



# New Relic Logs セットアップの流れ

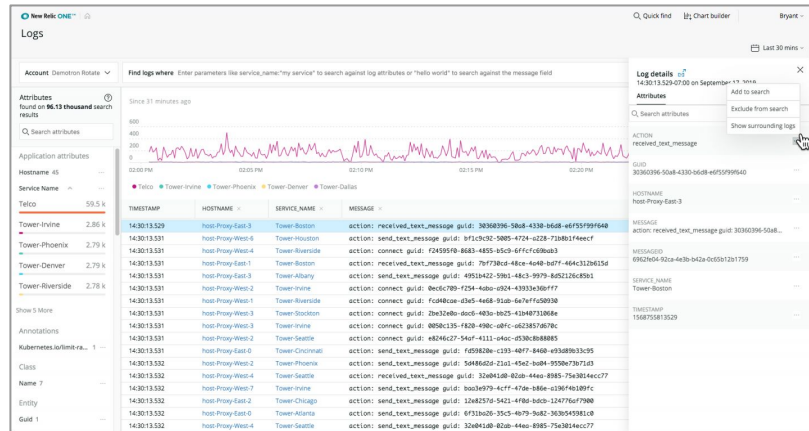


# 前提

## New Relic Logsとは


Fluentd などのLogコレクターエージェントからLogsを統合的にあつめて高速に検索・分析できる製品

(要New Relic Logs サブスクリプションライセンス)



# New Relic Logsを利用するまでのステップ

① 要件の確認



② 利用するプラグインの設定



③ Logs APIの有効化 [オプション]



④ Logsが機能しているかの確認

# セットアップの流れ

## ① 要件の確認

有効な New Relic APMおよびLogsのライセンスを保有してるか

- 担当営業にご確認ください

New Relic Logsに対応したプラグインを利用しているか

- Fluentd plugin
- AWS CloudWatch plugin
- AWS FireLens plugin
- Fluent Bit plugin
- Kubernetes plugin
- Logstash plugin

# セットアップの流れ

## ② 利用するプラグインの設定

それぞれのプラグインに合わせた設定を実施  
各プラグインの設定方法は下記URLを参照

- <https://docs.newrelic.com/docs/logs/new-relic-logs/enable-logs/enable-new-relic-logs#enable-logs>

## ③ New RelicのLogs APIの有効化 [オプション]

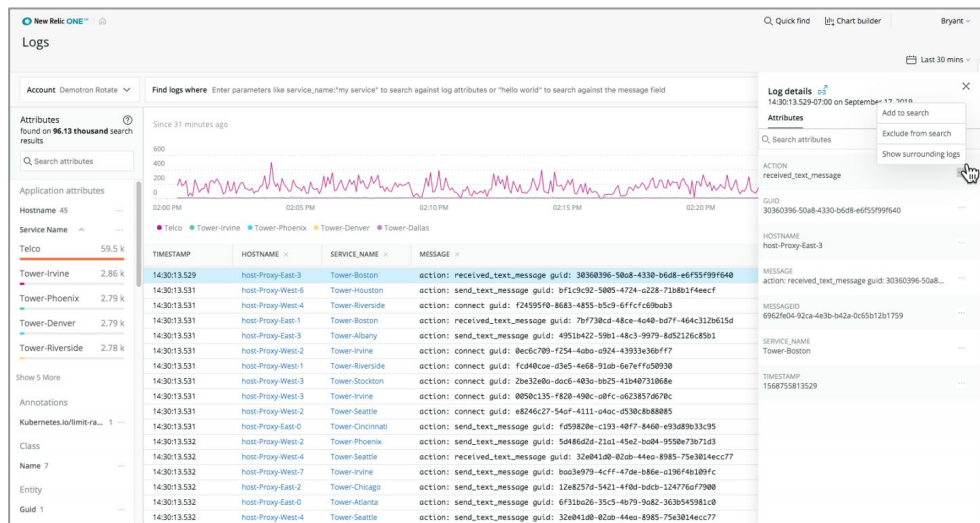
プラグインを利用しない場合はNew RelicのAPI経由で利用可能。  
詳細は下記URLを参照。

- <https://docs.newrelic.com/docs/logs/new-relic-logs/log-api/introduction-log-api>

# セットアップの流れ

## ④ Logsが機能しているかの確認

New Relic OneからLogsにアクセスし、期待しているLogsが見れるかどうか確認



The screenshot displays the New Relic One Logs interface. On the left, there are navigation panels for 'Account' (Demotron Rotate), 'Attributes' (96.13 thousand search results), and 'Application attributes' (Hostname: 45, Service Name: Telco, Tower-Irvine: 2.86 k, Tower-Phoenix: 2.79 k, Tower-Denver: 2.79 k, Tower-Riverside: 2.78 k). The main area shows a 'Find logs where' search bar and a line chart of log volume over time. Below the chart is a table of log entries with columns for Timestamp, Hostname, Service Name, and Message. The first entry is highlighted in blue. On the right, a 'Log details' panel shows the selected log's GUID, Hostname, Message, and Service Name.

