

Configurar o Kibana no DNA Center para visualização de logs

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar o Kibana para visualização de logs](#)

[Adicionar campos em Kibana](#)

[Adicionar e editar filtros no Kibana](#)

[Obter logs de uma data específica](#)

[Casos de uso com Lucene](#)

[Obter logs de um serviço específico](#)

[Obter logs que contenham uma palavra específica](#)

[Combine e agrupe sua pesquisa](#)

[Procurar um erro em dois serviços diferentes ao mesmo tempo](#)

[Referência](#)

Introdução

Este documento descreve como usar o Kibana para pesquisar logs específicos entre diferentes serviços do Cisco DNA Center.

Pré-requisitos

Requisitos

Você também deve ter acesso ao Cisco DNA Center através da GUI com FUNÇÃO DE ADMINISTRADOR, você deve estar familiarizado com os nomes e o uso dos serviços do Cisco DNA Center.

Componentes Utilizados

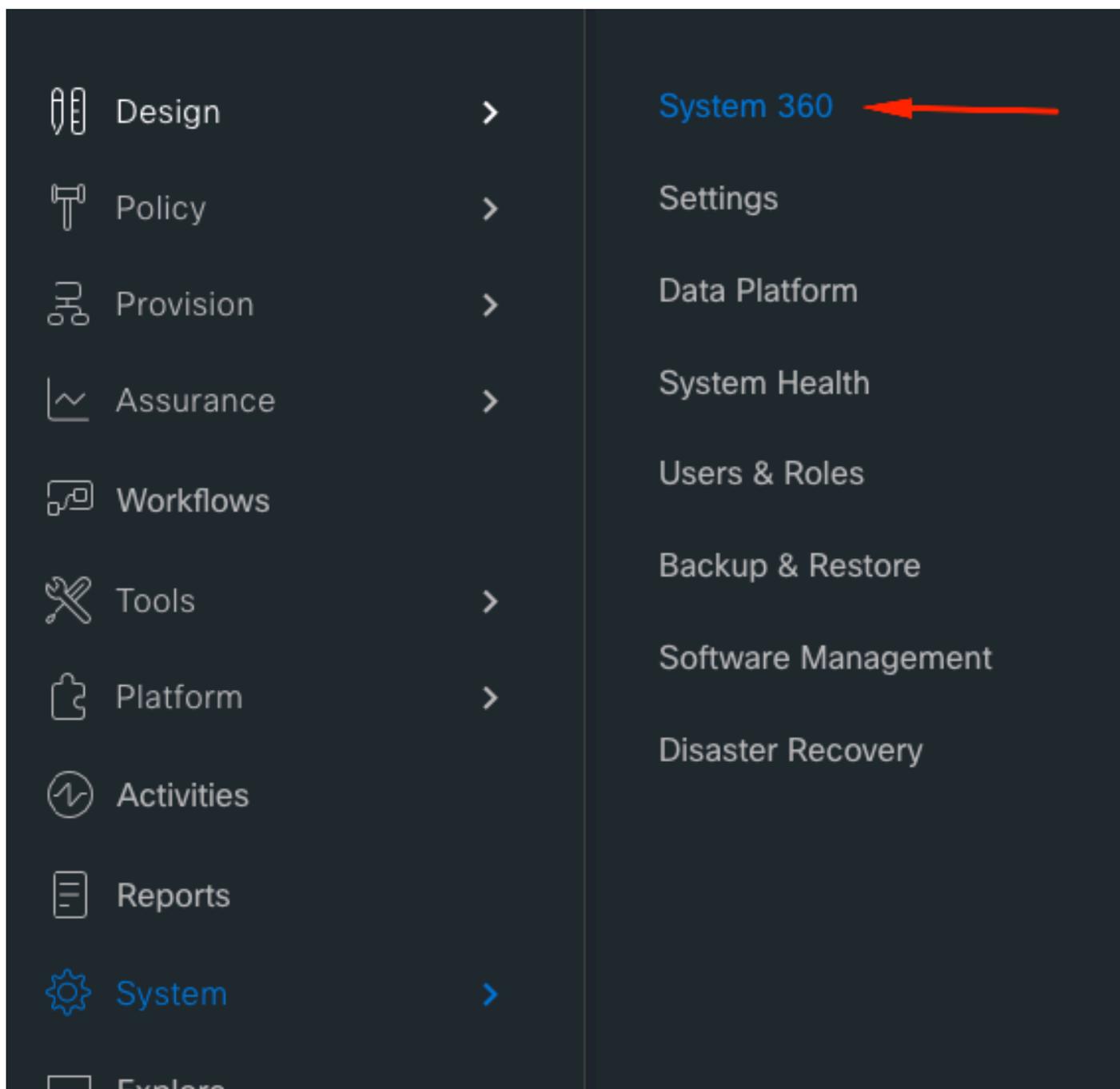
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Kibana é um plugin de visualização de dados de código aberto para Elasticsearch. Ele fornece recursos de visualização sobre o conteúdo indexado em um cluster Elasticsearch que está disponível no Cisco DNA Center.

