Comprensión de Log Analytics-ELK Stack en ISE

Contenido

Introducción

Este documento describe los componentes de la pila ELK incorporados desde Cisco Identity Services Engine (ISE) 3.3 hasta el análisis de registro de System 360.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Identity Service Engine
- Pila ELK

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ISE 3.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

System 360 incluye Monitoring y Log Analytics.

La **función Supervisión** permite supervisar una amplia gama de estadísticas de aplicaciones y sistemas, así como los indicadores clave de rendimiento (KPI) de todos los nodos de una implementación desde una consola centralizada. Los KPI son útiles para obtener información sobre el estado general del entorno de nodos. Las estadísticas ofrecen una representación simplificada de las configuraciones del sistema y los datos específicos de la utilización.

Log Analytics proporciona un sistema de análisis flexible para el análisis en profundidad de la autenticación, autorización y contabilidad (AAA) de terminales, y la creación de perfiles de los datos de syslog. También puede analizar el resumen de estado de Cisco ISE y los estados de los procesos. Puede generar informes similares a los informes de contadores y resumen de estado de Cisco ISE.

Pila ELK

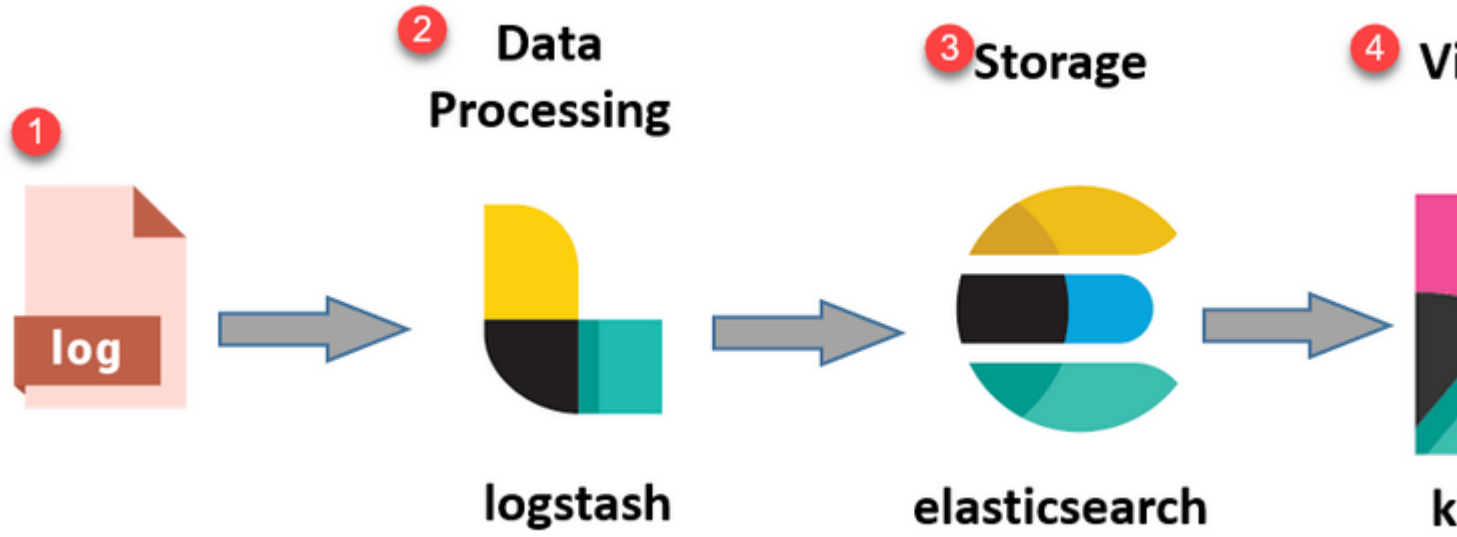
La pila ELK es una popular pila de software de código abierto utilizada para recopilar, procesar y visualizar grandes volúmenes de datos. Significa Elasticsearch, Logstash y Kibana.

- **Elasticsearch**: Elasticsearch es un motor de búsqueda y análisis distribuido. Está diseñado para almacenar, buscar y analizar grandes volúmenes de datos de forma rápida y casi en tiempo real. Utiliza un lenguaje de consulta basado en JSON y es muy escalable.

- **Logstash**: Logstash es una canalización de procesamiento de datos que ingiere, procesa y transforma datos de varios orígenes. Puede analizar y enriquecer los datos, haciéndolos más estructurados y adecuados para el análisis. Logstash admite una amplia gama de fuentes de entrada y destinos de salida.

- **Kibana**: Kibana es una plataforma de visualización de datos que funciona con Elasticsearch. Permite a los usuarios crear paneles interactivos, gráficos y visualizaciones para explorar y comprender los datos almacenados en Elasticsearch. La interfaz de Kibana facilita la consulta y visualización de datos.

Cuando se combinan, estos componentes forman una potente pila para gestionar y analizar diversos tipos de datos, desde archivos de registro hasta métricas y mucho más, a la vez que proporcionan funciones de visualización para dar sentido a la información.

