

# ISEのログ分析ELKスタックについて

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ELKスタック](#)

[ログ分析としてのELKスタック](#)

[ログ分析の有効化](#)

[ナビゲーションメニュー](#)

[組み込みダッシュボード](#)

[新しいダッシュボードの作成](#)

[ステップ 1: インデックスパターンの作成 \(データソース\)](#)

[ステップ 2: 視覚エフェクトの作成](#)

[ステップ 3: ダッシュボードの作成](#)

[\(「トラブルシューティング」\)](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)3.3からSystem 360 Log Analyticsに組み込まれているELKスタックコンポーネントについて説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ISE
- ELKスタック

### 使用するコンポーネント

このドキュメントの情報は、Cisco ISE 3.3に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

System 360には、モニタリングとログ分析が含まれています。

監視機能を使用すると、一元化されたコンソールから展開内のすべてのノードのアプリケーションおよびシステムの広範な統計情報と重要業績評価指標(KPI)を監視できます。KPIは、ノード環境全体の健全性を把握するのに役立ちます。統計情報は、システム構成と使用率固有のデータを簡略化して表示します。

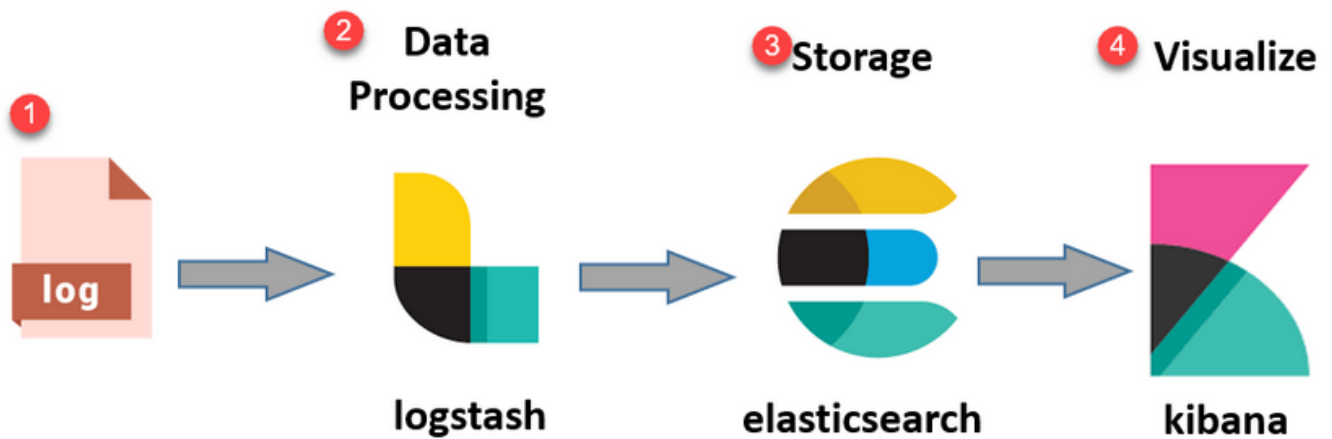
Log Analyticsは、エンドポイントの認証、許可、アカウントティング(AAA)、およびsyslogデータのプロファイリングを詳細に分析するための柔軟な分析システムを提供します。また、Cisco ISEのヘルスサマリーとプロセスのステータスを分析することもできます。Cisco ISE Counters and Health Summaryレポートに類似したレポートを生成できます。

## ELKスタック

ELKスタックは、大量のデータを収集、処理、および可視化するために使用される一般的なオープンソースソフトウェアスタックです。Elasticsearch、Logstash、およびKibanaを表します。

- Elasticsearch:Elasticsearchは分散型検索および分析エンジンです。大量のデータを迅速に、ほぼリアルタイムで保存、検索、分析するように設計されています。JSONベースのクエリ言語を使用し、スケーラビリティに優れています。
- Logstash:Logstashは、複数のソースからデータを取り込み、処理し、変換するデータ処理パイプラインです。データを解析して強化できるため、より構造化され、分析に適しています。Logstashは、幅広い入力ソースと出力先をサポートしています。
- Kibana:KibanaはElasticsearchと連携するデータビジュアライゼーションプラットフォームです。インタラクティブなダッシュボード、チャート、グラフ、ビジュアライゼーションを作成して、Elasticsearchに保存されているデータを調べ、理解することができます。Kibanaのインターフェースにより、データの照会と視覚化が容易になります。

