



CURSO 525

INFRAESTRUTURA ÁGIL COM PRÁTICAS DEVOPS





Construindo Dashboards com Kibana

Anotações

[illegible]

- ## Anotações

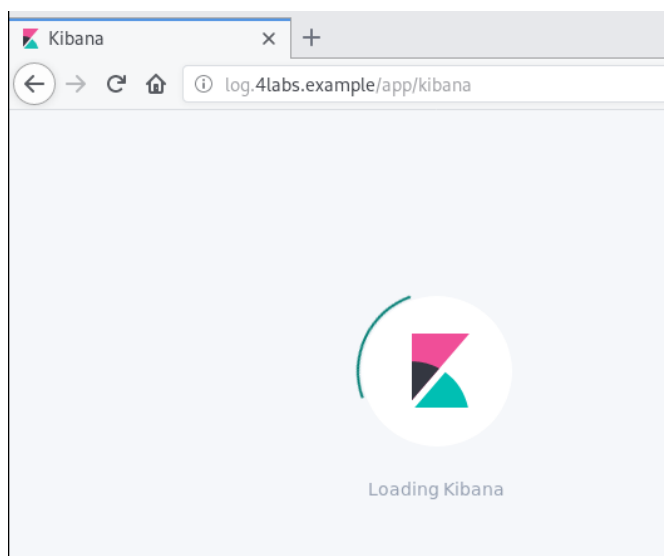
This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

The Kibana logo, featuring a stylized 'K' composed of a pink triangle, a black circle, and a teal circle, with the word 'kibana' in lowercase black text below it.

Anotações

[illegible]

Acesse a webpage do kibana, através do endereço <http://log4labs.example>.



Anotações

[illegible]

The screenshot shows the Kibana home page in a web browser. The address bar displays 'log-4labs.example/app/kibana#/home?g=0'. The page has a top navigation bar with a 'Home' link. The main content area is titled 'Add Data to Kibana' and provides instructions on using pre-built dashboards and monitoring systems. It features four primary options for data ingestion: APM (Application Performance Monitoring), Logging, Metrics, and SIEM (Security Information and Event Management). Each option includes a brief description and a button to proceed. Below these, there are three additional links: 'Add sample data', 'Upload data from log file', and 'Use Elasticsearch data'. The page is divided into two main sections: 'Visualize and Explore Data' and 'Manage and Administer the Elastic Stack'. The 'Visualize and Explore Data' section includes links for 'Dashboard', 'Discover', and 'Canvas'. The 'Manage and Administer the Elastic Stack' section includes links for 'Console', 'Index Patterns', 'Monitoring', and 'Rollups'. The bottom of the page shows a snippet of a log entry from 'log-4labs.example'.

Kibana

log-4labs.example/app/kibana#/home?g=0

Home

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add security events

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

Dashboard

Display and share a collection of visualizations

Discover

Interactively explore your data by querying and filtering raw documents

Canvas

Showcase your data in a pixel-perfect way.

Manage and Administer the Elastic Stack

Console

Skip cURL and use this JSON interface to work with your data directly.

Index Patterns

Manage the index patterns that help retrieve your data from Elasticsearch.

Monitoring

Track the real-time health and performance of your Elastic Stack.

Rollups

Summarize and store historical data in a smaller index for future analysis.

log-4labs.example/elastic-stack/elastic-stack/elastic-stack

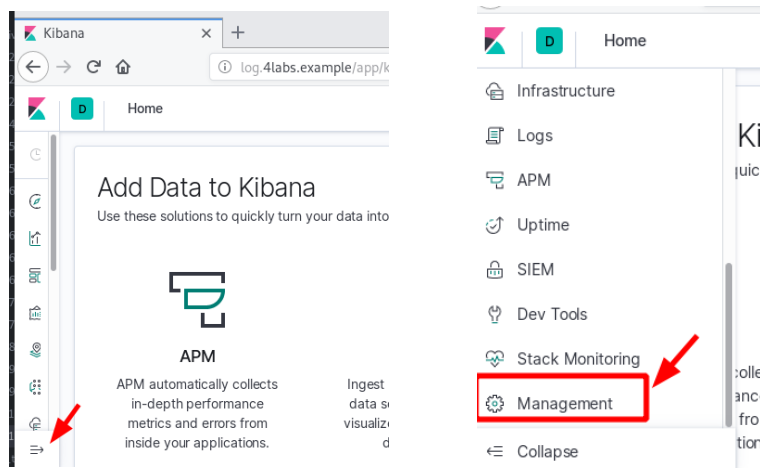
Anotações

[illegible]

- ## Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

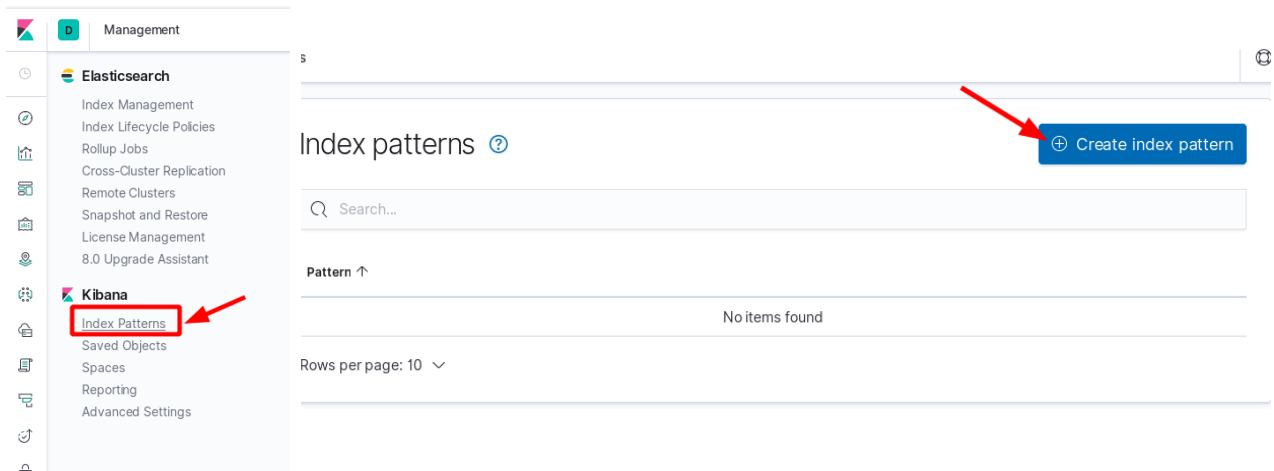
Primeiramente, precisamos configurar os padrões de índices. Clique no ícone para expandir o menu e depois clique em **Management**.



Anotações

[illegible]

Clique em **Index Patterns** e depois em **Create Index Patterns**.



Anotações

[illegible]

Preencha o Index Pattern com o valor **metricbeat*** e clique em **Next Step**.

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ ☒ Include system indices

Step 1 of 2: Define index pattern

Index pattern

metricbeat*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ **Success!** Your index pattern matches **2 indices**.

metricbeat-2019.09.01

metricbeat-2019.09.02

> Next step

Anotações

[illegible]

Selecione no dropdown o parâmetro **@timestamp** e clique em **Create index pattern**.

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ Include system indices

Step 2 of 2: Configure settings

You've defined **metricbeat*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name Refresh

@timestamp

The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range.
















> Show advanced options

[← Back](#)

Create index pattern

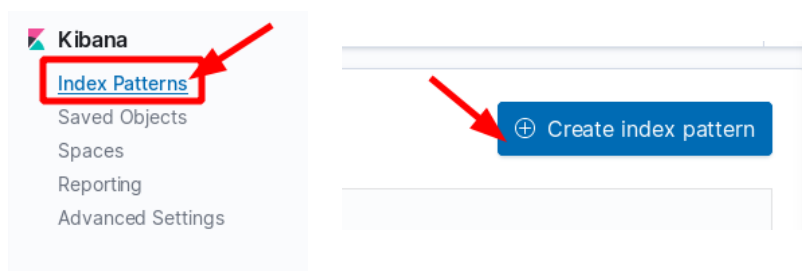
Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp 	date				
@version	string				
@version.keyword	string				
_id	string				
_index	string				

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Repita os passos para adicionar um novo índice para o filebeat.



Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Preencha o campo Index Pattern com **filebeat*** e clique em **Next Step**.

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ Include system indices

Step 1 of 2: Define index pattern

Index pattern

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ **Success!** Your index pattern matches **5 indices**.

[Next step](#)

filebeat-2019.08.28

Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Selecione no dropdown o parâmetro **@timestamp** e clique em **Create index pattern**.

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☐ ☒ Include system indices

Step 2 of 2: Configure settings

You've defined **filebeat*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name Refresh

@timestamp

The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

> Show advanced options

[← Back](#)

Create index pattern

Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

filebeat*

Time Filter field name: @timestamp









Fields (65)

Scripted fields (0)

Source filters (0)

Filter

All field types ▾

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp 	date				
@version	string				
@version.keyword	string				
._id	string				

Anotações

★ metricbeat*
★
↺
🗑️

Time Filter field name: @timestamp
Default

This page lists every field in the **metricbeat*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#) 🔗

Fields (2549)
Scripted fields (0)
Source filters (0)

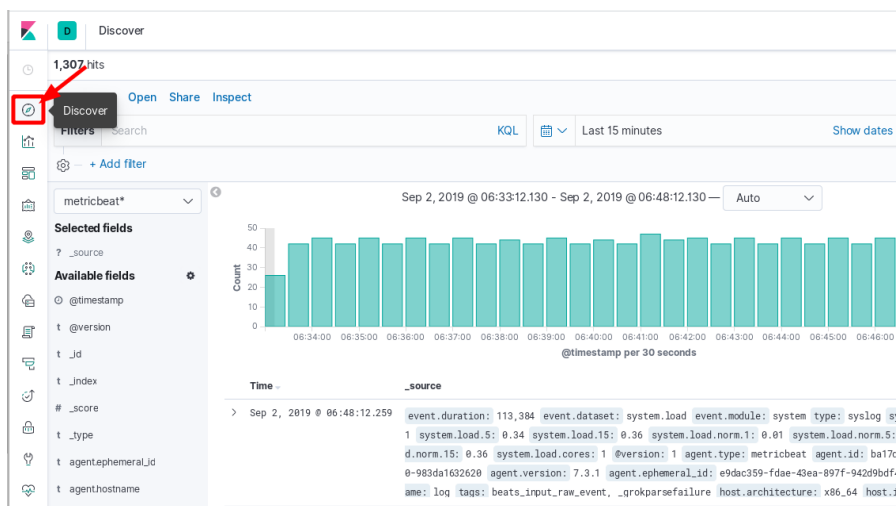
All field types ▼

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp 🕒	date		●	●	
@version	string		●		
@version.keyword	string		●	●	
_id	string		●	●	
_index	string		●	●	

Anotações

[illegible]

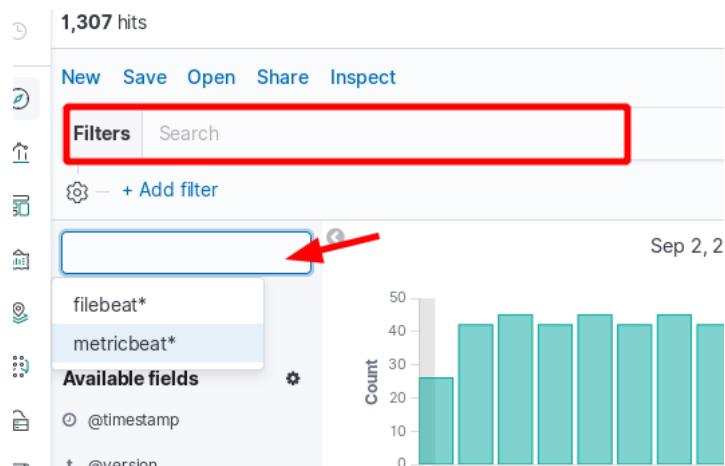
Para visualizar os dados no Kibana, basta clicar no ícone de **Discovery** e será exibida uma tela com os Index patterns e seus dados.



Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Através desta tela, podemos listar os dados por Index Pattern ou até mesmo efetuar seleções e filtros.



Anotações

[illegible]

0 hits

New

Save

Open

Share

Inspect

Filters

Search

KQL

⚙️

+ Add filter

filebeat*

⌵

Selected fields

? _source

Available fields

⚙️

@timestamp

@version

_id

_index

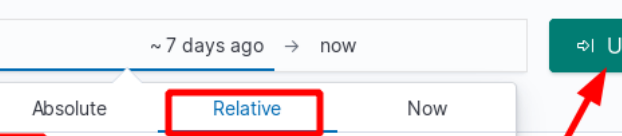
No results match your search criteria

Expand your time range

One or more of the indices you're looking at contains data or there may not be any data at all in the currently selected time range.

Anotações

[illegible]



The screenshot shows the Kibana 'Discover' interface. At the top, there's a date range filter set to '~ 7 days ago → now'. Below this, a dropdown menu is open, showing 'Absolute' and 'Relative' options. The 'Relative' option is selected and highlighted with a red box. Under 'Relative', there's a field with the number '7' (highlighted with a red box) and a unit dropdown set to 'Days ago' (also highlighted with a red box). To the right of the filter, there's a green 'Update' button with a red arrow pointing to it. The main table area shows a single row with a date 'Aug 26, 2019 @ 06:52:39.532'.

Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

NewSaveOpenShareInspect

FiltersSearch

filebeat*

Selected fields

?_source

Available fields

@timestamp

Count

2,500

2,000

1,500

1,000

500

host.id

host.name

add

Top 5 values in 500 / 500 records

scm

96.8%

compliance

3.2%

host.os.codename

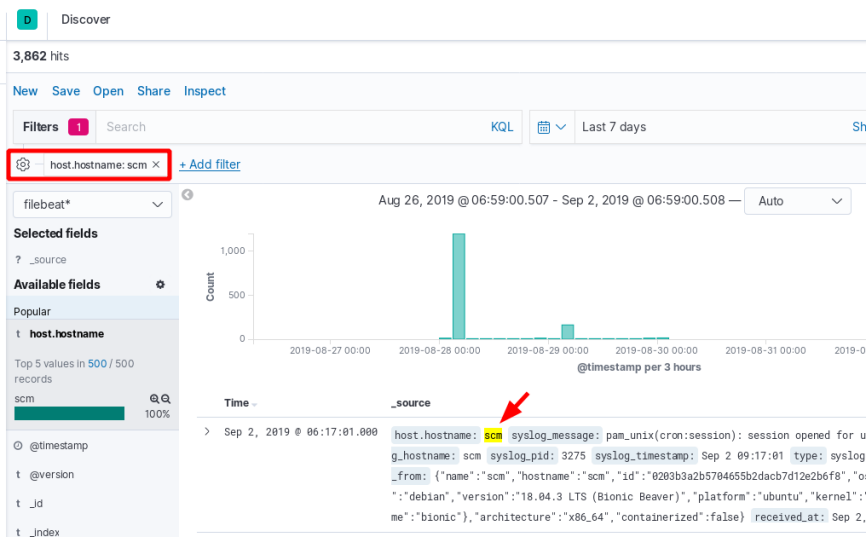
add

host.os.family

Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

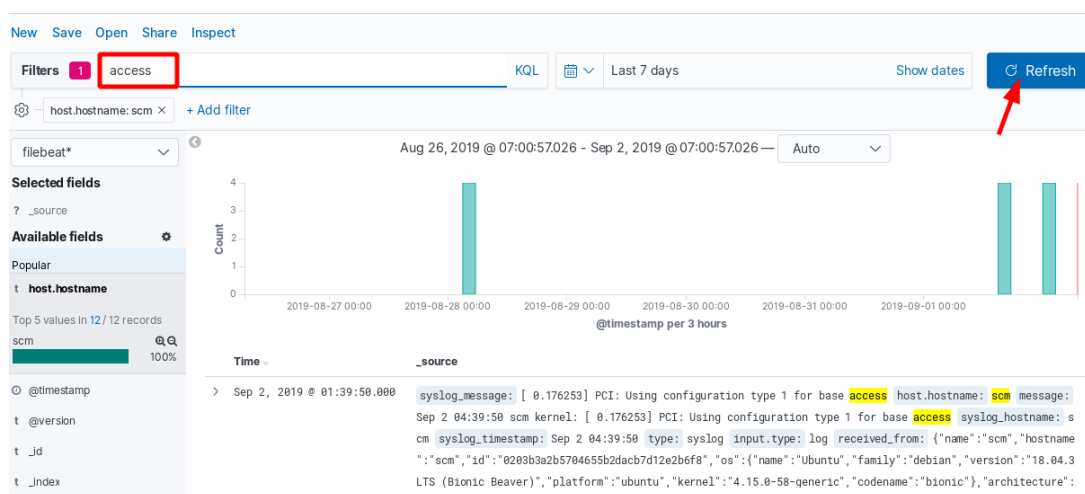
O filtro será adicionado e os campos correspondentes nos logs ficarão realçados.



Anotações

[illegible]

Também, podemos adicionar filtros no campo Filters e clicar em **refresh**. Um filtro composto será montado e suas correspondências serão realçadas.



Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

The left screenshot shows the Kibana search interface. The search bar contains 'metricbeat*'. A filter is applied: 'host.hostname: scm'. The search results show '0 hits'. A message states: 'No results match your search criteria'. The right screenshot shows the same search interface, but the search results show '2,610 hits'. A bar chart is displayed on the right, showing the count of results over time. The chart has a y-axis labeled 'Count' ranging from 0 to 50, and an x-axis showing time intervals from 06:35:00 to 06:40:00. The bars are teal and show a fluctuating count of results.

[illegible]

Anotações

[illegible]

Será exibida uma tela com diversos dashboards, disponíveis em um campo de pesquisa.

Dashboards

Create new dashboard

Search...

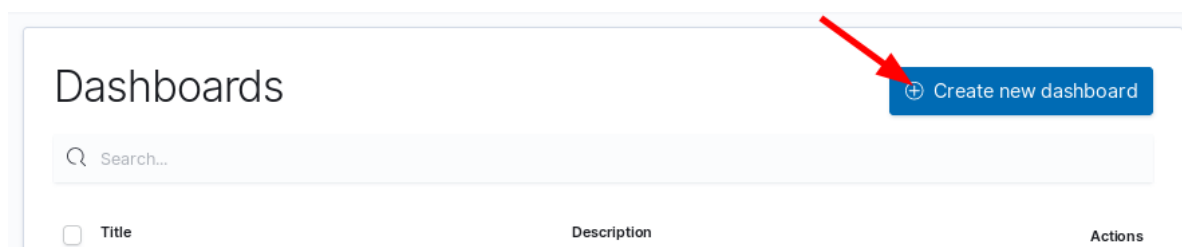
<input type="checkbox"/>	Title	Description	Actions
<input type="checkbox"/>	[Metricbeat AWS] EC2 Overview	Overview of AWS EC2 Metrics	
<input type="checkbox"/>	[Metricbeat AWS] Overview	Overview of AWS Metrics	
<input type="checkbox"/>	[Metricbeat AWS] RDS Overview	Overview of AWS RDS Metrics	
<input type="checkbox"/>	[Metricbeat AWS] S3 Overview	Overview of AWS S3 Metrics	
<input type="checkbox"/>	[Metricbeat AWS] SQS Overview	Overview of AWS SQS Metrics	
<input type="checkbox"/>	[Metricbeat Apache] Overview ECS	Overview of Apache server status	
<input type="checkbox"/>	[Metricbeat CockroachDB] Overview	Overview of the CockroachDB server status	
<input type="checkbox"/>	[Metricbeat Consul] Overview		
<input type="checkbox"/>	[Metricbeat CoreDNS] Overview ECS	Overview of CoreDNS server metrics.	
<input type="checkbox"/>	[Metricbeat Docker] Overview ECS	Overview of docker containers	

Rows per page: 10 < 1 2 3 4 >

Anotações

[illegible]

