

# 在DNA中心中配置Kibana以進行日誌視覺化

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[配置Kibana以進行日誌視覺化](#)

[在Kibana中增加欄位](#)

[在Kibana中增加和編輯篩選器](#)

[獲取特定日期的日誌](#)

[Lucene使用案例](#)

[獲取特定服務的日誌](#)

[取得包含特定字的記錄](#)

[混合併匹配您的搜尋](#)

[同時搜尋兩個不同的服務以找出錯誤](#)

[參考](#)

---

## 簡介

本文檔介紹如何使用Kibana在不同的Cisco DNA Center服務中搜尋特定日誌。

## 必要條件

### 需求

您必須透過GUI具有管理員角色才能訪問Cisco DNA Center，還必須熟悉Cisco DNA Center服務的名稱和用途。

### 採用元件

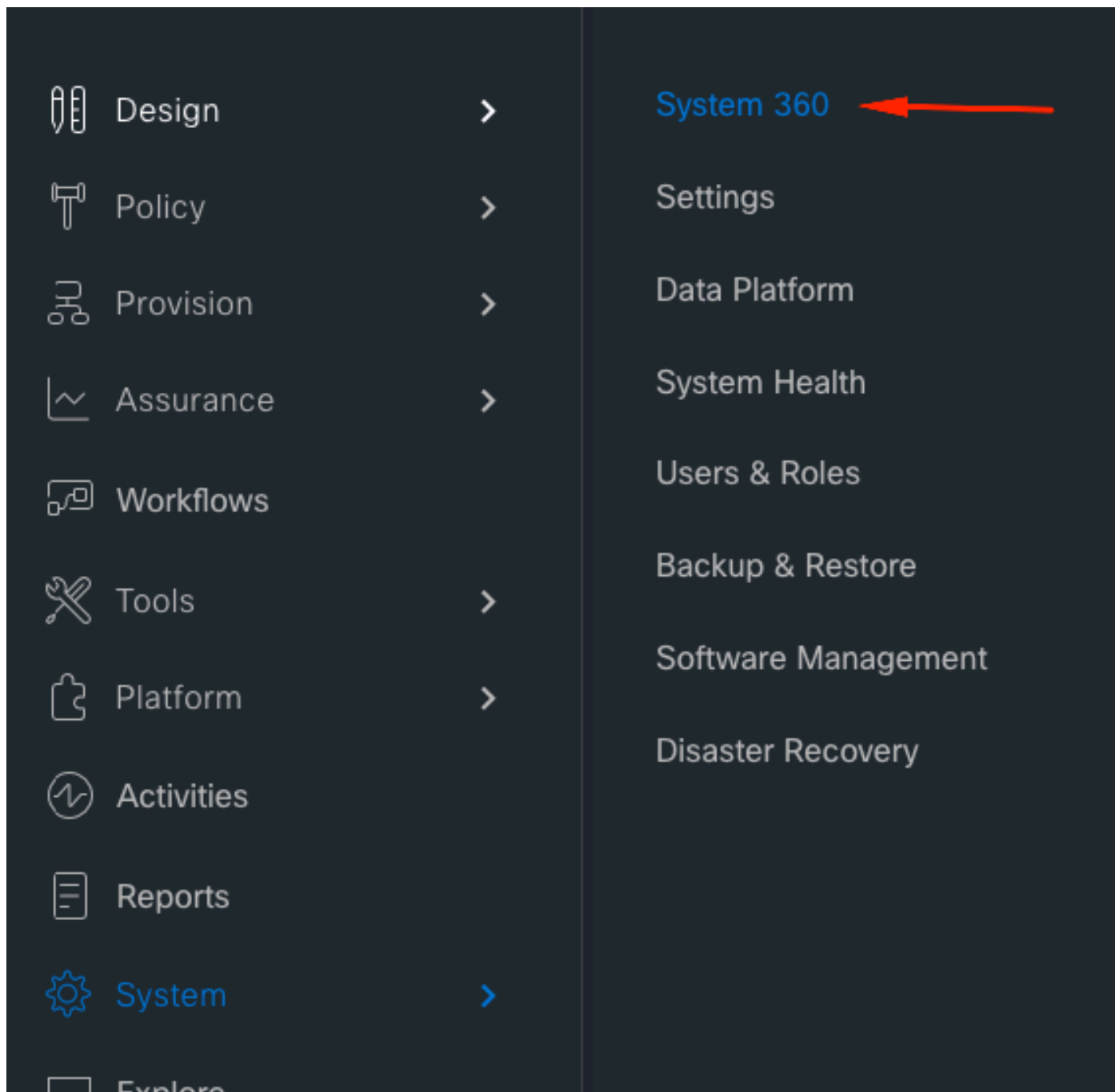
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

