new relic

NRU 304
「AIOps とアラート設計の基本」

November 22, 2023

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

原　健一郎

New Relic K.K.

Solutions Consultant

ネットワーク/パフォーマンス/サーバの運用監視にて
エンジニアとしてのキャリアを開始。
得意な技術は、

- **Content Delivery Network**
- **暗号化技術**
- **ID管理**
- **Cloud Security**

new relic

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、**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する

- New Relicの**AIOps機能**を活用して、アラート対応の効率化を実現する方法を知る

本セッションの想定対象者と前提条件

- 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、逆に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
- 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）

Agenda

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
16:00-16:15	座学(3)	アラートコンディションの作成
16:15-16:30	ハンズオン(2)	アラートコンディションを作る
16:30-16:40	ハンズオン(3)	発生したアラートの確認
16:40-16:55	座学(4)	New Relicのアラート分析支援機能とAIOps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

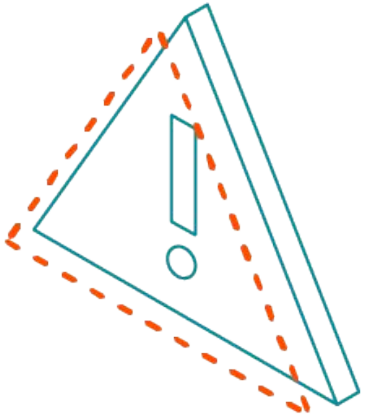
座学(1)
ユーザー視点のアラート

15:00 - 15:15 (15min)

new relic

突然ですが

- どんなアラートを設定していますか？



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ドを設定する

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)

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)

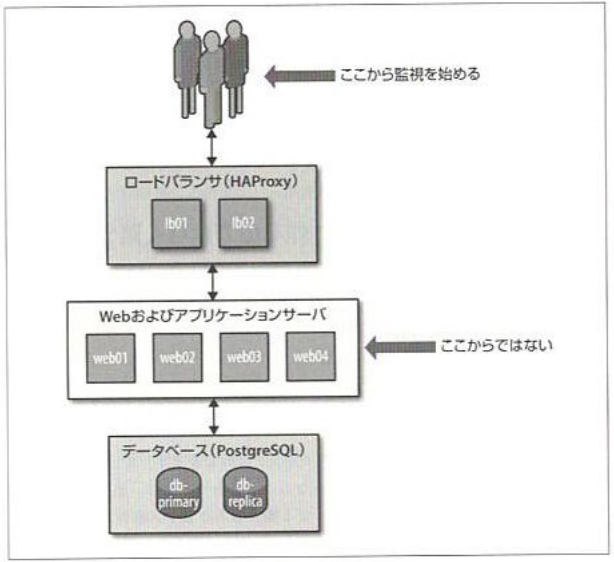
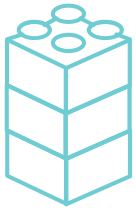