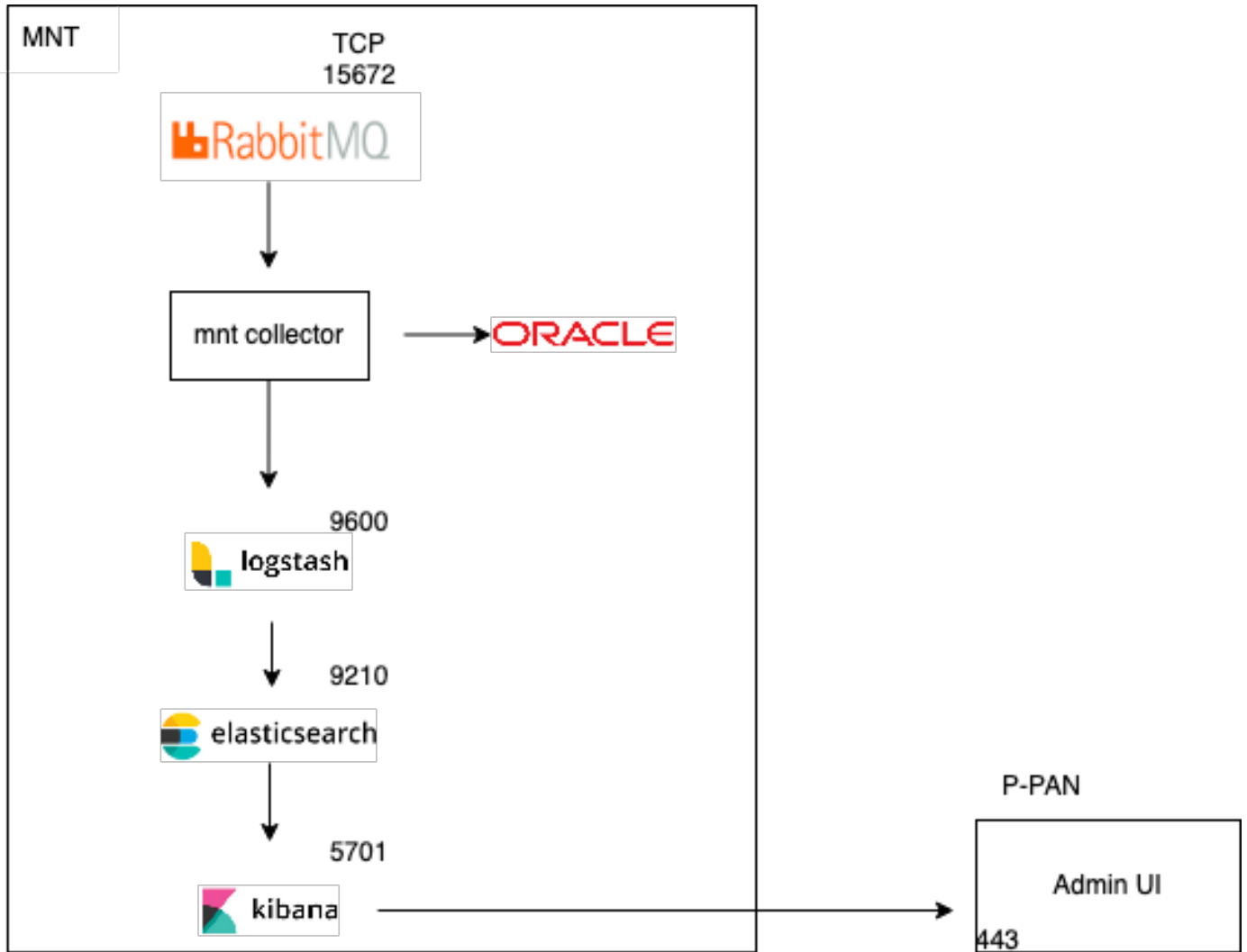
これらのコンポーネントを組み合わせることで、ログ・ファイルから測定値に至るまで、さまざまな種類のデータを管理および分析するための強力なスタックが形成され、情報を理解するためのビジュアライゼーション機能も提供されます。



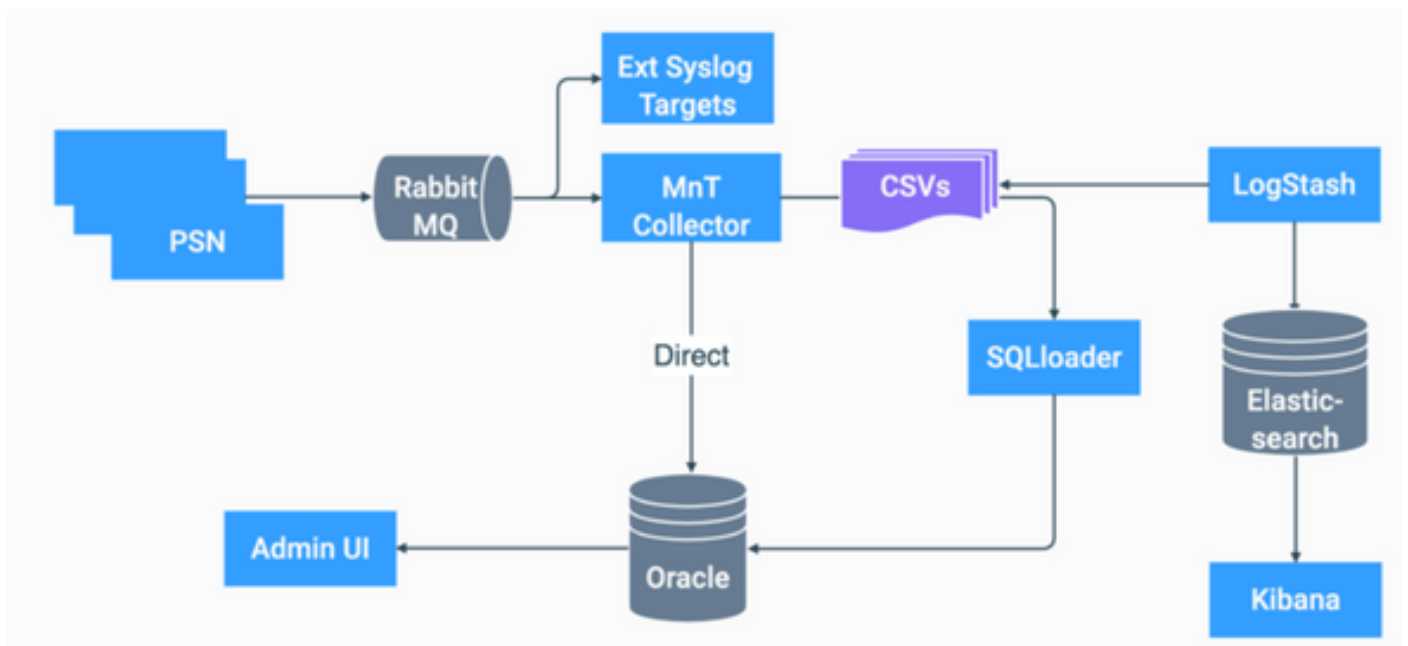
ELKスタックフロー

## ログ分析としてのELKスタック

- ElasticSearch+LogStash+Kibanaスタックの個別のインスタンスは、MnTノードでのみ実行されます。
  - これは、Context-VisibilityのElasticsearchとは何の相関関係もありません。
  - ELK 7.17の実行
- プライマリMNTとセカンダリMNTには、ELKの独自のインスタンスがあります。
  - Kibanaは、セカンダリMNTが使用可能な場合にのみ有効になり、このノードからのデータのみを表示します。
- ログ分析はデフォルトで無効になっています。
- Oracleリソースを消費します。
- 最大7日間のデータを保存します。
- ログ分析で消費されるデータの合計サイズは10 GBに制限されています。
  - いずれかの制限に達すると、ElasticSearchはデータを消去します。



