

Elasticstack

Grundlagen

Joachim Walther

Elasticstack

Elastic Agent lässt sich auf verschiedene Arten betreiben:

- 1. Docker Container**
- 2. Installiertes Programm**
- 3. Mit lokaler Elasticsearch Installation**
- 4. Mit Elastic Cloud**

Wir wählen die Konfiguration Docker Container <-> Elastic Cloud.

Elasticstack

Image laden:

[`docker pull docker.elastic.co/beats/elastic-agent:8.2.2-arm64`](#)

Elasticstack

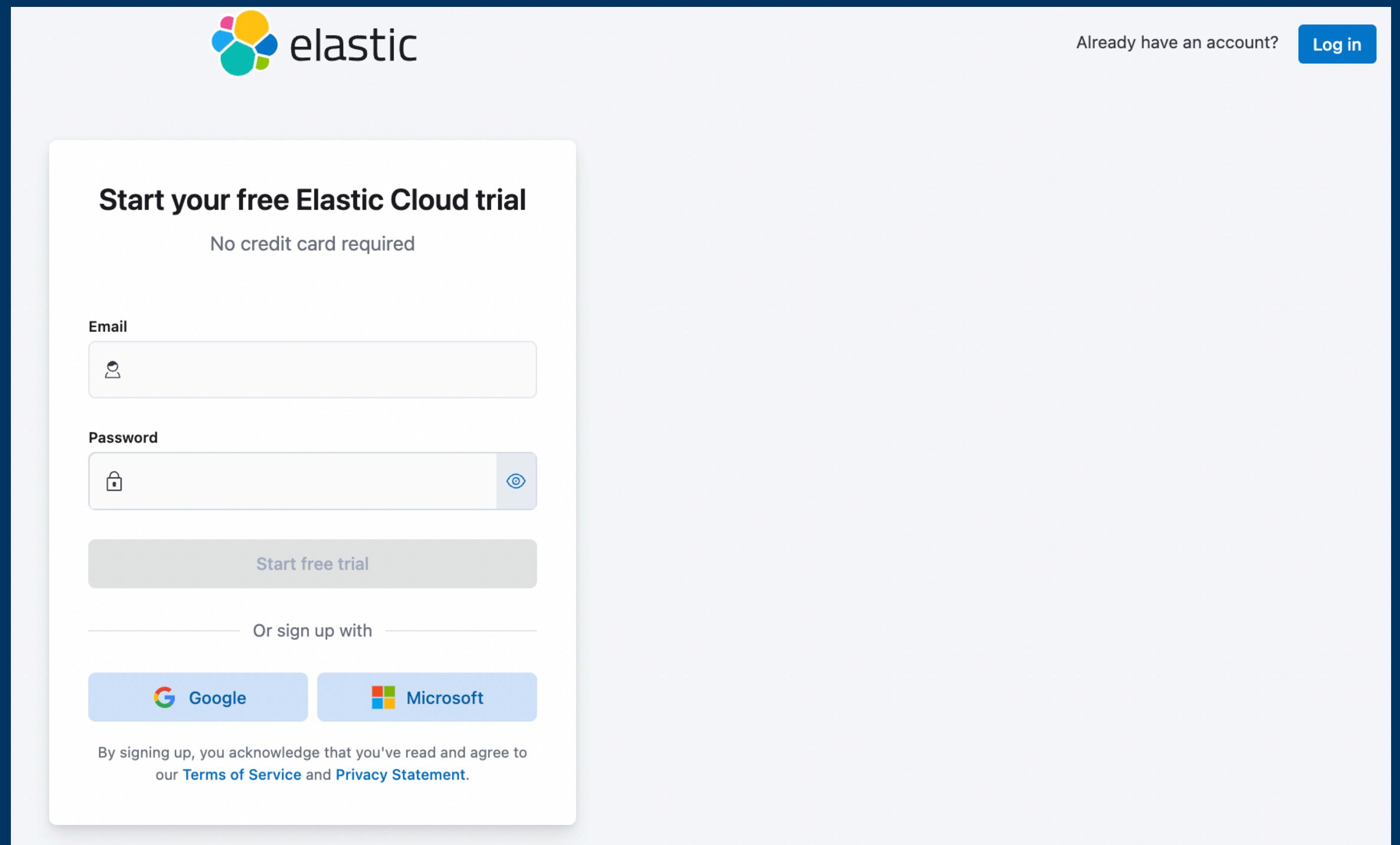
Container starten:

```
docker run \  
--env FLEET_ENROLL=1 \  
--env FLEET_URL={fleet-server-host-url} \  
--env FLEET_ENROLLMENT_TOKEN={enrollment-token} \  
--rm docker.elastic.co/beats/elastic-agent:8.2.2-arm64
```

Bevor wir dieses Kommando geben können, müssen wir auf Elastic Cloud ein Konto anlegen.

Elasticstack

<https://cloud.elastic.co/registration>



The image shows the registration page for the Elastic Cloud trial. At the top right, there are links for "Already have an account?" and "Log in". The main heading is "Start your free Elastic Cloud trial" with the subtext "No credit card required". Below this are fields for "Email" and "Password". A large "Start free trial" button is centered below the password field. Below the button is a "Or sign up with" section featuring "Google" and "Microsoft" social login options. At the bottom, a small note states: "By signing up, you acknowledge that you've read and agree to our [Terms of Service](#) and [Privacy Statement](#)".

Oder wenn man schon registriert ist, kann man rechts oben den Dialog wechseln und sich anmelden.
Wir nutzen den 30 Tage Erprobungszeitraum.

Elasticstack

Mit „create deployment“ fortfahren:

The screenshot shows a user interface for creating an Elasticsearch deployment. At the top left is a circular icon with a yellow and green gradient and the text "Elasticsearch Service". Below it is a large, semi-transparent circular graphic containing icons for various Elastic products: a blue circle with a magnifying glass, a teal circle with a gear, a pink circle with a Kibana visualization, and a green circle with an equals sign. To the right of this graphic is a yellow dotted grid icon. The main title "Create your first deployment" is centered in bold black text. Below the title is a descriptive paragraph: "Create your first deployment to manage an Elasticsearch cluster on the cloud platform of your choice. Add additional Elastic products to your deployment like Kibana, machine learning, or APM." At the bottom is a prominent blue button with white text that reads "Create deployment".

Create your first deployment

Create your first deployment to manage an Elasticsearch cluster on the cloud platform of your choice. Add additional Elastic products to your deployment like Kibana, machine learning, or APM.

Create deployment

Elasticstack

Mit Amazon bleiben wir in Deutschland ;-)

Welcome to Elastic!

Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

Name

Settings

Cloud provider aws Amazon Web Services

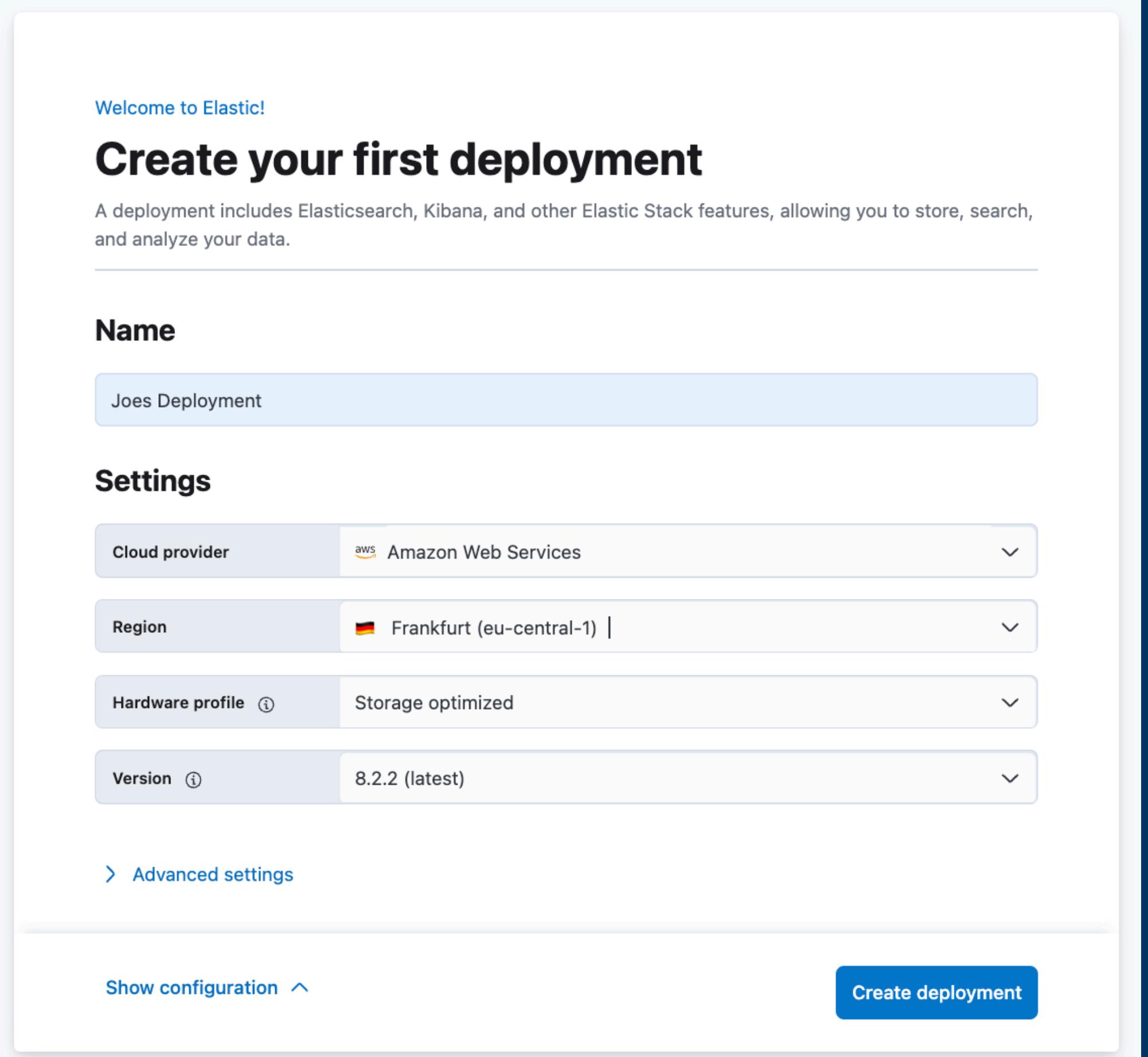
Region Frankfurt (eu-central-1) |

Hardware profile Storage optimized

Version 8.2.2 (latest)

[Advanced settings](#)

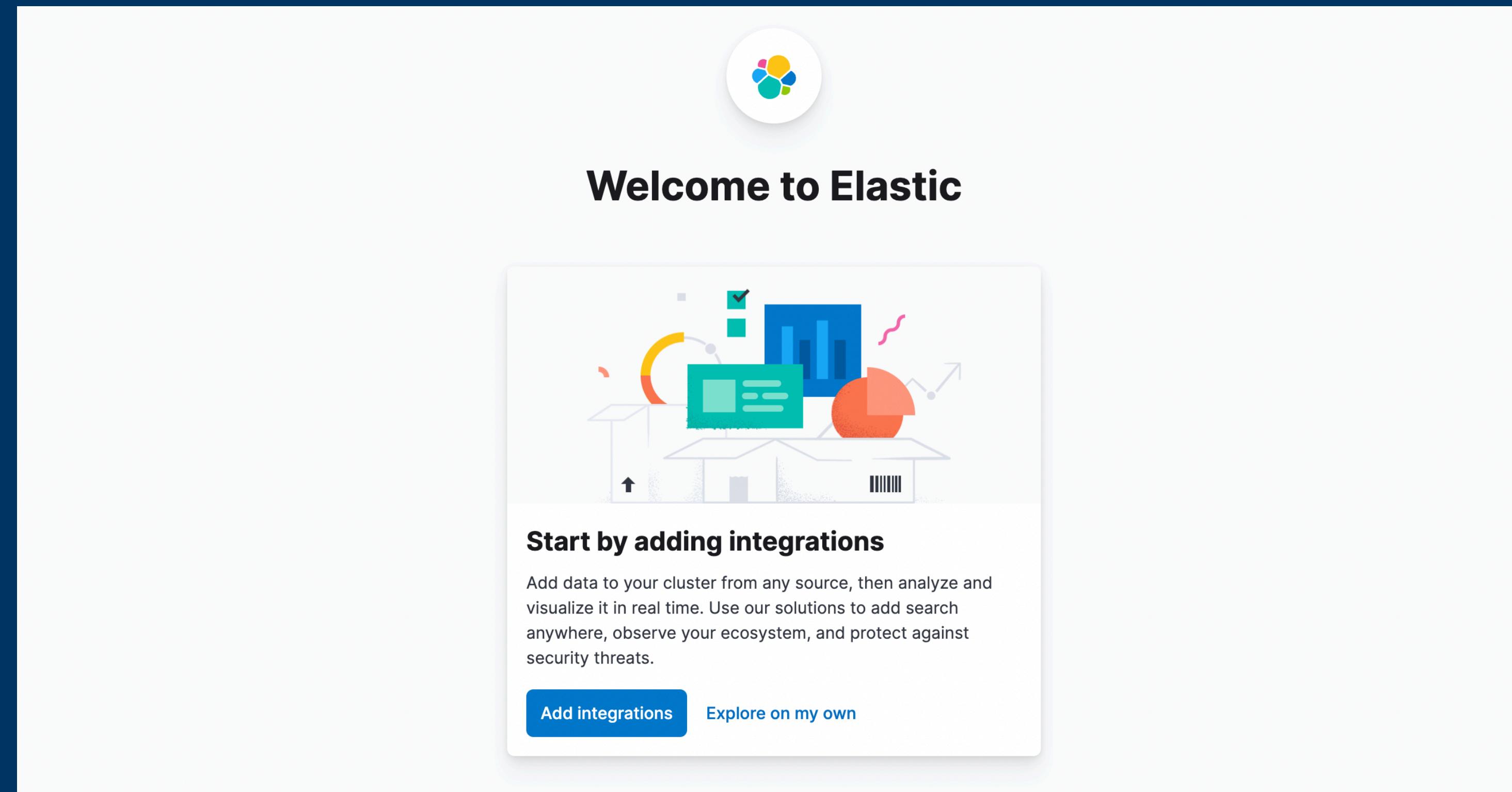
Show configuration ^ Create deployment



Credentials abspeichern, man weiß ja nie ...

Elasticstack

Mit „Explore on my own“ geht's weiter



Elasticstack

Damit sind wir auf einer bekannten Seite. Wir nehmen die Voreinstellung, fahren aber dieses mal mit „Add integrations“ fort.

Welcome home



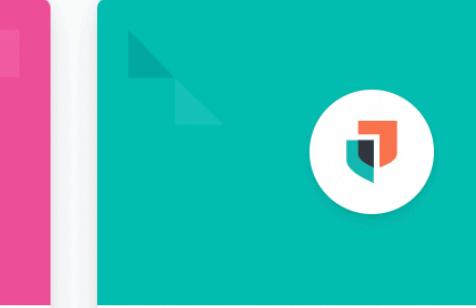
Enterprise Search

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 integrations

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 integrations](#) [Try sample data](#) [Upload a file](#)



Management



Manage permissions

Control who has access and what tasks they can perform.



Monitor the stack

Track the real-time health and performance of your deployment.



Back up and restore

Save snapshots to a backup repository, and restore to recover index and cluster state.



Manage index lifecycles

Define lifecycle policies to automatically perform operations as an index ages.

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

[Display a different page on log in](#)

Elasticstack

Über die Auswahl „Containers“ und „Docker Metrics“ sind wir hier

The screenshot shows the Elastic Stack interface with the Docker Metrics integration selected. The top navigation bar includes tabs for Todo App, Docker Metrics - Integrations, Ingest data from a relational database, Index recovery prioritization, and a plus sign. Below the navigation is a search bar with placeholder text "Find apps, content, and more. Ex: Discover". The main content area features the "Docker Metrics" integration card. The card includes a logo of a blue Docker container icon, the title "Docker Metrics", a status indicator "Elastic Agent", the version "1.2.0", and a "View deployment details" button. Below the card, there are sections for "Docker Integration" (describing it as fetching metrics from Docker containers), "Compatibility" (mentioning Linux and Mac support), "Running from within Docker" (with a command example), and "Screenshots" (showing a dashboard visualization). To the right of the card, a sidebar displays "Details" with information such as Version 1.2.0, Category Containers, OS & System, Kibana assets Dashboards 1, Saved searches 1, Visualizations 7, Features metrics, and License basic.

