

# 在DNA Center中配置Kibana以实现日志可视化

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置Kibana以实现日志可视化](#)

[在Kibana中添加字段](#)

[在Kibana中添加和编辑过滤器](#)

[从特定日期获取日志](#)

[Lucene使用案例](#)

[获取特定服务的日志](#)

[获取包含特定单词的日志](#)

[混合并匹配您的搜索](#)

[同时搜索两个不同的服务以查找错误](#)

[参考](#)

---

## 简介

本文档介绍如何使用Kibana在不同的Cisco DNA Center服务中搜索特定日志。

## 先决条件

### 要求

您必须具有管理员角色的GUI才能访问Cisco DNA Center。您还必须熟悉Cisco DNA Center服务的名称和用途。

### 使用的组件

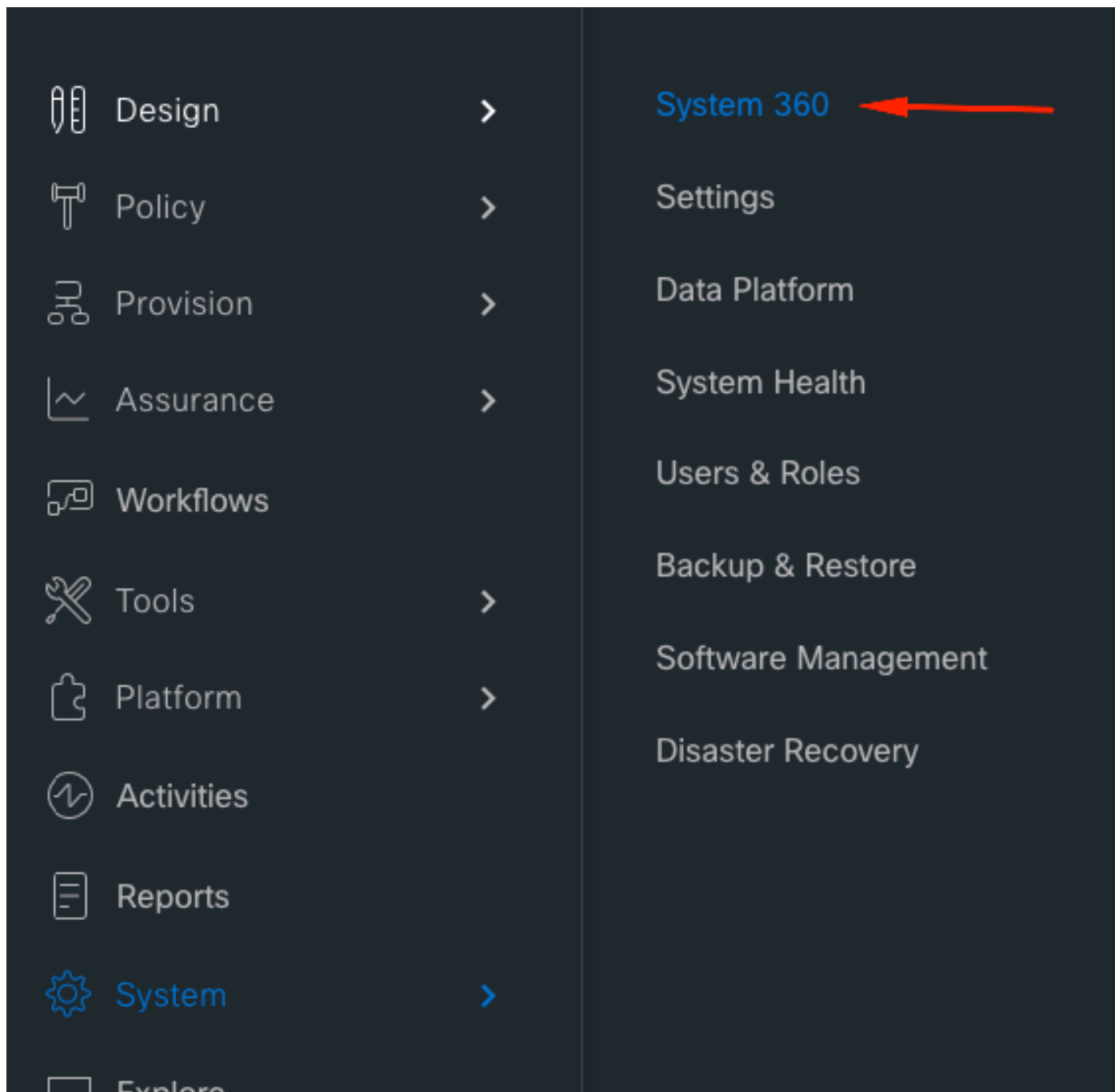
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

