

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](#)

[前提条件](#)

[要件](#)

[背景説明](#)

[デフォルトのKibana Webページの概要](#)

[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。](#)

[文字列「error」を含むすべてのログを取得します](#)

[検索の組み合わせ](#)

[特定の日付からすべてのログを取得](#)

[検索またはビューにフィールドを追加する](#)

[2つの異なるサービスからのエラーを同時に検索](#)

[参考](#)

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

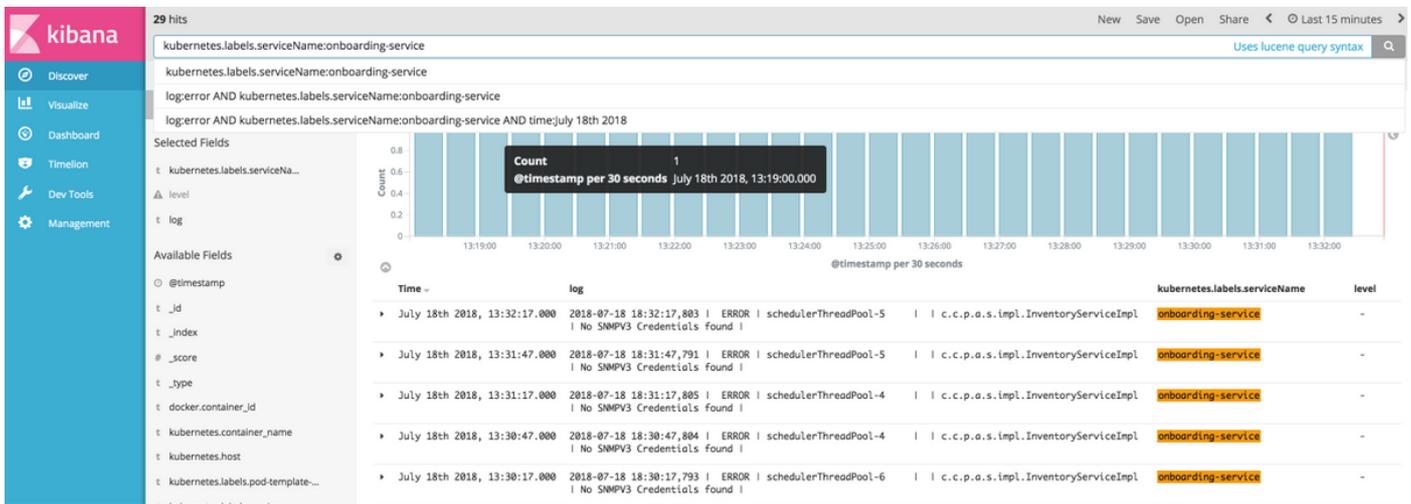
要件

- 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。

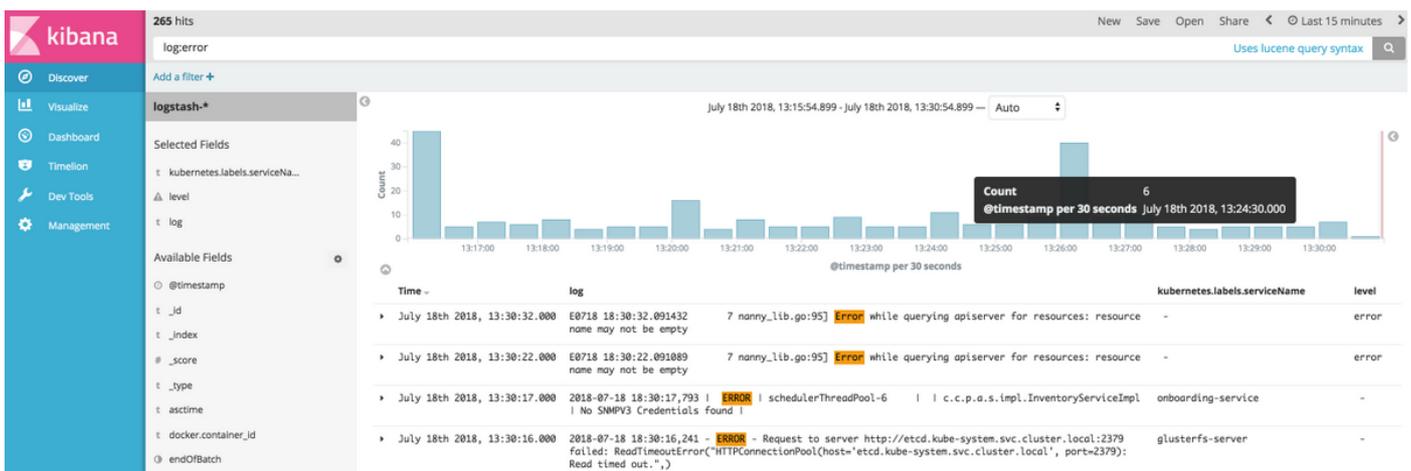
- <https://<DNA Center ip>/kibana>
- [System Settings] -> [System 360] -> [Tools] -> [Log exporter]



