Configurazione di Kibana in DNA Center per la visualizzazione del log

Sommario

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

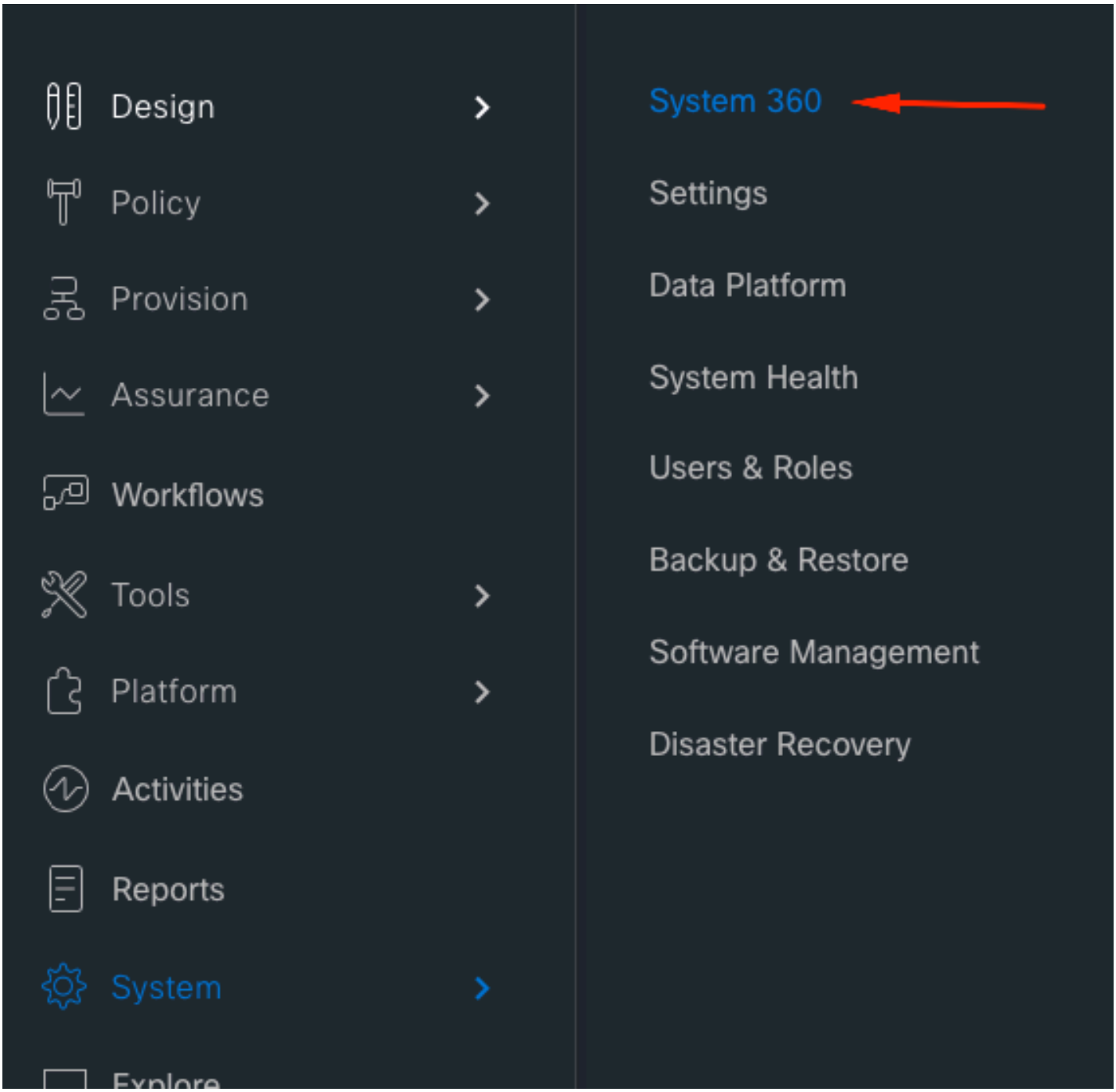
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

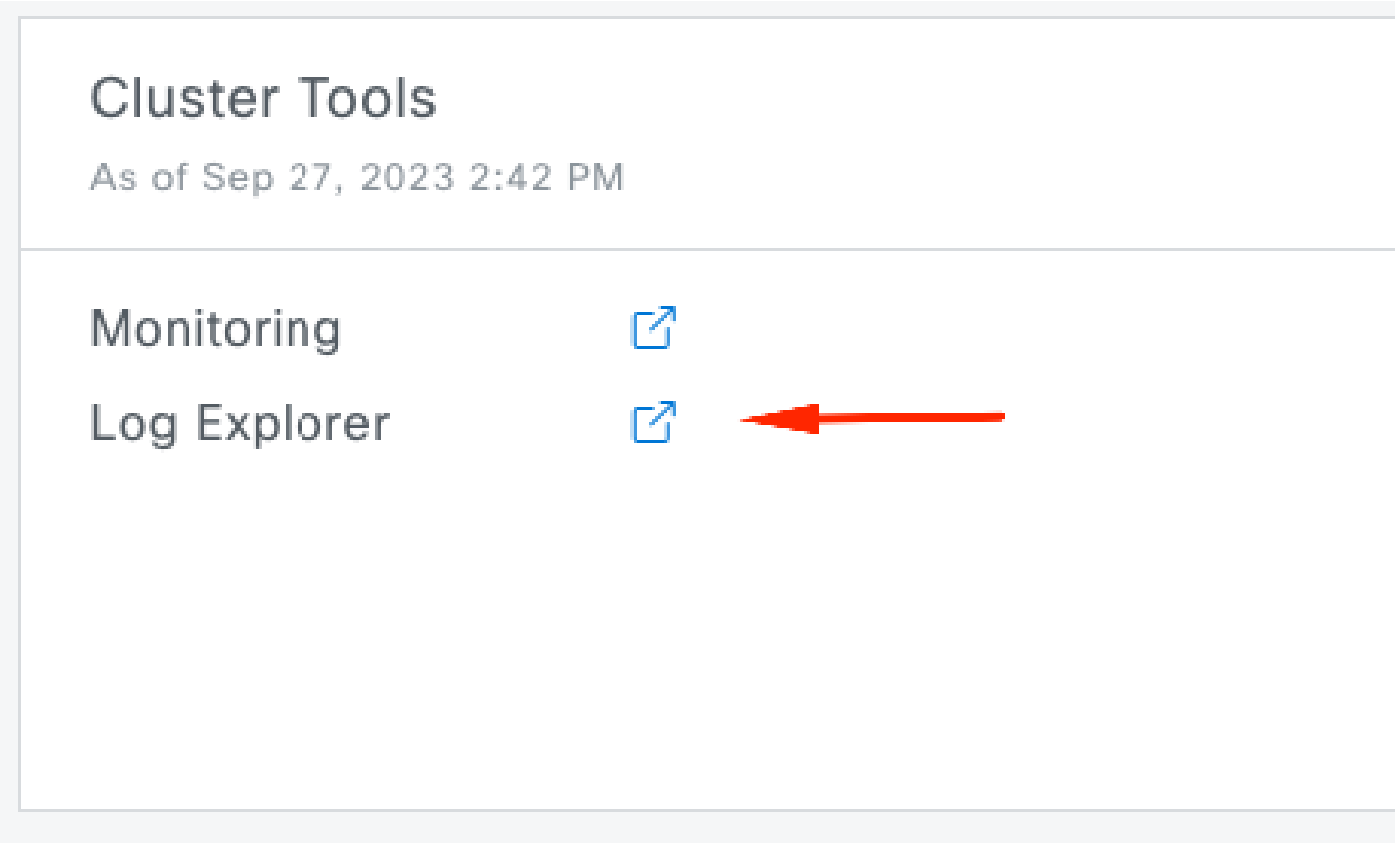
Premesse

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.