Kibana是Elasticsearch的开源数据可视化插件。它在Cisco DNA Center提供的Elasticsearch群集上索引的内容之上提供可视化功能。

您可以通过两种方式访问Kibana：

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



# Cluster Tools

As of Sep 27, 2023 2:42 PM

Monitoring



Log Explorer



默认Kibana网页

The screenshot displays the Cisco DNA Center interface with a sidebar on the left containing navigation icons. The main content area is titled "Add Data to Kibana" and includes a sub-header: "Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems." Below this, there are four primary options, each with an icon, a title, a description, and a button:

- APM**: APM automatically collects in-depth performance metrics and errors from inside your applications. Button: [Add APM](#)
- Logging**: Ingest logs from popular data sources and easily visualize in preconfigured dashboards. Button: [Add log data](#)
- Metrics**: Collect metrics from the operating system and services running on your servers. Button: [Add metric data](#)
- Security analytics**: Centralize security events for interactive investigation in ready-to-go visualizations. Button: [Add security events](#)

Below these options are two additional sections:

- Add sample data**: Load a data set and a Kibana dashboard
- Use Elasticsearch data**: Connect to your Elasticsearch index

The interface is divided into two main columns for further actions:

- 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.

At the bottom, there is a search prompt: "Didn't find what you were looking for?" with a button: [View full directory of Kibana plugins](#)