Docker Metrics

Elastic Agent

Version 1.2.0

Add Docker Metrics

Screenshots

Details

Version 1.2.0

Category Containers, OS & System

Kibana assets Dashboards 1

Saved searches 1

Visualizations 7

Features metrics

License basic

```
docker run -d \
--name=metricbeat \
--user=root \
--volume="/var/run/docker.sock:/var/run/docker.sock:ro" \
-docker.elastic.co/beats/metricbeat:latest metricbeat -e \
```

Elasticstack

Über die Auswahl „Containers“ und „Docker Metrics“ sind wir hier

The screenshot shows the Elastic Stack interface with the Docker Metrics integration selected. The top navigation bar includes tabs for Todo App, Docker Metrics - Integrations, Ingest data from a relational database, Index recovery prioritization, and a plus sign. Below the navigation is a search bar with placeholder text "Find apps, content, and more. Ex: Discover". The main content area features the elastic logo, a breadcrumb navigation with "Integrations" and "Docker Metrics", and a "View deployment details" button. A large card for the "Docker Metrics" integration is displayed, showing its icon (a blue Docker logo), name, status as "Elastic Agent", version 1.2.0, and a "Add Docker Metrics" button. The card also includes sections for "Overview" (selected), "Settings", "Docker Integration" (describing metric streams), "Compatibility" (Linux/Mac support), "Running from within Docker" (instructions for unix socket), and a code snippet for running Metricbeat. To the right of the card are "Screenshots" (one shown), "Details" (version 1.2.0, category Containers, OS & System, Kibana assets: Dashboards 1, Saved searches 1, Visualizations 7), "Features" (metrics), and "License" (basic). The browser's address bar shows the URL "joeatc.kb.eu-central-1.aws.cloud.es.io:9243/app/integrations/detail/docker-1.2.0/overview".

Elasticstack

und über Add integration sind wir hier, die Voreinstellungen mit „save and continue“ übernehmen.

The screenshot shows the 'Add integration' wizard for Docker Metrics in the Elastic Stack interface. The process is divided into two main steps:

- Step 1: Configure integration**
 - Integration settings**: Fields for 'Integration name' (set to 'docker-1') and 'Description' (marked as optional). A link to 'Advanced options' is available.
 - Collect Docker metrics**: A toggle switch is turned on, and a dropdown menu is open, showing the current selection.
- Step 2: Where to add this integration?**
 - Create agent policy**: Fields for 'New agent policy name' (set to 'Agent policy 1') and a checkbox for 'Collect system logs and metrics'. A link to 'Advanced options' is available.

At the bottom right, there are 'Cancel' and 'Save and continue' buttons.

Elasticstack

An dieser Stelle können wir nicht mit den Voreinstellungen weiter machen, da wir aufgrund unserer Technik mit Docker Containern arbeiten müssen.

Daher verlassen wir diesen Dialog mit Close.

Über das Hamburger Symbol links oben gehen wir im Abschnitt Management zu Fleet.

Elasticstack

Über die Dev Tools - Management gelangt man zu Fleet ...

The screenshot shows the Fleet management interface within the Dev Tools. The top navigation bar includes a menu icon, a 'D' icon, and tabs for 'Fleet' (which is active) and 'Agents'. A search bar and filter buttons for 'Status', 'Agent policy', and 'Upgrade available' are also present. A prominent blue button at the top right says '+ Add agent'. Below this, a summary bar indicates 'Showing 1 agent' and status counts: Healthy (1), Unhealthy (0), Updating (0), and Offline (0). The main table lists one agent with the following details:

Host	Status	Agent policy	Version	Last activity	Actions
d10e1f69705b	Healthy	Elastic Cloud agent policy (rev. 4)	8.2.2	15 seconds ago	...

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

Elasticstack

Bevor wir einen neuen Agenten einrichten können benötigt man eine „policy“. Diese wurde schon angelegt, Agent policy 1.

The screenshot shows the Elastic Fleet interface. At the top, there are navigation links: a menu icon, a 'D' button, 'Fleet' (which is highlighted in green), and 'Agent policies'. On the right, there is a 'Send feedback' link. Below the header, the word 'Fleet' is displayed in large bold letters, followed by the subtitle 'Centralized management for Elastic Agents.' A navigation bar below the subtitle includes tabs for 'Agents', 'Agent policies' (which is underlined in blue, indicating it is selected), 'Enrollment tokens', 'Data streams', and 'Settings'. To the right of the tabs are three buttons: a search bar with a magnifying glass icon labeled 'Search', a 'Reload' button with a circular arrow icon, and a blue 'Create agent policy' button with a plus sign and a circle icon. The main area contains a table with the following data:

Name	Description	Last updated on	Agents	Integrations	Actions
Agent policy 1 rev. 2		Jun 06, 2022	0	2	...
Elastic Cloud agent po... rev. 4	Default agent policy for agents hosted on Elastic Cloud	Jun 06, 2022	1	2	...

At the bottom left, there is a 'Rows per page: 20' dropdown. At the bottom right, there are navigation arrows for pagination.

Name	Description	Last updated on	Agents	Integrations	Actions
Agent policy 1 rev. 2		Jun 06, 2022	0	2	...
Elastic Cloud agent po... rev. 4	Default agent policy for agents hosted on Elastic Cloud	Jun 06, 2022	1	2	...

Elasticstack

Auf Fleet - Settings finden man die server host Adresse

The screenshot shows the Elastic Fleet Settings page. At the top, there is a navigation bar with a menu icon, a 'D' button, 'Fleet' (which is highlighted in blue), 'Settings' (which is also highlighted in blue), and a 'Send feedback' link. Below the navigation bar, the word 'Fleet' is displayed in large bold letters, followed by the subtitle 'Centralized management for Elastic Agents.' A horizontal navigation bar below the subtitle includes links for 'Agents', 'Agent policies', 'Enrollment tokens', 'Data streams', and 'Settings', with 'Settings' being underlined to indicate it is the active tab. The main content area is titled 'Fleet server hosts' and contains the instruction: 'Specify the URLs that your agents will use to connect to a Fleet Server. If multiple URLs exist, Fleet will show the first provided URL for enrollment purposes. For more information, see the [Fleet User Guide](#).'. Below this text is a 'Host URL' input field containing the value 'https://e4ff2a7d407d4f00bdcb270b52f5aef7.fleet.eu-central-1.aws.cloud.es.io:443'. At the bottom of the input field is a blue 'Edit hosts' button.

Elasticstack

Auf Fleet - Enrollment Token bekommt man das Token:

The screenshot shows the Fleet interface with the following details:

- Header:** D, Fleet, Enrollment tokens, Send feedback.
- Title:** Fleet
- Description:** Centralized management for Elastic Agents.
- Navigation:** Agents, Agent policies, **Enrollment tokens**, Data streams, Settings.
- Text:** Create and revoke enrollment tokens. An enrollment token enables one or more agents to enroll in Fleet and send data.
- Search Bar:** Search
- Create Enrollment Token Button:** Create enrollment token
- Table:** Enrollment tokens list with columns: Name, Secret, Agent policy, Created on, Active, Actions. A tooltip "Hide token" is shown over the Agent policy column for the first row.

Name	Secret	Agent policy	Created on	Active	Actions
Default (3c01b206-6c79-4386-882f-67f7f6...)	T21NTU9vRUJFdzJfV256eW FxOWo6dGc1ZHSTM1FRVzY 0NFdWUGwzRXBaUQ==	Agent policy 1	Jun 06, 2022	●	

- Pagination:** Rows per page: 20, Page: 1 of 1.

Elasticstack

Damit haben wir alle Informationen zusammen, um den Container zu starten:

```
docker run \
--env FLEET_ENROLL=1 \
--env FLEET_URL=https://e4ff2a7d407d4f00bdcb270b52f5aef7.fleet.eu-central-1.aws.cloud.es.io:443 \
--env
FLEET_ENROLLMENT_TOKEN=T21NTU9vRUJFdzJfV256eWFxOWo6dGc1ZHZTM1FRVzY0NFdWUGwzRXBaUQ== \
--rm docker.elastic.co/beats/elastic-agent:8.2.2-arm64
```

Im Terminal werden viele JSON Dokumente erstellt. Dieses Terminal nicht schließen!