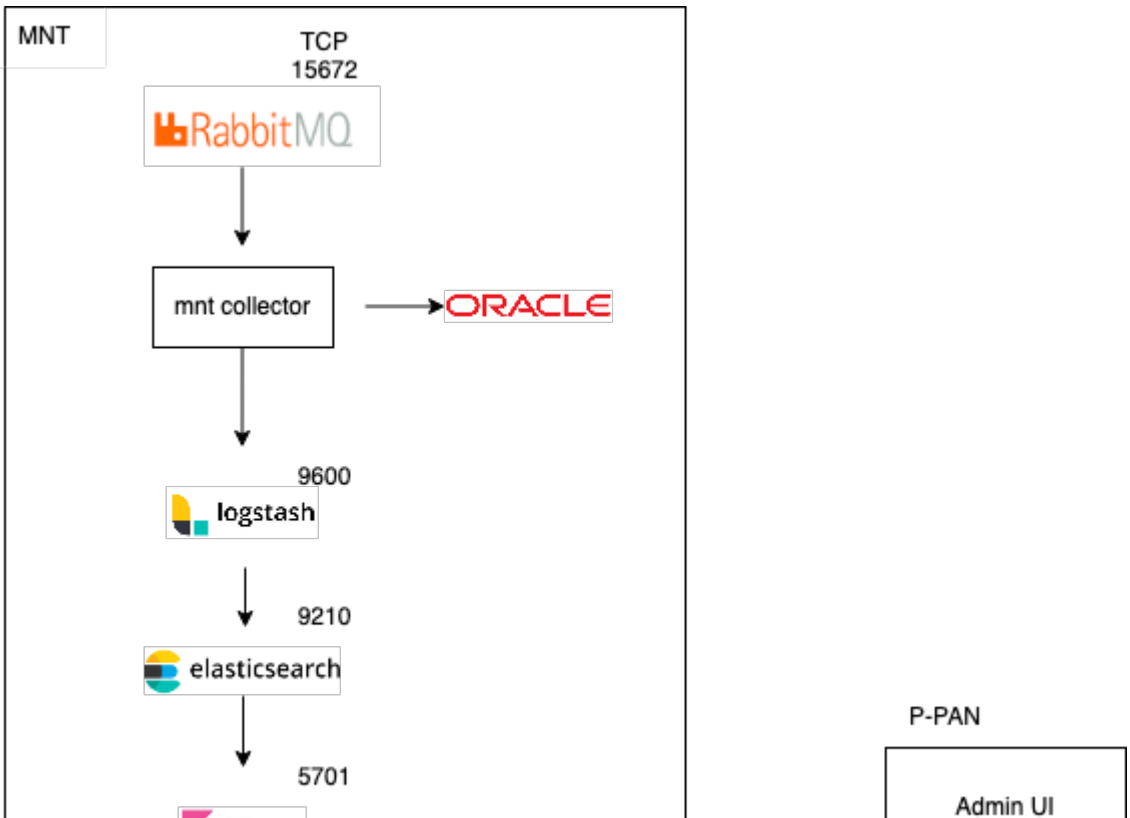


Flujo de pila ELK

Análisis de la pila ELK como registro

- Una instancia independiente de la pila ElasticSearch+LogStash+Kibana se está ejecutando sólo en nodos MnT.
  - Esto no tiene ninguna correlación con la Elastic Search of Context-Visibility.
  - Ejecución de ELK 7.17

- Los TMN primarios y secundarios tienen sus propias instancias separadas de ELK.
  - Kibana está habilitado solo en MNT secundario si está disponible, mostrando datos solo de este nodo.
- El análisis de registros está desactivado de forma predeterminada.
- Consume recursos de Oracle.
- Almacena un máximo de 7 días de datos.
- El tamaño total de los datos consumidos por Log Analytics está restringido a 10 GB.
  - Una vez alcanzado cualquiera de los límites, ElasticSearch purga los datos.



