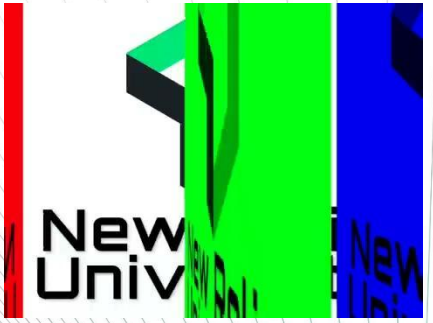


NRU 304
「アラート設計の 基本と活用」

Nov 20, 2024

new relic

ウェビナー　各種ご連絡

1. ご質問がある場合は、"Q＆A"からご入力ください。

2. 本日の資料はこの後"チャット"でURLを共有します。アクセスできない場合は、
"Q&A"よりお名前とメールアドレスをご連絡ください。

new relic

OBSERVABILITY

Safe Harbor

This presentation and the information herein (including any information that may be incorporated by reference) is provided for informational purposes only and should not be construed as an offer, commitment, promise or obligation on behalf of New Relic, Inc. ("New Relic") to sell securities or deliver any product, material, code, functionality, or other feature. Any information provided hereby is proprietary to New Relic and may not be replicated or disclosed without New Relic's express written permission.

Such information may contain forward-looking statements within the meaning of federal securities laws. Any statement that is not a historical fact or refers to expectations, projections, future plans, objectives, estimates, goals, or other characterizations of future events is a forward-looking statement. These forward-looking statements can often be identified as such because the context of the statement will include words such as "believes," "anticipates," "expects" or words of similar import.

Actual results may differ materially from those expressed in these forward-looking statements, which speak only as of the date hereof, and are subject to change at any time without notice. Existing and prospective investors, customers and other third parties transacting business with New Relic are cautioned not to place undue reliance on this forward-looking information. The achievement or success of the matters covered by such forward-looking statements are based on New Relic's current assumptions, expectations, and beliefs and are subject to substantial risks, uncertainties, assumptions, and changes in circumstances that may cause the actual results, performance, or achievements to differ materially from those expressed or implied in any forward-looking statement. Further information on factors that could affect such forward-looking statements is included in the filings New Relic makes with the SEC from time to time. Copies of these documents may be obtained by visiting New Relic's Investor Relations website at ir.newrelic.com or the SEC's website at www.sec.gov.

New Relic assumes no obligation and does not intend to update these forward-looking statements, except as required by law. New Relic makes no warranties, expressed or implied, in this presentation or otherwise, with respect to the information provided.

本セッションのゴール

- New Relicの収集データを活用したアラート設定手順を理解
  - **ユーザー体験に近い指標** に基づいたアラート設定を体験

- New Relicのアラート対応を効率化する方法を理解する

本セッションの想定対象者と前提条件

[対象者]

- これまでのインフラ監視から脱却し、ユーザー体験の悪化を迅速に知りたいと思っている
- 大量のアラートに悩んでいる、あるいは、アラートでは気づけない障害に悩んでいる
- アラートから素早く根本原因にたどり着きたい

[前提条件]

- New Relicの基本的な知識をお持ちであること
- 簡単なNRQLを知っている

New Relicの知識に不安のある方はこちらを受講ください！（オンデマンド視聴可）

- New Relicの基礎
- ダッシュボードワークショップ（NRQL入門編に相当）
- NRQL reference（公式ドキュメント）

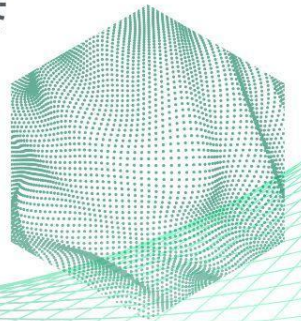
タイムテーブル

時間（目安）	内容	
15:00-15:15	座学(1)	ユーザー視点のアラート
15:15-15:30	座学(2)	New Relicのアラート機能
15:30-15:40	ハンズオン (0)	環境を確認する
15:40-16:00	ハンズオン (1)	アラートポリシー・ワークフローを作成する
16:00-16:20	座学(3)	アラートコンディションの作成
16:20-16:35	ハンズオン (2)	アラートコンディションを作る
16:35-16:45	ハンズオン (3)	発生したアラートの確認
16:45-16:55	座学(4)	New Relicのアラート分析支援機能を使った異常検知
16:55-17:00		まとめ、アンケートご記入

new relic

座学(1)
ユーザー視点のアラート

15:00 - 15:15 (15min)



new relic

突然ですが、、、
どんなアラート設定していますか？

アラートを設定する目的

対象システムが、**何らかの対応が必要な状態** であることの通知を受け取るため

1. システムの停止、またはパフォーマンスの悪化が発生

   → ユーザーへのサービス提供に支障が出ている

2. 1のような事象が近いうちに発生する**兆候が出ている**

"受け取った結果、何かしらのアクションを起こせるようなアラート "を設定する

アラートのアンチパターンとデザインパターン

アンチパターン：OSのメトリクスのアラート

" MySQLが継続的にCPU全部を使っていたとしても、
レスポンスタイムが許容範囲に収まっていれば何も問題ありません。 "

"OSのメトリクスは診断やパフォーマンス分析にとっては重要です。
しかし99%の場合、**これらのメトリクスは誰かを叩き起こすには値しません。** "

出典: 入門監視 (Oreilly, 2019)

new relic

アラートのアンチパターンとデザインパターン

デザインパターン：ユーザー視点の監視

"ユーザーが気にするのは、
アプリケーションが動いているかどうかです。"

"ユーザー視点優先の監視によって、
個別のノードを気にすることから解放されます。"

出典: 入門監視 (Oreilly, 2019)

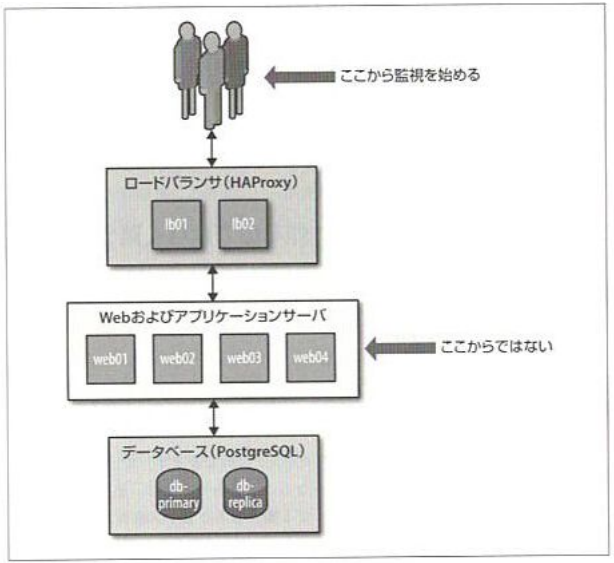


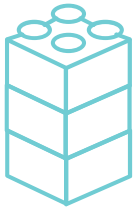
図2-1　できるだけユーザに近いところから監視を始める

new relic

なぜアンチパターンが生み出されたのか

過去のシステム

アプリ

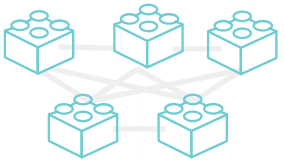


基盤

アプリがモノリシックかつ基盤が密結合だったため、**リソースが枯渇しなければ大きな問題が発生しなかった**

近年のシステム

アプリ



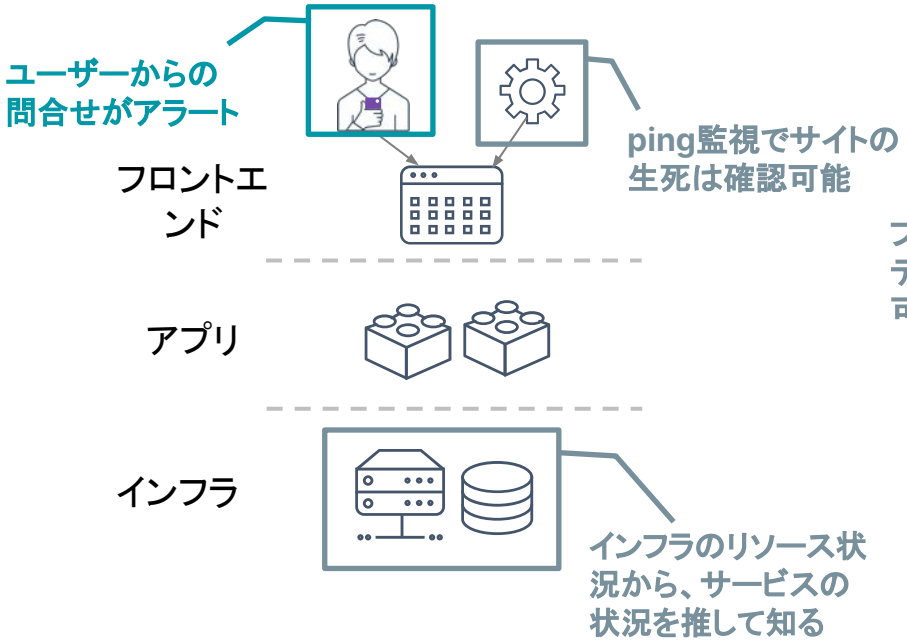
リソース抽象化
(仮想化、コンテナ等)

基盤

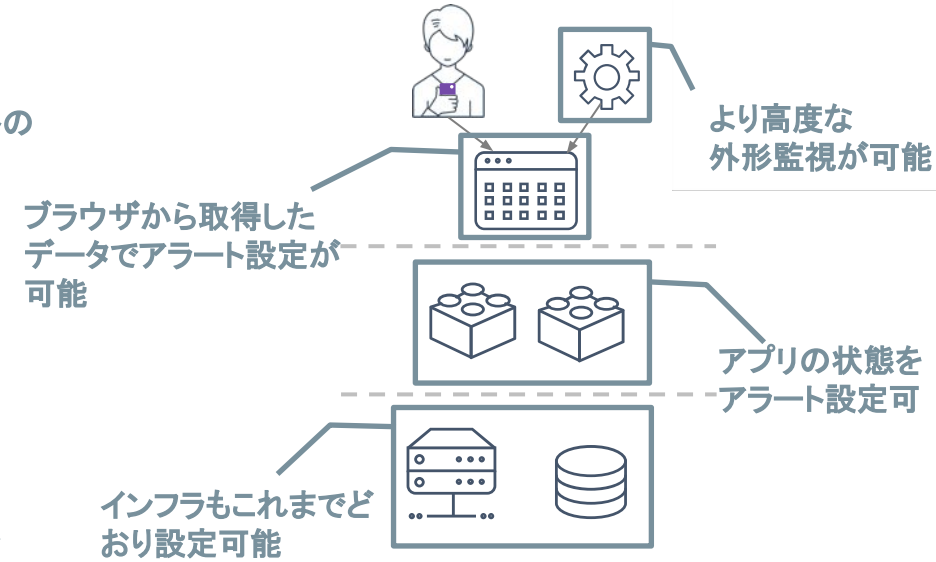
アプリがマイクロサービス化かつ基盤が疎結合なため、**基盤リソースと関係なく問題が発生しうる**

アラートのこれまでと、New Relicを使ったこれから

これまで



これから (with New Relic)



アラートのアンチパターンとデザインパターン

デザインパターン：ユーザー視点の監視

"ユーザーが気にするのは、
アプリケーションが動いているかどうかです。"

"ユーザー視点優先の監視によって、
個別のノードを気にすることから解放されます。"

出典: 入門監視 (Oreilly, 2019)

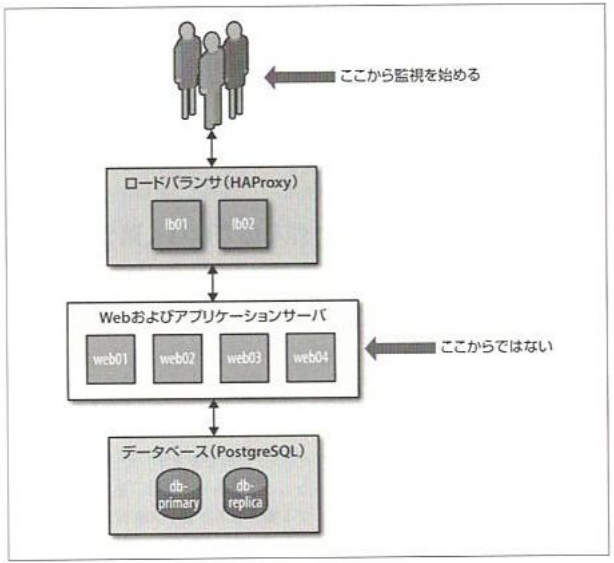


図2-1　できるだけユーザに近いところから監視を始める

new relic

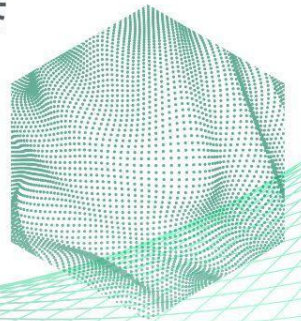
目的別のアラート設定例(Webアプリの一例)

カテゴリ	現在起こっているサービス影響		将来のリスクの兆候	
具体例	サイトが遅い	エラーを返す	キャパシティを超える	リソースが枯渇する
外形監視	応答時間	チェックエラー		
フロントエンド	CWV	JSエラー		
サーバーサイド	応答時間	4xx, 5xxエラー	スループット バッチ遅延	
インフラ				各種インフラ リソース

new relic

座学(2)
New Relicのアラート機能

15:15 - 15:30 (15min)



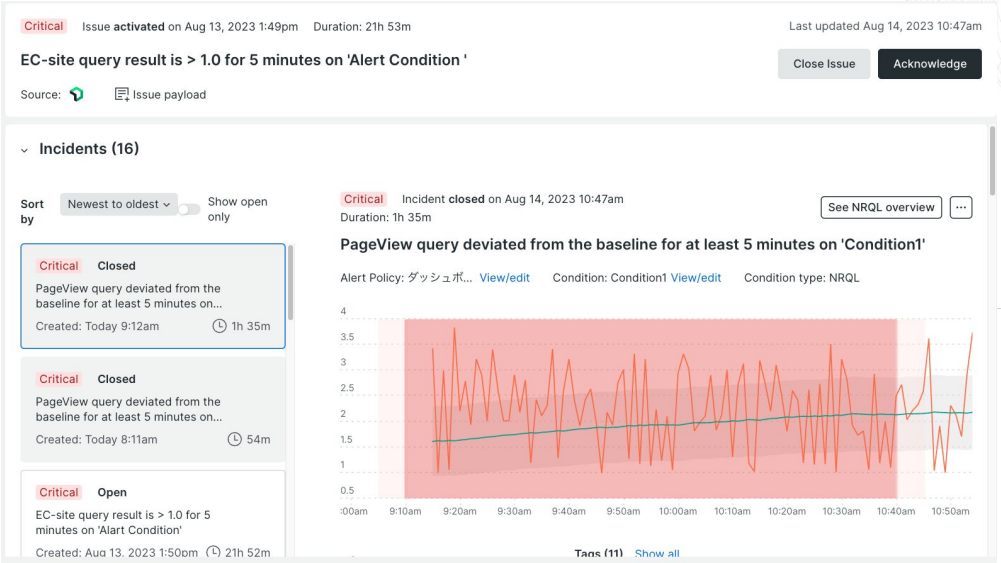
new relic

New Relicのアラート機能

New Relicがリアルタイムに**収集しているデー タ**を使って、アラートを設定可能

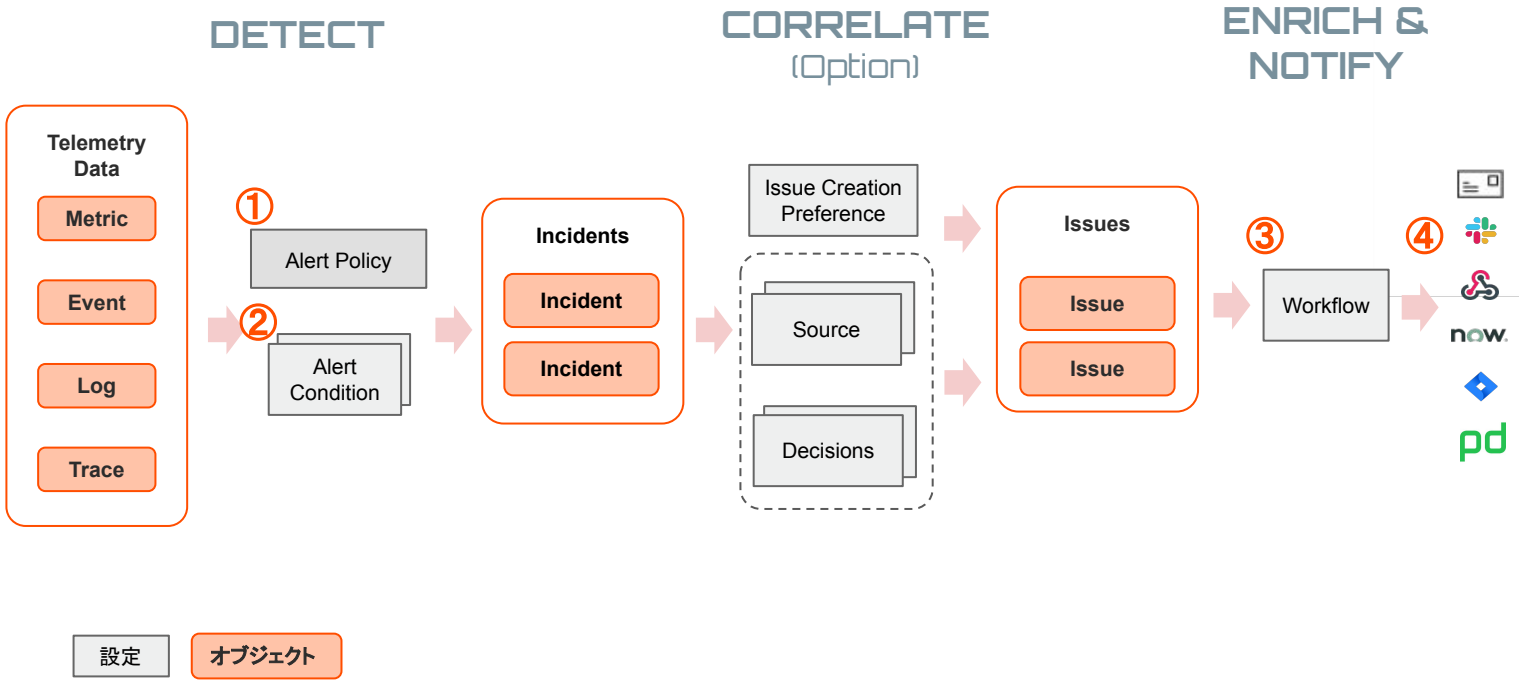
アラートを設定すると、アラート条件に従って **インシデントが起票され、通知を受信可能**

※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説します



new relic

New Relicのアラート構造全体像

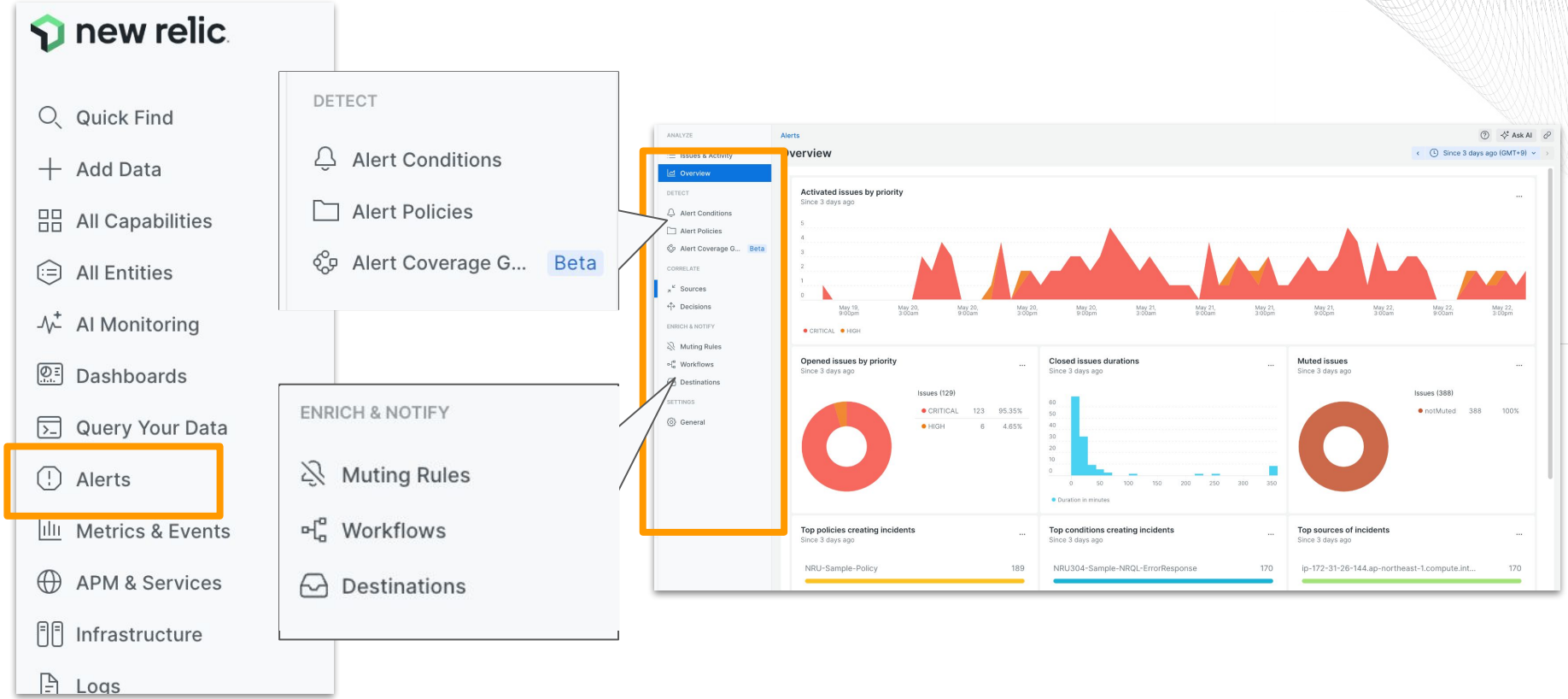


new relic

New Relic アラート基本用語の整理

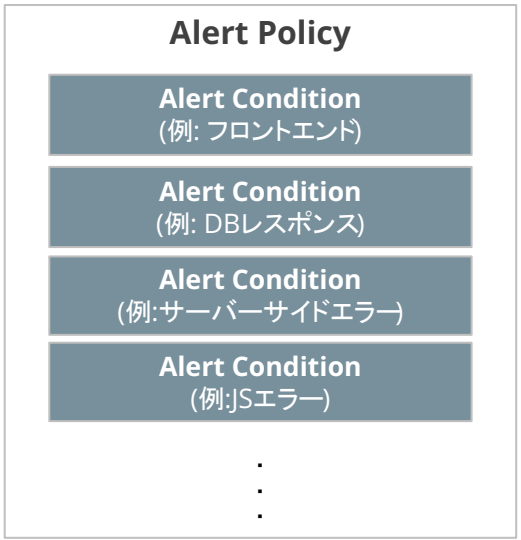
用語	概要
Alert Policy	● Alert Conditionをまとめて管理するためのグループ
Alert Condition	● アラート対象や閾値、集計方法の定義
Incident	● Alert Conditionで検出した個々の違反
Issue	● 1つ以上のIncidentが示す、発生中の問題 ● 実際の通知はIssueに対して行われる
Workflow	● 発生したIssueを元にどこに通知するかを定義 ● 実際の送付先はDestinations
Destinations	● メールやSlackなどの通知先

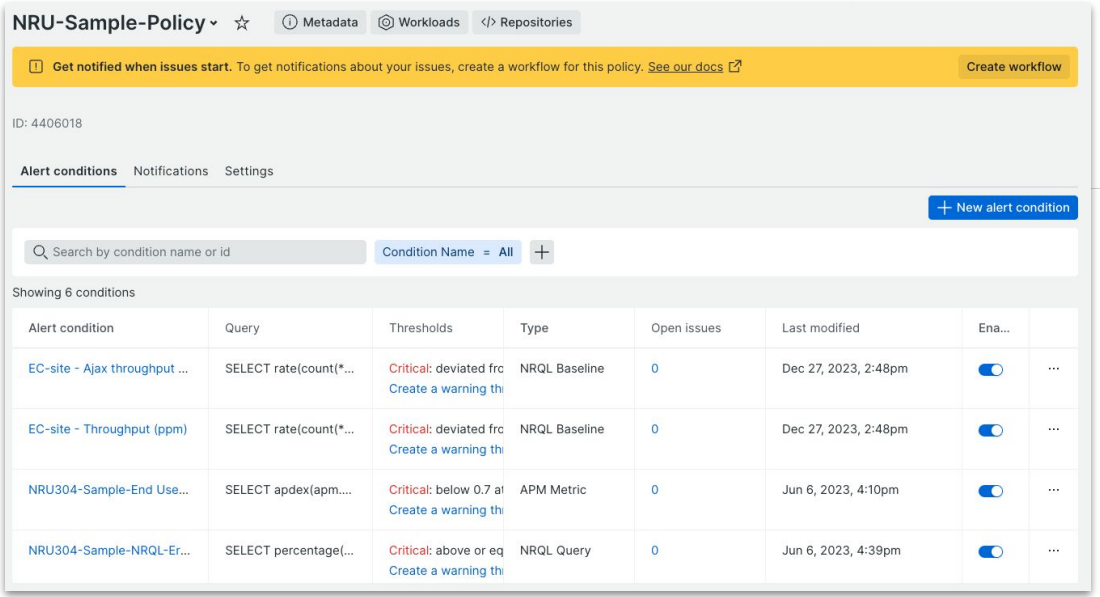
アラート機能の全体UIと重要メニュー



構成要素1: Alert Policy

New Relic のアラートは、Alert Policyという器にAlert Conditionを内包した構造となっている
Alert Policyごとにアラートをグループ化したり、通知先の制御ができる
※通常、送信先やアラートの目的別にポリシーを分けることが多い





new relic

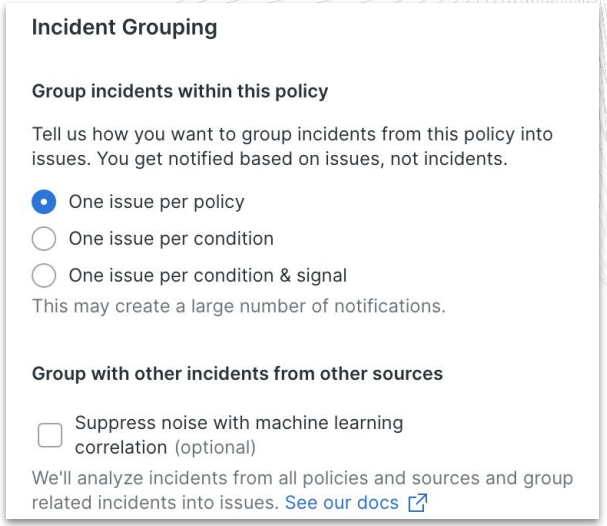
構成要素1: Alert Policy

Issue Creation Preference

IncidentをIssueにグループ化して、通知をまとめる設定

例）1つのAlert Policyに2つのAlert Conditionを設定し、
その全てがCriticalになった場合

Condition1：フロントエンドの JSエラー率（対象サイトは1つ）
Condition2：バックエンドのエラー率（ホスト別に集計、対象ホストは3台）



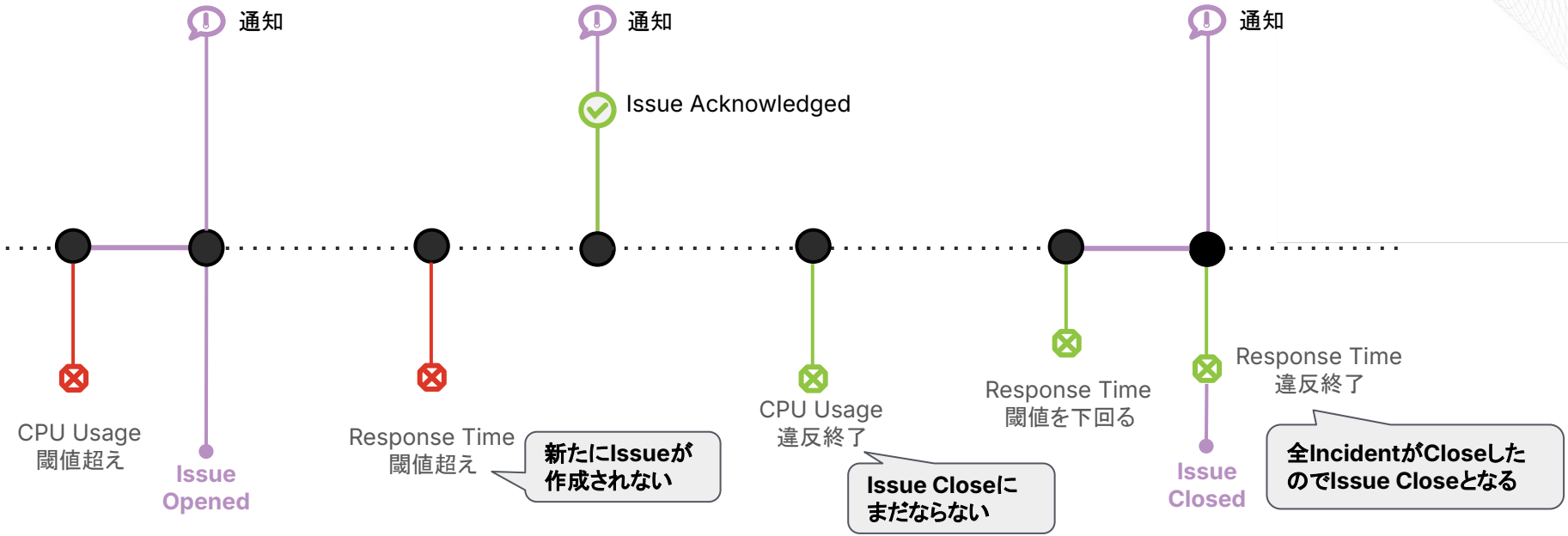
設定名	Incident発生時の挙動	起票されるIssue
One issue **per policy**	**同じAlert Policy**から発生したIncidentを**一つのIssue**にまとめる	**1件**
One issue **per condition**	**同じAlert Condition**から発生したIncidentを**一つのIssue**にまとめる	**2件**（フロントエンドは**1件**、バックエンド**全体で1件**）
One issue **per condition and signal**	同じConditionであっても、**アラート対象ごとに個別に Issue**を作成する	**4件**（フロントエンドは**1件**、バックエンドは**ホスト毎で3件**）

new relic

補足：One issue per policyの場合の Issueのライフサイクルと通知タイミング

例）Alert Policy

- Alert Condition (CPU Usage)
- Alert Condition (Response Time)