Elasticstack

Fleet Agents sollte dann in etwa so aussehen

The screenshot shows the Elastic Fleet interface. At the top, there's a navigation bar with icons for three, a 'D' button, 'Fleet' (which is highlighted in blue), and 'Agents'. On the far right is a 'Send feedback' button. Below the navigation, the word 'Fleet' is prominently displayed in large bold letters, followed by the subtitle 'Centralized management for Elastic Agents.' A horizontal menu bar below the subtitle includes tabs for 'Agents' (which is underlined in blue), 'Agent policies', 'Enrollment tokens', 'Data streams', and 'Settings'. To the left of the main content area is a search bar with a magnifying glass icon and the placeholder 'Search'. To the right of the search bar are filters for 'Status' (set to 'Healthy'), 'Agent policy' (set to '2'), and 'Upgrade available'. A large blue button labeled '+ Add agent' is also present. Below these controls, a message says 'Showing 2 agents'. To the right of the message are status counts: 2 Healthy, 0 Unhealthy, 0 Updating, and 0 Offline. A green horizontal bar spans the width of the table below. The main table has columns for 'Host' (with a checkbox), 'Status' (with a color-coded button), 'Agent policy' (with a link), 'Version' (8.2.2), 'Last activity' (35 seconds ago for the first row), and 'Actions' (with a three-dot menu icon). Two rows are listed: one for host 'b6c05a2c1a1e' (status 'Healthy', policy 'Joes Policy rev. 1') and another for host 'd10e1f69705b' (status 'Healthy', policy 'Elastic Cloud agent policy rev. 4'). At the bottom left, there's a 'Rows per page: 20' dropdown. At the bottom right, there are navigation arrows for page 1.

Host	Status	Agent policy	Version	Last activity	Actions
b6c05a2c1a1e	Healthy	Joes Policy rev. 1	8.2.2	35 seconds ago	...
d10e1f69705b	Healthy	Elastic Cloud agent policy rev. 4	8.2.2	46 seconds ago	...

Rows per page: 20 < 1 >

Elasticstack

Discover zeigt dann die eintreffenden Datenpakete ...

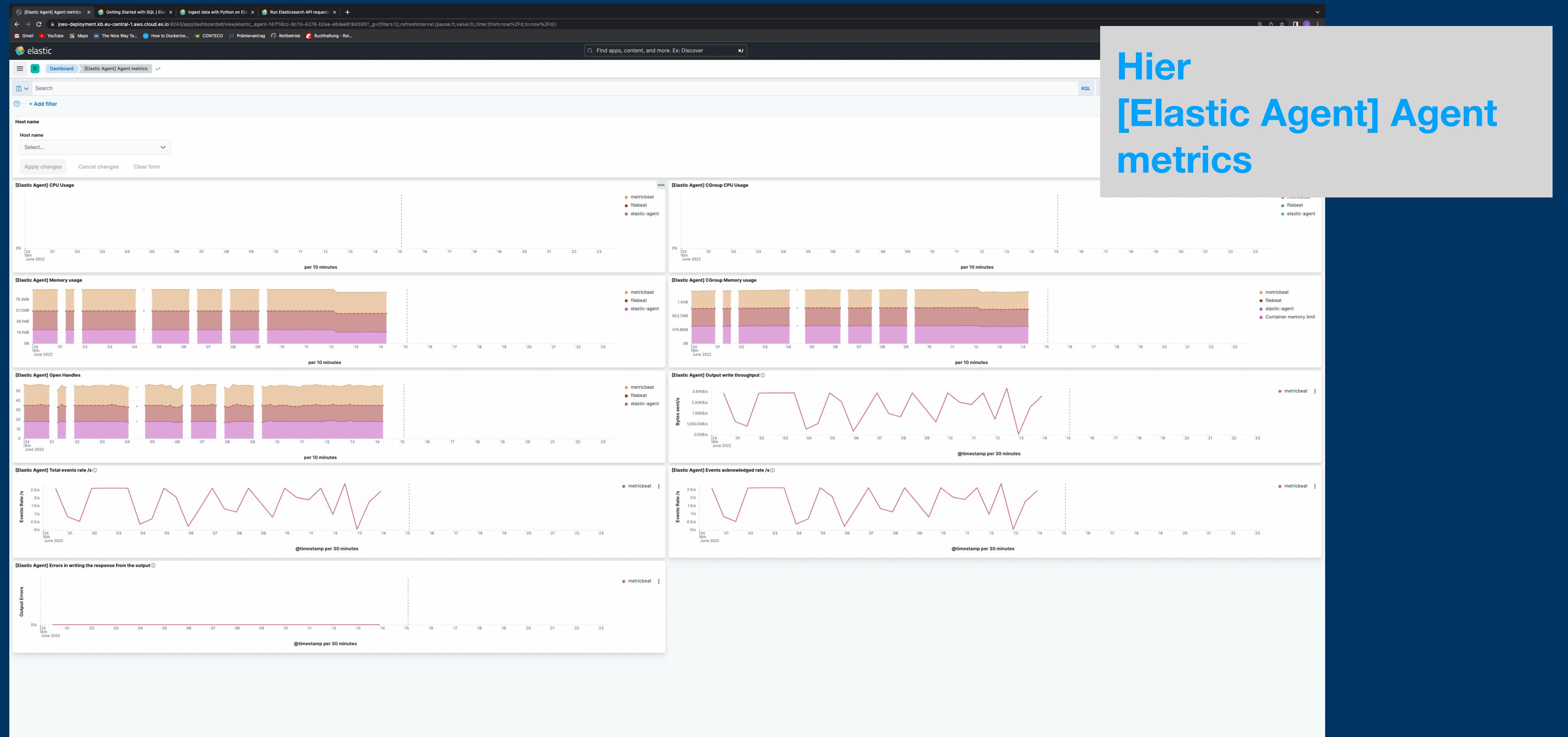
The screenshot shows the Elasticsearch Discover interface. At the top, there are tabs for 'Discover' (which is selected), 'New', 'Open', 'Share', and 'Inspect'. Below the tabs are search and filter fields. The search field contains 'logs-*' and the filter field shows '+ Add filter'. The main area displays 60 hits from the last 15 minutes. A histogram at the top shows document counts for each minute from Jun 5, 2022, 12h to Jun 5, 2022, 12:54. The time range is Jun 5, 2022 @ 12:39:37.554 - Jun 5, 2022 @ 12:54:37.554. Below the histogram, it says '1 field sorted' by '@timestamp'. The table shows two documents:

	↓ @timestamp	Document
Jun 5, 2022 @ 12:54:28.869		@timestamp Jun 5, 2022 @ 12:54:28.869 agent.ephemeral_id 39853a51-757c-4c93-b663-1e8cbfc564ce agent.id 658924bb-7d8b-4b13-924f-c0f53ca4284f agent.name b6c05a2c1a1e agent.type filebeat agent.version 8.2.2 data_stream.dataset elastic_agent.filebeat data_st...
Jun 5, 2022 @ 12:54:28.270		@timestamp Jun 5, 2022 @ 12:54:28.270 agent.ephemeral_id 39853a51-757c-4c93-b663-1e8cbfc564ce agent.id 658924bb-7d8b-4b13-924f-c0f53ca4284f agent.name b6c05a2c1a1e agent.type filebeat agent.version 8.2.2 data_stream.dataset elastic_agent.metricbeat dat...

At the bottom, it says 'Rows per page: 100' and has navigation arrows.

Elasticstack

Daten können mit Dashboards visualisiert werden.