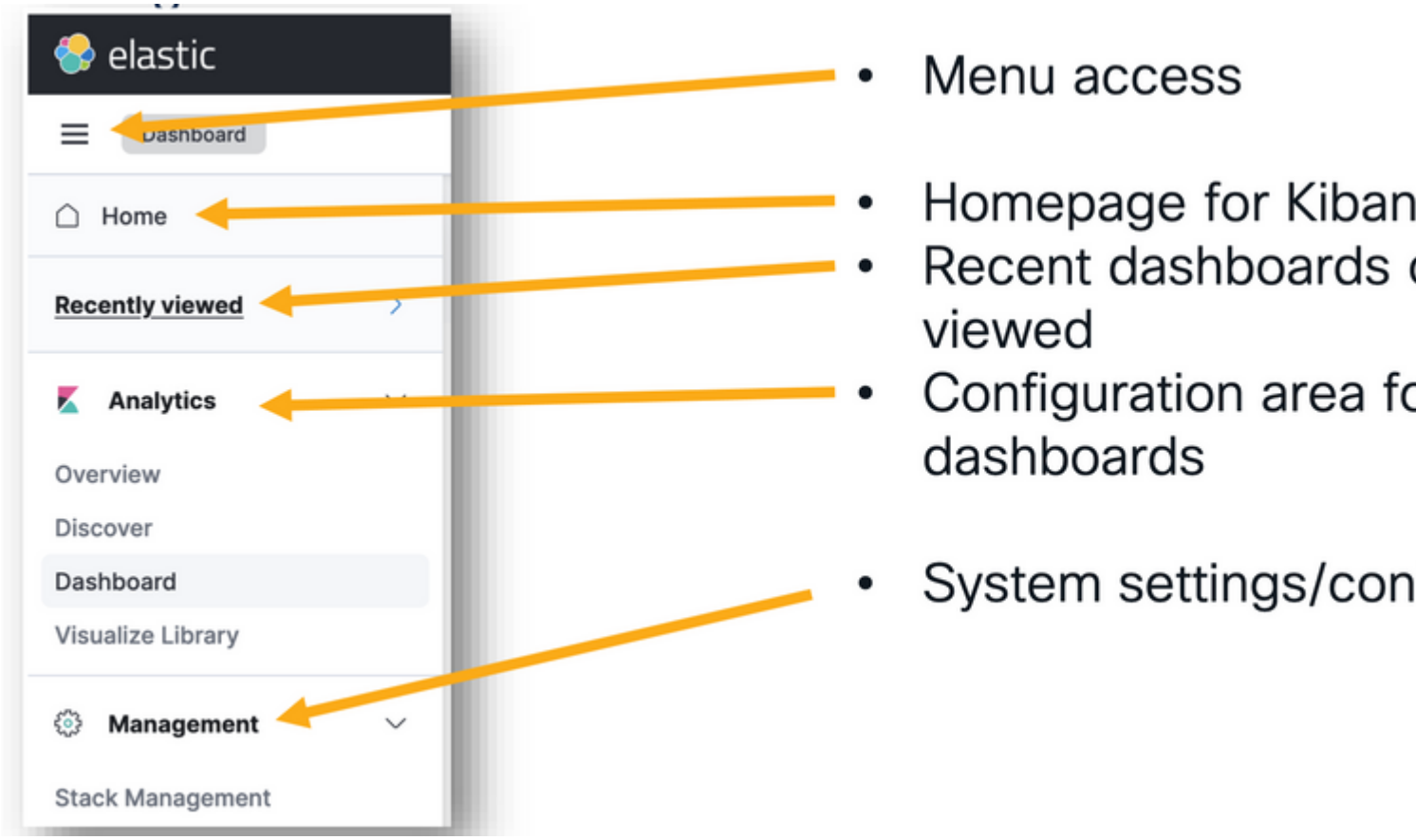
ISE Logstash Service running 614339

ISE Kibana Service running 616064

ISE Native IPSec Service running 75883
MFC Profiler running 651910

Menú de navegación

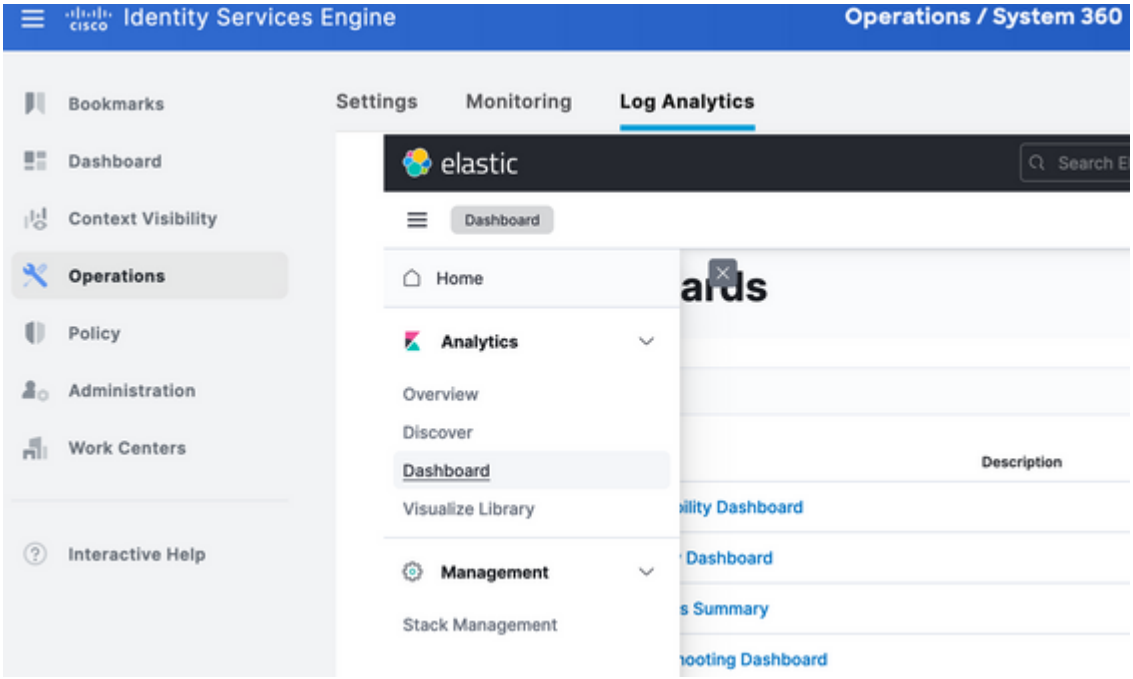
Una vez iniciados los servicios ELK, ahora tendrá acceso al menú de navegación Elastic (Elástico).



Menú de navegación

Paneles integrados.