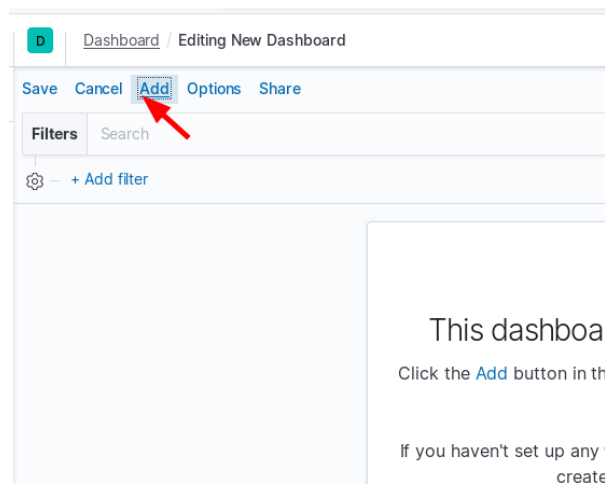
Vamos criar um novo dashboard, clicando no botão **Create new dashboard**.



Anotações

[illegible]

Clique em **Add** para adicionar uma visualização.



Anotações

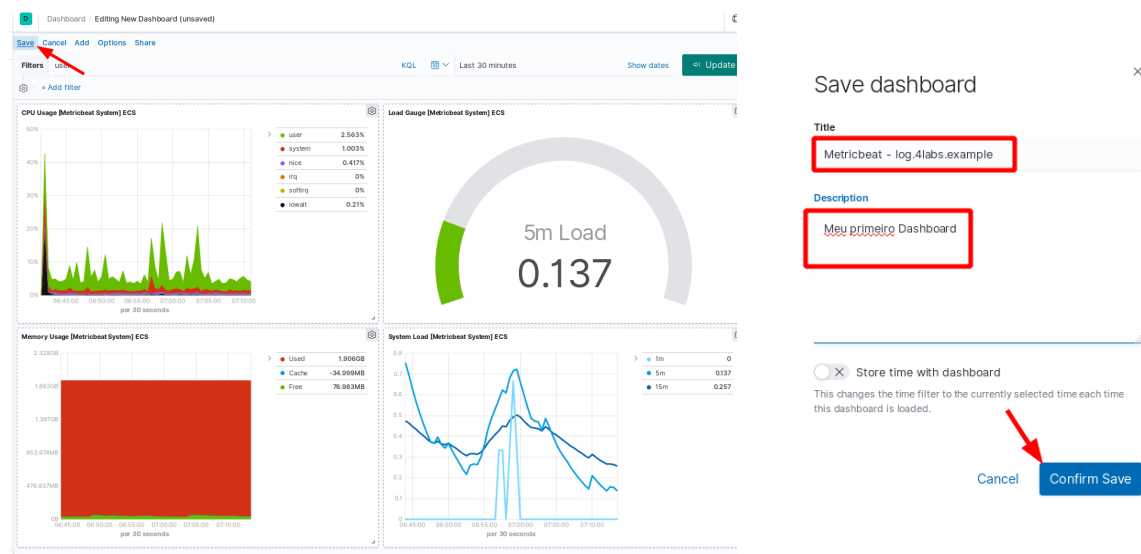
[illegible]

-
- Add panels
- Search: Metricbeat System ECS
- Sort: Types: 3
- System Load [Metricbeat System] ECS
 - System Navigation [Metricbeat System] ECS
 - System [Metricbeat Golang] ECS
 - Packetloss [Metricbeat System] ECS
 - Tip [Metricbeat System] ECS
 - Memory Usage [Metricbeat System] ECS
 - CPU Usage [Metricbeat System] ECS
 - Load Gauge [Metricbeat System] ECS
 - Disk Usage [Metricbeat System] ECS
 - Swap usage [Metricbeat System] ECS
- Rows per page: 10

Anotações

[illegible]

