デジタルネットワークアーキテクチャ(DNA)センターでKibanaを使用する方法

内容

概要

このドキュメントでは、さまざまなDNA Centerサービスの特定のメッセージやログを検索するためにKibanaを使用する方法について説明します。

著者：Cisco TACエンジニア、Alexandro Carrasquedo

前提条件

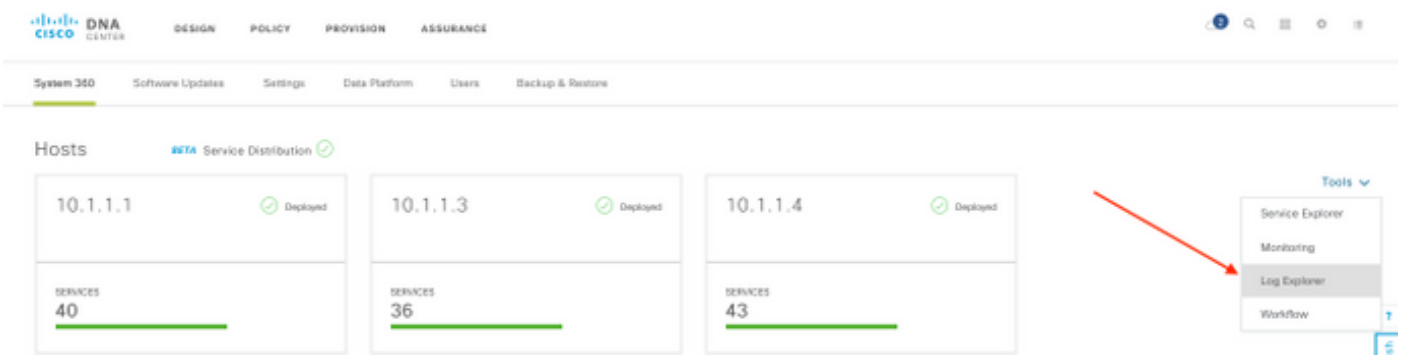
要件

- DNA Centerクラスタを実行している。
- DNA Centerサービスの名前と使用方法に精通していること。

背景説明

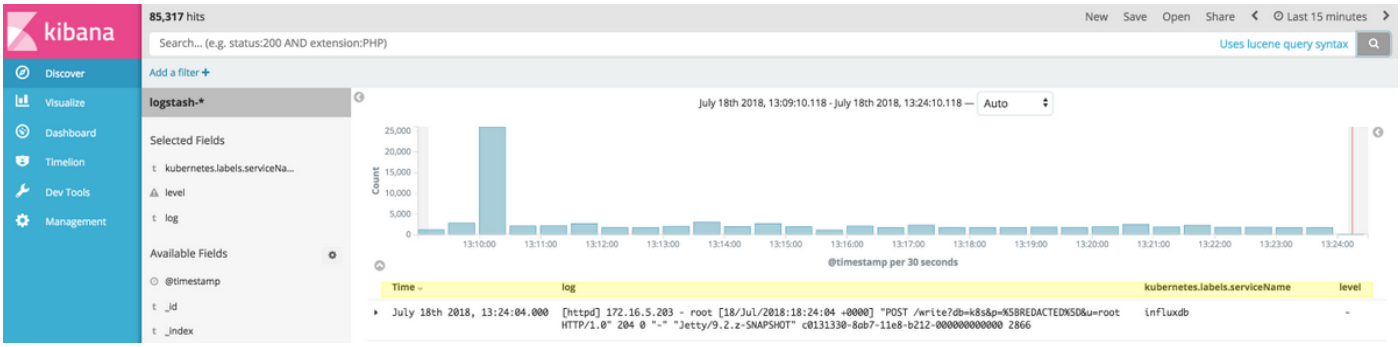
Kibanaは、Elasticsearchのオープンソースデータ可視化プラグインです。DNA Centerで利用可能なElasticsearchクラスターでインデックス付けされたコンテンツの上に可視化機能を提供します。次の2つの方法でアクセスできます。

- https://<DNA Center ip>/kibana
- [System Settings] -> [System 360] -> [Tools] -> [Log exporter]



デフォルトのKibana Webページの概要

Kibanaには、次の図で強調表示されている複数のデフォルトフィールドがあります。



- **Time：メッセージが表示された時刻。**
- **Log：ログの未加工コンテンツ。**
- **Kubernetes.labels.serviceName：特定のログを表示するサービス。**
- **Level：特定のログの緊急度。**