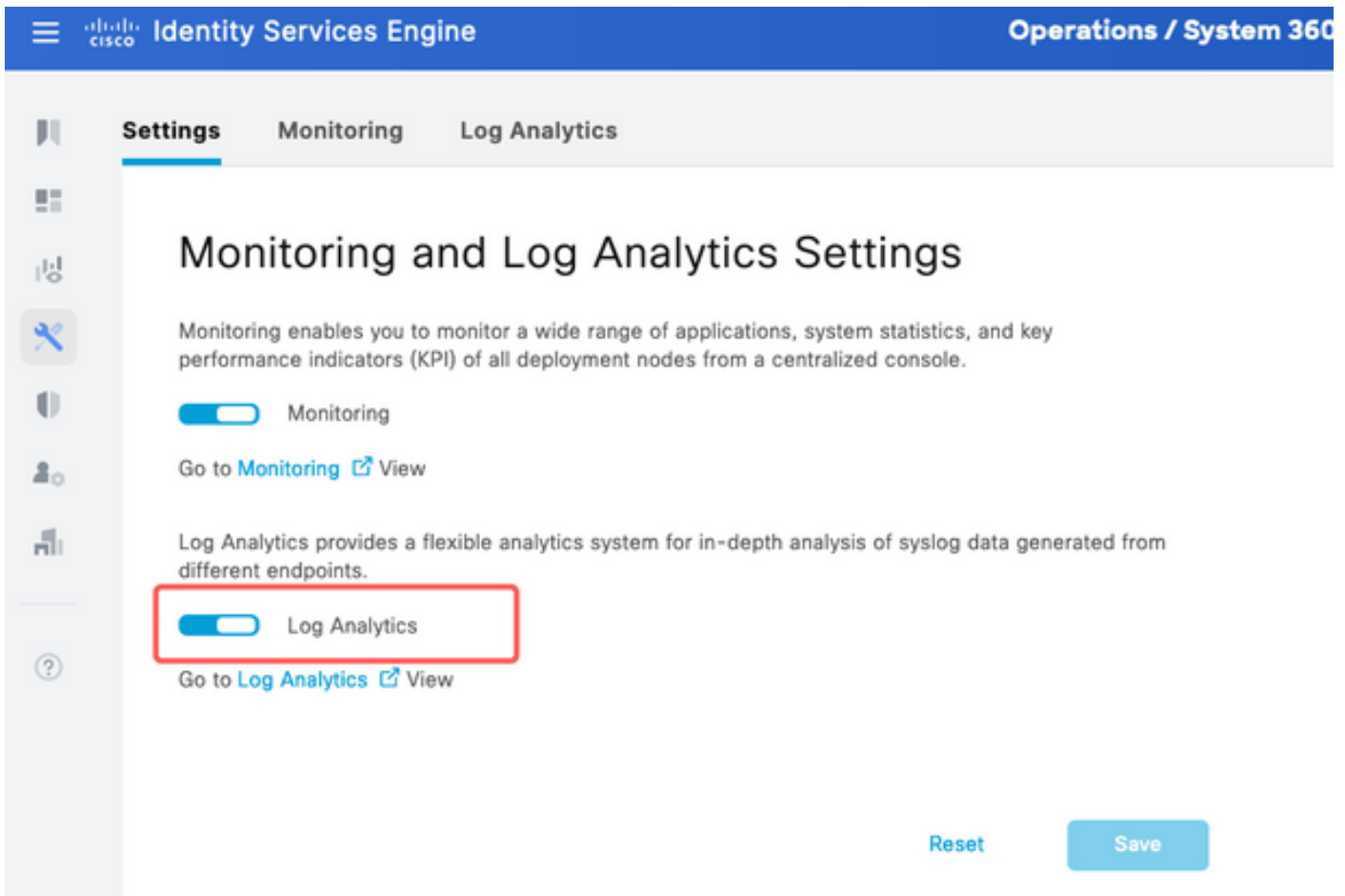
ログ分析としてのELKフロー



ISEでのELKのフローチャート

# ログ分析の有効化

ISEでは、ログ分析はデフォルトで無効になっています。有効にするには、 [Operations > System 360 > Settings](#) 図に示すように。