図2-1　できるだけユーザに近いところから監視を始める

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

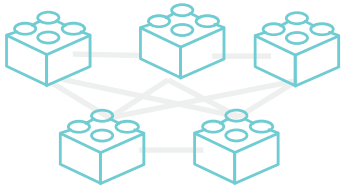


基盤

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



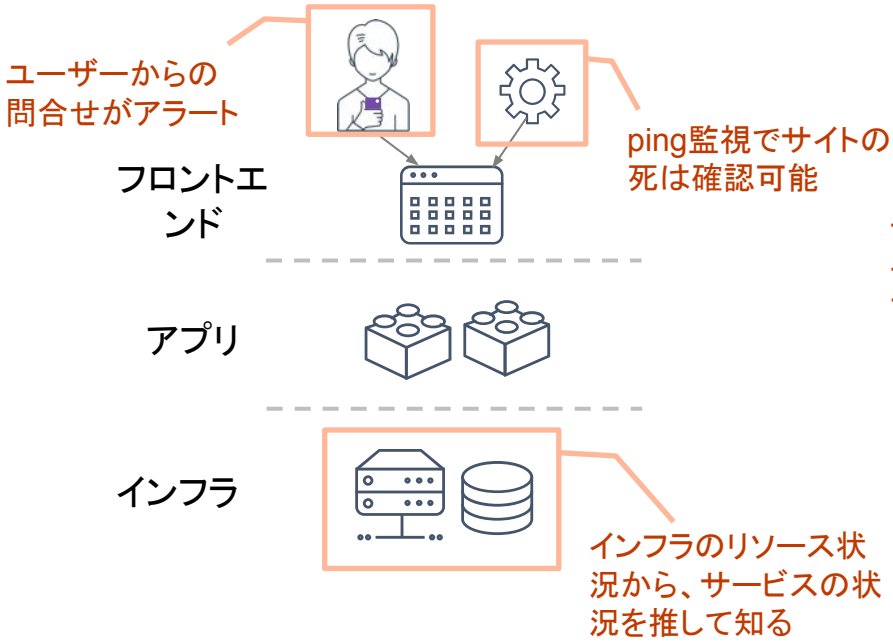
リソース抽象化
(仮想化、コンテナ等)

基盤

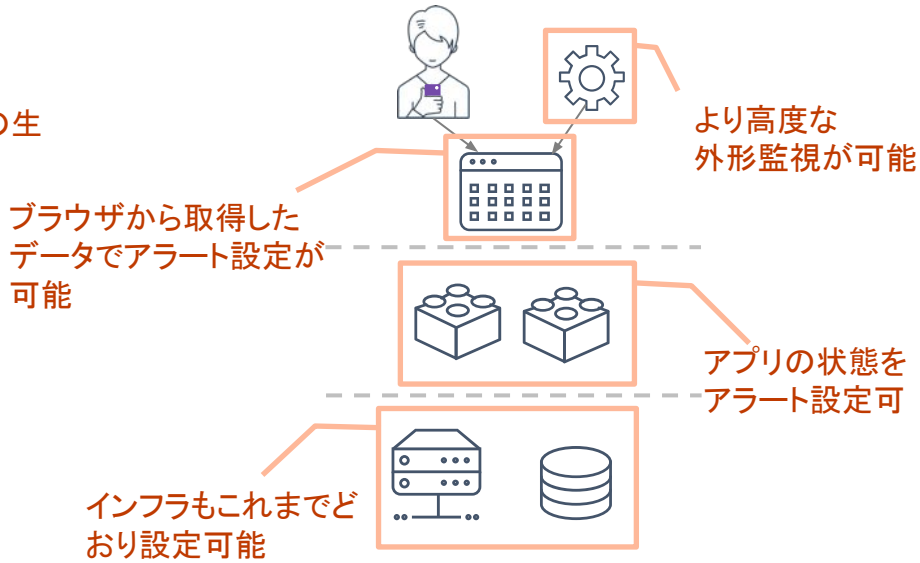
アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

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)



目的別、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	チェック応答時間	チェックエラー		
フロントエンド	CWV	JSエラー		
アプリケーション	Apdex 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

座学(2)
New Relicのアラート機能

15:15 - 15:30 (15min)