※Issue Opened、Acknowledge、Issue Closedのどこで通知をするかはNotify Whenでカスタム可能

new relic

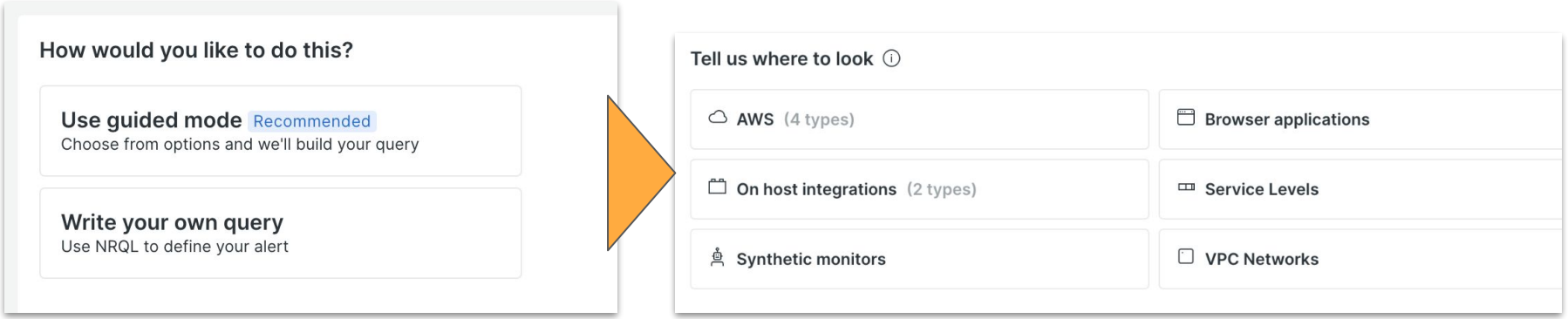
構成要素2: Alert Condition

New Relicが収集しているリアルタイムなデータを、集計・評価する仕組み

- どのような方法で集計を行うか（平均値・最大値・データ件数カウントなど）
- どのような状況をアラートとして通知するか

機能（例. APM, Browser等）ごとに用意されたプリセットから簡単にアラートを作れるほか、

自分で**NRQLクエリ**を記述して、独自の Alert Conditionを作成することも可能



new relic

構成要素3: Workflow

発生したIssueと、通知先・通知内容の関連付け

Filter data

どのようなIssueで、このWorkflowを起動するか

Enrich (Additional settings内)

通知に、Issueに関する付加情報を付与する

Mute issues (Additional settings内)

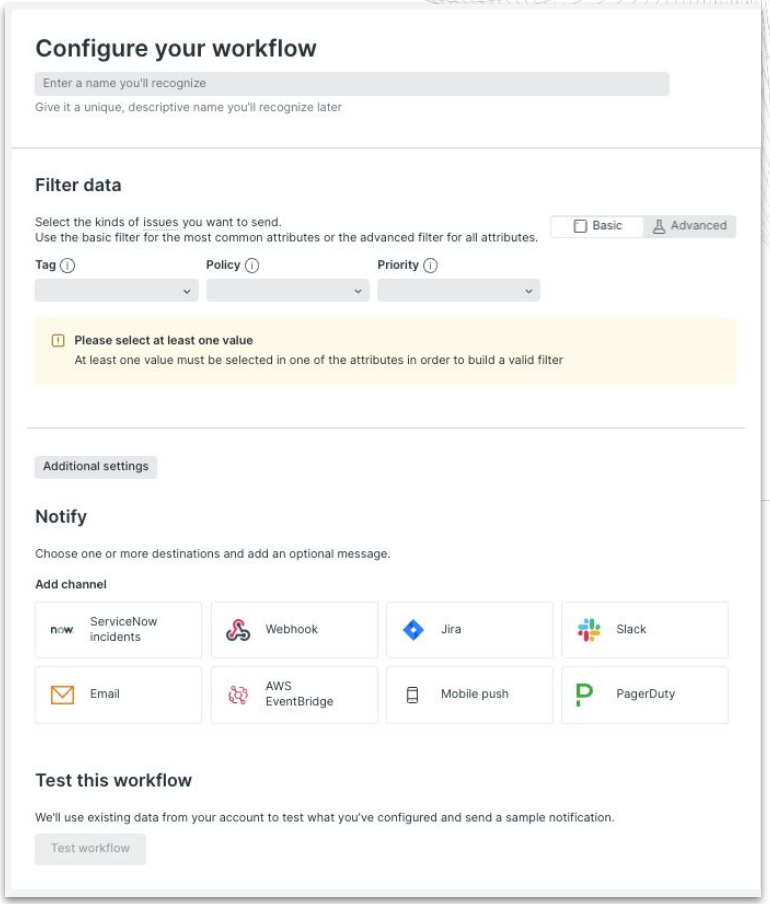
Muting Rulesが設定されていた場合の挙動の設定

Notify (Destinations：後述)

通知先の定義と、通知内容のカスタマイズ

Test workflow

過去の該当データを元に、Workflowの通知テストを実行



new relic

構成要素4: Destinations

Issueのライフサイクル変化（オープン/クローズ等）の通知を受け取ることができる

シンプルな通知

Email

Slack

Mobile push

連携サービスへの通知

Webhooks

servicenow

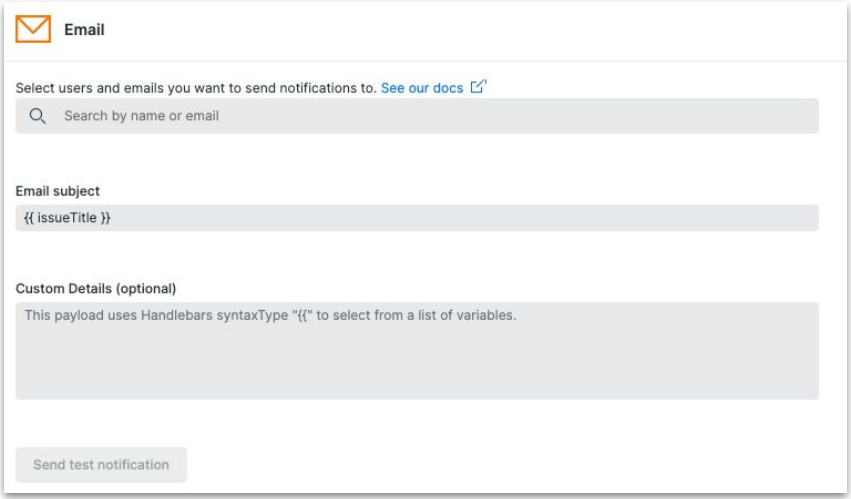
PagerDuty

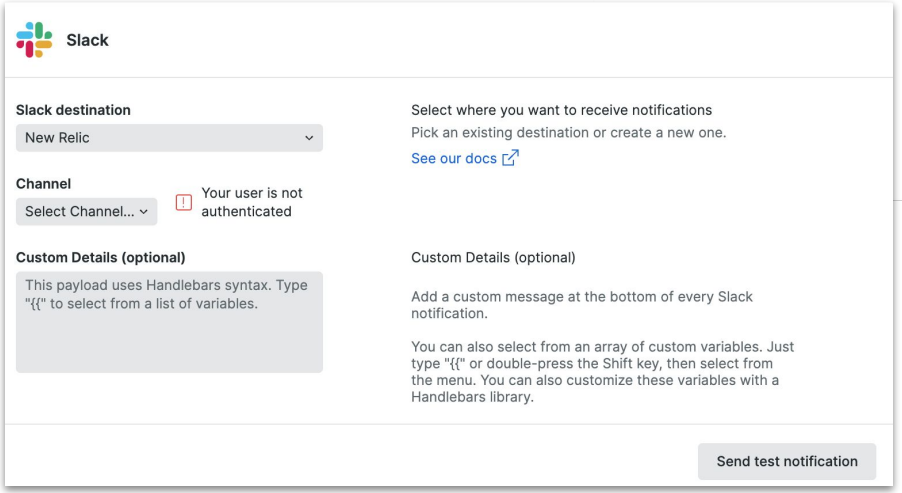
JIRA

Amazon EventBridge

構成要素4: Destinations

- Workflows変数や通知メッセージテンプレートを用いて、柔軟に標題や内容をカスタム可能
  ※補足: custom incident descriptionとは別の情報付加機能
- “{{“と入力することで、Workflows変数の補完機能を活用できます





Workflows変数: https://docs.newrelic.com/docs/alerts-applied-intelligence/applied-intelligence/incident-workflows/custom-variables-incident-workflows/
通知メッセージテンプレート: https://docs.newrelic.com/docs/alerts-applied-intelligence/notifications/message-templates/

new relic

ハンズオン(0)
環境を確認する

15:30 - 15:40 (10min)

今回監視対象のサイト

[NRUジェラートショップ](ECサイト)

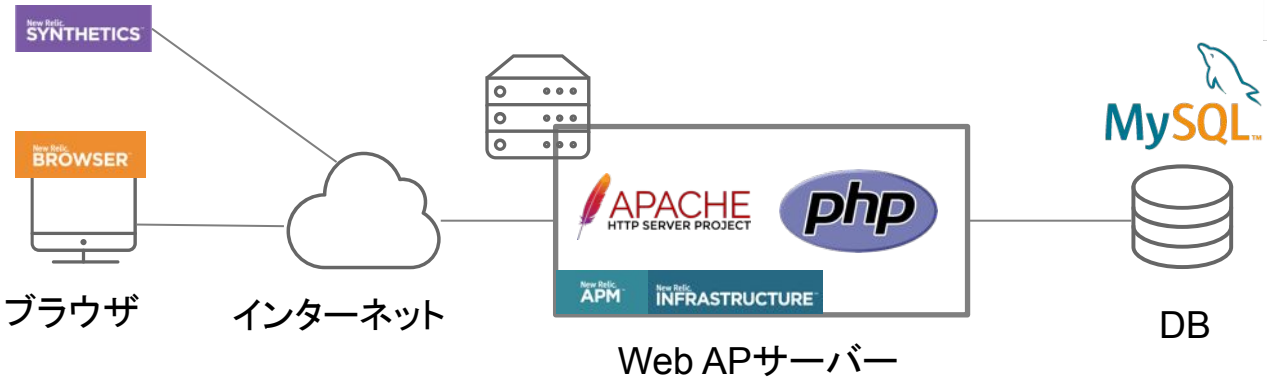
PHPおよびMySQLにより構築されたジェラート屋さんの ECサイトをモニタリングしています

http://ec2-3-113-215-132.ap-northeast-1.compute.amazonaws.com/ec-cube/index.php

new relic

今回の環境の監視構成

New Relicでモニタリング
- Synthetics（外形監視）
- Browser（フロントエンド）
- APM（バックエンド）
- Infrastructure（インフラ）



new relic

ハンズオン環境について

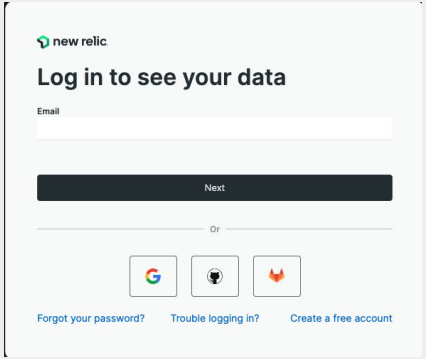
New Relic にログインして、
ユーザー名が “**New Relic University Japan**” であることを確認

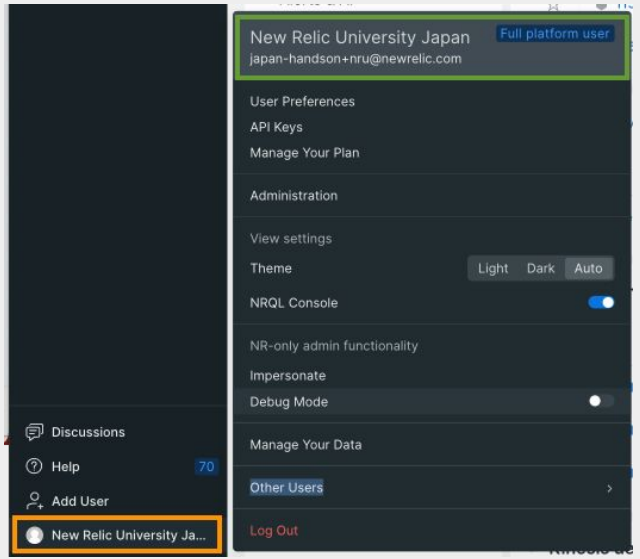
New Relic : **https://one.newrelic.com**

- ユーザー：**japan-handson+nru@newrelic.com**
- パスワード：**oSz6nrupas**
  (オー、エス、ゼット、ロク、エヌ、アール、ユー、ピー、エー、エス)

▼ご注意下さい
普段 New Relic をお使いの方はセッションが残っている場合があります。
下記のいずれかのブラウザのプライベートブラウジングをご利用ください。

- Chrome：シークレットウィンドウ
- Firefox：プライベートウィンドウ
- Edge：InPrivate ウィンドウ

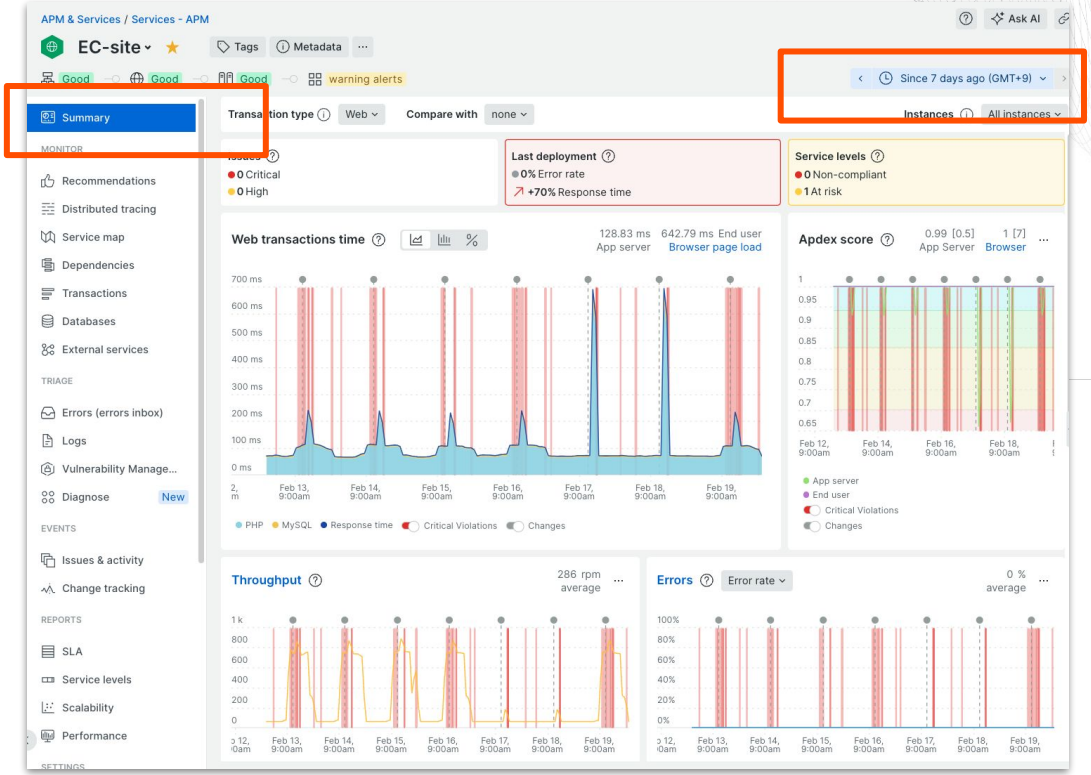




ハンズオン(0) UIの確認

- New Relicポータルの左ペインの"APM & Services"を選択し、EC-siteアプリを選択します。
- Summaryが選択されていることを確認します。
- 表示するデータの表示幅を 7 daysに変更します。

同様に、BrowserやInfrastructureを参照してください。



new relic

new relic

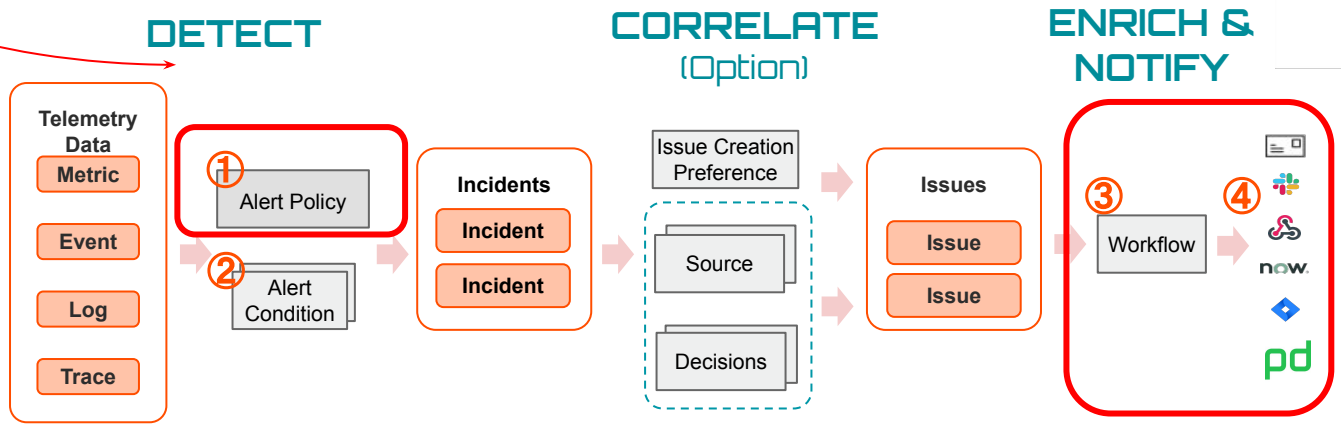
ハンズオン(1)
アラートポリシー・ワークフローを作成する

15:40 - 16:00 (20min)

ハンズオン(1)アラートを作成する

作業内容

1. Alert Policyを作成する
2. WorkflowとDestinationsを作成する



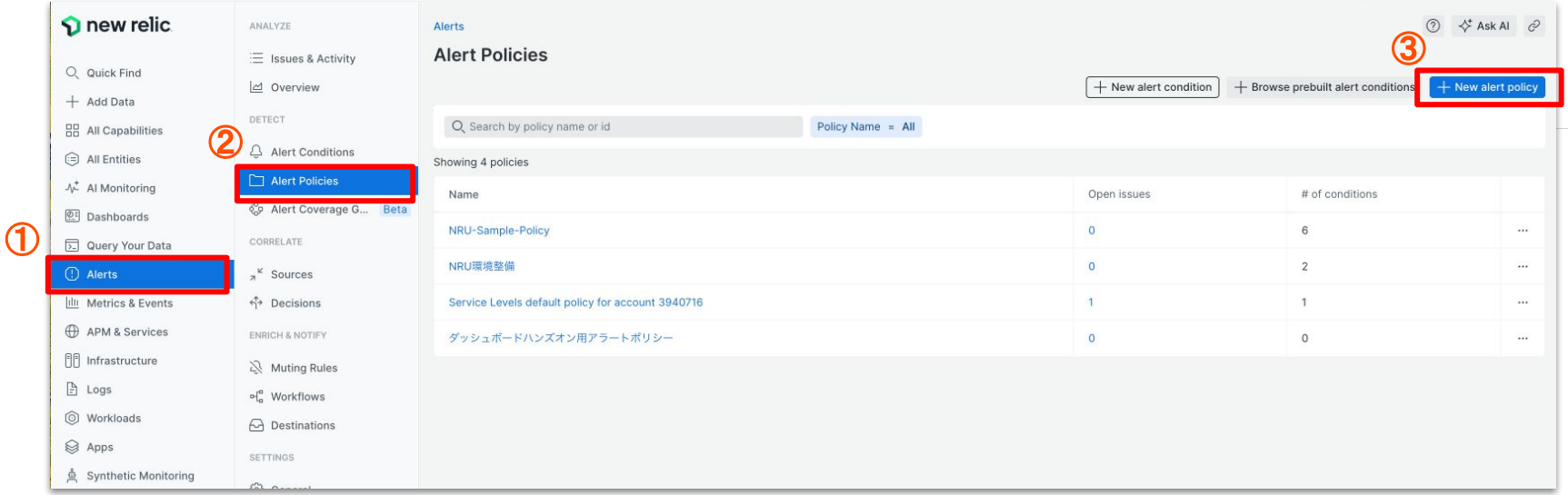
new relic


@brian is this the problem?
@suni yup. just pushed a fix!
Data for Engineers_
traceID.mod

手順・解説

ハンズオン(1-1) Alert policyを作成する 1/2

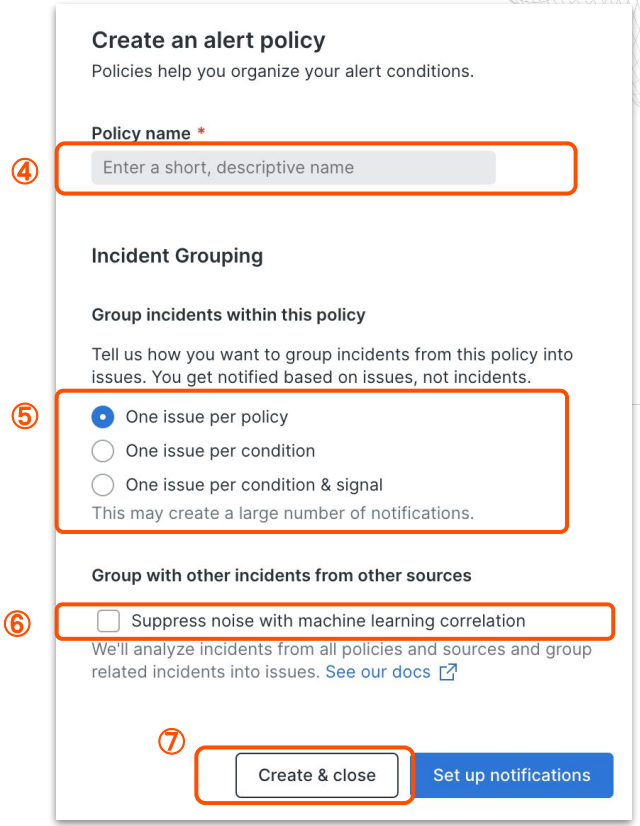
1. Alerts メニューを開きます。
2. Alert Policies を開きます。
3. [+New alert policy] を選択して、新しい Alert Policyを作成します。



ハンズオン(1-1) Alert policyを作成する 2/2

4. 右側から設定画面がスライドされてくるので、Policy nameには、ご自身が作成したとわかる名前をつけてください
5. こちらのスライド を参考に、好みの「Incident Grouping」を選択してください
6. [Suppress noise...]をチェック
7. [Create & close] をクリックします

