Entender a análise de log - Pilha ELK no ISE

Contents

Introdução

Este documento descreve os componentes da pilha ELK integrados ao Cisco Identity Services Engine (ISE) 3.3 através da análise de log do System 360.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Identity Service Engine
- Pilha ELK

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ISE 3.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O System 360 inclui Monitoring e Log Analytics.

O **recurso Monitoramento** permite monitorar uma ampla gama de estatísticas de aplicativos e do sistema, além dos indicadores-chave de desempenho (KPI) de todos os nós em uma implantação a partir de um console centralizado. Os KPIs são úteis para obter informações sobre a integridade geral do ambiente do nó. As estatísticas oferecem uma representação simplificada das configurações do sistema e dos dados específicos de utilização.

O Log Analytics fornece um sistema de análise flexível para análise detalhada de autenticação, autorização e contabilização (AAA) de endpoint e dados de syslog de criação de perfil. Você também pode analisar o resumo de integridade do Cisco ISE e os status do processo. Você pode gerar relatórios semelhantes ao relatório Contadores e Resumo da integridade do Cisco ISE.

Pilha ELK

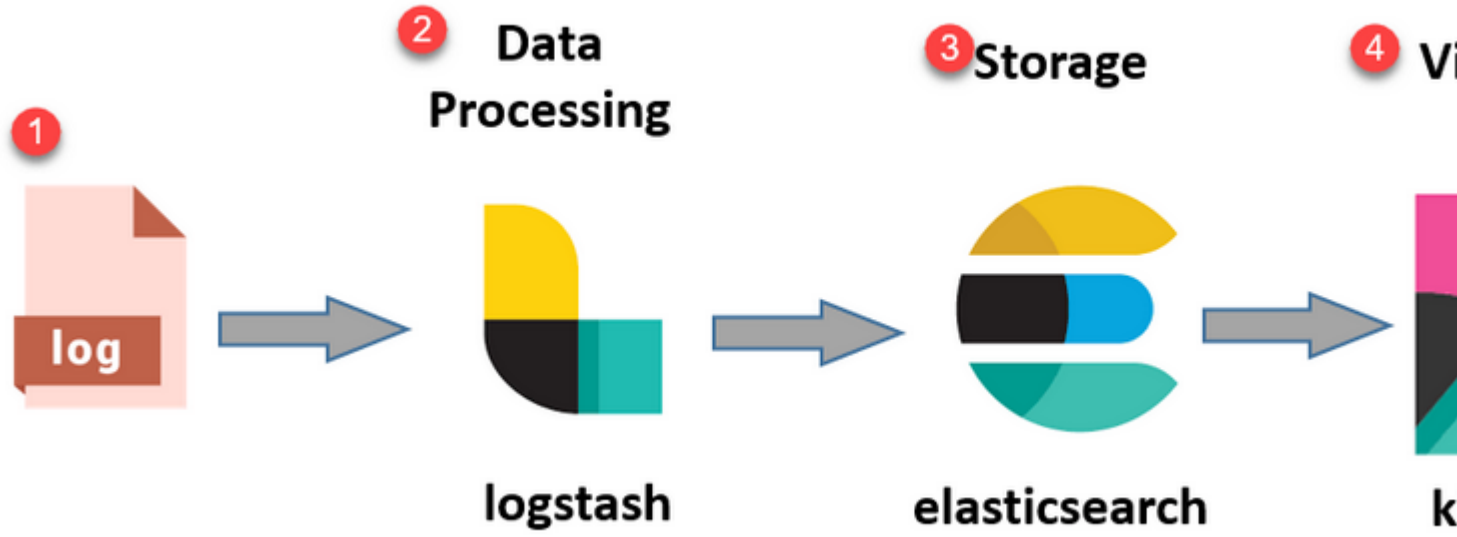
A Pilha ELK é uma pilha de software de código aberto popular usada para coletar, processar e visualizar grandes volumes de dados. Ele significa Elasticsearch, Logstash e Kibana.

- **Elasticsearch**: Elasticsearch é um mecanismo de pesquisa e análise distribuído. Ele foi projetado para armazenar, pesquisar e analisar grandes volumes de dados rapidamente e quase em tempo real. Ele usa uma linguagem de consulta baseada em JSON e é altamente escalável.

- **Logstash**: Logstash é um pipeline de processamento de dados que absorve, processa e transforma dados de várias fontes. Ele pode analisar e enriquecer dados, tornando-os mais estruturados e adequados para análise. O Logstash suporta uma grande variedade de fontes de entrada e destinos de saída.

- **Kibana**: Kibana é uma plataforma de visualização de dados que funciona com Elasticsearch. Ele permite que os usuários criem painéis, gráficos, gráficos e visualizações interativos para explorar e entender os dados armazenados no Elasticsearch. A interface do Kibana facilita a consulta e a visualização de dados.

Quando combinados, esses componentes formam uma pilha poderosa para gerenciar e analisar diversos tipos de dados, de arquivos de log a métricas e muito mais, enquanto fornecem recursos de visualização para dar sentido às informações.

