瞭解ISE上的日誌分析 — ELK堆疊

目錄

簡介

本文檔介紹內建Cisco Identity Services Engine(ISE)3.3至System 360日誌分析的ELK堆疊元件。

必要條件

需求

思科建議您瞭解以下主題：

- 思科ISE
- ELK堆疊

採用元件

本文檔中的資訊基於Cisco ISE 3.3。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

系統360包括監控和日誌分析。

Monitoring功能使您能夠從集中控制檯監視各種應用程式和系統統計資訊，以及部署中所有節點的關鍵效能指標(KPI)。KPI有助於深入瞭解節點環境的整體運行狀況。統計資訊提供了系統配置和特定於利用率的資料的簡化表示。

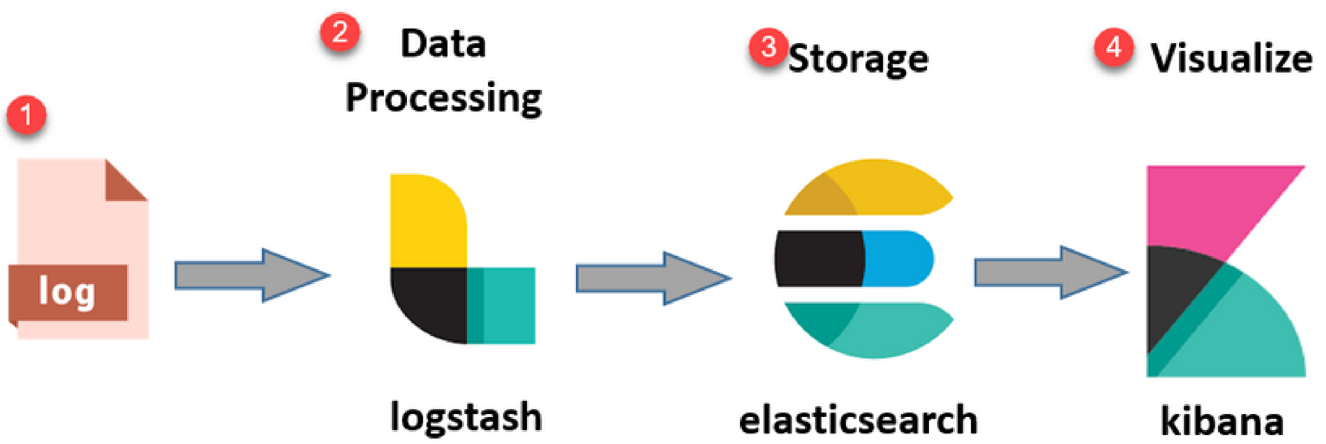
日誌分析提供靈活的分析系統，用於深入分析終端身份驗證、授權和記帳(AAA)以及分析系統日誌資料。您還可以分析思科ISE運行狀況摘要和處理狀態。您可以生成類似於思科ISE計數器和運行狀況摘要報告的報告。

ELK堆疊

ELK Stack是一種常用的開源軟體堆疊，用於收集、處理和視覺化大量資料。它代表Elasticsearch、Logstash和Kibana。

- Elasticsearch:Elasticsearch是一個分散式搜尋和分析引擎。它旨在以近乎即時的方式快速儲存、搜尋和分析大量資料。它使用基於JSON的查詢語言並且高度可擴展。
- Logstash:Logstash是一個資料處理管道，用於接收、處理和轉換來自多個源的資料。它可以對資料進行解析和豐富，使其更結構化，更適合分析。Logstash支援各種輸入源和輸出目標。
- Kibana:Kibana是一個與Elasticsearch配合使用的資料視覺化平台。它允許使用者建立互動式儀表板、圖表、圖形和視覺化，以瀏覽和瞭解Elasticsearch中儲存的資料。Kibana的介面方便了資料的查詢和視覺化。