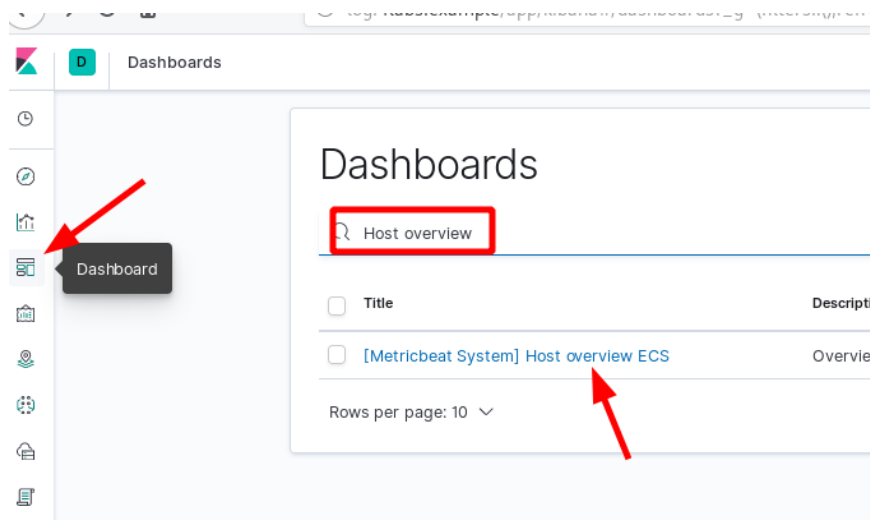
Clique em **Save** para salvar o dashboard e dê um nome ao mesmo.



Anotações

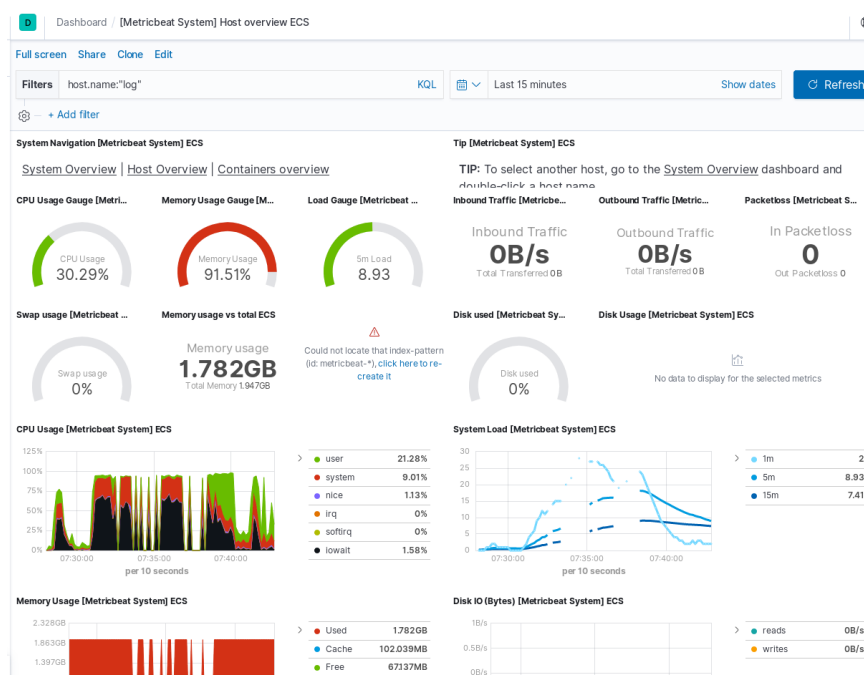
This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Podemos também selecionar um dashboard pronto para utilizar. Basta filtrar e clicar sobre o ícone.

