A device is still attempting to connect to the cluster over HTTP and not HTTPS

Resources

Upgrade Resources

- Documentation
- Support
- Training
- Consulting
- Community

Upgrade Resources

- Cross stack upgrade guide

  https://www.elastic.co/guide/en/elastic-stack/current/upgrading-elastic-stack.html

- Release highlights (per product)
  https://www.elastic.co/blog/category/releases

- Support Matrix (https://www.elastic.co/support/matrix)

- End of Life (EOL) Dates (https://www.elastic.co/support/eol)
- 5.6.X - March 11th, 2019
- 6.8.X - Nov 11th, 2020

Security for Elasticsearch is Now Free in 6.8 and 7.1

https://www.elastic.co/blog/security-for-elasticsearch-is-now-free

elastic

Thank You

- Web : www.elastic.co
- Demos: demo.elastic.co
- Products : https://www.elastic.co/products
- Forums : https://discuss.elastic.co/
- Community : https://www.elastic.co/community/meetups
- Twitter : @elastic

Questions?

SaaS

Elastic Cloud

Elasticsearch Service

Elastic Site Search Service

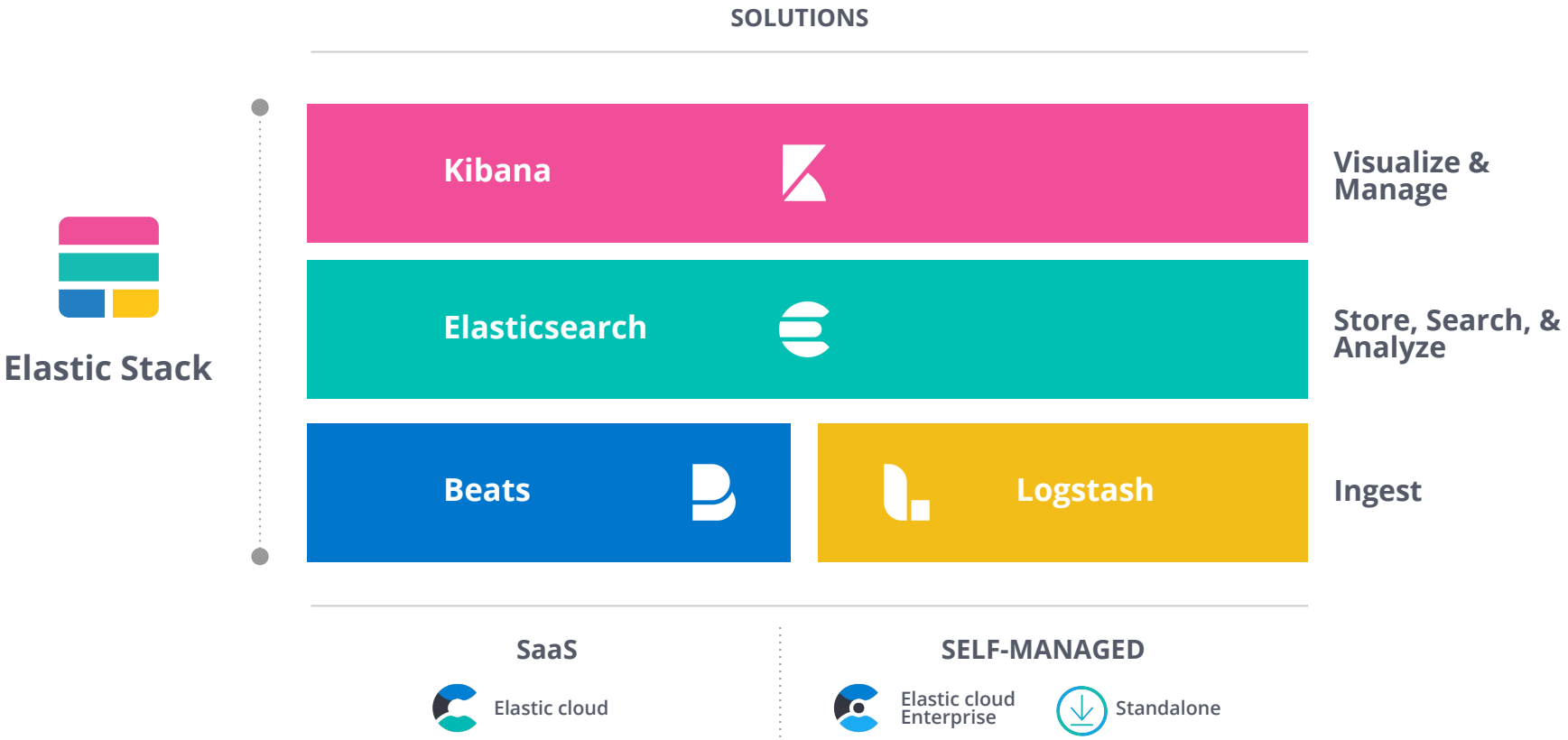
Elastic App Search Service

Self Managed

Elastic Cloud Enterprise

Standalone

Elastic **Stack**



elastic

Solutions

Logging	Metrics	APM	Security Analytics	FUTURE
App Search	Site Search	Enterprise Search	Business Analytics	

