

Cómo utilizar Kibana en el centro de arquitectura de red digital (DNA)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Antecedentes](#)

[Descripción general de la página web predeterminada de Kibana](#)

[Casos de uso](#)

[Obtenga todos los registros que forman parte del servicio de incorporación.](#)

[Obtener todos los registros que contienen la cadena "error"](#)

[Combinar y hacer coincidir la búsqueda](#)

[Obtener todos los registros de una fecha específica](#)

[Agregar campos a la búsqueda o vista](#)

[Buscar errores de dos servicios diferentes al mismo tiempo](#)

[Referencia](#)

Introducción

Este documento describe cómo utilizar Kibana para buscar mensajes específicos o registros entre los diferentes servicios del Centro de DNA.

Colaborado por Alexandro Carrasquedo, Ingeniero del TAC de Cisco.

Prerequisites

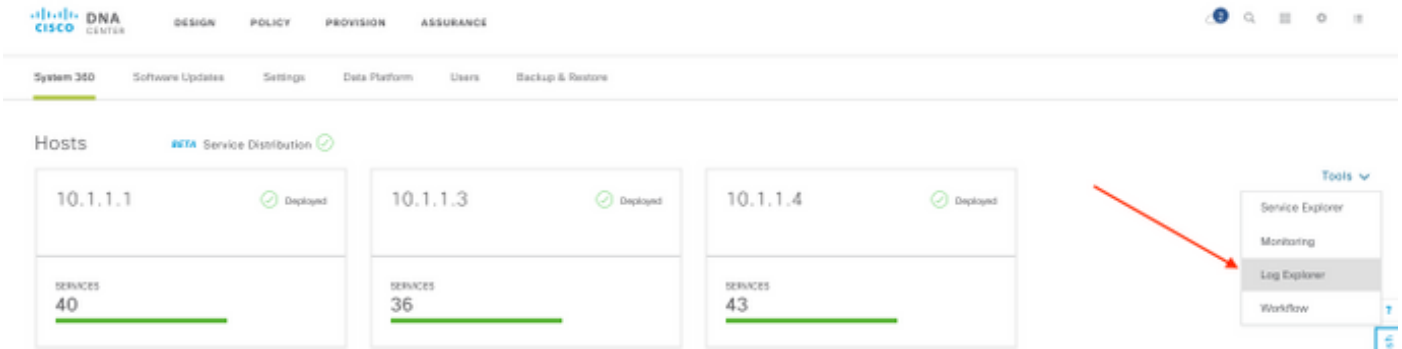
Requirements

- Que se ejecute un clúster del centro de ADN.
- Familiarícese con los nombres y el uso de los servicios del centro de ADN.

Antecedentes

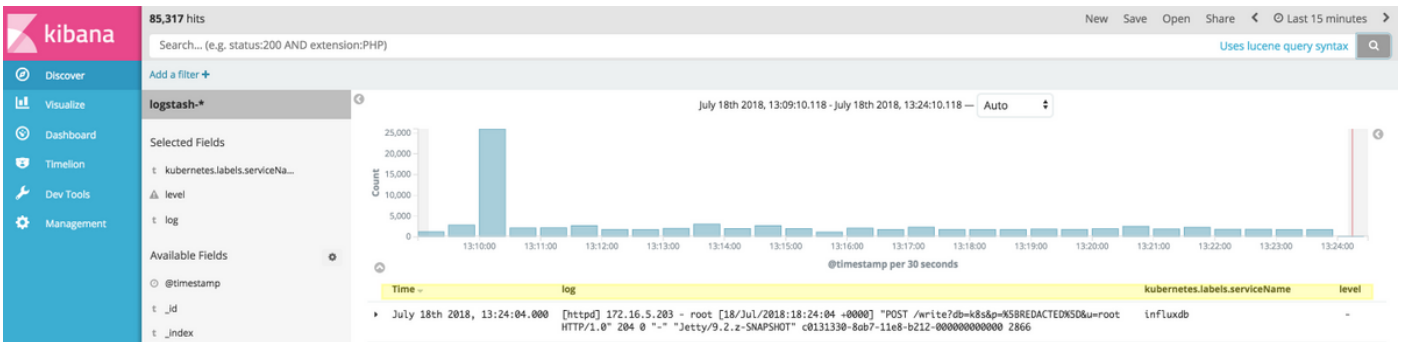
Kibana es un complemento de visualización de datos de código abierto para Elasticsearch. Proporciona capacidades de visualización además del contenido indexado en un clúster de Elasticsearch que están disponibles en el centro DNA. Puede acceder a él de dos maneras:

- <https://<DNA Center ip>/kibana>
- **System Settings -> System 360 -> Tools -> Log Exporter**



Descripción general de la página web predeterminada de Kibana

Kibana tiene varios campos predeterminados, que se resaltan en la siguiente imagen:



- Hora: hora en la que se vio el mensaje.
- Registro: contenido sin procesar del registro.
- Kubernetes.label.serviceName - Servicio que muestra el registro específico.
- Nivel: Urgencia de ese registro específico.

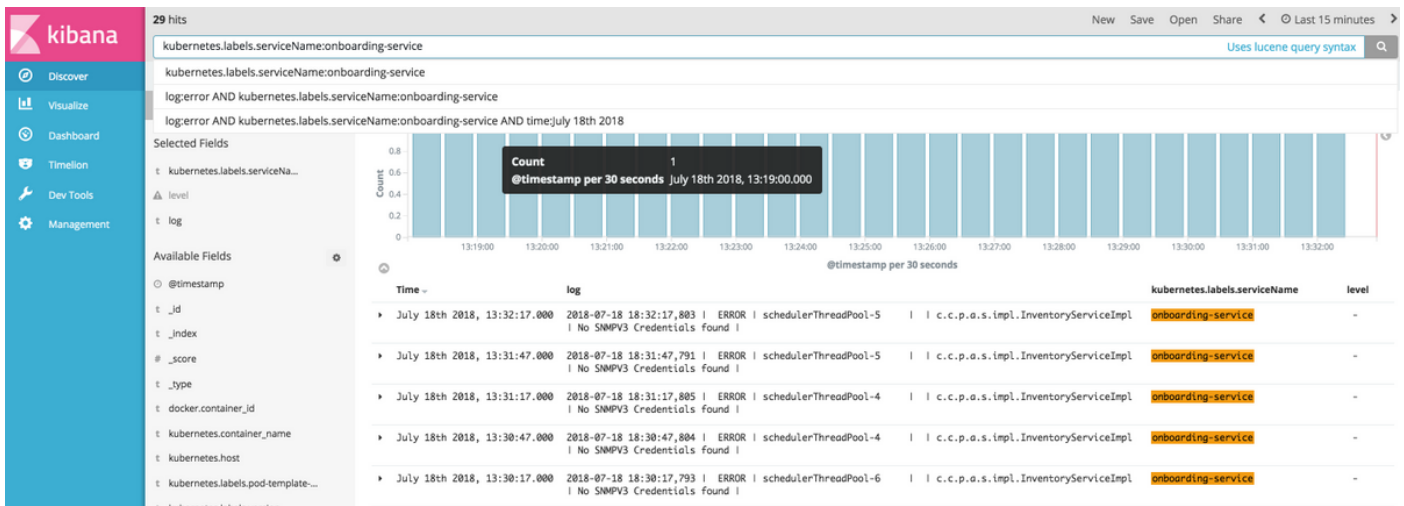
Puede utilizar estos campos para proporcionar un resultado completo que le ayude a diagnosticar problemas dentro del clúster de DNA Center. A continuación se muestran algunos ejemplos de casos prácticos que le ayudarán a empezar con Kibana.

Nota: Este documento proporciona ejemplos de servicios específicos. Sin embargo, puede probar estas búsquedas en los servicios que se ajustan a sus necesidades de resolución de problemas.

Casos de uso

Obtenga todos los registros que forman parte del servicio de incorporación.