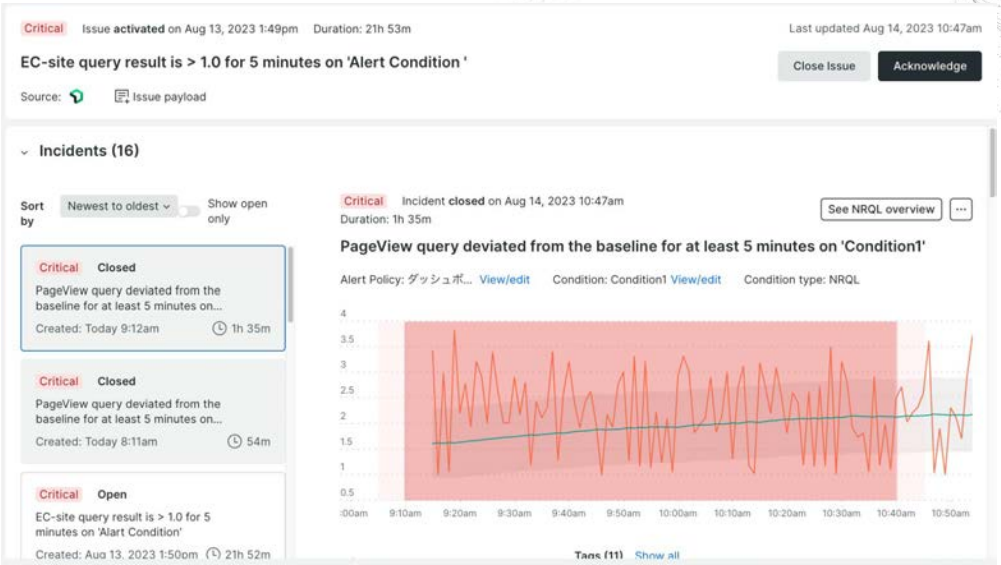
new relic

New Relicのアラート機能

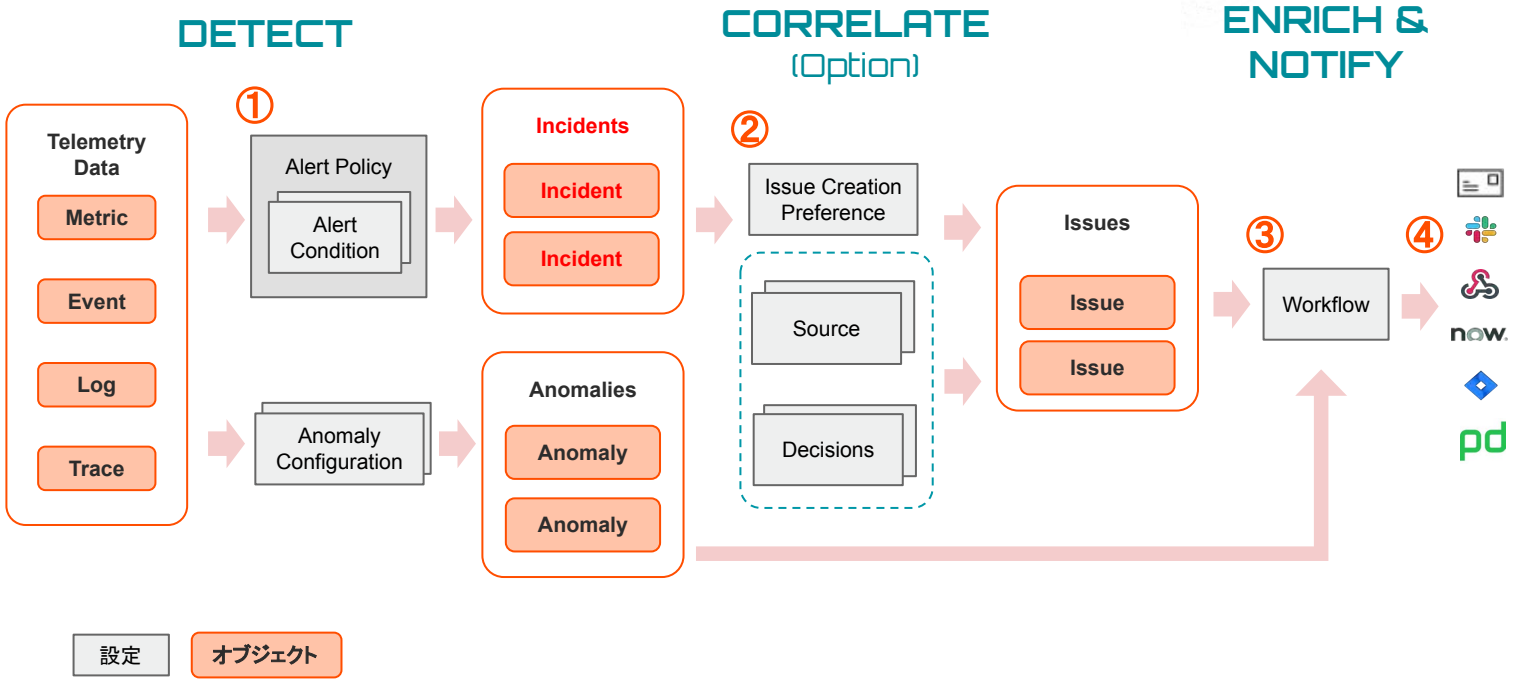
New Relicがリアルタイムに**収集しているデータ**を使って、アラートを設定することが可能

