

了解ISE上的日志分析 — ELK堆栈

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[ELK堆栈](#)

[ELK堆栈作为日志分析](#)

[启用日志分析](#)

[导航菜单](#)

[内置控制面板](#)

[创建新控制面板](#)

[步骤1:创建索引模式\(数据源\)](#)

[第二步:创建可视化效果](#)

[第三步:创建控制面板](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍内置Cisco身份服务引擎(ISE)3.3至System 360日志分析的ELK堆栈组件。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ISE
- ELK堆栈

使用的组件

本文档中的信息基于Cisco ISE 3.3。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

系统360包括监控和日志分析。

Monitoring功能使您能够从集中式控制台监视各种应用程序和系统统计信息，以及部署中所有节点的关键性能指标(KPI)。KPI有助于深入了解节点环境的整体运行状况。统计信息对系统配置和利用率特定数据提供了简化表示。

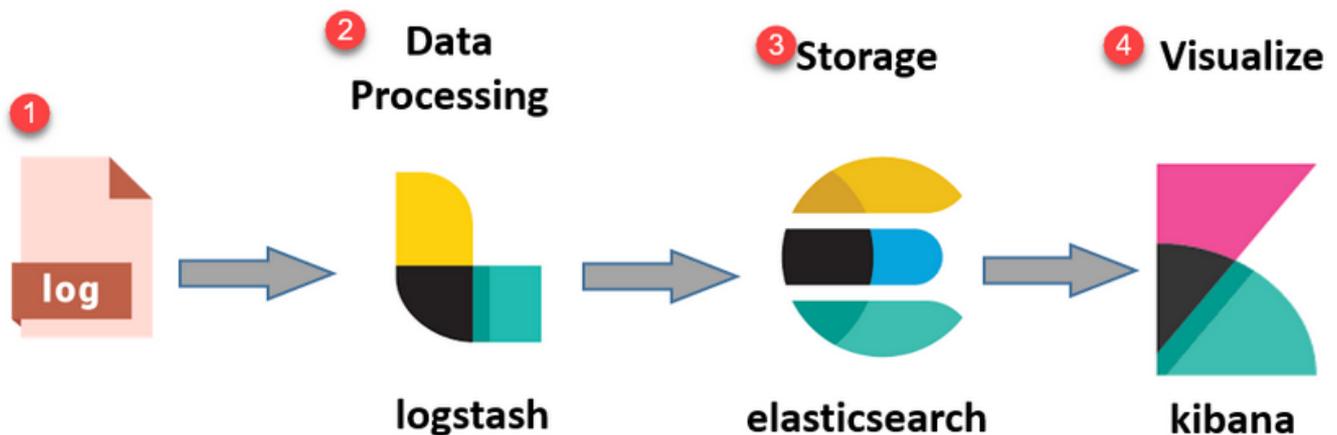
日志分析提供灵活的分析系统，用于深入分析终端身份验证、授权和记帐(AAA)并分析系统日志数据。您还可以分析思科ISE运行状况摘要和流程状态。您可以生成类似思科ISE计数器和运行状况摘要报告的报告。

ELK堆栈

ELK Stack是一种常用的开源软件堆栈，用于收集、处理和可视化大量数据。它代表Elasticsearch、Logstash和Kibana。

- Elasticsearch:Elasticsearch是一个分布式搜索和分析引擎。它旨在快速且接近实时地存储、搜索和分析大量数据。它使用基于JSON的查询语言并且高度可扩展。
- Logstash:Logstash是一个数据处理管道，用于接收、处理和转换来自多个源的数据。它可以对数据进行解析和丰富，使其更结构化，更适合于分析。Logstash支持各种输入源和输出目标。
- Kibana:Kibana是一个与Elasticsearch配合使用的数据可视化平台。它允许用户创建交互式控制面板、图表、图形和可视化，以浏览和了解Elasticsearch中存储的数据。Kibana的界面方便了数据的查询和可视化。