## ログ分析の有効化

ISEはELKスタックを初期化するのに約1分かかります。次のコマンドでステータスを確認できます。 `show app stat ise` を参照。

また、ルートからコンテナのステータスを確認することもできます。

<#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

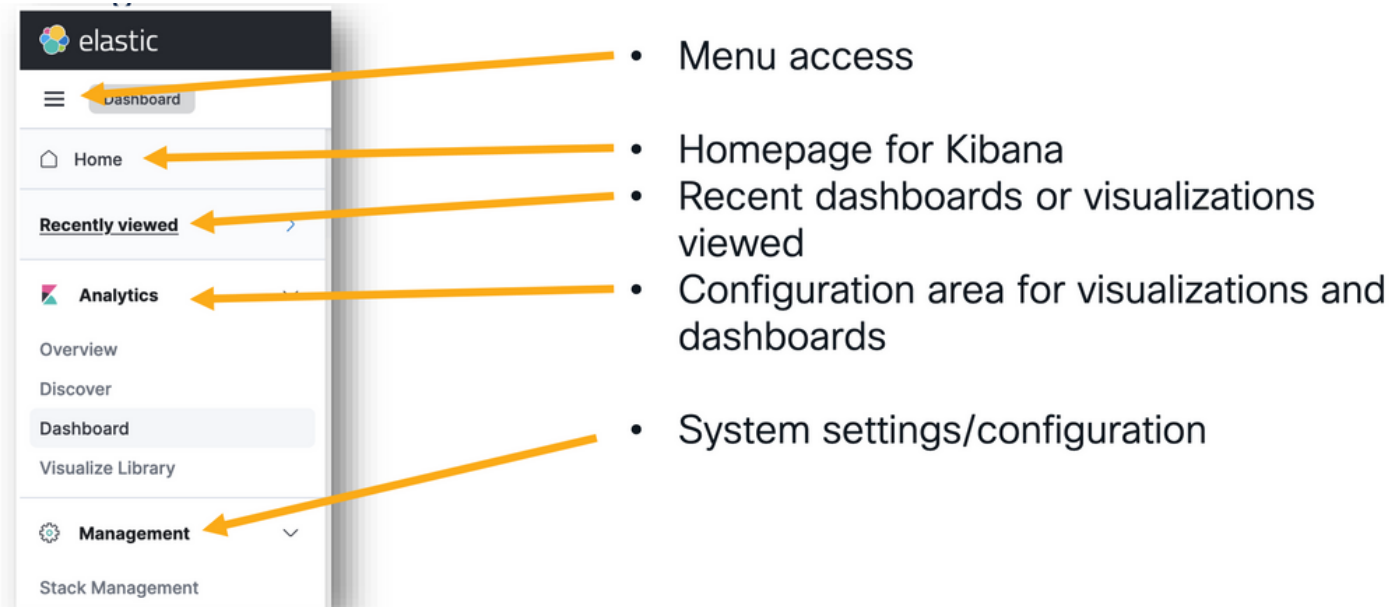
ISE Logstash Service running 614339

ISE Kibana Service running 616064

ISE Native IPSec Service running 75883  
MFC Profiler running 651910

## ナビゲーションメニュー

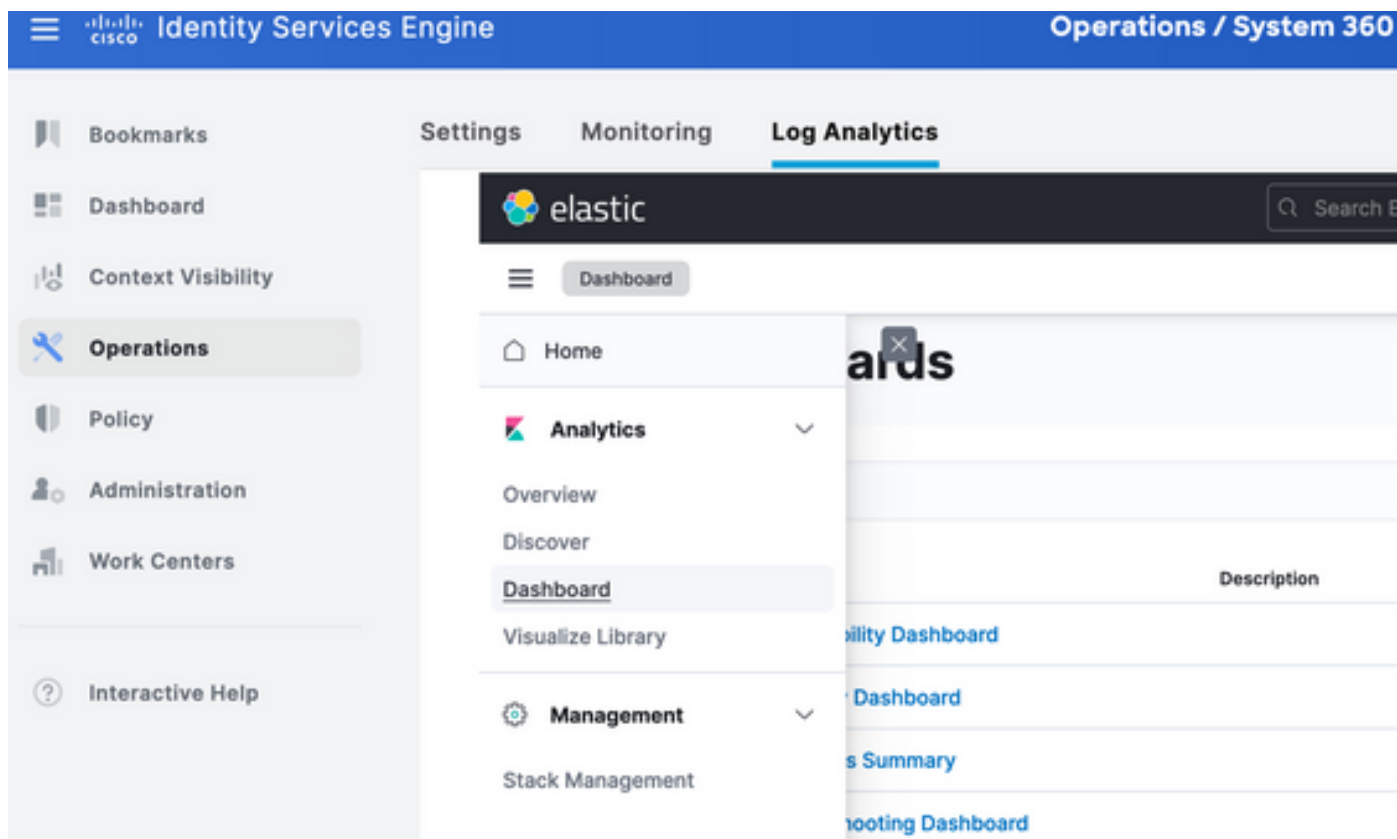
ELKサービスが開始されると、Elasticナビゲーションメニューにアクセスできます。



ナビゲーションメニュー

## 組み込みダッシュボード

- ISEにはデフォルトで、Radius、TACACS、システムパフォーマンス、およびISEの監視可能性からのデータを含むダッシュボードが組み込まれています。
- これらのダッシュボードにアクセスするには、[Operations > Log Analytics](#) を参照。
  - Elastic UIが開いたら、[Sandwich Menu > Analytics > Dashboards](#) を参照。