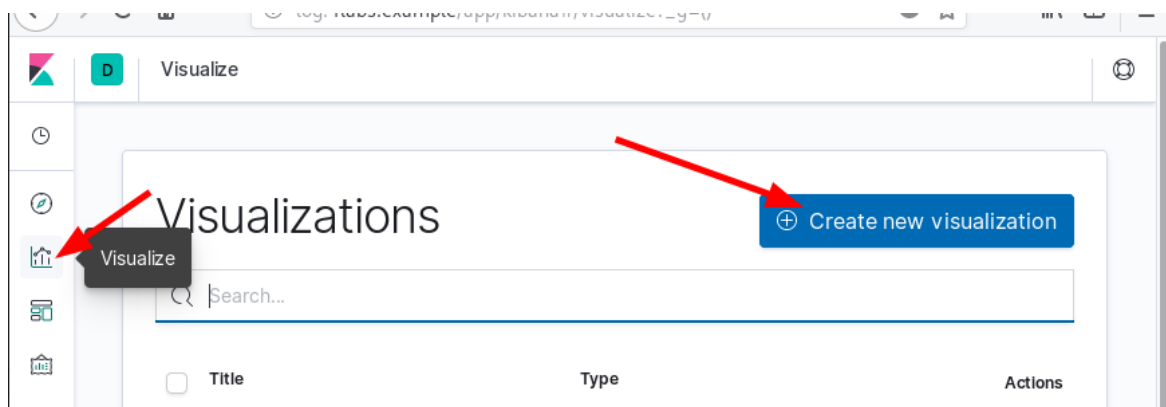


Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



É possível também criar visualizações através do menu **Visualize**.



Anotações

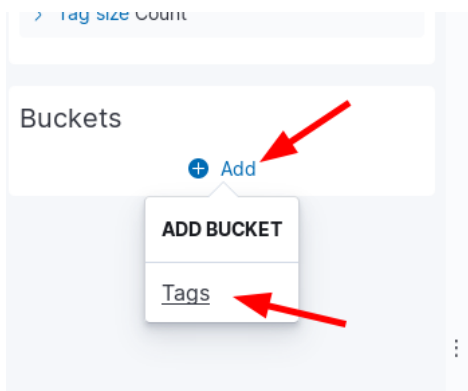
[illegible]

The screenshot shows the 'New Visualization' dialog in Kibana. The 'Tag Cloud' option is highlighted with a red arrow. A secondary window titled 'New Tag Cloud / Choose a source' is shown, displaying a search for 'filebeat*' which is also highlighted with a red arrow.

Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

The screenshot shows the Filebeat configuration interface. At the top, there is a header with a gear icon and the text "+ Add filter". Below this is a dark blue bar with the text "filebeat*". Underneath, there are two tabs: "Data" (selected) and "Options". To the right of the tabs are a play button icon and a close button icon. The main content area is titled "Metrics". Below this title, there is a dropdown menu labeled "Tag size" which is highlighted with a red box. Below the dropdown, there is a section for "Aggregation" with the text "Count help" to its right. The "Count" aggregation is highlighted with a red box. Below the aggregation, there is a "Custom label" field which is empty. At the bottom, there is a link labeled "> Advanced".



This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

filebeat*

Data

Options

<

X

Buckets

▼ Tags

Aggregation

Terms help

Terms

▼

Field

syslog_program.keyword

▼

Order by

Metric: Count

▼

Order

Size

Ascending

▼

10

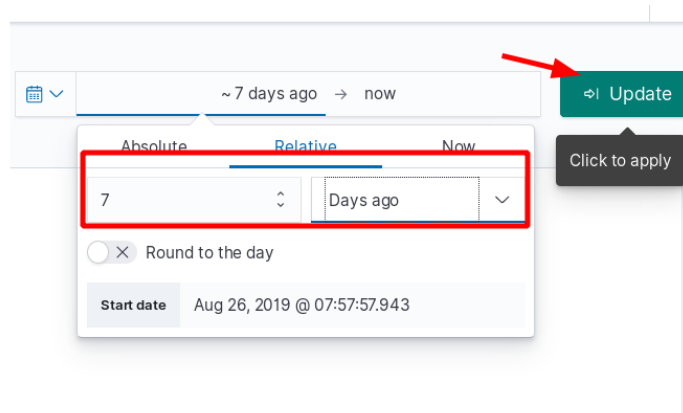
⌵

☐ X Group other values in separate bucket

Anotações


This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Altere a data para **7 days ago** e clique em **Update**.



Anotações

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

A word cloud featuring various Linux services. The word 'kernel' is the largest and most prominent in the center. Other visible words include 'systemd-logind', 'su', 'sudo', 'sshd', 'systemd', and 'CRON', each in different colors and sizes.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

- ## Anotações

[illegible]