Kibana是Elasticsearch的開源資料視覺化外掛。它在Cisco DNA Center中可用的Elasticsearch群集上的索引內容之上提供視覺化功能。

您可以使用兩種方式存取Kibana：

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



# Cluster Tools

As of Sep 27, 2023 2:42 PM

Monitoring



Log Explorer




預設Kibana網頁

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](#)

## 配置Kibana以進行日誌視覺化

導航到左側欄選單，然後點選Discover：



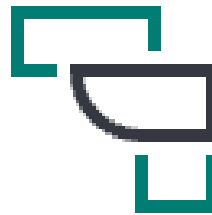
Home



Discover

# Add Data to Kibana

Use these solutions to quickly turn your data



APM

APM automatically collects in-

Kibana有數個欄位，這些欄位會在下一個影像中反白：

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\_l...
- kubernetes.container\_l...
- 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:
"x64", version: "5.4.0-139-generic" }, platform: "Node.js v12.16.1, LE, mongodb-core: 2.1.28" } stream: stdout
docker.container_id: 7ef2b92ac566143e8b33be01584ef65e887ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-system 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: 7ef2b92ac566143e8b33be01584ef65e887ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-system 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: 7ef2b92ac566143e8b33be01584ef65e887ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-system 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: 7ef2b92ac566143e8b33be01584ef65e887ad29a5f158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-system kubernetes.pod_name: mongodb-0

```

在Kibana中增加欄位

導航到過濾器>可用欄位

您必須為日誌視覺化新增的欄位包括：

- Kubernetes.labels.serviceName -顯示特定日誌的服務
- Log -日誌的原始內容

按一下「新增」按鈕

kubernetes.labels.serviceName **add**

確保您具有下一個配置：

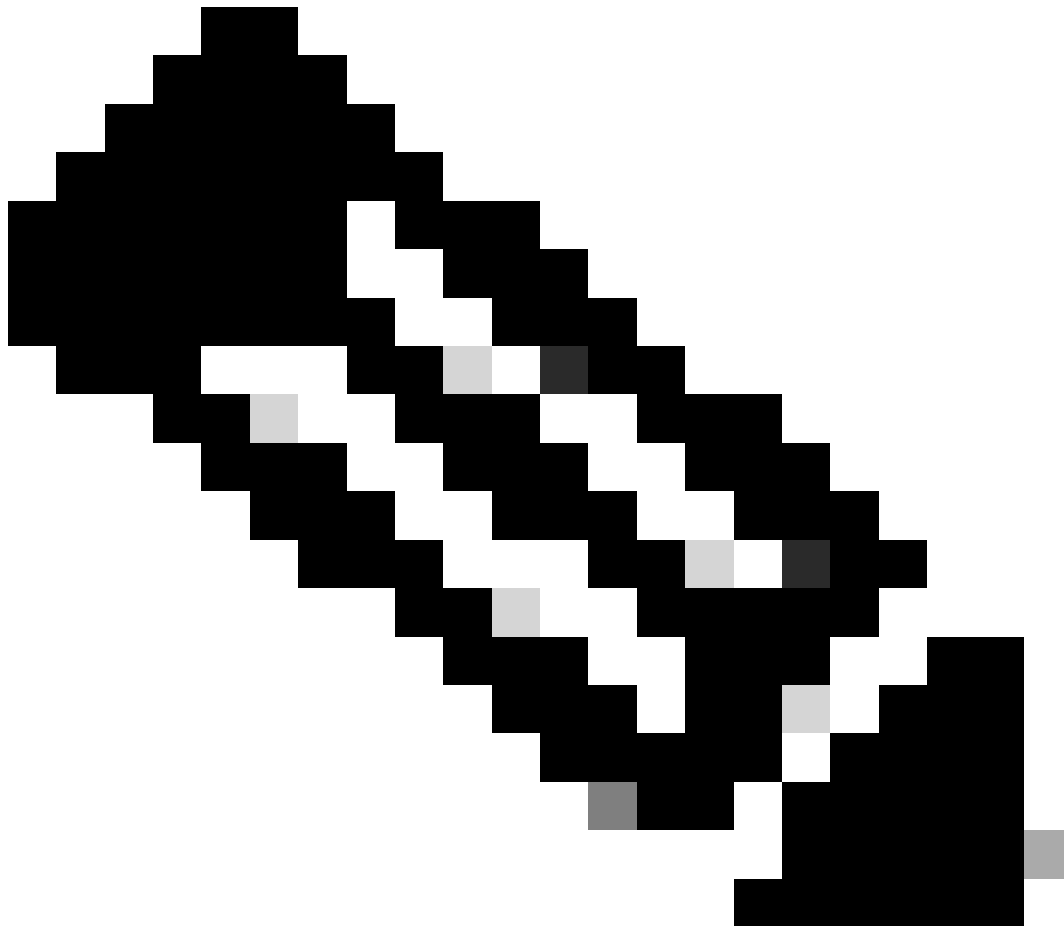
logstash-\*



## Selected fields

t kubernetes.labels.serviceName

t log



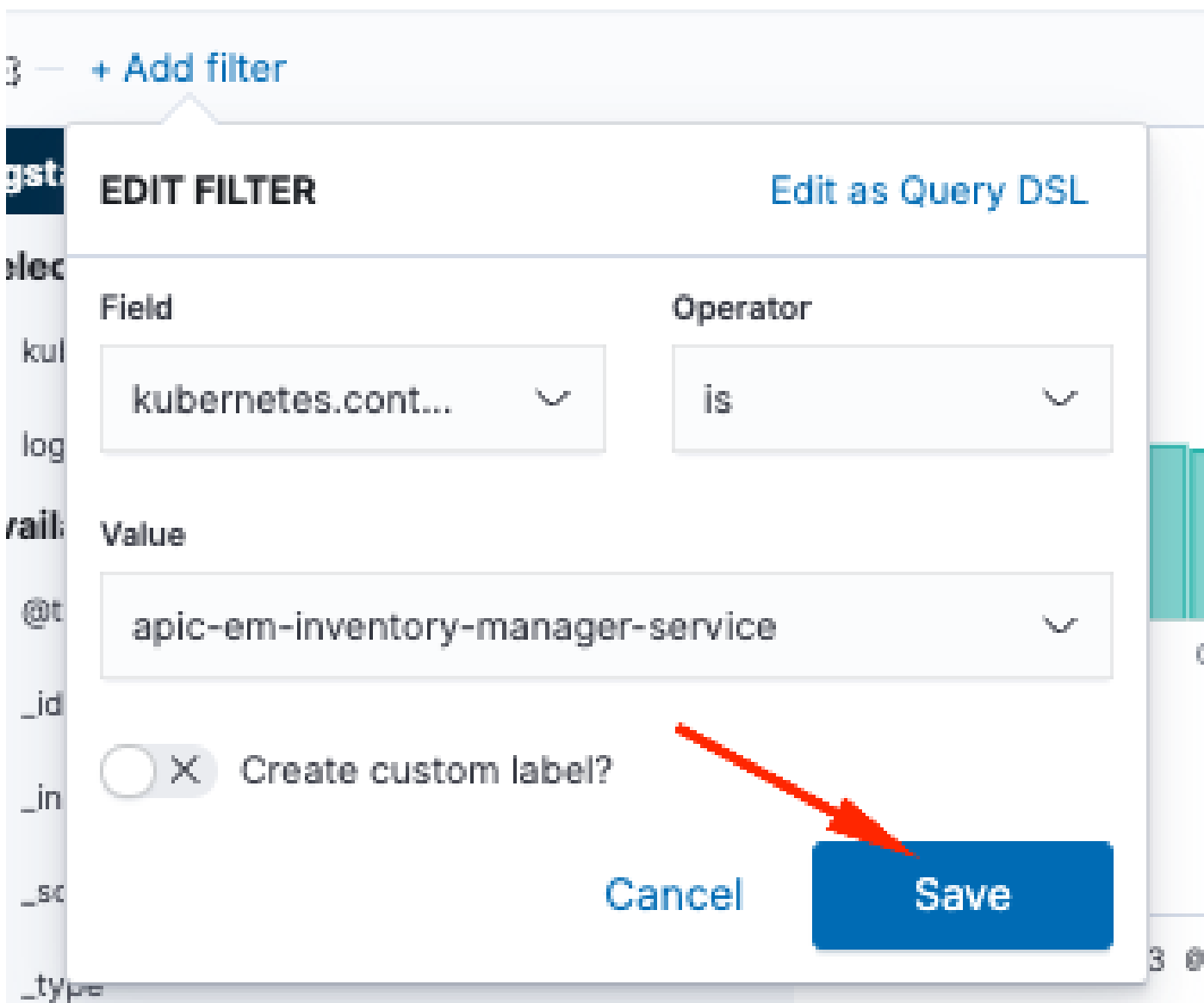
附註：預設會新增「時間」欄位。

## 在Kibana中增加和編輯篩選器

要增加過濾器，請執行以下活動：

- 點選增加過濾器
- 欄位選取：Kubernetes.labels.serviceName
- 運算子選取：是
- 值：選擇您感興趣的服務
- 點選儲存按鈕

請看下一個所選服務為apic-em-inventory-manager-service的示例：