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ーには、「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。

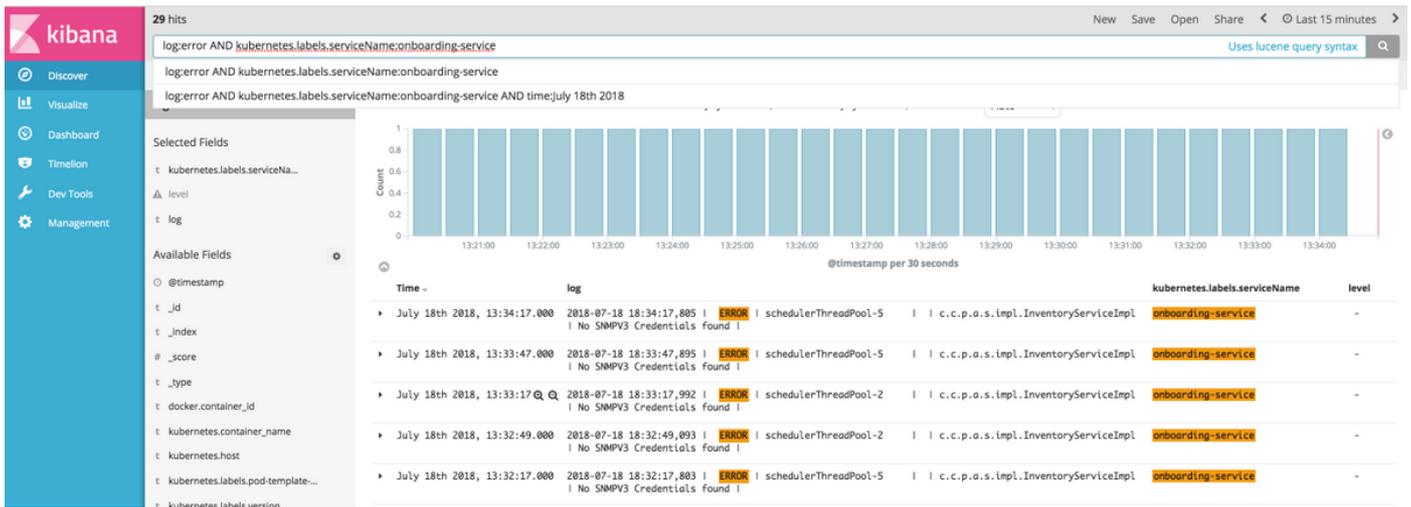
log:error



検索の組み合わせ

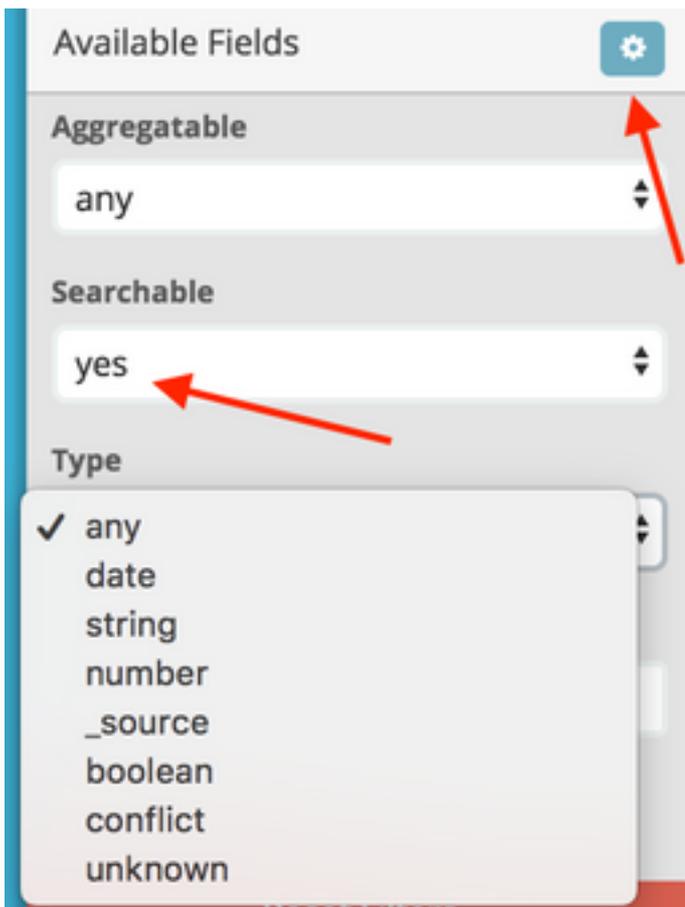