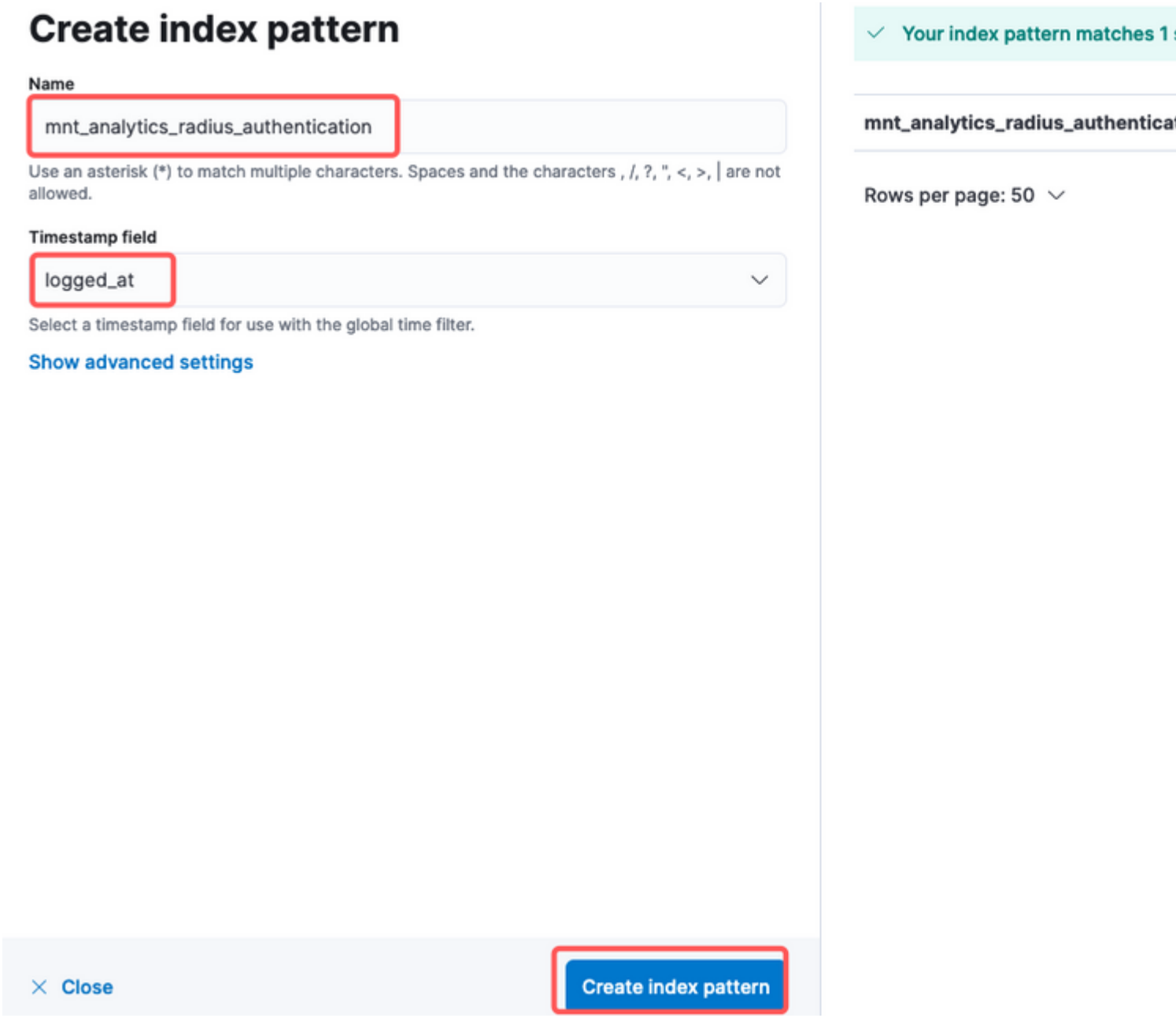
- ISE incorpora de forma predeterminada paneles con datos de Radius, TACAC, rendimiento del sistema y observabilidad de ISE.
- Se puede acceder a estos paneles accediendo a Operations>Log Analytics.
  - Una vez que esté abierta la interfaz de usuario elástica, haga clic en el menú intercalado >Análisis>Paneles.



Paneles integrados.