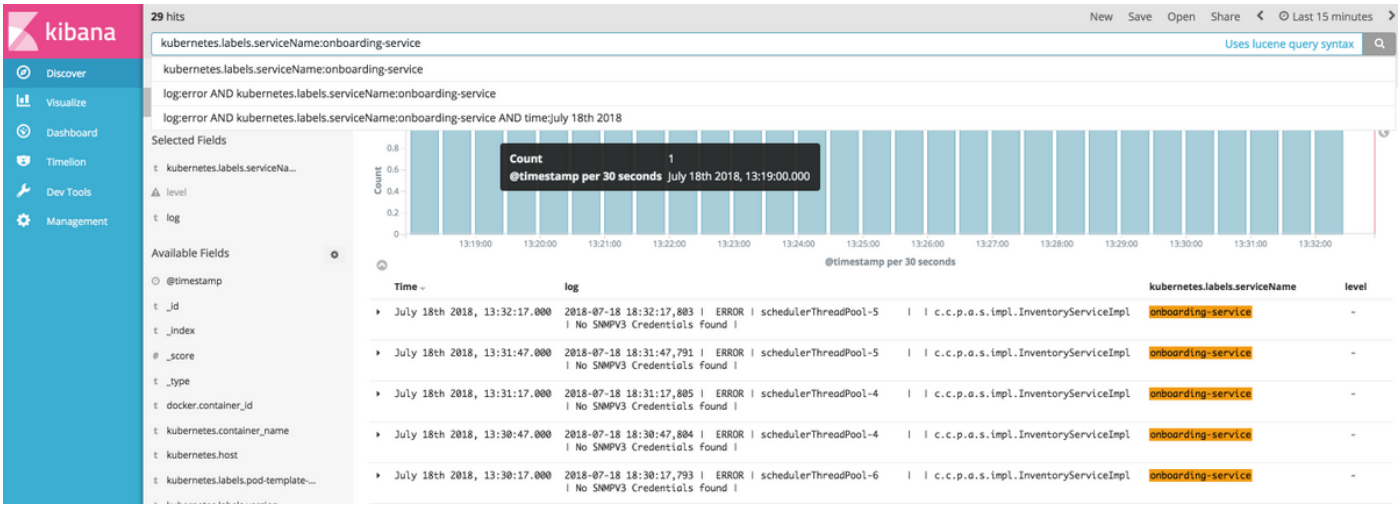
これらのフィールドを使用して、DNA Centerクラスタ内の問題の診断に役立つ包括的な出力を提供できます。次に、Kibanaの使用を開始する際に役立つ使用例を示します。

> **注**：このドキュメントでは、特定のサービスの例を示します。ただし、トラブルシューティングのニーズに合ったサービスでこれらの検索を試すことができます。

使用例

オンボーディングサービスに含まれるすべてのログを取得します。

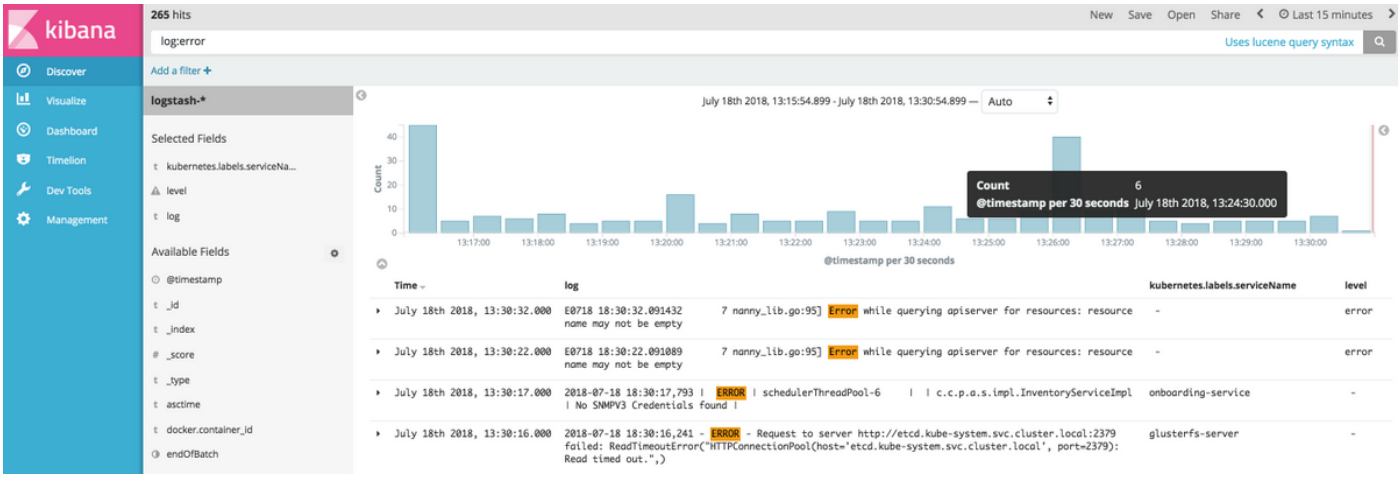
```
kubernetes.labels.serviceName:onboarding-service
```