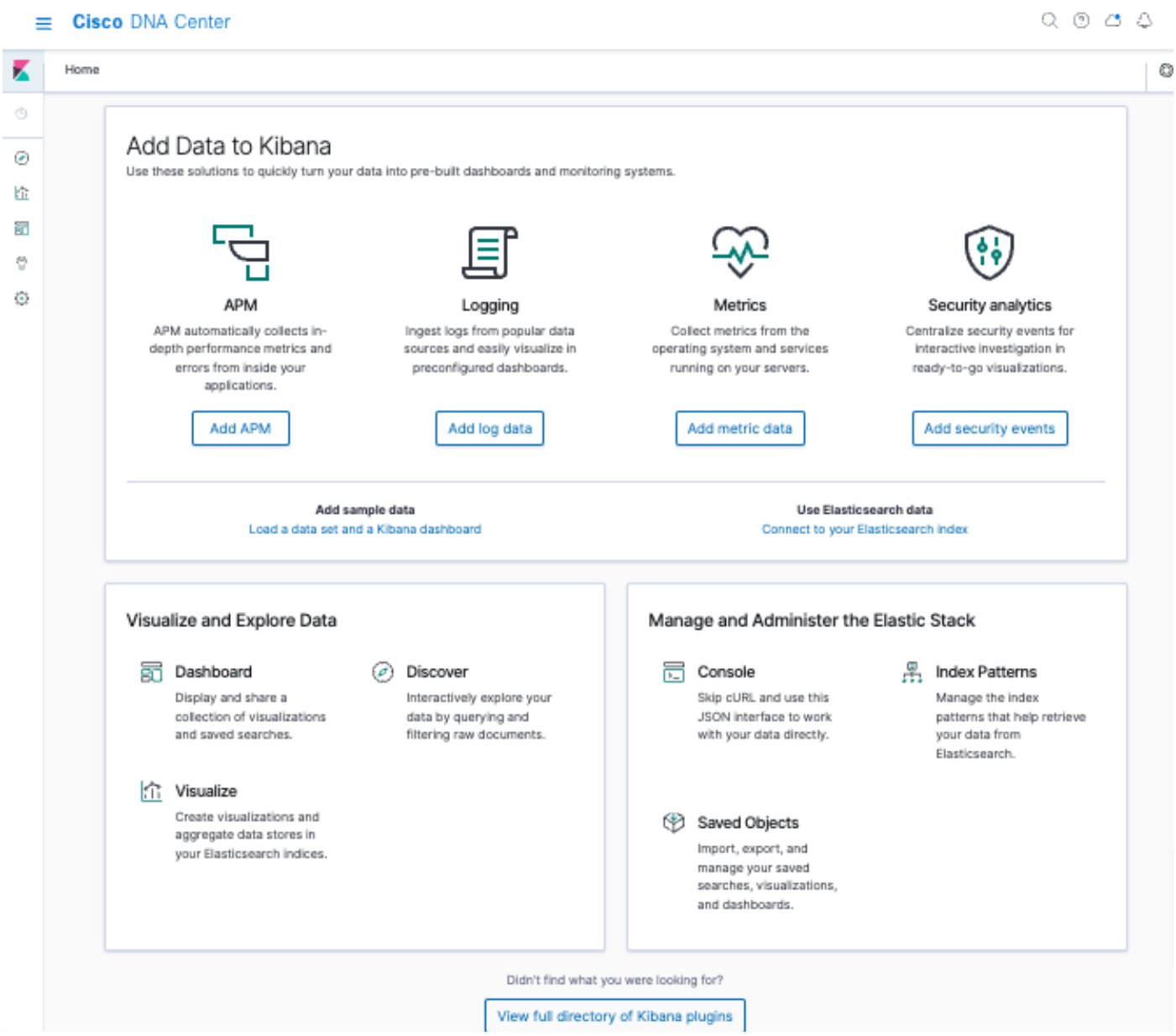
È possibile accedere a Kibana in due modi:

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



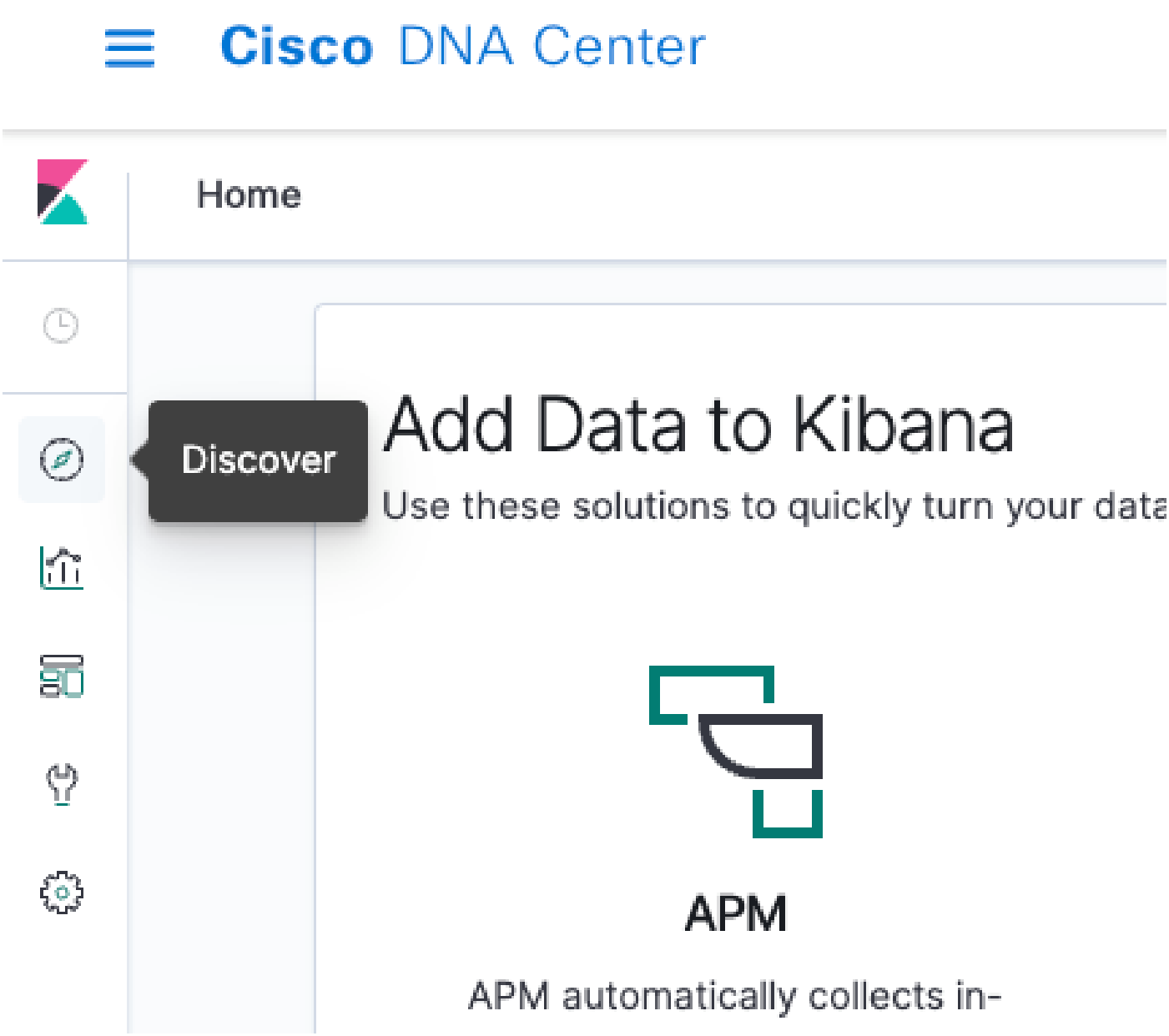


Pagina Web Kibana predefinita

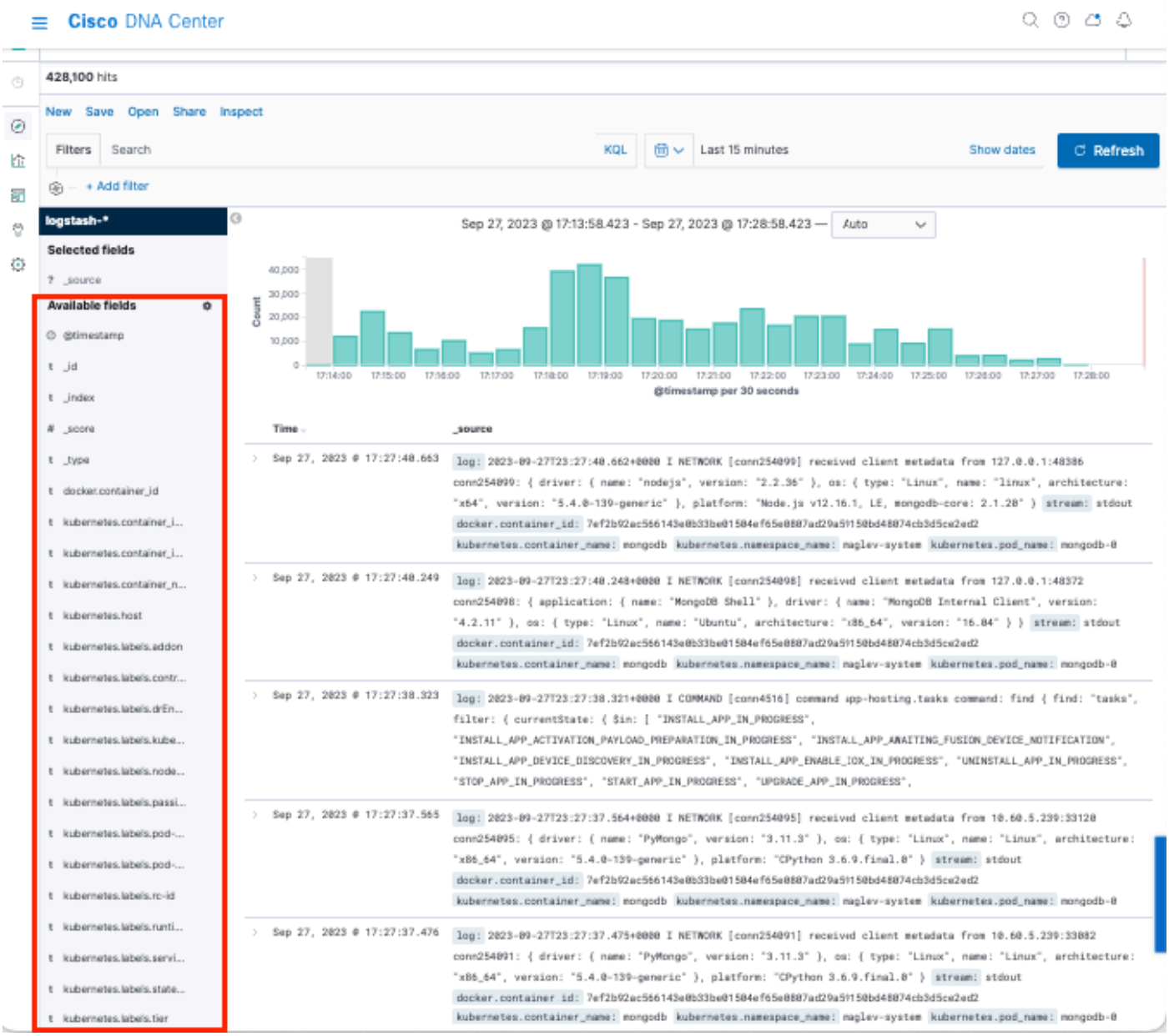


Configura Kibana per la visualizzazione del log

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



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



Aggiungi campi in Kibana