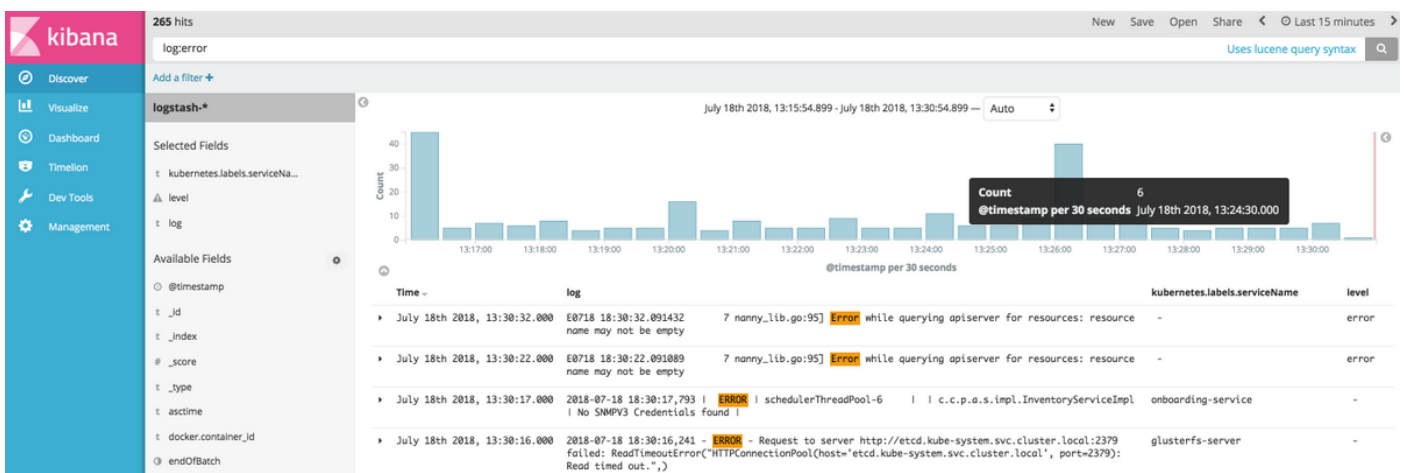
```
kubernetes.labels.serviceName:onboarding-service
```



Obtener todos los registros que contienen la cadena "error"

Consejo: Las entradas de registro más comunes que indican problemas contienen "Error", "Error" y "Excepción", se sienten libres de modificar la cadena para que sea cualquier otra cadena común que pueda guiarle en la resolución de problemas.

