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

Contenido

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

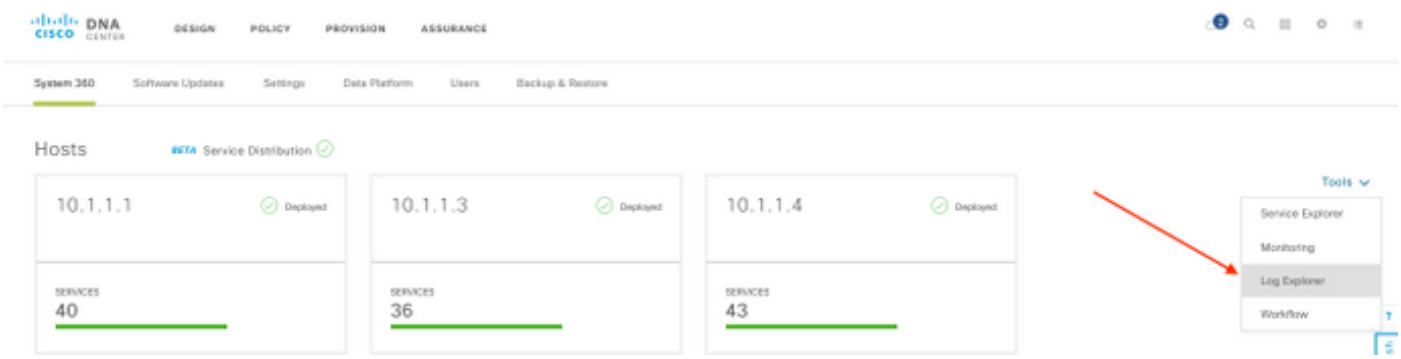
Requirements

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

Antecedentes

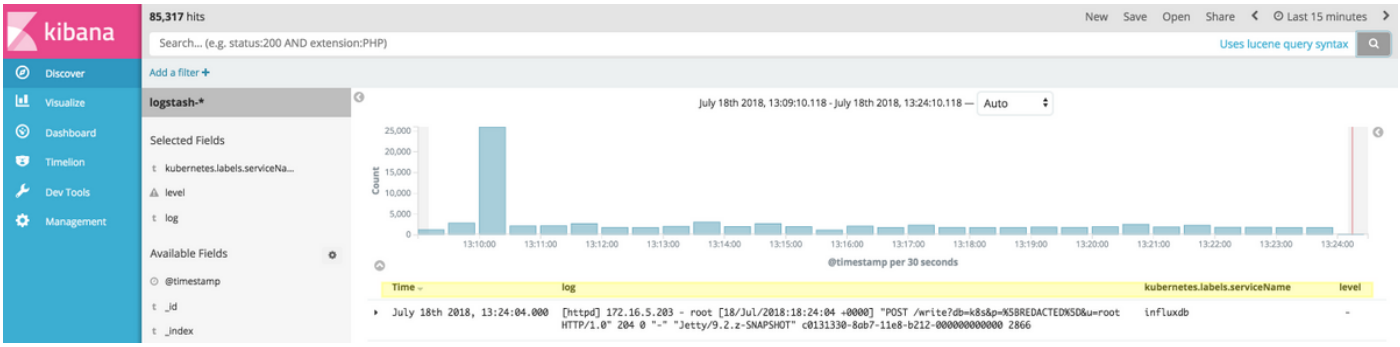
Kibana es un complemento de visualización de datos de código abierto para Elasticsearch. Proporciona capacidades de visualización además del contenido indexado en un clúster de Elasticsearch que están disponibles en el centro DNA. Puede acceder a él de dos maneras:

- **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.**

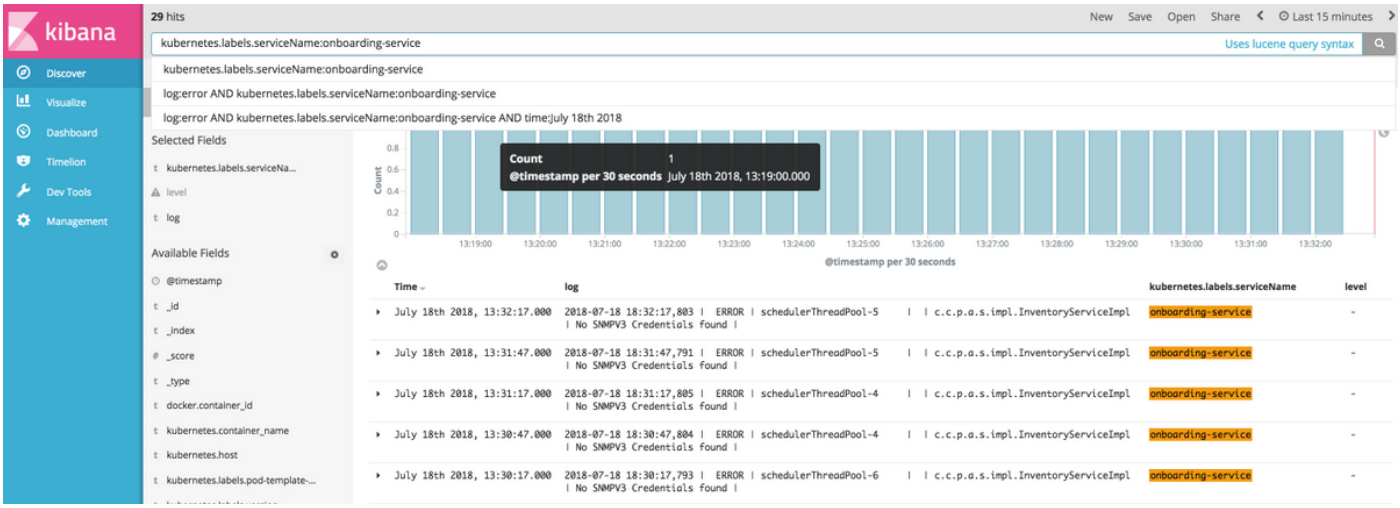
Puede utilizar estos campos para proporcionar un resultado completo que le ayude a diagnosticar problemas dentro del clúster de DNA Center. A continuación se muestran algunos ejemplos de casos prácticos que le ayudarán a empezar con Kibana.