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、通知を受けることができる

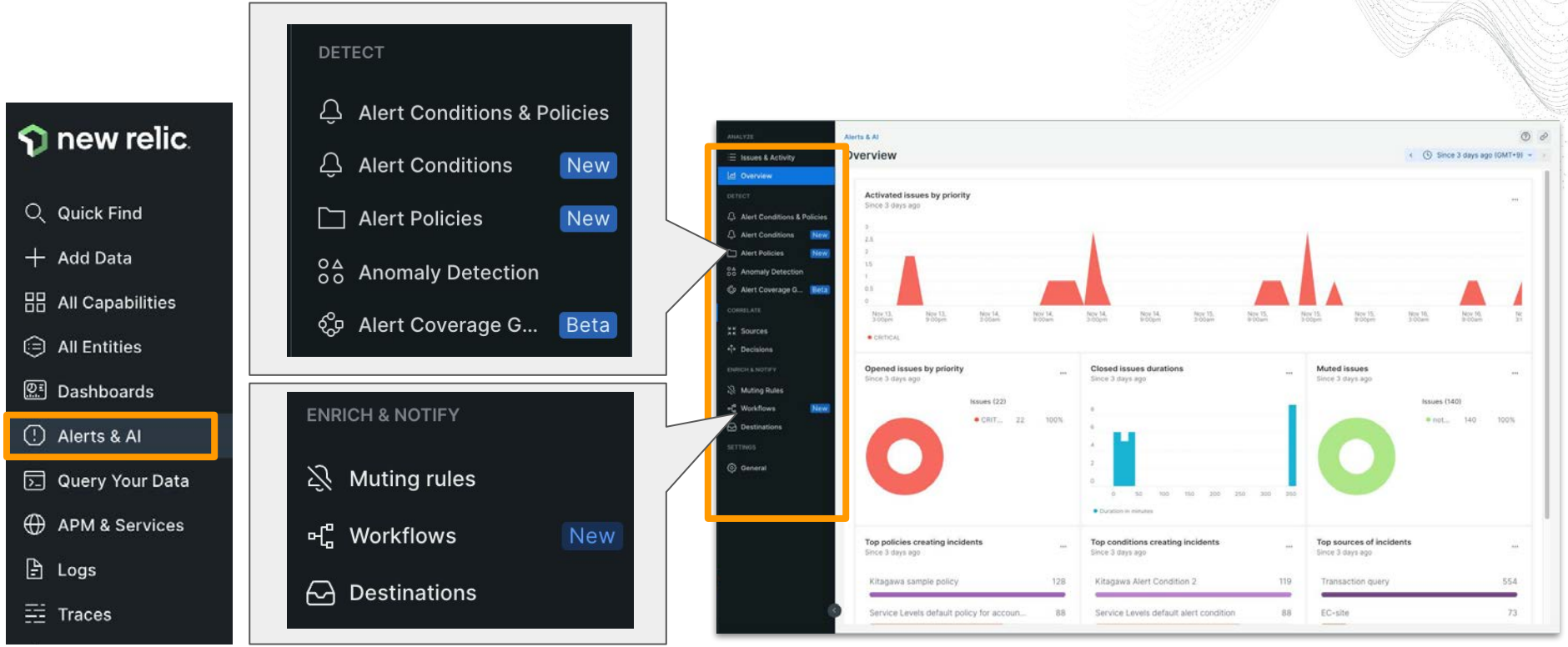
※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説していきます