ウィザードでの一括作成もできますが、今回は各コンポーネントを手動で作成したいため、ここでは **Alert policyのみ**を作成します

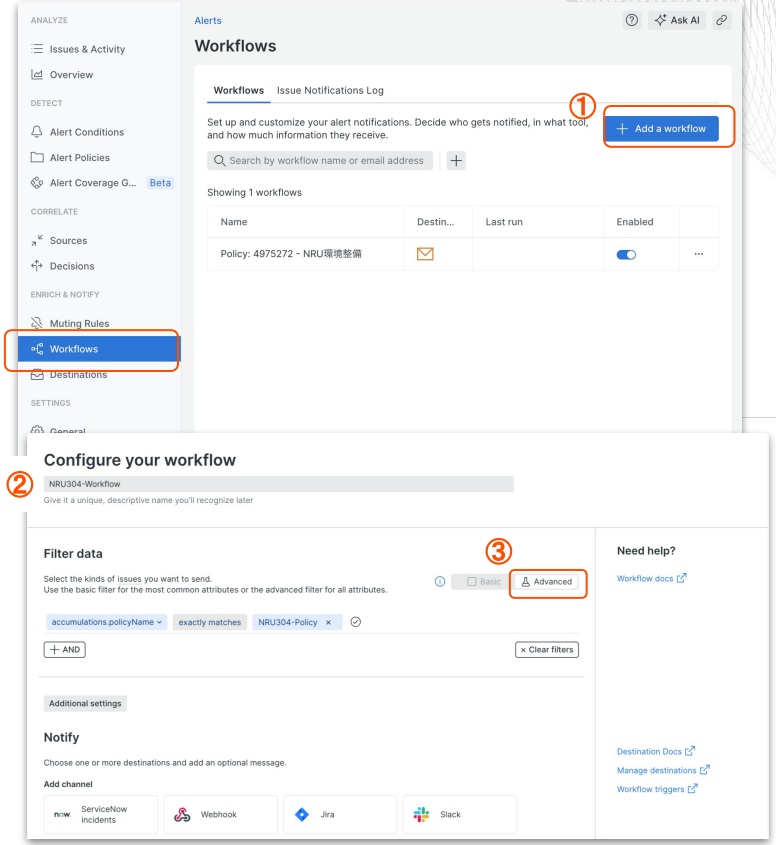


new relic

ハンズオン(1-2) Workflowを作成する 1/6

1. Alertsメニューの Workflowsをクリックし、
   [+ Add a workflow]をクリックします
2. ご自身のworkflowであることがわかる名前を入力します
3. Filter dataで"Advanced"を選択し、
   次のフィルタを設定します
   a. Select or enter attribute: policyName
   b. Select operator: exactly matches
   c. Select or enter value: 作成したポリシーを選択

補足: 上記3番の設定はBasicでも可能ですが、より柔軟な設定を行う場合にはAdvancedを活用します。



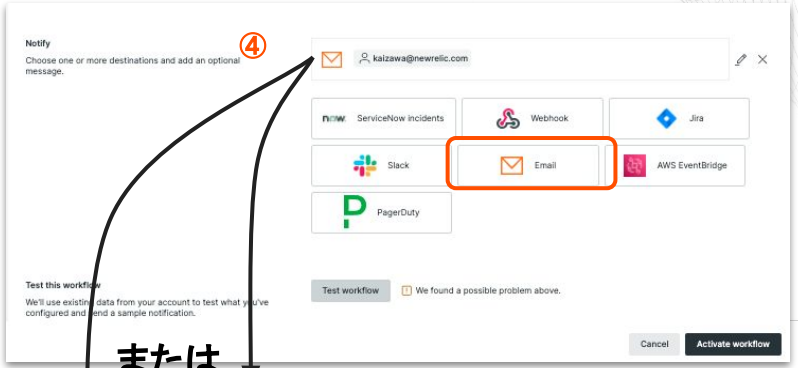
new relic

ハンズオン(1-2) Workflowを作成する 2/6

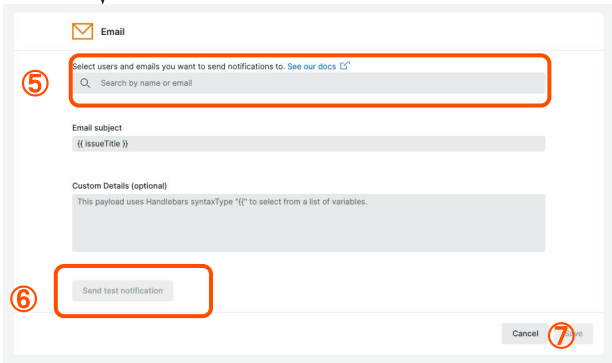
4. Notify: **Email**を選択します
5. メール送信内容を設定します

   ご自身のメールアドレスを入力して下さい。

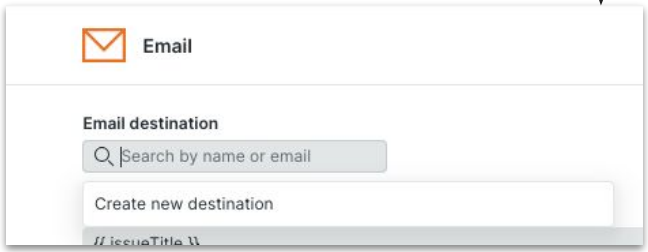
   (補足)新規で登録する場合、プルダウンメニューの
   "Create new destination"をクリックし、
   メールアドレスの新規登録作業を行います。
6. **Send test notification**ボタンをクリックし、テストメールを送信します。受信トレイを確認してみましょう。(次スライドで補足)
7. **Save**ボタンをクリックします



または



⑤



new relic

ハンズオン(1-2) Workflowを作成する 3/6

受信したテストメールを確認します。

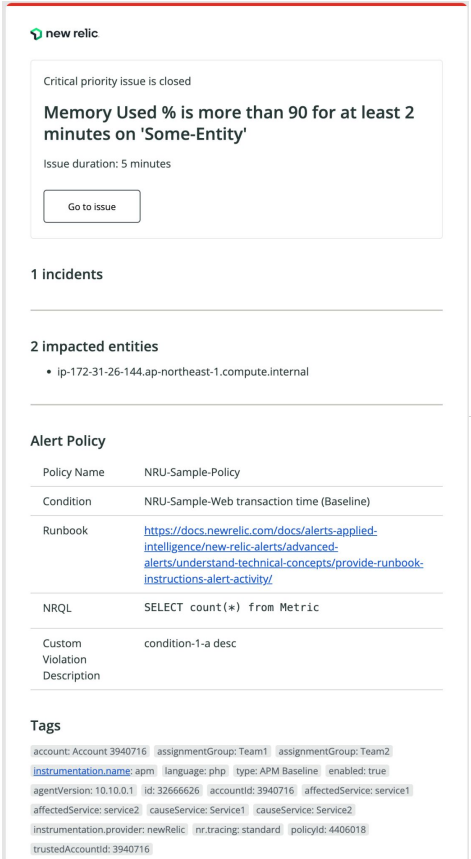
- Policy名やCondtion名は確認できますか？
- Runbook URLはどこに記載されていますか？
- Tagsというセクションには、どのような情報が含まれ ていますか？

余裕があれば、Email subjectやCustom Detailsを変更し、再度テストを行ってみてください。

- 例えばIssueが起票された時刻をCustom Detailsに含めるには、以下のように追記します。

```
Issue activated at : {{  issueActivatedAtUtc }}
```

- "{{"と入力すると、利用可能な環境変数の一覧が表示されます。

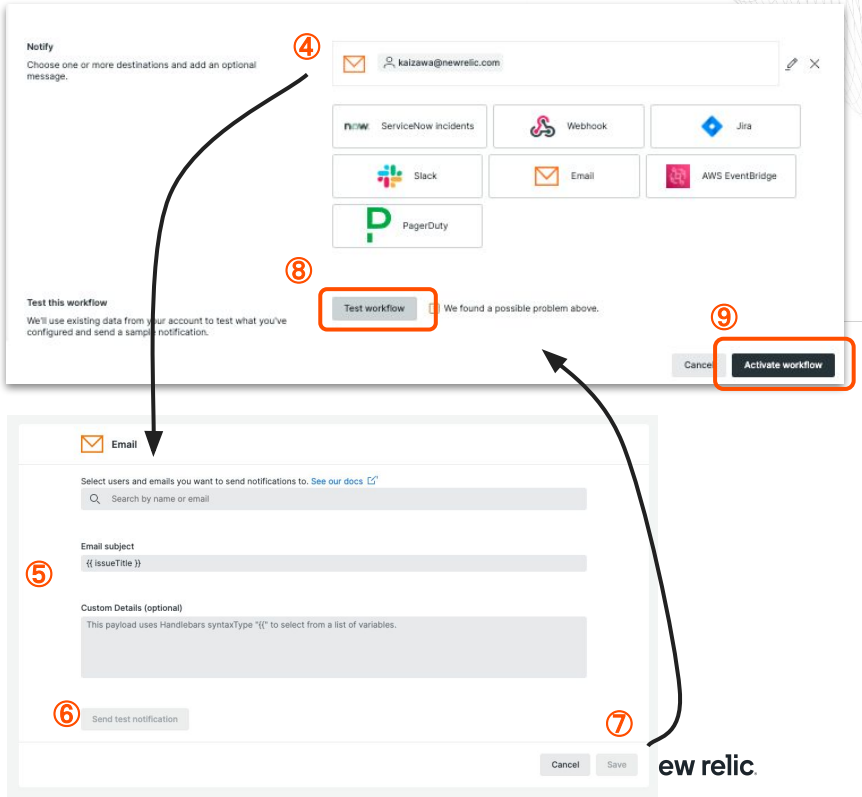


ハンズオン(1-2) Workflowを作成する 4/6

8. 実際のルールでテストする際は、Test workflowボタンを押します

※Alert Conditionをまだ設定していないためTest workflow ボタンを押しても今回メール送信はされません
(Warningが出ますが異常ではありません)

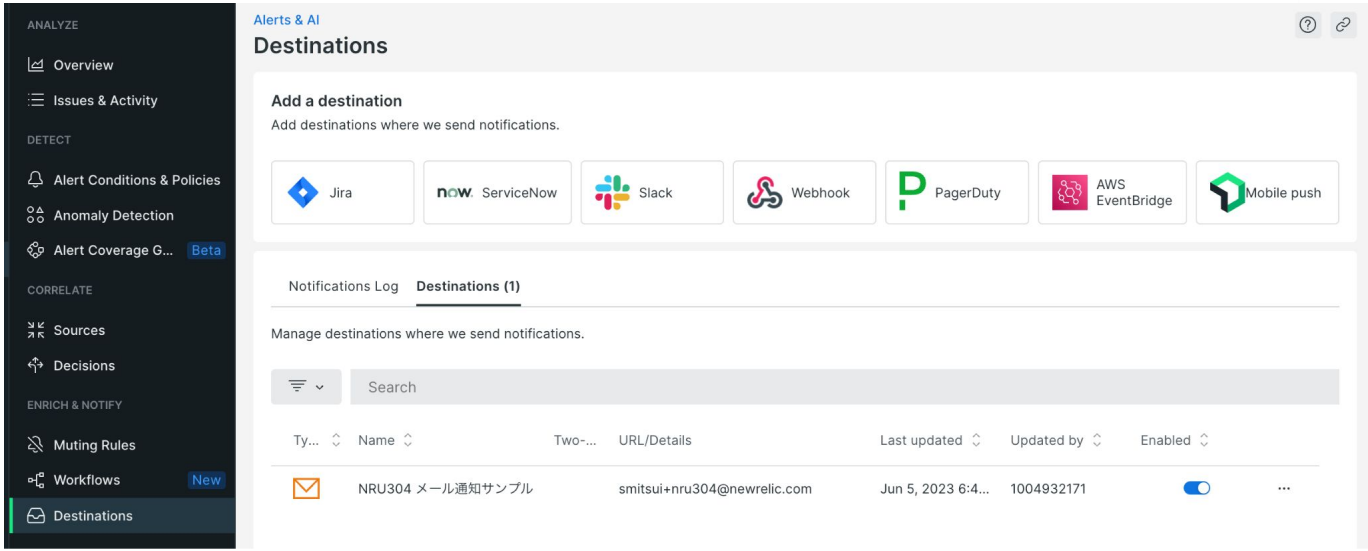
9. Activate workflowボタンをクリックし、設定を保存します



ハンズオン(1-2) Workflowを作成する 5/6

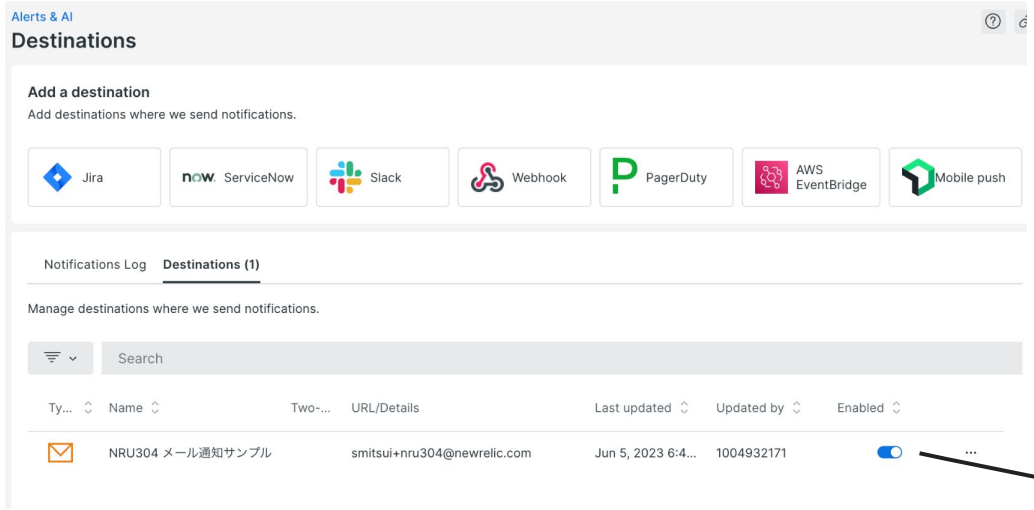
Workflows内でEmailを追加すると、Destinationも自動的に作成されます。

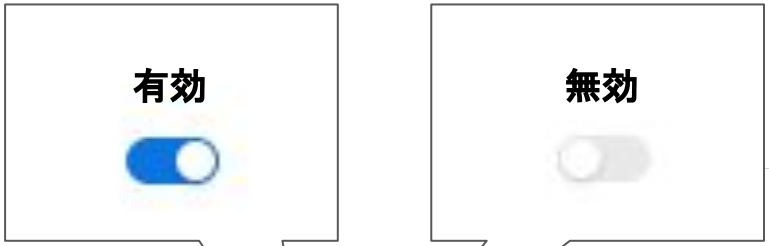
Alerts > Destinationsで、ご自身のメールアドレスが追加されていることを確認します。



ハンズオン(1-2) Workflowを作成する 6/6

メール通知をこのセッション中に無効にしたい場合、Enabledトグルボタンを無効化して下さい。





座学(3)
アラートコンディションの作成

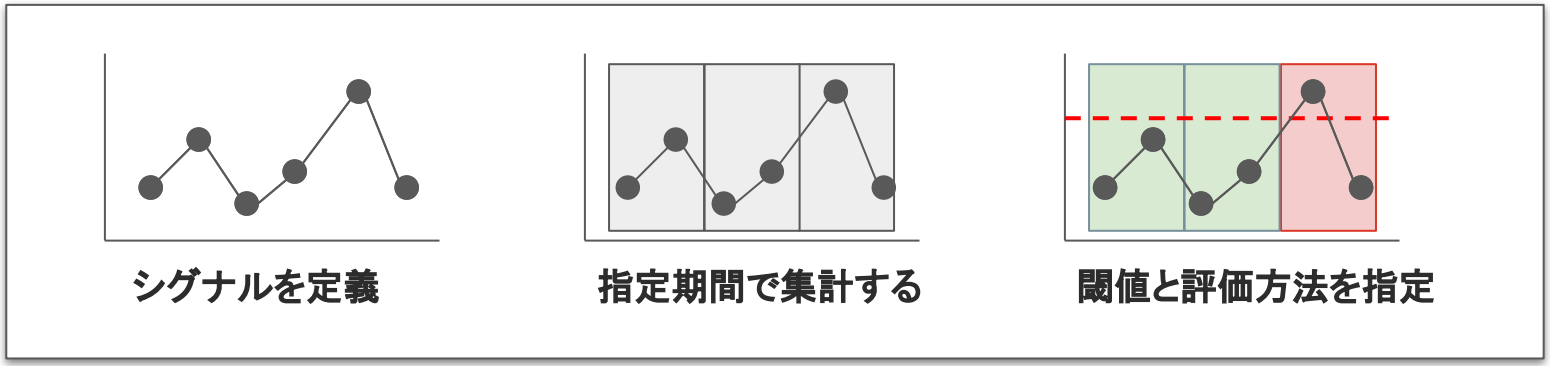
16:00 - 16:20 (20min)

new relic

Alert Condition

New Relicが収集しているリアルタイムなデータを、集計・評価する仕組み
以下の4ステップで設定

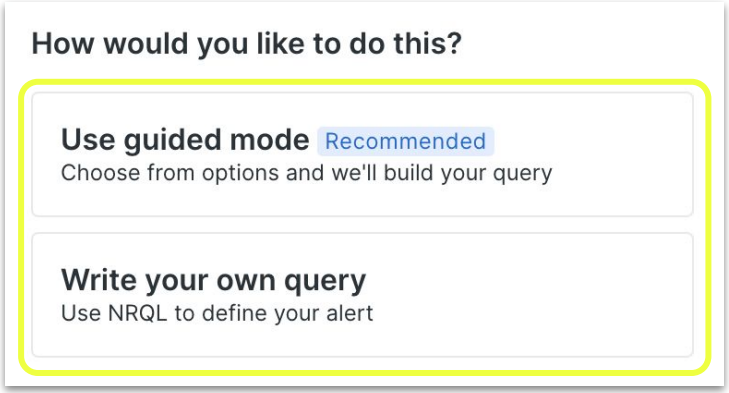
1. **シグナルを定義**（何を監視対象とするか）
2. **シグナルを集計**（シグナルをどう集計するか）
3. **閾値を設定**（集計結果をどう評価してインシデントを生成）
4. **インシデントに情報追加**



new relic

1. シグナルを定義

ガイドを使うか、直接 NRQLでシグナルを指定することでシグナルを設定
（平均値・最大値・データ件数カウントなど）

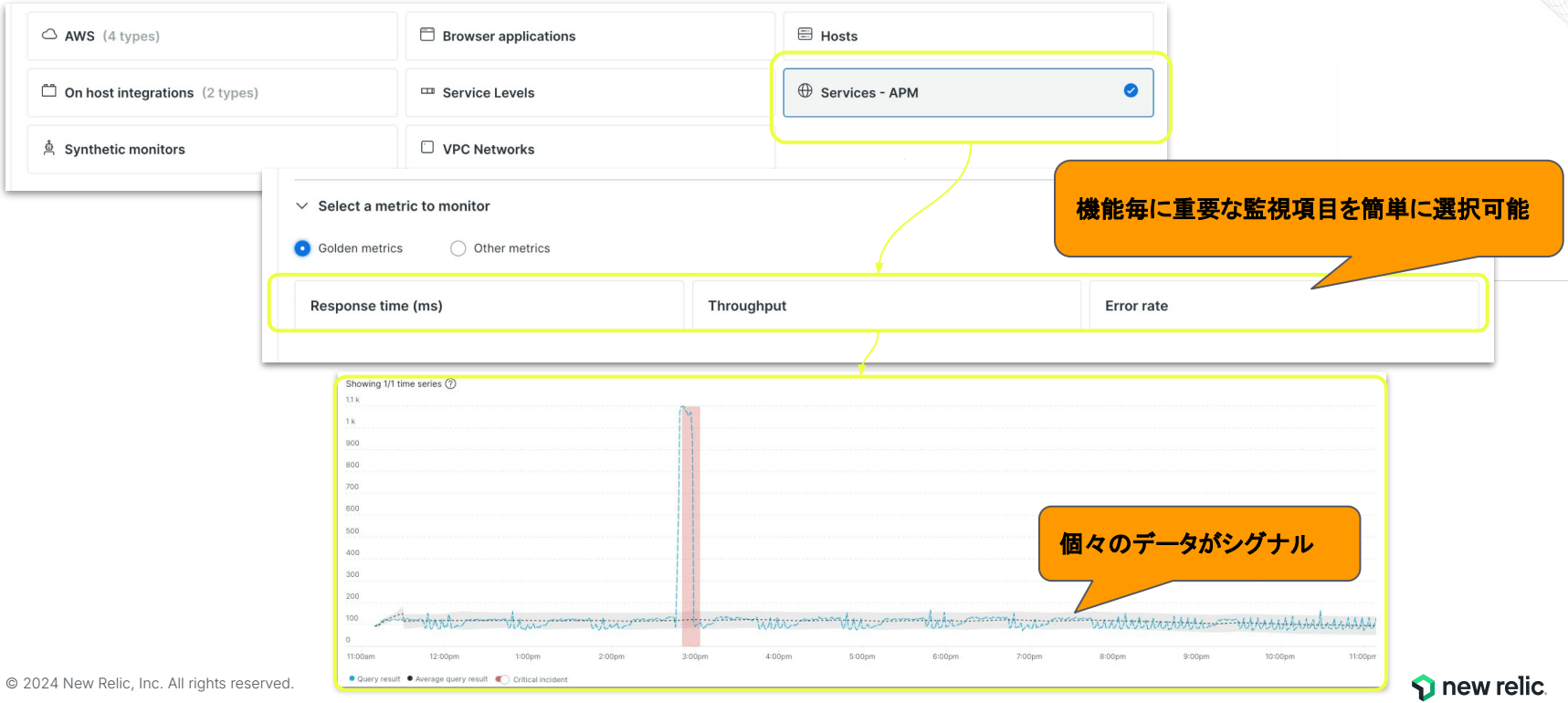


機能（例. APM, Browser等）ごとに用意されたプリセットから簡単にアラートを作れるほか、
自分でNRQLクエリを記述して、独自の Alert Conditionを作成することも可能

new relic

1. シグナルを定義 - Use guided mode

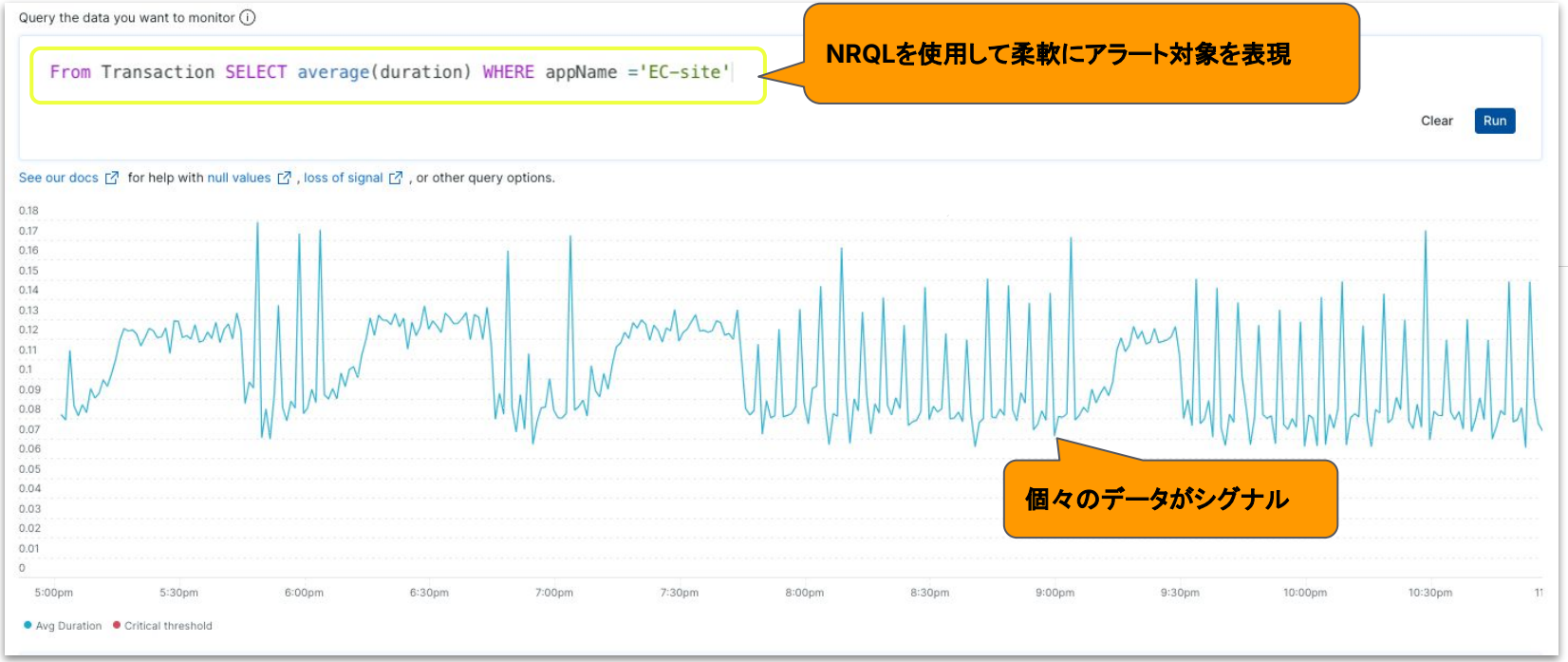
Golden Signalをベースにそれぞれの機能に合わせて、ガイド付きで対象となるシグナルを設定