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 off. At the bottom right, there are two buttons: 'Cancel' and 'Save'. A red arrow points to the 'Save' button.

您可以根據需要增加更多過濾器。

下一個範例新增了一個篩選條件，其中Field：log、operator：is和Value：error：



## EDIT FILTER

Edit as Query DSL

Field

log

Operator

is

Value

error

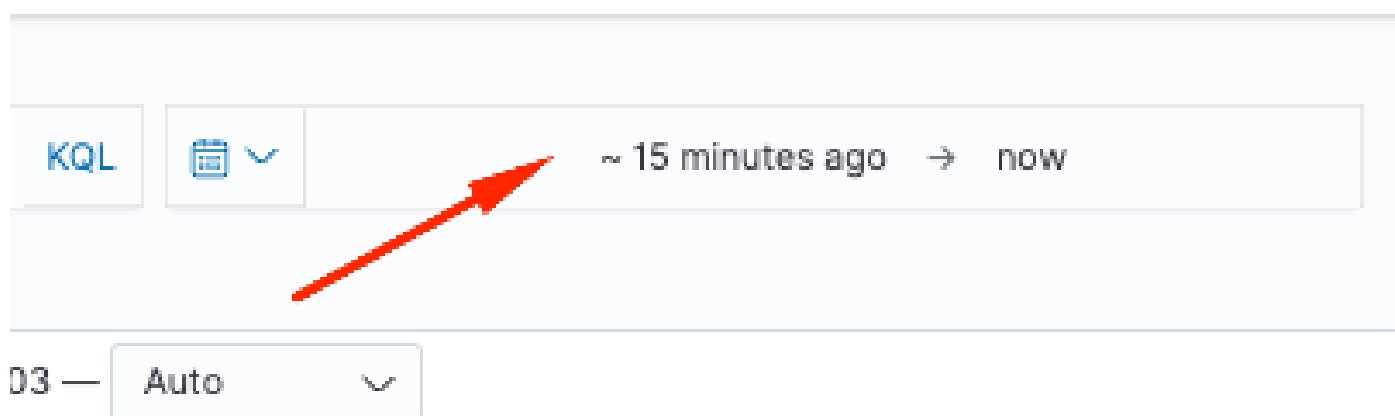
X Create custom label?

Cancel

Save

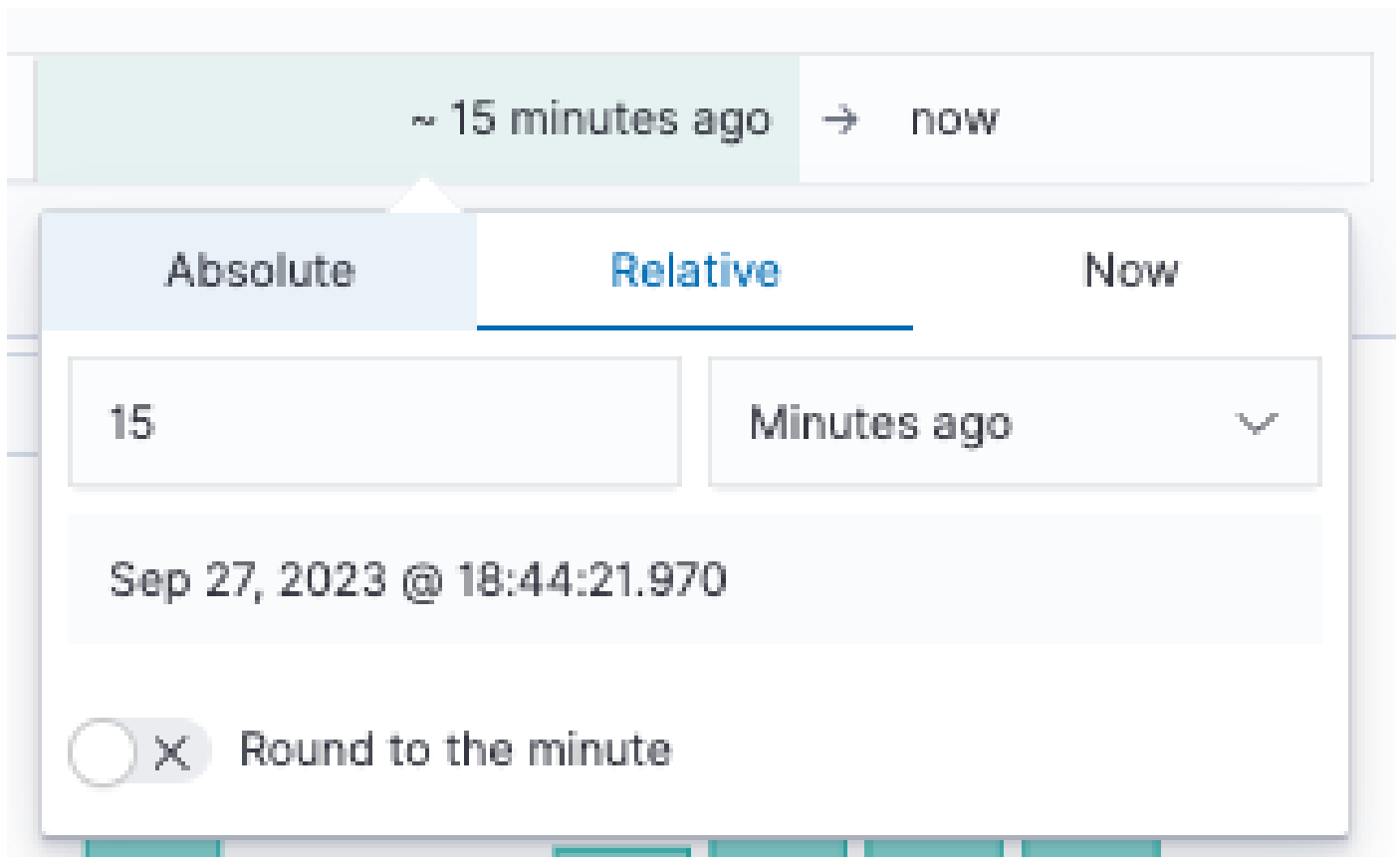
### 獲取特定日期的日誌

您可以將時間元素加入搜尋條件中。



The screenshot shows a search bar with the text "KQL" on the left, a calendar icon with a dropdown arrow, and a time range filter set to "~ 15 minutes ago" followed by a right-pointing arrow and the word "now". A red arrow points