内蔵ダッシュボード

- ISE 3.3で使用可能なダッシュボード。

<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			

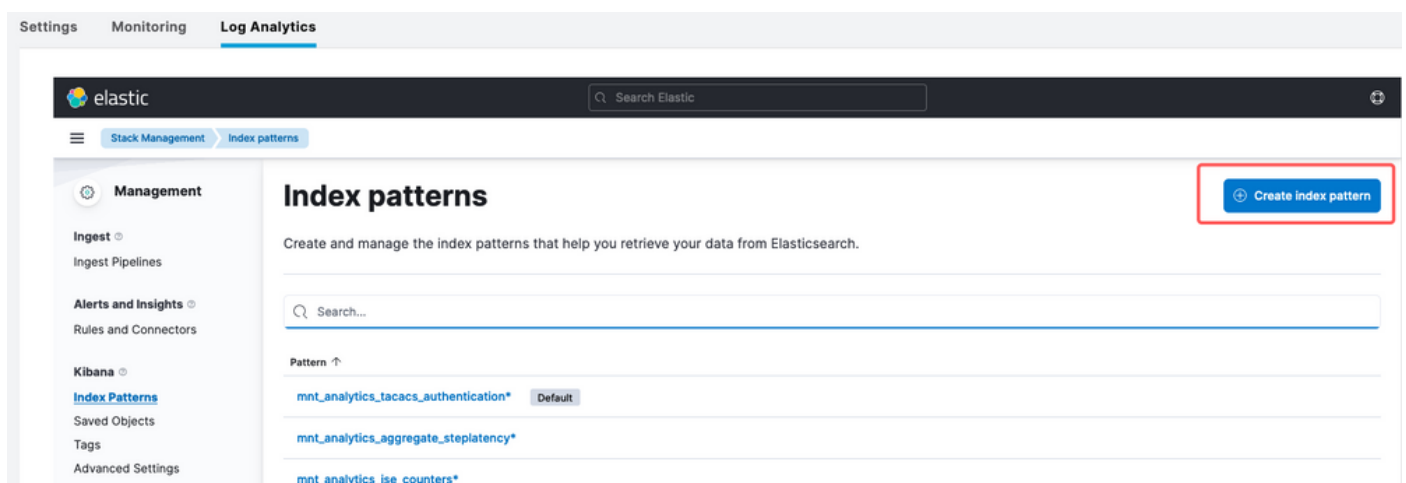
ISE 3.3ログ分析ダッシュボード

## 新しいダッシュボードの作成

### ステップ 1：インデックスパターンの作成（データソース）

Kibanaでは、「インデックスパターン」は、Kibanaが1つ以上のElasticsearchインデックスと相互作用する方法を定義できる設定です。

移動先 Management > Stack Management > Kibana > Index Patterns をクリックし、 Create Index Pattern に示すように



インデックスパターンの作成

次のウィンドウが表示され、ISEで使用可能なすべてのインデックスが一覧表示されます。

- 対象のインデックスの名前を入力します。完全一致または\*を使用したワイルドカードを使用できます。



- Timestamp field、logged\_at、logged\_at\_timezoneまたは「時間フィルタを使用しない」を選択します。
- 次に、 Create index patternを参照。

## Create index pattern

Name

mnt\_analytics\_radius\_authentication

Use an asterisk (\*) to match multiple characters. Spaces and the characters , / ? \* < > | are not allowed.

Timestamp field

logged\_at

Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

✓ Your index pattern matches 1 source.

mnt\_analytics\_radius\_authentication

Alias

Rows per page: 50

× Close

Create index pattern

インデックスの選択

索引を作成すると、後で視覚化の作成に使用できる関連するすべての変数が一覧表示されます。

Stack Management Index patterns mnt\_analytics\_radius\_authentication

### Management

Ingest ⊙  
Ingest Pipelines

Alerts and Insights ⊙  
Rules and Connectors

Kibana ⊙  
[Index Patterns](#)  
Saved Objects  
Tags  
Advanced Settings

## mnt\_analytics\_radius\_authentication

Time field: logged\_at

View and edit fields in mnt\_analytics\_radius\_authentication. Field attributes, such as type and searchability, are based on [field mappings](#) in Elasticsearch.

Fields (105) Scripted fields (0) Field filters (0)

Search

All field types Add field

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
._id	._id		●	●	
._index	._index		●	●	
._score					
._source	._source				
._type	._type		●	●	
access_service	text		●		
access_service.keyword	keyword		●	●	

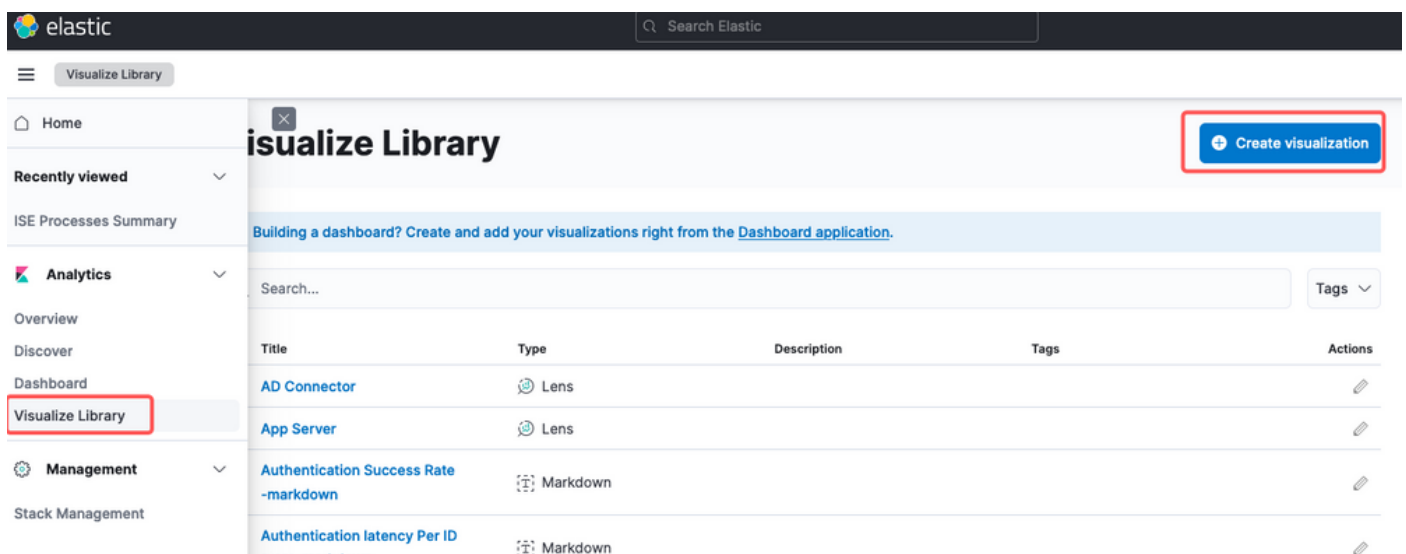
インデックス変数

## ステップ 2：視覚エフェクトの作成

Kibanaでは、「可視化」はデータをグラフィカルに表現したものです。これにより、Elasticsearchに保存されたデータを取得し、わかりやすいチャート、グラフ、図に変換して、理解と分析を容易にすることができます。作成できる視覚エフェクトの一般的なタイプを次に示します。