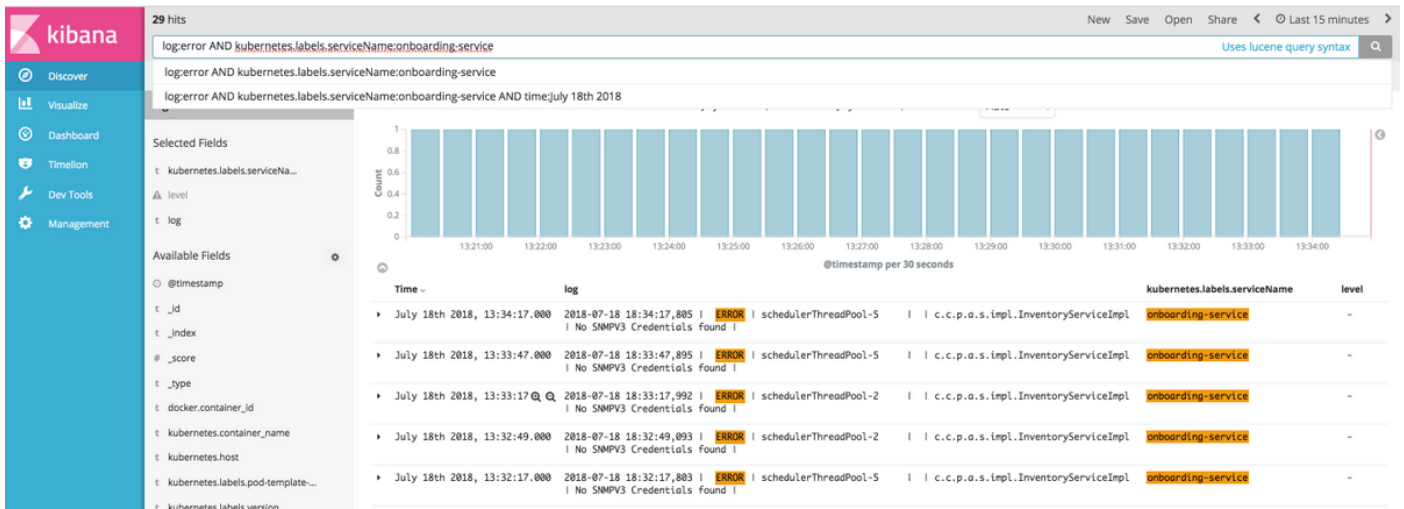
log:error



Combinar y hacer coincidir la búsqueda

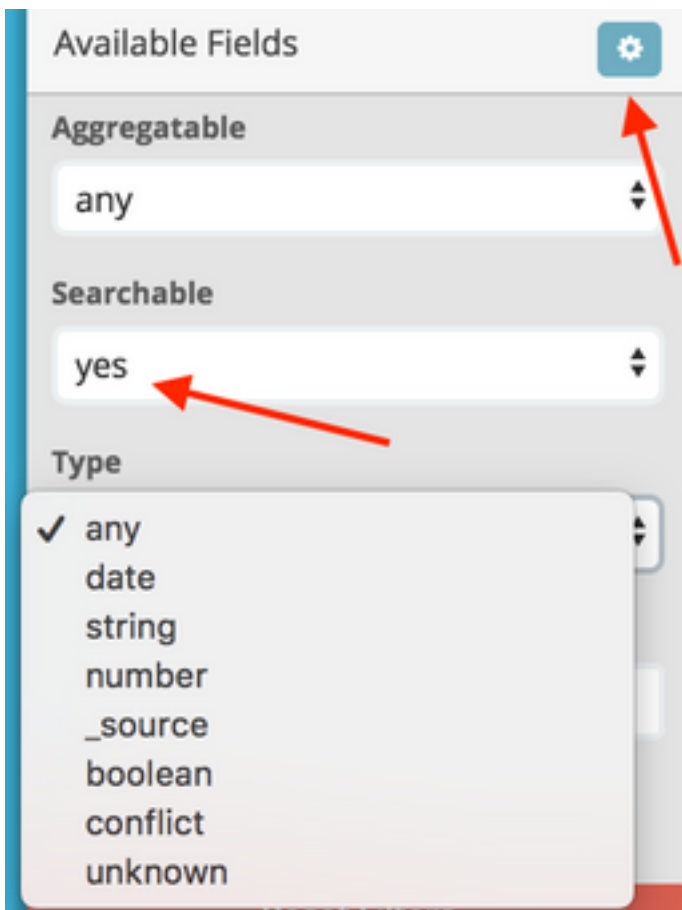
Puede buscar entradas que coincidan con una combinación de cadenas utilizando AND (o &&) entre las cadenas.

log:error **AND** kubernetes.labels.serviceName:onboarding-service



Nota: No se pueden buscar todos los campos.

Si desea ver sólo los campos en los que se puede buscar en el panel Campos disponibles, seleccione la rueda del programa y personalice la vista. También puede definir el tipo de búsqueda que desea utilizar, por ejemplo, cadena, Boolean, número, etc.