Elasticstack

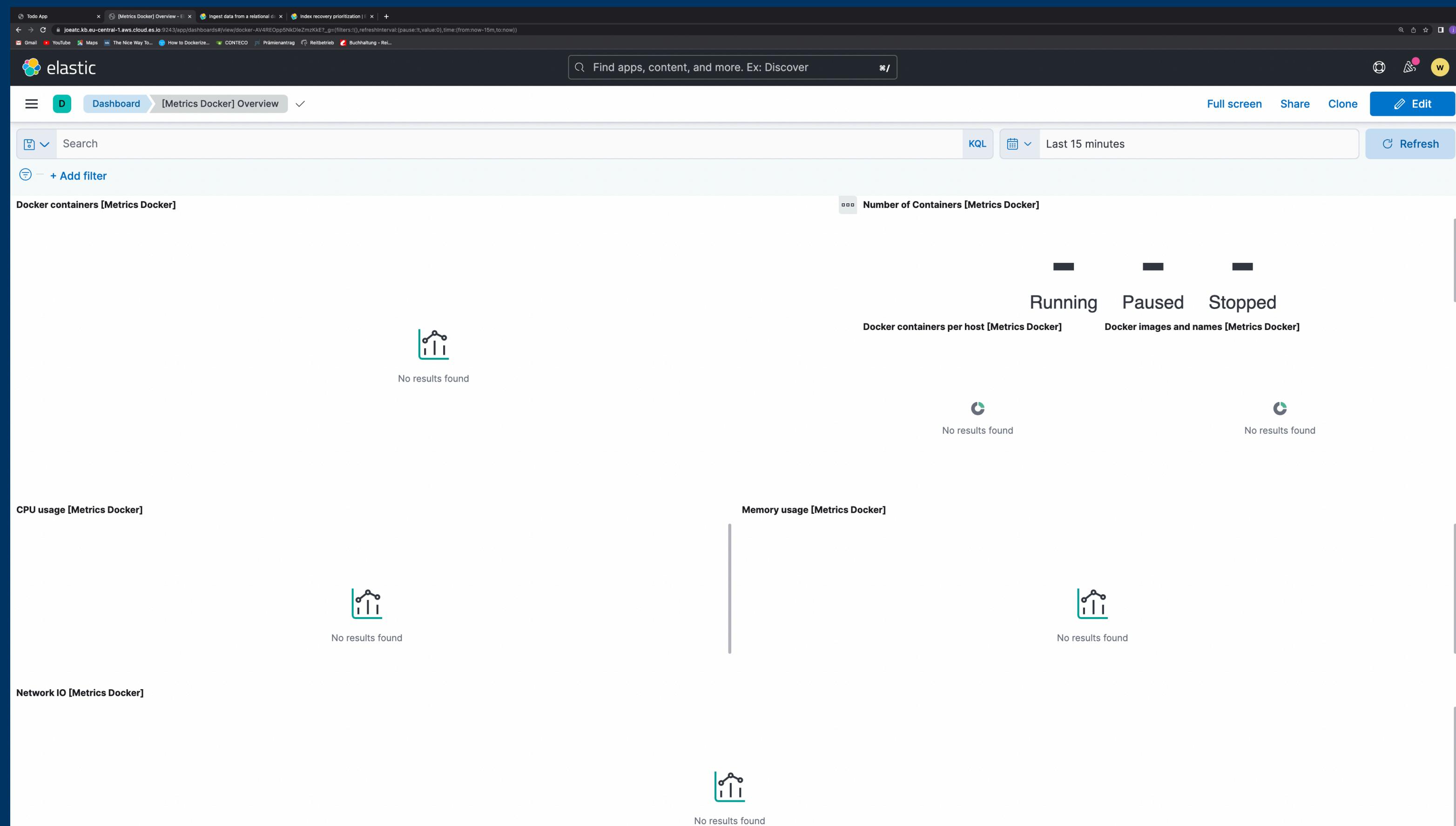
Daten können mit Dashboards visualisiert werden. Etliche Dashboards sind bereits vorgefertigt. Wie zu erwarten, gibt es auch für Docker ein Dashboard: [Metrics Docker] Overview.

The screenshot shows the 'Dashboards' section of the Elastic Stack interface. At the top, there is a search bar labeled 'Search...' and a 'Tags' dropdown. On the right, a blue button says '+ Create dashboard'. Below this, a table lists ten pre-built dashboards:

Title	Description	Tags	Actions
[Elastic Agent] Agent metrics	Elastic Agent metrics dashboard		
[Logs System] New users and groups	New users and groups dashboard for the System integration in Logs		
[Logs System] SSH login attempts	SSH dashboard for the System integration in Logs		
[Logs System] Sudo commands	Sudo commands dashboard from the Logs System integration		
[Logs System] Syslog dashboard	Syslog dashboard from the Logs System integration		
[Metrics Docker] Overview	Overview of docker containers		
[Metrics System] Host overview	Overview of host metrics		
[Metrics System] Overview	Overview of system metrics		
[System Windows Security] Failed and Blocked	Failed and blocked accounts with TSVB metrics		

Elasticstack

Dieser zeigt aber noch keine Daten. Der gestartete Container Elastic Agent ist dafür nicht zuständig. Wir benötigen einen weiteren Container.



Elasticstack

Auf der Seite des Integrationsmoduls findet sich ein Hinweis auf die Installation dieses Containers. Leider nicht genug für unsere Konfiguration.

The screenshot shows the Elastic Stack interface with the URL <https://joaotc.kb.eu-central-1.aws.cloud.es.io:9243/app/integrations/detail/docker-1.2.0/overview>. The page displays the Docker Metrics integration details:

- Docker Metrics** (Version 1.2.0)
- Elastic Agent**
- Agent policies**: 1
- Add Docker Metrics** button
- Screenshots**: One screenshot showing a dashboard with various metrics and charts.
- Details** section:
 - Version: 1.2.0
 - Category: Containers, OS & System
 - Kibana assets: Dashboards 1, Saved searches 1, Visualizations 7
 - Features: metrics
 - License: basic
- Compatibility**: Docker module tested on Linux and Mac with community edition engine versions 1.11 and 17.09.0-ce. Not tested on Windows.
- Running from within Docker**: Instructions for connecting to the docker socket.
- Module-specific configuration notes**: Recommendation to run Docker metricsets with a period of 3 seconds or longer.

Elasticstack

Drei Informationen müssen gefunden werden:

1. output host —> Manage this Deployment —> Elastic Search copy endpoint
2. cloud id —> ebenda
3. cloud authentication —> die herunter geladenen credentials user und password

```
joe@MacBook % docker pull docker.elastic.co/beats/metricbeat:8.2.2-arm64
```

```
joe@MacBook % docker run -d \
--name=metricbeat \
--user=root \
--volume="/var/run/docker.sock:/var/run/docker.sock:ro" \
docker.elastic.co/beats/metricbeat:8.2.2-arm64 metricbeat -e \
-E output.elasticsearch.hosts=https://joeatc.es.eu-central-1.aws.cloud.es.io:9243 \
-E
cloud.id=joeatc:ZXUtY2VudHJhbC0xLmF3cy5jbG91ZC5lcy5pbvQxNTM3ODIzZGU1ZTU0OWI2OTZhM2NINWRhO
TczMGZINCQ4NTg3N2QzYzZjNWQ0ZjE2OTYwYzYyNWEwZDY5OTI5NQ== \
-E cloud.auth=elastic:DVoxjSjZSEPgB4KV2X7OKOYH
```

Elasticstack

Die Konsole meldet:

```
{"log.level":"info","@timestamp":"2022-06-06T18:16:36.846Z","log.logger":"publisher_pipeline_output","log.origin": {"file.name":"pipeline/client_worker.go","file.line":147}, "message": "Connection to backoff(elasticsearch(https://1537823de5e549b696a3ce5da9730fe4.eu-central-1.aws.cloud.es.io:443)) established", "service.name": "metricbeat", "ecs.version": "1.6.0"} {"log.level":"info","@timestamp":"2022-06-06T18:17:00.817Z","log.logger":"monitoring","log.origin": {"file.name":"log/log.go","file.line":184}, "message": "Non-zero metrics in the last 30s", "service.name": "metricbeat", "monitoring": {"metrics": {"beat": {"cgroup": {"cpu": {"id": "/"}, "memory": {"id": "/", "mem": {"usage": {"bytes": 68763648}}}}, "cpu": {"system": {"ticks": 270, "time": {"ms": 270}}, "total": {"ticks": 860, "time": {"ms": 860}, "value": 0}, "user": {"ticks": 590, "time": {"ms": 590}}}, "handles": {"limit": {"hard": 1048576, "soft": 1048576}, "open": 12}, "info": {"ephemeral_id": "8d8bf070-4ce7-4af4-b88a-c4c806d7f70b", "uptime": {"ms": 33150}, "version": "8.2.2"}, "memstats": {"gc_next": 21345648, "memory_alloc": 12867840, "memory_sys": 56050696, "memory_total": 127438176, "rss": 149110784}, "runtime": {"goroutines": 71}, "libbeat": {"config": {"module": {"running": 3, "starts": 3}, "reloads": 1, "scans": 1}, "output": {"events": {"acked": 37, "active": 0, "batches": 5, "total": 37}, "read": {"bytes": 8467}, "type": "elasticsearch", "write": {"bytes": 380905}}, "pipeline": {"clients": 10, "events": {"active": 4, "filtered": 1, "published": 41, "retry": 13, "total": 42}, "queue": {"acked": 37, "max_events": 4096}}, "metricbeat": {"system": {"cpu": {"events": 4, "success": 4}, "filesystem": {"events": 1, "success": 1}, "fsstat": {"events": 1, "success": 1}, "load": {"events": 4, "success": 4}, "memory": {"events": 4, "success": 4}, "network": {"events": 14, "success": 14}, "process": {"events": 6, "success": 6}, "process_summary": {"events": 4, "success": 4}, "socket_summary": {"events": 3, "success": 3}, "uptime": {"events": 1, "success": 1}}, "system": {"cpu": {"cores": 4}, "load": {"1": 0.09, "15": 0, "5": 0.04}, "norm": {"1": 0.0225, "15": 0, "5": 0.01}}}, "ecs.version": "1.6.0"}}
```