結合使用時，這些元件可形成強大的堆疊，用於管理和分析各種型別的資料（從日誌檔案到指標等），同時提供視覺化功能來理解資訊。

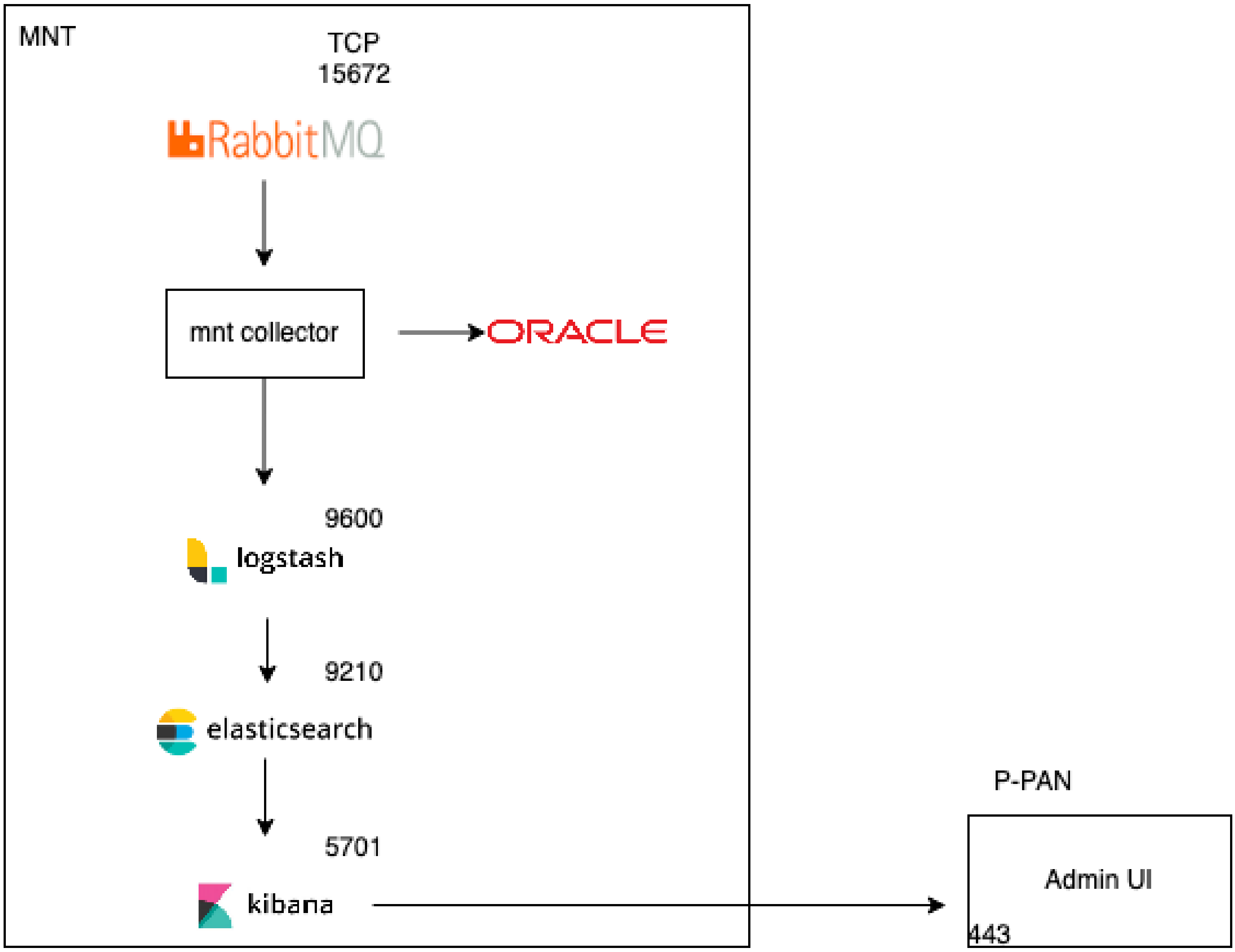


ELK堆疊流

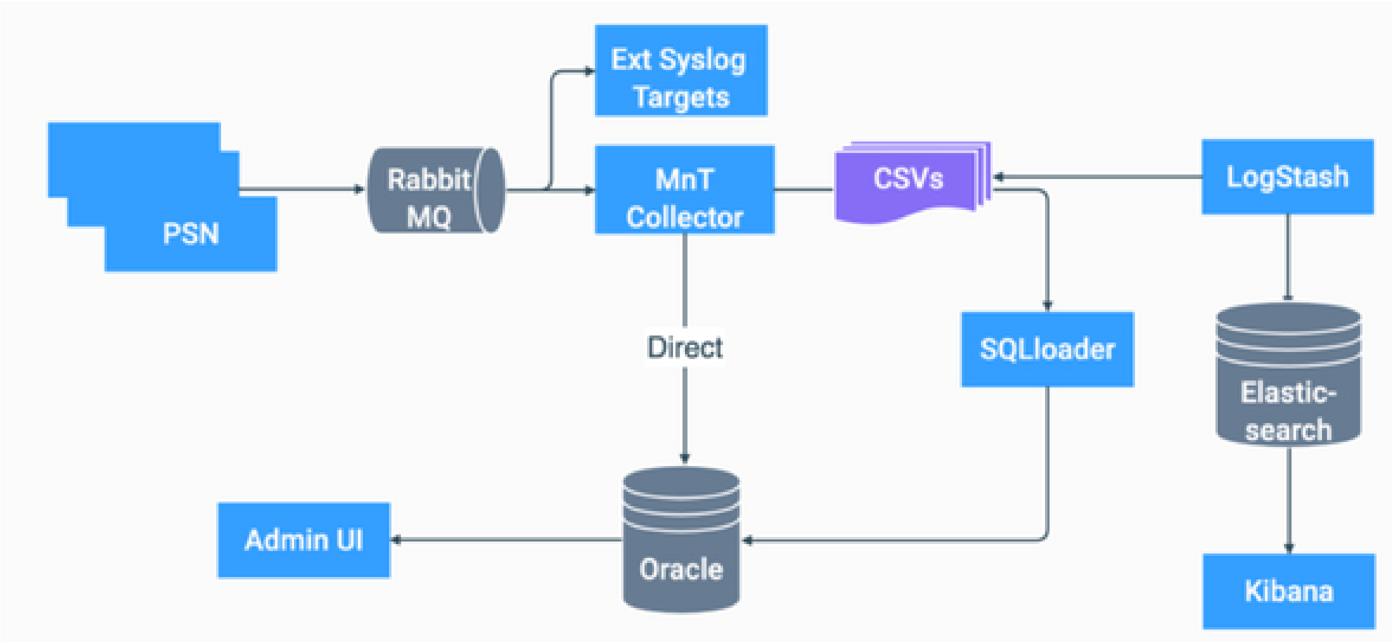
作為日誌分析的ELK堆疊

- ElasticSearch+LogStash+Kibana堆疊的單獨例項僅在MnT節點上運行。
  - 這與情景可視性的Elasticsearch沒有任何關聯。
  - 運行ELK 7.17

- 主要和輔助MNT具有各自的ELK例項。
  - Kibana僅在輔助MNT上啟用（如果可用），僅顯示來自此節點的資料。
- 預設情況下禁用日誌分析。
- 衝減Oracle資源。
- 儲存最長7天的資料。
- 日誌分析使用的總資料大小限製為10 GB。
  - 一旦達到任何限制，ElasticSearch就會清除資料。