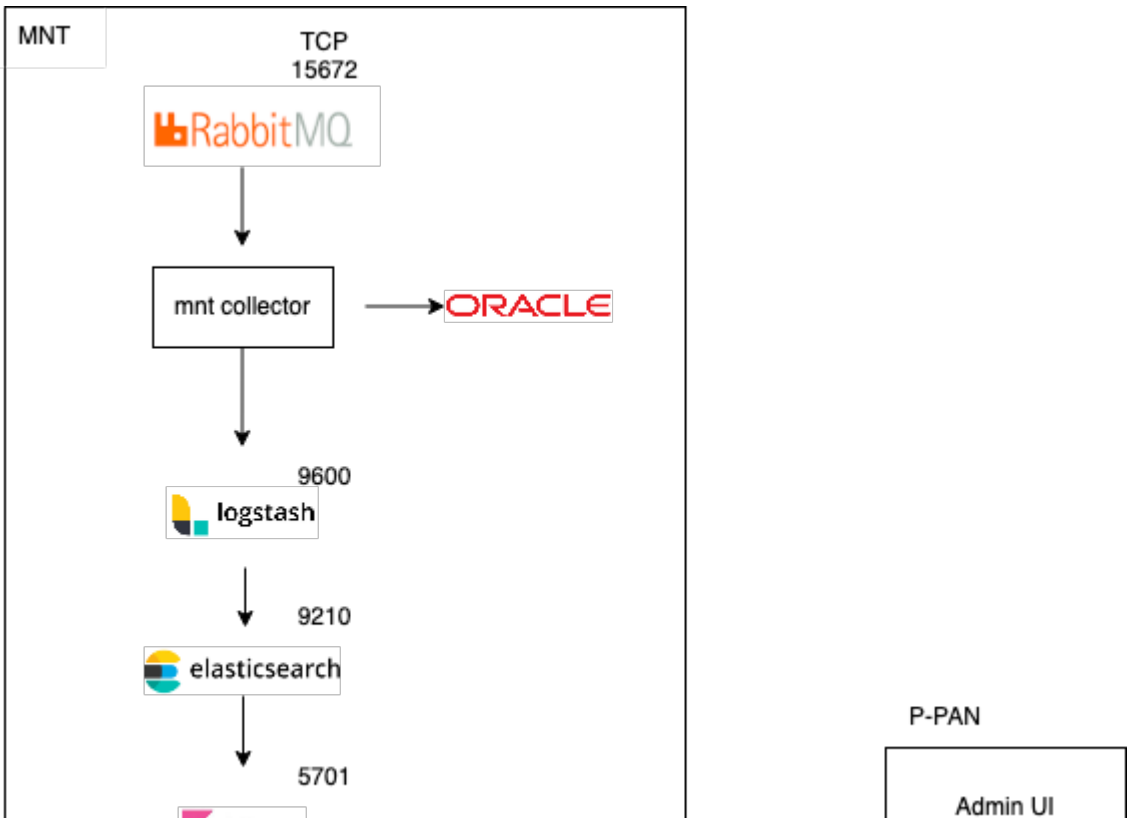


Fluxo de pilha ELK

Pilha ELK como análise de log

- Uma instância separada da pilha ElasticSearch+LogStash+Kibana está sendo executada apenas em nós MnT.
  - Isso não tem nenhuma correlação com a Elasticsearch of Context-Visibility.
  - Executando o ELK 7.17

- Os MNTs primário e secundário têm suas próprias instâncias separadas de ELK.
  - Kibana é habilitado somente no MNT secundário se estiver disponível, exibindo dados somente deste nó.
- A Análise de log é desabilitada por padrão.
- Consome recursos Oracle.
- Armazena no máximo 7 dias de dados.
- O tamanho total dos dados consumidos pela análise de log é restrito a 10 GB.
  - Quando qualquer um dos limites for atingido, o ElasticSearch removerá os dados.



