

What's new in the Elastic Stack?

8.x edition & AMA

Philipp Krenn | @xeraa

Alexander Reelsen | @spinscale



Late 7.x

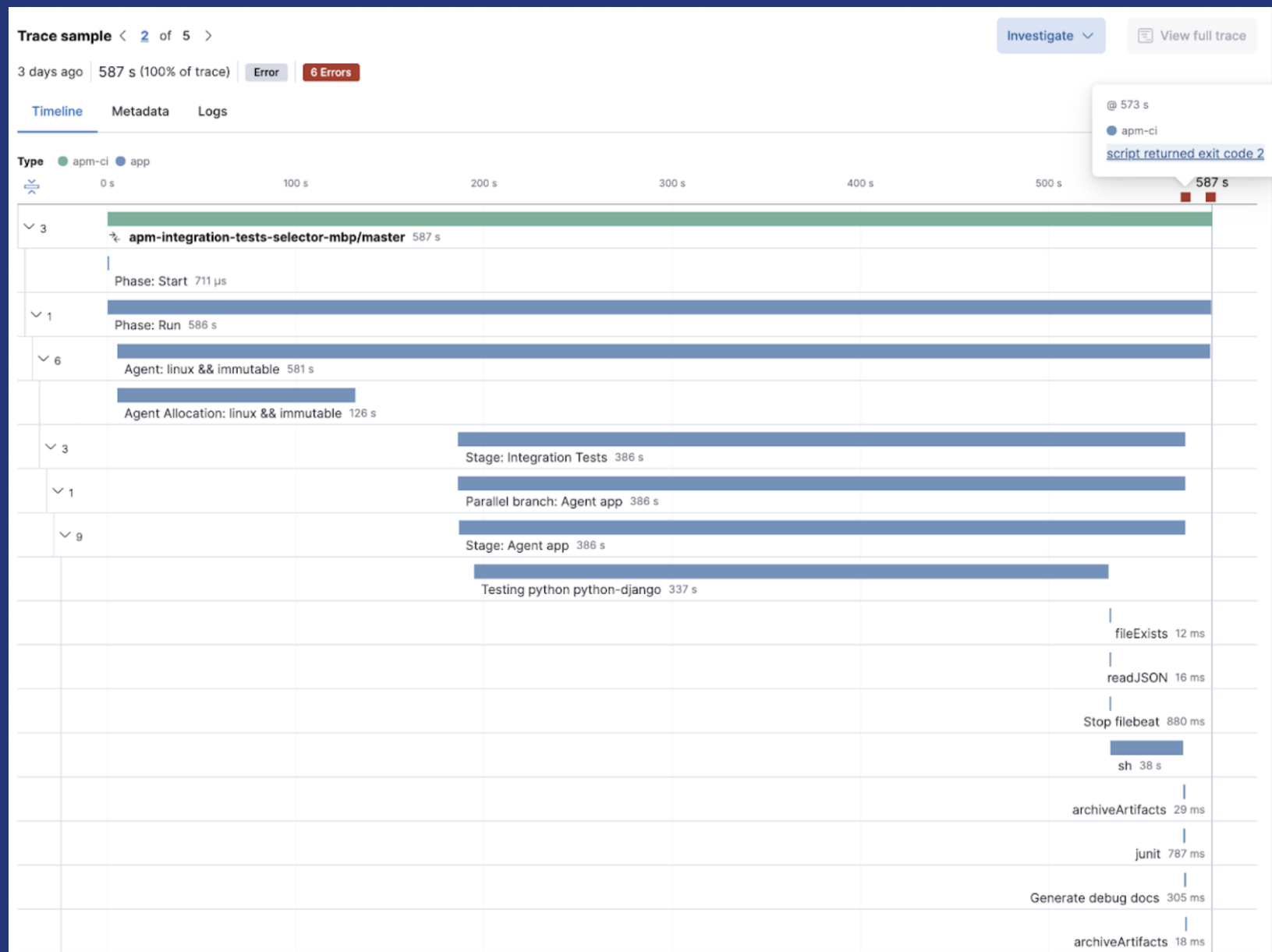
- Observability: Google Cloud Logs Integration, User Experience & Synthetic Monitoring
- Enterprise Search: Kibana Integration, Crawler
- Security: Osquery integration
- Stack: Runtime fields & Searchable Snapshots

8.x

- Observability: CI/CD, AWS Lambda visibility
- Enterprise Search: SharePoint Connector
- Stack: **Security on by default**, ANN & NLP, Field usage & Disk usage APIs, Lucene 9
- Geo: Hex tiles, Vector tiles
- ARM support