Obtener todos los registros de una fecha específica

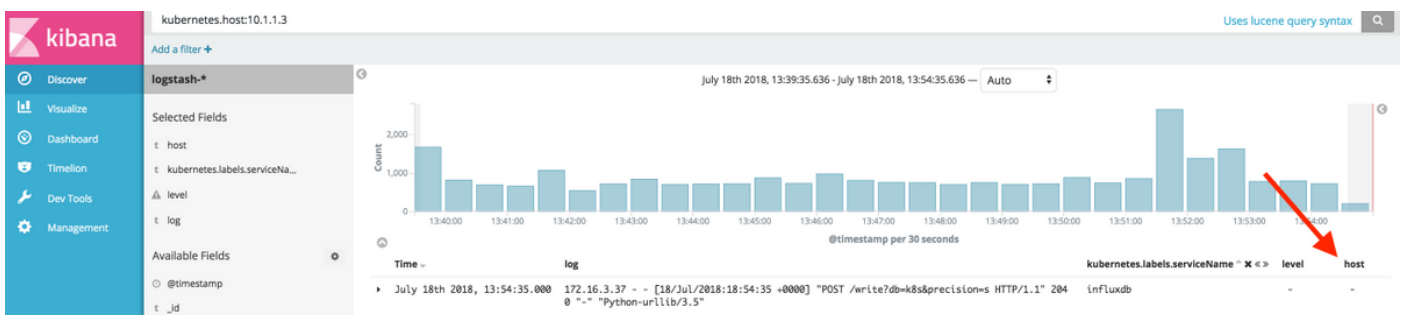
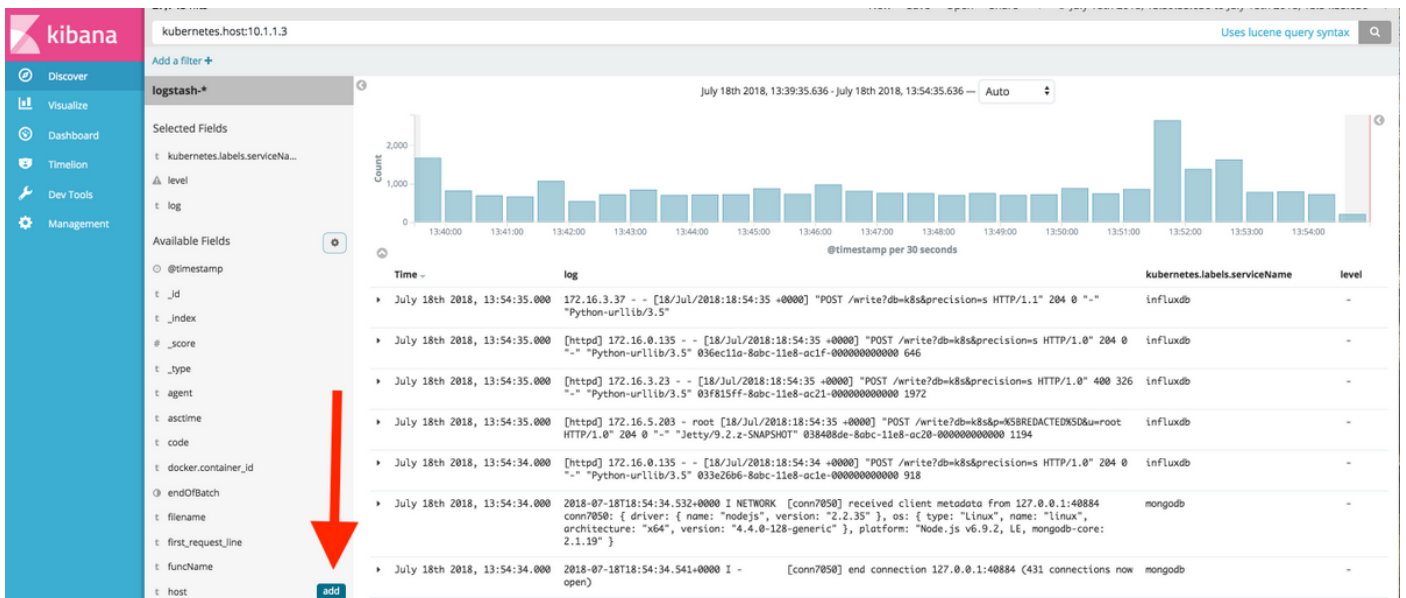
Puede agregar un elemento de tiempo a los criterios de búsqueda. Utilice una de las siguientes opciones del campo Rango de tiempo:



- **Rápido:** desde los últimos X minutos, horas, días o semanas.
- **Relativo:** desde los últimos X minutos, horas, días o semanas hasta una fecha específica.
- **Absoluto:** de una fecha específica a otra fecha específica.