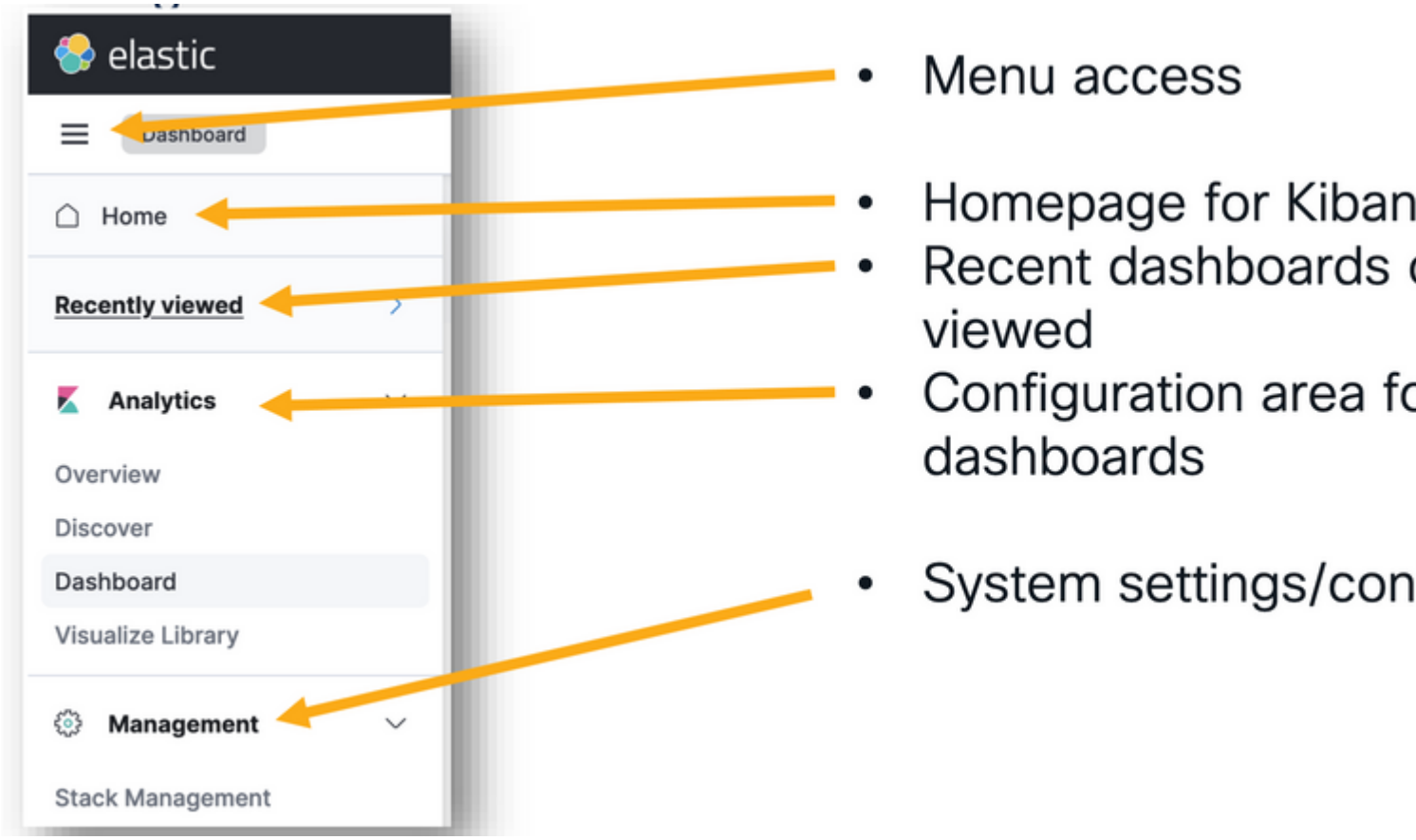
ISE Logstash Service running 614339

ISE Kibana Service running 616064

ISE Native IPSec Service running 75883
MFC Profiler running 651910

Menu Navegação

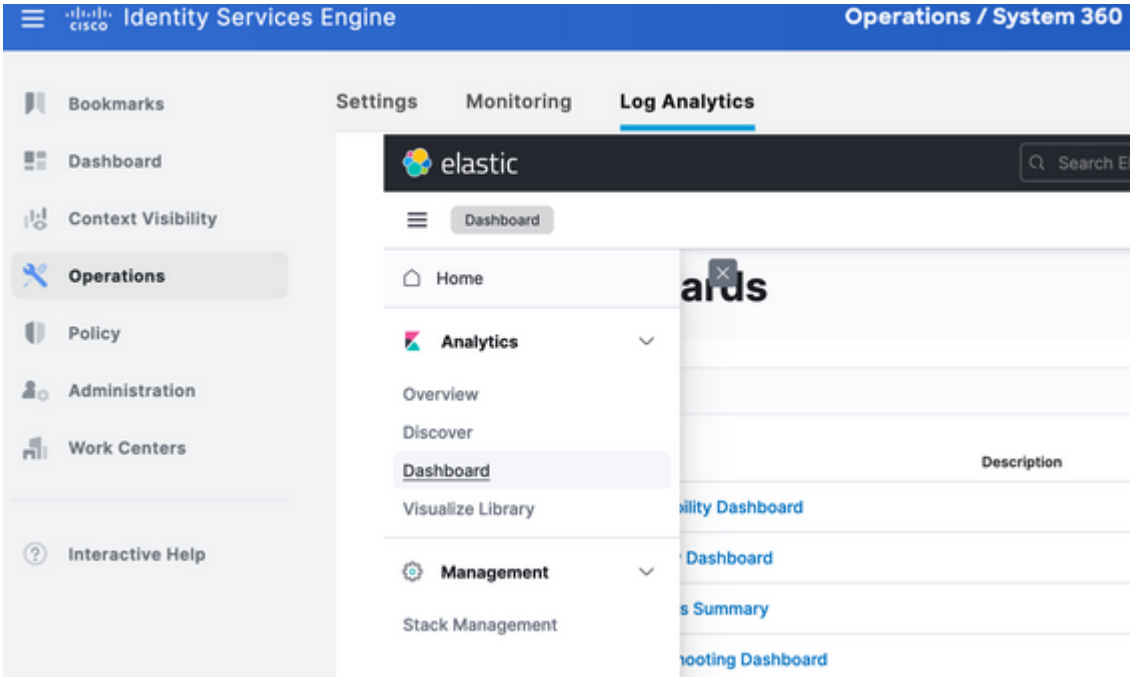
Quando os serviços ELK forem iniciados, você terá acesso ao menu de navegação Elastic.