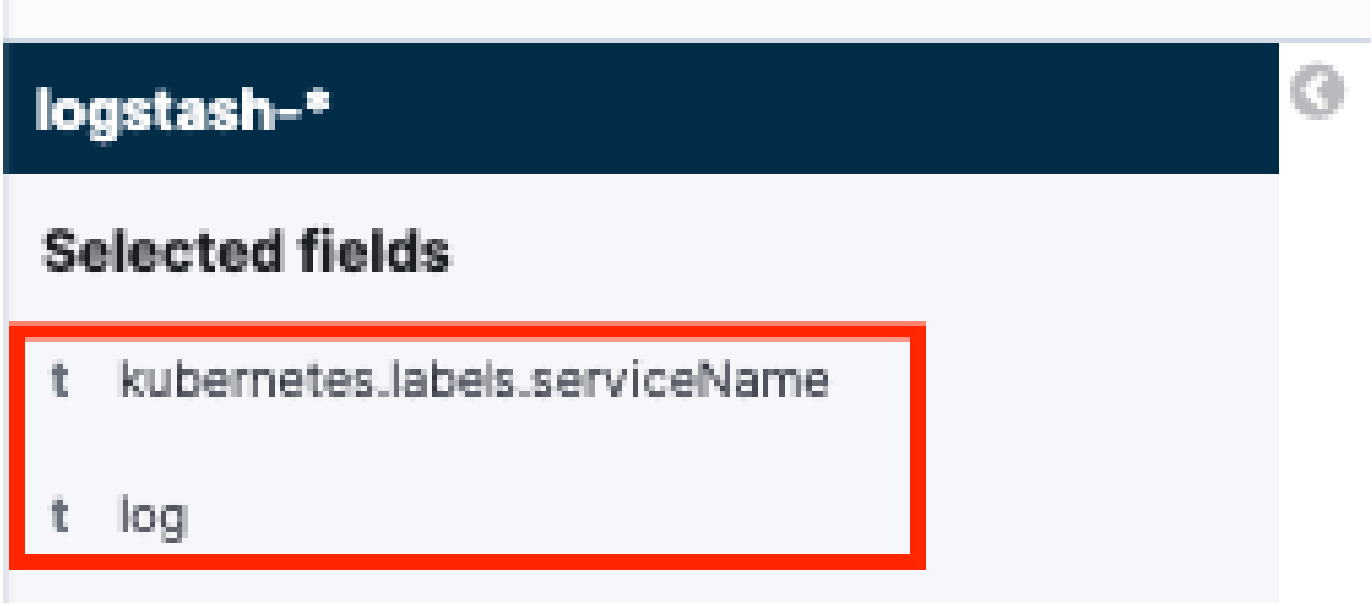
Selezionare Filtri > Campi disponibili

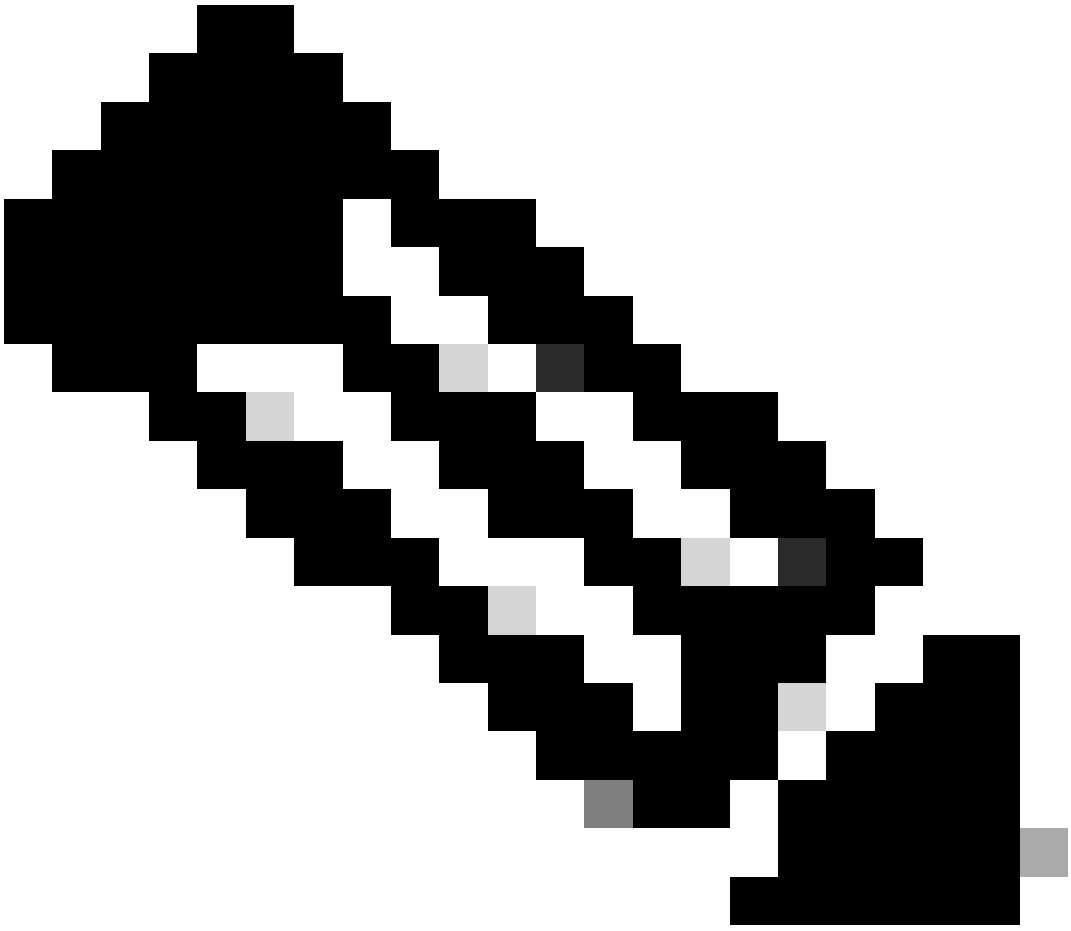
I campi da aggiungere per la visualizzazione dei log sono:

- 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:





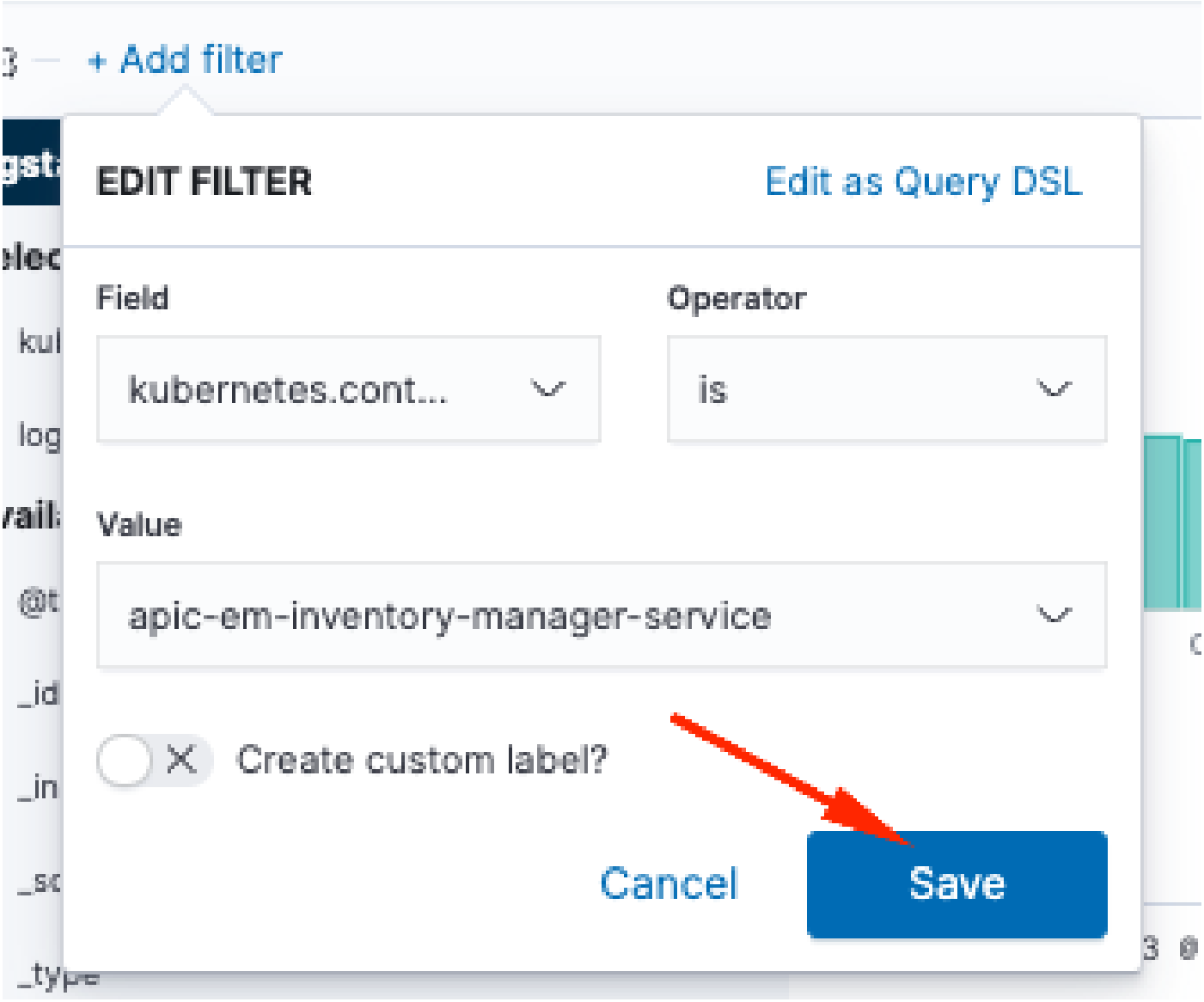
Nota: il campo Ora viene aggiunto per impostazione predefinita.