Você pode acessar o Kibana de duas maneiras:

- <https://<Cisco DNA Center ip>/kibana>
- Menu principal > Sistema > System 360 -> Cluster Tools -> Log Explorer



Cluster Tools

As of Sep 27, 2023 2:42 PM

Monitoring



Log Explorer



Página Web padrão do Kibana

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](#)



Security analytics

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

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data



Dashboard

Display and share a collection of visualizations and saved searches.



Discover

Interactively explore your data by querying and filtering raw documents.



Visualize

Create visualizations and aggregate data stores in your Elasticsearch indices.

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.



Saved Objects

Import, export, and manage your saved searches, visualizations, and dashboards.

Didn't find what you were looking for?

[View full directory of Kibana plugins](#)

Configurar o Kibana para visualização de logs

Navegue até o menu da barra esquerda e clique em Discover:



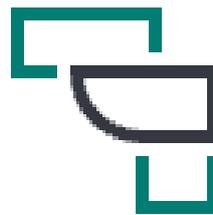
Home



Discover

Add Data to Kibana

Use these solutions to quickly turn your data



APM

APM automatically collects in-

Kibana tem vários campos, que estão destacados na próxima imagem:

Cisco DNA Center

428,100 hits

New Save Open Share Inspect

Filters Search KQL Last 15 minutes Show dates Refresh

logstash-*

Selected fields

Available fields

- @timestamp
- _id
- _index
- _score
- _type
- docker.container_id
- kubernetes.container_...
- kubernetes.container_...
- kubernetes.container_n...
- kubernetes.host
- kubernetes.labels.addon
- kubernetes.labels.contr...
- kubernetes.labels.drEn...
- kubernetes.labels.kube...
- kubernetes.labels.node...
- kubernetes.labels.passi...
- kubernetes.labels.pod-...
- kubernetes.labels.pod-...
- kubernetes.labels.rc-id
- kubernetes.labels.runtl...
- kubernetes.labels.servi...
- kubernetes.labels.state...
- kubernetes.labels.tier