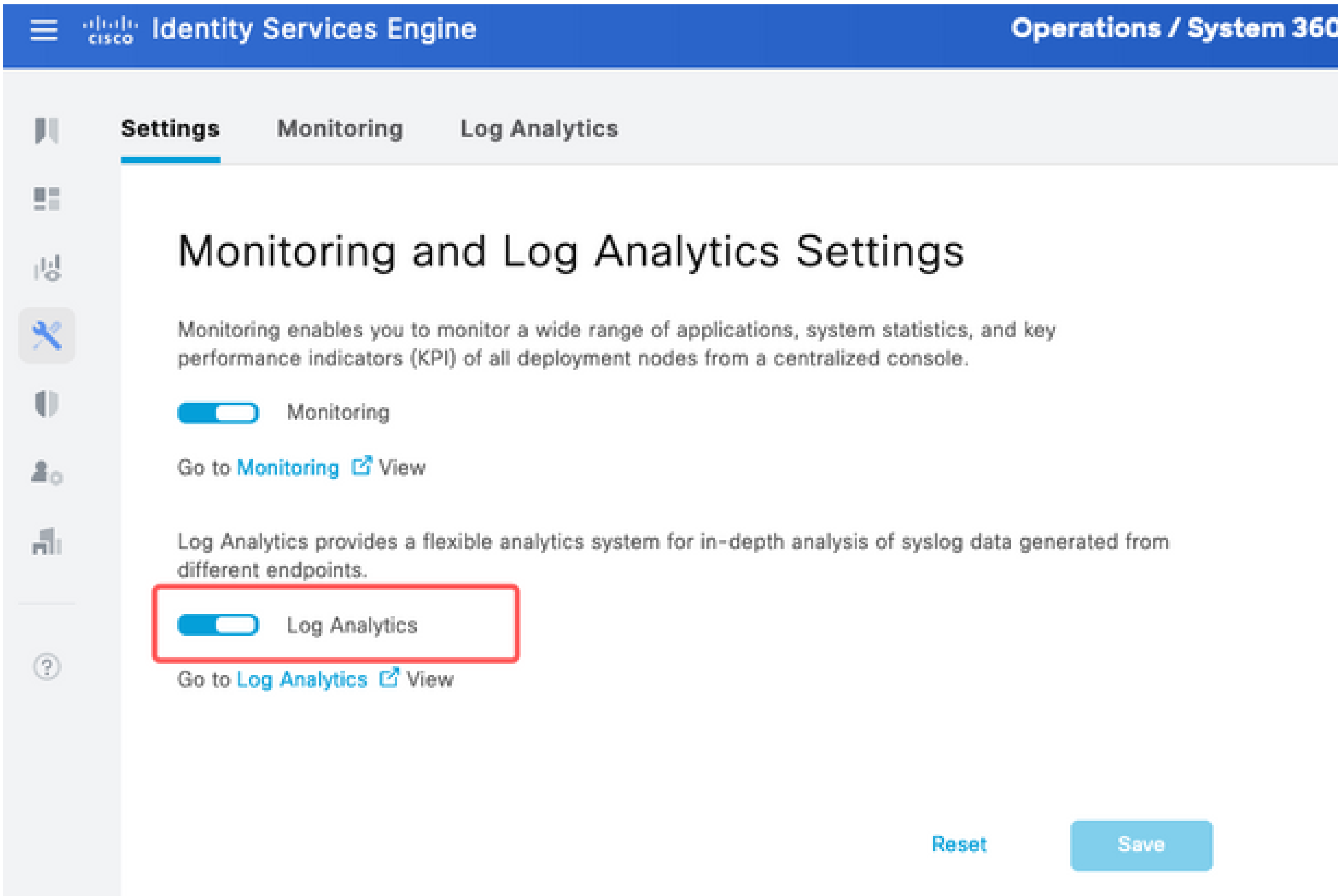
作為日誌分析的ELK流



ISE中ELK的流程圖

啟用日誌分析

日誌分析在ISE上預設禁用。要啟用它，請導航至 Operations > System 360 > Settings 如下圖所示。



啟用日誌分析

ISE大約需要一分鐘來初始化ELK堆疊，您可以使用 show app stat ise.

此外，還可以從根目錄檢查容器狀態。

<#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

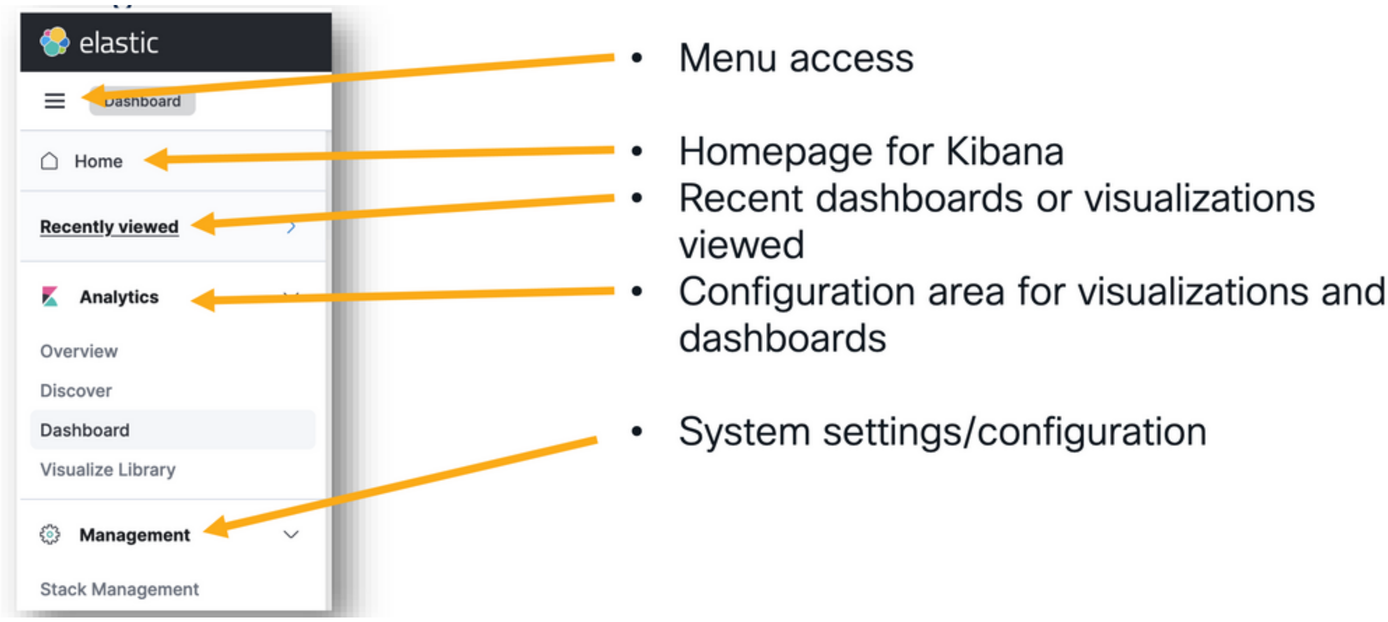
ISE Logstash Service running 614339

ISE Kibana Service running 616064

```
ISE Native IPSec Service running 75883
MFC Profiler running 651910
```

