

Configurazione di Kibana in DNA Center per la visualizzazione del log

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configura Kibana per la visualizzazione del log](#)

[Aggiungi campi in Kibana](#)

[Aggiungi e modifica filtri in Kibana](#)

[Ottieni registri da una data specifica](#)

[Casi d'uso con Lucene](#)

[Ottieni registri per un servizio specifico](#)

[Ottiene i registri che contengono una parola specifica](#)

[Combinazione e corrispondenza con la ricerca](#)

[Ricerca di un errore in due servizi diversi contemporaneamente](#)

[Riferimento](#)

Introduzione

Questo documento descrive come usare Kibana per cercare log specifici tra diversi servizi Cisco DNA Center.

Prerequisiti

Requisiti

È necessario disporre dell'accesso a Cisco DNA Center tramite GUI con ruolo di amministratore, nonché conoscere i nomi e l'utilizzo dei servizi di Cisco DNA Center.

Componenti usati

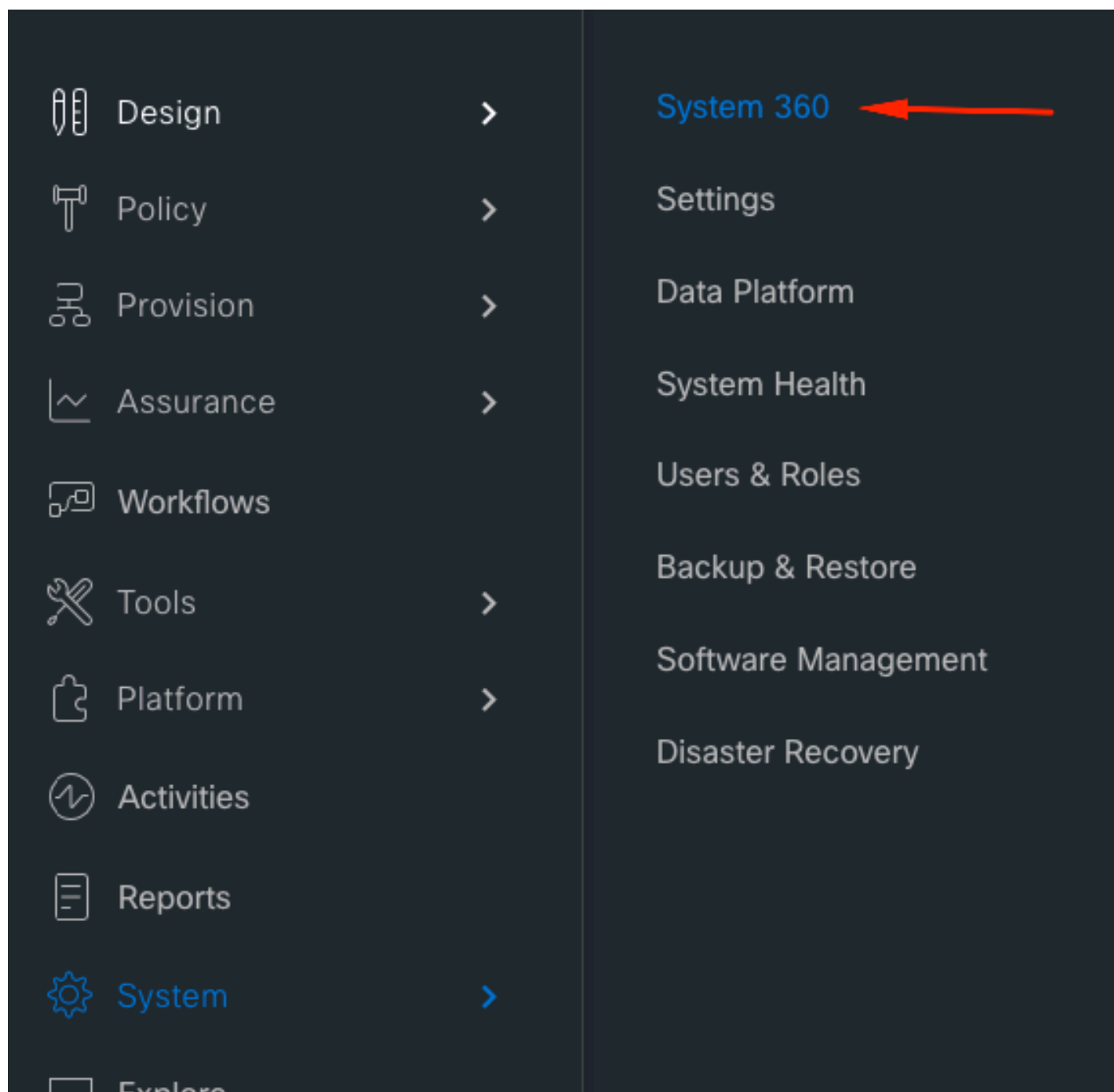
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Kibana è un plug-in di visualizzazione dati open source per Elasticsearch. Fornisce funzionalità di visualizzazione su contenuto indicizzato in un cluster Elasticsearch disponibile in Cisco DNA Center.