Aggiungi e modifica filtri in Kibana

Per aggiungere un filtro, eseguire l'attività successiva:

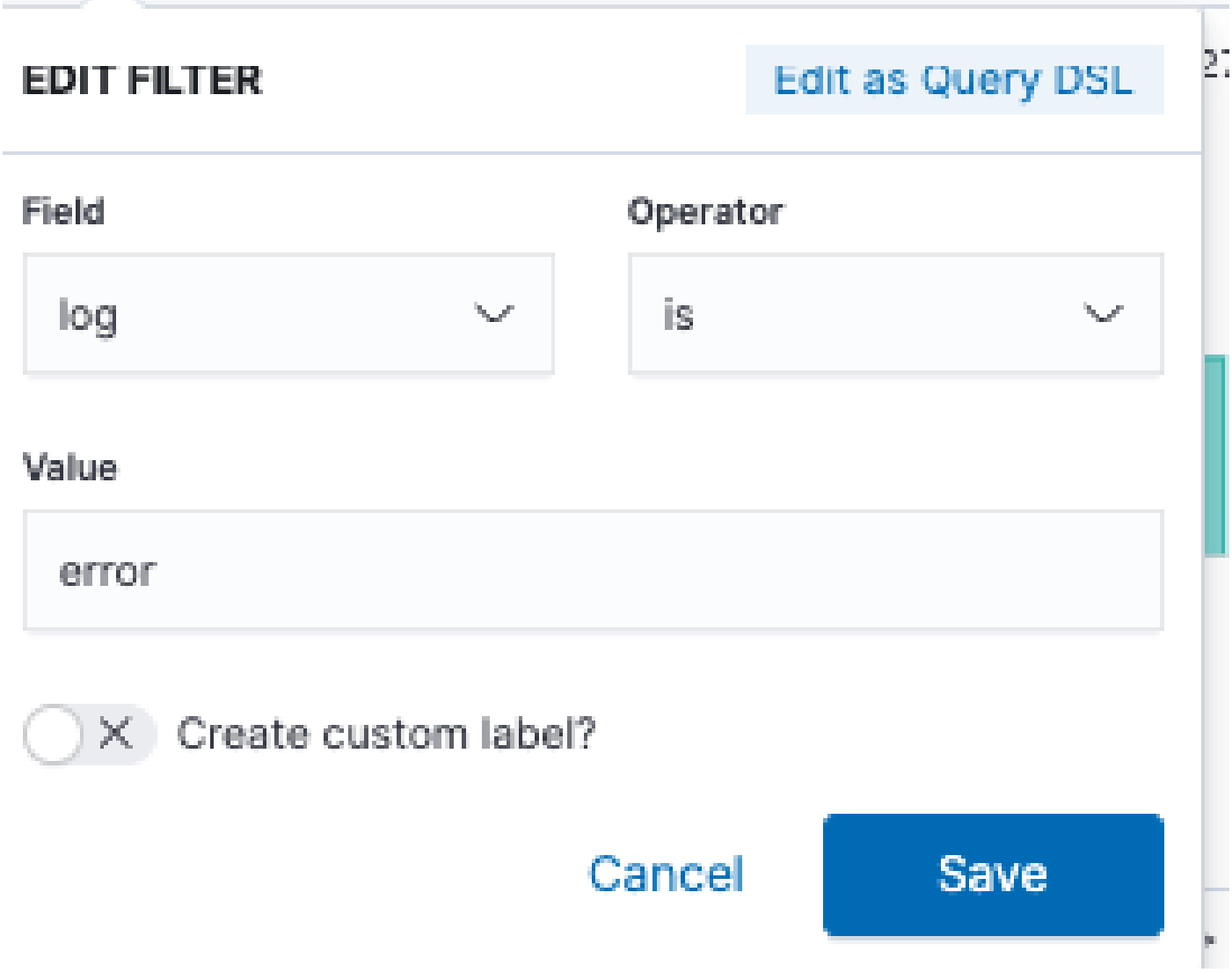
- Fare clic in Aggiungi filtro
- Selezione campo: Kubernetes.labels.serviceName
- Operatore select: è
- Valore: selezionare il servizio desiderato
- Fare clic sul pulsante Salva

Osservare l'esempio successivo in cui il servizio selezionato è apic-em-inventory-manager-service:



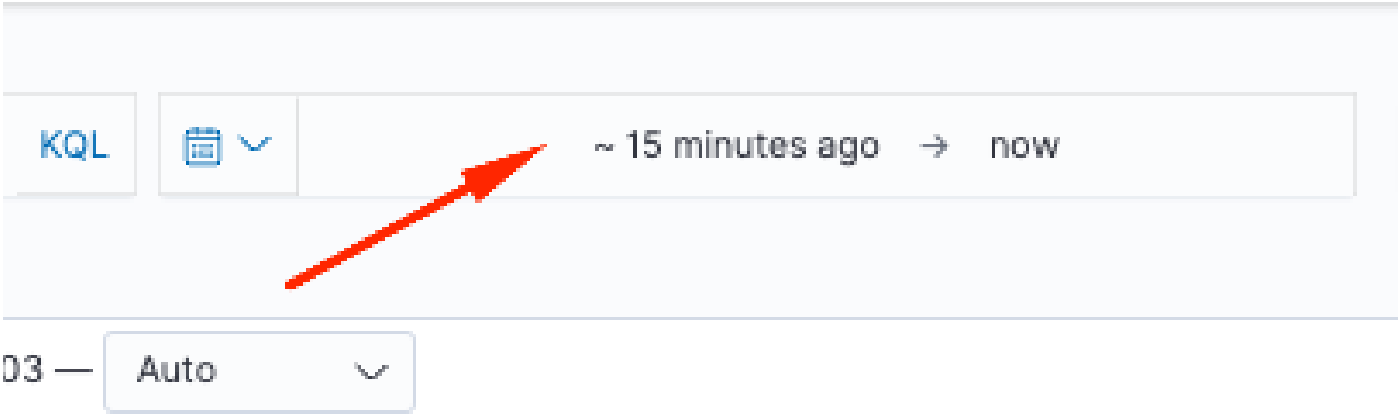
È possibile aggiungere altri filtri in base alle esigenze.