结合使用时，这些组件可形成强大的堆栈，用于管理和分析各种类型的数据（从日志文件到指标等），同时提供可视化功能来理解信息。



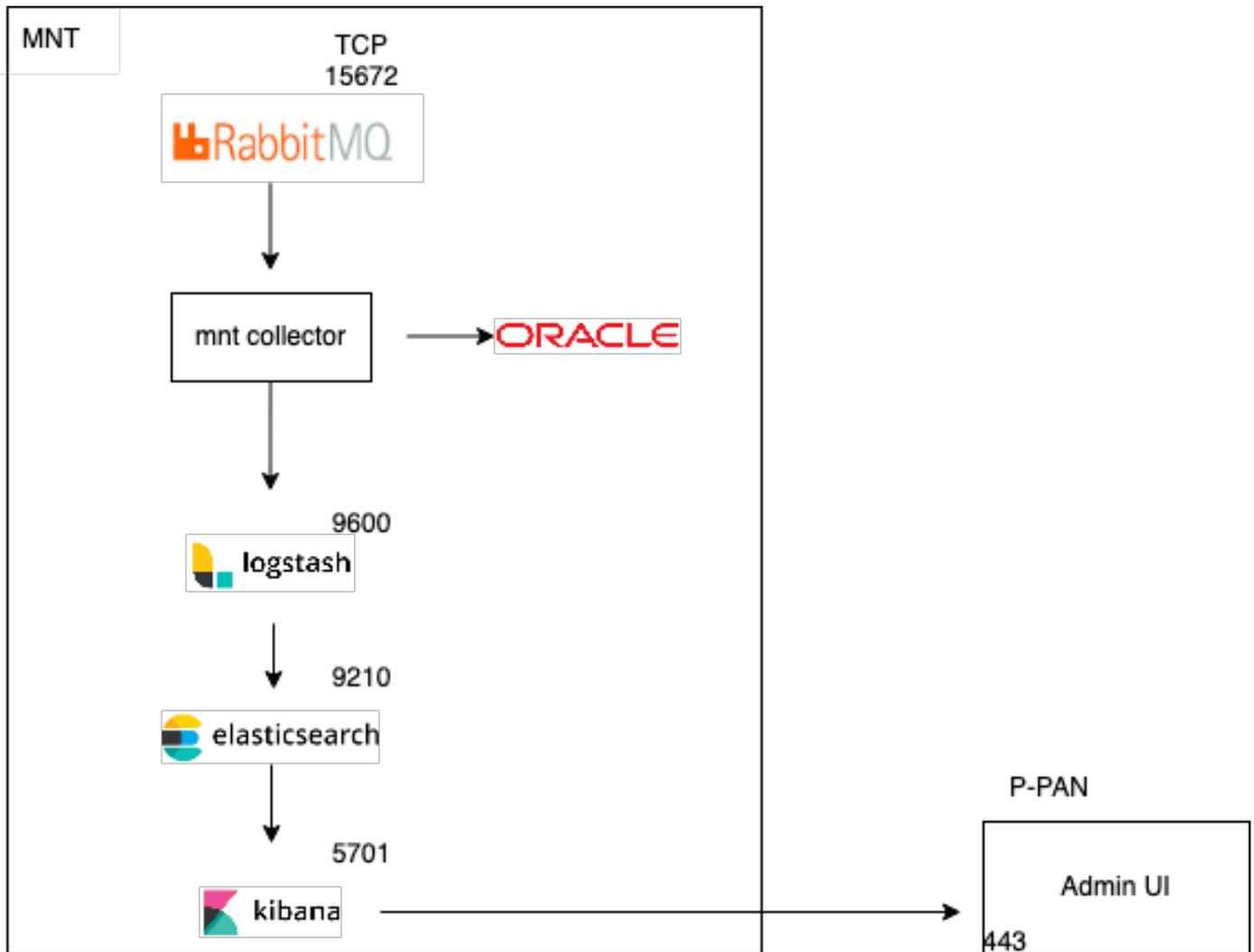
ELK堆栈流

ELK堆栈作为日志分析

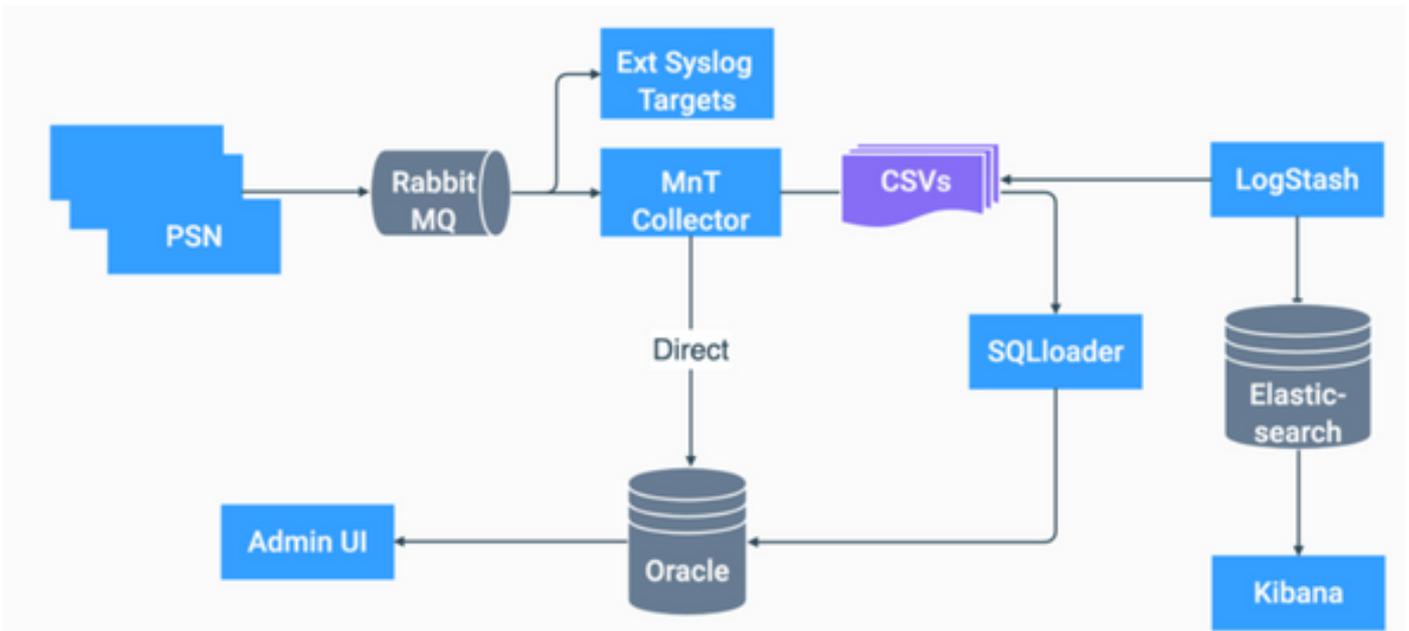
- ElasticSearch+LogStash+Kibana堆栈的独立实例仅在MnT节点上运行。
 - 这与情景可视性的Elasticsearch没有任何关联。

- 运行ELK 7.17

- 主MNT和辅助MNT具有各自的ELK实例。
 - Kibana仅在辅助MNT上启用（如果可用），仅显示来自此节点的数据。
- 默认情况下禁用日志分析。
- 冲减Oracle资源。
- 最多存储7天的数据。
- 日志分析所使用的数据总大小限制为10 GB。
 - 一旦达到任何限制，ElasticSearch就会清除数据。