Menu Navegação

Painéis integrados

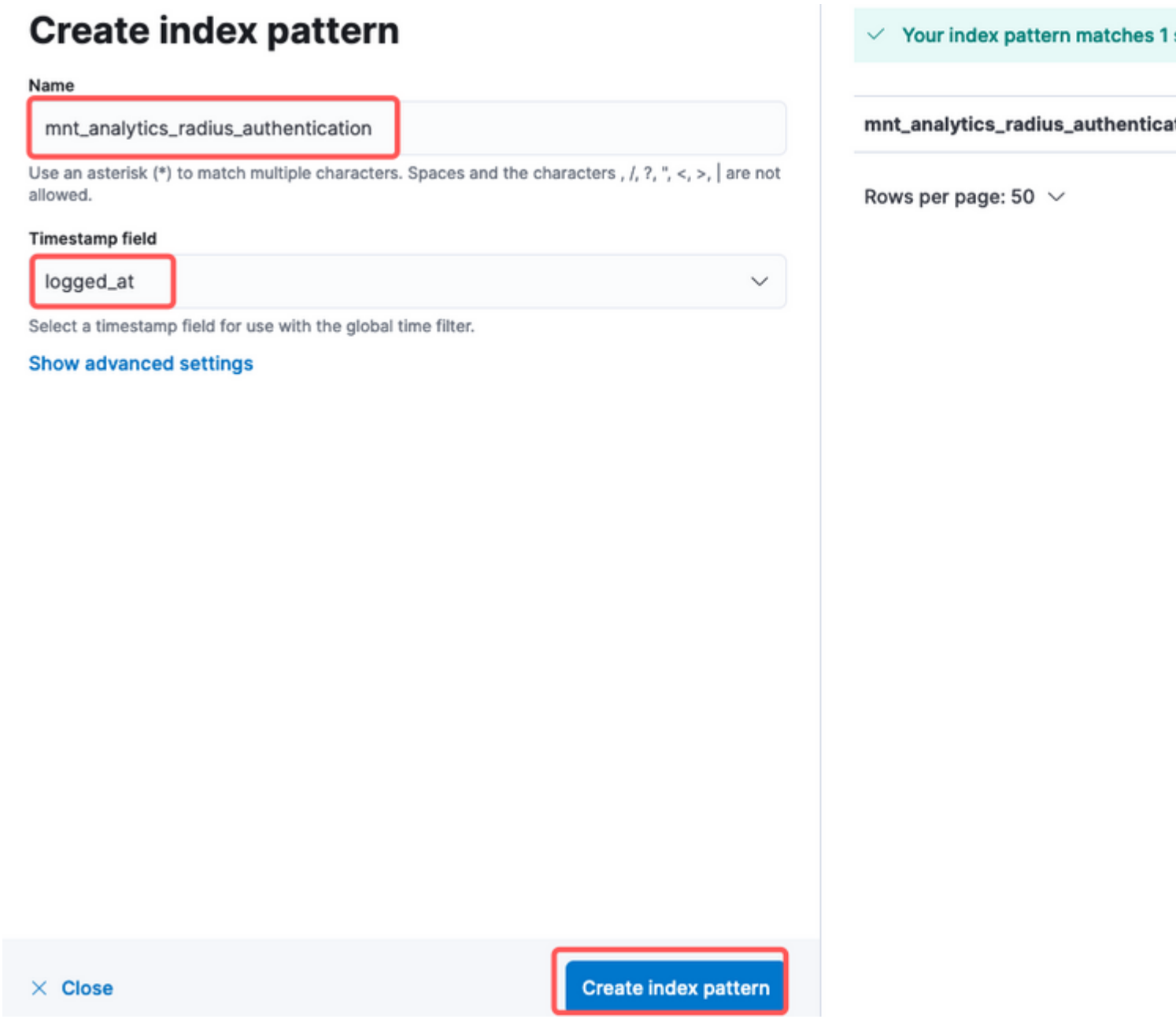
- Por padrão, o ISE tem painéis integrados com dados do Radius, TACACs, desempenho do sistema e observabilidade do ISE.
- Esses painéis podem ser acessados navegando até Operações>Log Analytics.
    - Quando a interface de usuário elástica estiver aberta, clique no menu sanduíche >Análise>Painéis.