È possibile accedere a Kibana in due modi:

- <https://<Cisco DNA Center ip>/kibana>
- Menu principale > Sistema > System 360 -> Strumenti cluster -> Esplora log



Cluster Tools

As of Sep 27, 2023 2:42 PM

Monitoring



Log Explorer




Pagina Web Kibana predefinita

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](#)

Configura Kibana per la visualizzazione del log

Accedere al menu della barra di sinistra e fare clic su Discover:



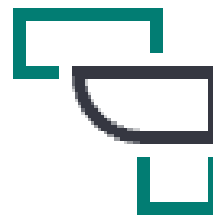
Home



Discover

Add Data to Kibana

Use these solutions to quickly turn your data



APM

APM automatically collects in-

Kibana ha diversi campi, che sono evidenziati nell'immagine seguente:

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: 7ef2b92ac566143e8b33be01584ef65e8807ad29a51158bd48074cb3d5ca2ed2
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: 7ef2b92ac566143e8b33be01584ef65e8807ad29a51158bd48074cb3d5ca2ed2
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: 7ef2b92ac566143e8b33be01584ef65e8807ad29a51158bd48074cb3d5ca2ed2
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: 7ef2b92ac566143e8b33be01584ef65e8807ad29a51158bd48074cb3d5ca2ed2
kubernetes.container_name: mongodb kubernetes.namespace_name: naglev-aystem kubernetes.pod_name: mongodb-0

```

Aggiungi campi in Kibana

Selezionare Filtri > Campi disponibili

I campi da aggiungere per la visualizzazione dei log sono:

- Kubernetes.labels.serviceName - Servizio che visualizza il registro specifico
- Registro - Contenuto non elaborato del registro

Fare clic sul pulsante Aggiungi



Accertarsi di disporre della configurazione successiva:

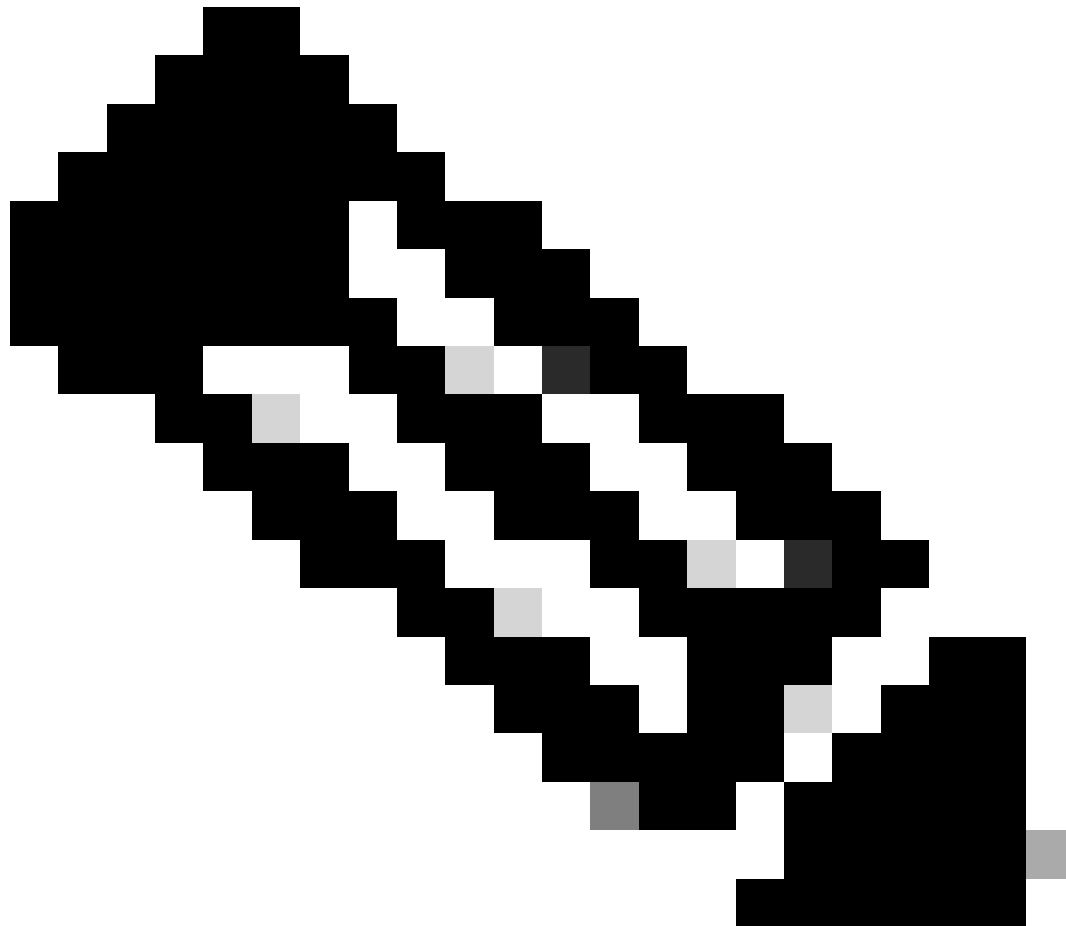
logstash-*



Selected fields

t kubernetes.labels.serviceName

t log



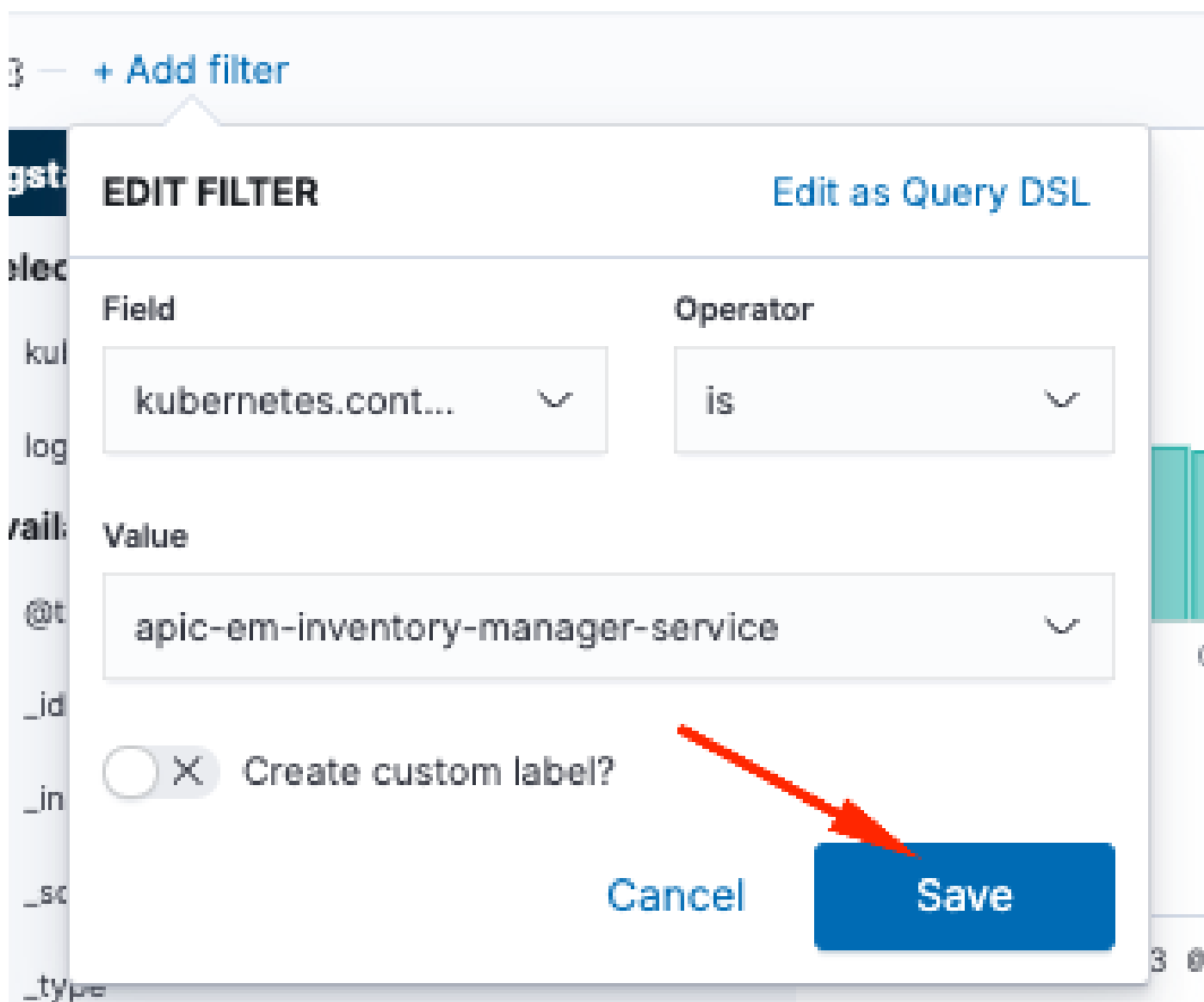
Nota: il campo Ora viene aggiunto per impostazione predefinita.

Aggiungi e modifica filtri in Kibana

Per aggiungere un filtro, eseguire l'attività successiva:

- Fare clic in Aggiungi filtro
- Selezione campo: Kubernetes.labels.serviceName
- Operatore select: è
- Valore: selezionare il servizio desiderato
- Fare clic sul pulsante Salva

Osservare l'esempio successivo in cui il servizio selezionato è 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 title is 'EDIT FILTER' with a link 'Edit as Query DSL' on the right. Below the title, 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 labeled '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.