New Relicのアラート構造全体像



アラート機能の全体UIと重要メニュー



new relic

New Relic アラートの構成要素1: Alert Policy

Alert Policy

Alert Conditionのグループ

Alert Condition

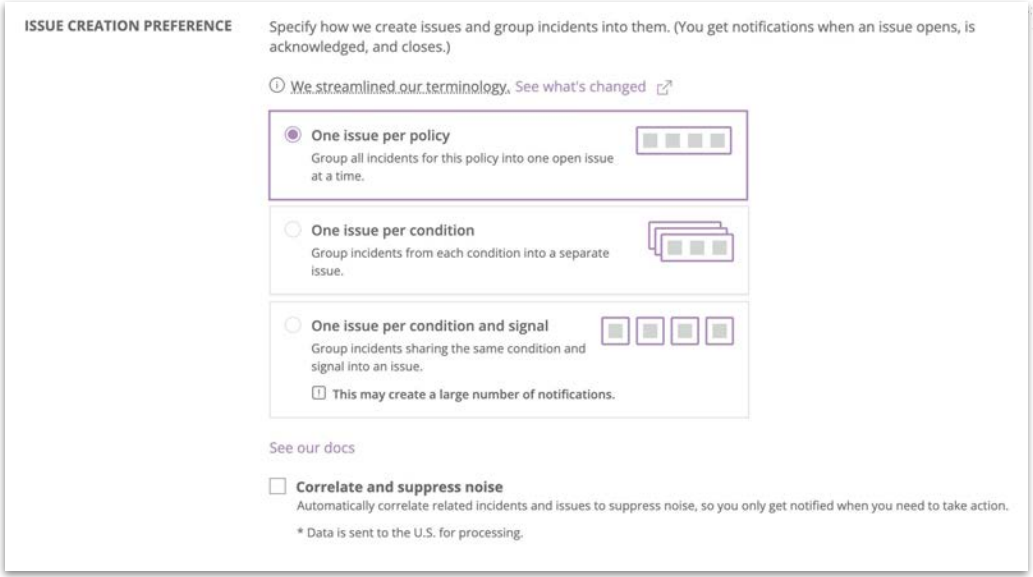
アラート対象や閾値、集計方法の定義

Incident

Alert Conditionで検出した個々の違反

Issue

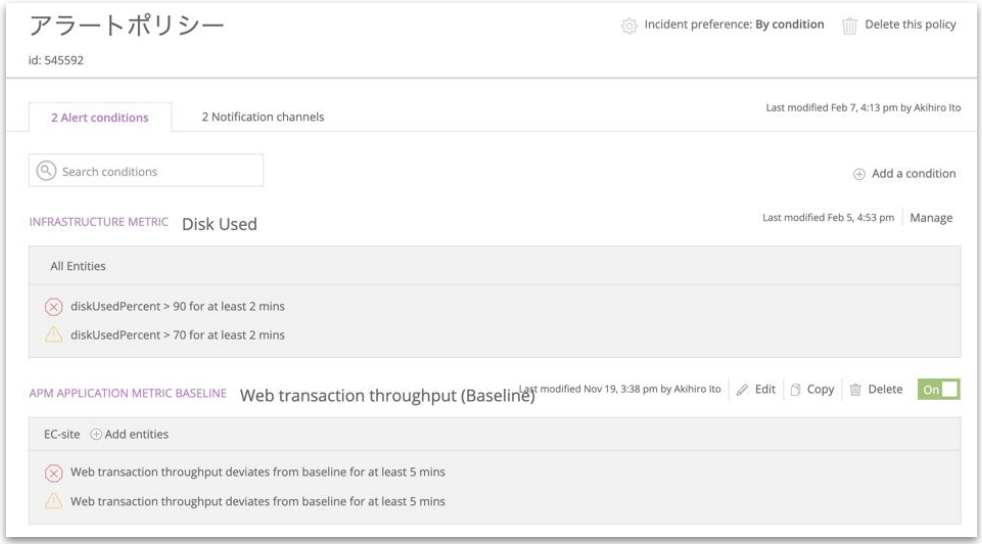
一つ以上のIncidentが示す、発生中の問題
実際の通知はIssueに対して行われる