Painéis integrados

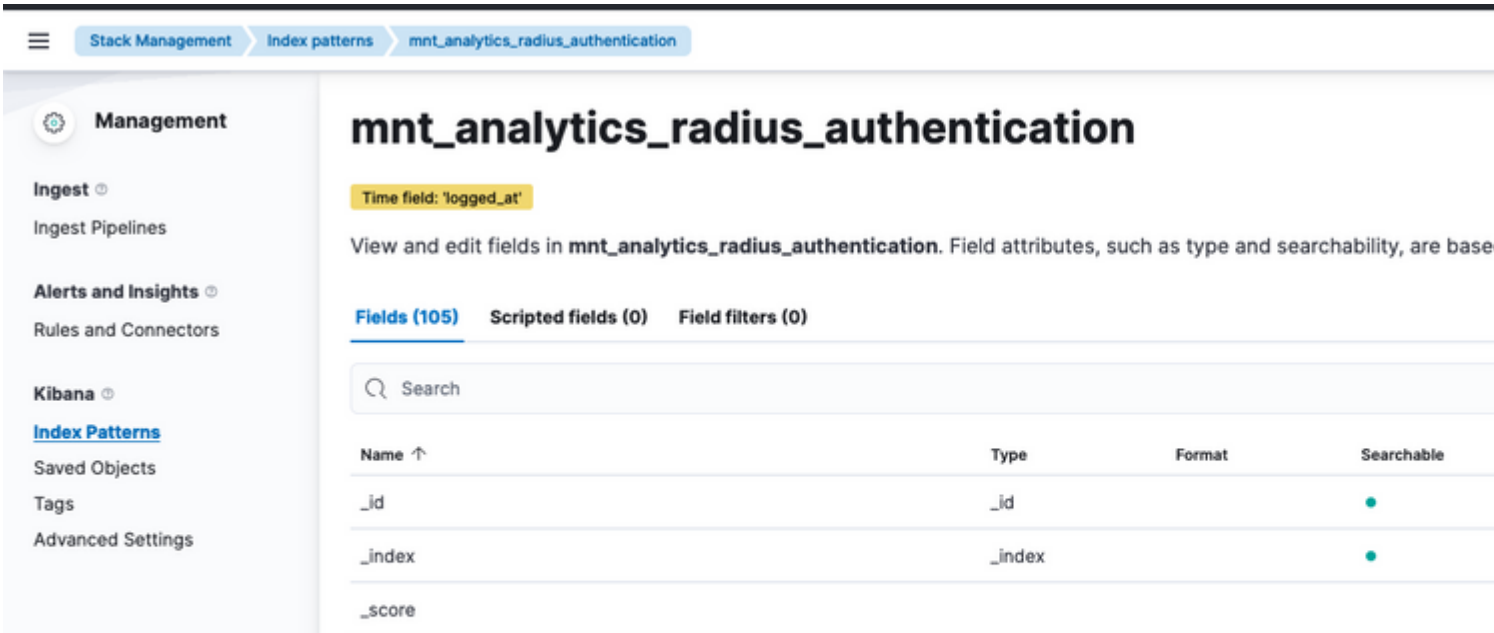
- Painéis disponíveis no ISE 3.3

- Selecione o campo Timestamp, logged_at, logged_at_timezone ou "Eu não quero usar o filtro de tempo".
- Em seguida, clique em "Criar padrão de índice".



Selecionar índice

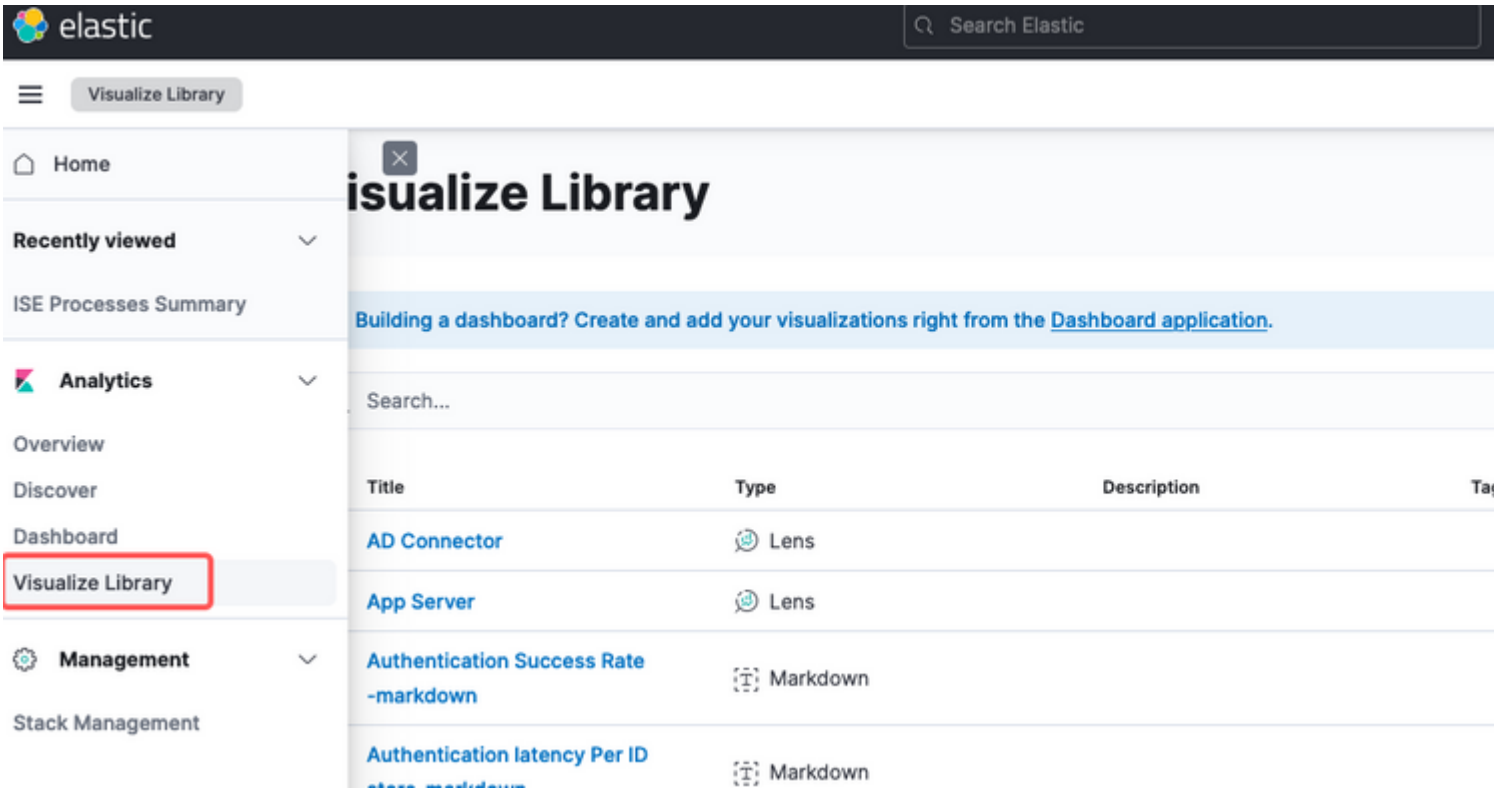
Depois de criado, o índice lista todas as variáveis associadas que podem ser usadas posteriormente para criar visualizações.