È possibile aggiungere altri filtri in base alle esigenze.

Nell'esempio successivo è stato aggiunto un nuovo filtro dove Field:log, operator:is e Value: error:

EDIT FILTER Edit as Query DSL

Field log **Operator** is

Value error

X Create custom label?

Cancel Save

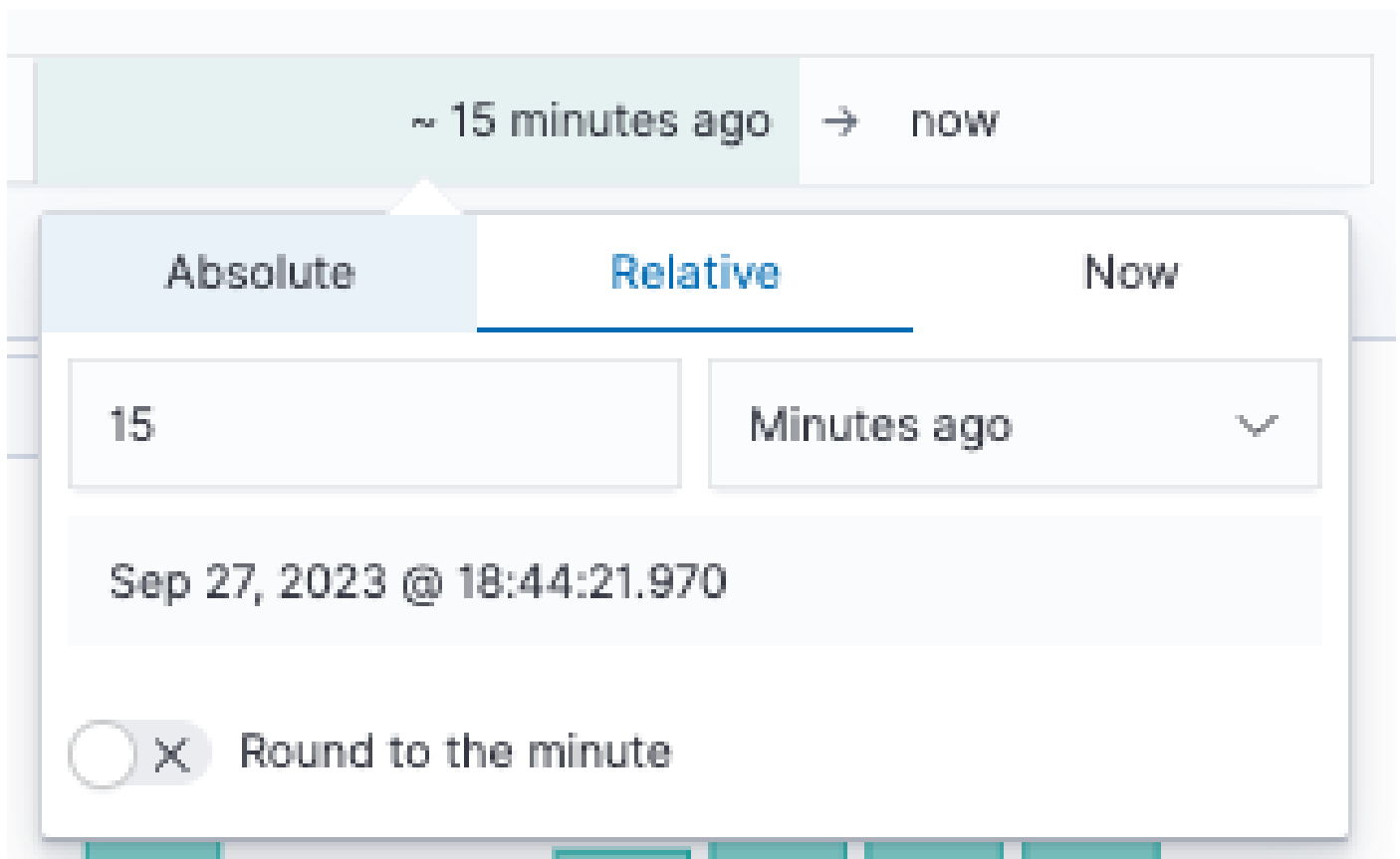
Otteni registri da una data specifica

È possibile aggiungere un elemento temporale ai criteri di ricerca.

KQL 📅 ~ 15 minutes ago → now

03 — Auto

Utilizzare una delle opzioni successive del campo Intervallo di tempo:



- Assoluto - Da una data specifica a un'altra data specifica.
- Relativo: a partire dagli ultimi X minuti, ore, giorni o settimane fino a una data specifica.
- Ora - Se si imposta l'ora su "adesso", ad ogni aggiornamento questa ora verrà impostata sull'ora dell'aggiornamento.

Casi d'uso con Lucene