導航選單

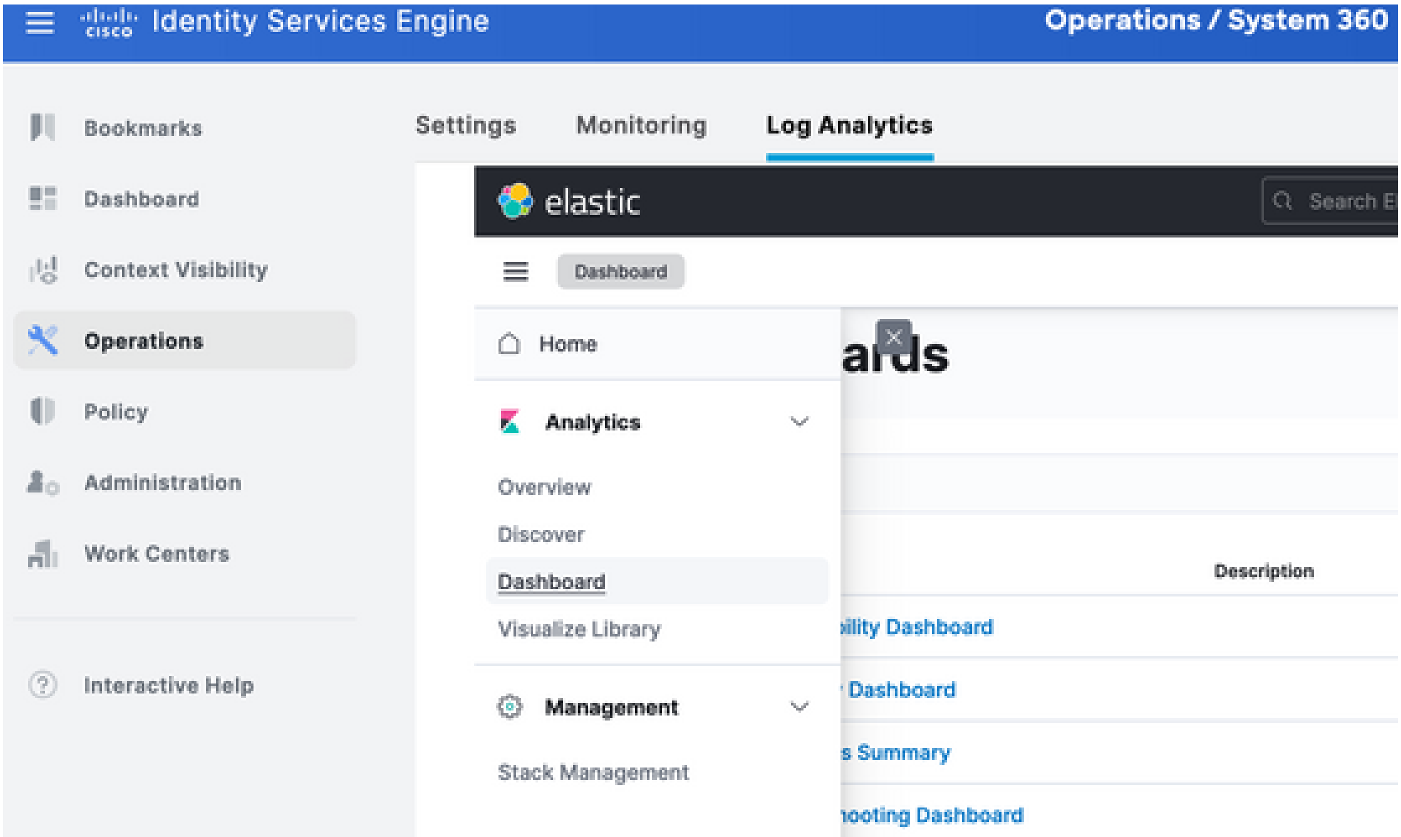
ELK服務啟動後，您就可以訪問Elastic導航選單。



導航選單

內建控制面板

- 預設情況下，ISE具有內建控制面板，其中包含來自Radius、TACACS、系統效能和ISE觀察的資料。
- 您可以通過導航至 Operations > Log Analytics 。
  - Elastic UI開啟後，按一下 Sandwich Menu > Analytics > Dashboards 。



內建控制面板

- ISE 3.3上的可用儀表板。

Title	Description	Tags	Actions
ISE Observability Dashboard			
ISE Overview Dashboard			
ISE Processes Summary			
ISE Troubleshooting Dashboard			
Profiler Performance			
Profiler Summary			
RADIUS Accounting Summary			
RADIUS Authentication Summary			
RADIUS Performance			
RADIUS Step Latency			
TACACS Accounting Summary			
TACACS Authentication Summary			

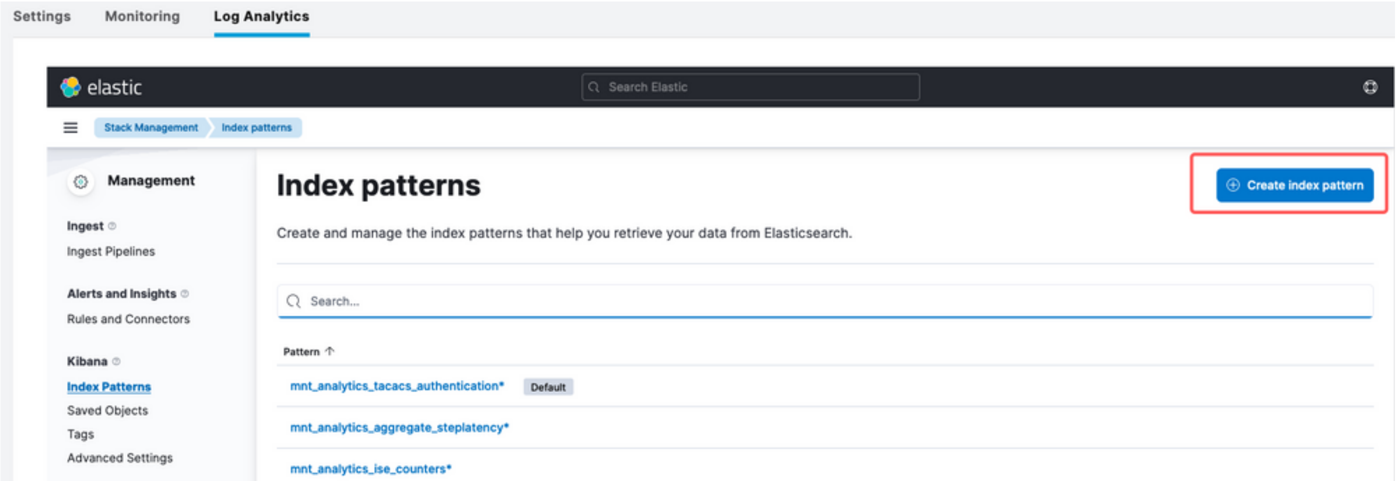
ISE 3.3日誌分析儀表板

建立新儀表板

步驟 1.建立索引模式（資料來源）

在Kibana中，「索引模式」是允許定義Kibana如何與一個或多個彈性搜尋索引互動的配置。

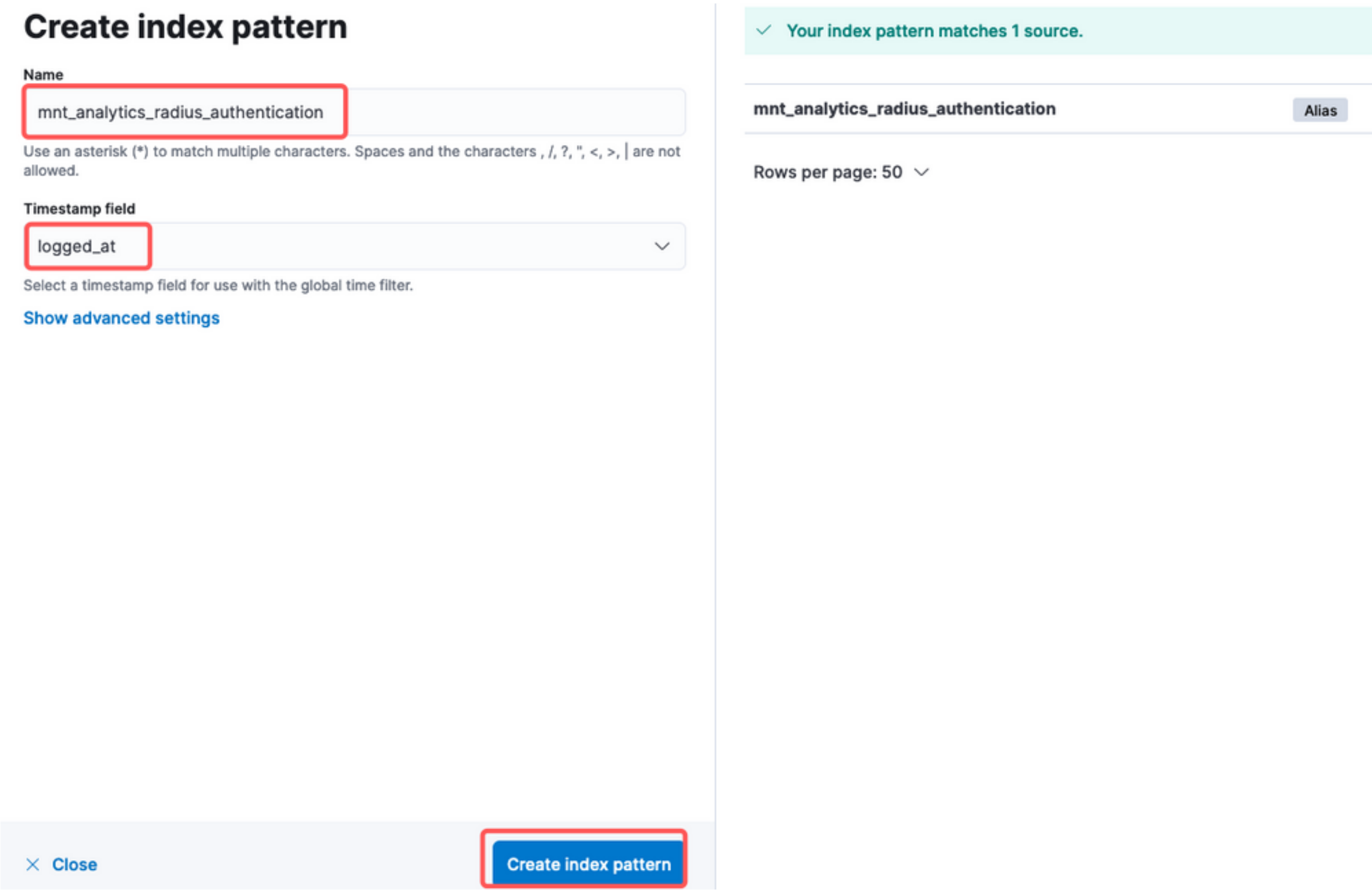
導航至 Management > Stack Management > Kibana > Index Patterns，然後按一下 Create Index Pattern 如下圖所示。