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

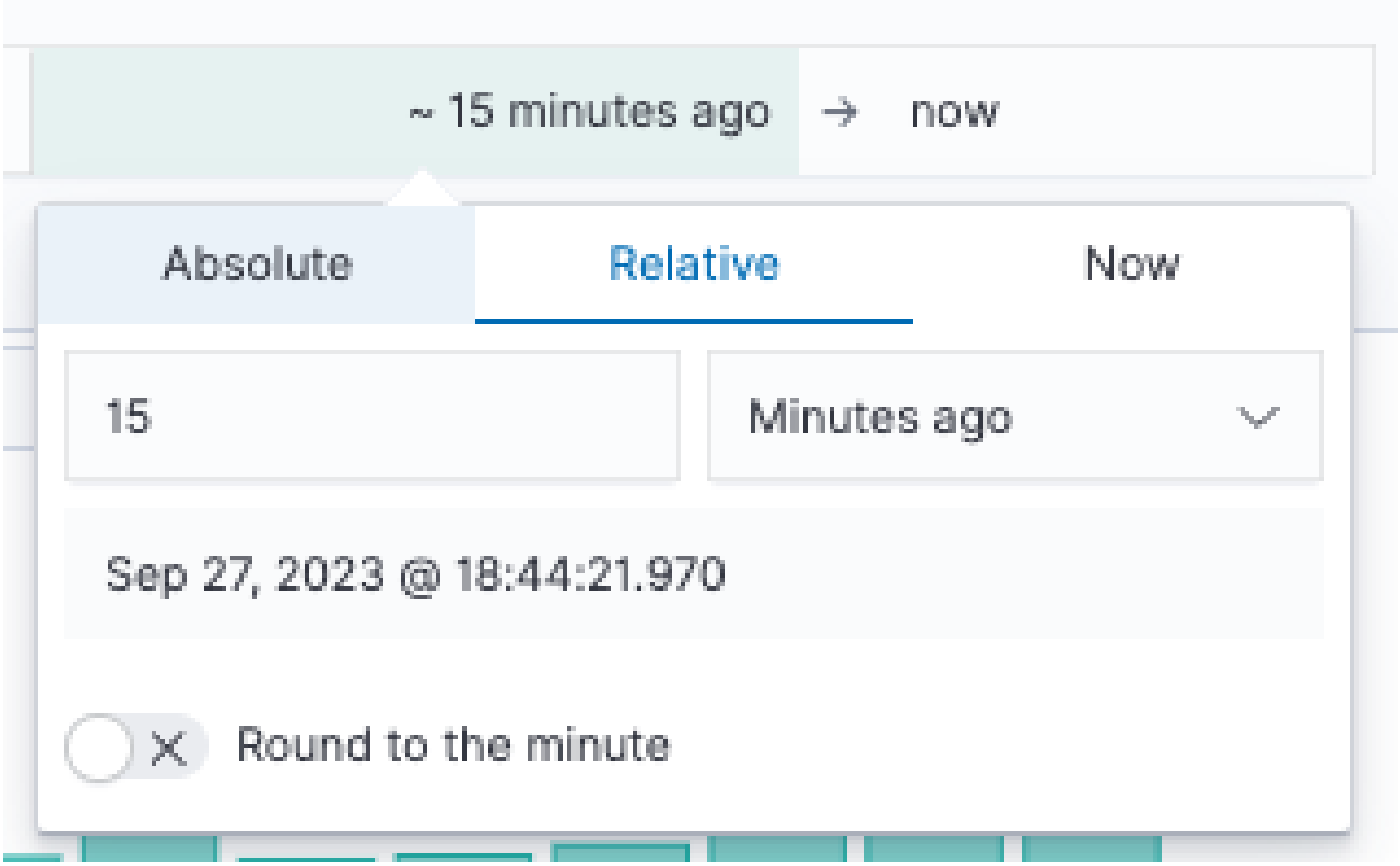


Ottieni registri da una data specifica

È possibile aggiungere un elemento temporale ai criteri di ricerca.



Utilizzare una delle opzioni successive del campo Intervallo di tempo:

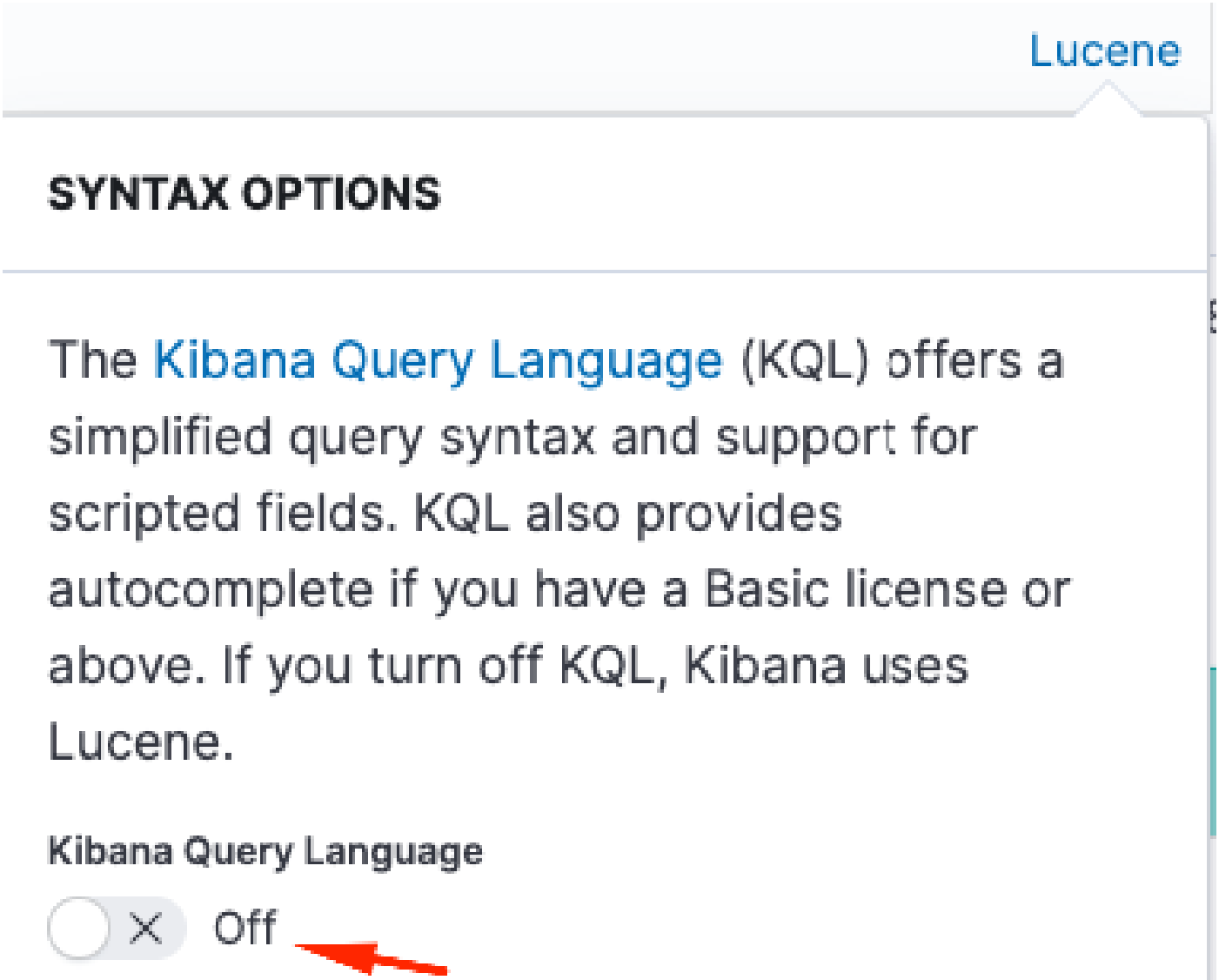


- Assoluto - Da una data specifica a un'altra data specifica.
- Relativo: a partire dagli ultimi X minuti, ore, giorni o settimane fino a una data specifica.
- Ora - Se si imposta l'ora su "adesso", ad ogni aggiornamento questa ora verrà impostata sull'ora dell'aggiornamento.

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:



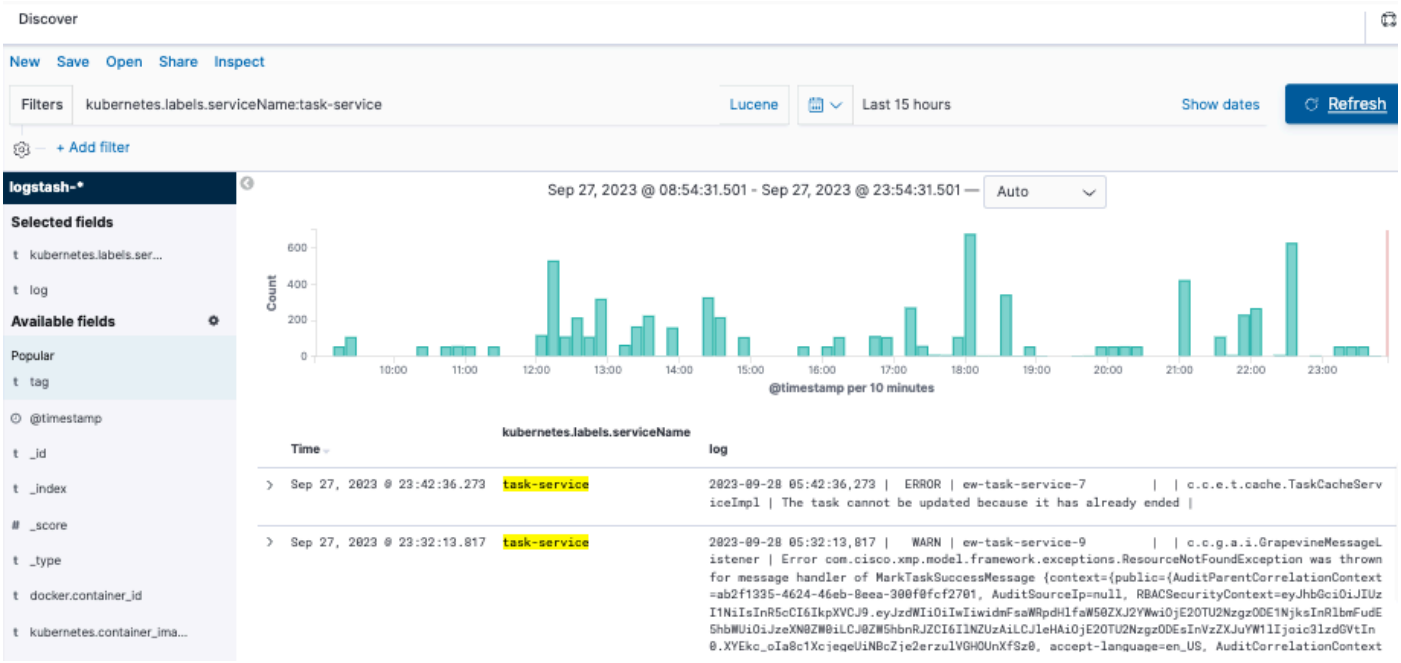
Ottieni registri per un servizio specifico