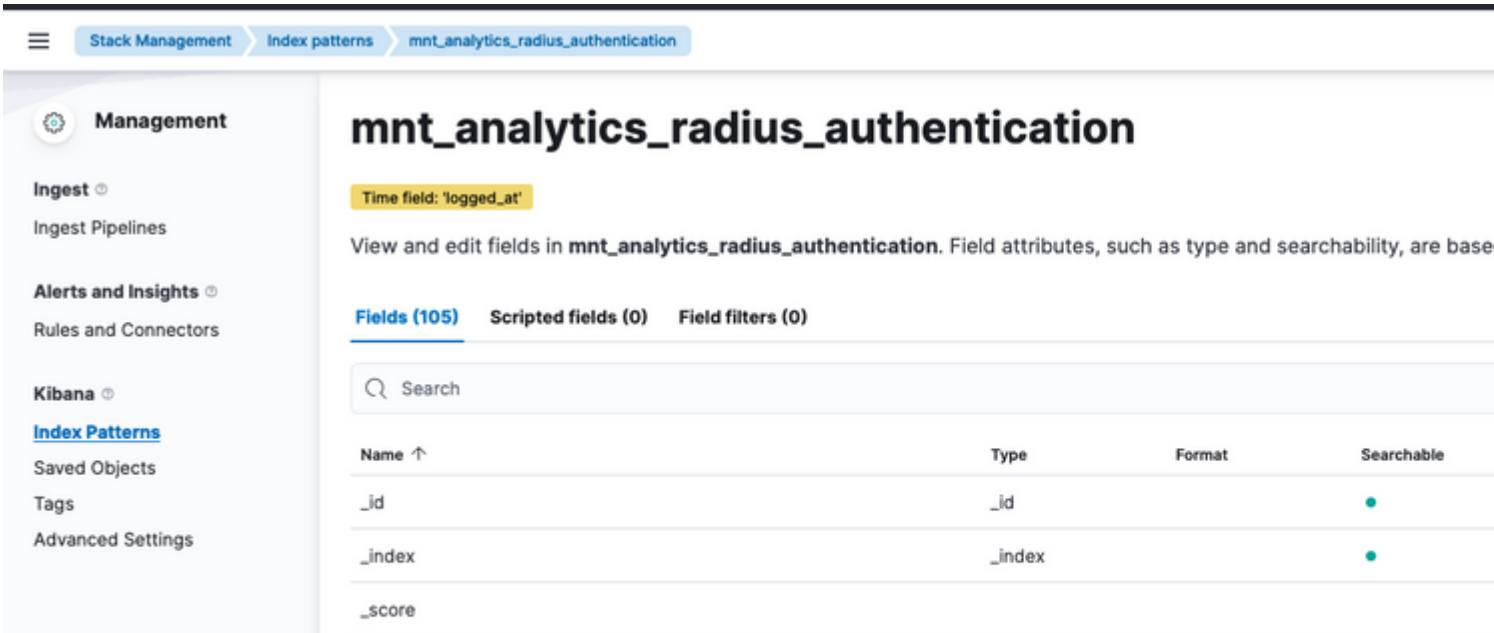
- Paneles disponibles en ISE 3.3

- Seleccione el campo Timestamp, logging_at, logging_at_timezone o "No deseo utilizar el filtro de tiempo".
- A continuación, haga clic en "Crear patrón de índice".



Seleccionar índice

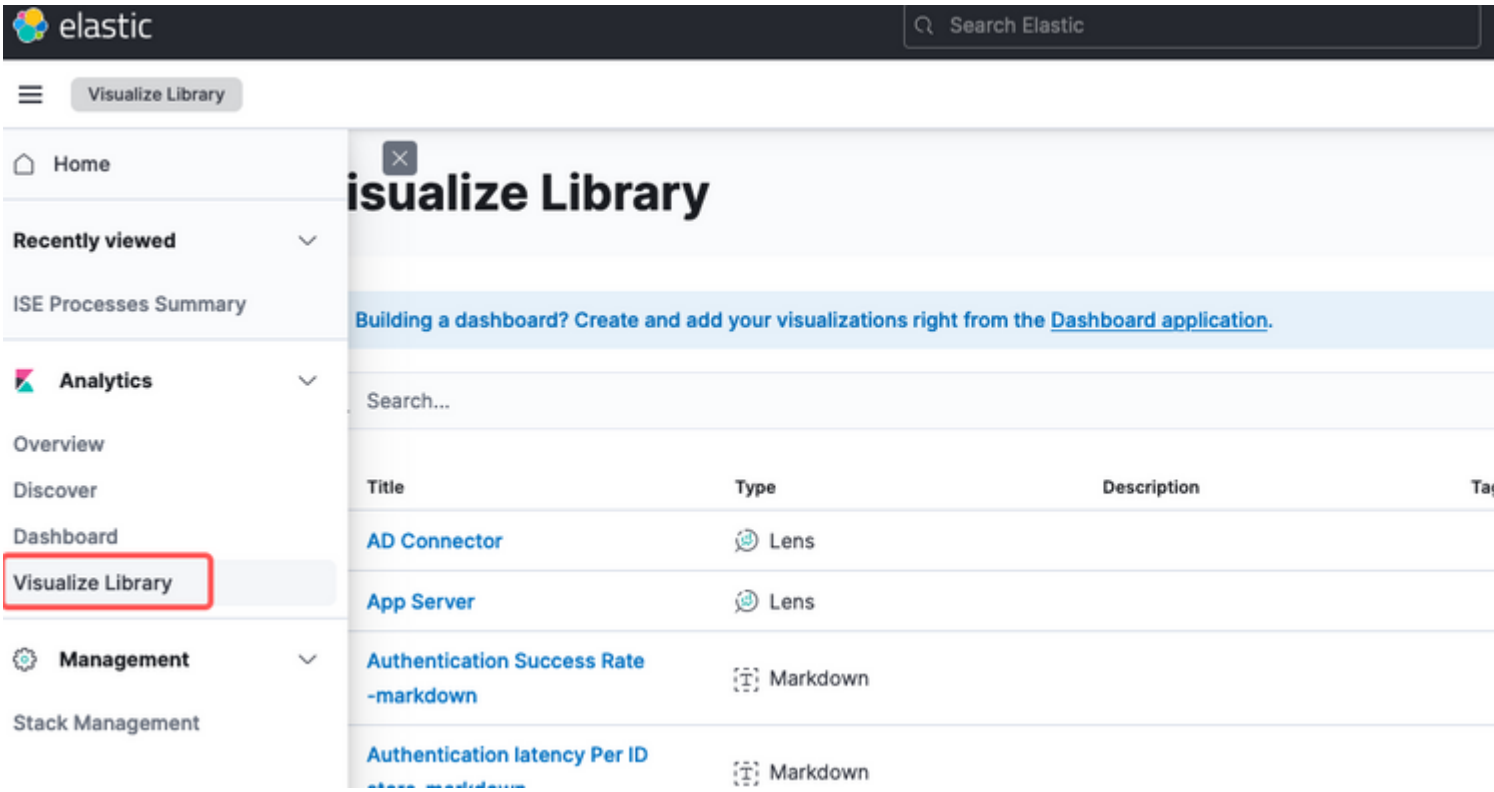
Una vez creado, el índice muestra todas las variables asociadas que se pueden utilizar más adelante para crear visualizaciones.