Elasticstack

Ein Blick in Fleet mit einem gelegentliche Reload zeigt, dass die Daten fließen.
Wenn man im Feld Integration „Docker“ wählt, erhält man diese Ansicht:

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens **Data streams** Settings

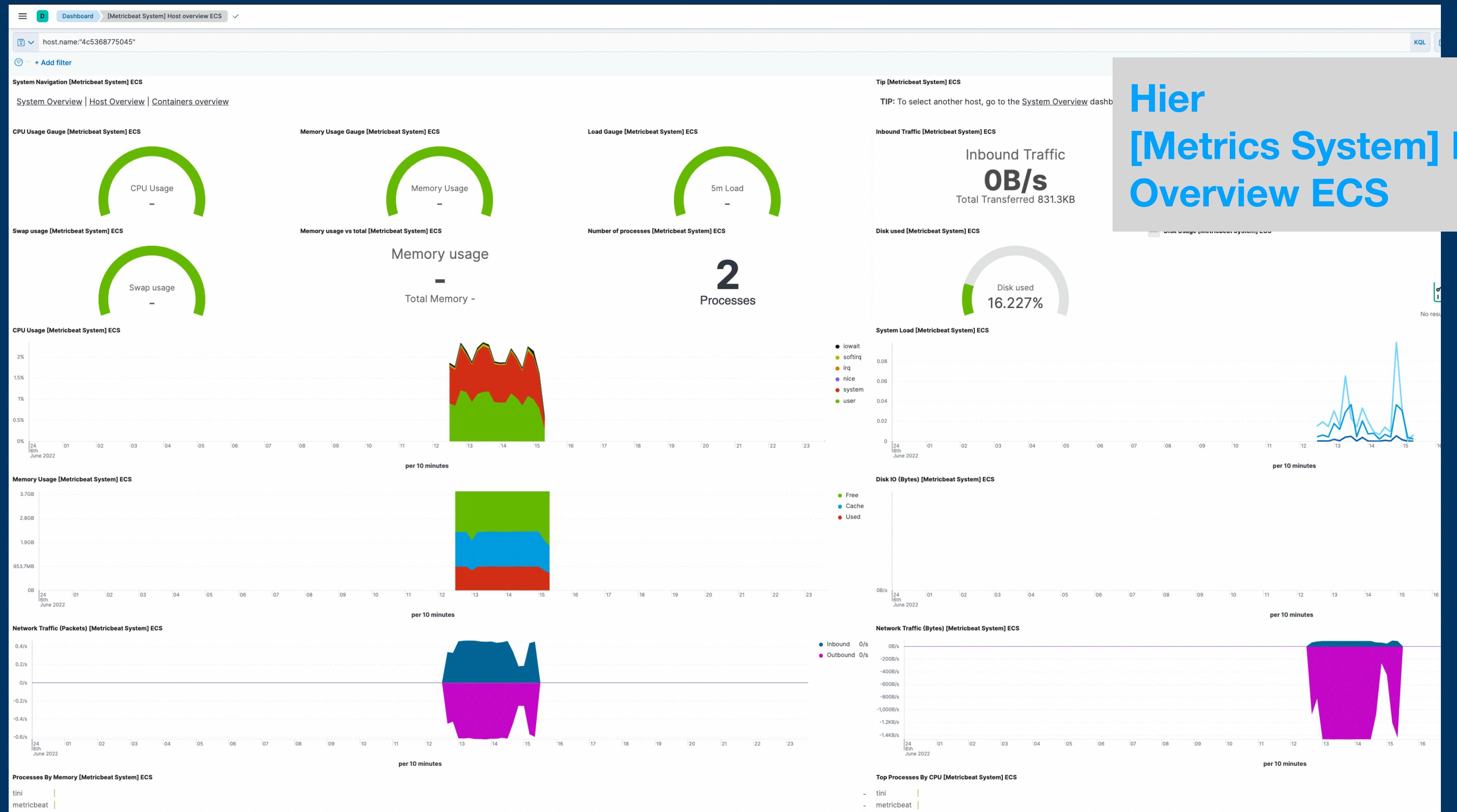
package=(docker) (X) Dataset Type Namespace Integration 1 Reload

Dataset	Type	Namespace	Integration	Last activity	Size	Actions
docker.container	metrics	default	docker	Jun 6, 2022 @ 8:22:55 PM	502.8kb	...
docker.cpu	metrics	default	docker	Jun 6, 2022 @ 8:22:55 PM	477.9kb	...
docker.diskio	metrics	default	docker	Jun 6, 2022 @ 8:22:55 PM	610.4kb	...
docker.healthcheck	metrics	default	docker	Jun 6, 2022 @ 8:22:55 PM	504.6kb	...
docker.info	metrics	default	docker	Jun 6, 2022 @ 8:22:55 PM	500.6kb	...
docker.memory	metrics	default	docker	Jun 6, 2022 @ 8:22:55 PM	576kb	...
docker.network	metrics	default	docker	Jun 6, 2022 @ 8:22:55 PM	462.4kb	...

Rows per page: 20 < 1 >

Elasticstack

Daten können mit Dashboards visualisiert werden.



Hier
[Metrics System] Host
Overview ECS

Elasticstack

Verwendung von Kibana

Klickt man auf Dashboard, so wird die Liste der bestehenden Dashboards angezeigt.

The screenshot shows the Kibana Dashboards interface. At the top, there is a search bar labeled "Search..." and a "Create dashboard" button. Below the search bar is a table with columns: "Title", "Description", "Tags", and "Actions". There are six rows in the table, each representing a dashboard:

Title	Description	Tags	Actions
Diabetes Prediction			edit
[Elastic Agent] Agent metrics	Elastic Agent metrics dashboard		edit
[Logs System] New users and groups	New users and groups dashboard for the System integration in Logs		edit
[Logs System] SSH login attempts	SSH dashboard for the System integration in Logs		edit
[Logs System] Sudo commands	Sudo commands dashboard from the Logs		edit

The screenshot shows the Kibana Dashboard view for the "[Metricbeat System] Overview ECS" dashboard. At the top, there is a breadcrumb navigation: "Dashboard" (highlighted with a red circle), "Search", "+ Add filter", and "System Navigation [Metricbeat System] ECS". Below the navigation, there are three links: "System Overview", "Host Overview", and "Containers overview". A large number "3" is displayed, indicating the count of hosts. The overall interface is clean and modern, typical of the Kibana web application.

Nicht alle Dashboards zeigen etwas an, oft fehlen die entsprechenden Daten.

Elasticstack

Stellt sich die Frage, ob unsere Lineare Regression auf das Deployment anwendbar ist:

In der Dokumentation über Python Integration finden sich die Anweisungen die für die Anbindung an die Cloud notwendig sind:

- ini-Datei erzeugen
- credentials eintragen
- package laden
- Elasticsearch Instanz anpassen

Elasticstack

example.ini

```
[ELASTIC]
cloud_id =
Joes_Deployment:ZXUtY2VudHJhbC0xLmF3cy5jbG91ZC5lcy5pbyRmM2ZmYWlwODcyNTI0OGRIOTU4
MDVhYTM0MDJiODc4MyQwMDNIMzE2YmlxYWQ0ZTUzOTZmZjJjNzM3NWEzOTdiYw==
user = elastic
password = ML7v7y9hT5UGBwv4KEHYwuPP
```

Elasticstack

Pakete und Einstellungen in der Python Datei:

```
import configparser

config = configparser.ConfigParser()
config.read('example.ini')

# Create the client instance
es = Elasticsearch(
    cloud_id=config['ELASTIC']['cloud_id'],
    http_auth=(config['ELASTIC']['user'], config['ELASTIC']['password'])
)
```

Elasticstack

Nach einem run Kommando sollte in Kibana - DevTools - Stack Management - Index Management der neue Index vorliegen

The screenshot shows the Elasticsearch Stack Management - Index Management interface. The left sidebar has a navigation menu with 'Management', 'Ingest', 'Data', and 'Alerts and Insights'. Under 'Data', 'Index Management' is selected, which is also reflected in the breadcrumb at the top of the main content area. The main content area is titled 'Index Management' and includes tabs for 'Indices', 'Data Streams', 'Index Templates', and 'Component Templates'. Below the tabs, there is a search bar, filter options for 'Lifecycle status' and 'Lifecycle phase', and a 'Reload indices' button. A table lists the indices, showing one entry: 'diabetes-index' with a green health status, open status, 1 primary, 1 replica, 40 documents, and 28.9kb storage size. At the bottom, there are buttons for 'Rows per page' (set to 10) and navigation arrows.