> **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.

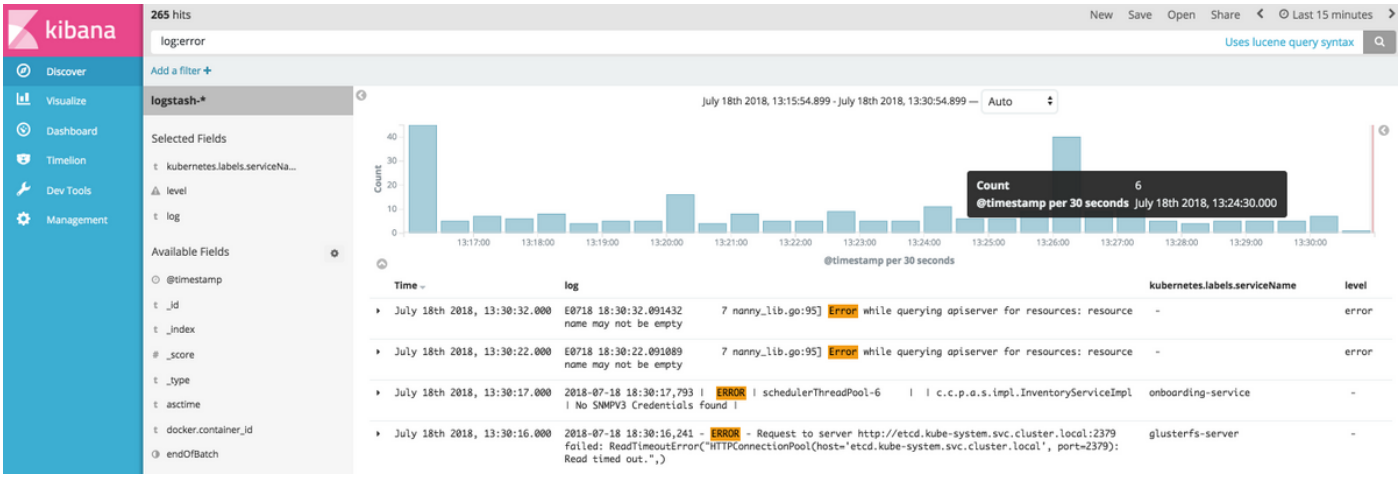
```
kubernetes.labels.serviceName:onboarding-service
```



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.