建立索引模式

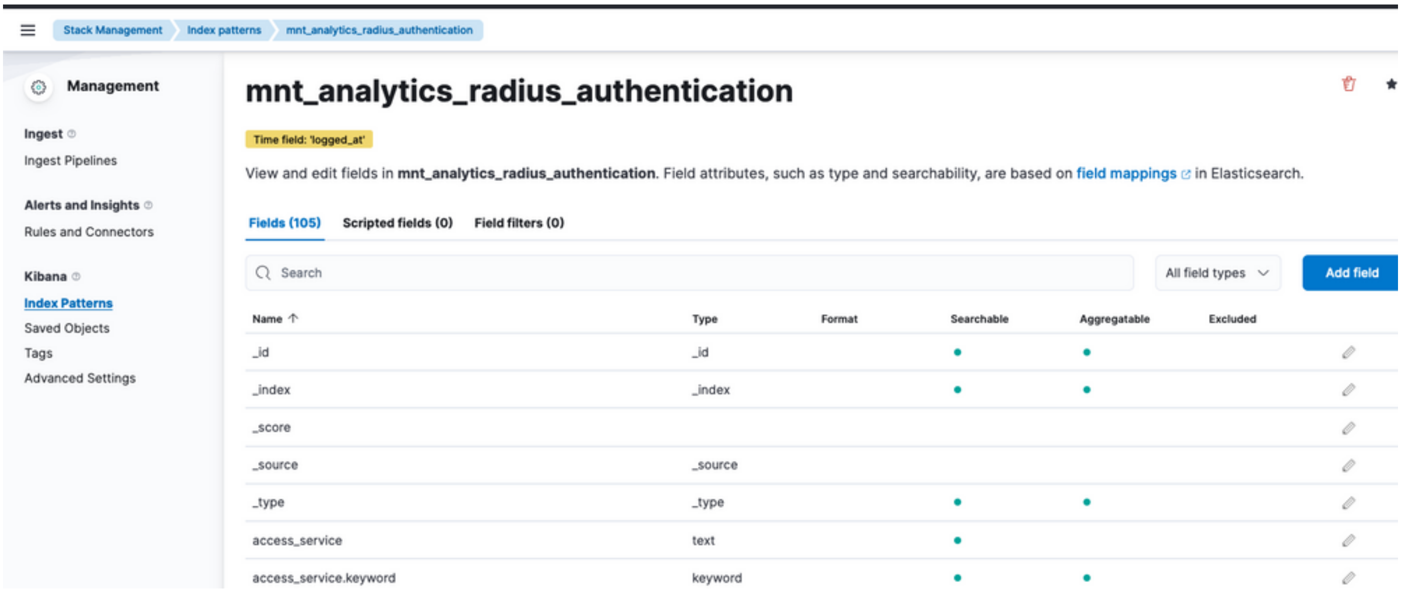
下一個視窗將列出ISE上的所有可用索引。

- 鍵入您感興趣的索引的名稱，它可以是使用*的完全匹配項或萬用字元。
- 選擇Timestamp欄位、logged_at、logged_at_timezone或「我不想使用時間過濾器」。
- 然後，按一下 Create index pattern.



選擇索引

建立後，索引將列出所有關聯變數，這些變數以後可用於建立視覺化效果。



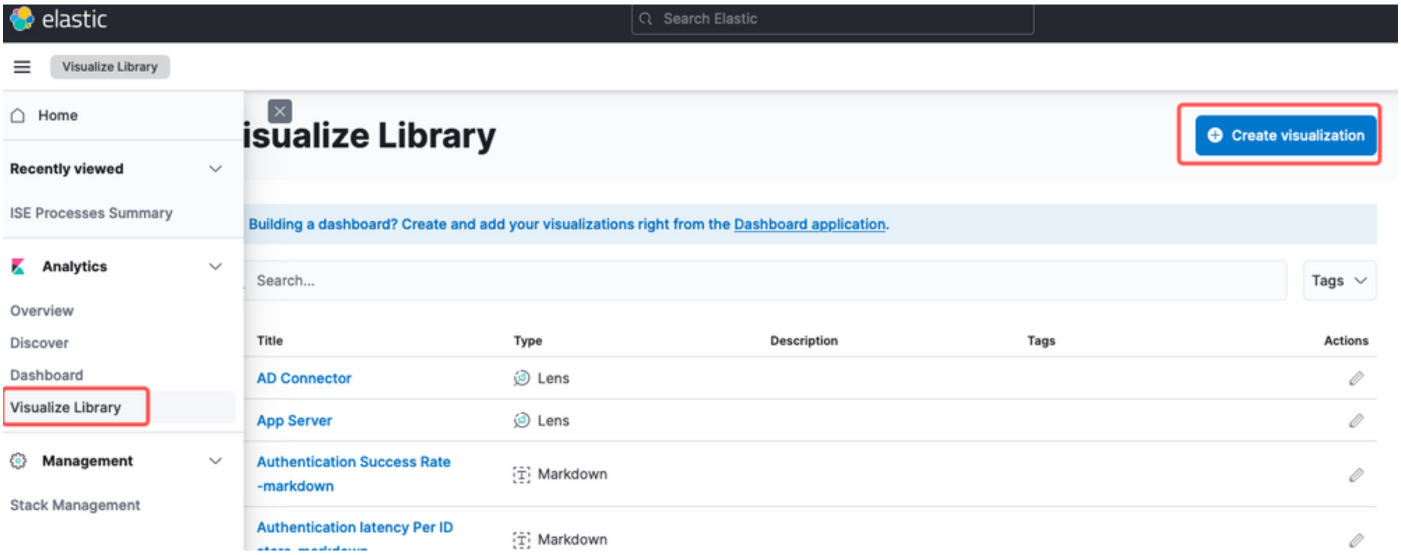
索引變數

步驟 2.建立視覺化效果

在Kibana中，「視覺化」是資料的圖形表示。它們允許您將Elasticsearch中儲存的資料轉換為有意義的圖表、圖形和圖，以便更容易理解和分析。以下是您可以建立的常見視覺化型別：