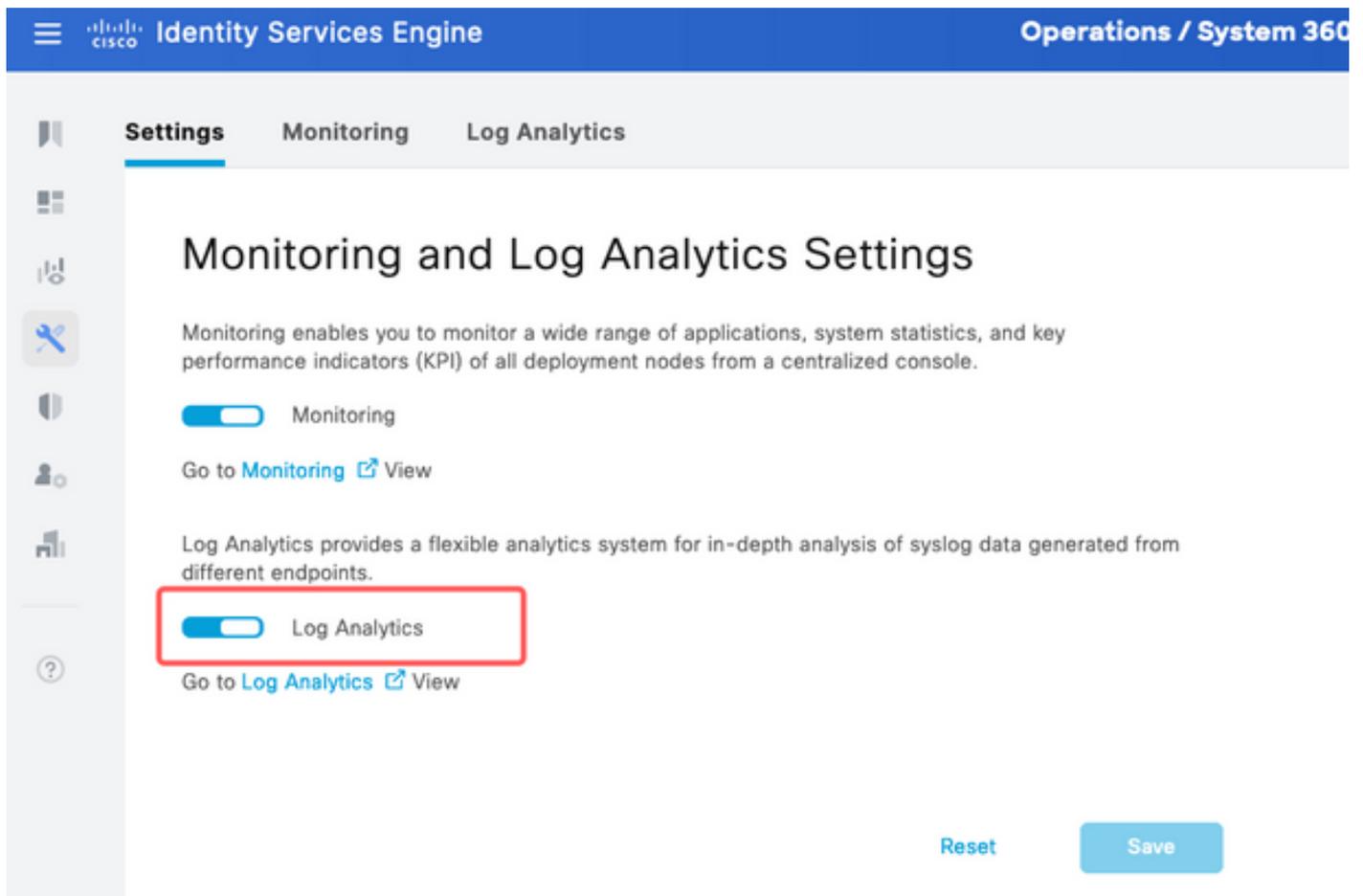
作为日志分析的ELK流



ISE中ELK的流程图

启用日志分析

默认情况下在ISE上禁用日志分析。要启用它，请导航至 `Operations > System 360 > Settings` 如图所示。



启用日志分析

ISE大约需要一分钟来初始化ELK堆栈，您可以使用 `show app stat ise.`

此外，还可以从根目录检查容器状态。

<#root>

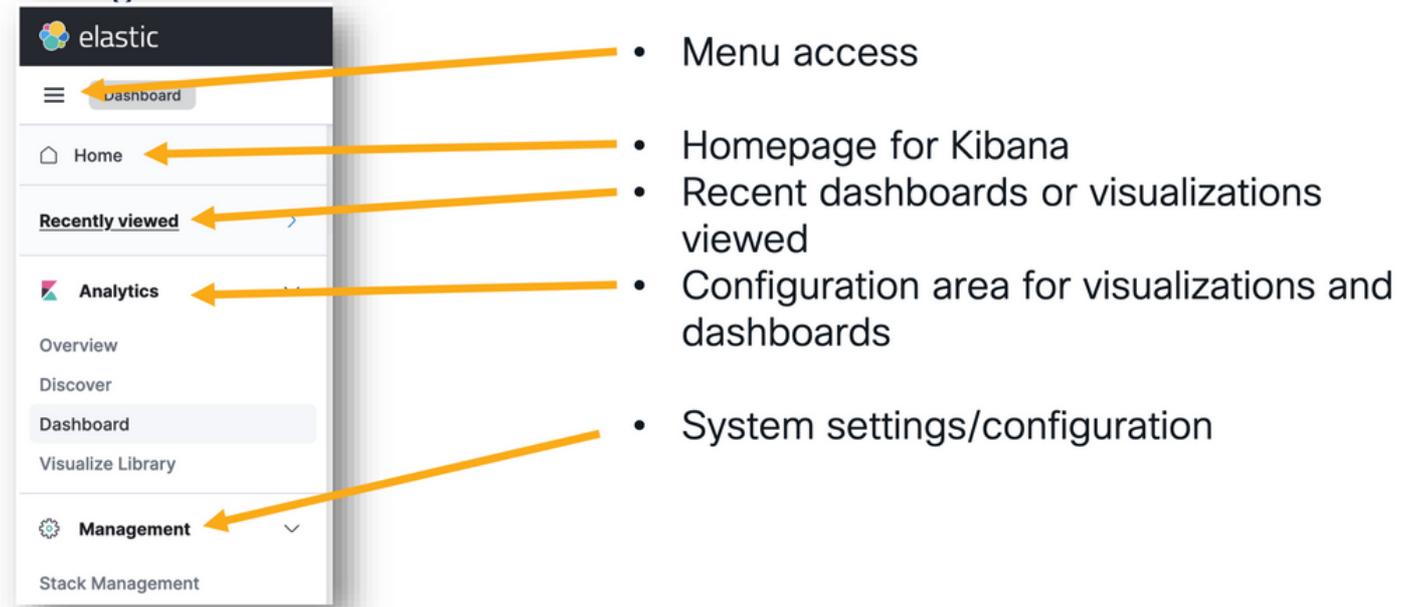
```
admin#show application status ise
```

```
ISE PROCESS NAME STATE PROCESS ID
```

```
-----  
Database Listener running 7708  
Database Server running 132 PROCESSES  
Application Server running 551493  
Profiler Database running 14281  
ISE Indexing Engine running 553168  
AD Connector running 41413  
M&T Session Database running 26017  
M&T Log Processor running 33547  
Certificate Authority Service running 41230  
EST Service running 659568  
SXP Engine Service disabled  
TC-NAC Service disabled  
PassiveID WMI Service disabled  
PassiveID Syslog Service disabled  
PassiveID API Service disabled  
PassiveID Agent Service disabled  
PassiveID Endpoint Service disabled  
PassiveID SPAN Service disabled  
DHCP Server (dhcpd) disabled  
DNS Server (named) disabled  
ISE Messaging Service running 10937  
ISE API Gateway Database Service running 13294  
ISE API Gateway Service running 586762  
ISE pxGrid Direct Service running 637606  
Segmentation Policy Service disabled  
REST Auth Service disabled  
SSE Connector disabled  
Hermes (pxGrid Cloud Agent) disabled  
McTrust (Meraki Sync Service) disabled  
ISE Node Exporter running 44422  
ISE Prometheus Service running 47890  
ISE Grafana Service running 51094  
  
ISE MNT LogAnalytics Elasticsearch running 611684  
  
ISE Logstash Service running 614339  
  
ISE Kibana Service running 616064  
  
ISE Native IPSec Service running 75883  
MFC Profiler running 651910
```