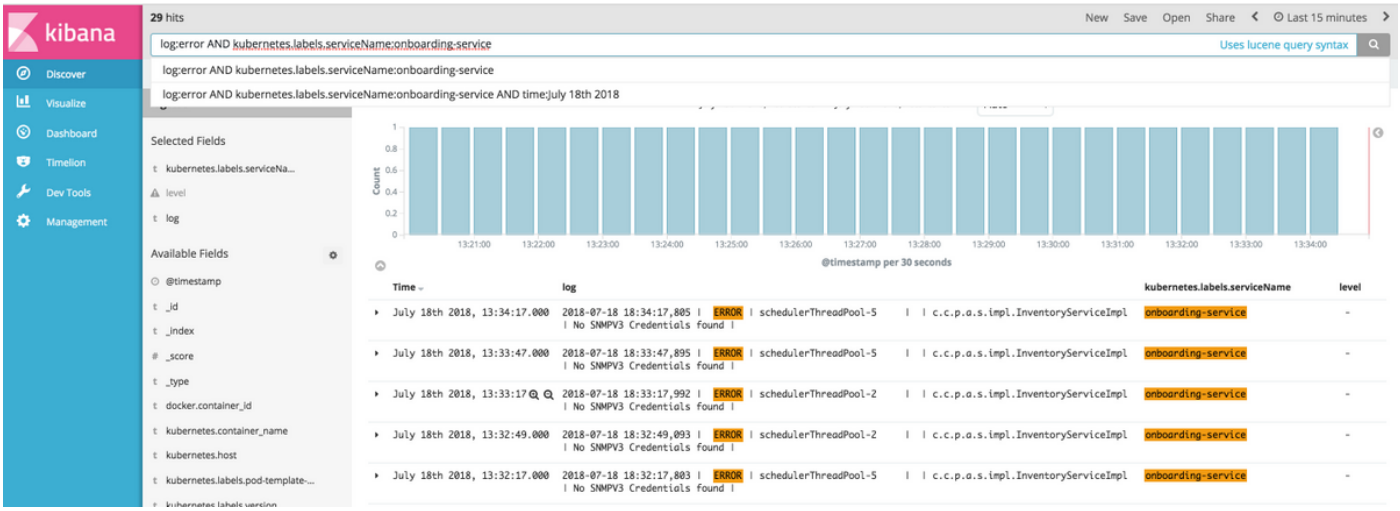
```
log:error
```



Combinar y hacer coincidir la búsqueda

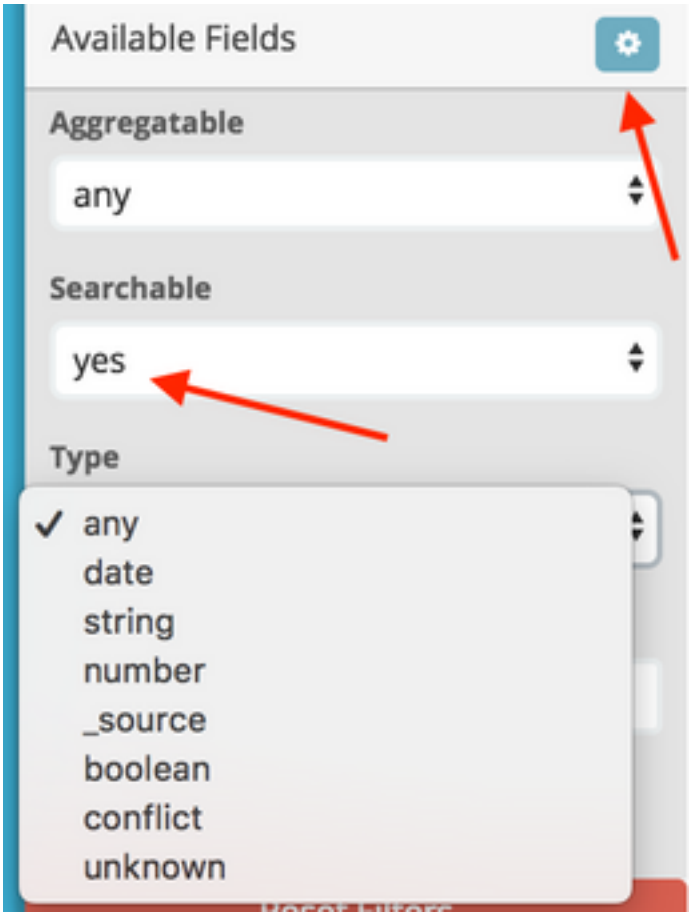
Puede buscar entradas que coincidan con una combinación de cadenas utilizando AND (o &&) entre las cadenas.

```
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.



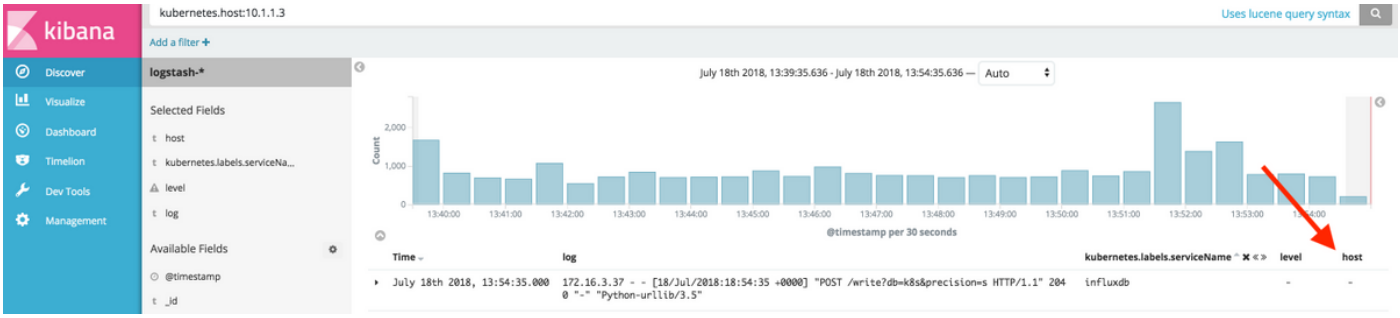
Obtener todos los registros de una fecha específica

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)
```

Referencia

- Opciones comunes de búsqueda elástica
- Apache Lucene - Sintaxis del analizador de consultas