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
```

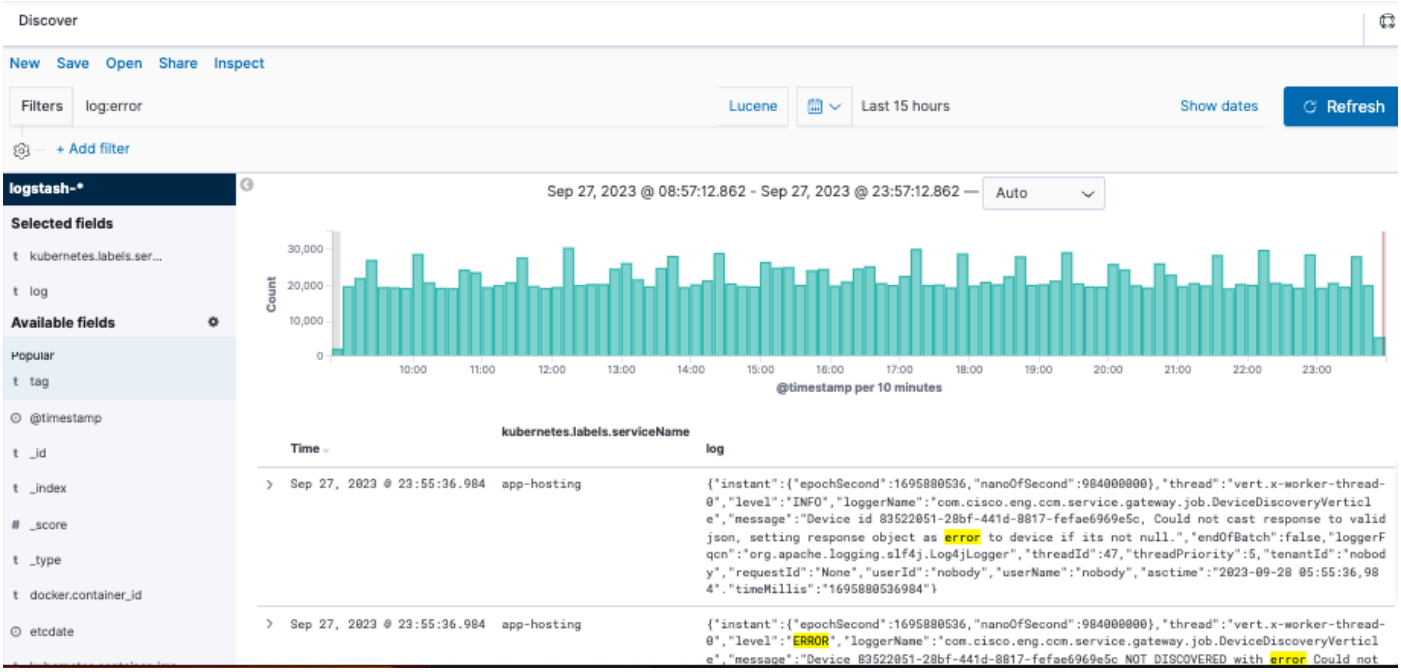


Ottiene i registri che contengono una parola specifica

Suggerimento: le voci più comuni del registro che indicano problemi contengono " Errore " , " Errore " e " Eccezione ". Tuttavia, è possibile modificare la stringa in modo che sia qualsiasi altra stringa comune che possa essere utile per la risoluzione dei problemi.

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