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
diabetes-index	green	open	1	1	40	28.9kb	

Elasticstack

Mittels Create data view wird eine neue Sicht auf die Daten erstellt

The screenshot shows the Elasticsearch Stack Management interface, specifically the Data Views section. The URL in the browser is `joes-deployment.kb.eu-central-1.aws.cloud.es.io:9243/app/management/kibana/dataViews/`. The left sidebar includes links for Reporting, Machine Learning, Watcher, Security, Users, Roles, API keys, Role Mappings, Kibana, Data Views (which is the active tab), Saved Objects, Tags, Search Sessions, Spaces, and Advanced Settings. The main content area is titled "Data Views" and contains the sub-instruction "Create and manage the data views that help you retrieve your data from Elasticsearch." A search bar labeled "Search..." is present. Below is a table listing data views:

	Name ↑	Spaces	Actions
<input type="checkbox"/>	logs-* Default	D	Edit
<input type="checkbox"/>	diabetes-index	D	Edit
<input type="checkbox"/>	metricbeat-*	D	Edit
<input type="checkbox"/>	metrics-*	D	Edit

At the bottom, there is a "Rows per page: 10" dropdown and a page navigation indicator "< 1 >".

Elasticstack

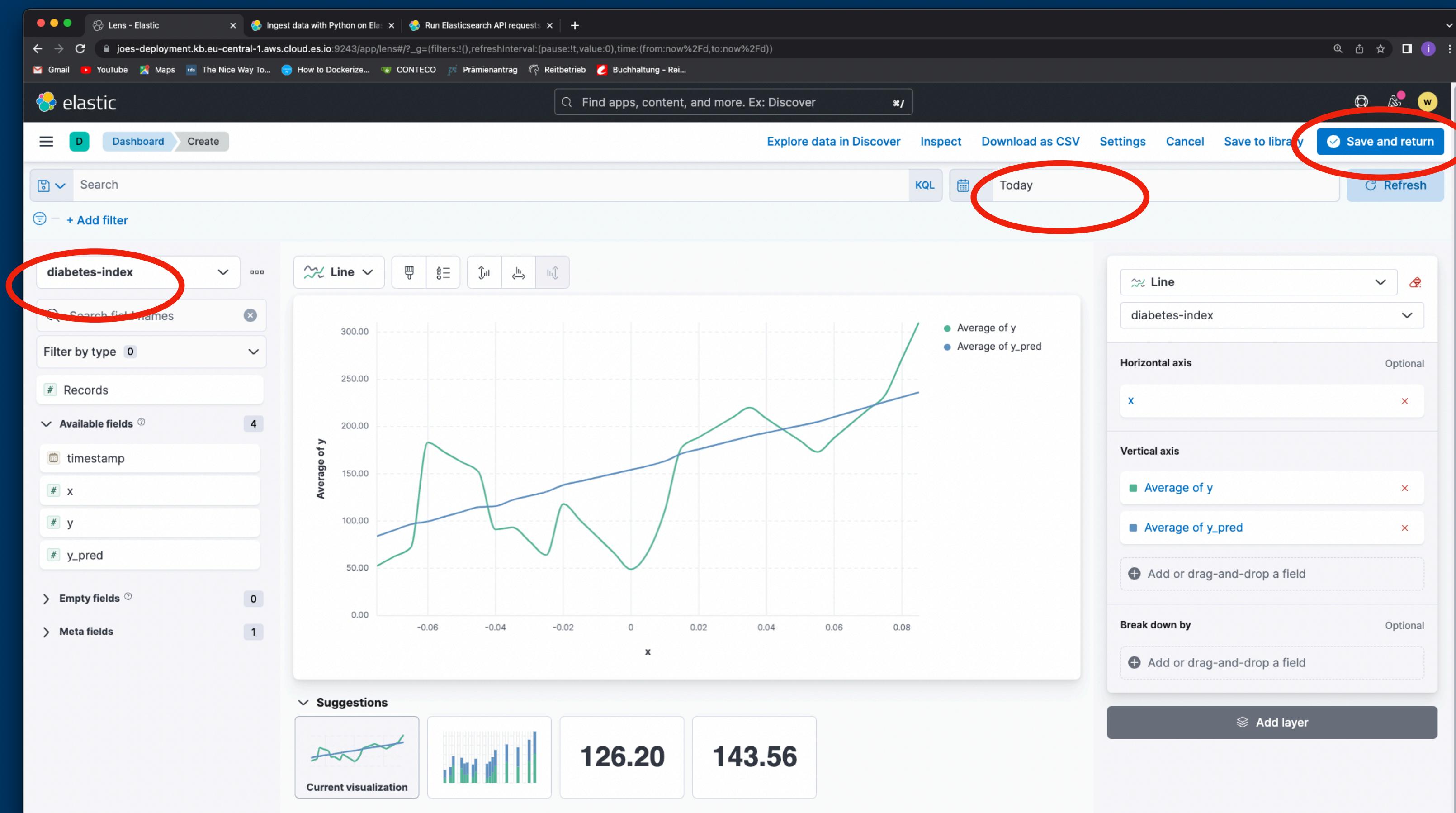
Wählt man in discover den richtigen Index und passt den Zeitraum an („Today“), so sollten die Daten sichtbar sein.

The screenshot shows the Elasticsearch Discover interface. At the top left, there are three tabs: 'Discover' (which is selected and highlighted in blue), 'Ingest data with Python on Elastic' (disabled), and 'Run Elasticsearch API requests' (disabled). The URL in the address bar is `joes-deployment.kb.eu-central-1.aws.cloud.es.io:9243/app/discover#/?_g=()&_a=(columns:!(),filters:!(),index:'1a2a0c10-e58f-11ec-8ed5-dbba90d387db',interval:auto,query:(language:kuery,query:""),sort:[!(_id,desc)])`. The main search bar contains the placeholder 'Find apps, content, and more. Ex: Discover'. On the right side of the header, there are buttons for 'Options', 'New', 'Open', 'Share', 'Inspect', and 'Save'. Below the header, there's a toolbar with icons for 'Search' (magnifying glass), '+ Add filter' (gear icon), and a date range selector. The date range selector has three options: 'KQL' (selected), 'Today' (highlighted with a red oval), and 'This week'. To the right of the date range is a 'Refresh' button. The main area displays '20 hits' of data. A histogram at the top shows the distribution of timestamps from Jun 6, 2022, to Jun 7, 2022. Below the histogram, a table lists the data, sorted by timestamp. Each row contains a timestamp, a timestamp field, and a document object. The first few rows of the table are:

	↓ timestamp	Document
Jun 6, 2022 @ 15:48:42.454	timestamp	Jun 6, 2022 @ 15:48:42.454 x -0.073 y 57 y_pred 84.399 _id 20 _index diabetes-index _score -
Jun 6, 2022 @ 15:48:42.421	timestamp	Jun 6, 2022 @ 15:48:42.421 x 0.039 y 220 y_pred 189.568 _id 19 _index diabetes-index _score -
Jun 6, 2022 @ 15:48:42.379	timestamp	Jun 6, 2022 @ 15:48:42.379 x -0.016 y 132 y_pred 137.995 _id 18 _index diabetes-index _score -
Jun 6, 2022 @ 15:48:42.336	timestamp	Jun 6, 2022 @ 15:48:42.336 x -0.016 y 104 y_pred 137.995 _id 17 _index diabetes-index _score -
Jun 6, 2022 @ 15:48:42.309	timestamp	Jun 6, 2022 @ 15:48:42.309 x 0.02 y 178 y_pred 171.366 _id 16 _index diabetes-index _score -
Jun 6, 2022 @ 15:48:42.183	timestamp	Jun 6, 2022 @ 15:48:42.183 x -0.074 y 48 y_pred 83.388 _id 15 _index diabetes-index _score -