## 配置Kibana以实现日志可视化

导航到左侧栏菜单并单击Discover：



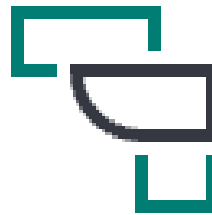
Home



Discover

# Add Data to Kibana

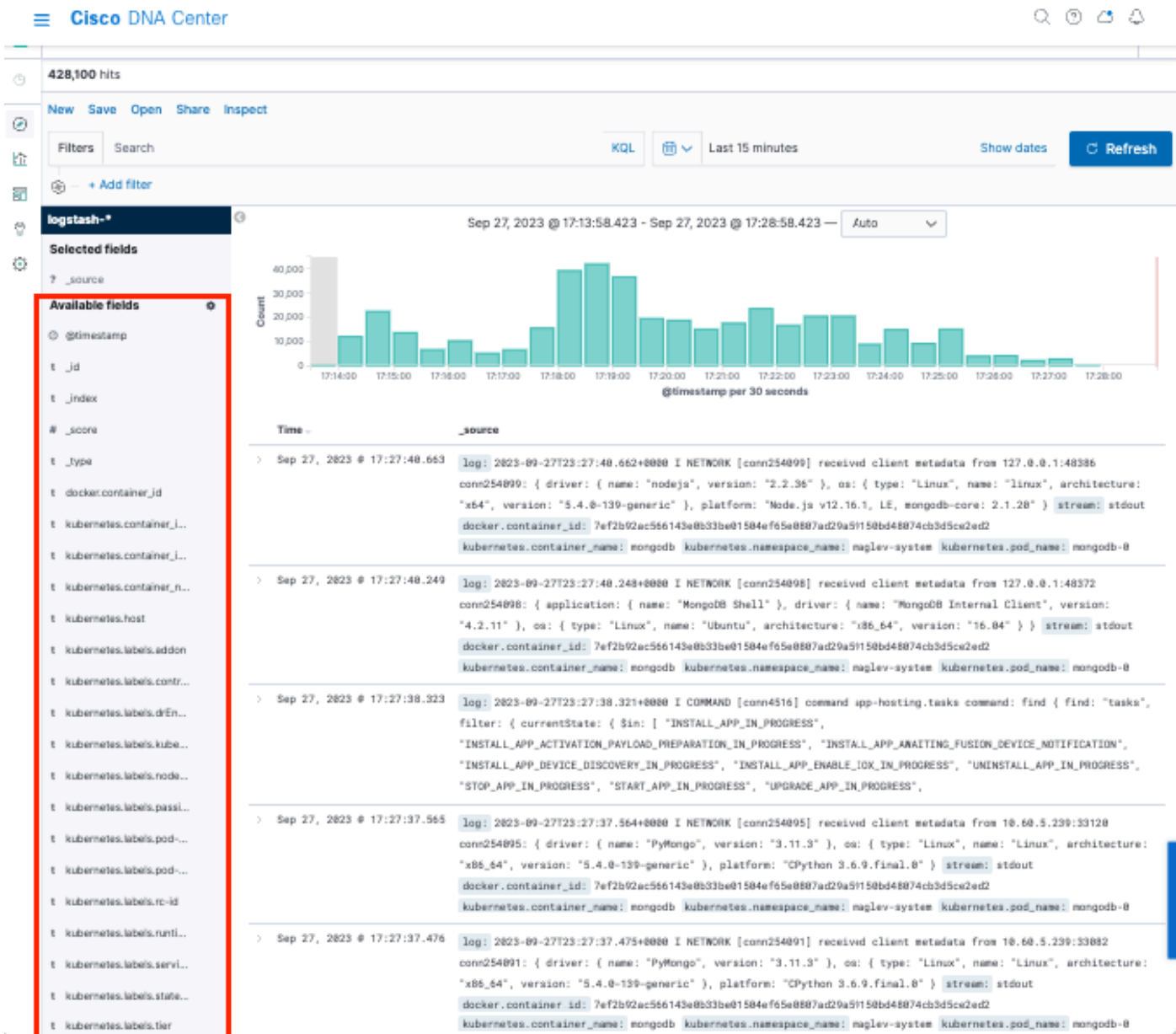
Use these solutions to quickly turn your data