文字列の組み合わせに一致するエントリーを検索するには、文字列の間でAND (または&) を使用します。

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。



特定の目付からすべてのログを取得

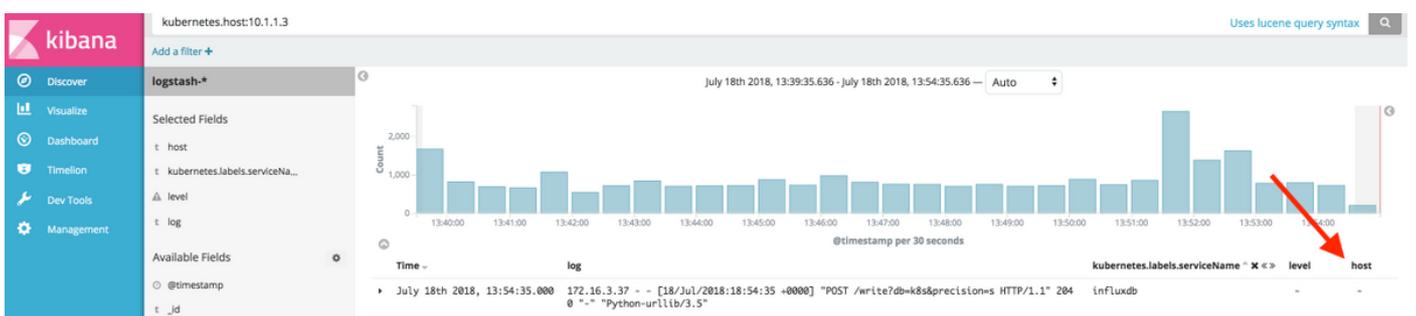
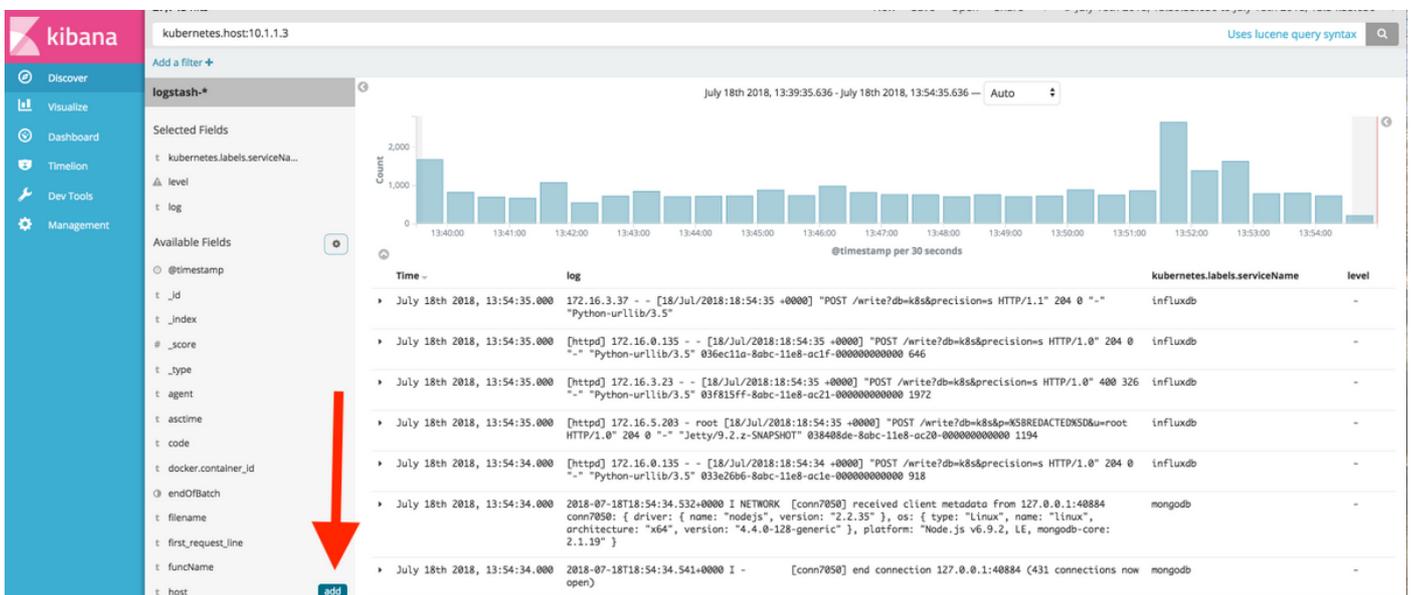
検索基準に時間要素を追加できます。「時間範囲」フィールドから次のいずれかのオプションを使用します。