: muestran datos en barras verticales, lo que facilita la comparación de valores entre categorías o intervalos de tiempo.

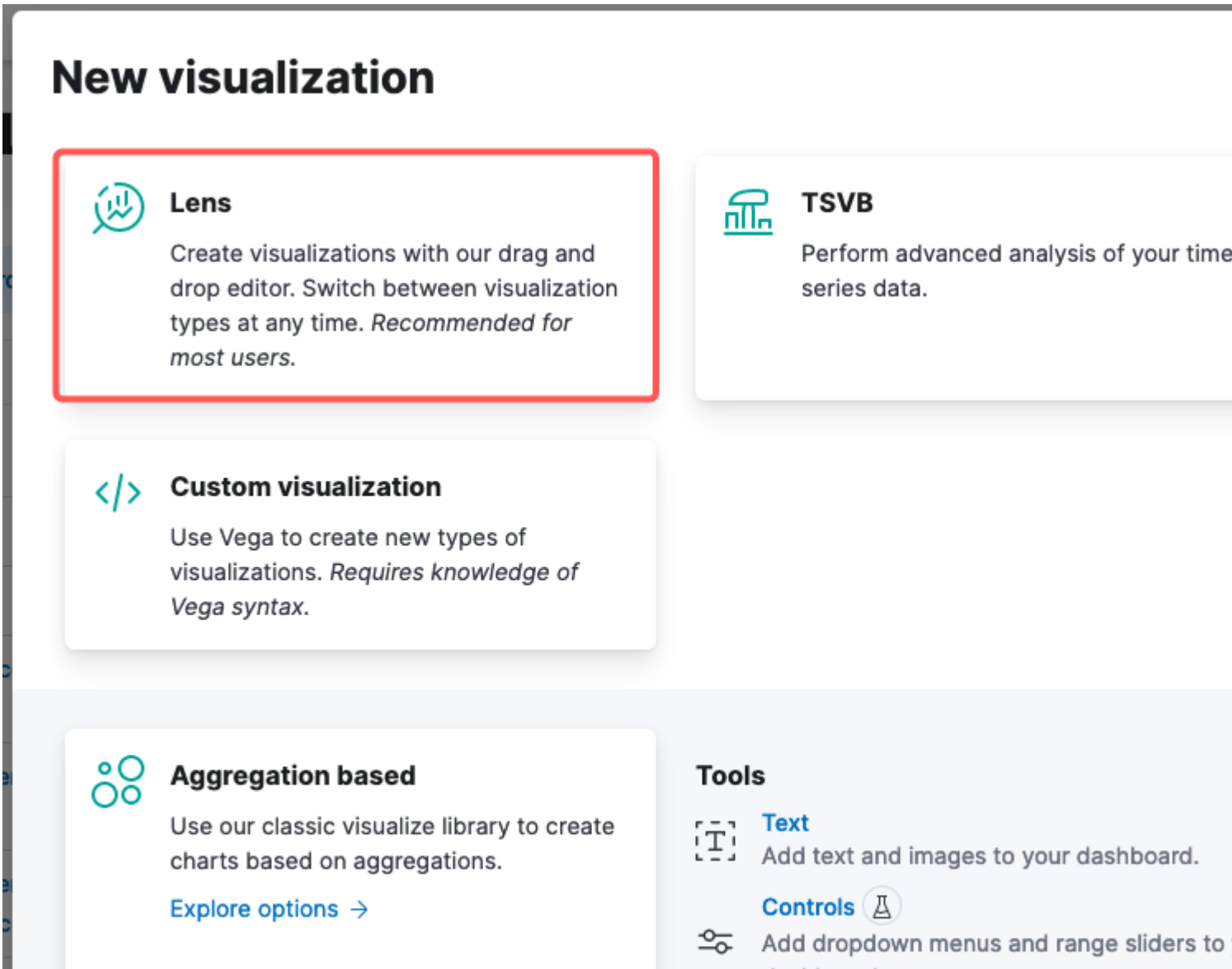
- **Gráficos de líneas**: los gráficos de líneas muestran los datos como una serie de puntos de datos conectados por líneas. Son útiles para visualizar tendencias a lo largo del tiempo.
- **Gráficos circulares**: los gráficos circulares representan datos en un gráfico circular, en el que cada segmento del gráfico circular representa una categoría y el tamaño del segmento indica su proporción.
- **Gráficos de área**: de forma similar a los gráficos de líneas, los gráficos de área también muestran tendencias a lo largo del tiempo, pero rellenan el área debajo de las líneas, lo que facilita la visualización de la magnitud de los cambios.
- **Mapas de calor**: Los mapas de calor utilizan colores para representar valores de datos en una matriz o cuadrícula. Son útiles para mostrar concentraciones o variaciones en los datos.
- **Visualizaciones de Métricas**: Muestran valores numéricos únicos, como recuentos o promedios. A menudo se utilizan para mostrar indicadores clave de rendimiento (KPI).
- **Tablas de datos**: las tablas de datos presentan datos sin formato en forma de tabla, lo que le permite ver información detallada y ordenar o filtrar los datos.
- **Histogramas**: Los histogramas dividen los datos en contenedores o intervalos y muestran la frecuencia o el recuento de puntos de datos en cada contenedor. Resultan útiles para comprender las distribuciones de datos.
- **Mapas de coordenadas**: visualizan datos geoespaciales, lo que le permite mostrar datos en un mapa y utilizar varios marcadores, colores o tamaños para representar atributos de datos.
- **Nubes de etiquetas**: las nubes de etiquetas muestran frecuencias de palabras, con el tamaño de cada palabra que indica su importancia o frecuencia en un conjunto de datos.