Observability

CI/CD



Security-on-by-default

- Whole stack!
- TLS
- Authorization + Authentication
- Running with Testcontainers

knn search

- Using `dense_vector` fields for efficient vector search
- HNSW (Hierarchical Navigable Small World)
- `8.2`: Filtering support
- Attention: **Dedicated endpoint!**

NLP - Language detection

```
POST _ingest/pipeline/_simulate
{
  "pipeline": {
    "processors": [
      {
        "inference": { "model_id": "lang_ident_model_1", "inference_config": { "classification": {} } }
      }
    ]
  },
  "docs": [
    {
      "_source": {
        "text": "This is an english text, albeit rather short."
      }
    },
    {
      "_source": {
        "text": "Bitte melden Sie sich schnellstmöglich bei uns. Wir sind jederzeit telefonisch zu erreichen."
      }
    }
  ]
}
```

NLP - Language detection

```
{
  "docs" : [
    {
      "doc" : {
        "_source" : {
          "text" : "This is an english text, albeit rather short.",
          "ml" : {
            "inference" : {
              "prediction_score" : 0.997576998993641, "model_id" : "lang_ident_model_1", "prediction_probability" : 0.997576998993641,
              "predicted_value" : "en"
            }
          }
        }
      }
    },
    {
      "doc" : {
        "_source" : {
          "text" : "Bitte melden Sie sich schnellstmöglich bei uns. Wir sind jederzeit telefonisch zu erreichen.",
          "ml" : {
            "inference" : {
              "prediction_score" : 0.9999990788535671, "model_id" : "lang_ident_model_1", "prediction_probability" : 0.9999990788535671,
              "predicted_value" : "de"
            }
          }
        }
      }
    }
  ]
}
```


NLP - Named Entity Recognition

```
# sentence transformers require cmake  
pip3 install eland tqdm torch transformers sentence_transformers
```

```
~/Library/Python/3.8/bin/eland_import_hub_model \  
  --url "https://elastic:s3cr3t@my-elasticsearch-endpoint.europe-west3.gcp.cloud.es.io:9243" \  
  --hub-model-id elastic/distilbert-base-cased-finetuned-conll03-english \  
  --task-type ner \  
  --start
```

NLP - Named Entity Recognition

```
POST _ingest/pipeline/_simulate
{
  "pipeline": {
    "processors": [
      {
        "inference": {
          "model_id": "elastic__distilbert-base-cased-finetuned-conll03-english",
          "inference_config": { "ner": { } }
        }
      }
    ]
  },
  "docs": [
    { "_source": { "text_field": "I've been living in Munich for 15 years." } },
    { "_source": { "text_field": "One of the nicest places in Munich is the Englischer Garten." } },
    { "_source": { "text_field": "Been working at Elastic for more than 9 years." } }
  ]
}
```

NLP - Named Entity Recognition

```
{
  "doc" : {
    "_index" : "_index", "_id" : "_id",
    "_source" : {
      "text_field" : "I've been living in Munich for 15 years.",
      "ml" : {
        "inference" : {
          "model_id" : "elastic__distilbert-base-cased-finetuned-conll03-english",
          "entities" : [
            {
              "start_pos" : 20, "end_pos" : 26,
              "class_name" : "LOC", "class_probability" : 0.9992382591441749,
              "entity" : "Munich"
            }
          ]
        },
        "predicted_value" : "I've been living in [Munich](LOC&Munich) for 15 years."
      }
    }
  }
}
```

NLP - Named Entity Recognition

```
{
  "doc" : {
    "_index" : "_index", "_id" : "_id",
    "_source" : {
      "text_field" : "One of the nicest places in Munich is the Englischer Garten.",
      "ml" : {
        "inference" : {
          "model_id" : "elastic__distilbert-base-cased-finetuned-conll03-english",
          "entities" : [
            {
              "start_pos" : 28, "end_pos" : 34,
              "class_name" : "LOC", "class_probability" : 0.9993211907123687,
              "entity" : "Munich"
            },
            {
              "start_pos" : 42, "end_pos" : 59,
              "class_name" : "ORG", "class_probability" : 0.9521962770340935,
              "entity" : "Englischer Garten"
            }
          ],
          "predicted_value" : "One of the nicest places in [Munich](LOC&Munich) is the [Englischer Garten](ORG&Englischer+Garten)."
        }
      }
    }
  }
}
```

NLP - Named Entity Recognition

```
{
  "doc" : {
    "_index" : "_index", "_id" : "_id",
    "_source" : {
      "text_field" : "Been working at Elastic for more than 9 years.",
      "ml" : {
        "inference" : {
          "model_id" : "elastic__distilbert-base-cased-finetuned-conll03-english",
          "entities" : [
            {
              "start_pos" : 16, "end_pos" : 23,
              "class_name" : "ORG", "class_probability" : 0.9996217159395848,
              "entity" : "Elastic"
            }
          ],
          "predicted_value" : "Been working at [Elastic](ORG&Elastic) for more than 9 years."
        }
      }
    }
  }
}
```


More NLP...