Lucene è una libreria di motori di ricerca di testo ad alte prestazioni e con funzionalità complete. Si tratta di una tecnologia adatta a quasi tutte le applicazioni che richiedono la ricerca full-text.

Passare alla barra di ricerca e disabilitare KQL per abilitare 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



Ottieni registri per un servizio specifico

Digitare la query successiva nella barra dei filtri e premere il pulsante Aggiorna

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

Osservare l'esempio successivo con task-service:

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


Combinazione e corrispondenza con la ricerca

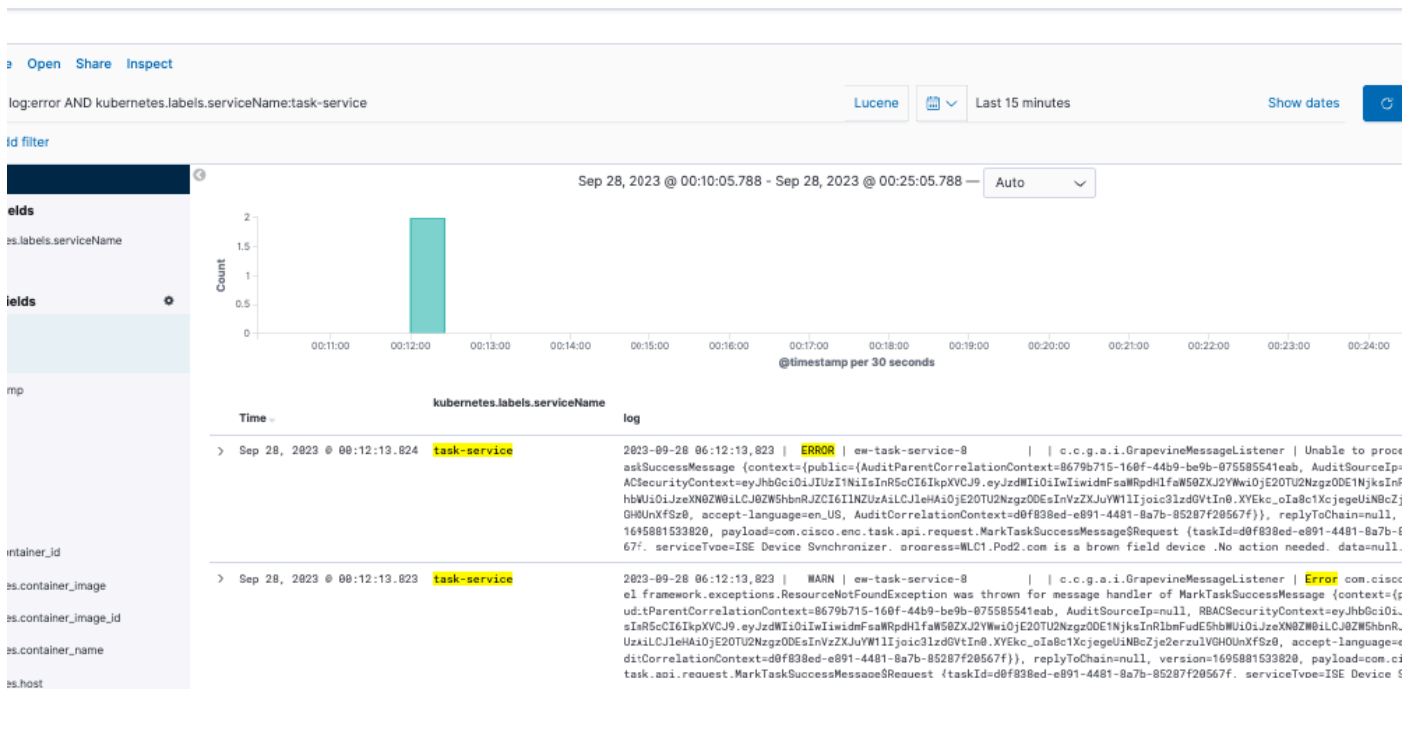
È possibile cercare le voci che corrispondono a una combinazione di stringhe utilizzando l'operatore AND (o &&) tra le stringhe.