to the time range filter. Below the search bar, there is a dropdown menu with "03" on the left and "Auto" with a dropdown arrow on the right.

使用「時間範圍」欄位中的以下選項之一：



- 絕對- 從特定日期到另一個特定日期。
- 相對 -從過去X分鐘、小時、天或周到特定日期。
- Now -將時間設定為「now」意味著每次刷新時，此時間都將設定為刷新時間。

## Lucene使用案例

Lucene是一個高效能、全功能的文本搜尋引擎庫。這項技術幾乎適用於任何需要全文檢索的應用程式。

導航到搜尋欄並停用KQL以啟用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



獲取特定服務的日誌

在過濾器欄中鍵入下一個查詢，然後按刷新按鈕

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

接下來我們來看一個關於task-service的示例：

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



## 混合併匹配您的搜尋

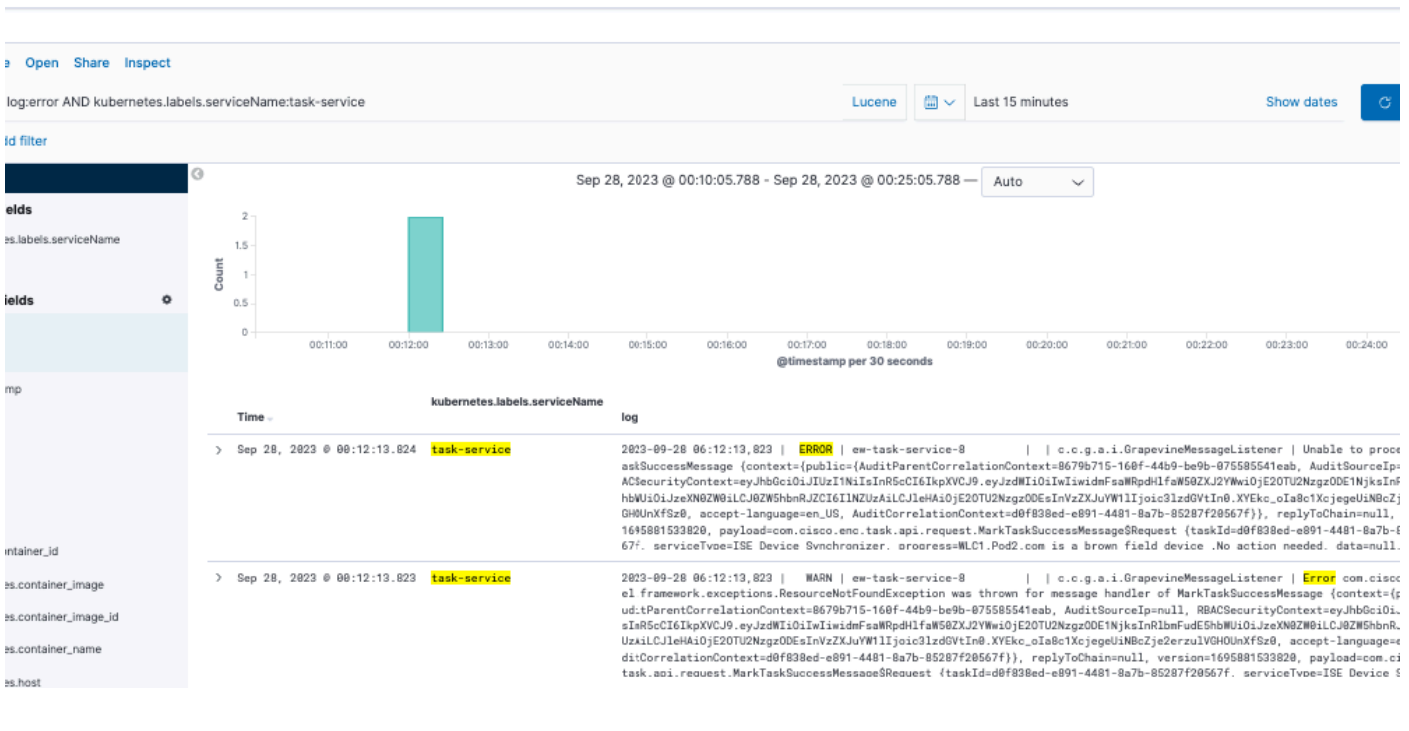
您可以在字串之間使用AND ( 或&& ) 來搜尋符合字串組合的專案。