APM

APM automatically collects in-

Kibana有几个字段，这些字段在下一张图中突出显示：



## 在Kibana中添加字段

导航到过滤器>可用字段

为日志可视化而必须添加的字段包括：

- Kubernetes.labels.serviceName -显示特定日志的服务
- Log —日志的原始内容

点击add按钮



确保您具有下一个配置：

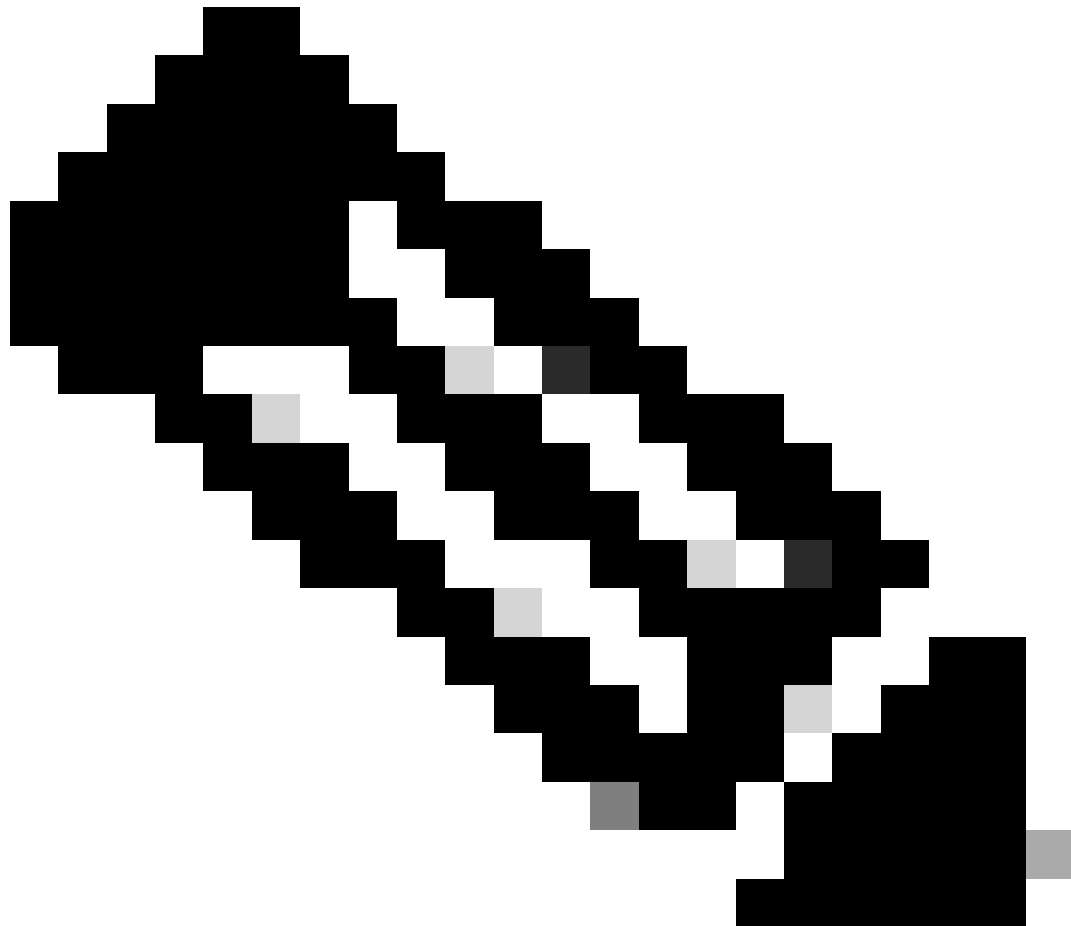
logstash-\*



## Selected fields

t kubernetes.labels.serviceName

t log



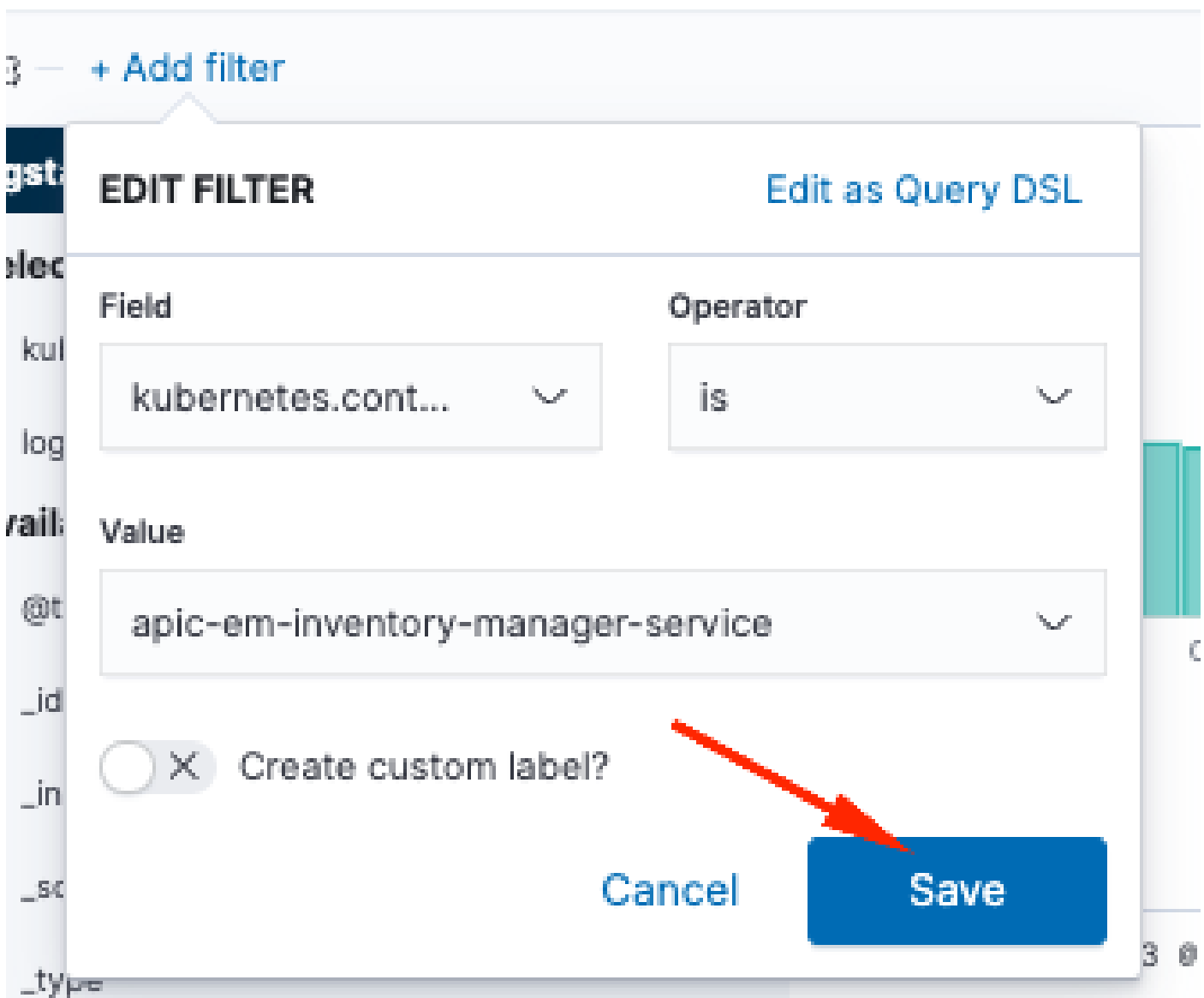
注意：默认情况下会添加时间字段。

## 在Kibana中添加和编辑过滤器

要添加过滤器，请执行以下活动：

- 点击添加过滤器
- 字段选择：Kubernetes.labels.serviceName
- 操作员选择：是
- 价值：选择您感兴趣的服务
- 点击保存按钮

请看下一个示例，其中所选服务为apic-em-inventory-manager-service：



The screenshot shows the 'EDIT FILTER' dialog in Kibana. The dialog has a title bar with 'EDIT FILTER' and 'Edit as Query DSL'. Below the title bar, there are two columns: 'Field' and 'Operator'. The 'Field' dropdown is set to 'kubernetes.cont...' and the 'Operator' dropdown is set to 'is'. Below these, there is a 'Value' dropdown set to 'apic-em-inventory-manager-service'. At the bottom left, there is a toggle switch for 'Create custom label?' which is currently turned off. At the bottom right, there are two buttons: 'Cancel' and 'Save'. A red arrow points to the 'Save' button.

您可以根据需要添加更多过滤器。

下一个示例添加了一个新的过滤器，其中Field：log、operator：is和Value：error：



**EDIT FILTER** Edit as Query DSL

---

**Field** log **Operator** is

**Value** error

X Create custom label?