- Check out the [annotated text field type](#) for the `predicted_value` field
- Check out the [third party model documentation](#)

Upgrade Assistant



elastic AR

Stack Management Upgrade Assistant

Management

- Ingest
 - Ingest Pipelines
 - Logstash Pipelines
- Data
 - Index Management
 - Index Lifecycle Policies
 - Snapshot and Restore
 - Rollup Jobs
 - Transforms
 - Cross-Cluster Replication
 - Remote Clusters
- Alerts and Insights
 - Rules and Connectors
 - Reporting
 - Machine Learning Jobs
 - Watcher
- Security
 - Users
 - Roles
 - API keys
 - Role Mappings
- Kibana
 - Index Patterns
 - Saved Objects
 - Tags
 - Search Sessions
 - Spaces
 - Advanced Settings
- Stack
 - [Upgrade Assistant](#)

Upgrade Assistant

Get ready for the next version of Elastic!

[What's new in 8.x?](#)

- Back up your data**
 - ✓ Last snapshot created on April 04, 2022 10:29 GMT+2.
 - [Create snapshot](#)
- Migrate system indices**

Prepare the system indices that store internal information for the upgrade. Any [hidden indices](#) that need to be reindexed are shown in the next step.

 - [Migrate indices](#) [View migration details](#)
- Review deprecated settings and resolve issues**

You must resolve any critical Elasticsearch and Kibana configuration issues before upgrading to Elastic 8.x. Ignoring warnings might result in differences in behavior after you upgrade.

Elasticsearch		Kibana	
Critical	Warning	Critical	Warning
12	1	✓ None	2
- Address API deprecations**

Review the Elasticsearch deprecation logs to ensure you're not using deprecated APIs.

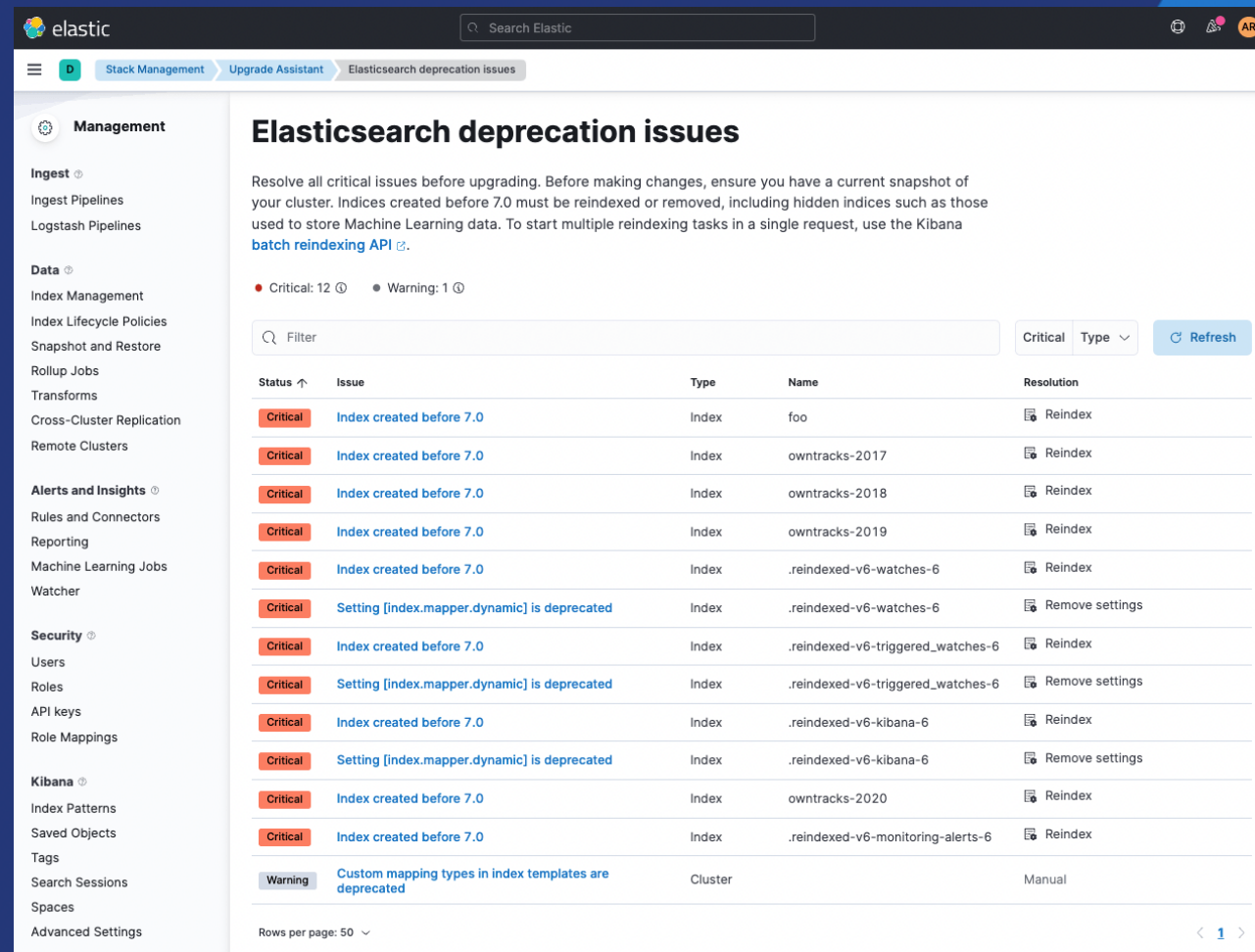
You have no deprecation issues since April 04, 2022 11:05 GMT+2.