: mostram os dados em barras verticais, facilitando a comparação de valores entre categorias ou intervalos de tempo.

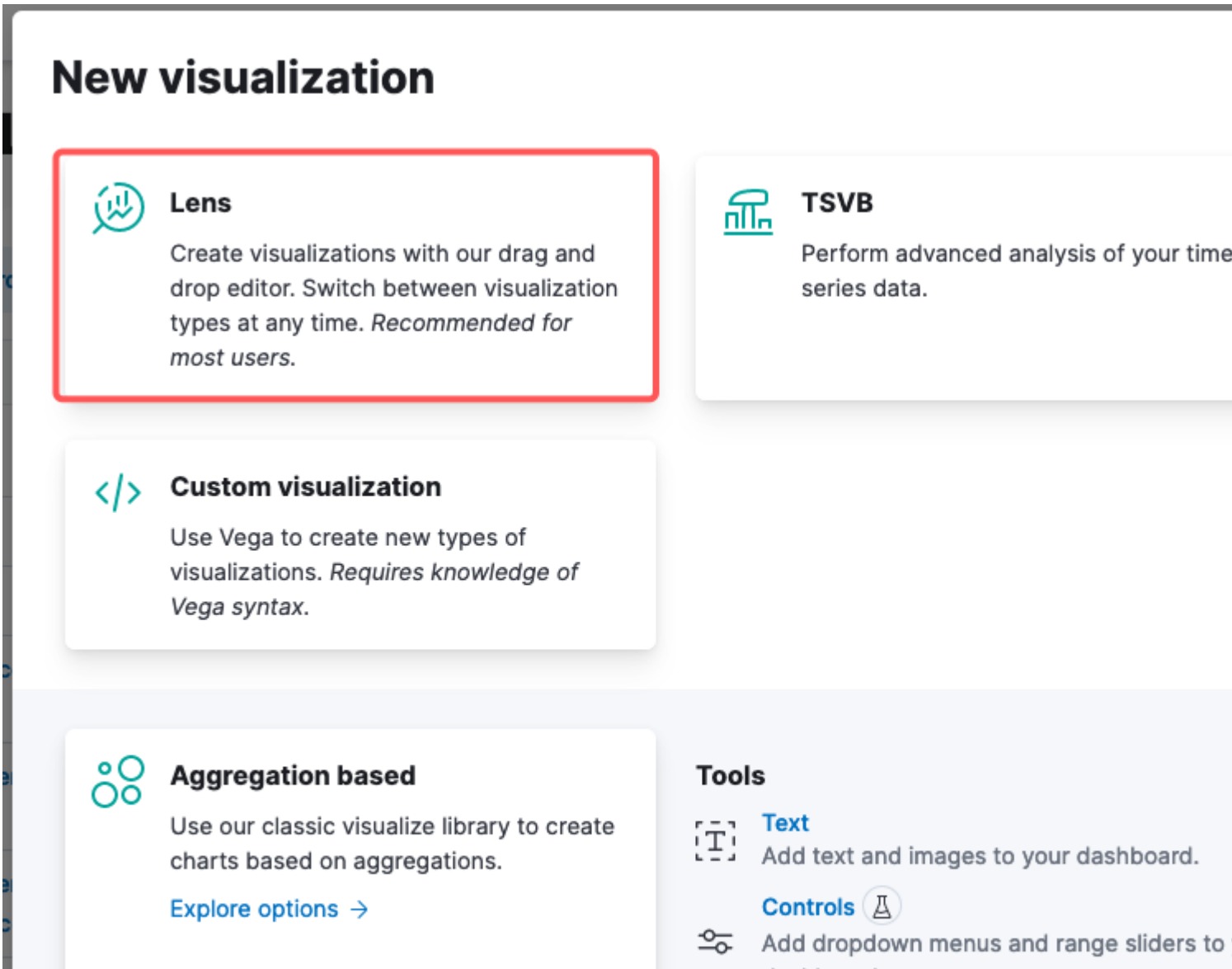
- **Gráficos de Linhas**: Os gráficos de linhas exibem dados como uma série de pontos de dados conectados por linhas. Eles são úteis para visualizar tendências ao longo do tempo.
- **Gráficos de Pizza**: Os gráficos de pizza representam dados em um gráfico circular, com cada segmento da pizza representando uma categoria e o tamanho do segmento indicando sua proporção.
- **Gráficos de Área**: Semelhantes aos gráficos de linha, os gráficos de área também mostram tendências ao longo do tempo, mas preenchem a área abaixo das linhas, facilitando a visualização da magnitude das alterações.
- **Mapas de calor**: os mapas de calor usam cores para representar valores de dados em uma matriz ou grade. Eles são úteis para mostrar concentrações ou variações nos dados.
- **Visualizações de Métricas**: exibem valores numéricos únicos, como contagens ou médias. Eles são frequentemente usados para mostrar os KPIs (indicadores chave de desempenho).
- **Tabelas de Dados**: As tabelas de dados apresentam dados brutos em formato tabular, permitindo que você veja informações detalhadas e classifique ou filtre os dados.
- **Histogramas**: os histogramas dividem os dados em compartimentos ou intervalos e exibem a frequência ou contagem de pontos de dados em cada compartimento. Eles são úteis para entender as distribuições de dados.
- **Mapas de coordenadas**: visualizam dados geoespaciais, permitindo exibir dados em um mapa e usar vários marcadores, cores ou tamanhos para representar atributos de dados.
- **Nuvens de tag**: nuvens de tag exibem frequências de palavra, com o tamanho de cada palavra indicando sua importância ou frequência em um conjunto de dados.