```
<#root>
```

```
log:error
```

```
AND
```

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



 附註：並非所有欄位都可搜尋。

如果您只想在可用欄位窗格中看到可搜尋的欄位，請選擇齒輪並自定義檢視。您也可以定義要使用的搜尋型別，例如字串、布林、數字等。

## Available fields



### Aggregatable

### Searchable

### Type

### Field name

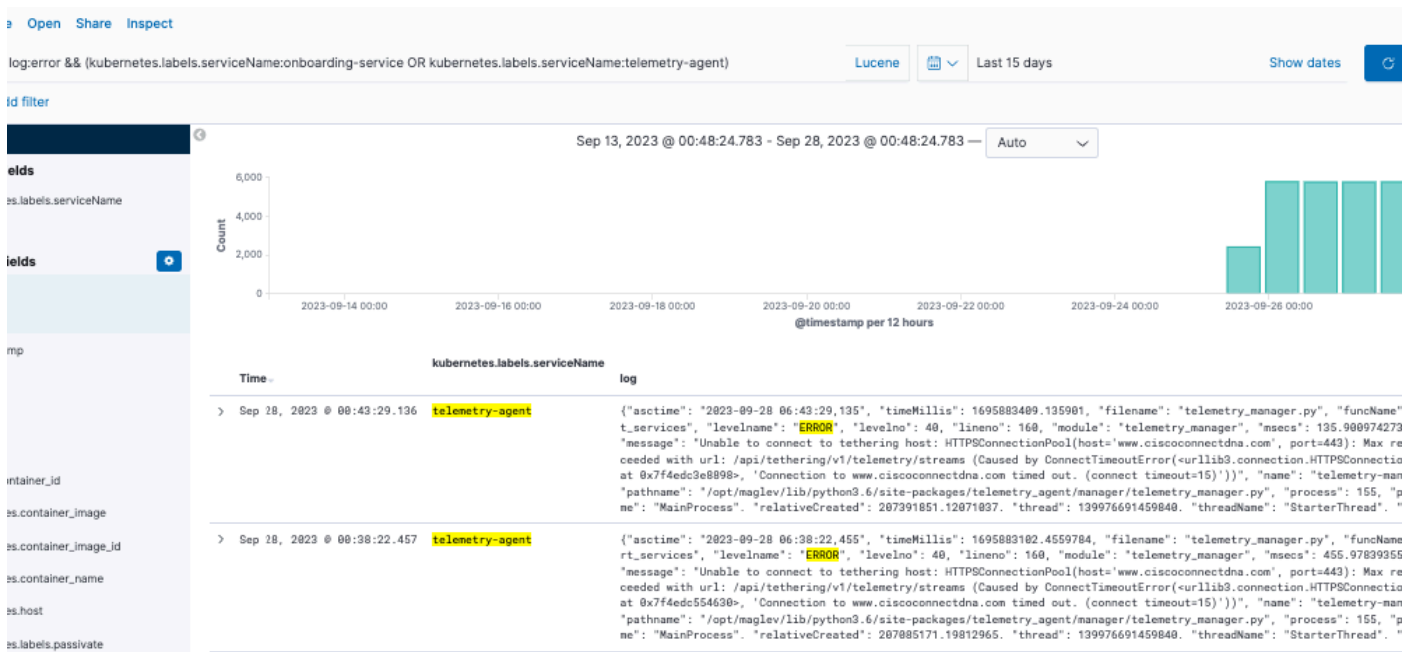
Hide missing fields

[Reset filters](#)

同時搜尋兩個不同的服務以找出錯誤

在您的搜尋條件中包含兩個或多個服務。確保服務名稱在括弧中輸入，並用OR分隔開。

log:error && (kubernetes.labels.serviceName:onboarding-service OR kubernetes.labels.serviceName:telemetry-agent)



## 參考

- [彈性搜尋通用選項](#)
- [Apache Lucene -查詢剖析器語法](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。