- レンズ：ドラッグアンドドロップエディタを使用してビジュアライゼーションを作成します。推奨
- 棒グラフ：データを縦棒で表示し、カテゴリや時間間隔で値を簡単に比較できます。
- 折れ線グラフ：折れ線グラフでは、データが線で結ばれた一連のデータポイントとして表示されます。これらは、時間の経過に伴う傾向を視覚化するのに役立ちます。
- 円グラフ：円グラフは円グラフでデータを表し、円の各セグメントはカテゴリを表し、セグメントのサイズはその比率を表します。
- 面グラフ：面グラフは、折れ線グラフと同様に、時間の経過に伴う傾向も示しますが、線の下領域を埋め、変化の大きさを確認しやすくなります。
- ヒートマップ：ヒートマップでは、色を使用してマトリックスまたはグリッド内のデータ値を表します。これらは、データの濃度や変動を示すのに便利です。
- メトリック可視化：カウントや平均などの単一の数値を表示します。これらは、主な業績評価指標(KPI)を示すためによく使用されます。
- データテーブル：データテーブルは生データを表形式で表示し、詳細情報を表示したり、データを並べ替えたりフィルタ処理したりできます。
- ヒストグラム：データをビンまたは間隔に分割し、各ビンのデータポイントの頻度または数を表示します。データの分布を理解するのに役立ちます。
- 座標マップ：空間データを視覚化し、マップ上にデータを表示し、さまざまなマーカー、色、サイズを使用してデータ属性を表すことができます。
- タグクラウド：タグクラウドには、単語の頻度が表示されます。各単語のサイズは、データセット内の重要度または頻度を示します。


移動先 [Analytics > Visualize Library](#) をクリックし、 [Create Visualization](#) 図に示すように。





ビジュアル化の作成


この例では、好みの視覚化を選択してください実用性のためにレンズが優先されます。

# New visualization


 **Lens**  
Create visualizations with our drag and drop editor. Switch between visualization types at any time. *Recommended for most users.*



 **TSVB**  
Perform advanced analysis of your time series data.


 **Custom visualization**  
Use Vega to create new types of visualizations. *Requires knowledge of Vega syntax.*

 **Aggregation based**  
Use our classic visualize library to create charts based on aggregations.  
[Explore options](#) →

**Tools**

 **Text**  
Add text and images to your dashboard.

 **Controls**   
Add dropdown menus and range sliders to your dashboard.

**Want to learn more?** [Read documentation](#) 

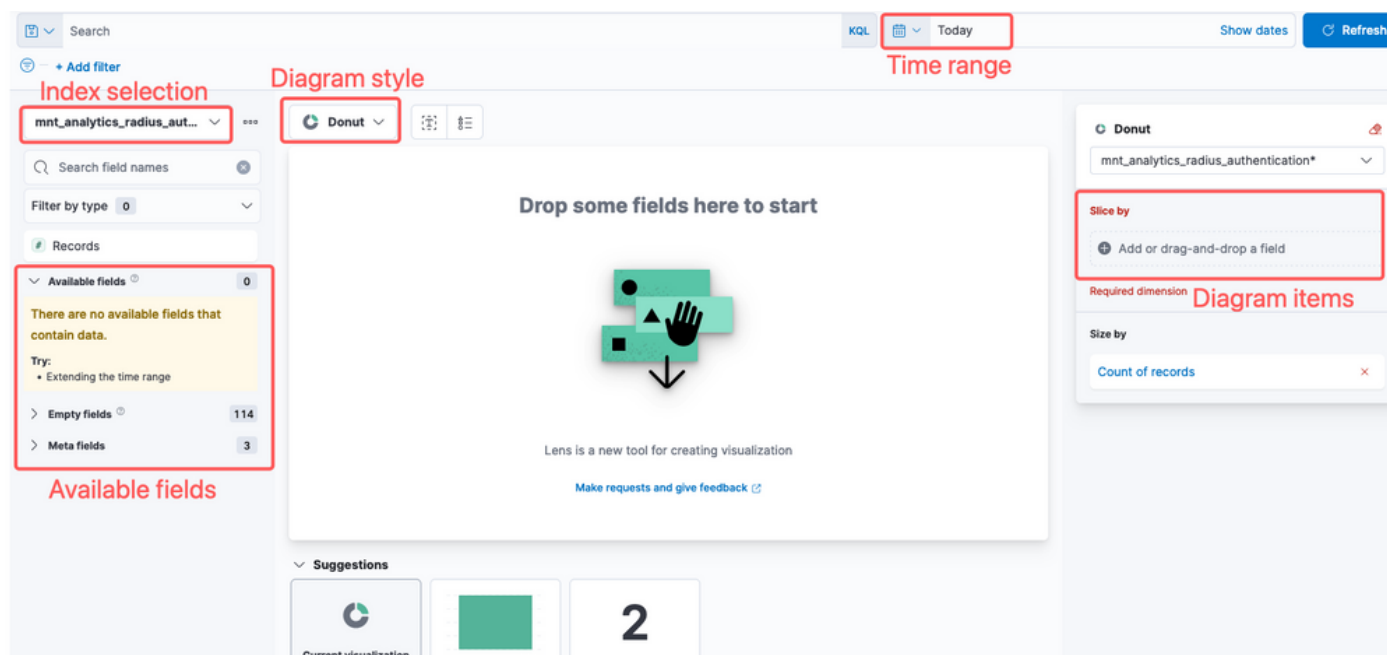
ビジュアル化の種類の選択

Kibana Lensのナビゲーションアイテムは次の要素で構成されています。

- データソースの選択：左側のパネルで、視覚化に使用するデータソースまたはElasticsearchインデックスパターンを選択できます。
- Visualization Canvas：中央の領域では、フィールドのドラッグアンドドロップ、グラフの種類の選択、およびグラフ設定の構成によってビジュアライゼーションを作成します。
- Visualizationツールバー：キャンバスの上にあるツールバーを使用すると、グラフの種類の変更、フィルタの追加、およびグラフ設定の構成のオプションなど、ビジュアライゼーションをカスタマイズできます。
- データパネル：右側の「データ」パネルにアクセスして、データ変換、集計、フィールド設定を管理できます。
- レイヤ管理：作成するビジュアライゼーションのタイプ（たとえば、階層型チャート）に応じて、ビジュアライゼーションで複数のレイヤを設定するためのレイヤ管理領域を設定できます。
- プレビュー：ビジュアライゼーションに変更を加えると、通常はリアルタイムのプレビュー