导航菜单

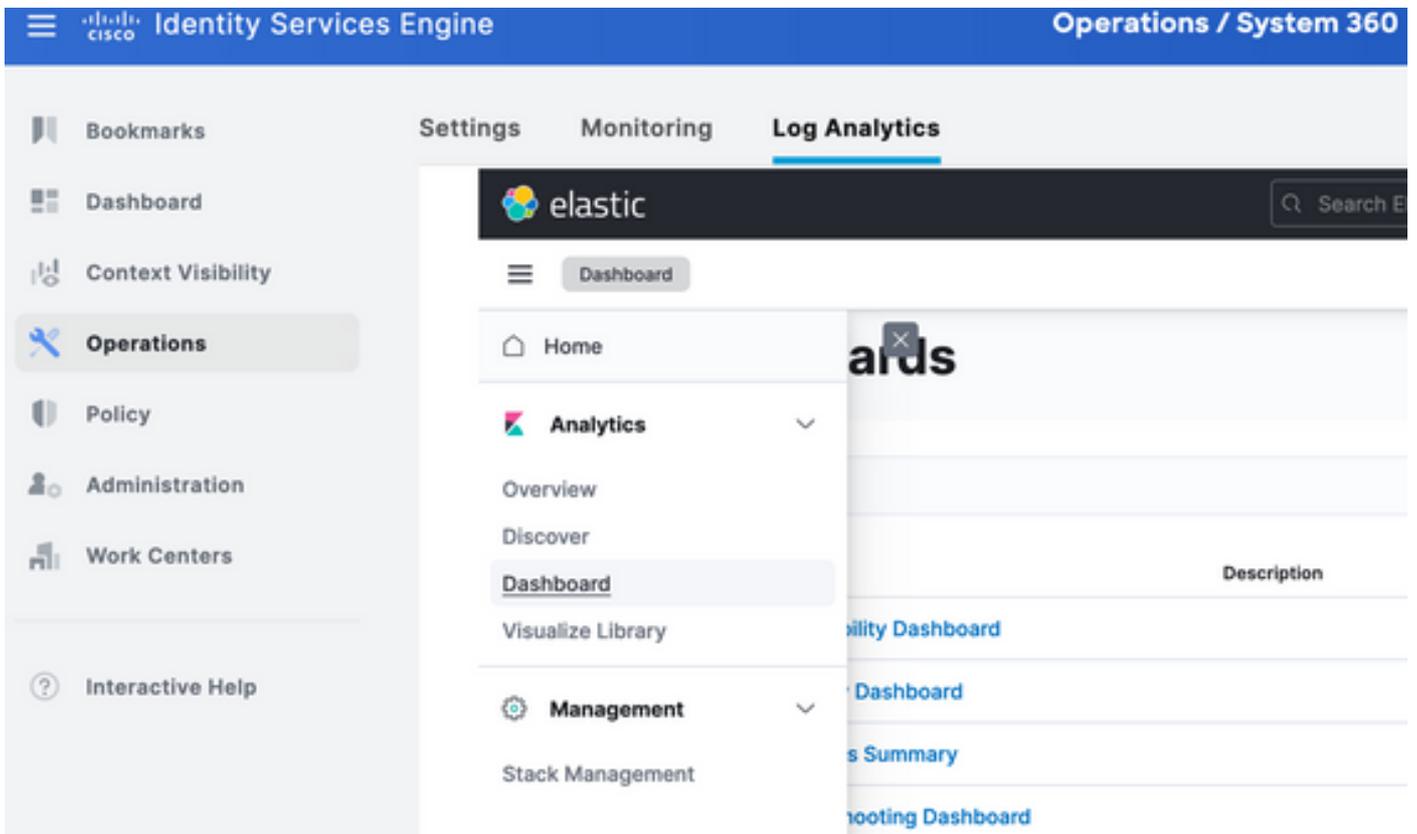
启动ELK服务后，您可以访问Elastic导航菜单。



导航菜单

内置控制面板

- 默认情况下，ISE具有内置控制面板，其中包含来自Radius、TACACS、系统性能和ISE可观察性的数据。
- 您可以通过导航至 `Operations > Log Analytics` .
 - Elastic UI打开后，单击 `Sandwich Menu > Analytics > Dashboards` .



内置控制面板

- ISE 3.3上可用的控制面板。

<input type="checkbox"/>	Title	Description	Tags	Actions
<input type="checkbox"/>	ISE Observability Dashboard			
<input type="checkbox"/>	ISE Overview Dashboard			
<input type="checkbox"/>	ISE Processes Summary			
<input type="checkbox"/>	ISE Troubleshooting Dashboard			
<input type="checkbox"/>	Profiler Performance			
<input type="checkbox"/>	Profiler Summary			
<input type="checkbox"/>	RADIUS Accounting Summary			
<input type="checkbox"/>	RADIUS Authentication Summary			
<input type="checkbox"/>	RADIUS Performance			
<input type="checkbox"/>	RADIUS Step Latency			
<input type="checkbox"/>	TACACS Accounting Summary			
<input type="checkbox"/>	TACACS Authentication Summary			

ISE 3.3日志分析控制面板

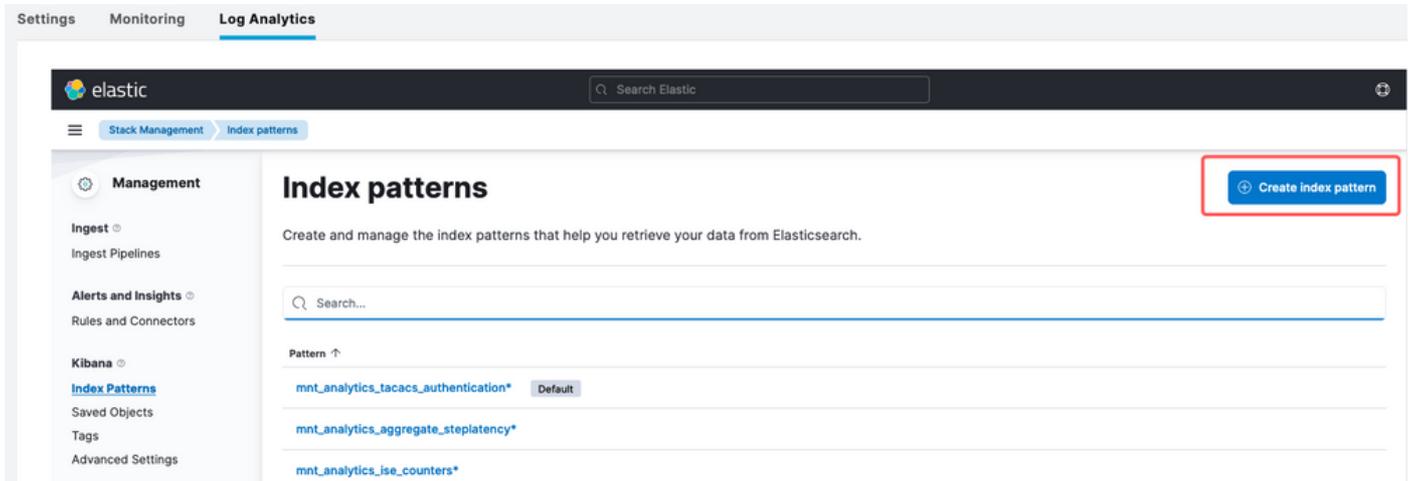
创建新控制面板

步骤1:创建索引模式 (数据源)