new relic

1. シグナルを定義 - Write your own query

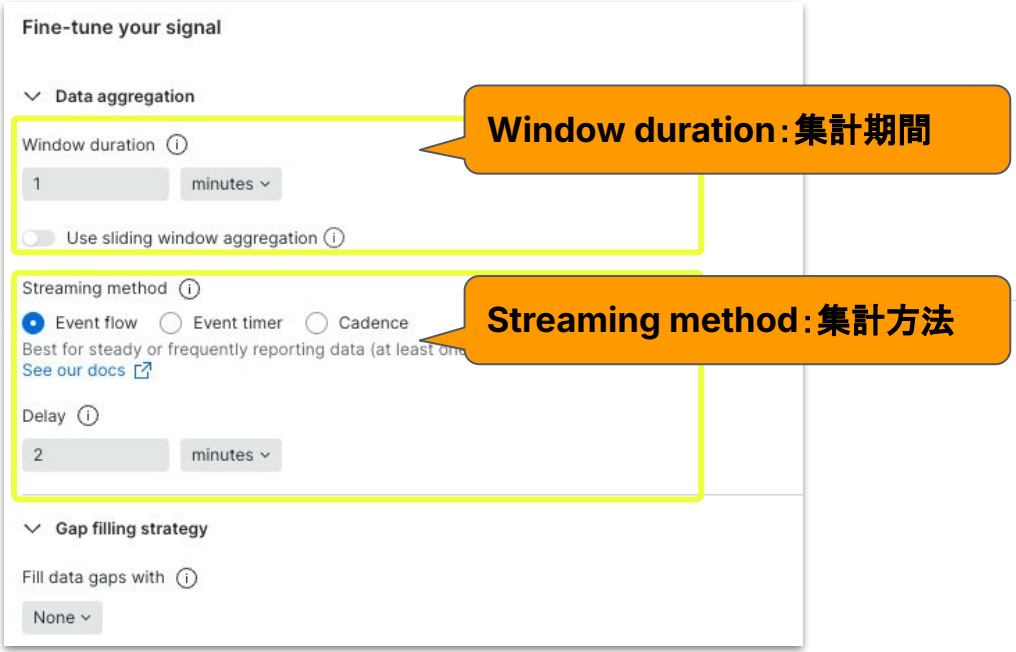
NRQLを使用してベースとなるシグナルを設定



new relic

2. シグナルを集計

データの性質に合わせてシグナルをどう集計するか設定



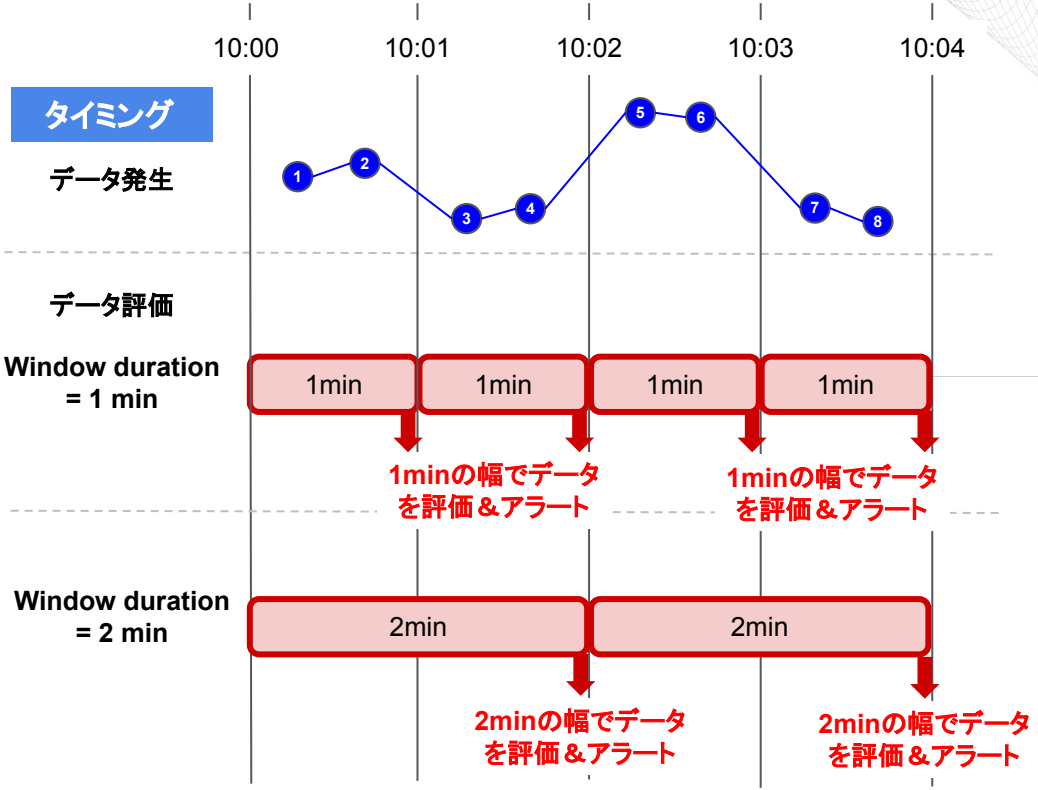
new relic

2. シグナルを集計 - Window Duration

アラート条件ごとに**集計ウインドウの期間を Window Duration** として設定します。

プレビューにおいて、チャート上にプロットされる個々の点がシグナル、

点と点の間隔が集計ウインドウにあたります。



new relic

2. シグナルを集計 - Window Duration（Sliding window）

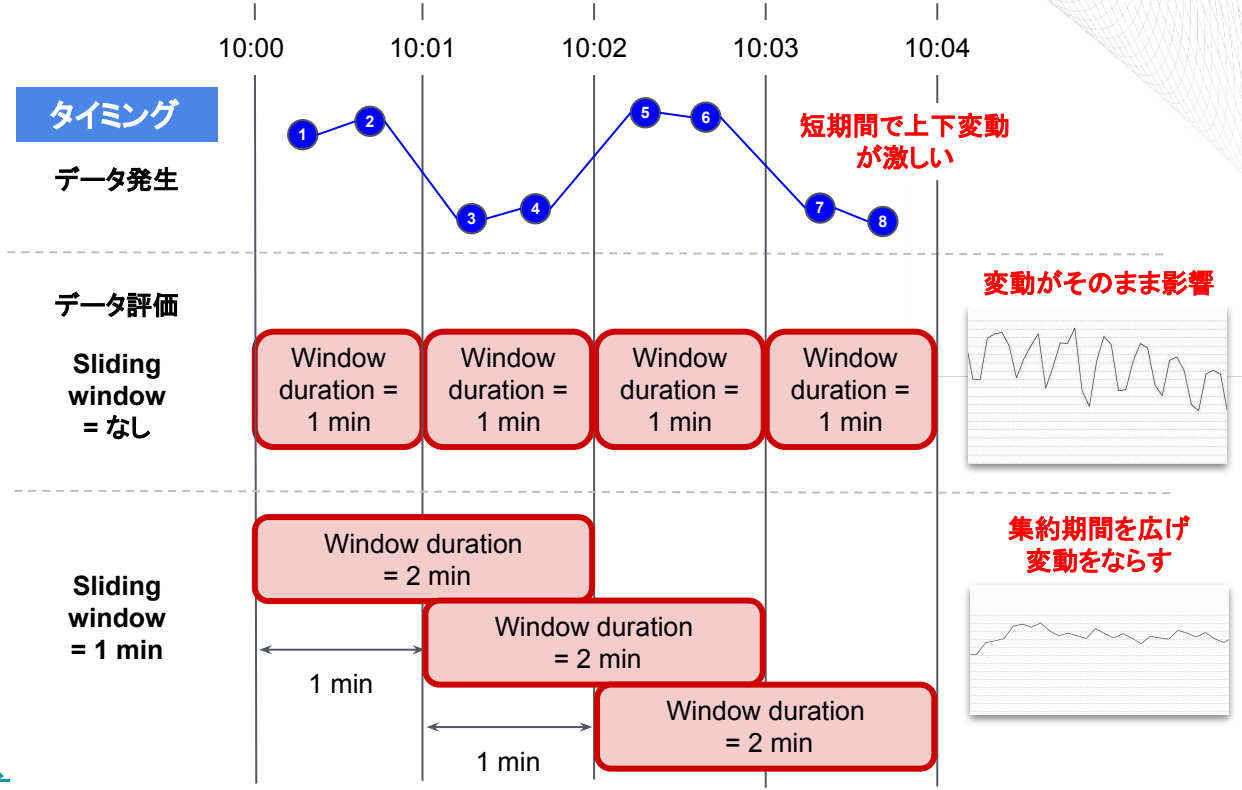
通常、集計ウィンドウの期間は互いに重なりません。
Sliding Windowオプションを有効にすると、**指定した時間分スライドさせた複数の集計ウィンドウが並行して開かれる**ため、よりきめ細かい集計結果を得ることができます。

適しているデータ

データの山谷が激しく、かつ短期間の集約では適切に評価することができないデータ

- CPU%、スループット
- 不安定、頻繁でない、または一貫性のないシグナル

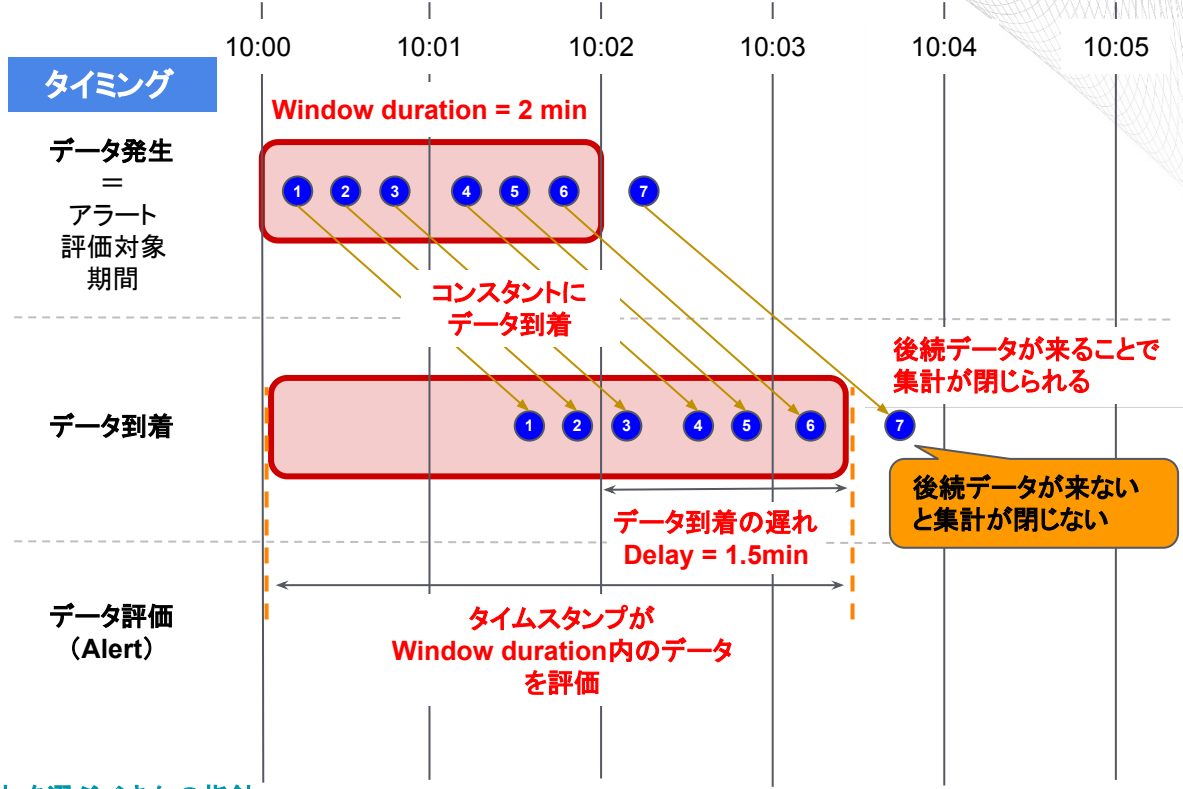
出典：新機能スライディングウィンドウアラートのリリース



new relic

2. シグナルを集計 - Streaming method（Event Flow）

指定した**遅延（Delay）の時間経過**し、**後続のウィンドウのデータが到着したタイミングで評価対象期間のデータを集約**する。それを超えて到着したデータは評価対象外。
後続データが到着しないと集計が閉じないので注意が必要。

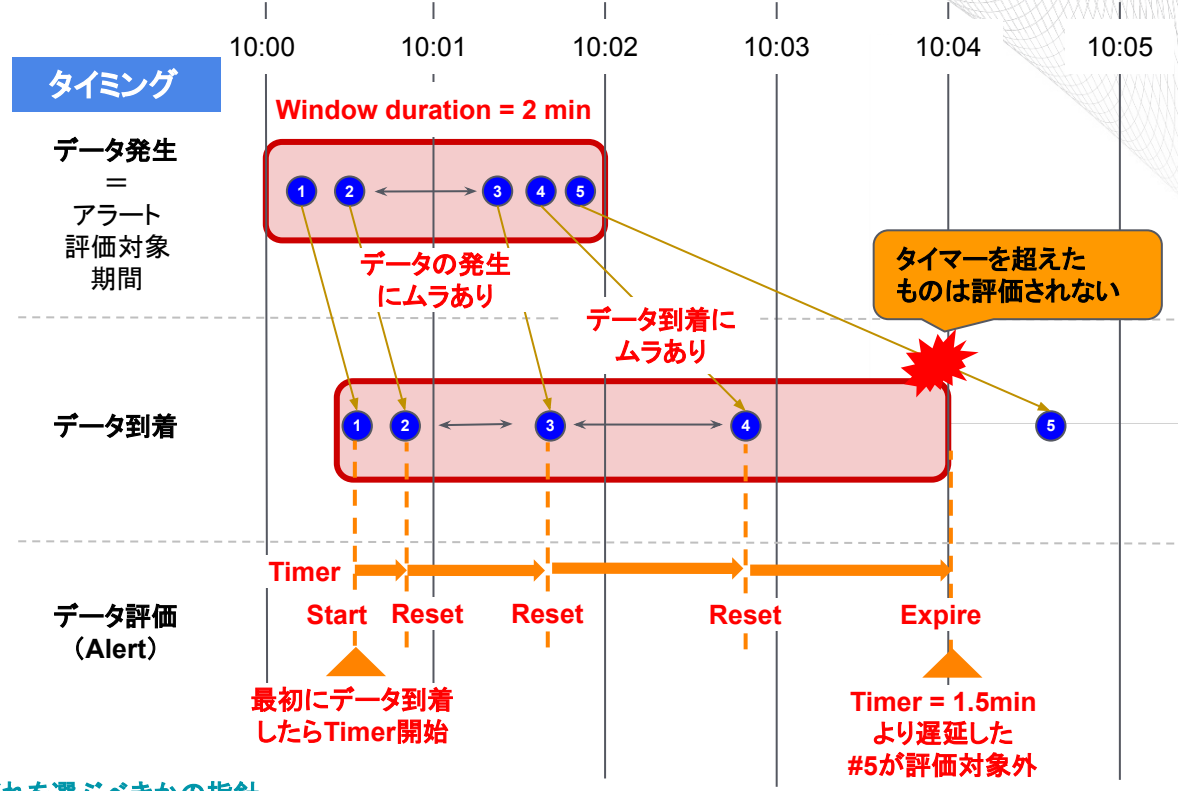


出典：[NRQLアラート条件に追加された新しい集計方法とどれを選ぶべきかの指針]

new relic

2. シグナルを集計 - Streaming method（Event Timer）

到着順序や発生間隔に一貫性のない
データを評価するのに最適な方式です。
集計ウィンドウ内のデータが最後に到着してからの**時間経過によって、集計ウィンドウが閉じられます 。**



出典：[NRQLアラート条件に追加された新しい集計方法とどれを選ぶべきかの指針 LogやSyntheticの監視のベストプラクティス]

new relic

2. シグナルを集計 - Streaming method（Cadence）

Cadenceは、データのタイムスタンプではなく、
New Relic内部のシステムクロックに基づいて、一定の間隔で集計を行う方法　です。

多くのケースではEvent FlowまたはEvent Timerが適していますが、
モバイル端末やブラウザから送信されるイベントのように、
ユーザー端末の時刻設定に影響されて、タイムスタンプに一貫性がないデータを対象にする場合　に有効。

補足：データ転送の頻度を加味した設定例

データソース	説明	Streaming method	Delay/Timer
クラウド統合(GCP, Azure, AWS API Polling, AWS MetricStream)	ポーリングは離散的にデータが届く。ストリーミングはコンスタントにデータが到着する。タイムラグを考慮しつつ、メトリクスの特性に合わせて設定	Event Timer / Event Flow	ポーリング間隔以上/10分前後
Infrastructureエージェント（OHI含む）	エージェントが1分間隔でデータをコンスタントに送信	Event Flow	2分 (デフォルト)
APMエージェント	APMエージェントはデフォルトで5秒間隔でデータをコンスタントに送信	Event Flow	2分 (デフォルト)
Browserエージェント	最長でも1分以内にコンスタントにデータを送信	Event Flow	2分 (デフォルト)
Mobileエージェント	Mobileエージェントはデフォルトで10分間隔でデータを送信。また、アプリのオフライン、バックグラウンド実行によるデータ転送遅延を考慮	Event Timer / Cadence	10分以上
Serverless（Lambdaレイヤ）	実行中/後にすぐにデータが送信される	Event Flow	2分 (デフォルト)
Log	ログ連携方法によるがAPIで直接転送を実装する以外は最長でも1分以内には送信される(AWS S3経由が最も遅延)	Event Timer (*) / Event Flow	2分 (デフォルト)
Synthetics	実行後すぐにデータが送信される	Event Timer (*) / Event Flow	2分 (デフォルト)
APIによる転送	API（Trace/Metric/Event/Log）の利用方法に依存	Event Timer / Event Flow	API実行頻度による

*: NRQLアラートのWHERE句の絞り込み条件により0件になることが多い場合はデータロスと認識されて評価されないので Event Timerが適切

new relic

補足: Gap-filling strategy

概要

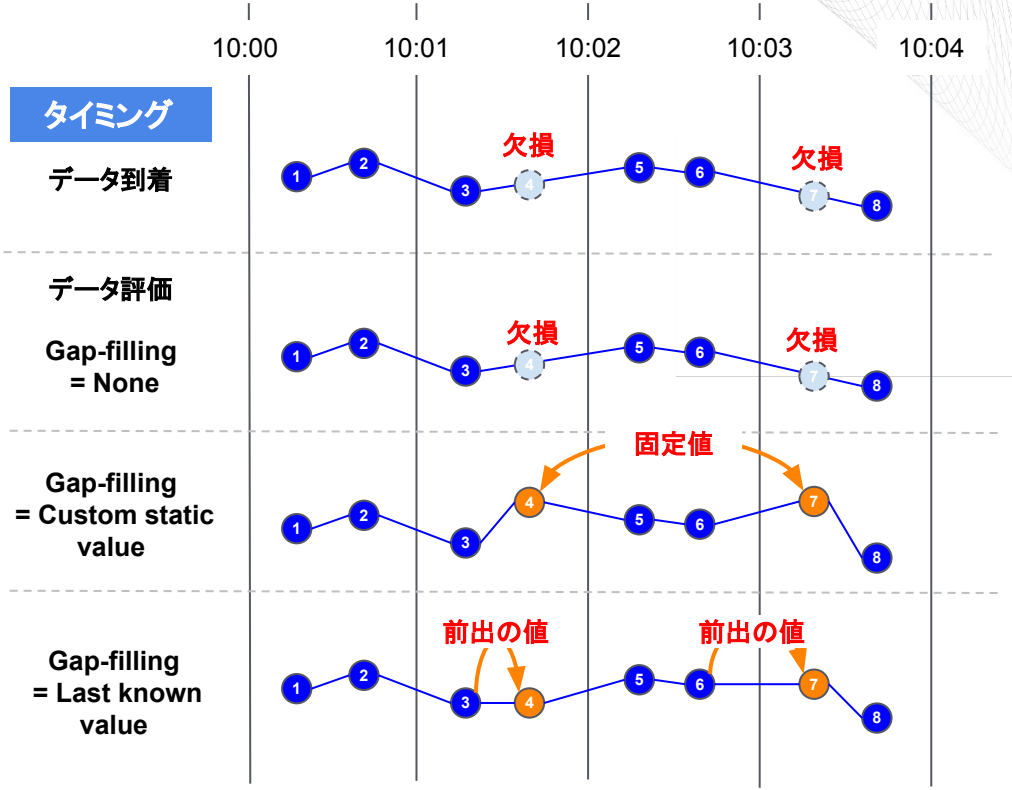
到着したデータに欠損が存在する場合に、欠損データをどう扱って評価するか。以下の設定が可能

欠損のまま（None）:
欠損データは閾値の違反に該当しないので、欠損がある場合に違反のアクションを起こしたくない場合に適しています。欠損データはそのまま欠損データ（Null）として扱われます。

固定値（Custom static value）:
妥当な固定値はケースによる。欠損した場合に違反の方に倒す、安全サイドに倒す、もしくは対象メトリクスに応じた値。

前出の値（Last known value）:
値の変化が予測可能なもので、短時間で大きく変化しないもの。例えばディスク使用率など。

出典：[データのギャップを埋める]



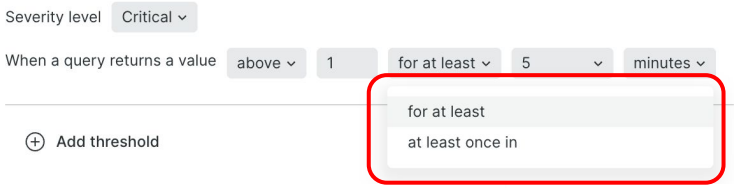
new relic

3. 閾値を設定

アラートのしきい値設定は2種類から選択可能

種類	説明	アラートトリガー例
静的(Static)	ある特定の数値を上回った、または下回った場合にアラートをトリガー	エラー発生割合が5%を超過した
動的(Anomaly)	いつもと異なる振る舞いをした場合にアラートをトリガー、どの程度の変動を許容するかを設定できる https://docs.newrelic.com/jp/docs/alerts-applied-intelligence/applied-intelligence/anomaly-detection/	エラー発生割合がいつもよりも増加した

3. 閾値を設定



静的(Static) しきい値の超過を評価する方法

- **For at least xx minutes**

  xx分間、しきい値を**超過する状態が続いた場合**に、Incidentが起票される

- **at least once in xx minutes**

  xx分間で、しきい値を**1回でも超過した場合**に、Incidentが起票される

一つのAlert Conditionには、CriticalとWarning(オプション)の閾値を設定可能

その他、アラート設定に関する詳細は以下もご参照ください:

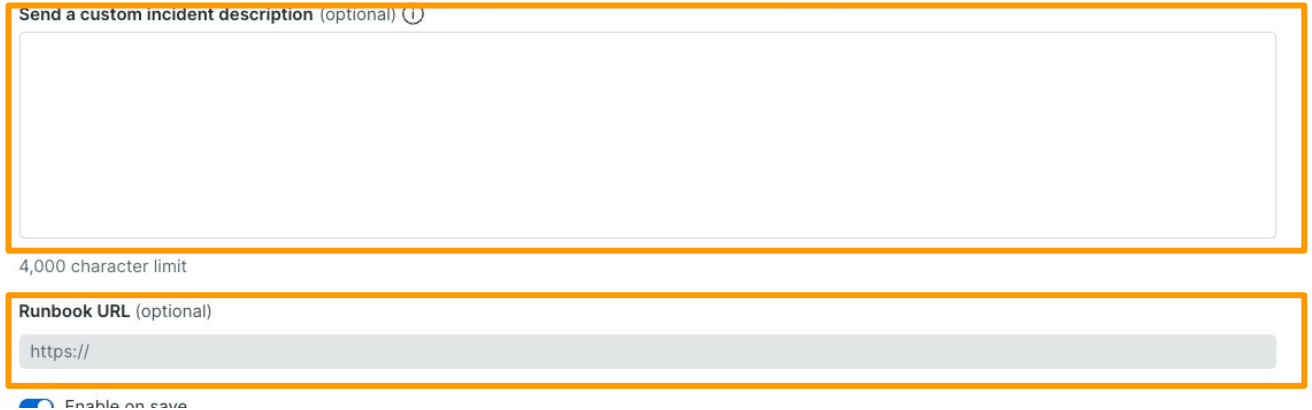
ストリーミング・アラートの概念 | New Relic (https://newrelic.com/jp/blog/how-to-relic/streaming-alert-concept)
アラート条件を正しく設定するための詳細ガイド | New Relic (https://newrelic.com/jp/blog/how-to-relic/understand-nrql-alert-condition)
アラート定義のガイダンス | New Relic (https://newrelic.com/jp/blog/how-to-relic/alert-configuration-guidance)

new relic

4. インシデントに情報追加

効果的な通知を送るためのプラクティス

- Send a custom incident description
  発報されるアラートに任意の情報を付加することが可能 (参考情報)
- Runbook URL
  アラート対応手順書や、情報を集約したダッシュボードにすぐにアクセスすることが可能



new relic

ハンズオン(2)
アラートコンディションを作成

16:20 - 16:35 (15min)

ハンズオン(2-1) Alert Conditionを作成する 1/21

新規Alert Conditionの追加

4つのアラートを順番に設定していきます

1. フロントエンド：ページロード時間
2. アプリケーション：4xx,5xxエラー(ホストごと発生数を設定する)
3. アプリケーション：応答時間(動的)
4. 外形監視:チェックエラー

Tips: Conditionの作成は、各自で作成したポリシーにアクセスし、"New alert condition"ボタンから開始すると、後続のステップが理解しやすいかと思います。

具体的な手順は後続のスライドからご確認下さい。

new relic

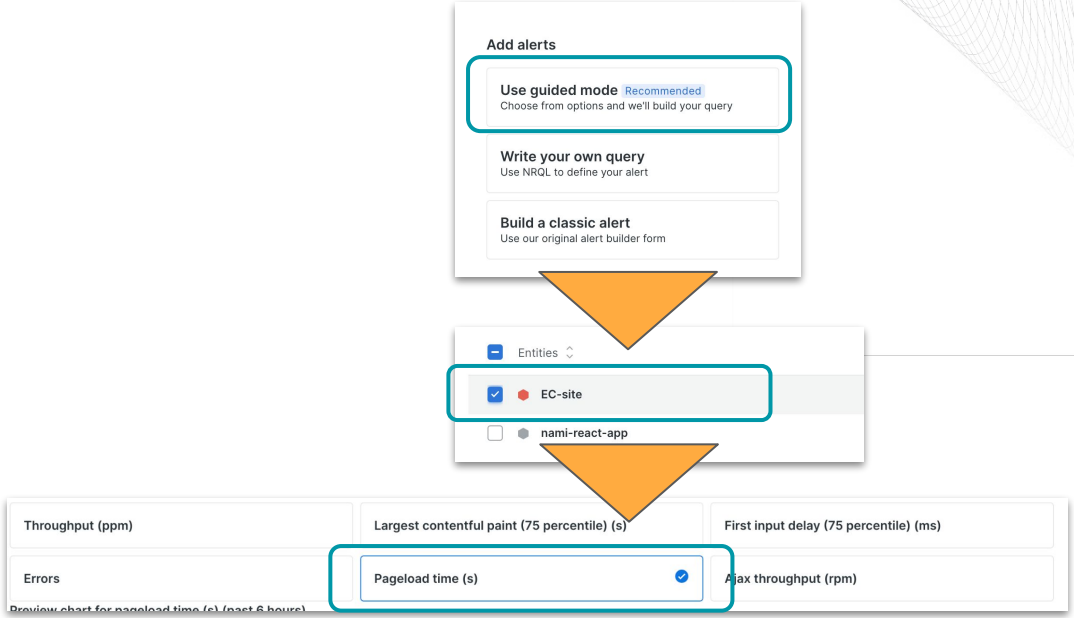
ハンズオン(2-1) Alert Conditionを作成する 2/21

- **新規Alert Conditionの追加**

①フロントエンド：ページロード時間

1. **Add alerts**
   a. Use guided mode
2. **Tell us what where to look**
   a. Browser applications
3. **Tell us what to watch**
   a. EC-site
4. **Select a metric to monitor**
   a. Pageload time(s)

画面遷移(一部スキップあり)のヒント



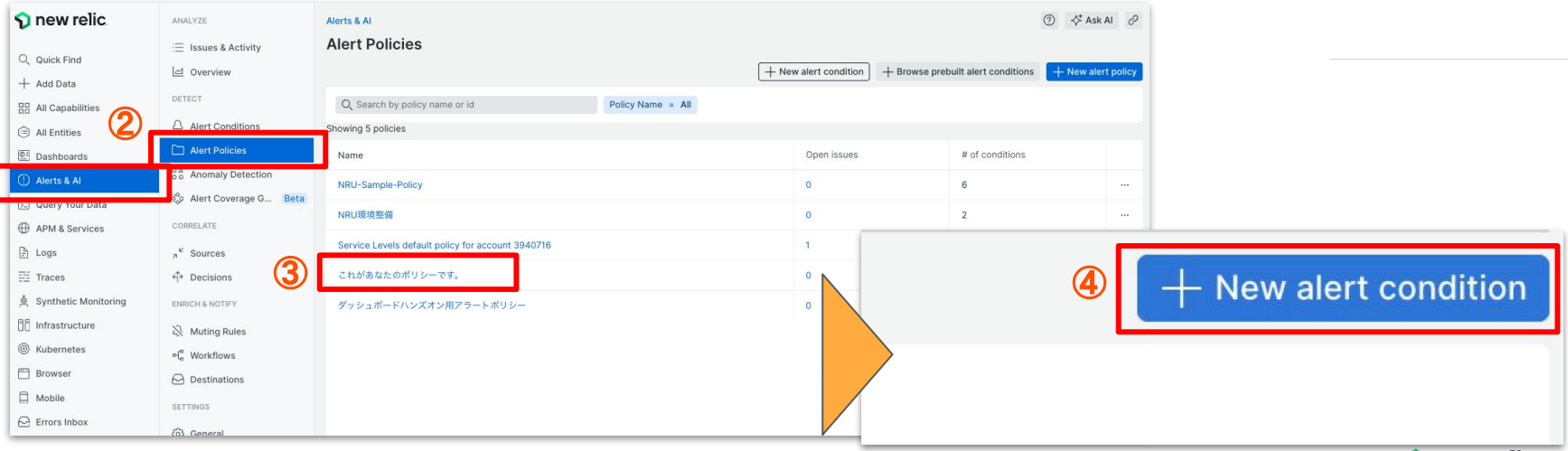
Condition名は適切なものを各自設定してください

（例：NRU304-yourname-NRQL-pageloadtime）

具体的な手順は後続のスライドからご確認下さい。

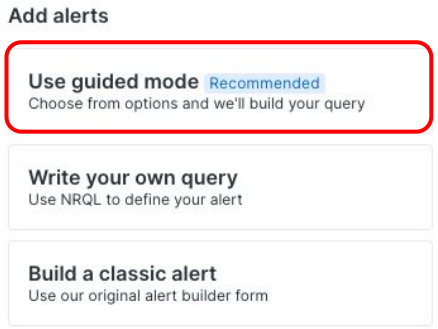
ハンズオン(2-1) Alert Conditionを作成する 3/21

1. Alerts メニューを開きます。
2. Alert Policies を開きます。
3. 前のハンズオンセクションで作成したポリシーを選択します。
4. 画面右側にある[+New alert condition] を選択して、新しいAlert Conditionを作成します。