文字列「error」を含むすべてのログを取得します

> **ヒント**：問題を示す最も一般的なログエントリには、「Error」、「Failed」、および「Exception」が含まれています。トラブルシューティングに役立つ他の一般的な文字列になるように、文字列を自由に変更してください。

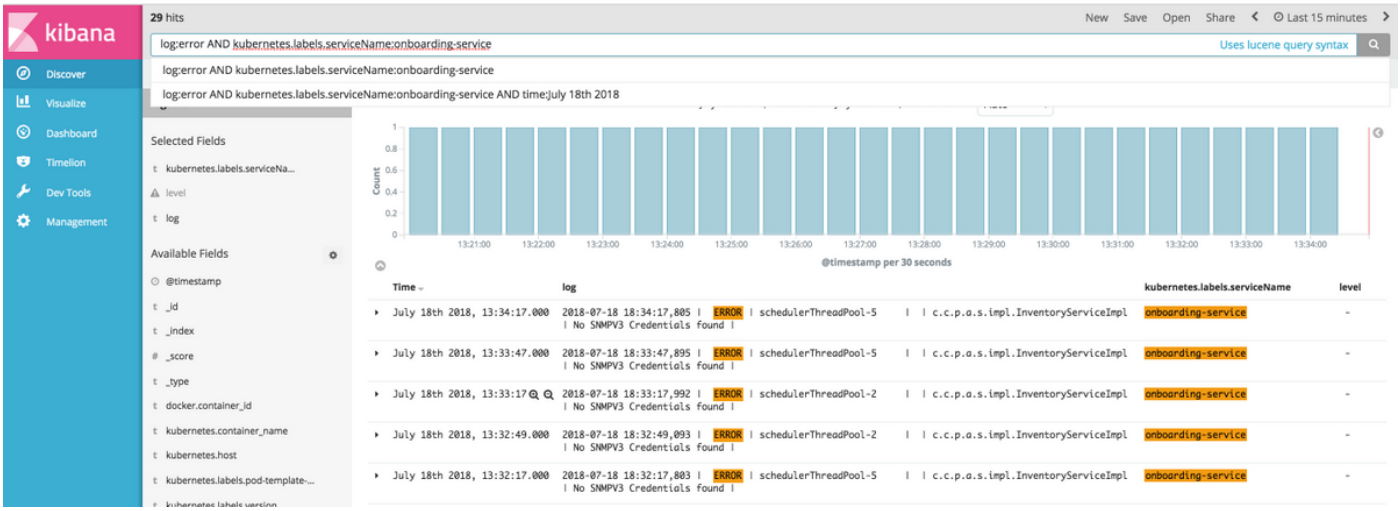
```
log:error
```



検索の組み合わせ

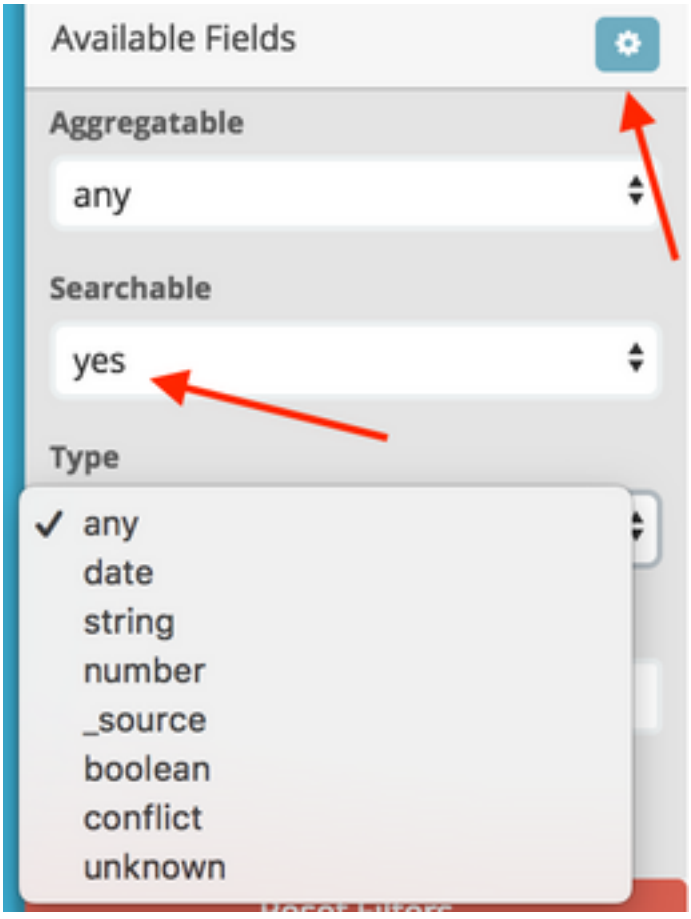
文字列の組み合わせに一致するエントリを検索するには、文字列の間でAND（または&）を使用します。

```
log:error AND kubernetes.labels.serviceName:onboarding-service
```



注：一部のフィールドは検索可能ではありません。

[利用可能なフィールド]ペインに検索可能なフィールドのみを表示するには、歯車を選択してビューをカスタマイズします。文字列、ブール値、数値など、使用する検索の種類を定義することもできます。



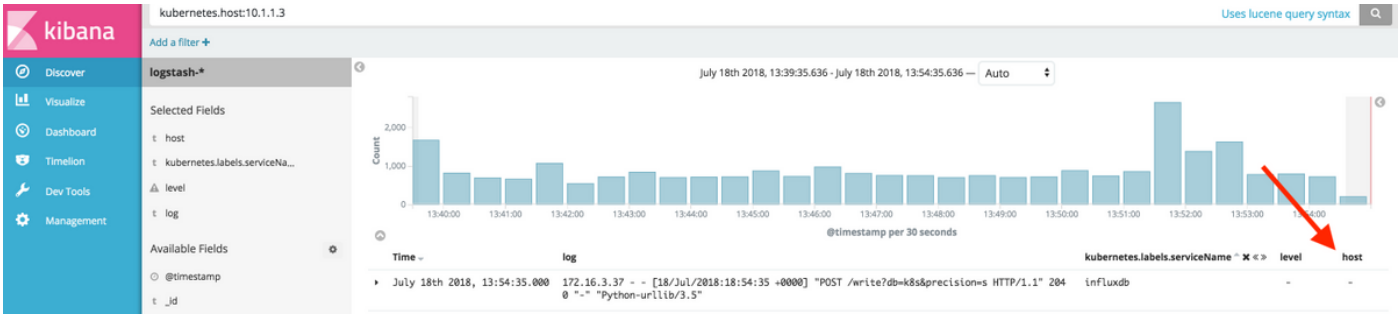
特定の日付からすべてのログを取得

検索基準に時間要素を追加できます。「時間範囲」フィールドから次のいずれかのオプションを使用します。

- **Quick**：最後のX分、時間、日、または週から。
- **相対**：過去X分間、時間、日、または週から特定の日付まで。
- **Absolute**：特定の日付から別の特定の日付まで。

検索またはビューにフィールドを追加する

ログの詳細を取得するには、デフォルトビューにさらにフィールドを追加できます。[利用可能なフィールド]ペインに移動し、[追加]を選択して、表示するフィールドを選択します。選択内容を保存すると、フィールドがメインビューに表示されます。



2つの異なるサービスからのエラーを同時に検索

検索条件に2つ以上のサービスを含めます。サービス名がカッコで囲まれて入力され、ORで区切られてください。

```
log:error && (kubernetes.labels.serviceName:onboarding-service OR
kubernetes.labels.serviceName:telemetry-agent)
```

参考

- 弾性検索の共通オプション
- Apache Lucene – クエリパーサーの構文