Navegue até Analytics>Visualize a biblioteca e clique em "Criar visualização".



Criar visualização

Selecione a visualização de sua preferência, neste exemplo, a Lente é preferida para a prática.



: No painel esquerdo, você pode selecionar a origem de dados ou o padrão de índice de pesquisa Elástica que deseja usar para a visualização.

- **Visualização Canvas**: a área central é onde você constrói sua visualização arrastando e soltando campos, selecionando tipos de gráfico e definindo configurações de gráfico.
- **Barra de ferramentas de visualização**: Acima da tela, você poderá encontrar uma barra de ferramentas que lhe permita personalizar sua visualização, incluindo opções para alterar tipos de gráficos, adicionar filtros e definir configurações de gráficos.

- **Painel de dados**: No lado direito, você pode acessar o painel "Dados", que permite gerenciar a transformação de dados, agregação e configurações de campo.

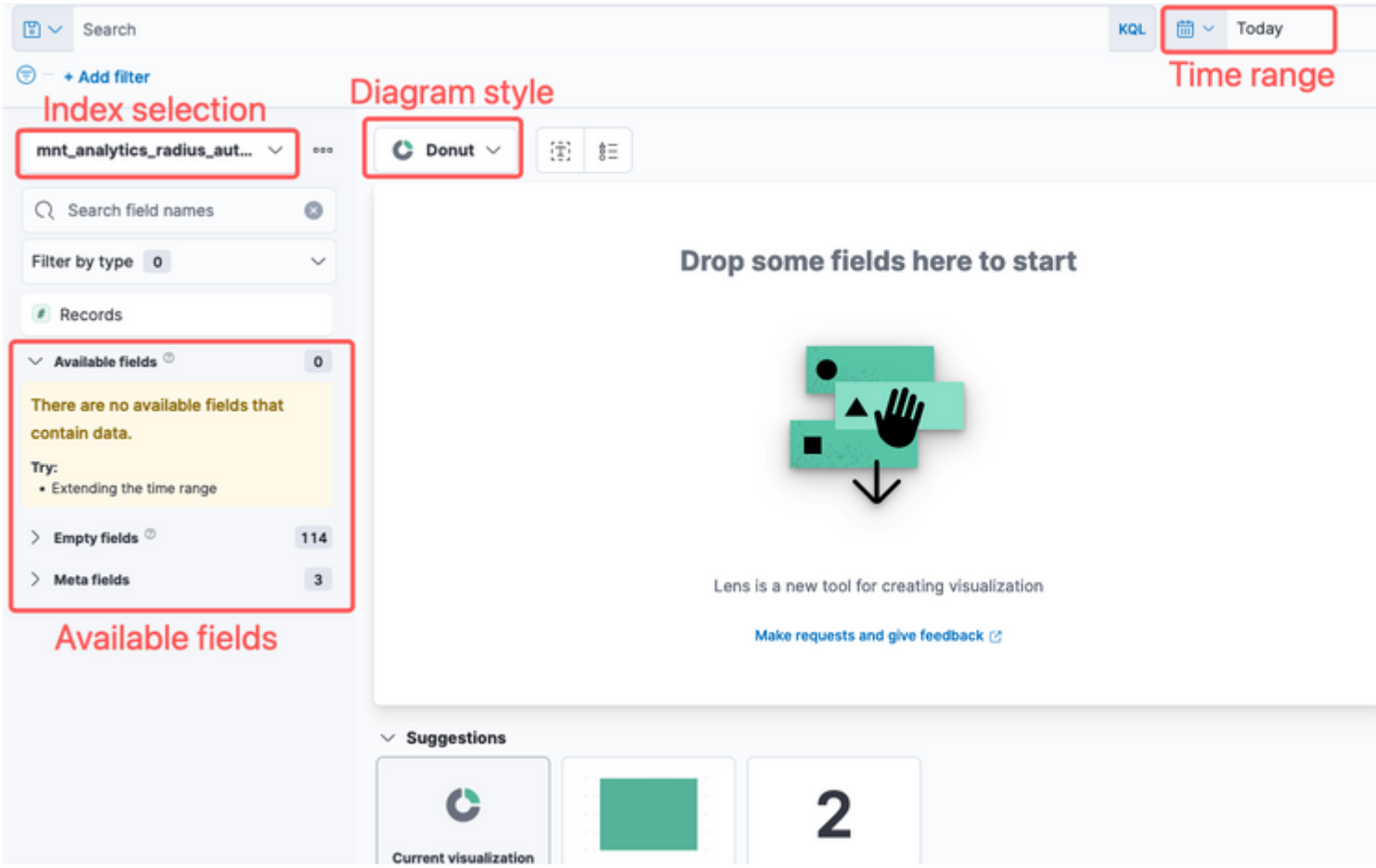
- **Gerenciamento de camadas**: dependendo do tipo de visualização que você está criando (por exemplo, gráficos de camadas), você pode ter uma área de gerenciamento de camadas para configurar várias camadas em sua visualização.