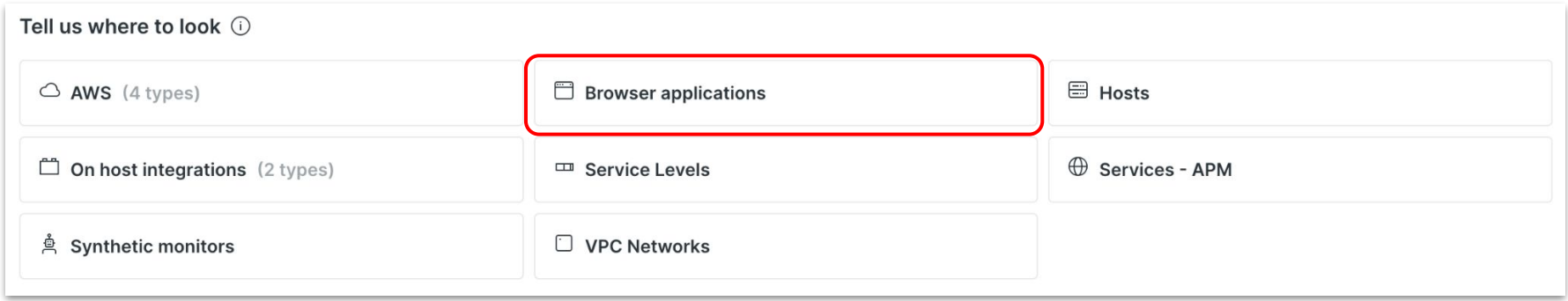


ハンズオン(2-1) Alert Conditionを作成する 4/21

- 「Use guided mode」を選択



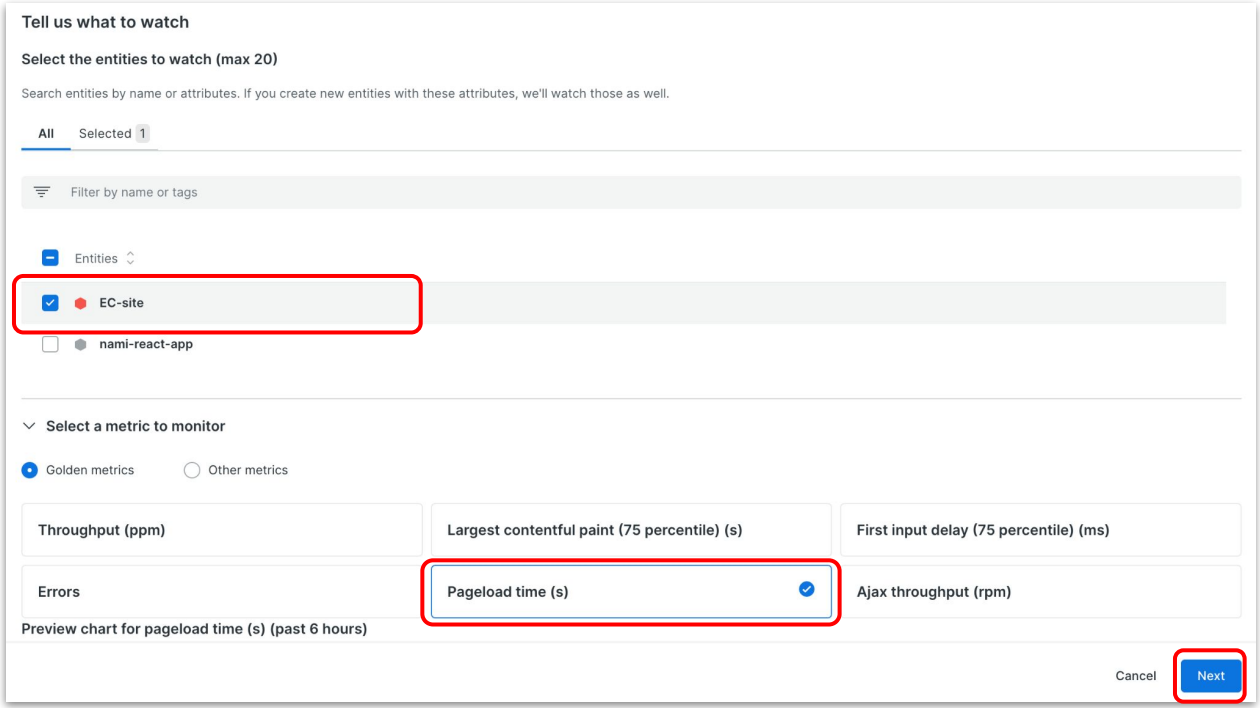
- 「Browser applications」を選択して、「Next」を押下



new relic

ハンズオン(2-1) Alert Conditionを作成する 5/21

- 「EC-site」、「Pageload time(s)」を選択し「Next」をクリックします。



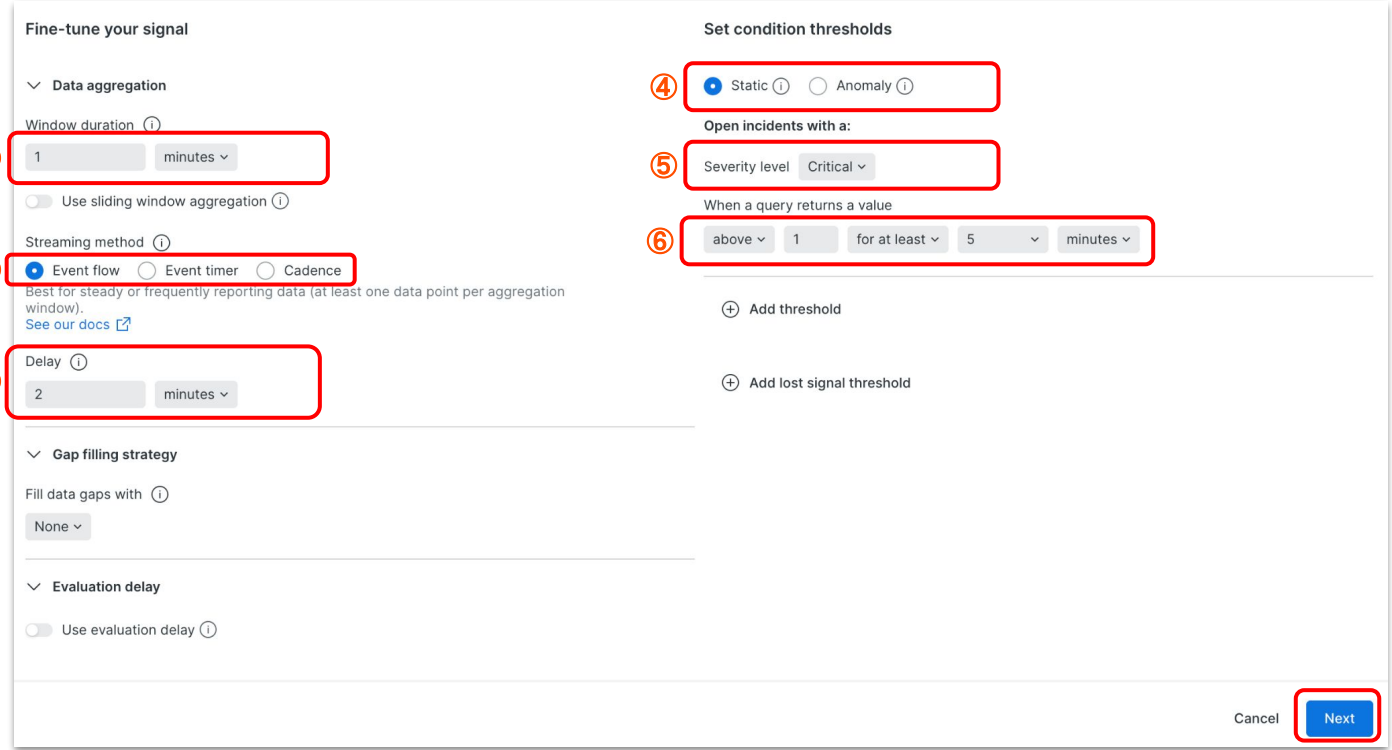
ハンズオン(2-1) Alert Conditionを作成する 6/21

- 監視設定は次のようにしてください。

1. **Window Duration**
   a. 1 minutes
2. **Streaming method**
   a. Event flow
3. **Delay**
   a. 2minutes
4. **Set condition thresholds**
   a. Static
5. **Severity level**
   a. Critical
6. **When a query returns a value**
   a. above 1 for at least 5 minutes

ハンズオン(2-1) Alert Conditionを作成する 7/21

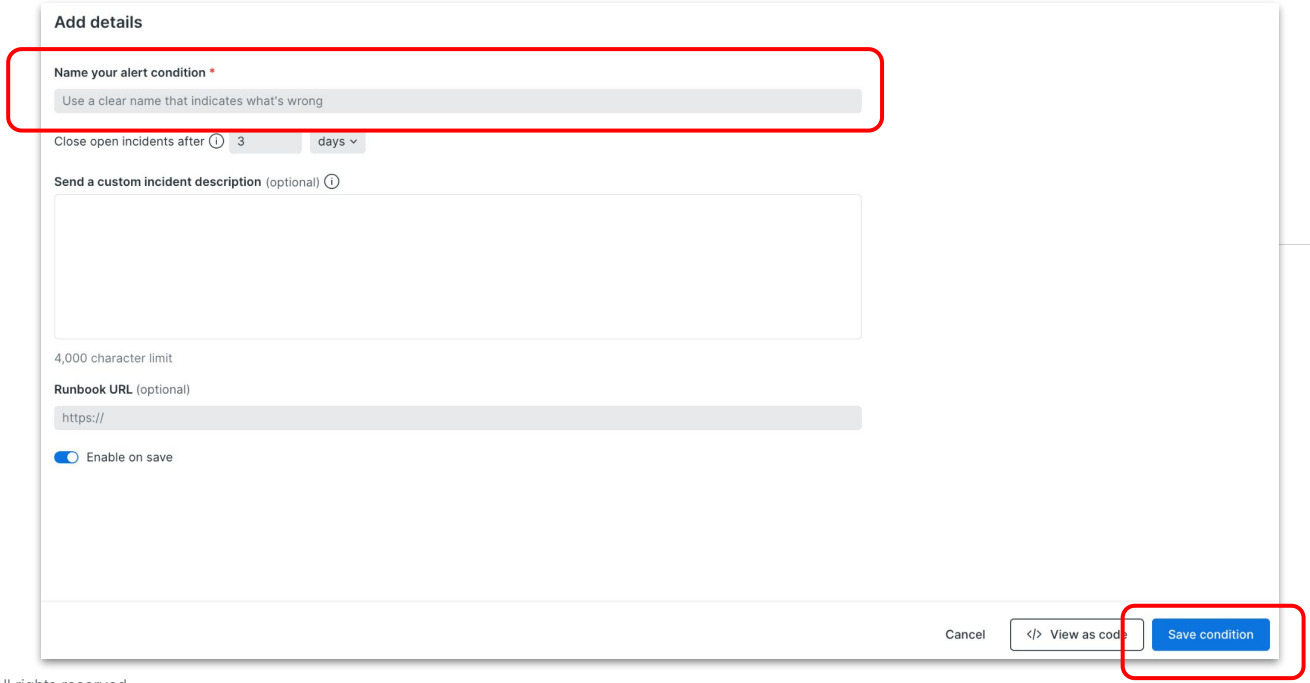
- それぞれ 設定を確認し「Next」をクリック。



new relic

ハンズオン(2-1) Alert Conditionを作成する 8/21

- コンディション名にわかりやすい名前を入力し、「 Save condition」をクリックする。
  （例：NRU304-yourname-Performance）



new relic

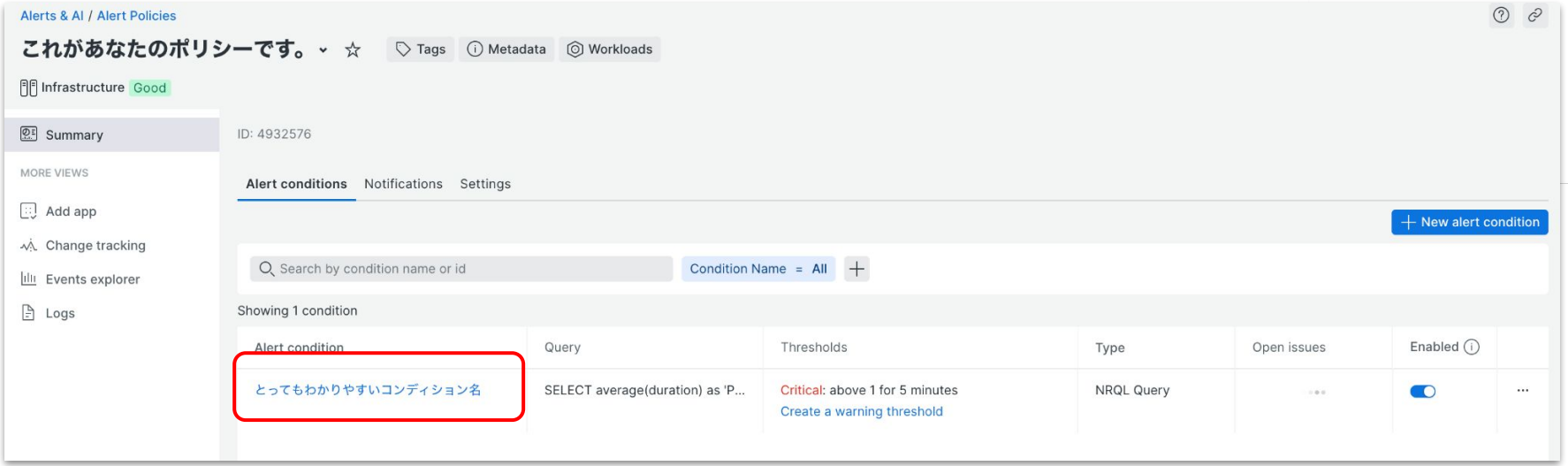
ハンズオン(2-1) Alert Conditionを作成する 9/21

- Summaryページが開き、Queryの内容やチャートが表示されます。「 Close」をクリックします。

new relic

ハンズオン(2-1) Alert Conditionを作成する 10/21

- コンディションが作成されました。 名前やcategoryをクリックすれば設定を編集できます。



ハンズオン(2-1) Alert Conditionを作成する 11/21

- **新規Alert Conditionの追加**

  ②アプリケーション：4xx,5xxエラー(ホストごとに評価)

1. **Categories**
   a. NRQL
2. **Define your signal > Query the data you want to monitor**

```
SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction FACET host
```

Condition名は適切なものを各自設定してください

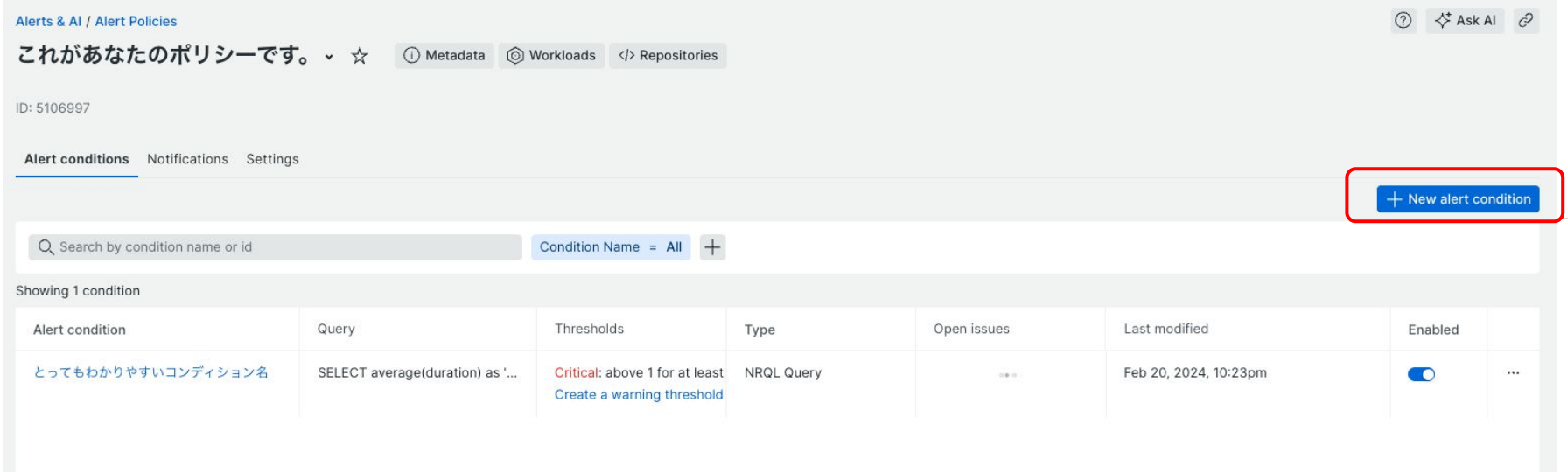
（例：NRU304-yourname-NRQL-ErrorResponse）

具体的な手順は後続のスライドからご確認下さい。

new relic

ハンズオン(2-1) Alert Conditionを作成する 12/22

- 作成したポリシー内にて「 + New alert condition」をクリックする。



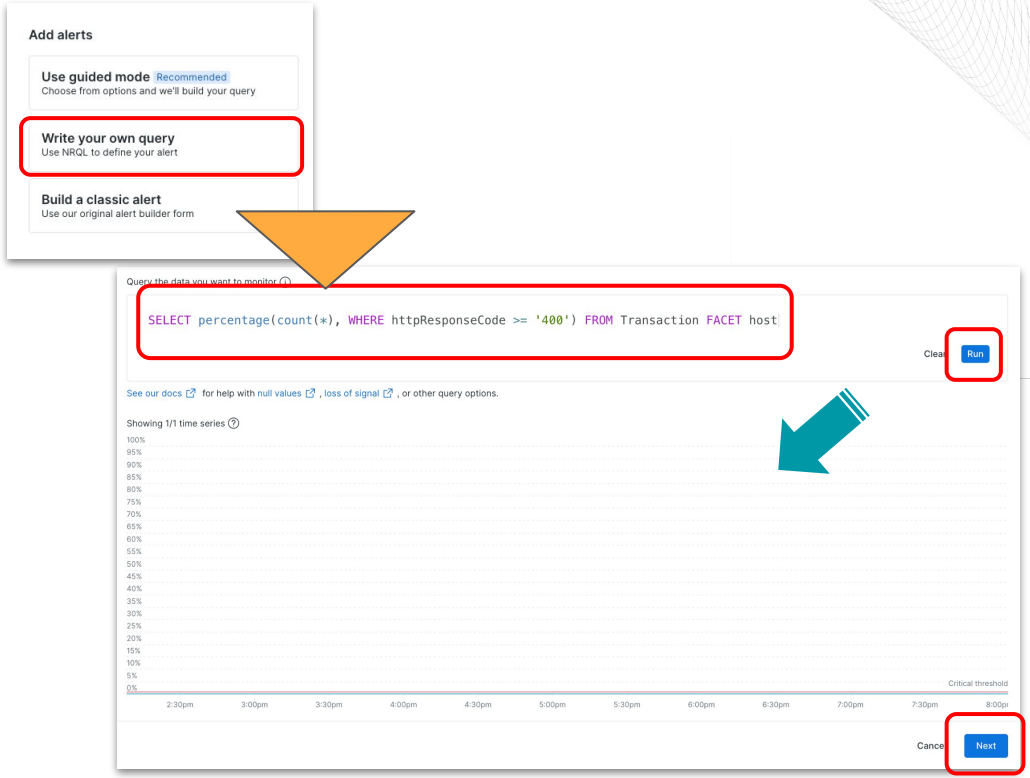
new relic

ハンズオン(2-1) Alert Conditionを作成する 13/21

- 右側からスライドして表示される Add alerts画面から「Write your own query」を選択する。
- クエリ入力欄に次の NRQLクエリをコピー＆ペーストして、Runをクリックします。

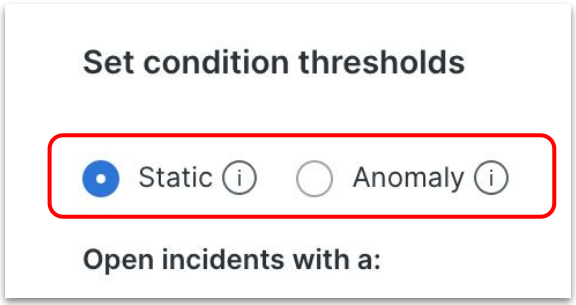
  SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction FACET host

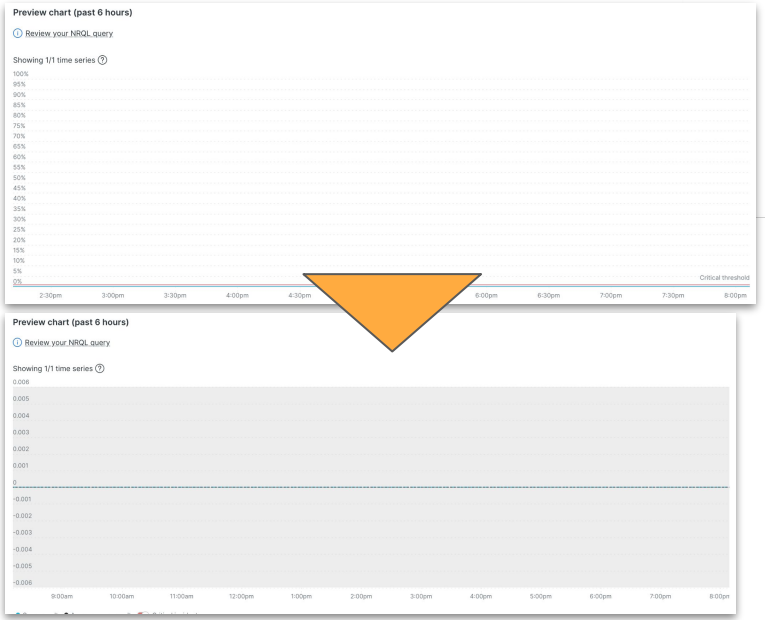
- クエリ実行後、直近の状態を示す参考チャートが表示されることを確認し、Nextをクリックする。



ハンズオン(2-1) Alert Conditionを作成する 14/21

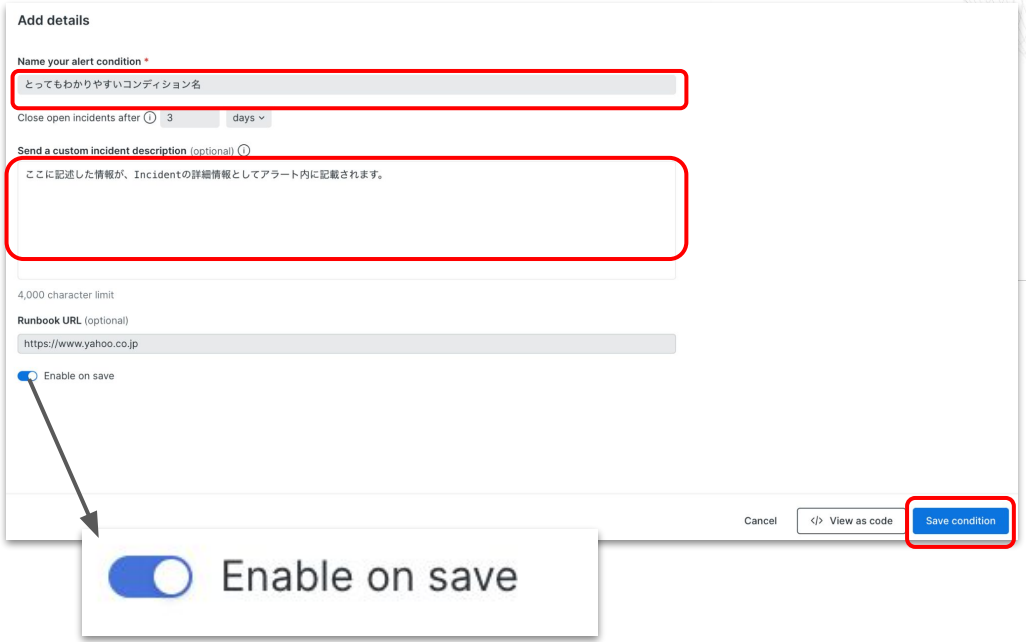
- Fine-tune your signalはすべて初期値のままNextをクリックします。
- 補足: もし時間がある場合は、閾値条件の設定項目にある「Static」を「Anomaly」に変更した場合、チャートがどのように変更されるかを確認してください。





ハンズオン(2-1) Alert Conditionを作成する 15/21

- 任意のAlert Condition名を設定します。
（例：NRU304-yourname-http-error）
- Send a custom incident descriptionとRunbook URLはオプションです。何か思いついた内容を記載してみてください。
- Enable on saveが図の状態になっていることを確認し、Save conditionをクリックします。
- 設定確認画面が表示されるので、Closeをクリックして閉じます。



ハンズオン(2-1) Alert Conditionを作成する 16/21

- **新規Alert Conditionの追加**

  ③アプリケーション：応答時間(動的)

1. **Categories**
   a. NRQL
2. **Define your signal > Query the data you want to monitor**

From Transaction **SELECT** average(duration) **WHERE** appName ='EC-site'