```
<#root>
```

```
log:error
```

```
AND
```

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



 Nota: non tutti i campi sono ricercabili.

Se si desidera visualizzare solo i campi in cui è possibile eseguire ricerche nel riquadro Campi disponibili, selezionare la ruota dentata e personalizzare la visualizzazione. È inoltre possibile definire il tipo di ricerca da utilizzare, ad esempio stringa, booleano, numero e così via.

Available fields



Aggregatable

Searchable

Type

Field name

Hide missing fields

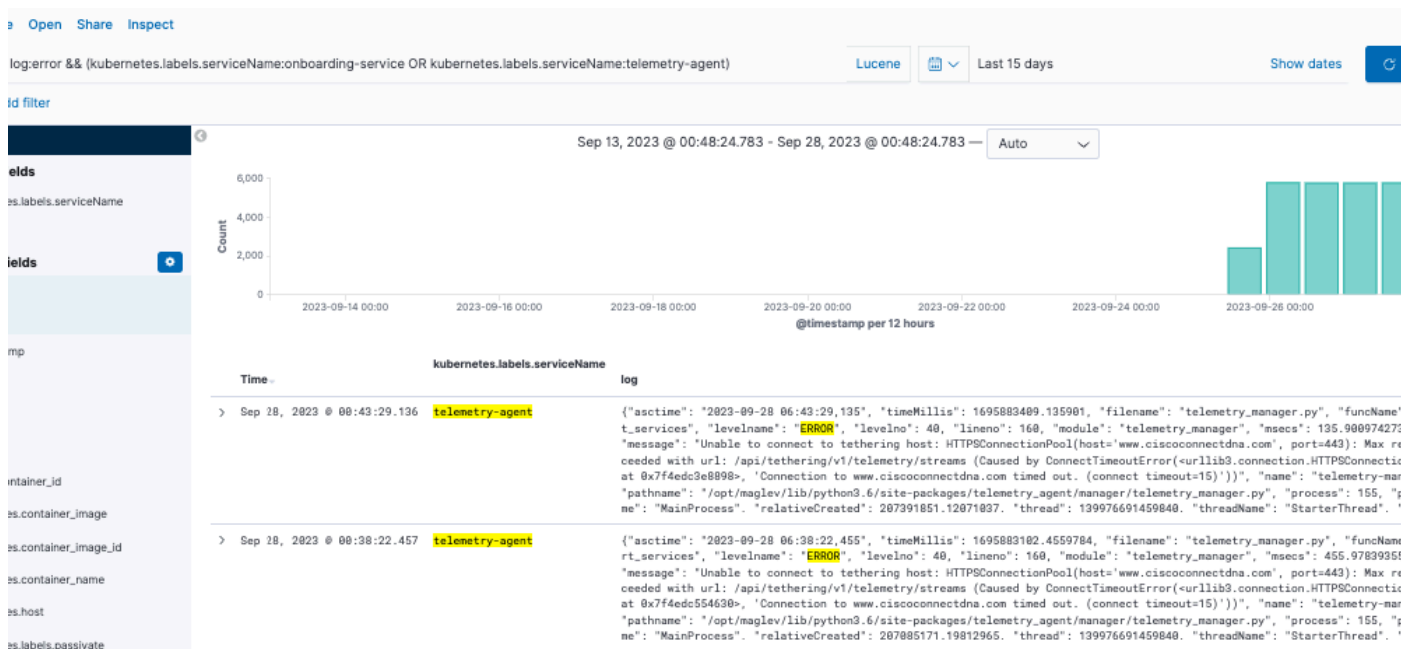
[Reset filters](#)

Ricerca di un errore in due servizi diversi contemporaneamente

Includere due o più servizi nei criteri di ricerca. Assicurarsi che i nomi dei servizi siano inseriti tra

parentesi e separarli con OR.

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



Riferimento

- [Opzioni comuni di ricerca elastica](#)
- [Apache Lucene - Sintassi parser query](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).