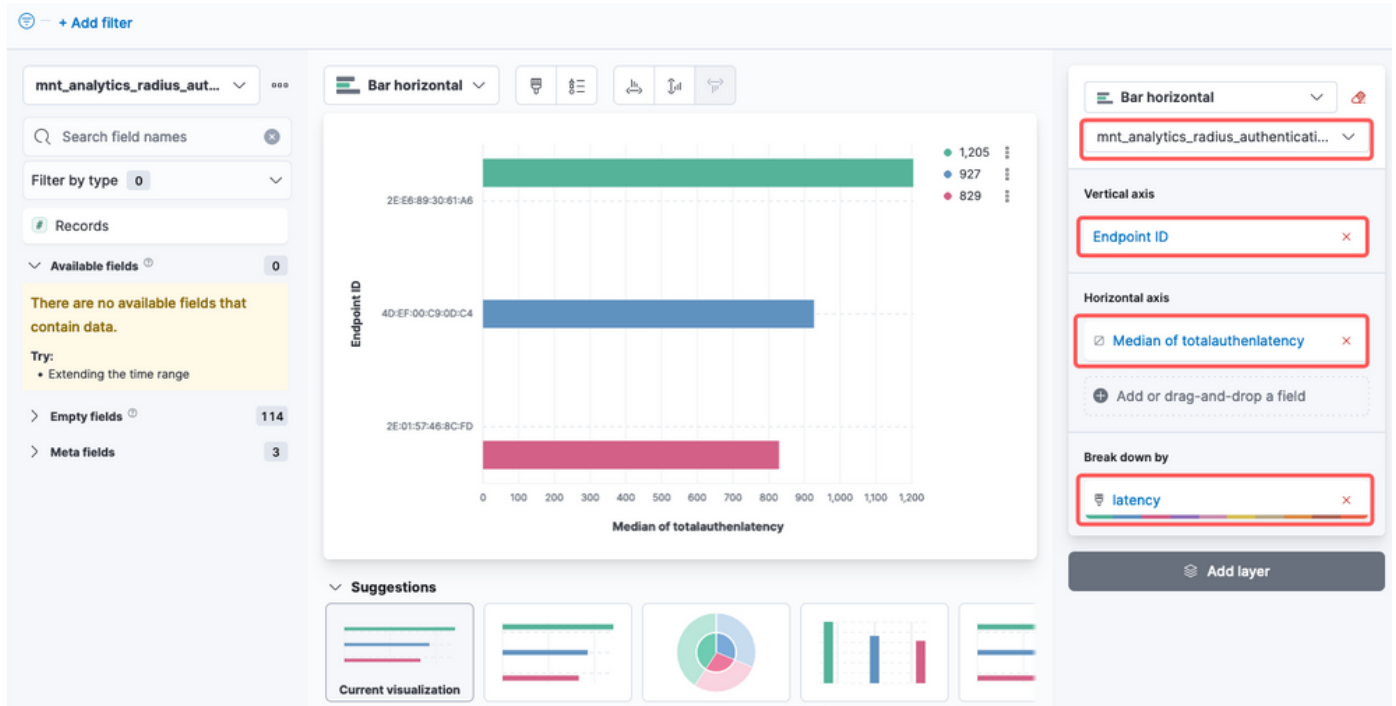
が表示され、現在の設定でグラフがどのように表示されるかを確認できます。

- Visualization Settings : 選択したグラフの種類に応じて、軸の構成、配色、ラベルなど、そのVisualizationの種類に固有の設定にアクセスできます。
- インタラクティブ設定 : ビジュアライゼーションにインタラクションとアクションを追加して、データをフィルタリングしたり、Kibanaダッシュボードの他の部分に移動したりできます。
- 保存と共有 : レンズインターフェイスの上部には、通常、ビジュアライゼーションを保存したり、ダッシュボードに追加したり、他のユーザーと共有したりするオプションがあります。