```
log:error
```



Combinazione e corrispondenza con la ricerca

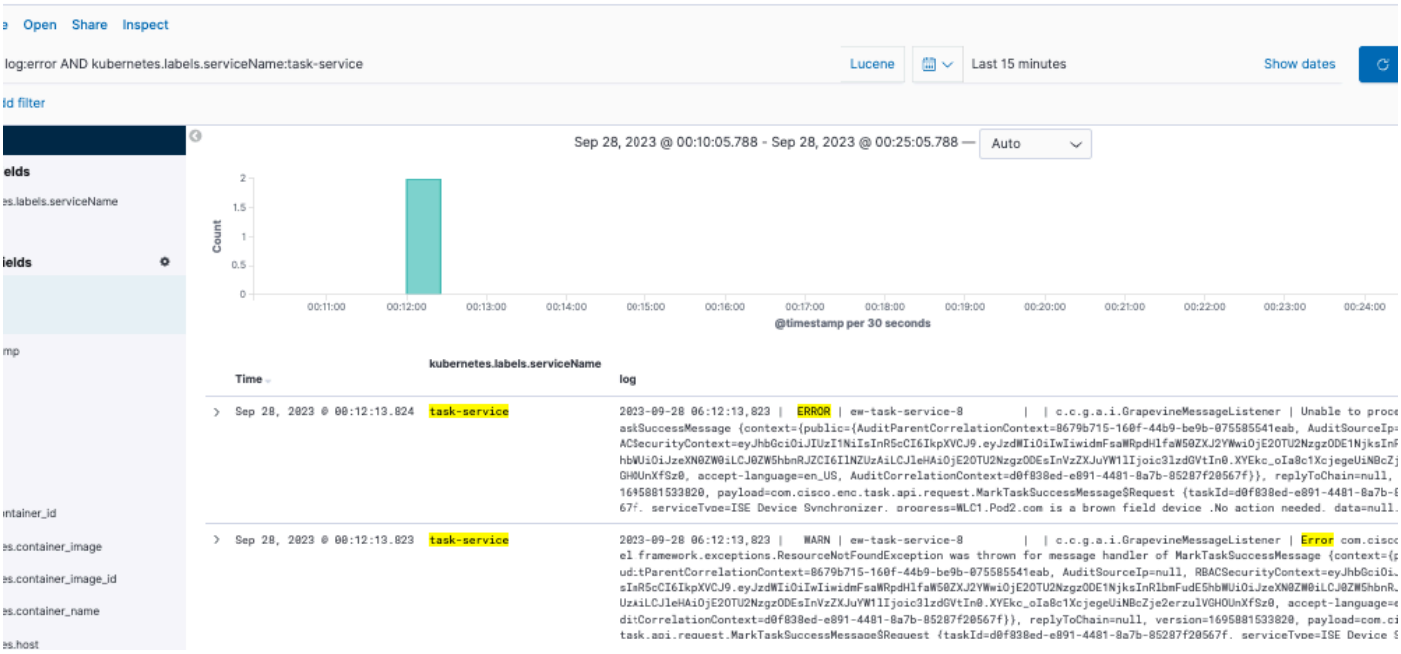
È possibile cercare le voci che corrispondono a una combinazione di stringhe utilizzando l'operatore AND (o &&) tra le stringhe.

<#root>

`log:error`

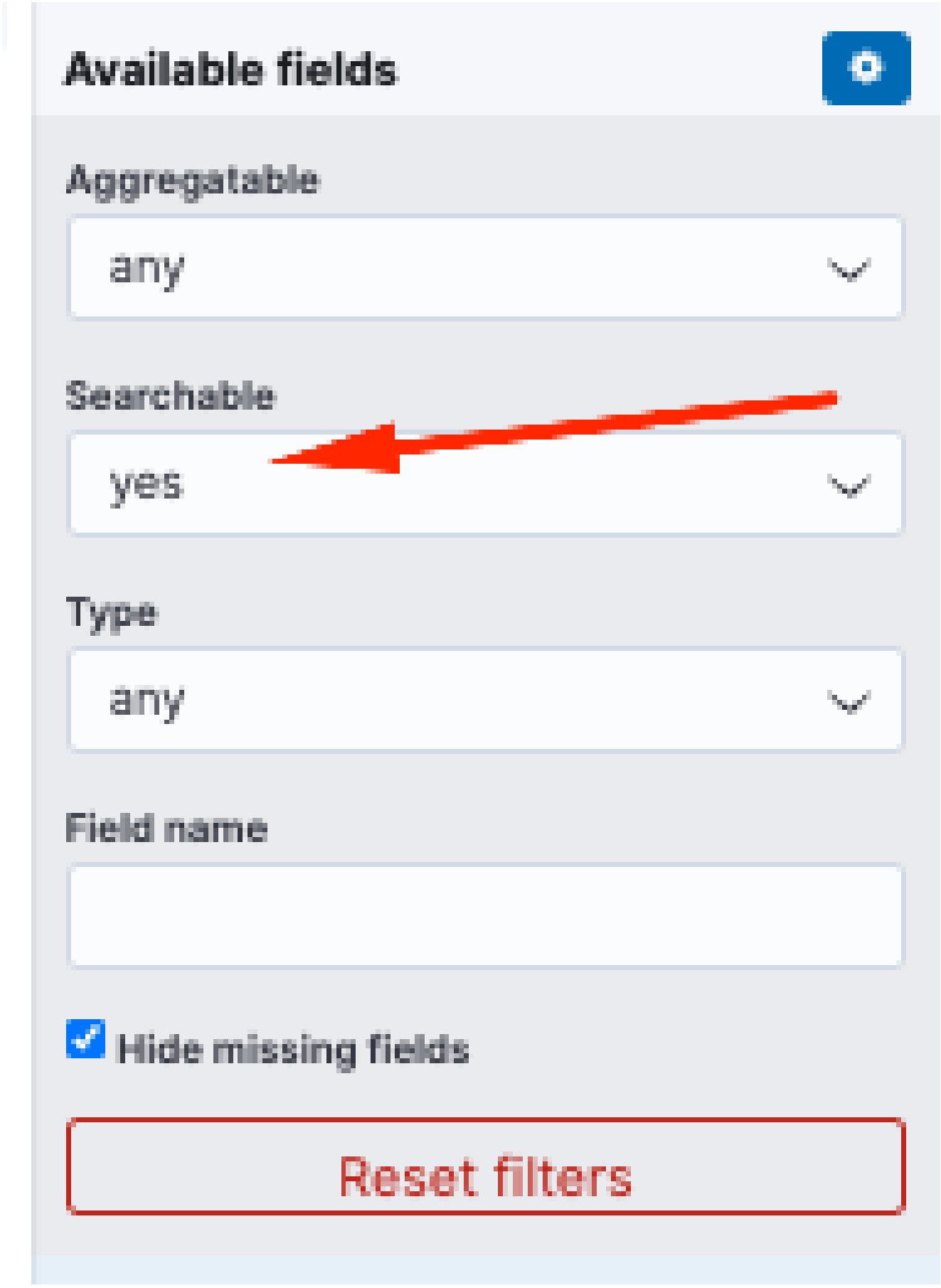
AND

`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.

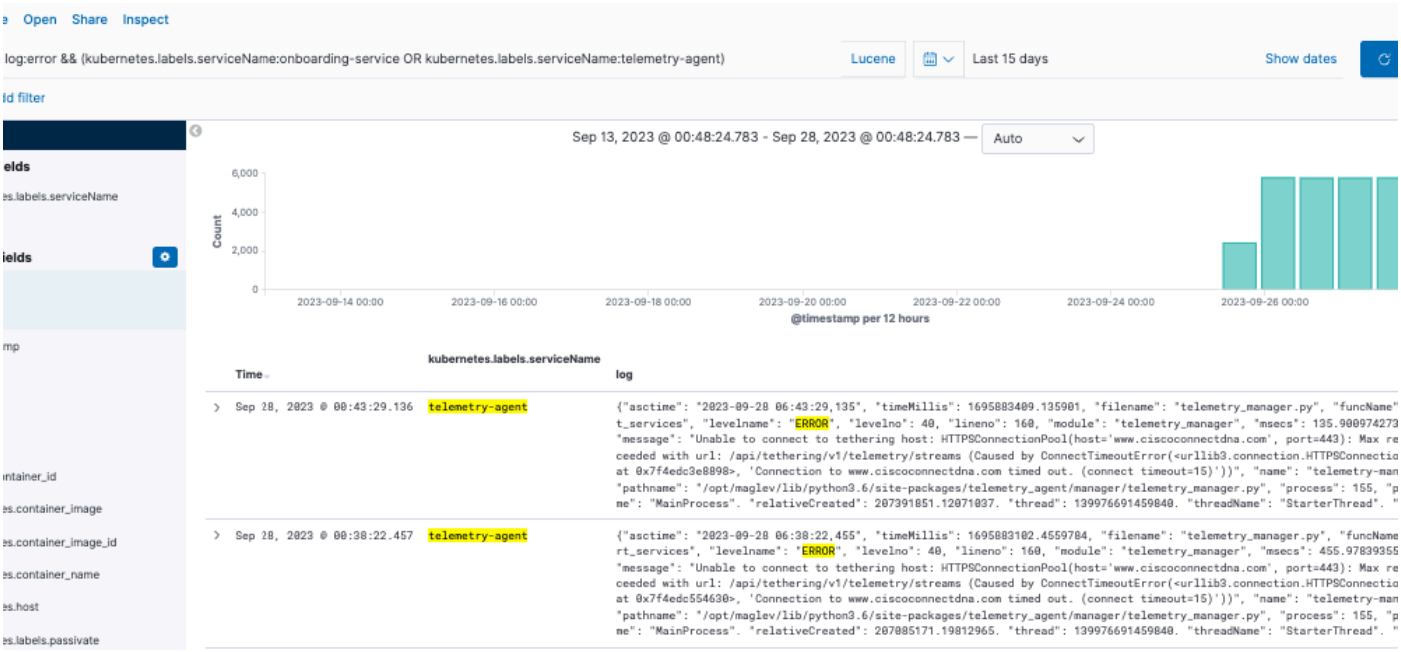


Ricerca di un errore in due servizi diversi contemporaneamente

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).