Count

Sep 27, 2023 @ 17:13:58.423 - Sep 27, 2023 @ 17:28:58.423 — Auto

Time

_source

```

> Sep 27, 2023 @ 17:27:48.663 log: 2023-09-27T23:27:48.662+0000 I NETWORK [conn254099] received client metadata from 127.0.0.1:48386
conn254099: { driver: { name: "nodejs", version: "2.2.36" }, os: { type: "Linux", name: "linux", architecture:
"x86_64", version: "5.4.0-139-generic" }, platform: "Node.js v12.16.1, LE, mongodb-core: 2.1.28" } stream: stdout
docker.container_id: 7ef2b92ac566143e8b33be01584ef65e8807ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-aystem kubernetes.pod_name: mongodb-0

> Sep 27, 2023 @ 17:27:48.249 log: 2023-09-27T23:27:48.248+0000 I NETWORK [conn254098] received client metadata from 127.0.0.1:48372
conn254098: { application: { name: "MongoDB Shell" }, driver: { name: "MongoDB Internal Client", version:
"4.2.11" }, os: { type: "Linux", name: "Ubuntu", architecture: "x86_64", version: "16.04" } } stream: stdout
docker.container_id: 7ef2b92ac566143e8b33be01584ef65e8807ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-aystem kubernetes.pod_name: mongodb-0

> Sep 27, 2023 @ 17:27:38.323 log: 2023-09-27T23:27:38.321+0000 I COMMAND [conn4516] command app-hosting.tasks command: find { find: "tasks",
filter: { currentState: { $in: [ "INSTALL_APP_IN_PROGRESS",
"INSTALL_APP_ACTIVATION_PAYLOAD_PREPARATION_IN_PROGRESS", "INSTALL_APP_AWAITING_FUSION_DEVICE_NOTIFICATION",
"INSTALL_APP_DEVICE_DISCOVERY_IN_PROGRESS", "INSTALL_APP_ENABLE_TOX_IN_PROGRESS", "UNINSTALL_APP_IN_PROGRESS",
"STOP_APP_IN_PROGRESS", "START_APP_IN_PROGRESS", "UPGRADE_APP_IN_PROGRESS",

> Sep 27, 2023 @ 17:27:37.565 log: 2023-09-27T23:27:37.564+0000 I NETWORK [conn254095] received client metadata from 10.60.5.239:33128
conn254095: { driver: { name: "PyMongo", version: "3.11.3" }, os: { type: "Linux", name: "Linux", architecture:
"x86_64", version: "5.4.0-139-generic" }, platform: "CPython 3.6.9.final.0" } stream: stdout
docker.container_id: 7ef2b92ac566143e8b33be01584ef65e8807ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-aystem kubernetes.pod_name: mongodb-0

> Sep 27, 2023 @ 17:27:37.476 log: 2023-09-27T23:27:37.475+0000 I NETWORK [conn254091] received client metadata from 10.60.5.239:33882
conn254091: { driver: { name: "PyMongo", version: "3.11.3" }, os: { type: "Linux", name: "Linux", architecture:
"x86_64", version: "5.4.0-139-generic" }, platform: "CPython 3.6.9.final.0" } stream: stdout
docker.container_id: 7ef2b92ac566143e8b33be01584ef65e8807ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-aystem kubernetes.pod_name: mongodb-0

```

Adicionar campos em Kibana

Navegue até Filtros > Campos disponíveis

Os campos que você deve adicionar para visualização de logs são:

- Kubernetes.labels.serviceName - Serviço que exibe o log específico
- Log - Conteúdo bruto do log

Clique no botão Adicionar



Certifique-se de ter a próxima configuração:

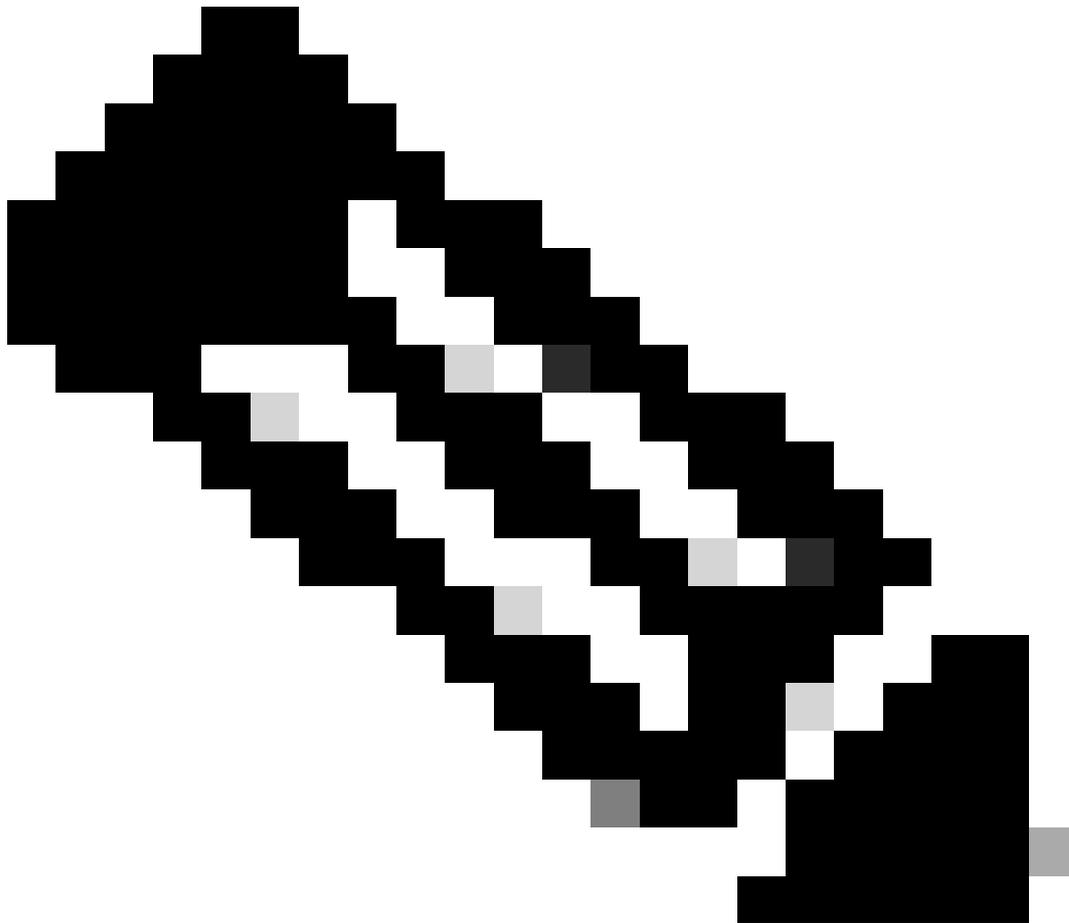
logstash-*



Selected fields

t kubernetes.labels.serviceName