Condition名は適切なものを各自設定してください

（例：NRU304-yourname-transaction-time-baseline）

具体的な手順は後続のスライドからご確認下さい。

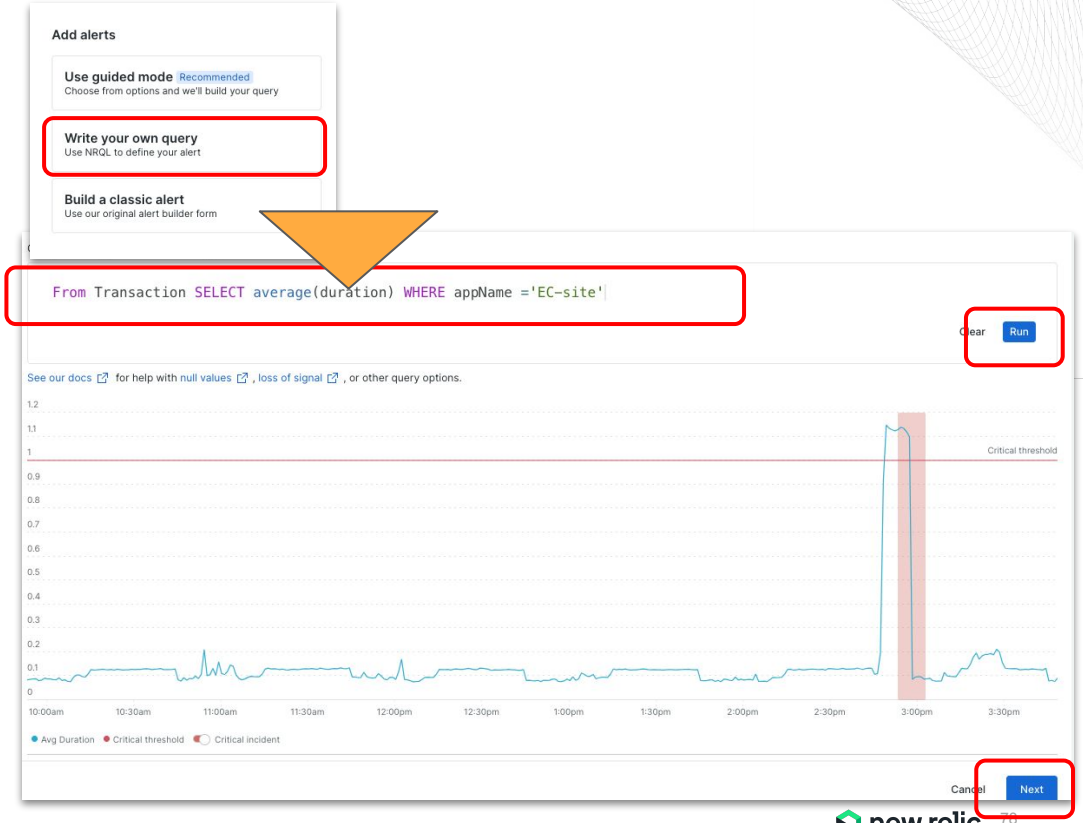
new relic

ハンズオン(2-1) Alert Conditionを作成する 17/21

- 右側からスライドして表示される Add alerts画面から「Write your own query」を選択する。
- クエリ入力欄に次の NRQLクエリをコピー＆ペーストして、Runをクリックします。

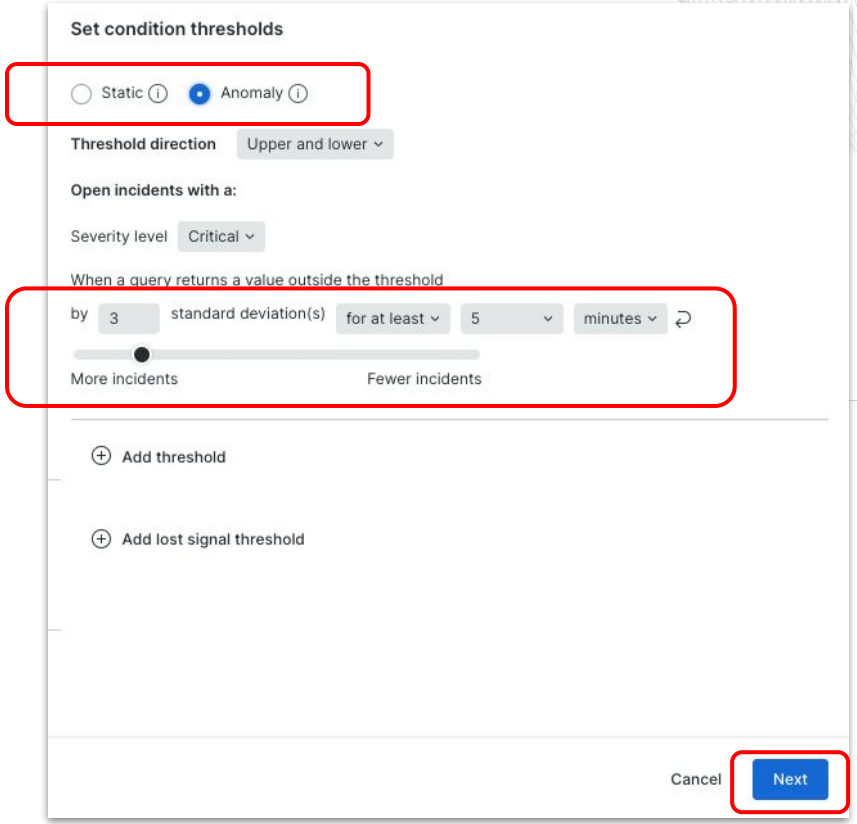
  From Transaction SELECT average(duration) WHERE appName ='EC-site'

- クエリ実行後、直近の状態を示す参考チャートが表示されることを確認し、Nextをクリックする。



ハンズオン(2-1) Alert Conditionを作成する 18/21

- Set condition thresholdsの閾値のタイプをStaticからAnomalyに変更する。
- これまでの手順同様「Save condition」で保存する。
  - もし時間の余裕がある場合、「XXX standard deviation(s)」のXXXの値を変えることで、上部のチャートがどのように表示を変えるかを確認してください。



ハンズオン(2-1) Alert Conditionを作成する 19/21

- **新規Alert Conditionの追加**

④外形監視:チェックエラー

1. **Categories**
   a. NRQL
2. **Define your signal > Query the data you want to monitor**

```
FROM SyntheticCheck SELECT filter(count(*), WHERE result = 'FAILED')
WHERE monitorName ='NRU304-Synthetic Check'
```

Condition名は適切なものを各自設定してください

（例：NRU304-yourname-synthetics-check）

具体的な手順は後続のスライドからご確認下さい。

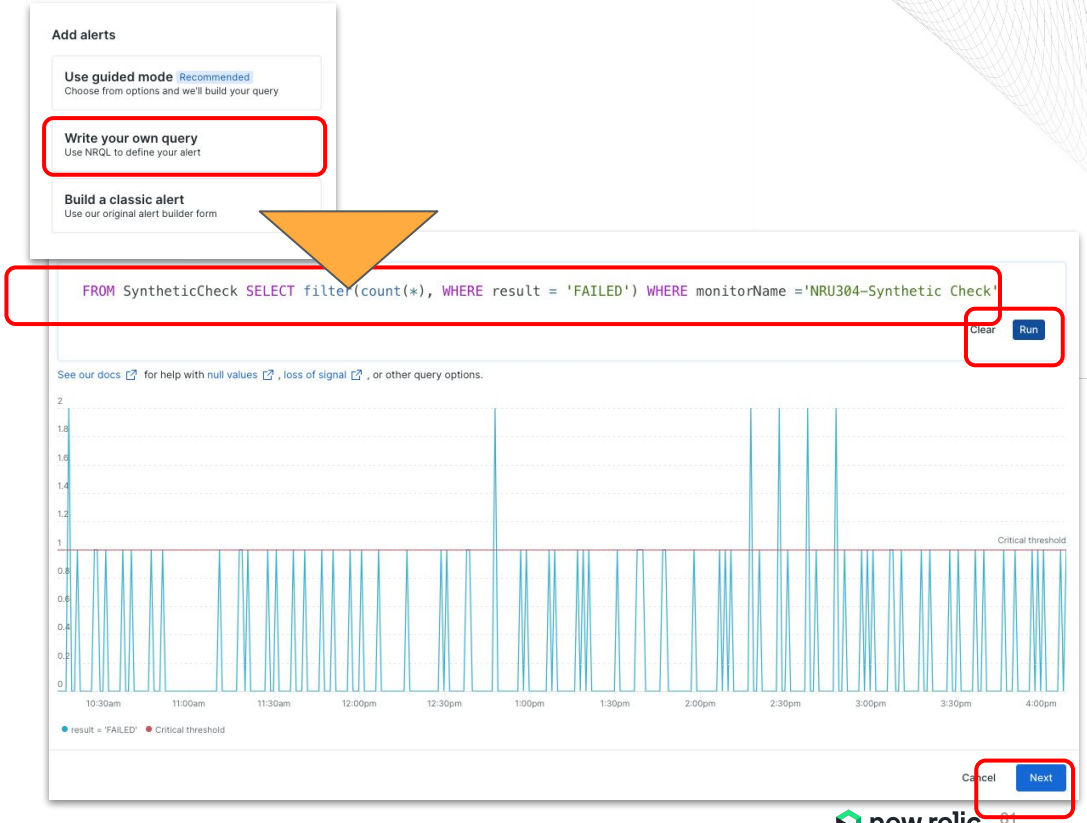
new relic

ハンズオン(2-1) Alert Conditionを作成する 20/21

- 右側からスライドして表示される Add alerts画面から「Write your own query」を選択する。
- クエリ入力欄に次の NRQLクエリをコピー＆ペーストして、Runをクリックします。

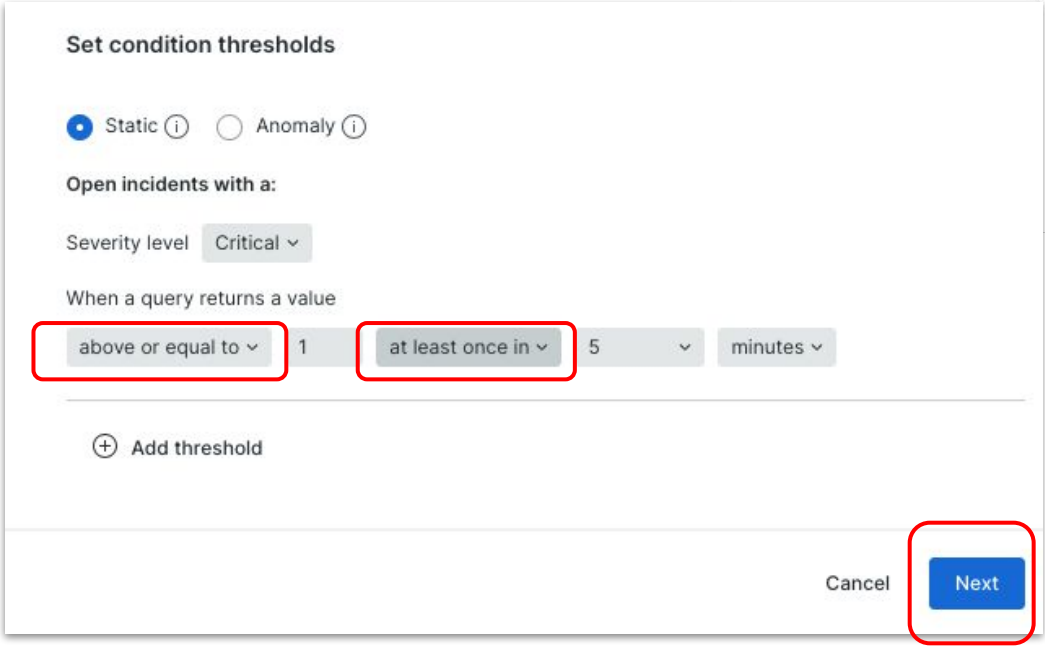
  FROM SyntheticCheck SELECT filter(count(*), WHERE result = 'FAILED') WHERE monitorName ='NRU304-Synthetic Check'

- クエリ実行後、直近の状態を示す参考チャートが表示されることを確認し、Nextをクリックする。



ハンズオン(2-1) Alert Conditionを作成する 21/21

- Set condition thresholdsの閾値条件を変更する。
  - 右側のサンプルを参考にして変更する。
    - Above or equal toの適用
    - At least once inの適用
- これまでの手順同様「Save condition」で保存する。



参考：該当しない状態を「0」として扱いたい場合

アラート条件の評価が行われるのは、クエリのWhere句に該当する値が発生した場合です。
そのためWhere句で絞り込んだ結果が0件の場合はデータなし（NULL）扱いとなりアラート条件として評価されません。
例えば全てのresultが'SUCCESS'だった場合、以下のクエリでは「該当データなし」となります。アラートとして通知できますが、復旧判定ができず状況によっては適切に通知できない場合があります。

```
FROM SyntheticCheck SELECT count(*)
WHERE result = 'FAILED' AND monitorName ='NRU304-Synthetic Check'
```

その場合**filter**関数の中で絞り込むことで評価対象にすることができます

```
FROM SyntheticCheck SELECT filter(count(*), WHERE result = 'FAILED')
WHERE monitorName ='NRU304-Synthetic Check'
```

参考：Example: null value returned (有用なブログ情報：こちらとこちら)

new relic

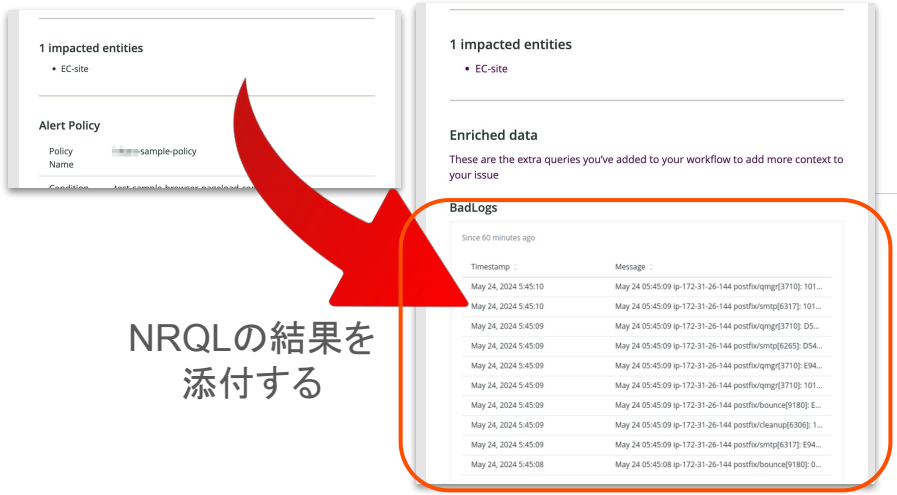
ハンズオン(Optional#1) Enrichmentを試す 1/3

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Enrichmentの設定が**通知内容にどう変更があるかを確認**　します。

こちらのスライドで簡単に紹介したEnrichの機能を試してみましょう

Enrichmentとは:

- Workflow内で任意のNRQLを設定することで、そのクエリ結果を補足情報として通知内容に含めることができます (より詳細は、下部のドキュメント[1]をご確認ください)
- メール通知やSLACK通知では、NRQLのクエリ結果が画像としてが添付されます



参考:
ドキュメント[1] Enrichment機能の概要
ドキュメント[2] アラート対象エンティティの絞り込み

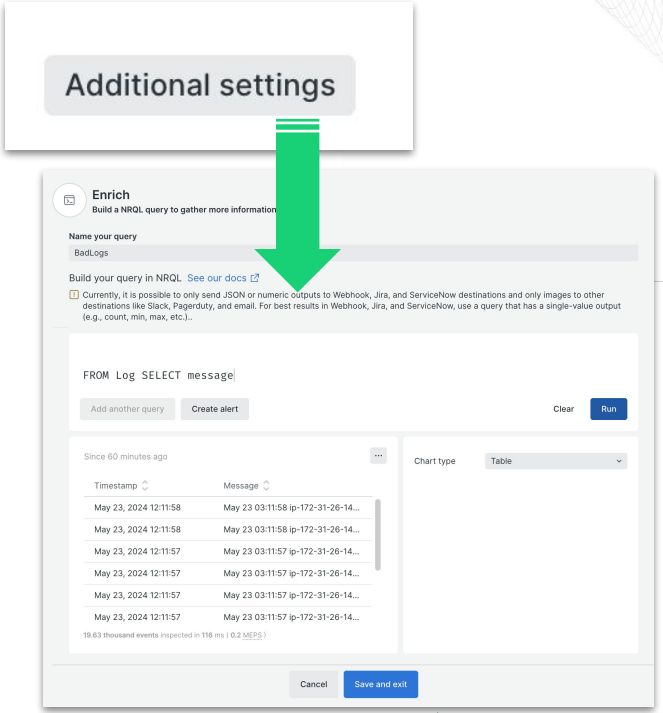
具体的な手順は後続のスライドからご確認下さい。

new relic

ハンズオン(Optional#1) Enrichmentを試す 2/3

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Enrichmentの設定が**通知内容にどう変更があるかを確認**　します。

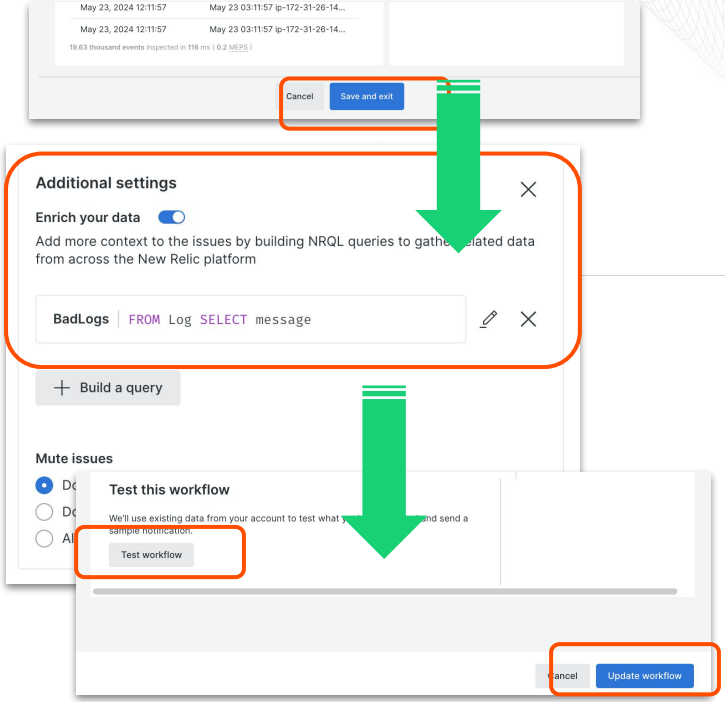
1. Alerts > Workflowsにアクセスし、ハンズオンで利用しているWorkflow設定を開きます
2. Workflow設定内の**Additional settings**ボタンをクリックし、**Enrich your data**トグルを有効化します
3. 有効化すると右側から設定 UIがスライド表示されるので、**Name your query**にEnrichment名を指定し、下部にNRQLを設定します
   a. サンプルNRQL: **FROM Log SELECT message**
   b. Runボタンを押して、設定したNRQLの挙動をテストします



ハンズオン(Optional#1) Enrichmentを試す 3/3

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Enrichmentの設定が**通知内容にどう変更があるかを確認**　します。

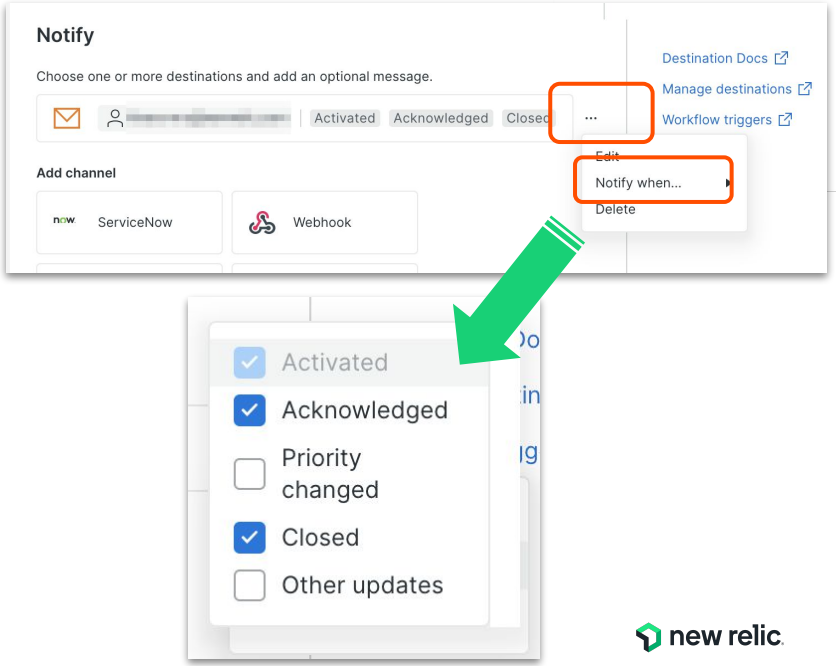
4. **Save and exit**ボタンをクリックし、設定を保存します
5. Workflow設定のUI内にある**Test workflow**ボタンからテスト通知を行います
   a. 補足: テスト用の通知は過去に発生したアラートを基にして発報します。過去に発生したアラートがないような新規の設定の場合、テスト用アラート発報を行わないケースがあります
6. テスト後、**Update workflow**ボタンをクリックし、Enrichmentの設定を保存します



ハンズオン(Optional#2) Notify Whenを試す

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Notify Whenの設定が**通知内容にどう変更があるかを確認**　します。

1. Alerts > Workflowsにアクセスし、ハンズオンで利用しているWorkflow設定を開きます
2. Workflow設定のNotifyセクション内で設定している通知項目の**[...]**をクリックし、ポップアップメニューから**Notify when...**を選択する
3. 任意の箇所にチェックを入れたり、外します
4. Workflowの設定UIに戻り**Update workflow**ボタンを押し、設定を更新する
5. 実際にアラートが発生した際に通知される内容に変化があるかを確認する

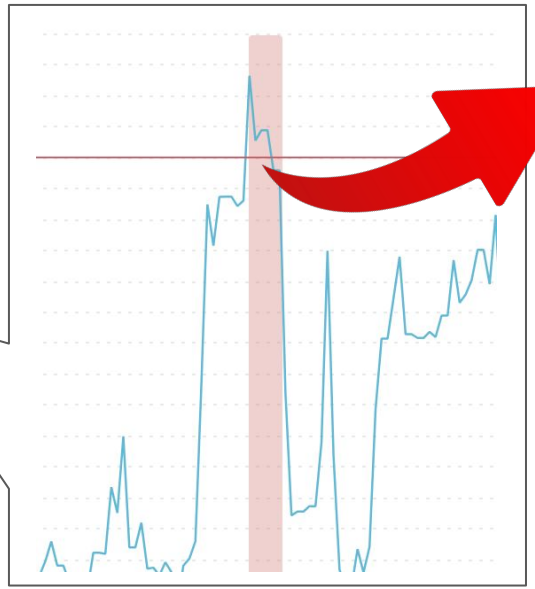


new relic

補足: APIを活用してアラートテストを行う

New Relicが提供しているAPIを用いることで、仮想的にアラートを発報させるデータを生成することができます。(NRU302でもEvent APIの活用をオプションのハンズオンとして体験可能です)

Event API
スクリプトやツールで
繰り返し実行



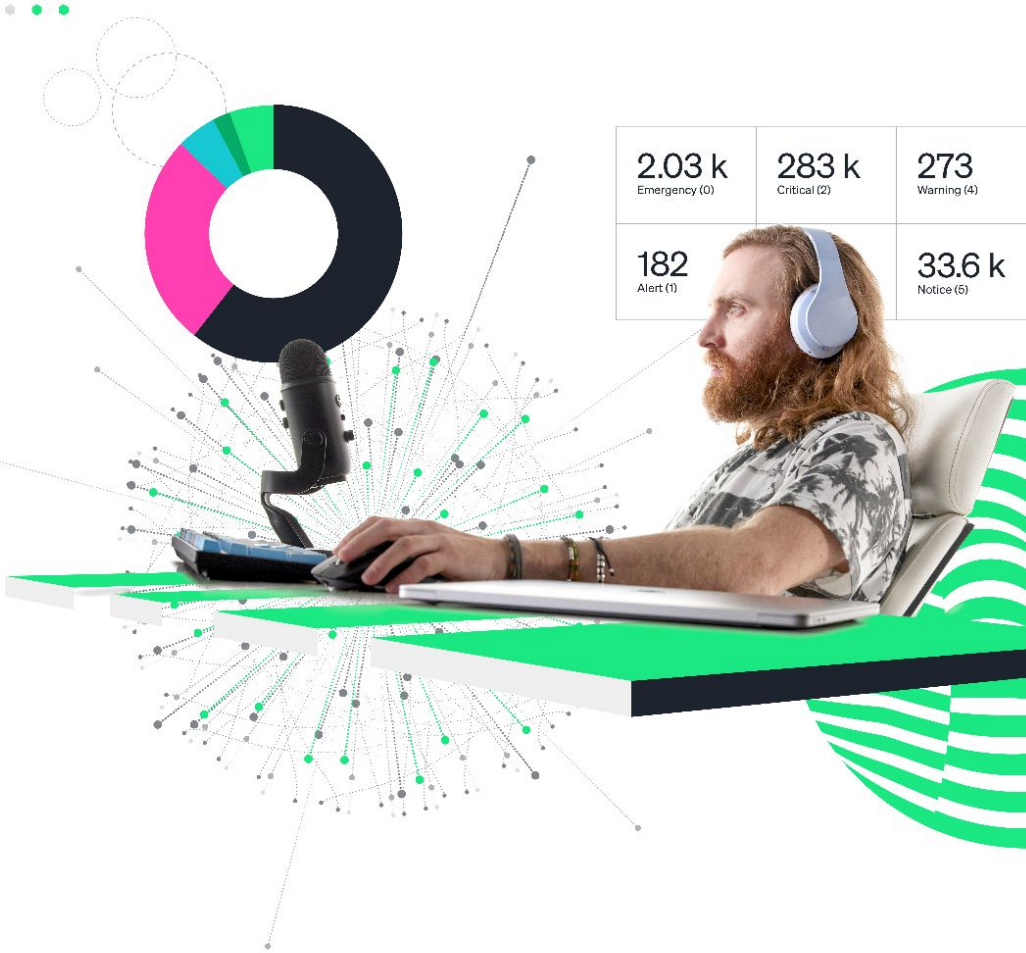
参考: Event APIを使用したカスタムイベントの送信 (有用なブログ情報: こちら)

new relic

new relic

ハンズオン(3)
発生したアラートの確認

16:35 - 16:45 (10min)