- **Visualização:** à medida que você faz alterações em sua visualização, uma visualização em tempo real normalmente é fornecida para que você possa ver a aparência do seu gráfico com as configurações atuais**.**

- **Configurações de visualização**: Dependendo do tipo de gráfico selecionado, você pode acessar configurações específicas para esse tipo de visualização, como configuração de eixo, esquemas de cores e rótulos.

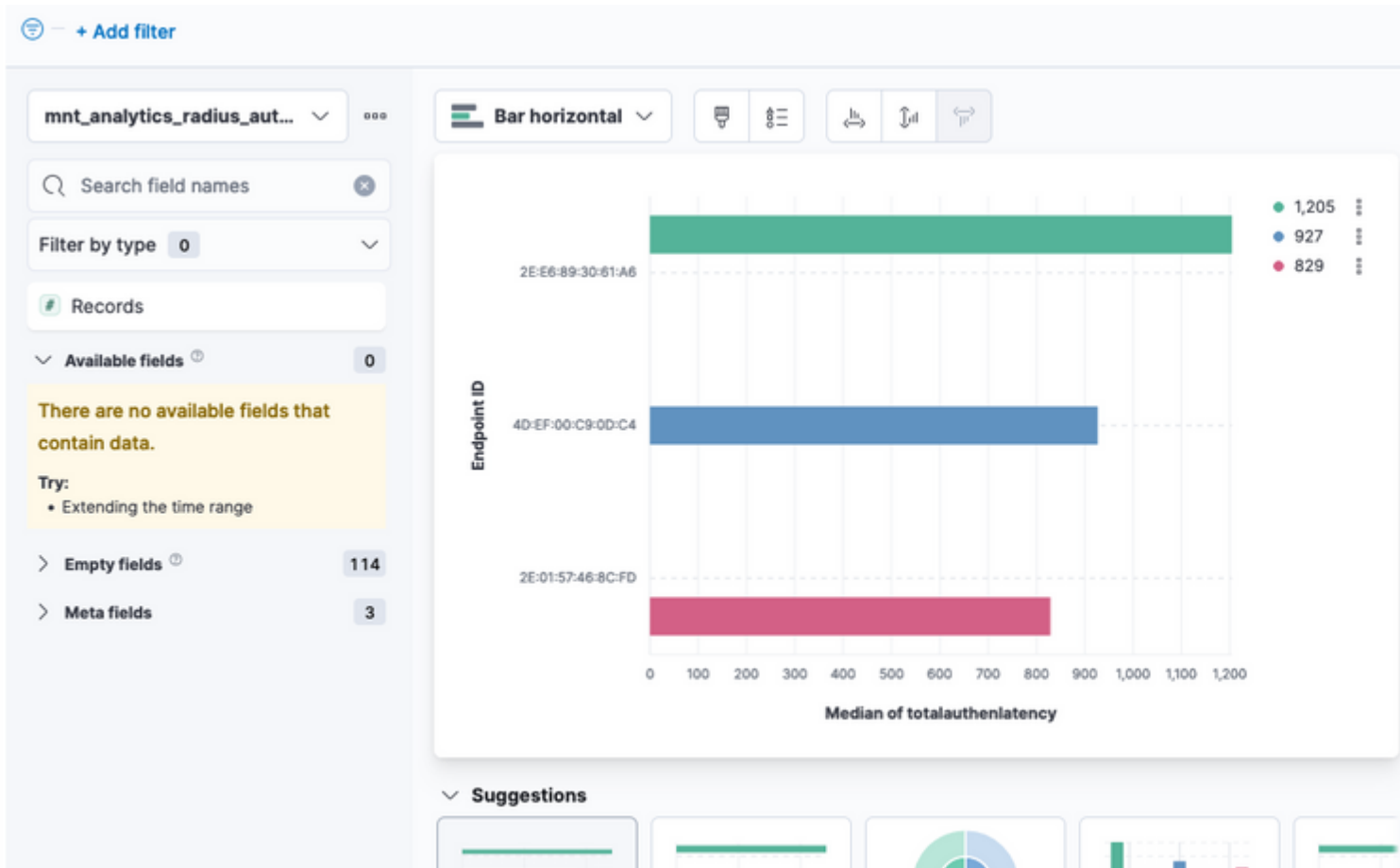
- **Configurações de interatividade**: Você pode adicionar interações e ações à sua visualização, permitindo que os usuários filtrem dados ou naveguem para outras partes dos seus painéis Kibana.

- **Salvar e compartilhar**: na parte superior da interface da Lente, normalmente há opções para salvar sua visualização, adicioná-la a um painel ou compartilhá-la com outras pessoas.



Visualização da lente

Devido ao bug da Cisco ID CSCwh48057, o painel esquerdo não mostra os campos disponíveis para uso. No entanto, do lado direito, você pode selecionar os campos necessários mais o estilo do diagrama. Neste exemplo, como a latência de autenticação é um tópico de interesse comum, o gráfico é criado para visualizar a latência de autenticação versus o id do ponto final.



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

Informações Relacionadas

Guia do administrador do ISE 3.3

Documentação do Kibana

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.