t log



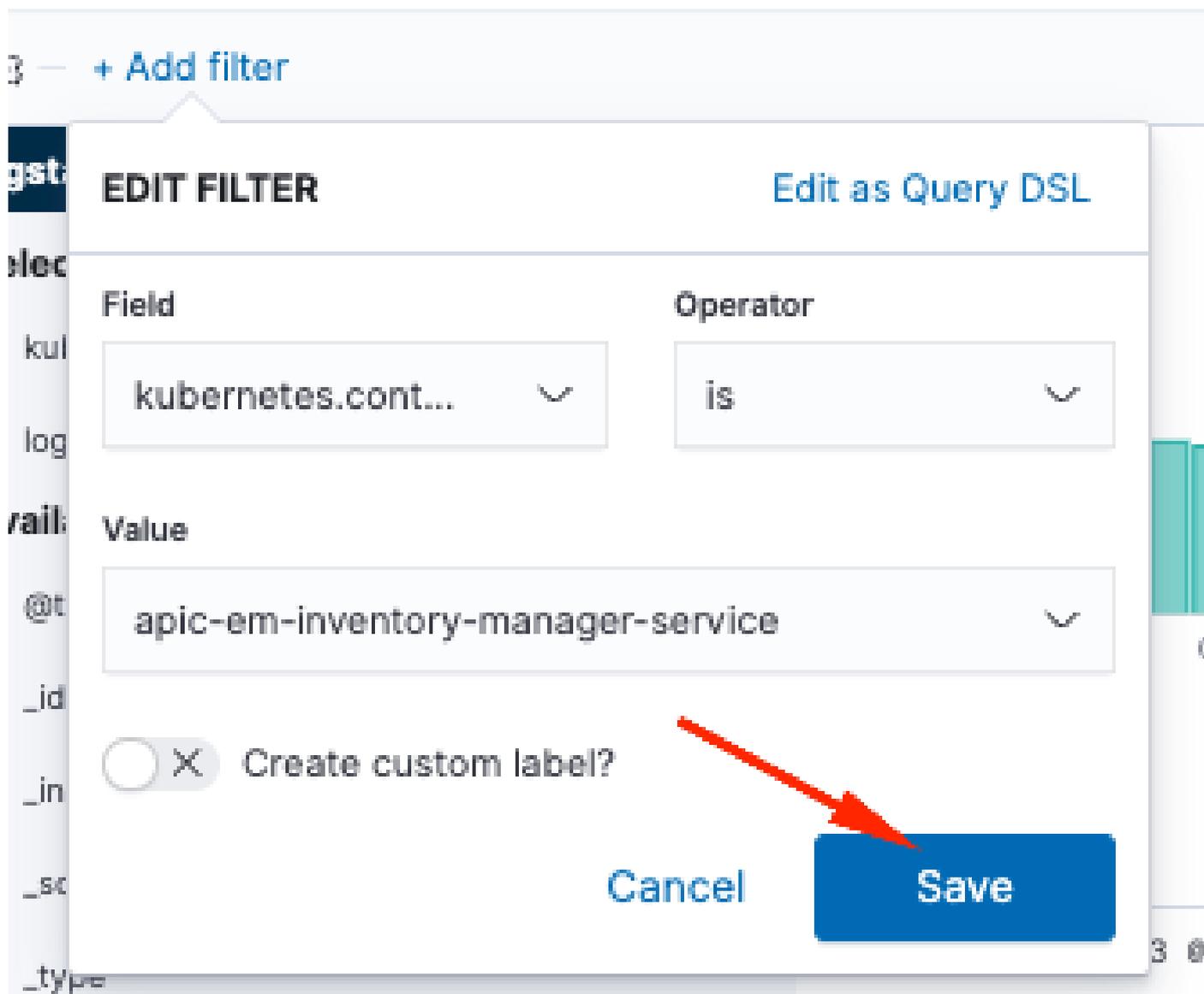
Observação: o campo Hora é adicionado por padrão.