在Kibana中，“索引模式”是允许您定义Kibana如何与一个或多个Elasticsearch索引进行交互的配置

o

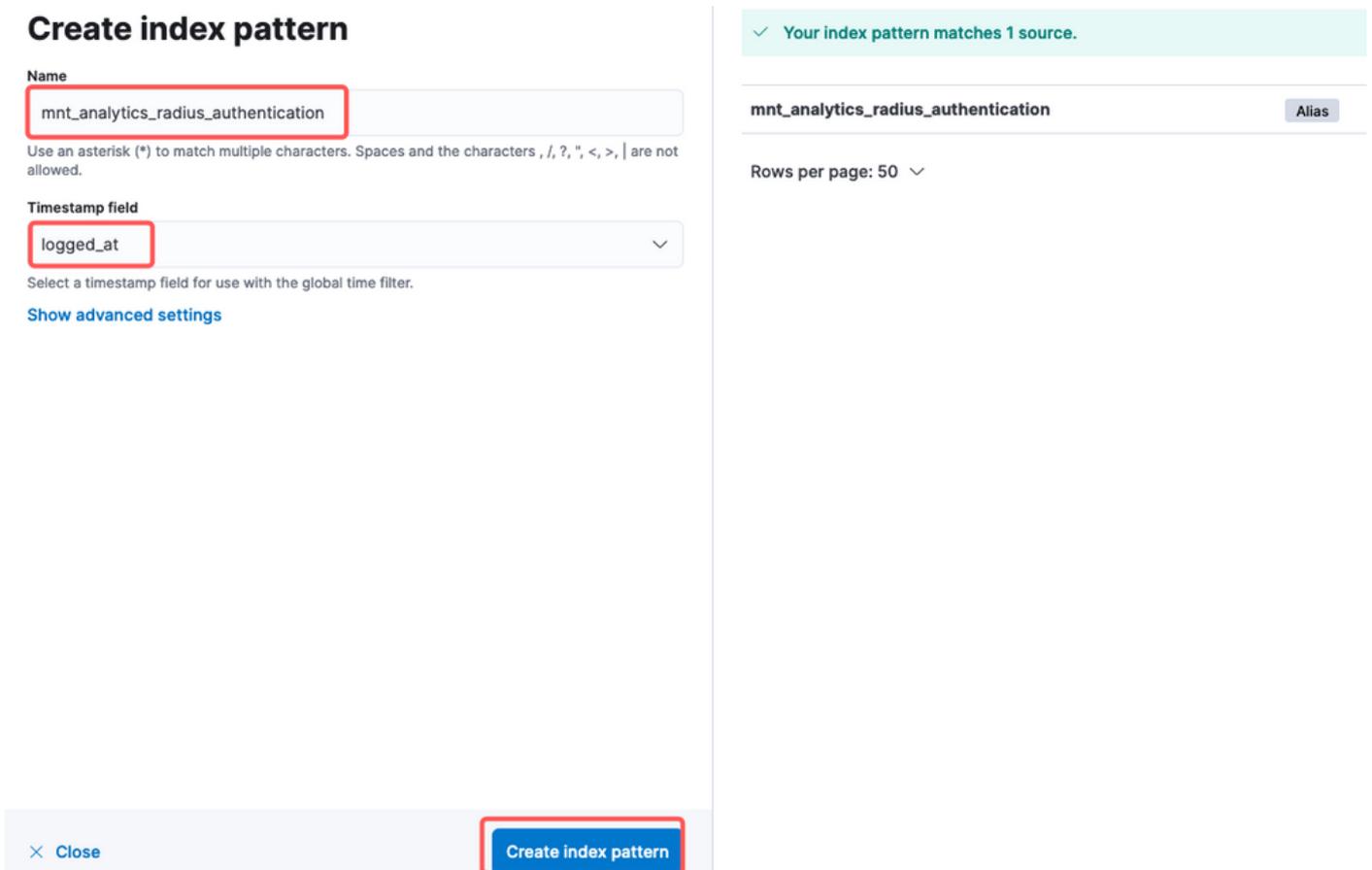
导航至 Management > Stack Management > Kibana > Index Patterns, 并点击 Create Index Pattern 如图所示。



创建索引模式

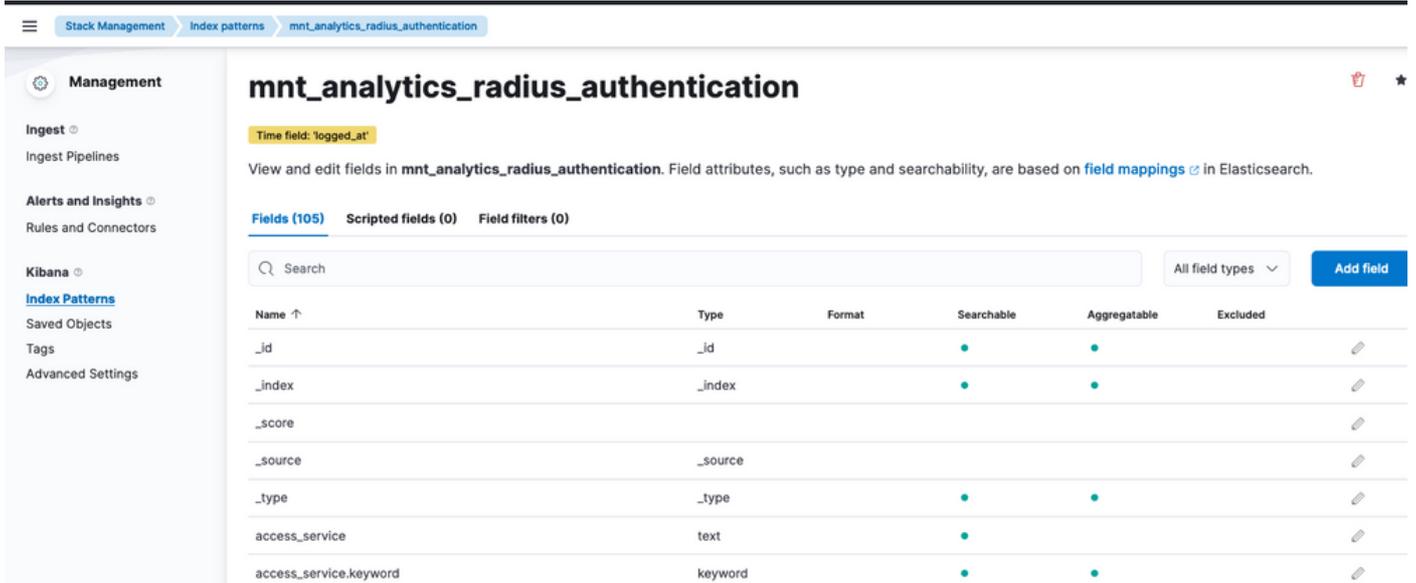
下一个窗口将列出ISE上的所有可用索引。

- 键入您感兴趣的索引的名称，可以使用*作为完全匹配项或通配符。
- 选择Timestamp字段、logged_at、logged_at_timezone或“I don't want to use time filter”。
- 然后，单击 Create index pattern.