Navegue hasta Análisis>Visualizar biblioteca y haga clic en "Crear visualización".



Crear visualización

Seleccione la visualización de su preferencia, en este ejemplo se prefiere la lente para la práctica.



: en el panel izquierdo, puede seleccionar el origen de datos o el patrón de índice de Elastic Search que desea utilizar para la visualización.

- **Lienzo de visualización**: el área central es donde se crea la visualización arrastrando y soltando campos, seleccionando tipos de gráficos y configurando la configuración del gráfico.
- **Barra de herramientas de visualización**: encima del lienzo, puede encontrar una barra de herramientas que le permite personalizar su visualización, incluidas opciones para cambiar los tipos de gráficos, agregar filtros y configurar las opciones del gráfico.

- **Panel de datos**: en el lado derecho, puede acceder al panel "Datos", que le permite administrar la transformación de datos, la agregación y la configuración de campo.

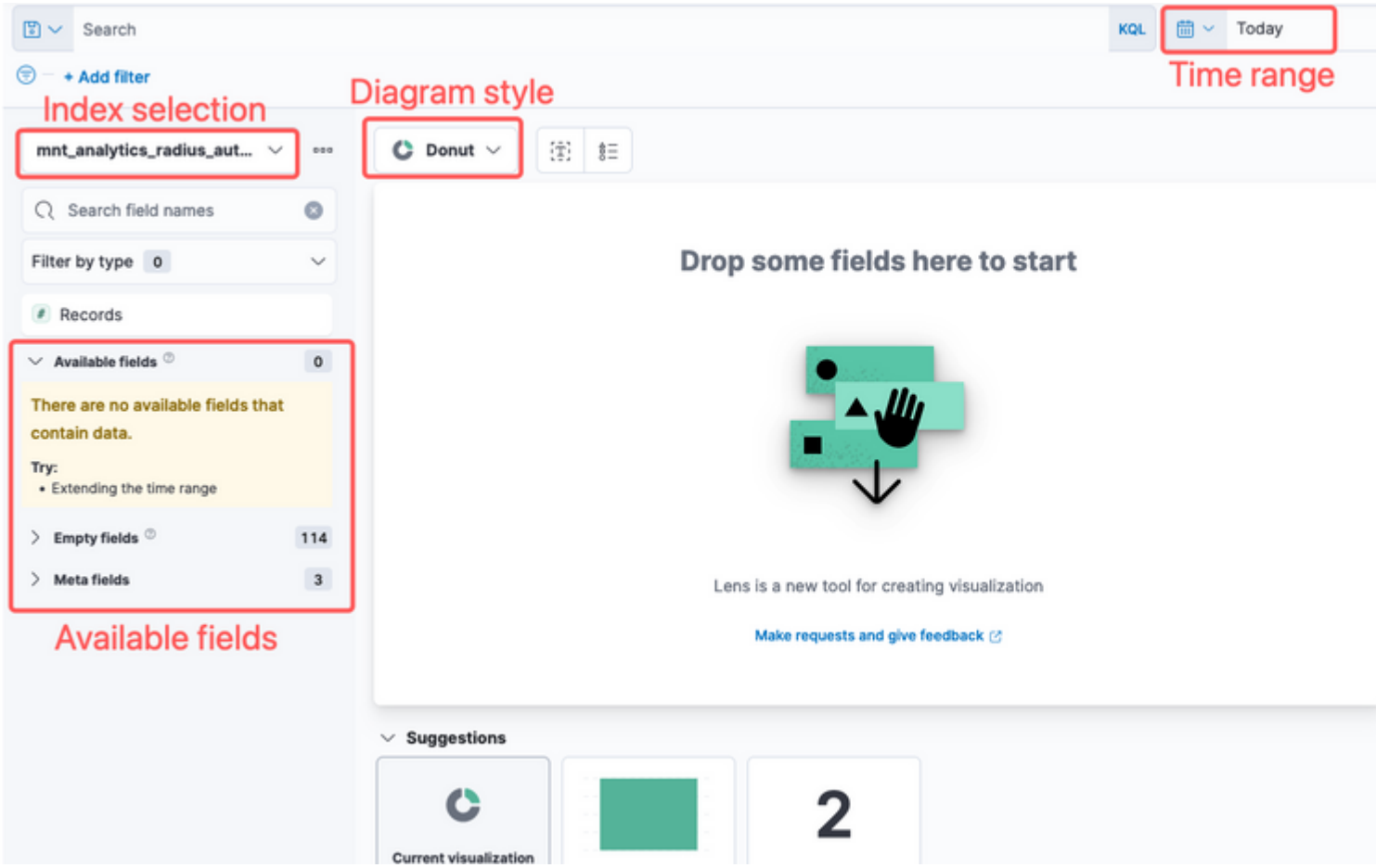
- **Administración de capas**: en función del tipo de visualización que esté creando (por ejemplo, gráficos de capas), puede tener un área de administración de capas para configurar varias capas en la visualización.