 - [View logs](#)
- Upgrade to Elastic 8.x**

Once you've resolved all critical issues and verified that your applications are ready, you can upgrade to Elastic 8.x. Be sure to back up your data again before upgrading. Upgrade your deployment on Elastic Cloud.

 - [Upgrade on Cloud](#) [View upgrade guide](#)

Upgrade Assistant



The screenshot displays the Elastic Upgrade Assistant interface. At the top, the Elastic logo and a search bar are visible. The navigation bar includes 'Stack Management', 'Upgrade Assistant', and 'Elasticsearch deprecation issues'. The left sidebar lists various management categories: Ingest, Data, Alerts and Insights, Security, and Kibana. The main content area is titled 'Elasticsearch deprecation issues' and contains a summary of critical and warning counts, a filter input, and a table of issues.

Elasticsearch deprecation issues

Resolve all critical issues before upgrading. Before making changes, ensure you have a current snapshot of your cluster. Indices created before 7.0 must be reindexed or removed, including hidden indices such as those used to store Machine Learning data. To start multiple reindexing tasks in a single request, use the Kibana [batch reindexing API](#).

● Critical: 12 ● Warning: 1

Filter

Status	Issue	Type	Name	Resolution
Critical	Index created before 7.0	Index	foo	Reindex
Critical	Index created before 7.0	Index	owntracks-2017	Reindex
Critical	Index created before 7.0	Index	owntracks-2018	Reindex
Critical	Index created before 7.0	Index	owntracks-2019	Reindex
Critical	Index created before 7.0	Index	.reindexed-v6-watches-6	Reindex
Critical	Setting [index.mapper.dynamic] is deprecated	Index	.reindexed-v6-watches-6	Remove settings
Critical	Index created before 7.0	Index	.reindexed-v6-triggered_watches-6	Reindex
Critical	Setting [index.mapper.dynamic] is deprecated	Index	.reindexed-v6-triggered_watches-6	Remove settings
Critical	Index created before 7.0	Index	.reindexed-v6-kibana-6	Reindex
Critical	Setting [index.mapper.dynamic] is deprecated	Index	.reindexed-v6-kibana-6	Remove settings
Critical	Index created before 7.0	Index	owntracks-2020	Reindex
Critical	Index created before 7.0	Index	.reindexed-v6-monitoring-alerts-6	Reindex
Warning	Custom mapping types in index templates are deprecated	Cluster		Manual

Rows per page: 50

Elasticsearch Java Client

- Created from spec like all other clients
- Also exists for 7.x allowing for smooth migration.

Terraform Provider

- Elastic Cloud Provider
- Elasticstack Provider

Terraform Provider

```
resource "ec_deployment" "spring-boot-app-search" {
  name      = "spring-boot-app-search"

  region      = "azure-westeuropa"
  version     = "8.1.0"
  deployment_template_id = "azure-memory-optimized"

  elasticsearch {}

  kibana {}

  integrations_server {}

  enterprise_search {}
}
```

What's next

- ANN search filtering
- Lookup runtime fields
- doc-values only fields (for more efficient searchable snapshots)
- random sampler aggregation

Thanks for listening!

Q & A

Philipp Krenn | @xeraa

Alexander Reelsen | @spinscale