New Relic アラートの構成要素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 アラートの構成要素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: サーバーサイドのエラー率 (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	この例で起票されるIssue(通知件数)
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(JSエラーで1件、サーバーサイドエラー全体で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(JSエラーで1件, ホスト毎のサーバーサイドエラーで3件)

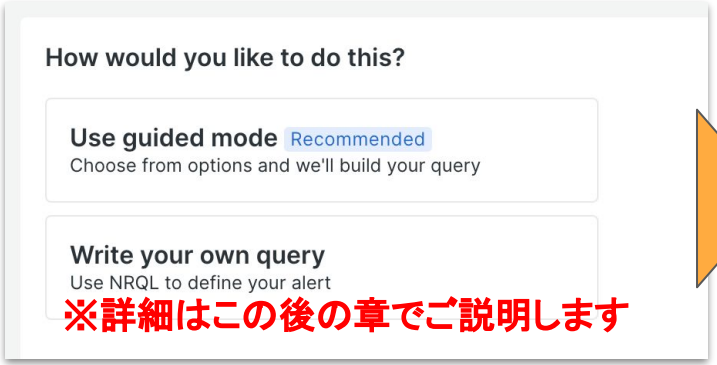
New Relic アラートの構成要素2: Alert Condition

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

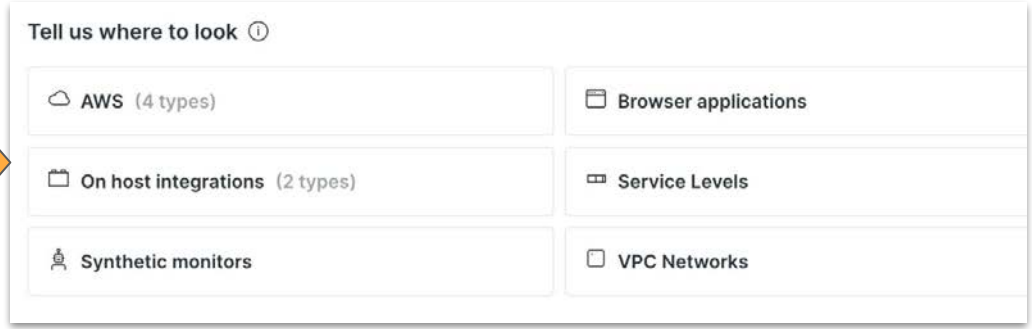
- どのような方法で集計を行うか（平均値・最大値・データ件数カウントなど）
- どのような状況をアラートとして通知するか

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



※詳細はこの後の章でご説明します



New Relic アラートの構成要素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)