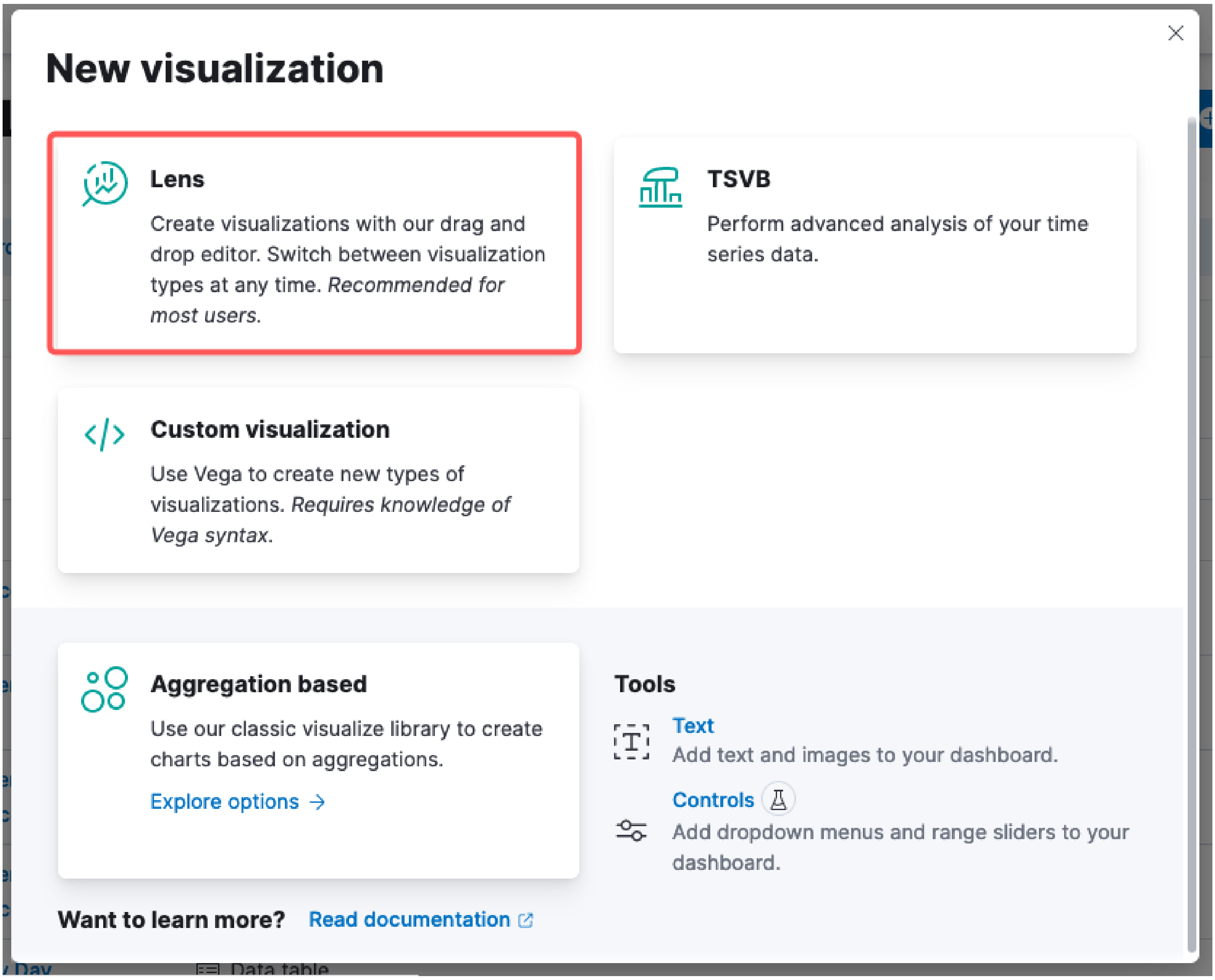
- Lens:使用拖放編輯器建立視覺化。建議。
- 條形圖：這些條形圖以垂直條形圖顯示資料，便於跨類別或時間間隔比較值。
- 折線圖：折線圖將資料顯示為一系列通過折線連線的資料點。它們對於直觀顯示隨時間變化的趨勢非常有用。
- 餅圖：餅圖以圓形圖形表示資料，餅圖的每個段表示一個類別，段的大小表示其比例。
- 面積圖：與折線圖類似，面積圖也顯示隨時間變化的趨勢，但是它們填充了線條下的區域，從而更易於檢視變化的幅度。
- 熱圖：熱圖使用顏色來表示矩陣或網格中的資料值。它們有助於顯示資料的濃度或變化。
- 度量可視化：這些顯示單個數值，如計數或平均值。它們通常用於顯示關鍵績效指標(KPI)。
- 資料表：資料表以表格形式顯示原始資料，使您可以檢視詳細資訊並對資料進行排序或篩選。
- 直方圖：直方圖將資料劃分成多個儲存區或間隔，並顯示每個儲存區中資料點的頻率或計數。它們對於理解資料分佈非常有用。
- 座標圖：這些檢視可視覺化地理空間資料，允許您在地圖上顯示資料，並使用各種標籤、顏色或大小來表示資料屬性。
- 標籤雲：標籤雲顯示字頻，每個字的大小表示其在資料集中的重要性或頻率。

導航至 Analytics > Visualize Library ，然後按一下 Create Visualization 如下圖所示。



建立視覺化

選擇首選項的視覺化，在此示例上，Lens更適合實用。



選擇視覺化型別

Kibana Lens，導航專案包括：

- 資料來源選擇：在左側面板中，可以選擇要用於視覺化的資料來源或Elasticsearch索引模式。
- 視覺化畫布：通過拖放欄位、選擇圖表型別和配置圖表設定，在中心區域構建視覺化。
- 視覺化工具欄：在畫布的頂部，您可以找到用於自定義視覺化的工具欄，其中包括用於更改圖表型別、新增篩選器和配置圖表設定的選項。