Agregar campos a la búsqueda o vista

Puede agregar más campos a la vista predeterminada para obtener más información sobre sus registros. Vaya al panel Campos disponibles, seleccione Agregar y seleccione los campos que desea mostrar. Después de guardar las selecciones, los campos aparecen en la vista principal.



Buscar errores de dos servicios diferentes al mismo tiempo

Incluya dos o más servicios en los criterios de búsqueda. Asegúrese de que los nombres de los servicios se introducen entre paréntesis y separarlos con **OR**.

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

50 hits New Save Open Share < Last 15 minutes >

log:error && (kubernetes.labels.serviceName:onboarding-service OR kubernetes.labels.serviceName:telemetry-agent) Uses lucene query syntax 🔍

Discover

Visualize

Dashboard

Timeline

Dev Tools

Management

Add a filter +

logstash*

Selected Fields

- t kubernetes.labels.serviceNa...
- ▲ level
- t log

Available Fields

Popular

- t _index
- t kubernetes.host
- @timestamp
- t _id
- # _score
- t _type
- t ascTime
- t docker.container_id
- t exc_info
- t filename
- t funcName
- t kubernetes.container_name
- t kubernetes.labels.pod-template...

| Time | log | kubernetes.labels.serviceName | level |
|------------------------------|--|-------------------------------|-------|
| July 23rd 2018, 09:07:24.000 | 2018-07-23 14:07:24,245 ERROR schedulerThreadPool-3 c.c.p.a.s.impl.InventoryServiceImpl No SNMPV3 Credentials found | onboarding-service | - |
| July 23rd 2018, 09:07:00.000 | {@ascTime": "2018-07-23 14:07:00,743", "timeMillis": 1532354820.7431946, "filename": "telemetry_manager.py", "funcName": "_start_services", "levelName": "ERROR", "levelNo": 40, "lineno": 101, "module": "telemetry_manager", "msecs": 743.194580078125, "message": "Unable to connect to tethering host: You are not authorized to perform this operation", "name": "telemetry-manager", "pathname": "/opt/maglev/lib/python3.5/site-packages/telemetry_agent/manager/telemetry_manager.py", "process": 24, "processName": "MainProcess", "relativeCreated": 438813335.45684814, "thread": 140658652190464, "threadName": "StarterThread", "level": "ERROR", "exc_info": "Traceback (most recent | telemetry-agent | ERROR |
| July 23rd 2018, 09:06:54.000 | 2018-07-23 14:06:54,173 ERROR schedulerThreadPool-4 c.c.p.a.s.impl.InventoryServiceImpl No SNMPV3 Credentials found | onboarding-service | - |
| July 23rd 2018, 09:06:24.000 | 2018-07-23 14:06:24,159 ERROR schedulerThreadPool-4 c.c.p.a.s.impl.InventoryServiceImpl No SNMPV3 Credentials found | onboarding-service | - |
| July 23rd 2018, 09:06:15.000 | {@ascTime": "2018-07-23 14:06:15,644", "timeMillis": 1532354775.6448857, "filename": "telemetry_manager.py", "funcName": "_start_services", "levelName": "ERROR", "levelNo": 40, "lineno": 101, "module": "telemetry_manager", "msecs": 644.805697845459, "message": "Unable to connect to tethering host: You are not authorized to perform this operation", "name": "telemetry-manager", "pathname": "/opt/maglev/lib/python3.5/site-packages/telemetry_agent/manager/telemetry_manager.py", "process": 24, "processName": "MainProcess", "relativeCreated": 438768237.06793785, "thread": 140658652190464, "threadName": "StarterThread", "level": "ERROR", "exc_info": "Traceback (most recent | telemetry-agent | ERROR |

Referencia

- [Opciones comunes de búsqueda elástica](#)
- [Apache Lucene - Sintaxis del analizador de consultas](#)