选择索引

创建后，索引将列出所有关联变量，这些变量以后可用于创建可视化效果。



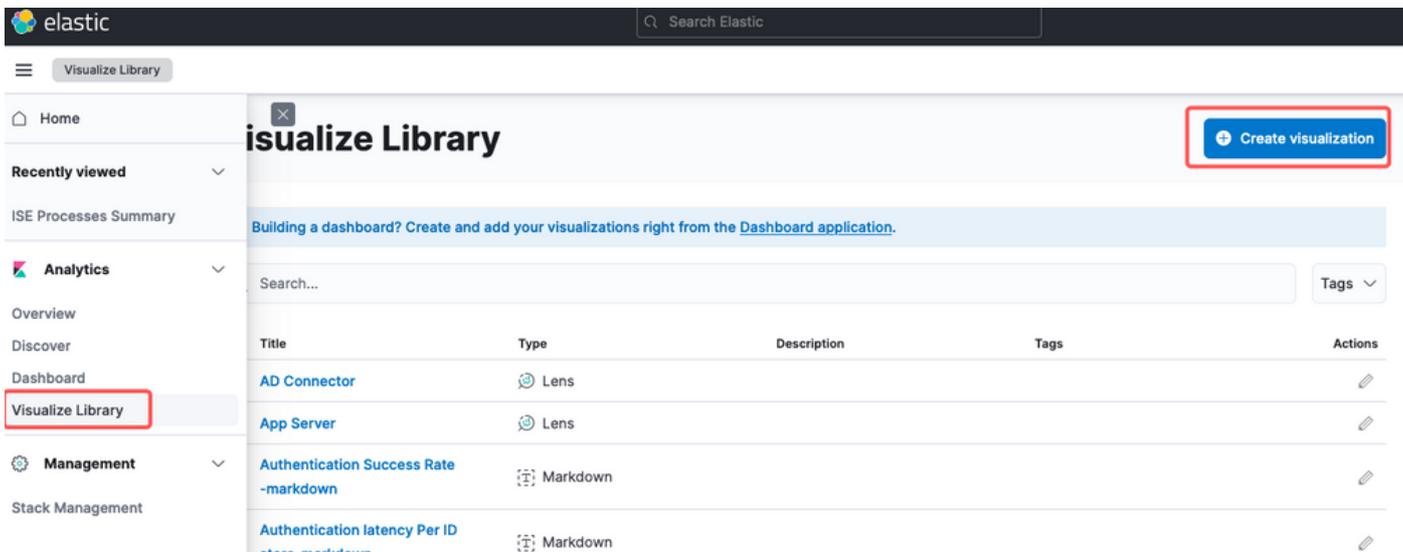
索引变量

第二步：创建可视化效果

在Kibana中，“可视化”是数据的图形表示。它们允许您将Elasticsearch中存储的数据转换为有意义的图表、图形和图表，以便更容易理解和分析。以下是您可以创建的一些常见可视化类型：

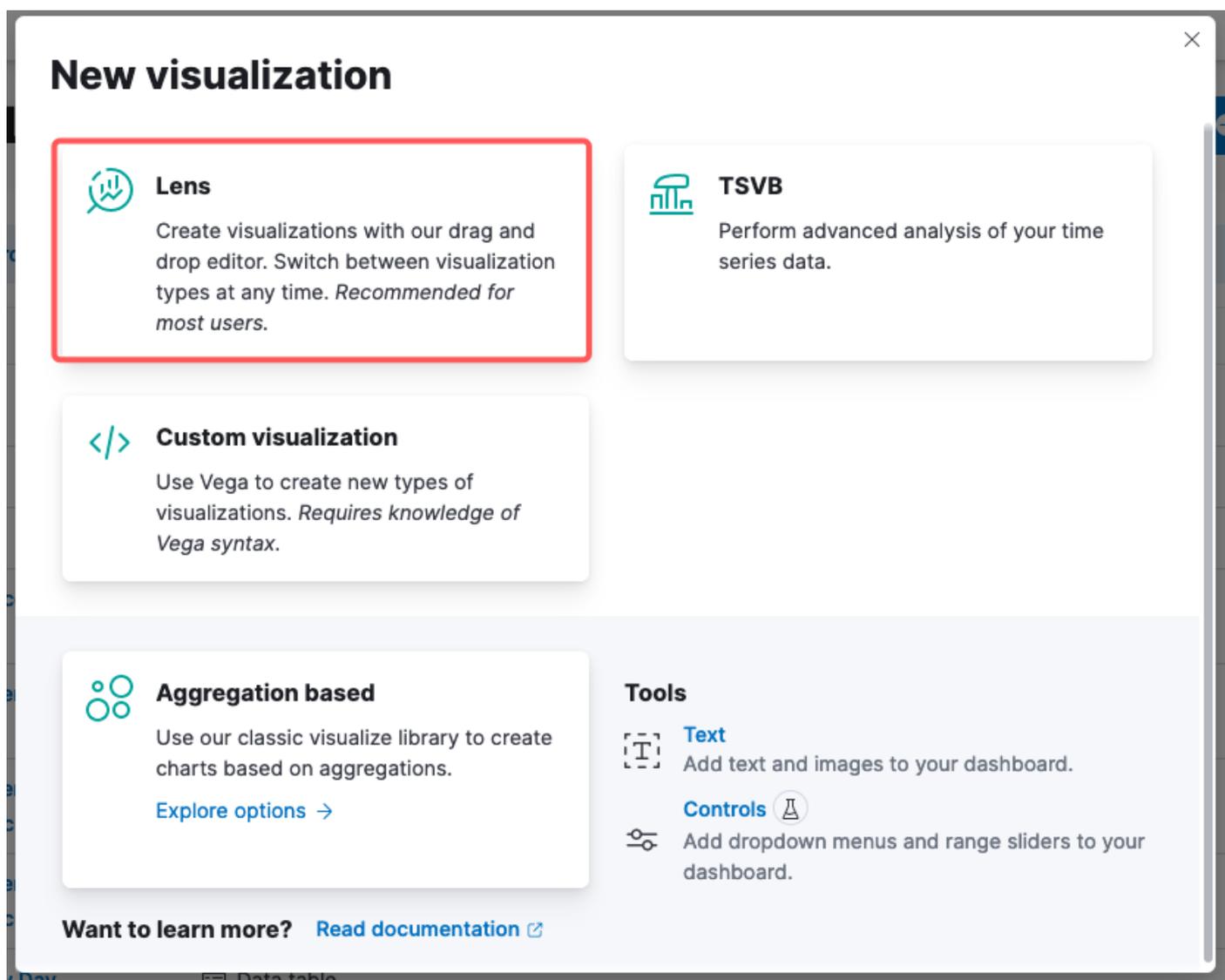
- Lens:使用拖放编辑器创建可视化。推荐。
- 条形图：这些条形图以垂直条形图显示数据，便于跨类别或时间间隔比较值。
- 折线图：折线图将数据显示为一系列通过折线连接的数据点。它们有助于直观显示随时间变化的趋势。
- 饼图：饼图以圆形图形表示数据，饼图的每个段表示一个类别，段的大小表示其比例。
- 面积图：与折线图类似，面积图也显示随时间变化的趋势，但它们填充了折线下的区域，从而更容易查看变化的幅度。
- 热图：热图使用颜色来表示矩阵或网格中的数据值。它们有助于显示数据中的浓度或变化。
- 度量可视化：这些显示单个数值，例如计数或平均值。它们通常用于显示关键绩效指标 (KPI)。
- 数据表：数据表以表格形式显示原始数据，使您可以查看详细信息并对数据进行排序或过滤。
- 直方图：直方图将数据划分为存储区或间隔，并显示每个存储区中的数据点频率或计数。它们对于了解数据分布非常有用。
- 坐标图：这些视图可显示地理空间数据，允许您在地图上显示数据，并使用各种标记、颜色或大小来表示数据属性。
- 标记云：标记云显示单词频率，每个单词的大小表示其在数据集中的重要性或频率。