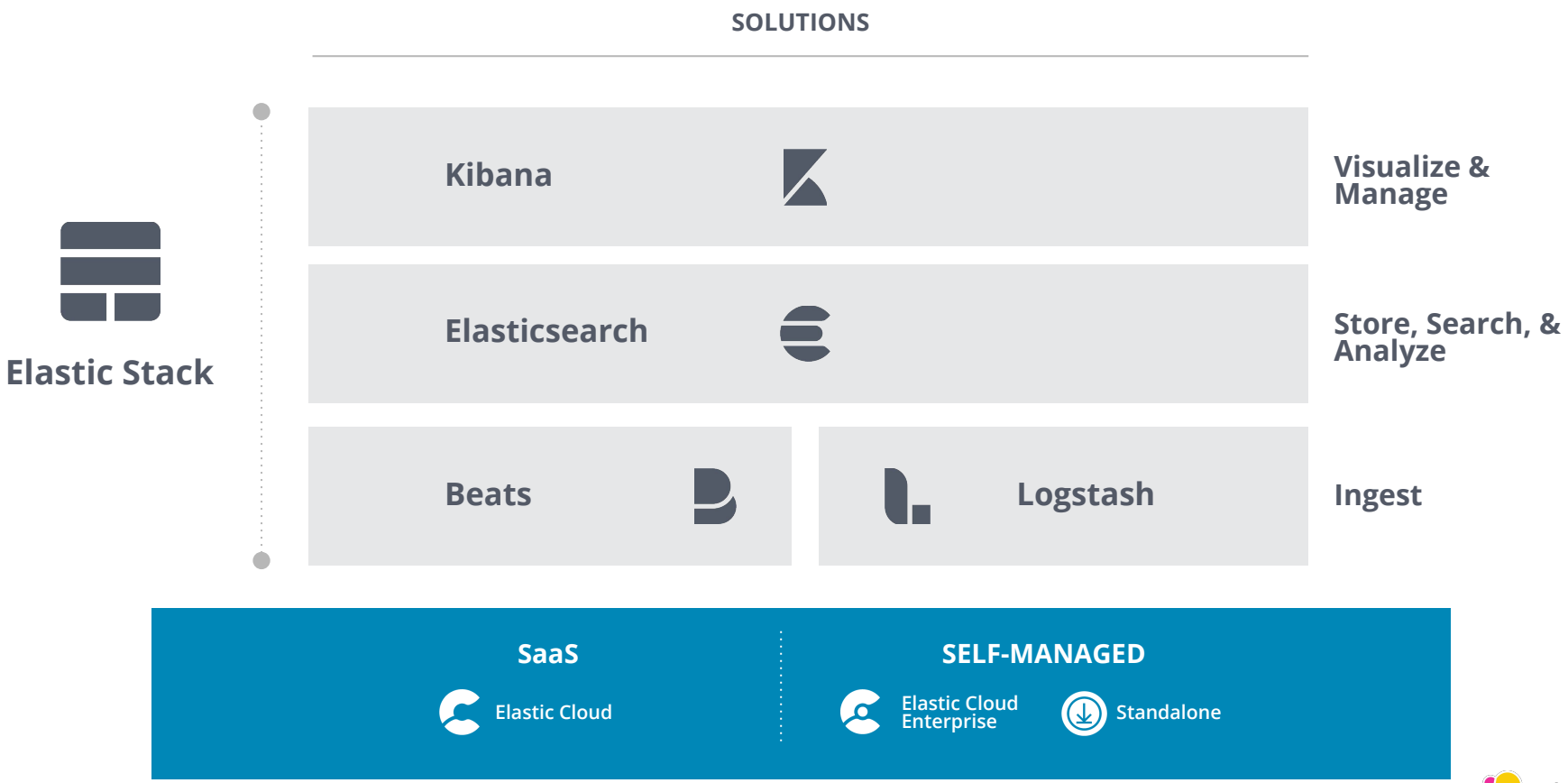
Elastic Stack

Kibana		Visualize & Manage
Elasticsearch		Store, Search, & Analyze
Beats	Logstash	Ingest

SaaS | SELF-MANAGED

elastic

Deployment **options**



elastic

Demo Time