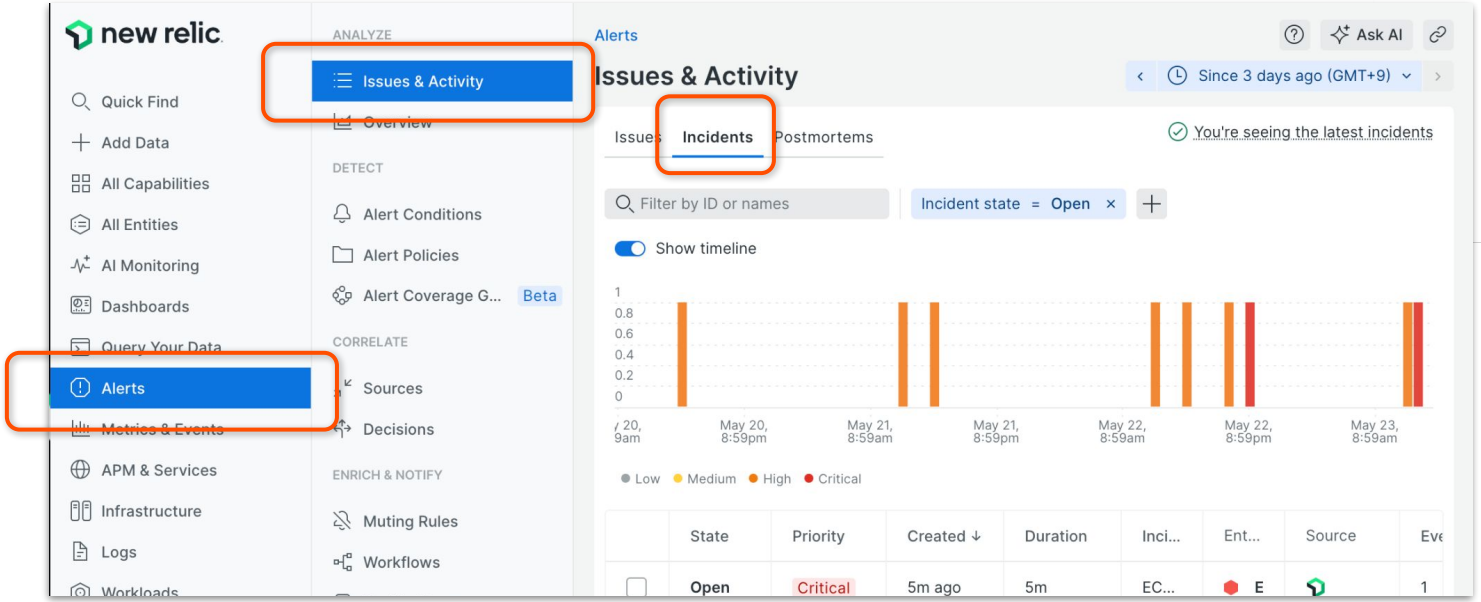



@brian is this the problem?
@suni yup. just pushed a fix!
Data for Engineers_
traceID.mod

手順・解説

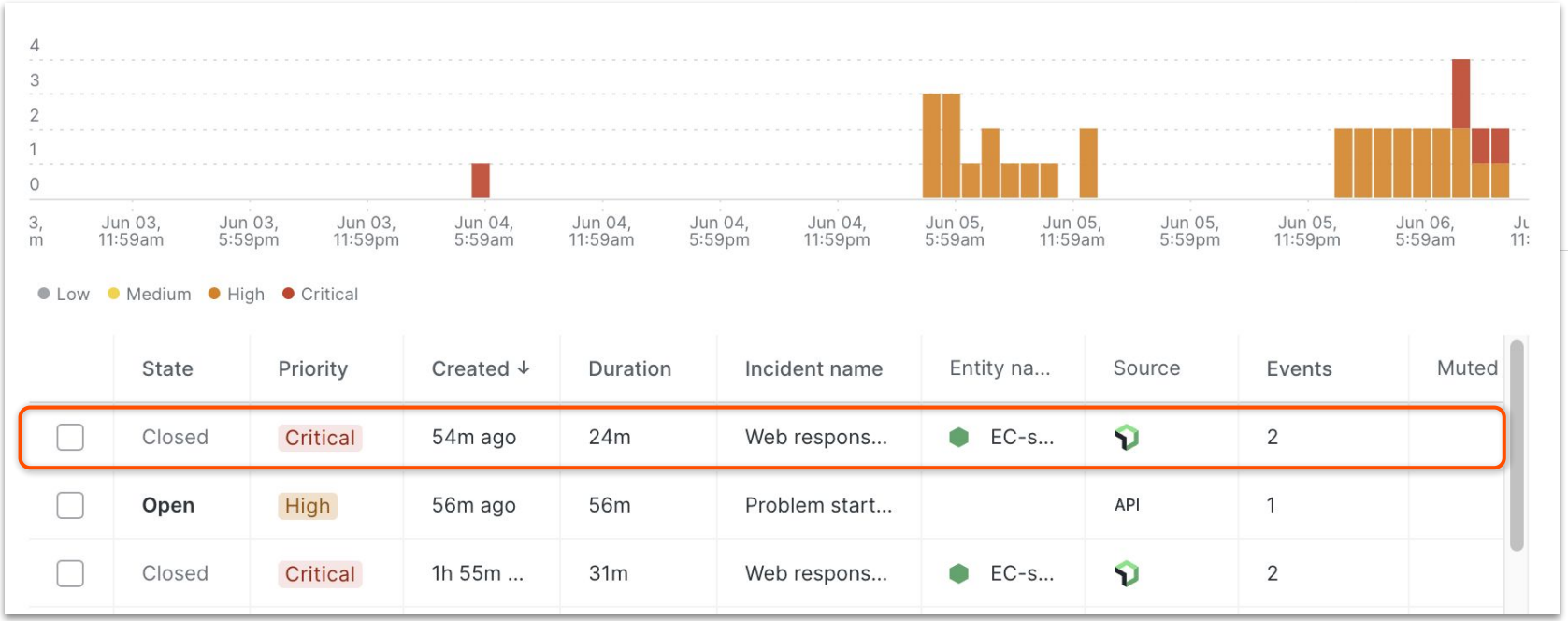
ハンズオン(3-1) 個々のアラートを確認する 1/3

- [Alerts] > [Issues & Activity] > [Incidents]タブをクリックします。



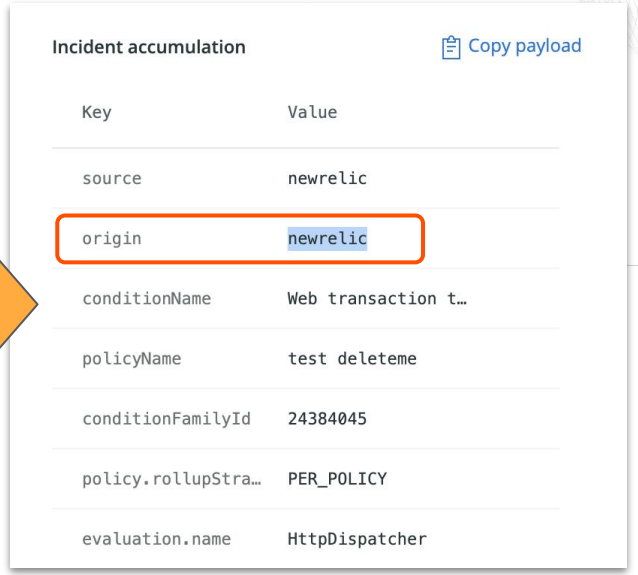
ハンズオン(3-1) 個々のアラートを確認する 2/3

- Incidentをクリックします。



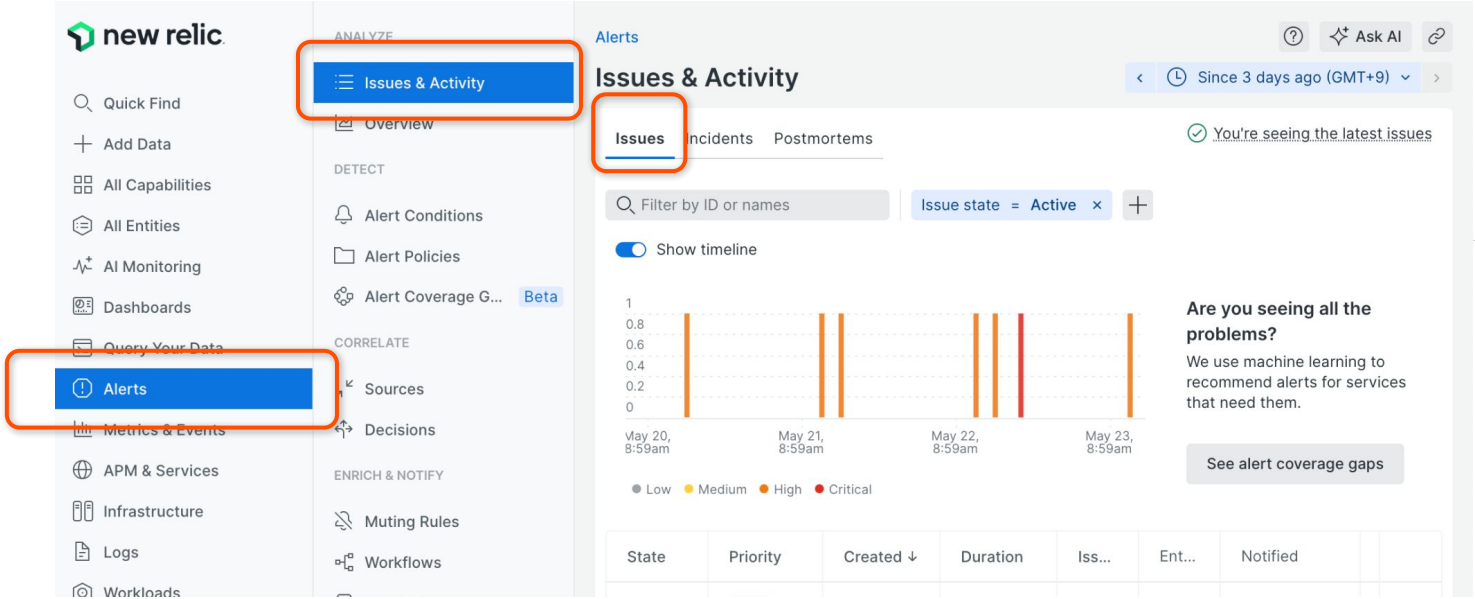
ハンズオン(3-1) 個々のアラートを確認する 3/3

- Origin Key の値を確認することで、どのツールによって判定されたアラートかを確認することができます。



ハンズオン(3-2) 複数のアラートを紐付けトラブルシューティングに役立てる 1/5

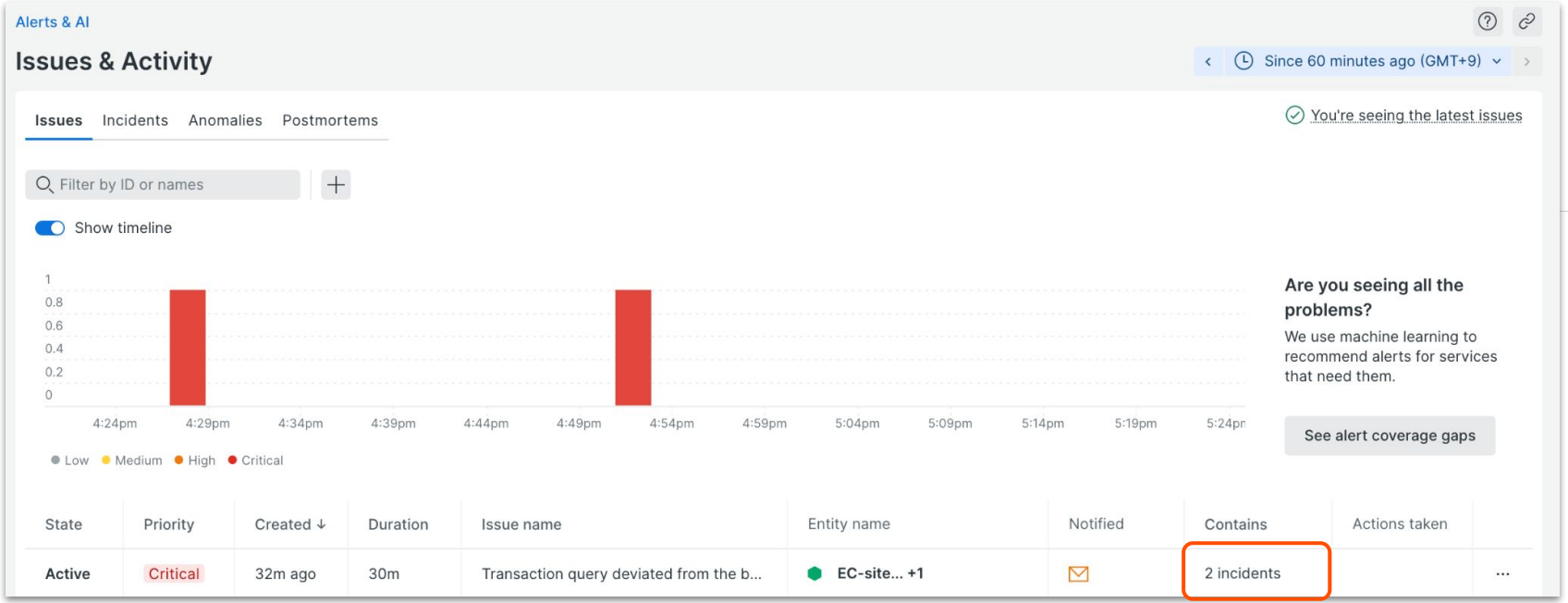
- [Alerts] > [Issues & Activity] > [Issues]タブをクリックします。



new relic

ハンズオン(3-2) 複数のアラートを紐付け トラブルシューティングに役立てる 2/5

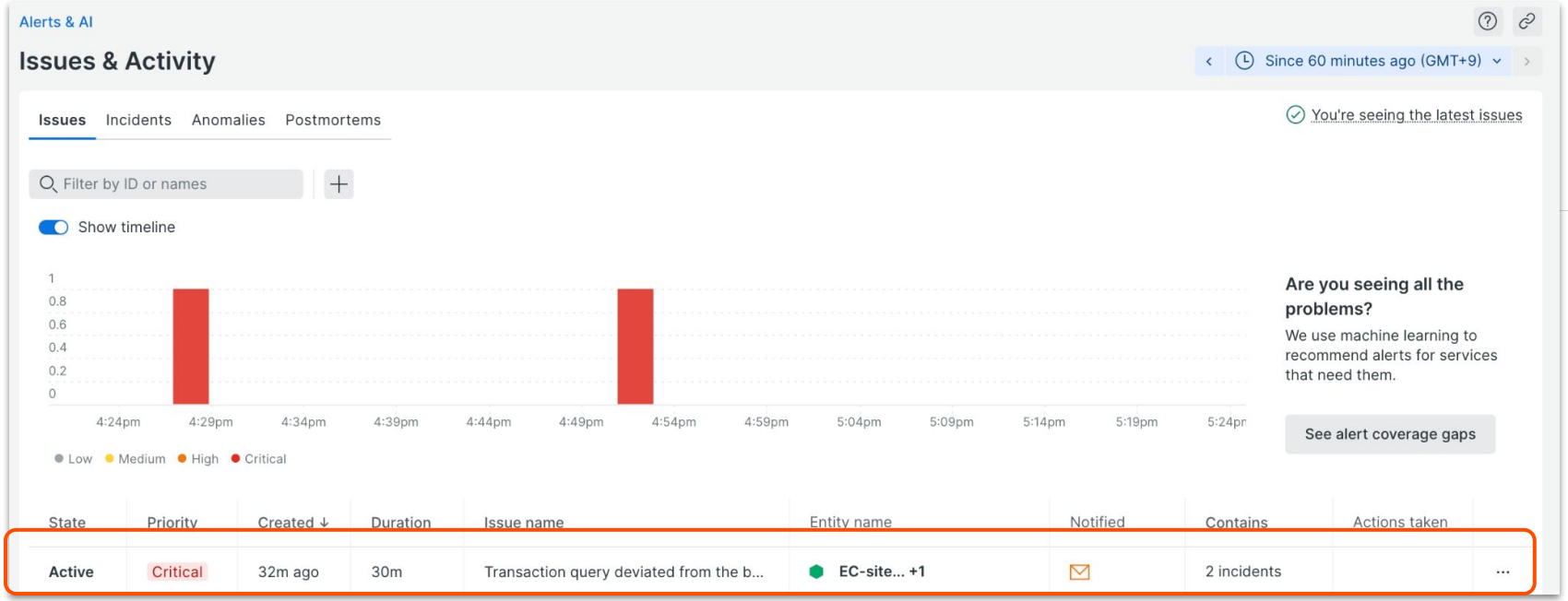
- Issues ではユーザーが設定した AlertやAnomaly、API連携などの複数のアラートの中で関連しそうなものをまとめて取り扱います。



new relic

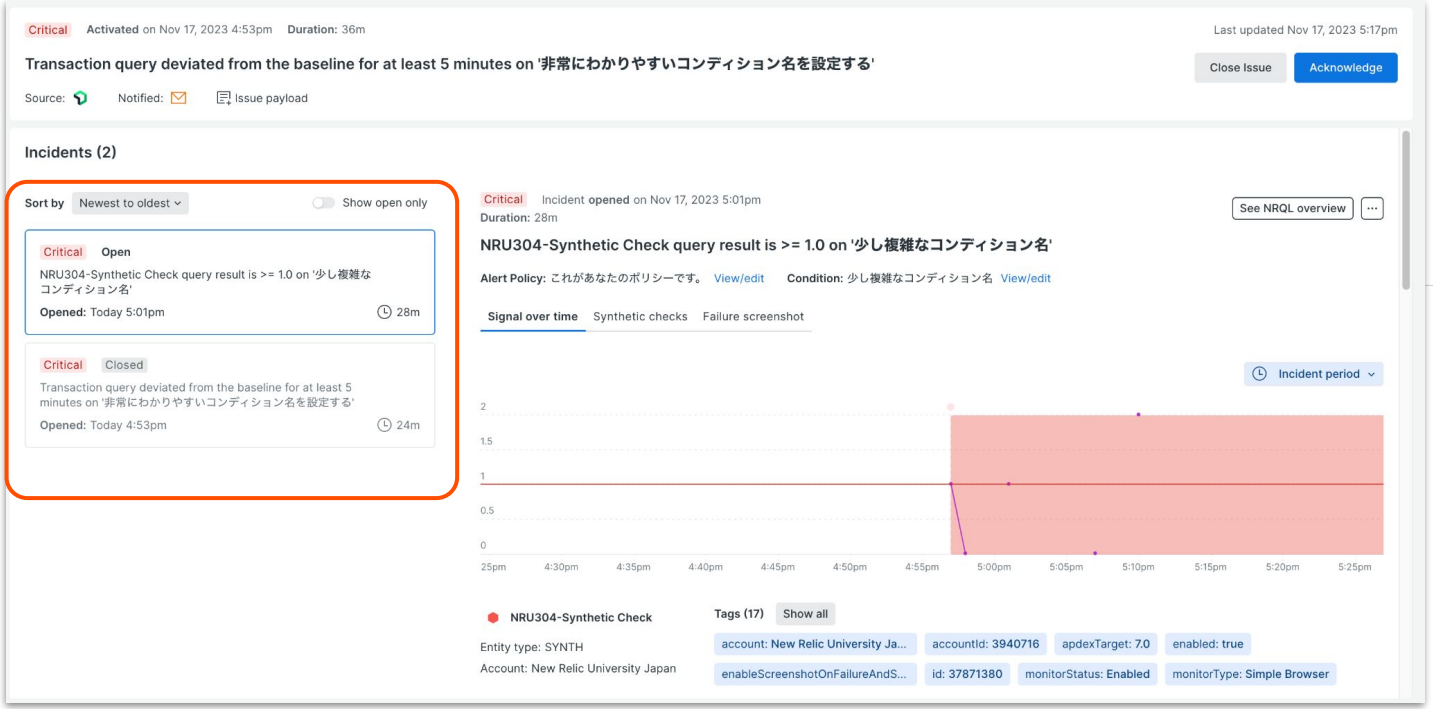
ハンズオン(3-2) 複数のアラートを紐付けトラブルシューティングに役立てる 3/5

- Issueをクリックすると詳細が表示されます。



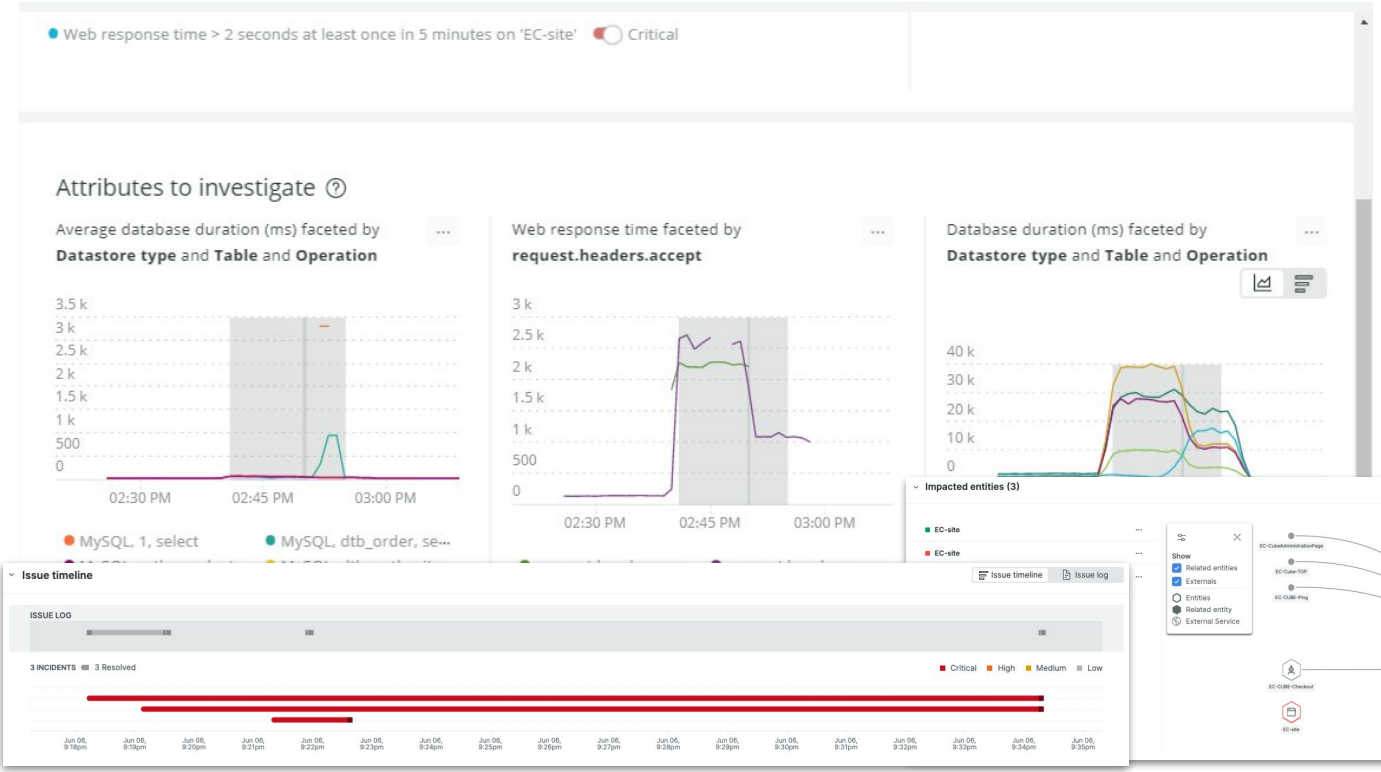
ハンズオン(3-2) 複数のアラートを紐付けトラブルシューティングに役立てる 4/5

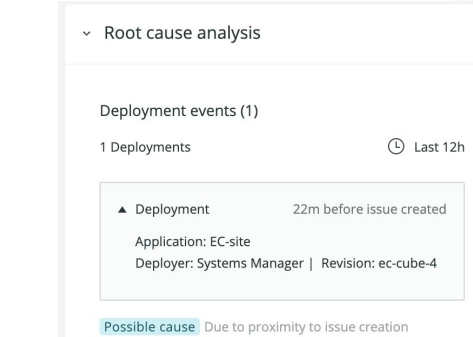
- どのIncidentがまとめられているのか確認することができます



ハンズオン(3-2) 複数のアラートを紐付け トラブルシューティングに役立てる 5/5

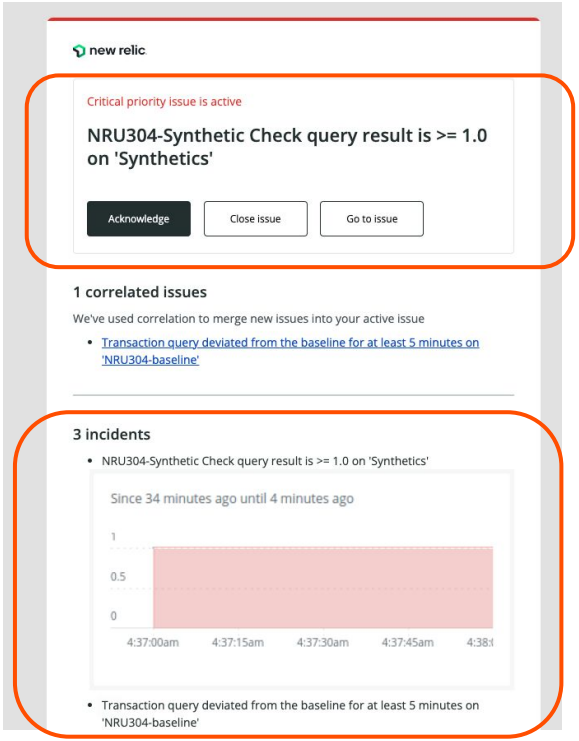
- Issue timelineや関連するEntity情報、デプロイ履歴など、原因分析に役立つ情報が表示されます





ハンズオン(3-3) 届いたメール通知を確認する

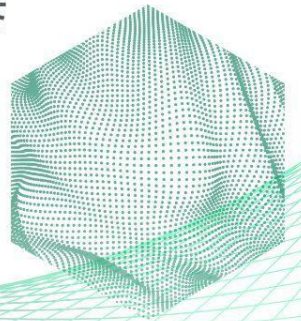
- 通知されたEmailからIssue の詳細など、確認に役立つ情報が表示されます



new relic

座学(4)
New Relicのアラート分析支援機能

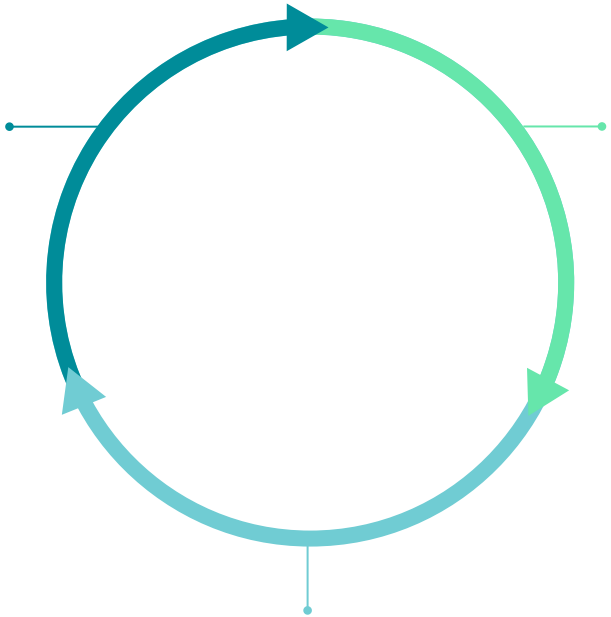
16:45 - 16:55 (10min)



New Relic によるインシデント対応フロー

検知

潜在的な問題が実際の障害になる前に気づく
(“気づける”状態にする)



診断

問題を理解し、根本原因にたどり着く
(”理解できる”状態にする)

対処

障害を解消するための行動を起こす

new relic

検知1: 重要な指標に対するアラートによる気づき

検知

アラート通知

傾向分析
(可視化)