- 資料面板：在右側，您可以訪問「資料」面板，該面板允許您管理資料轉換、聚合和欄位設定。

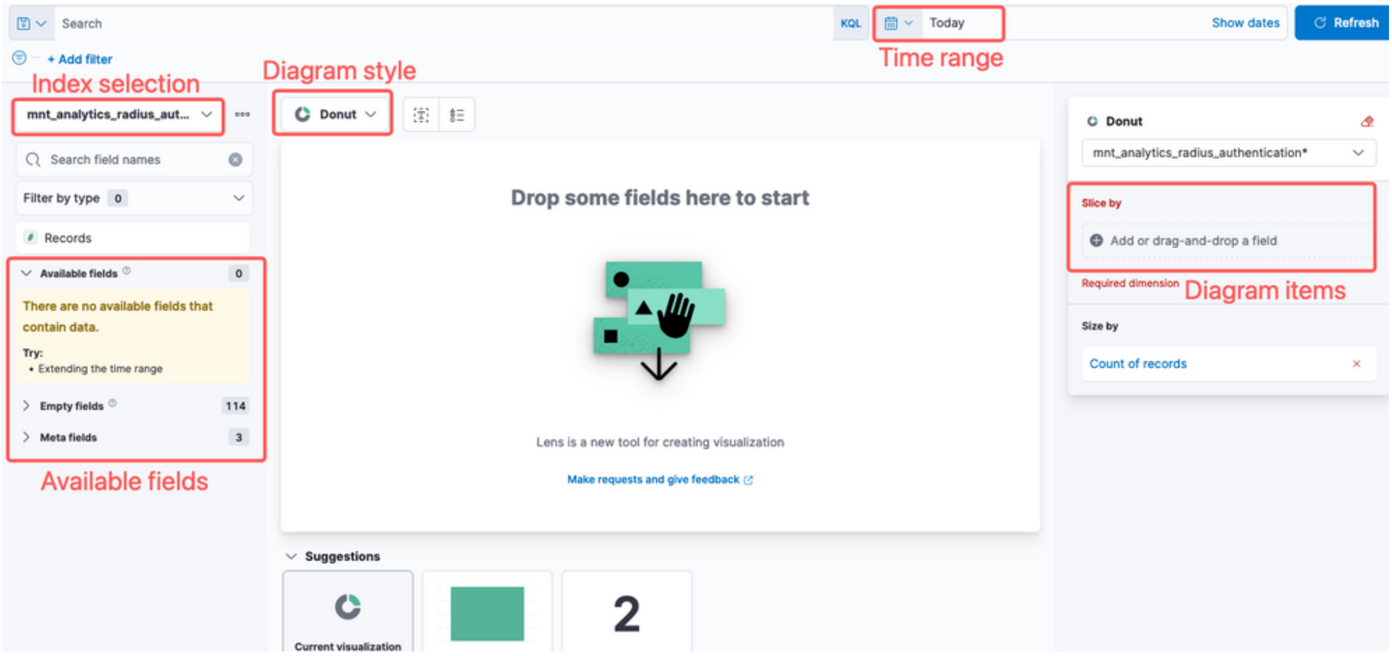
- 圖層管理：根據您正在建立的視覺化型別（例如，分層圖表），可以有一個圖層管理區域，用於在視覺化中配置多個圖層。

- 預覽：在對視覺化進行更改時，通常會提供即時預覽，這樣您就可以使用當前設定檢視圖表的外觀。

- 視覺化設置：根據選定的圖表型別，您可以訪問該視覺化型別的特定設定，如軸配置、顏色方案和標籤。

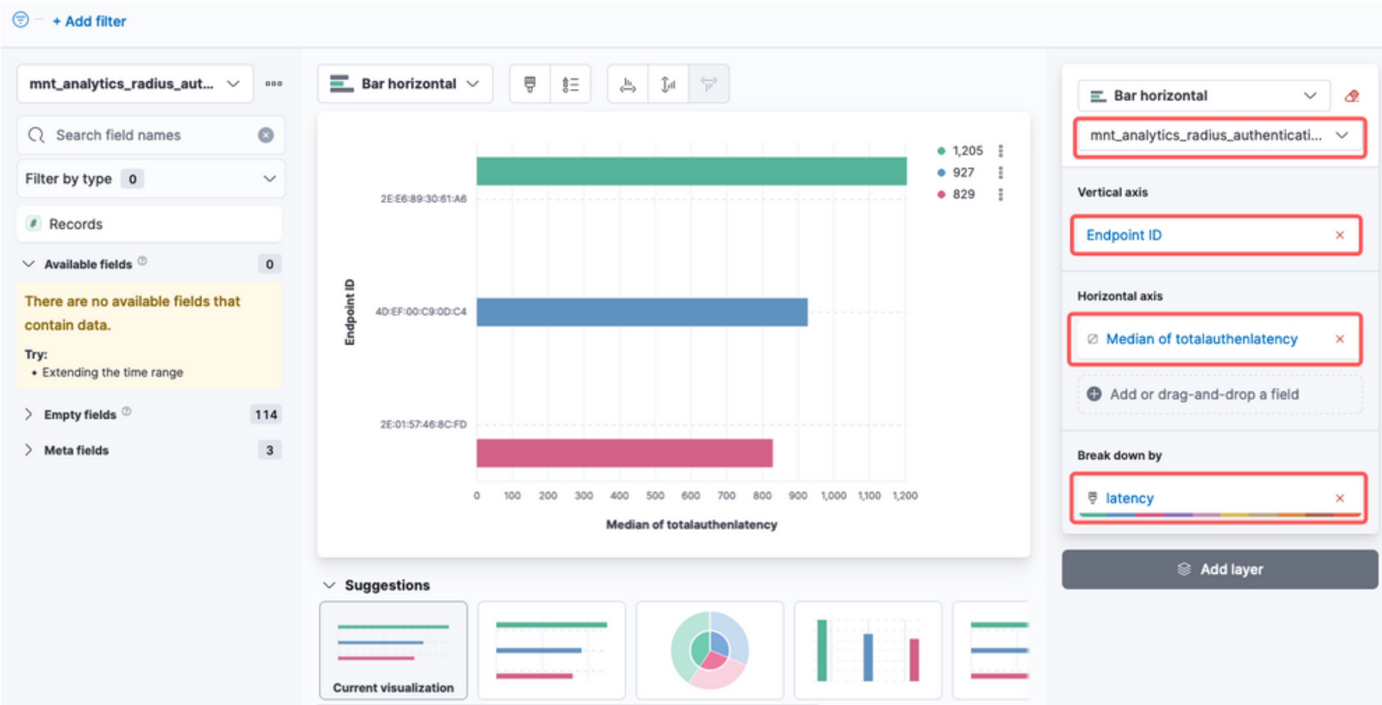
- 互動設置：您可以將互動和操作新增到視覺化，從而允許使用者篩選資料或導航到Kibana儀表板的其它部分。