导航至 [Analytics > Visualize Library](#) ，然后单击 [Create Visualization](#) 如图所示。



创建可视化

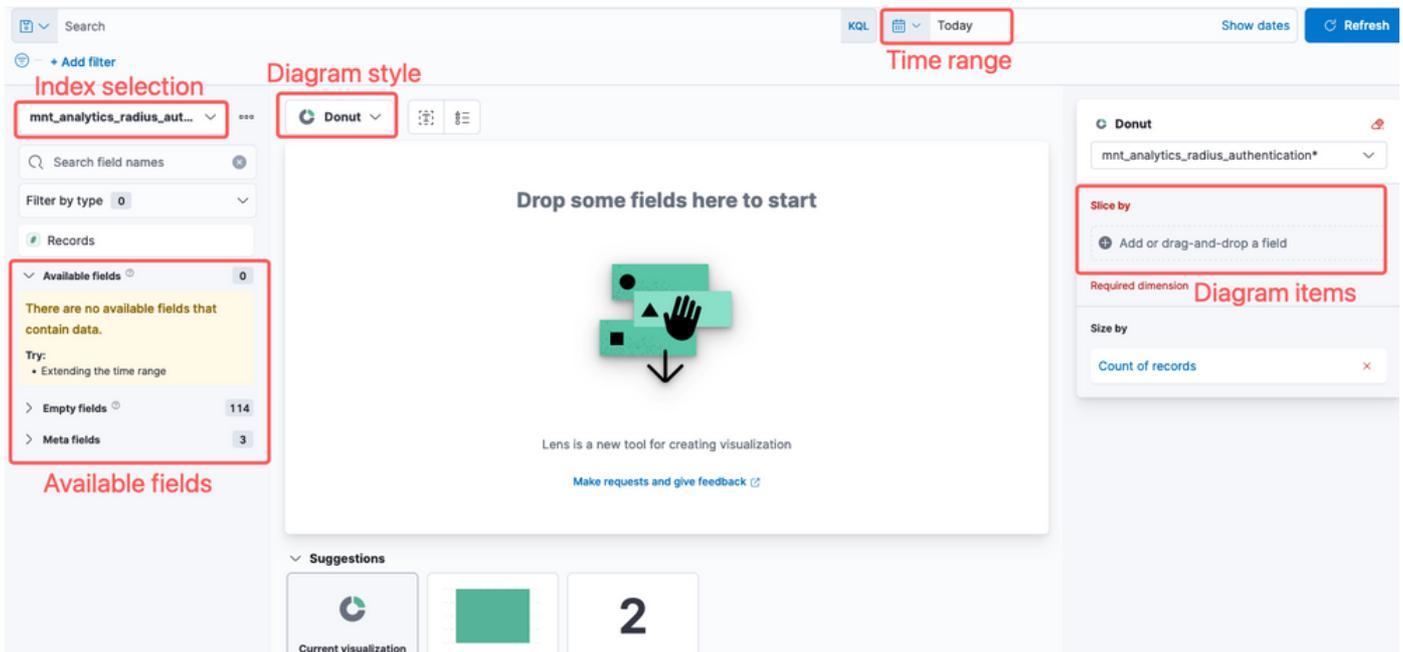
选择您偏好的可视化效果，在本例中，Lens为实用性首选。



选择可视化类型

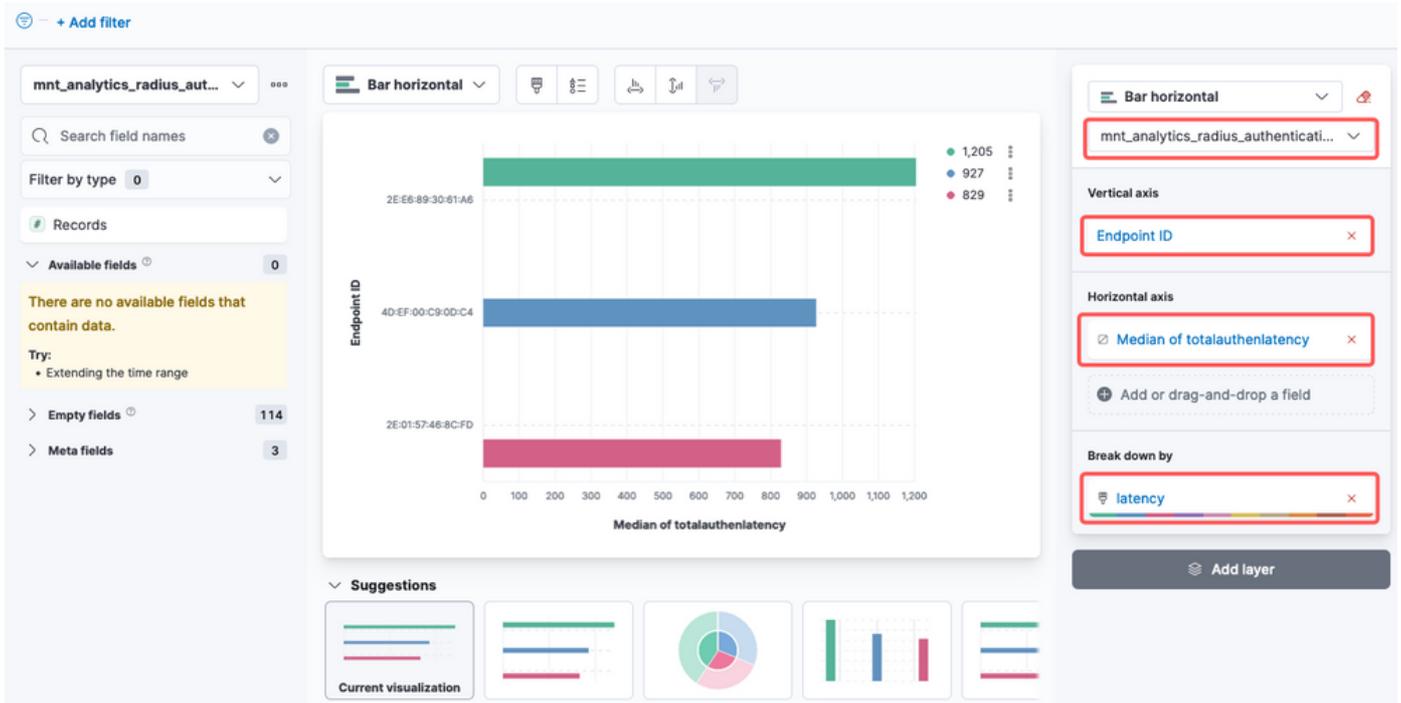
Kibana Lens，导航项目包括：

- 数据源选择：在左侧面板中，可以选择用于可视化的数据源或Elasticsearch索引模式。
- 可视化画布：通过拖放字段、选择图表类型和配置图表设置，可以在其中构建可视化的中心区域。
- 可视化工具栏：在画布的顶部，您可以找到用于自定义可视化的工具栏，包括用于更改图表类型、添加过滤器和配置图表设置的选项。
- 数据面板：在右侧，您可以访问“数据”面板，该面板允许您管理数据转换、聚合和字段设置。
- 层管理：根据正在创建的可视化类型（例如分层图表），可以有一个层管理区域，用于配置可视化中的多个层。
- 预览：在对可视化进行更改时，通常会提供实时预览，这样您就可以使用当前设置查看图表的外观。
- 可视化设置：根据所选的图表类型，您可以访问该可视化类型的特定设置，如轴配置、颜色方案和标签。
- 交互设置：您可以将交互和操作添加到可视化，从而允许用户筛选数据或导航到Kibana控制面板的其他部分。
- 保存和共享：在Lens界面的顶部，通常有用于保存您的可视化、将其添加到控制面板或与他人共享的选项。