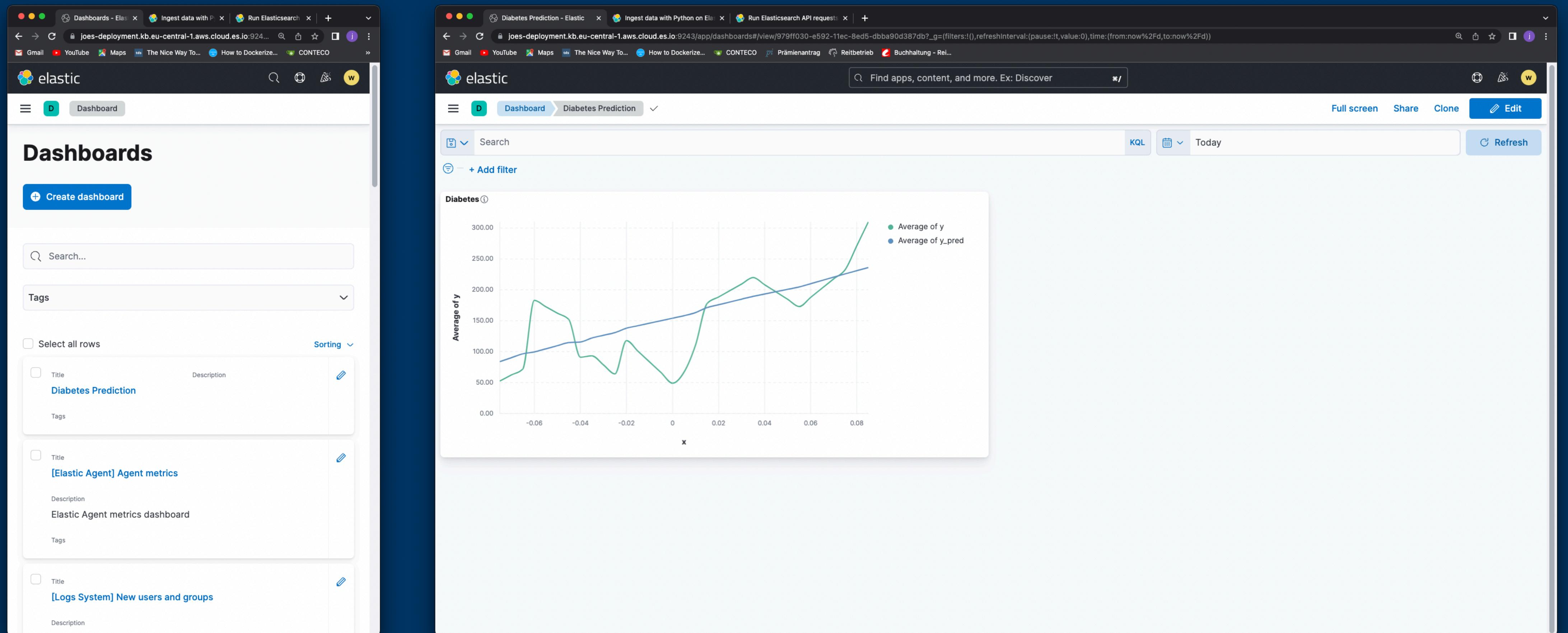
Elasticstack

Über dashboard create gelangt man in die visualisation. Hier Kann der Grafiktyp und das Aussehen der Grafik angepasst werden. Speichern und zurück sichert die Arbeit.



Elasticstack

Über dashboard create gelangt man in die visualisation. Hier Kann der Grafiktyp und das Aussehen der Grafik angepasst werden. Speichern und zurück sichert die Arbeit.



Elasticstack

Konklusion

- Es wurden zwei Container erstellt, die kontinuierlich Daten an die Elastic Cloud senden.
- Dabei ist der Elastic Agent notwendig, um die Integration des Docker Metricbeats zu gewährleisten.
- Trotzdem laufend Daten ankommen, ist es möglich, Daten ganz anderer Art in den Cluster zu laden und auszuwerten.

Elasticstack

Konklusion

- Beim Arbeiten mit Containern ist darauf Rücksicht zu nehmen, dass das Schließen der Konsole zur Beendigung des Containers führt.
- Dadurch kommt es zu diesem Bild:

Fleet

Centralized management for Elastic Agents.

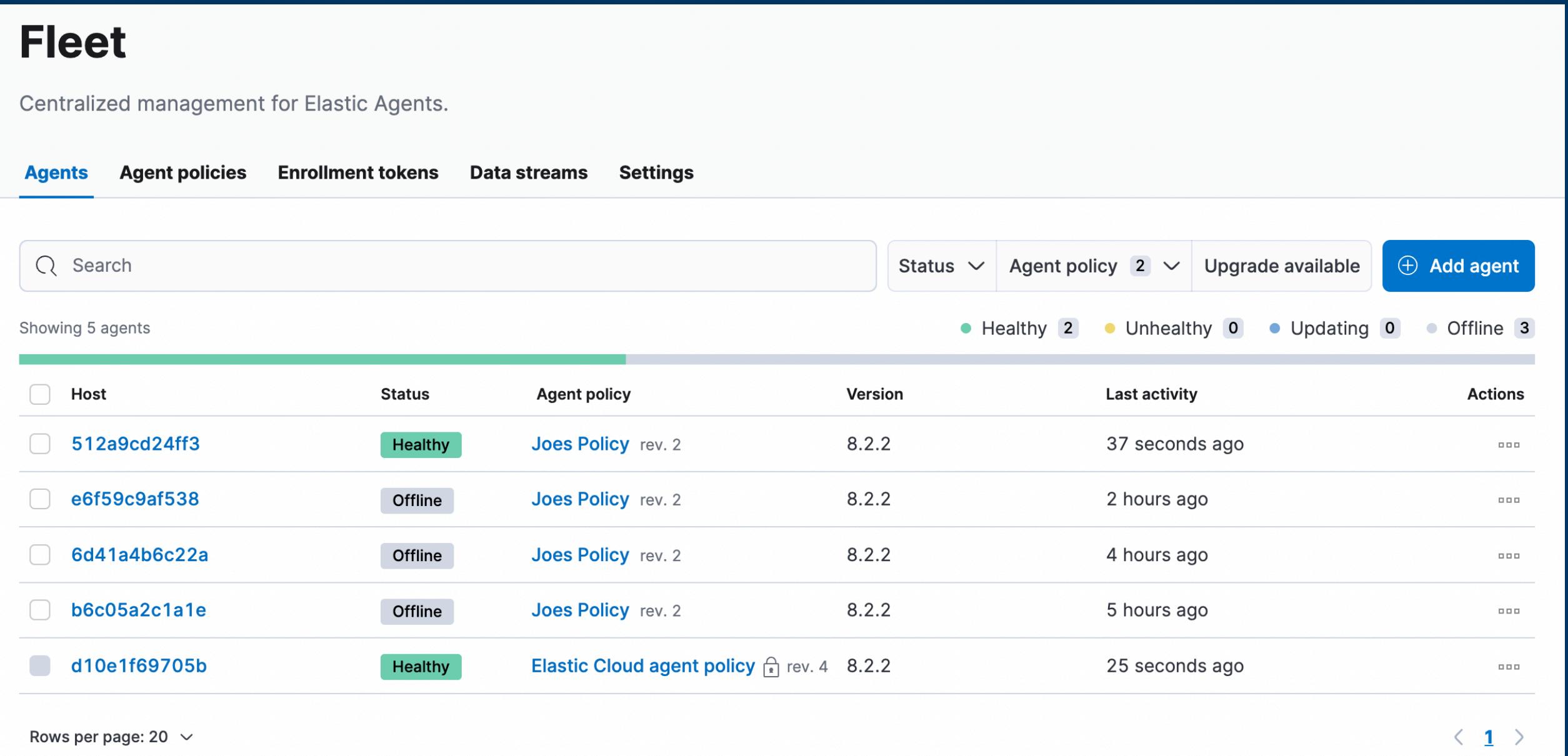
Agents Agent policies Enrollment tokens Data streams Settings

Search Status Agent policy 2 Upgrade available Add agent

Showing 5 agents

Host	Status	Agent policy	Version	Last activity	Actions
512a9cd24ff3	Healthy	Joes Policy rev. 2	8.2.2	37 seconds ago	...
e6f59c9af538	Offline	Joes Policy rev. 2	8.2.2	2 hours ago	...
6d41a4b6c22a	Offline	Joes Policy rev. 2	8.2.2	4 hours ago	...
b6c05a2c1a1e	Offline	Joes Policy rev. 2	8.2.2	5 hours ago	...
d10e1f69705b	Healthy	Elastic Cloud agent policy rev. 4	8.2.2	25 seconds ago	...

Rows per page: 20 < 1 >



Offline Instanzen können gelöscht werden, da es sich um die alten, geschlossenen Container handelt. Es sei denn, man möchte die alten Daten noch auswerten.

Elasticstack

Fleet Agent Instanz löschen über Unenroll agent