Cancel Save

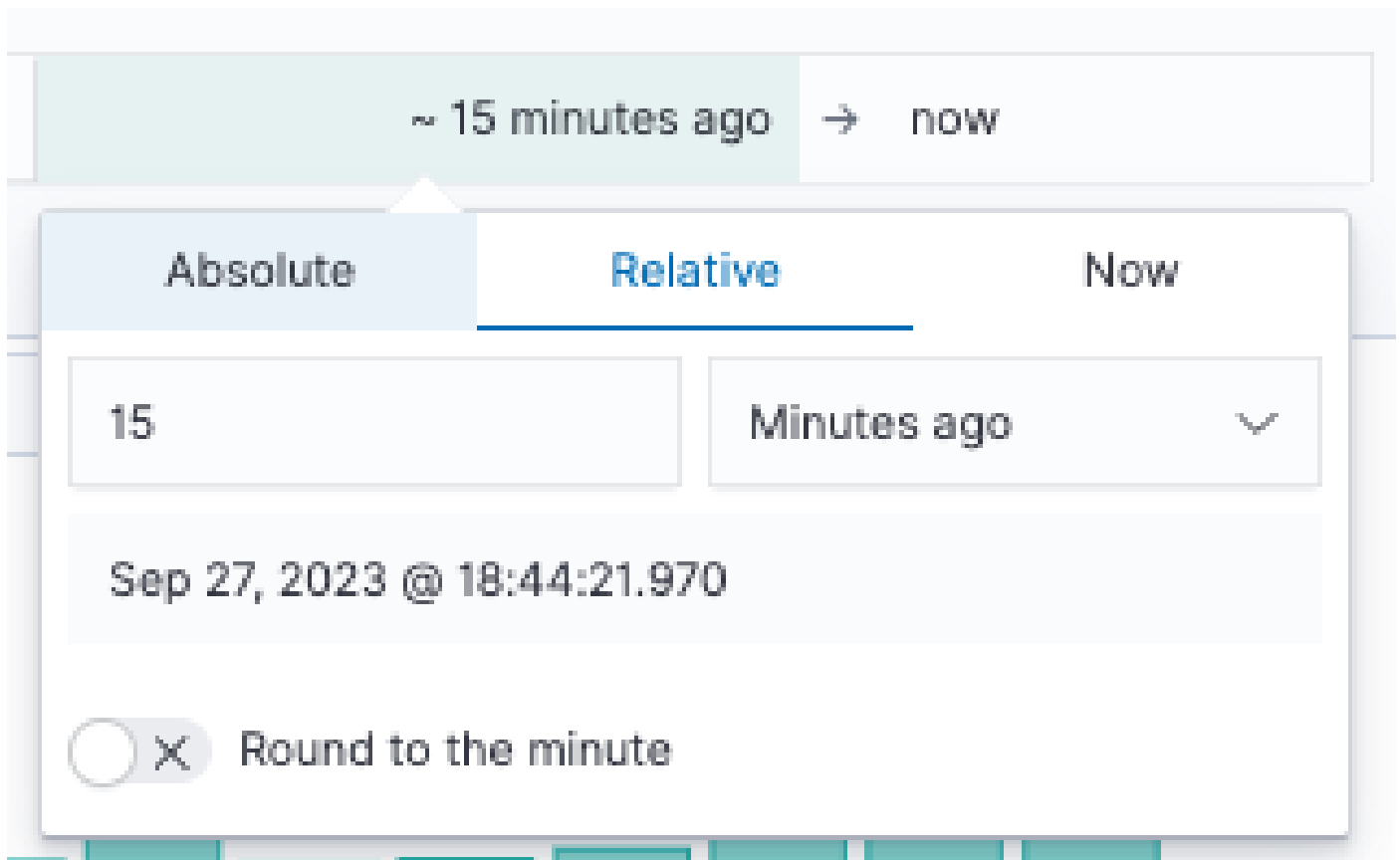
### 从特定日期获取日志

可以将时间元素添加到搜索条件。

KQL 📅 ~ 15 minutes ago → now

03 — Auto

使用时间 Range 字段中的以下选项之一：



- 绝对- 从特定日期到另一个特定日期。
- Relative -从最近X分钟、小时、天或周到某个特定日期。
- Now -将时间设置为“now”，意味着在每次刷新时，此时间都将设置为刷新时间。

## Lucene使用案例

Lucene是一个高性能、全功能的文本搜索引擎库。该技术几乎适用于任何需要全文搜索的应用程序。

导航到搜索栏并禁用KQL以启用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



获取特定服务的日志

在过滤器栏中键入下一个查询，然后按刷新按钮

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

接下来我们来看一个任务服务示例：

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



# 混合并匹配您的搜索

您可以在字符串之间使用AND ( 或&& ) 来搜索与字符串组合匹配的条目。

<#root>

log:error

AND

kubernetes.labels.serviceName:onboarding-service

The screenshot shows a search interface with the following components:

- Search Bar:** Contains the query `log:error AND kubernetes.labels.serviceName:task-service`. Buttons for `Open`, `Share`, and `Inspect` are visible.
- Filters:** Includes `Lucene`, a dropdown menu, `Last 15 minutes`, and `Show dates`.
- Id filter:** A sidebar on the left lists fields such as `els`, `ks.labels.serviceName`, `ields`, `mp`, `ntainer_id`, `bs.container_image`, `bs.container_image_id`, `bs.container_name`, and `bs.host`.
- Bar Chart:** A chart titled `Count` showing a single bar at `00:12:00` with a count of 2. The x-axis is labeled `@timestamp per 30 seconds`.
- Log Table:** A table with columns `Time`, `kubernetes.labels.serviceName`, and `log`. It contains two entries for `task-service` at `2023-09-28 06:12:13.823`. The first entry is an `ERROR` message, and the second is a `WARN` message.