Adicionar e editar filtros no Kibana

Para adicionar um filtro, execute a próxima atividade:

- Clique em Adicionar filtro
- Seleção de campo: Kubernetes.labels.serviceName
- Operador select: is
- Valor: selecione o serviço de seu interesse
- Clique no botão Salvar

Examine o próximo exemplo onde o serviço selecionado é apic-em-inventory-manager-service:



The screenshot shows the 'EDIT FILTER' dialog in Kibana. At the top left, there is a '+ Add filter' button. The dialog has a title bar with 'EDIT FILTER' and a link to 'Edit as Query DSL'. Below the title bar, there are three main sections: 'Field', 'Operator', and 'Value'. The 'Field' section has a dropdown menu showing 'kubernetes.cont...'. The 'Operator' section has a dropdown menu showing 'is'. The 'Value' section has a text input field containing 'apic-em-inventory-manager-service'. Below these sections, there is a toggle switch for 'Create custom label?' which is currently turned off. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Save'. A red arrow points to the 'Save' button.

Você pode adicionar mais filtros conforme necessário.

No próximo exemplo, um novo filtro foi adicionado, onde o erro Field:log, operator:is e Value:

EDIT FILTER Edit as Query DSL

Field log **Operator** is

Value error

X Create custom label?

Cancel Save

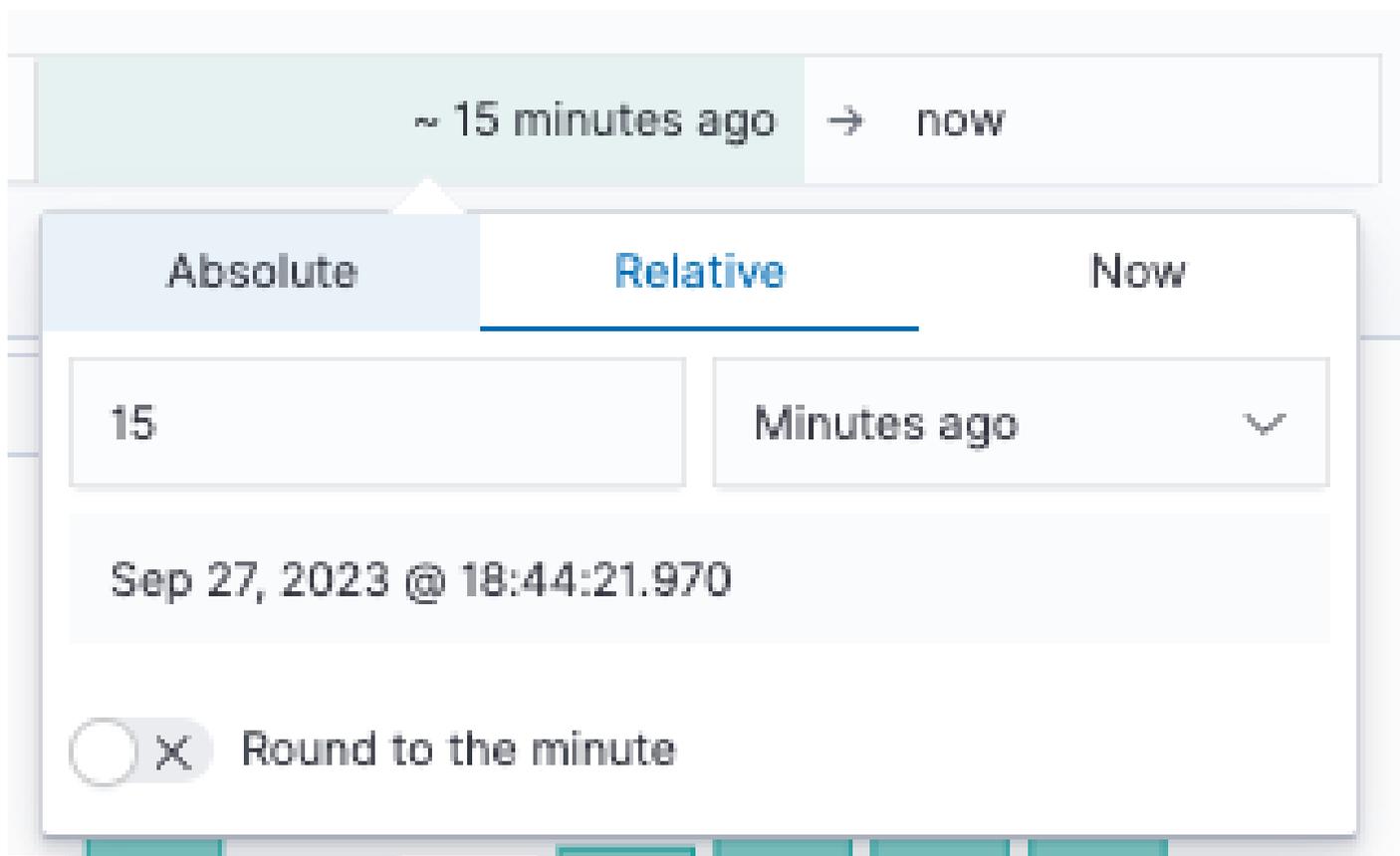
Obter logs de uma data específica

Você pode adicionar um elemento de tempo aos seus critérios de pesquisa.

KQL 📅 ~ 15 minutes ago → now

03 — Auto

Use uma das próximas opções do campo Intervalo de tempo:



- Absoluto - De uma data específica para outra.
- Relativo - Dos últimos X minutos, horas, dias ou semanas até uma data específica.
- Agora - Definir o horário como "agora" significa que, em cada atualização, esse horário será definido como o horário da atualização.

Casos de uso com Lucene

Lucene é uma biblioteca de mecanismo de pesquisa de texto completo de alto desempenho. É uma tecnologia adequada para praticamente qualquer aplicativo que exija pesquisa de texto completo.

Navegue para a barra de pesquisa e desative o KQL para ativar o Lucene:

SYNTAX OPTIONS

The [Kibana Query Language](#) (KQL) offers a simplified query syntax and support for scripted fields. KQL also provides autocomplete if you have a Basic license or above. If you turn off KQL, Kibana uses Lucene.