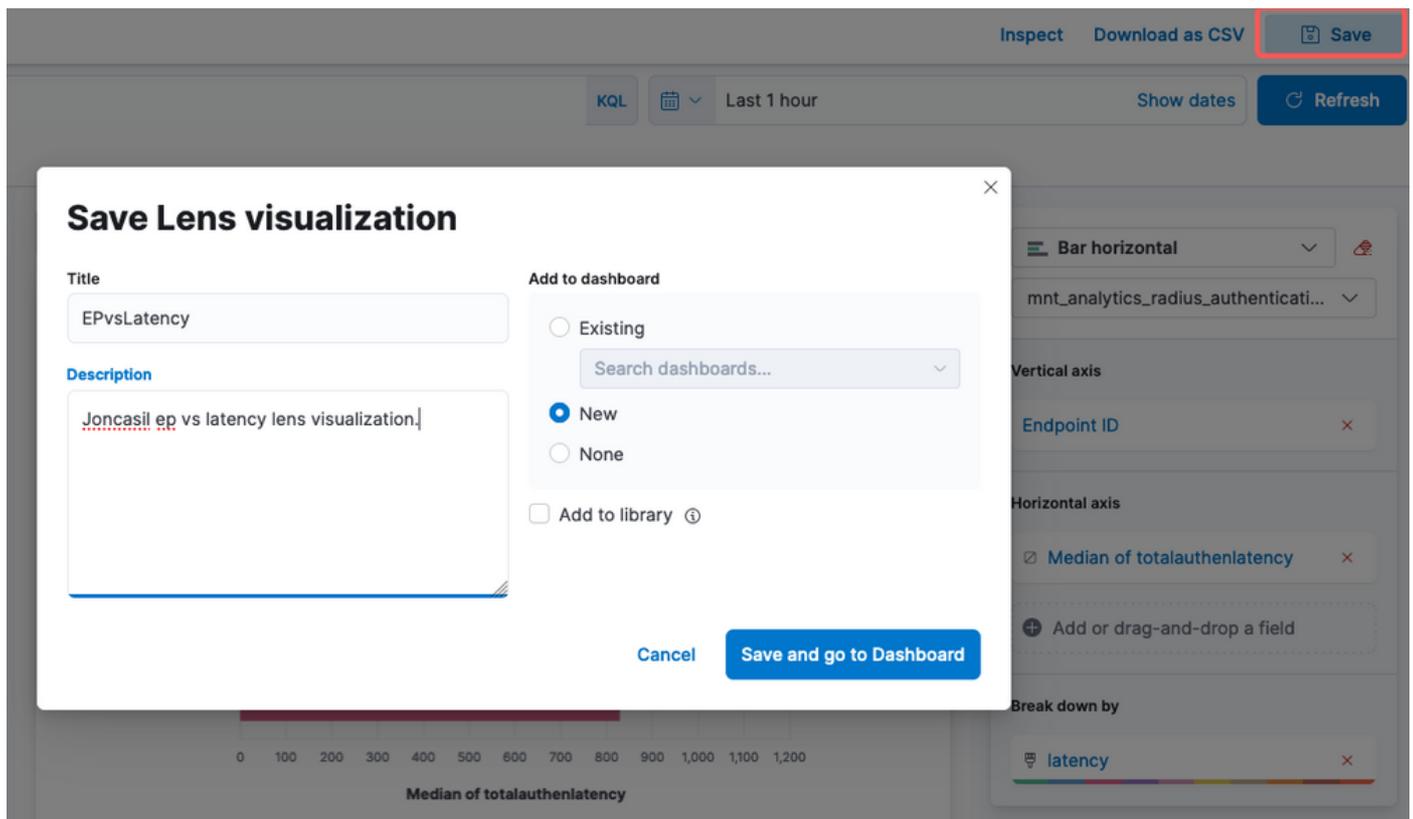
镜头可视化

由于Cisco Bug ID [CSCwh48057](#)，左侧面板未显示可用的字段可供使用。但是，您可以从右侧选择所需的字段和图样式。在本例中，由于身份验证延迟是一个共同关注的主题，因此构建该图是为了直观显示身份验证延迟与终端ID。



终端ID与延迟

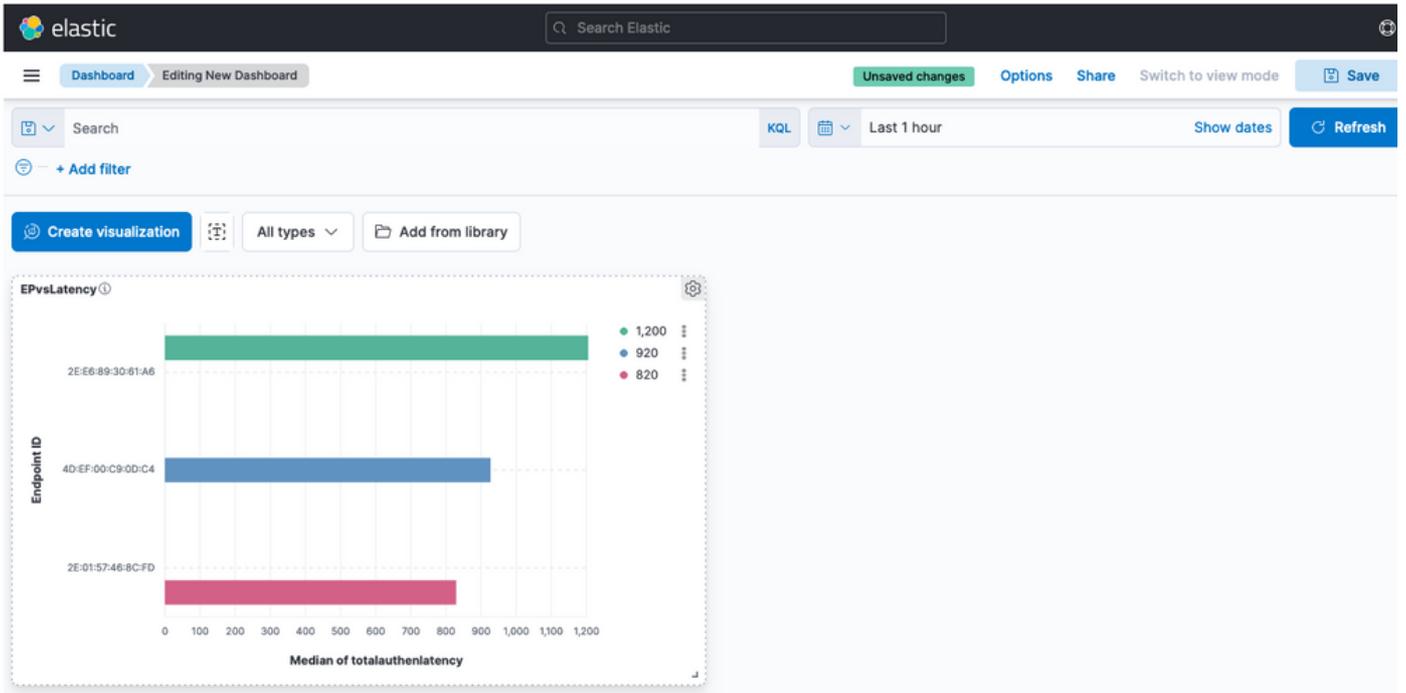
完成后，您可以点击 Save 按钮，如图所示。



保存可视化

第三步：创建控制面板

它会自动将新的可视化添加到新的控制面板中。请记住，Kibana控制面板使用户能够根据Elasticsearch索引中存储的数据创建、自定义和共享交互式可视化效果和报告。



新控制面板

故障排除

- 验证ELK堆栈服务是否在MNT上运行。
- 由于Kibana、Logstash和Elasticsearch在容器上运行，日志位于：

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

相关信息

- [ISE 3.3管理指南](#)
- [Kibana文档](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。