- **Vista previa:** A medida que realiza cambios en la visualización, normalmente se proporciona una vista previa en tiempo real para que pueda ver el aspecto del gráfico con la configuración actual**.**

- **Configuración de visualización**: en función del tipo de gráfico seleccionado, puede acceder a la configuración específica de ese tipo de visualización, como la configuración de ejes, las combinaciones de colores y las etiquetas.

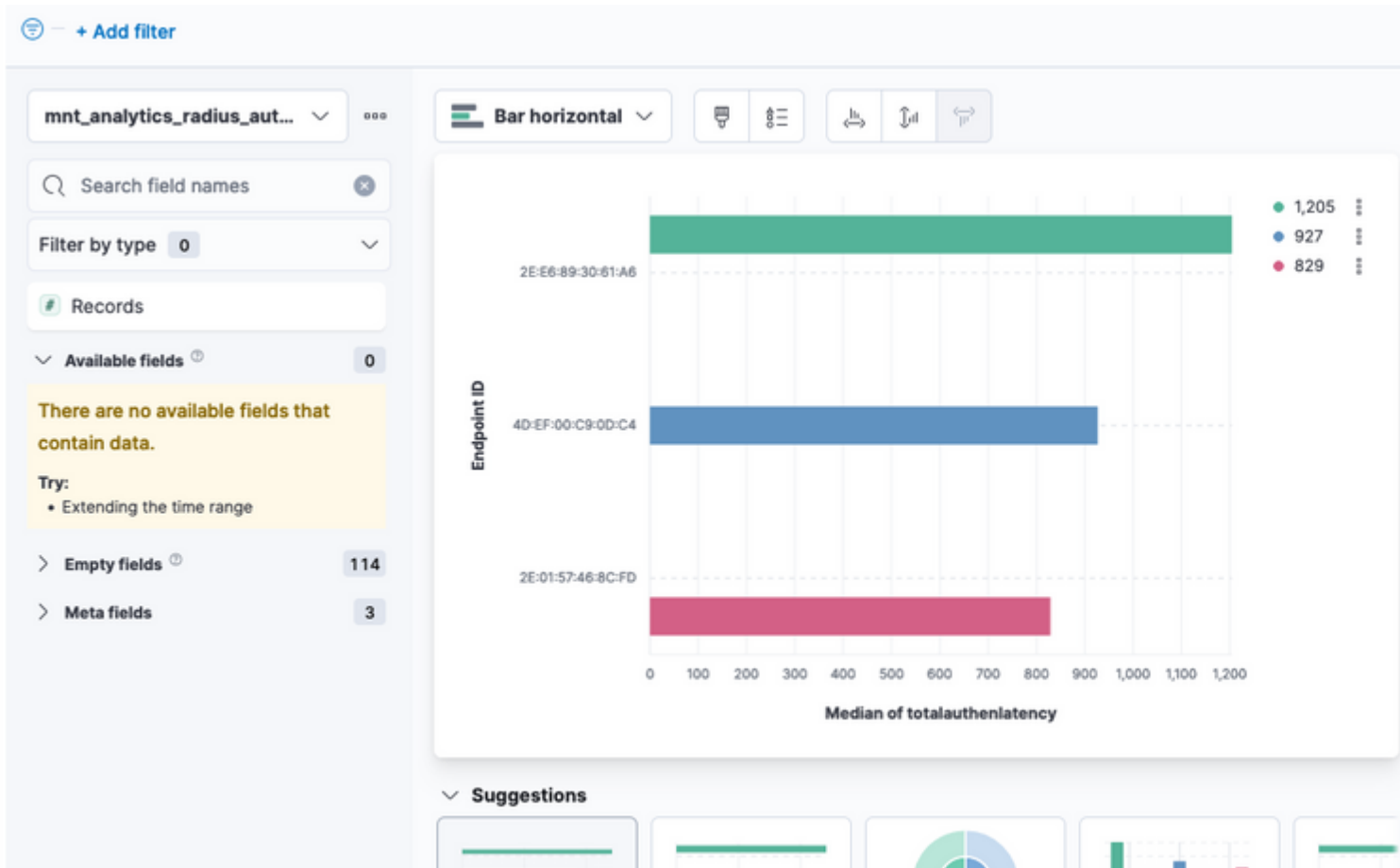
- **Configuración de interactividad**: puedes añadir interacciones y acciones a tu visualización, permitiendo a los usuarios filtrar datos o navegar a otras partes de tus tableros de Kibana.

- **Guardar y compartir**: en la parte superior de la interfaz del objetivo, normalmente hay opciones para guardar la visualización, agregarla a un panel o compartirla con otros usuarios.



Visualización del objetivo

Debido al ID de bug de Cisco CSCwh48057, el panel izquierdo no muestra los campos disponibles para utilizar. Sin embargo, desde el lado derecho puede seleccionar los campos requeridos más el estilo del diagrama. En este ejemplo, dado que la latencia de autenticación es un tema de interés común, el gráfico se construye para visualizar la latencia de autenticación frente a la identificación del terminal.



```
admin#show logging application ise-logstash/logstash.log
admin#show logging application mnt-la-elasticsearch/mnt-la-elasticsearch.log
```

Información Relacionada

Guía de administración de ISE 3.3

Documentación de Kibana

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).