注意：并非所有字段都可搜索。

如果您希望在Available Fields窗格中仅看到可搜索的字段，请选择齿轮并自定义视图。您还可以定义要使用的搜索类型，例如字符串、布尔值、数字等。

## Available fields



### Aggregatable

### Searchable

### Type

### Field name

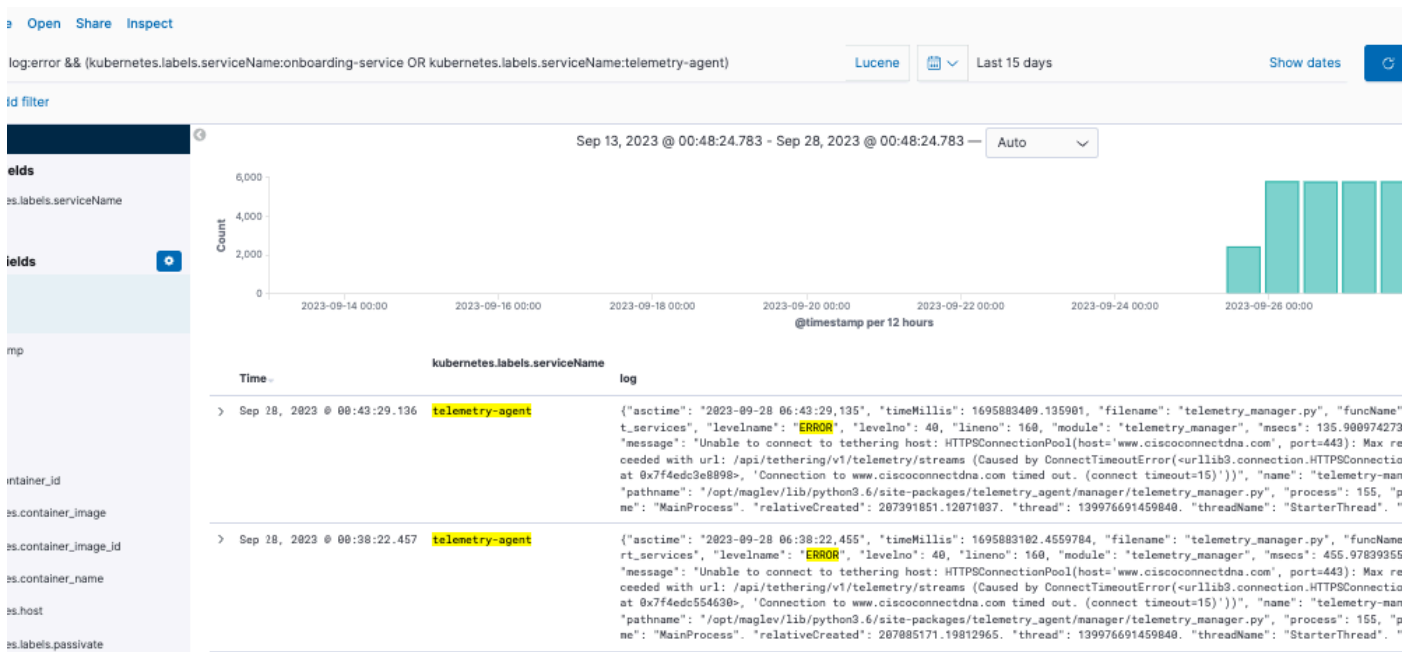
Hide missing fields

[Reset filters](#)

同时搜索两个不同的服务以查找错误

在搜索条件中包含两个或多个服务。确保服务名称在括号中输入，用OR分隔开。

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



## 参考

- [弹性搜索常用选项](#)
- [Apache Lucene - 查询解析器语法](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。