TIMESTAMP	HOSTNAME	SERVICE_NAME	MESSAGE
14:30:13.529	host-Proxy-East-3	Tower-Boston	action: received_text_message guid: 30360396-50a8-4330-b6d8-e6f55f99f640
14:30:13.531	host-Proxy-West-6	Tower-Houston	action: send_text_message guid: bf1c9c92-5005-4724-e228-71d8b1f4eeef
14:30:13.531	host-Proxy-West-4	Tower-Riverside	action: connect guid: f24595f0-8683-4855-b5c3-6fffc0bab3
14:30:13.531	host-Proxy-East-1	Tower-Boston	action: received_text_message guid: 7b738cd-48ce-4e40-bd7f-464c312b615d
14:30:13.531	host-Proxy-East-3	Tower-Albany	action: send_text_message guid: 49518422-5901-48c3-9979-8d52126c8501
14:30:13.531	host-Proxy-West-2	Tower-Irvine	action: connect guid: 0ec6c709-f254-40ba-e924-43933a36ff7
14:30:13.531	host-Proxy-West-1	Tower-Riverside	action: connect guid: fc040c0e-d3e5-4e68-91a0-6e7ef650930
14:30:13.531	host-Proxy-West-3	Tower-Stockton	action: connect guid: 2bc32e0a-d0c6-403a-bb25-41b407f31068e
14:30:13.531	host-Proxy-West-3	Tower-Irvine	action: connect guid: 0058c135-f820-490c-08fc-0623857d678c
14:30:13.531	host-Proxy-West-2	Tower-Seattle	action: connect guid: e8246c27-54cf-4111-04ac-d538c8b88085
14:30:13.531	host-Proxy-East-0	Tower-Cincinnati	action: send_text_message guid: fd59820e-c193-40f7-8400-e93d89b3c395
14:30:13.532	host-Proxy-West-2	Tower-Phoenix	action: send_text_message guid: 5d486d20-c21a1-45e2-ba04-9550e73b71d3
14:30:13.532	host-Proxy-West-4	Tower-Seattle	action: received_text_message guid: 32e04100-020b-44e0-8985-75e3014ecc77
14:30:13.532	host-Proxy-West-7	Tower-Irvine	action: send_text_message guid: ba03e979-4c7f-470e-b80e-6196f4b109fc
14:30:13.532	host-Proxy-East-2	Tower-Chicago	action: send_text_message guid: 12e82570-5421-4f00-bd0c-1247760f7900
14:30:13.532	host-Proxy-East-0	Tower-Atlanta	action: send_text_message guid: 6f731ba26-35c5-4079-50e2-3630549301c0
14:30:13.532	host-Proxy-West-4	Tower-Seattle	action: send_text_message guid: 32e04100-020b-44e0-8985-75e3014ecc77

# (オプション) Logs in Context [Beta]を利用する場合

Logs in Contextとは: [New Relic APM](#)と[New Relic Logs](#)を有機的に繋ぐことでAPMなどから関連Logsに直接アクセスできる[連携機能](#)

## Logs in Context機能の有効化方法(2019.12現在Beta)

- a. 前提:[New Relic Logs](#)有効化されていること
- b. [New Relic APM Pro](#)サブスクリプション準備
- c. APMエージェントをLogs in Context対応バージョンへ[アップデート](#)
- d. エージェントの[分散トレース](#)を有効化
- e. APMやk8s explorerなどでLogsの確認

# 例: Kubernetes integrationsからのLogs in context

The screenshot displays the New Relic ONE interface for a Kubernetes cluster. The main visualization is a radial pod map with a central cluster of yellow hexagons labeled 'PENDING' and 'ALERTING', surrounded by various pod icons. A legend on the left lists metrics: 5 NAMESPACES, 15 DEPLOYMENTS, 50 NODES, 254 PODS, CRITICAL (red), WARNING (yellow), CPU (square), MEM(ORY) (vertical bar), and STO(RAGE) (circle). A green arrow points from a pod in the visualization to the 'canal-98n5r' Pod details panel on the right. This panel shows the pod is 'Running' with a '1 WARNING' and provides metadata like namespace 'kube-system' and node 'ip-172-31-247-152.us-west-2.compute.internal'. Below this, another green arrow points from the 'install-cni' Container details panel to its 'See logs' link. The 'install-cni' panel shows it is 'Running' with a '1 WARNING' and includes two line graphs: 'CPU core usage' (0 to 0.1) and 'Memory byte usage' (0 to 800 k), both for the period from 09:20 AM to 09:5 AM.



# 例: Distributed TracingからのLogs in context



## New Relic Logsの詳細に关しまして

Logs関連の情報に关しては下記ドキュメントに詳細が紹介されていますのでご確認ください。

<https://docs.newrelic.com/docs/logs/new-relic-logs>

# Thank you