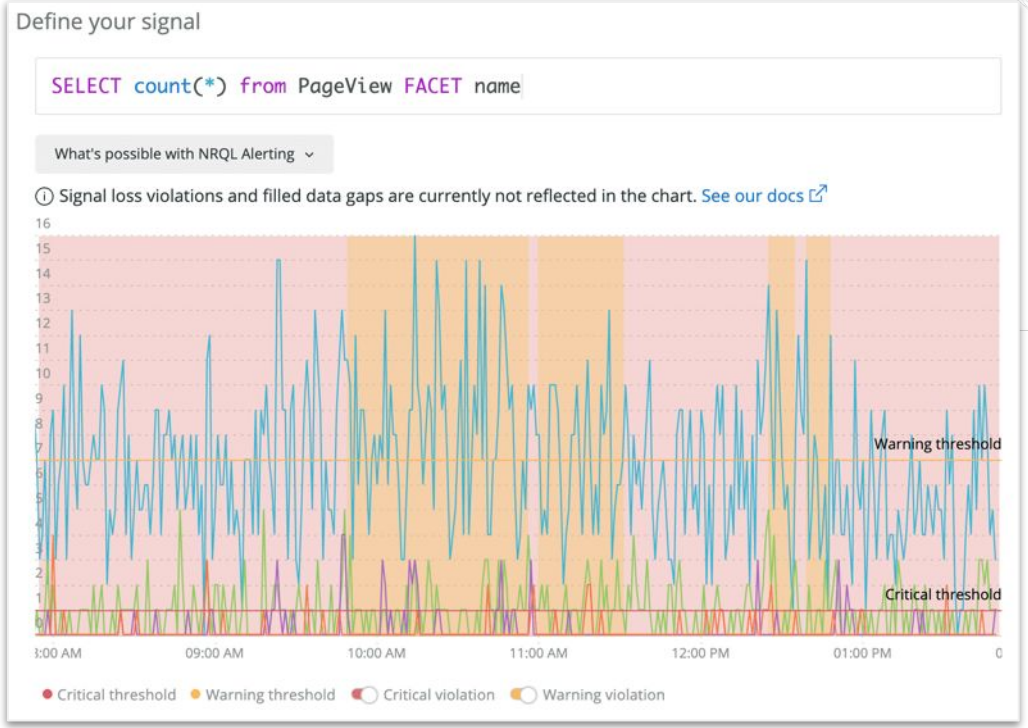
診断

イベントの相関分析

根本原因分析

対処

(外部ITSMツール: Servicenow, Pagerduty等)



new relic

検知2: Lookoutによる傾向の可視化と探索

検知

アラート通知

傾向分析（可視化）

↓

診断

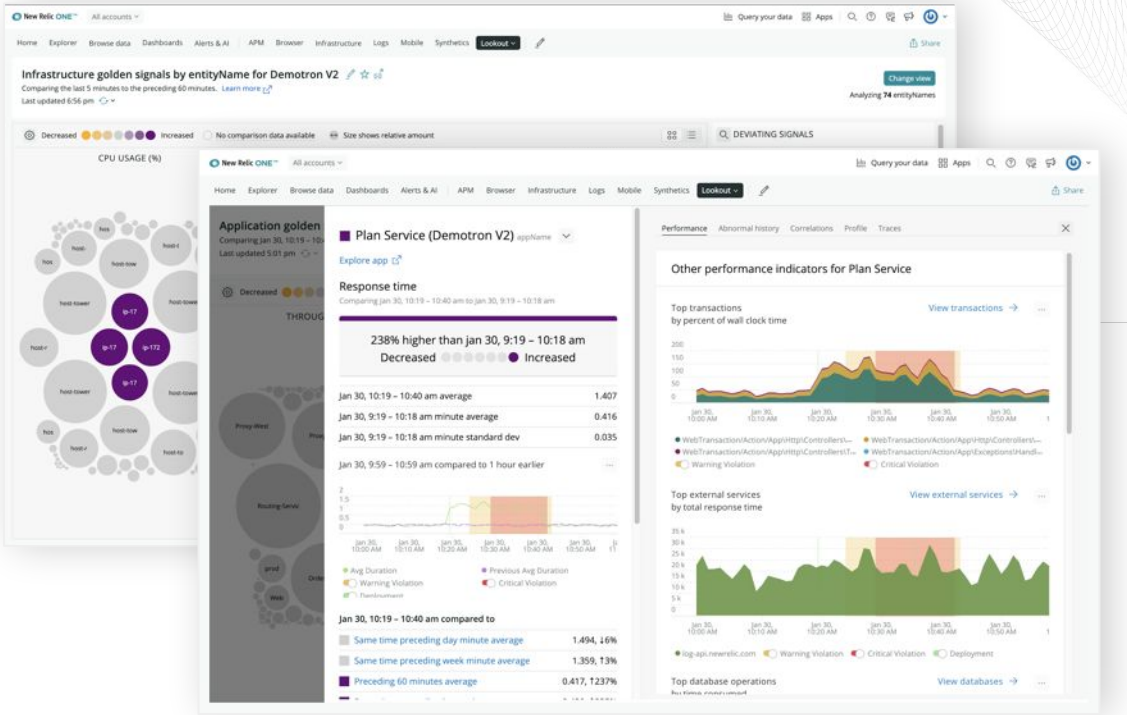
イベントの相関分析

根本原因分析

↓

対処

(外部ITSMツール: Servicenow, Pagerduty等)



new relic

診断1: Correlationによるアラート統合とノイズの削減

検知

アラート通知

傾向分析
(可視化)

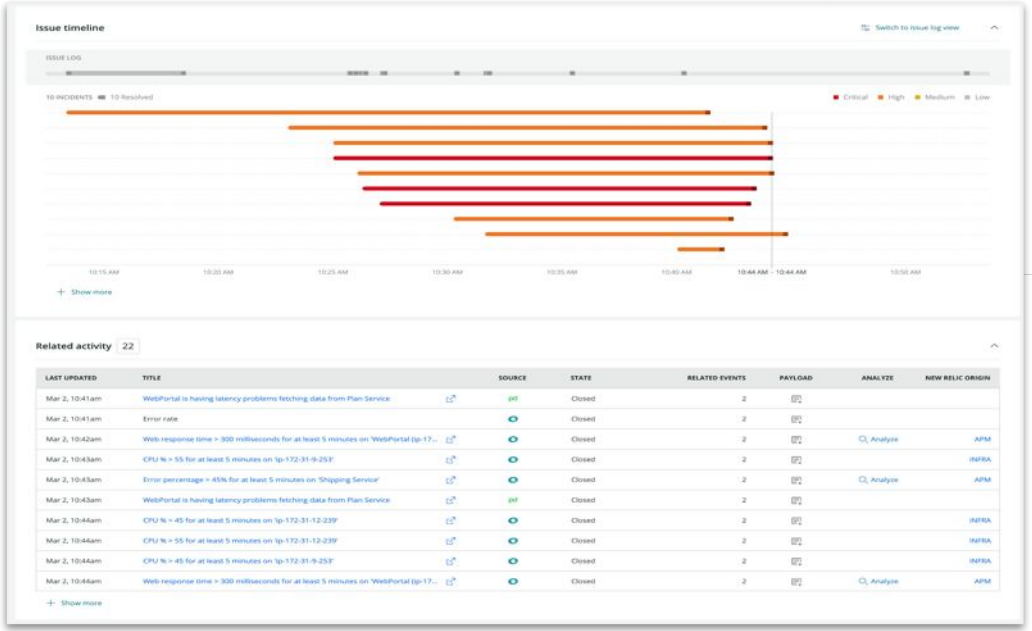
診断

イベントの相関分析

根本原因分析

対処

(外部ITSMツール: Servicenow, Pagerduty等)



new relic

診断2: Correlationによる根本原因の示唆

検知

アラート通知

傾向分析
(可視化)

↓

診断

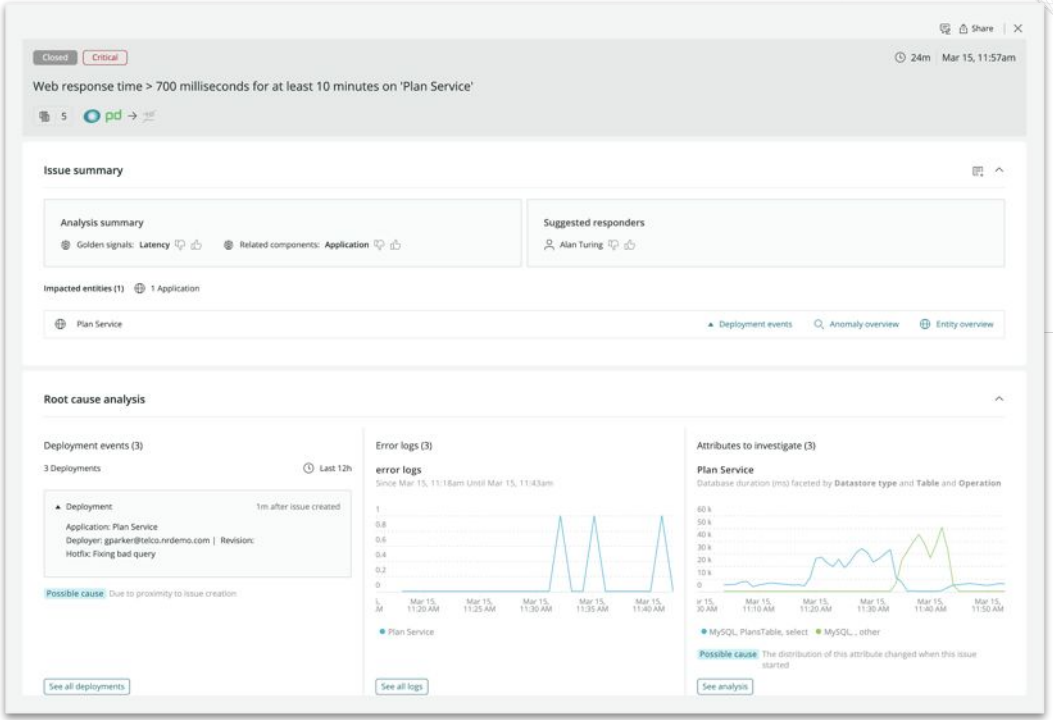
イベントの相関分析

根本原因分析

↓

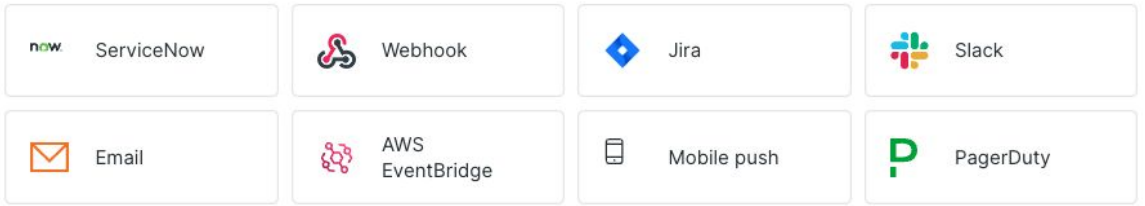
対処

(外部ITSMツール: Servicenow, Pagerduty等)



new relic

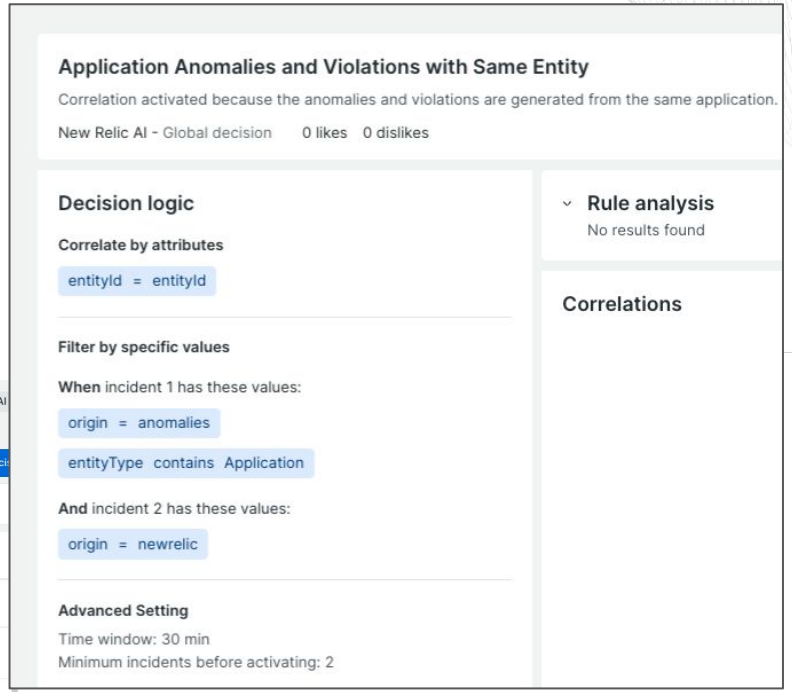
対処: 様々なツールと連携しアクションを実行

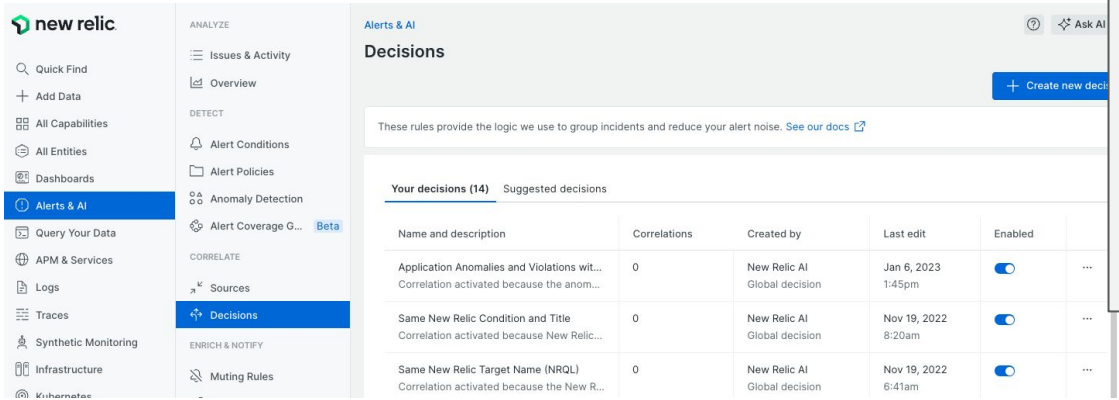


機能紹介: Correlate (Decisions)

Alerts → Decisions

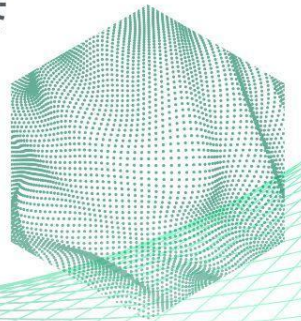
- Incidentの構造を分析して、関連性の高いものを一つのIssueにまとめる
（対象エンティティ、Incidentデータ構造の一致度）
- 相関関係を持たせる基準はプリセットが用意されているほか、独自に設定可





new relic

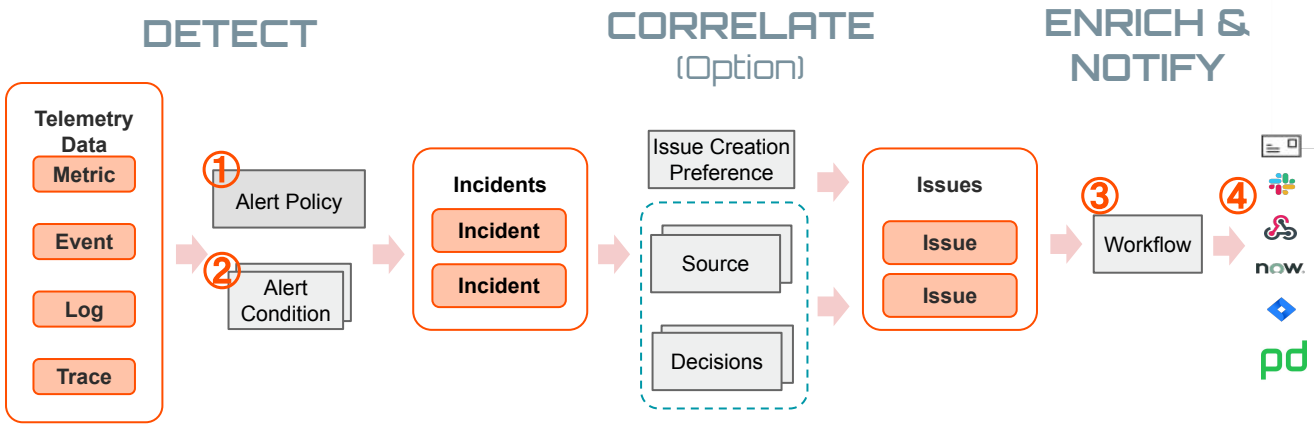
まとめ



new relic

まとめ

- ユーザー体験に近い指標でアラートを設定しよう
  - インフラ監視だけではサービスの異常に気付くには不十分
- New Relicのアラート構造と設定方法を理解しよう



- New Relicのアラート機能を活用して、アラート分析を効率化しましょう

new relic

アラート関連の情報

- アラート条件を正しく設定するための詳細ガイド
  - https://newrelic.com/jp/blog/how-to-relic/understand-nrql-alert-condition
- アラート通知にログメッセージを記載する
  - https://newrelic.com/jp/blog/best-practices/notification-with-log-message
- New Relicアラートで0判定するにはfilter関数を使おう
  - https://newrelic.com/jp/blog/best-practices/use-filer-fuction-if-you-want-to-detect-0-alert

New Relic 公式ドキュメント

https://docs.newrelic.com/jp/

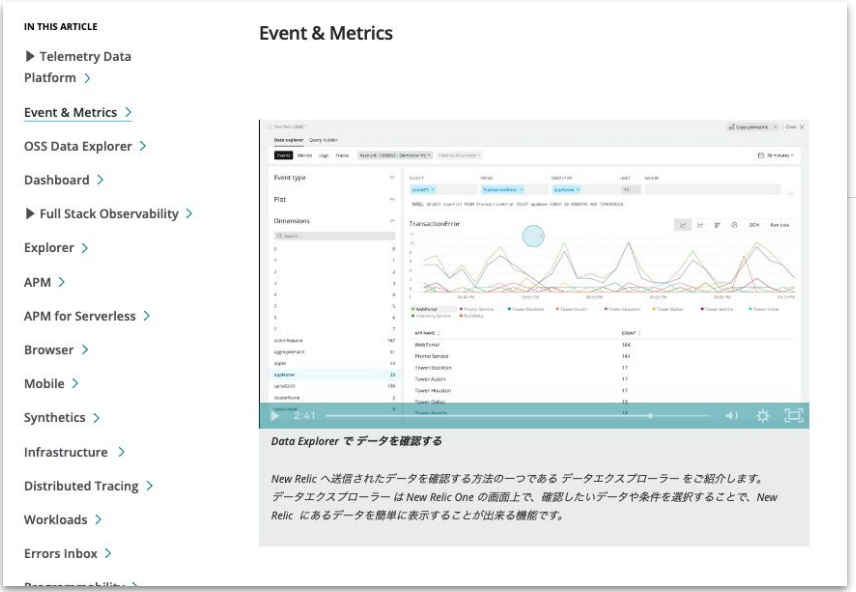
New Relicを活用するための様々な情報を確認できるドキュメントとなります

new relic

New Relic University

https://newrelic.com/jp/learn

New Relicについて基本から応用まで学べるコンテンツです



new relic

New Relic University (詳細)

New Relicの基礎から応用までを学べ、認定資格も取得できるセルフラーニングコンテンツです

Install

New Relic を使い始める

New Relic One へのサインアップやエージェントインストールの方法などのガイドを提供

APM / Browser / Infrastructure / Logs / Mobile (iOS/Android) / AWS統合 / Azure統合 / GCP統合 インストール手順

▸サインアップ方法
https://newrelic.com/jp/blog/how-to-relic/create-new-account

▸インストールガイド
https://newrelic.com/jp/blog/how-to-relic/new-relic-faststep-guide

NRU 100

Observability/New Relic を知る

New Relic One やオブザーバビリティに関する基礎知識を座学にて学習

NRU Practitioner オブザーバビリティ入門

NRU 101 New Relic One 入門

NRU 200

New Relic の主要機能を学ぶ

New Relic One に含まれる3つの主要機能に含まれる4の機能群を動画で説明

NRU201 Telemetry Data Platform

NRU202 Full Stack Observability

NRU203 Applied Intelligence

NRU 300/400

New Relic の使い方を体感する

New Relic One を実際に操作し、主要機能を利用できる状態にするためのトレーニング

NRU 301 アプリケーションとインフラ性能観測の基本

NRU 302 ダッシュボード開発とNRQLの基本

NRU 303 SLI/SLO設計の基本

NRU 304 AIOps とアラート設計の基本

NRU 401 CodeStream による DevOps を想定したエラー分析対応の基本

Exam

資格を得る

New Relicの知識を有していることを証明するための試験、合格すると資格バッジを授与

フルスタックオブザーバビリティ認定試験

Observabilityのスペシャリストを目指せ！
Full Stack Observability Practitioner認定試験

【この認定試験を通じて身につくスキル】

- Observabilityの実現のためにNew Relicが取得するデータの理解と、目的に応じたデータ分析やアラート設定
- バックエンドおよびフロントエンドの問題発見とトラブルシューティング

【認定試験に向けた準備】

- New Relicの基本的な操作経験
- ラーニングパスに沿った学習

【合格者特典】

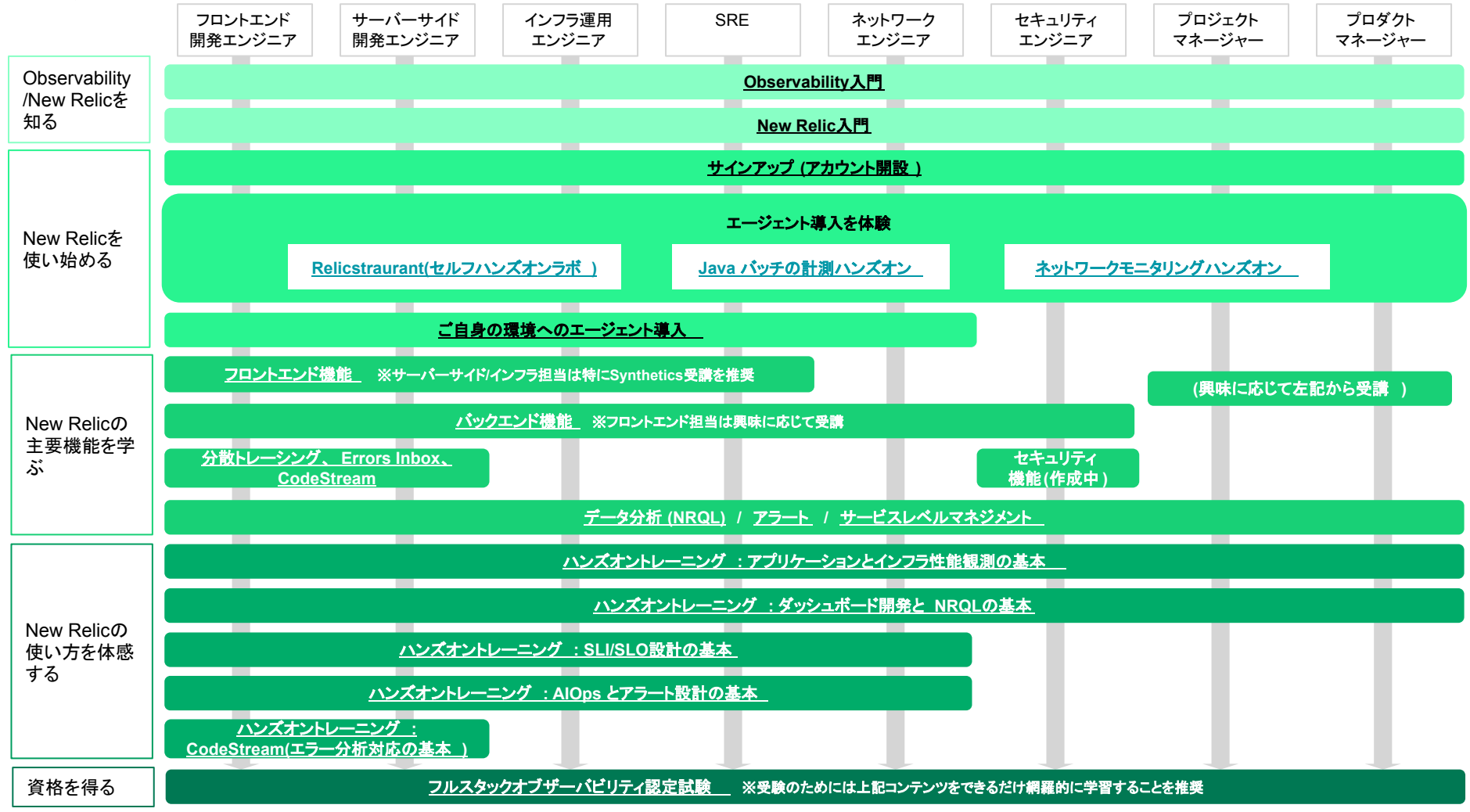
- デジタル認定証とバッジ
- 合格者限定ノベルティの送付
  ⭐**今だけ認定者限定デザイン　Tシャツ！**

認定試験受験サイトは こちら

- **受験料：無料**
- **試験の言語：日本語**
- **受験形態：オンライン（いつでも受験可能）**

new relic

ロール別 New Relic ラーニングパス



お知らせ

New Relic サインアップのご案内

- 全機能が無料で使い放題（1名）！
- 転送データが 100GB/月まで無料！
- 必要事項記入ですぐに利用開始！
- クレジットカード記入不要！
- 利用期限なし！

※ New Relic フリープランで始めるオブザーバビリティ！

サインアップされた方に抽選で
New Relic Tシャツプレゼント！！
🔗 応募フォーム

🔗 newrelic.com/jp/sign-up-japan

new relic

New Relic実践入門 第2版 オブザーバビリティの基礎と実現

発売日：2023年12月11日
価格：3,410円（税込み）

翔泳社、Amazon等から販売中
https://www.shoeisha.co.jp/book/detail/9784798184500

new relic

お知らせ

最新情報のキャッチアップにぜひ活用ください！

X(Twitter)

New Relicに関する情報発信

https://twitter.com/NewRelicJapan

Qiita Organization

やってみた系の記事を公開

https://qiita.com/organizations/newrelic

最新情報はこちら

- What's new
- リリースノート
- 公式ブログ

new relic

お知らせ

New Relic 学習オンラインコンテンツのご案内

「New Relic を使ってアプリケーションを改善しよう」 がオンライン学習サービス Progate Path で公開されました！！

エンジニアの実務に即した体験ができる実践的なコンテンツ になっており、**無料で学習** することができます！！

学習コンテンツは
こちらから

[学べること]

- **New Relic APM / Browser の導入方法**
- **アプリケーションのエラーを特定して修正する流れを理解する**
- **アプリケーションのパフォーマンスのボトルネックを見つけて改善する流れを理解する**

new relic

NRUG
ぬるぐで学ぶ

New Relic User Group

New Relic ユーザーが集い、実践事例や最新機能紹介などを実施。初心者支部や SRE 支部などが形成されており、エンジニア同士でのネットワーキングや信頼性の高い情報交換が可能。

ConnpassのNRUGページより
ご登録ください。

NRUG 本部

new relic

アンケートご協力のお願い

Zoom画面を終了の際にアンケートの画面が表示されます。
是非、**アンケートへのご協力** をお願いいたします。

また、もっと詳しい話を聞きたい方は、
その旨を**アンケートにご記載** ください。

Thank you.

new relic

お疲れさまでした。

Thank you.