- **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)
```

50 hits New Save Open Share < Last 15 minutes >

log:error && (kubernetes.labels.serviceName:onboarding-service OR kubernetes.labels.serviceName:telemetry-agent) Uses lucene query syntax

Discover

Visualize

Dashboard

Timeline

Dev Tools

Management

logstash*

Selected Fields

- kubernetes.labels.serviceName
- level
- log

Available Fields

Popular

- _index
- kubernetes.host
- @timestamp
- _id
- _score
- _type
- asctime
- docker.container_id
- exc_info
- filename
- funcName
- kubernetes.container_name
- kubernetes.labels.pod-template...

Time	log	kubernetes.labels.serviceName	level
July 23rd 2018, 09:07:24.000	2018-07-23 14:07:24,245 ERROR schedulerThreadPool-3 c.c.p.a.s.impl.InventoryServiceImpl No SNMPV3 Credentials found	onboarding-service	-
July 23rd 2018, 09:07:00.000	{"@asctime": "2018-07-23 14:07:00,743", "timeMillis": 1532354820.7431946, "filename": "telemetry_manager.py", "funcName": "_start_services", "levelname": " ERROR ", "lineno": 101, "module": "telemetry_manager", "secs": 743.194580078125, "message": "Unable to connect to tethering host: You are not authorized to perform this operation", "name": "telemetry-manager", "pathname": "/opt/maglev/lib/python3.5/site-packages/telemetry_agent/manager/telemetry_manager.py", "process": 24, "processName": "MainProcess", "relativeCreated": 438813335.45684814, "thread": 140658652190464, "threadName": "StarterThread", "level": " ERROR ", "exc_info": "Traceback (most recent	telemetry-agent	ERROR
July 23rd 2018, 09:06:54.000	2018-07-23 14:06:54,173 ERROR schedulerThreadPool-4 c.c.p.a.s.impl.InventoryServiceImpl No SNMPV3 Credentials found	onboarding-service	-
July 23rd 2018, 09:06:24.000	2018-07-23 14:06:24,159 ERROR schedulerThreadPool-4 c.c.p.a.s.impl.InventoryServiceImpl No SNMPV3 Credentials found	onboarding-service	-
July 23rd 2018, 09:06:15.000	{"@asctime": "2018-07-23 14:06:15,644", "timeMillis": 1532354775.6448857, "filename": "telemetry_manager.py", "funcName": "_start_services", "levelname": " ERROR ", "lineno": 101, "module": "telemetry_manager", "secs": 644.885697845459, "message": "Unable to connect to tethering host: You are not authorized to perform this operation", "name": "telemetry-manager", "pathname": "/opt/maglev/lib/python3.5/site-packages/telemetry_agent/manager/telemetry_manager.py", "process": 24, "processName": "MainProcess", "relativeCreated": 438768237.06793785, "thread": 140658652190464, "threadName": "StarterThread", "level": " ERROR ", "exc_info": "Traceback (most recent	telemetry-agent	ERROR

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](#)