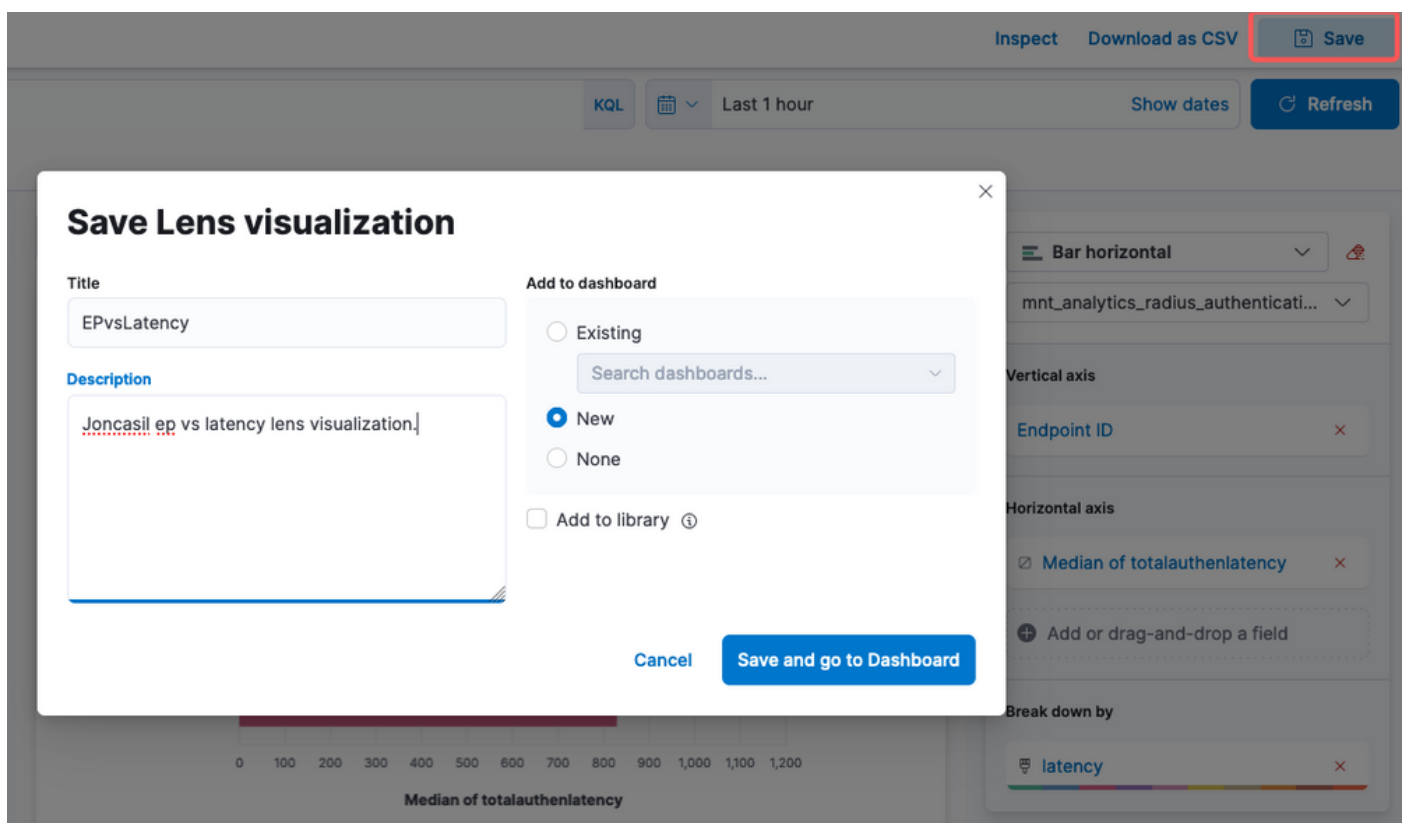
レンズ可視化

Cisco Bug ID [CSCwh48057](#)が原因で、左側のパネルに使用可能なフィールドが表示されません。ただし、右側から、必要なフィールドと図のスタイルを選択できます。この例では、認証の遅延が共通の関心事項であるため、認証の遅延とエンドポイントIDを視覚化するグラフが作成されています。



エンドポイントIDと遅延

完了したら、 Save ボタンをクリックします。

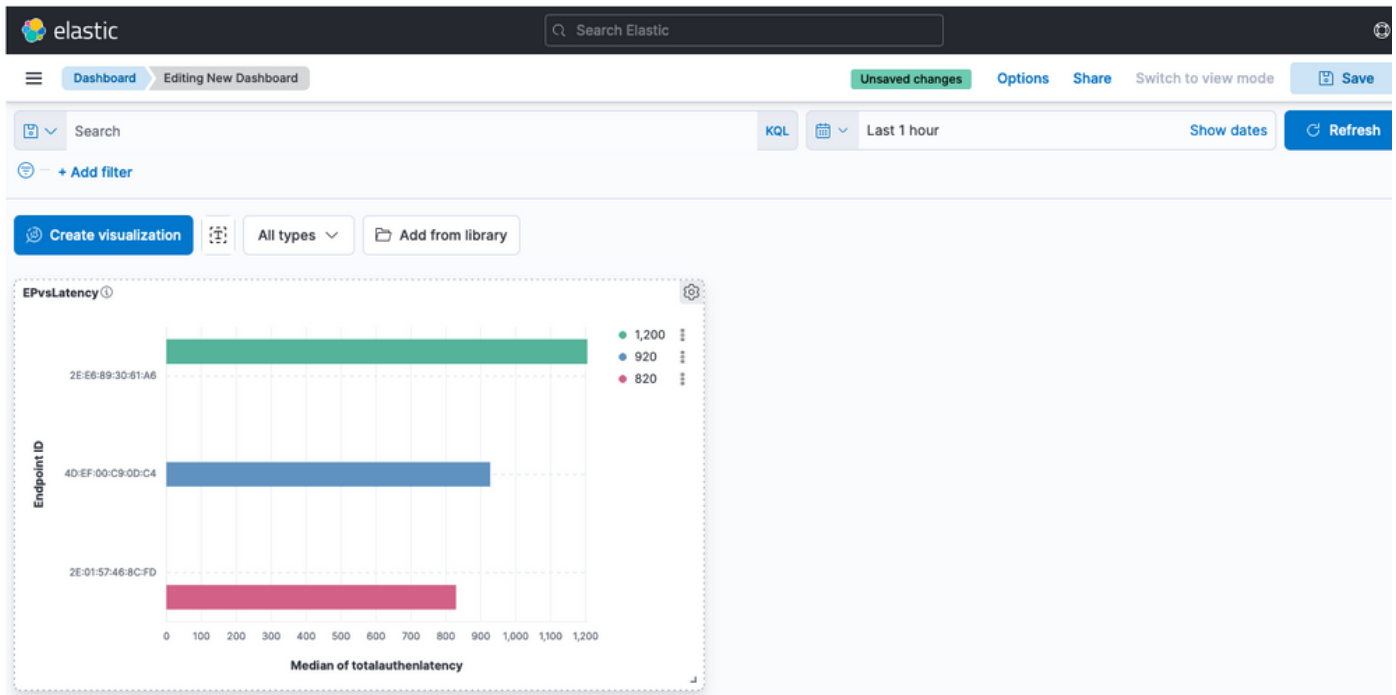


ビジュアル化の保存

### ステップ 3 : ダッシュボードの作成

新しい可視化が新しいダッシュボードに自動的に追加されます。Kibanaダッシュボードを使用すると、Elasticsearchインデックスに保存されたデータに基づいて、インタラクティブな視覚化お

よびレポートを作成、カスタマイズ、共有できます。



新しいダッシュボード

## ( 「トラブルシューティング」 )

- ELKスタックサービスがMNTで実行されていることを確認します。
- Kibana、Logstash、およびElasticsearchがコンテナで実行されているため、ログは次の場所にあります。

```
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
```

## 関連情報

- [ISE 3.3管理ガイド](#)
- [Kibanaドキュメント](#)
- [シスコテクニカルサポートおよびダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。