- 儲存和共享：在Lens介面的頂部，通常有用於儲存您的視覺化、將其新增到儀表板或與他人共用的選項。



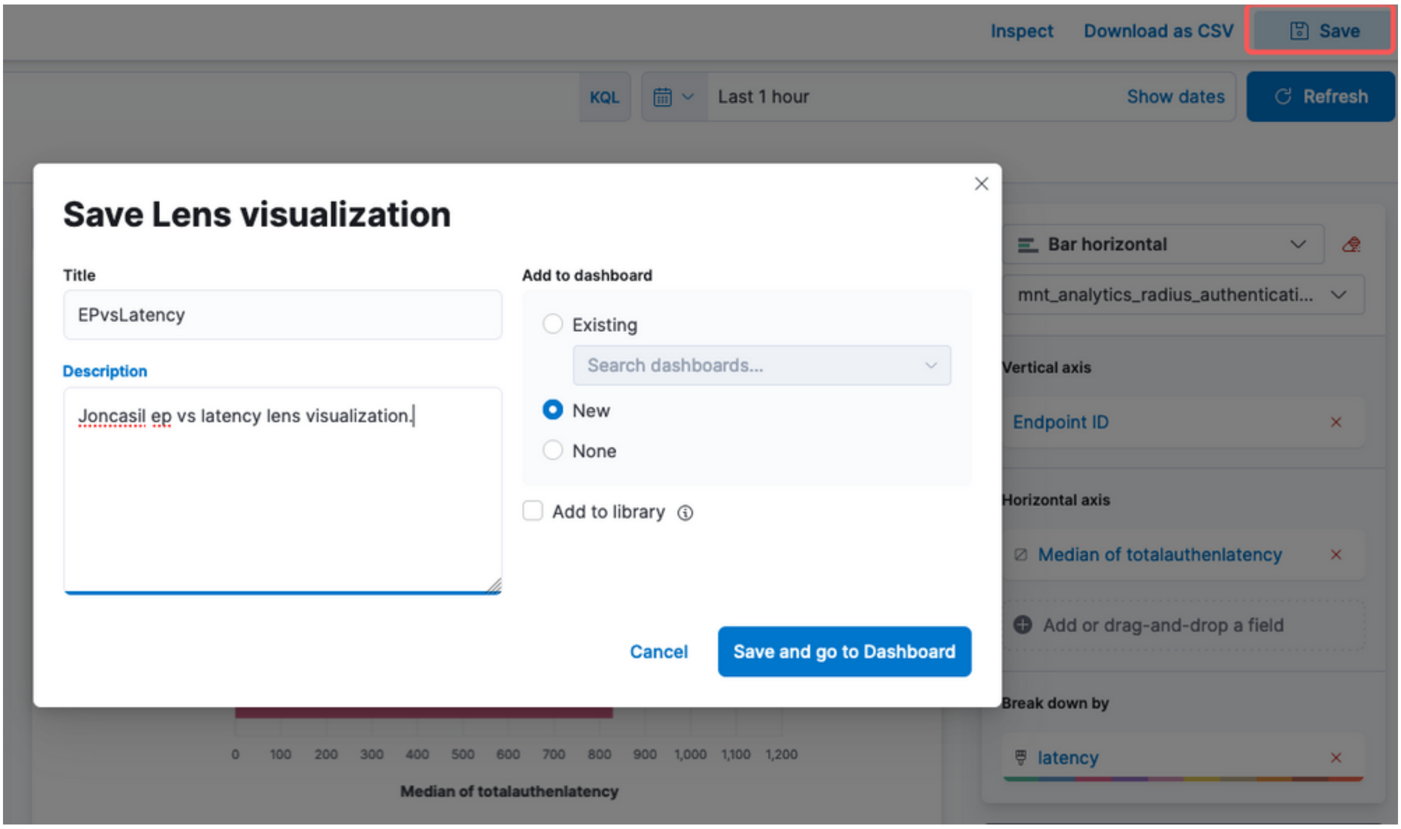
鏡頭視覺化

由於Cisco錯誤ID CSCwh48057，左側面板未顯示可用的欄位可供使用。但是，您可以從右側選擇所需的欄位和圖樣式。在本例中，由於身份驗證延遲是一個常見主題，因此構建該圖是為了直觀顯示身份驗證延遲與終端ID。



終端ID與延遲

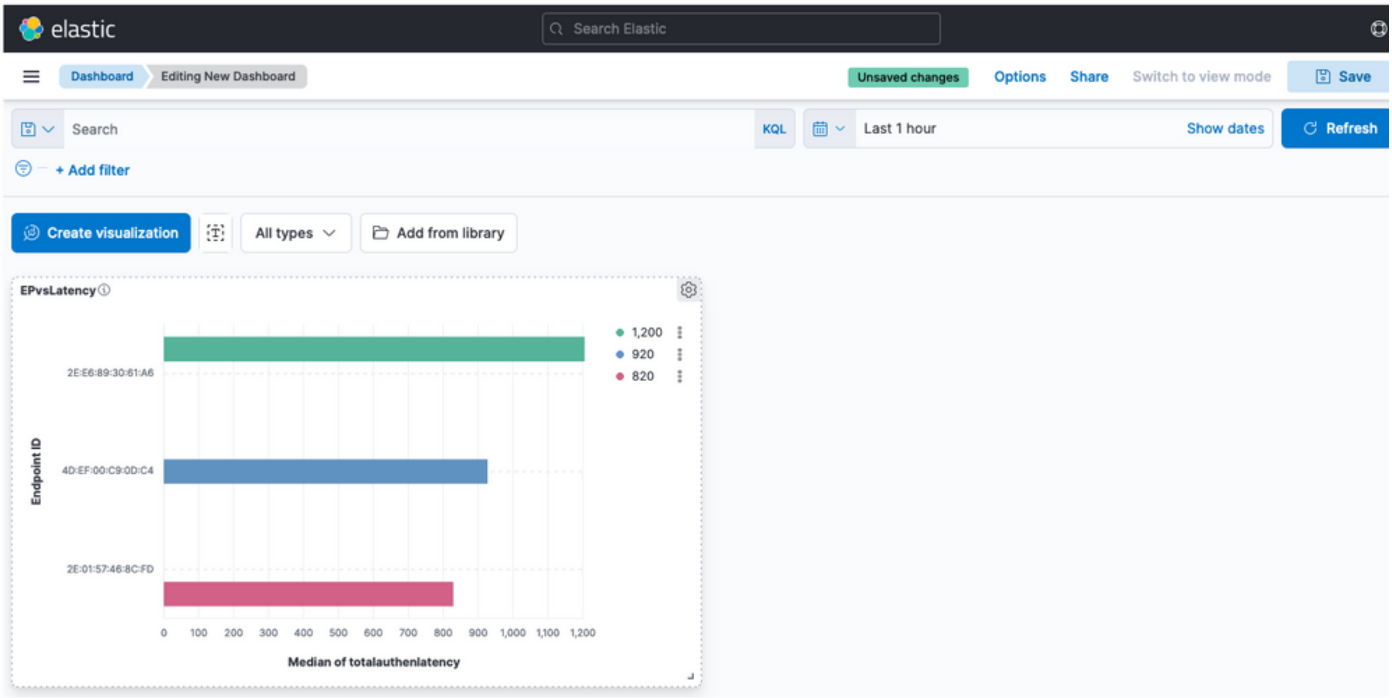
完成後，您可以按一下 Save 按鈕的右上角，如下圖所示。



儲存視覺化

步驟 3.建立儀表板

它自動將新的視覺化內容新增到新的儀表板中。請記住，Kibana儀表板使使用者能夠根據Elasticsearch索引中儲存的資料建立、自定義和共用互動式視覺化效果和報告。



新建儀表板

疑難排解

- 驗證ELK堆疊服務是否在MNT上運行。
- 由於Kibana、Logstash和Elasticsearch在容器上運行，日誌位於：

```
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
```

相關資訊

- [ISE 3.3管理員指南]
- [Kibana文檔]
- [思科技術支援與下載]

關於此翻譯