Kibana Query Language



Obter logs de um serviço específico

Digite a próxima consulta na barra de filtros e pressione o botão Atualizar

```
kubernetes.labels.serviceName:<service-name>
```

Dê uma olhada no próximo exemplo com task-service:

```
kubernetes.labels.serviceName:task-service
```


Available fields



Aggregatable

Searchable

Type

Field name

Hide missing fields

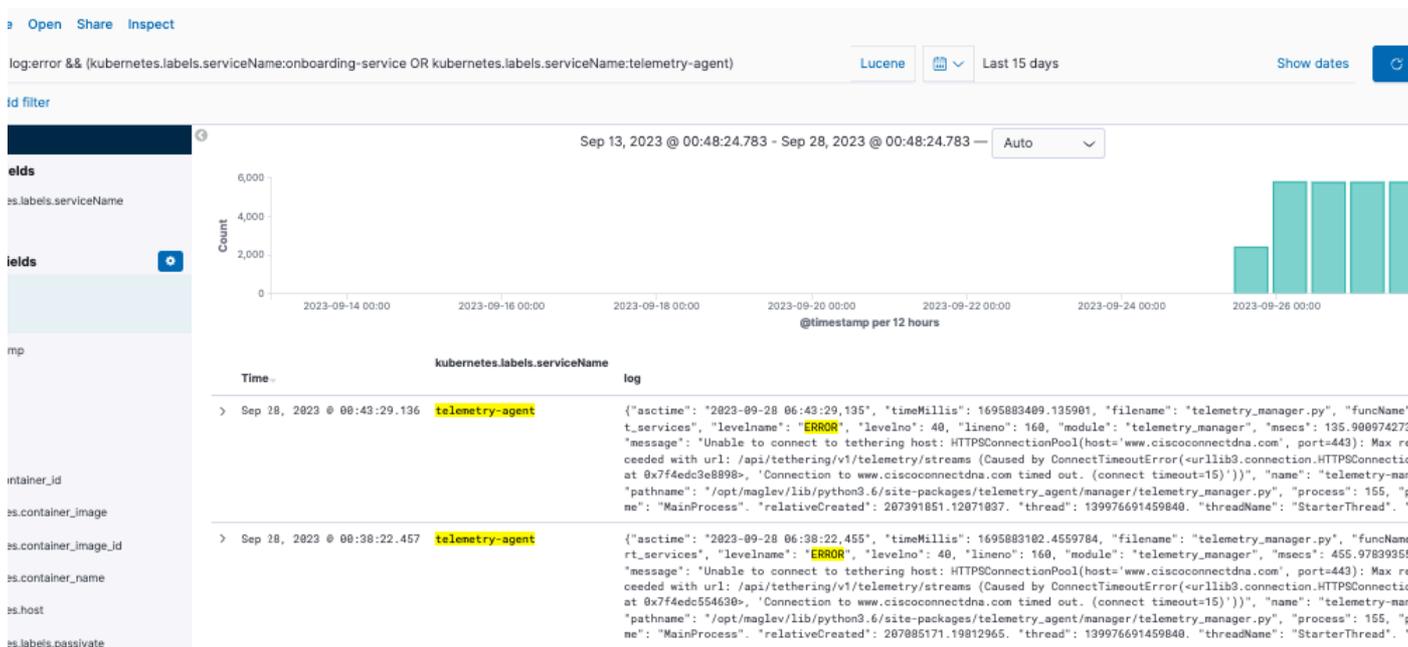
[Reset filters](#)

Procurar um erro em dois serviços diferentes ao mesmo tempo

Inclua dois ou mais serviços em seus critérios de pesquisa. Certifique-se de que os nomes dos

serviços sejam inseridos entre parênteses e separe-os com OR.

log:error && (kubernetes.labels.serviceName:onboarding-service OR kubernetes.labels.serviceName:telemet



Referência

- [Opções comuns de pesquisa elástica](#)
- [Apache Lucene - Sintaxe do Analisador de Consulta](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.