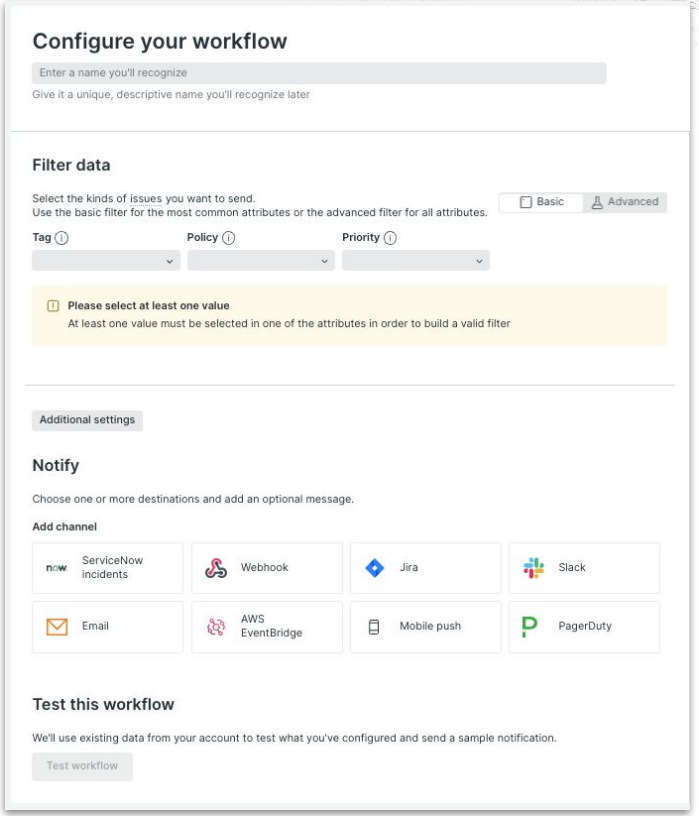
Muting Rulesが設定されていた場合の挙動の設定

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 アラートの構成要素4: Destinations

Issueのライフサイクル変化（オープン・クローズ）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

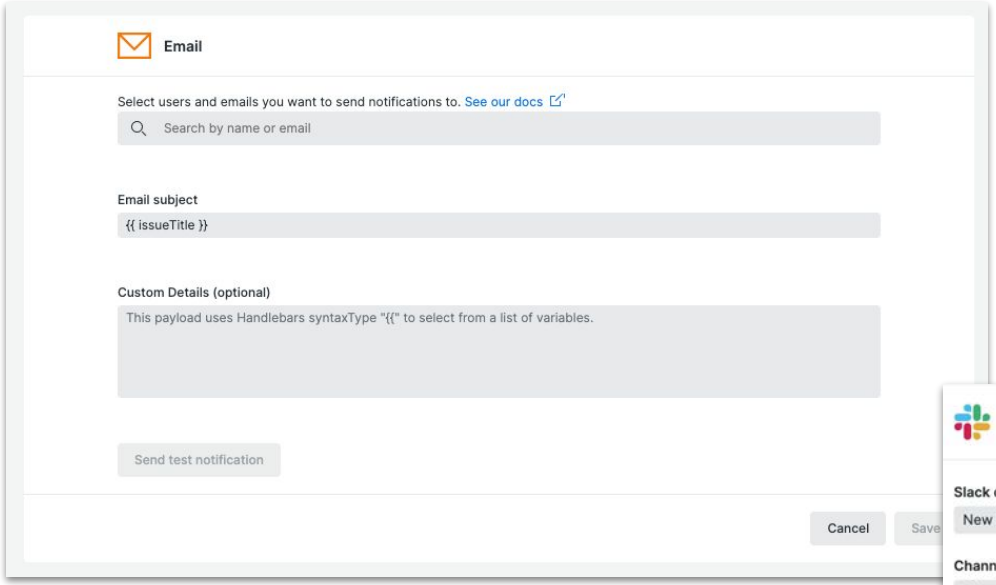
servicenow

PagerDuty

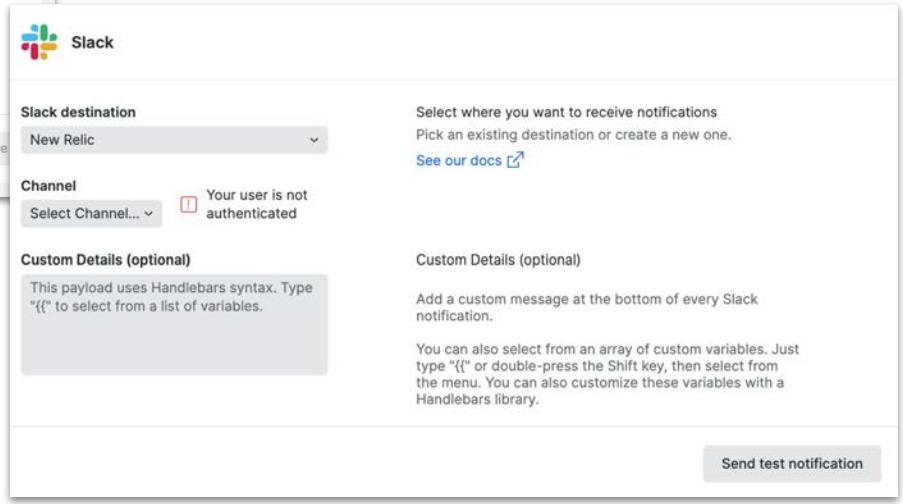
JIRA

Amazon EventBridge

New Relic アラートの構成要素4: Destinations



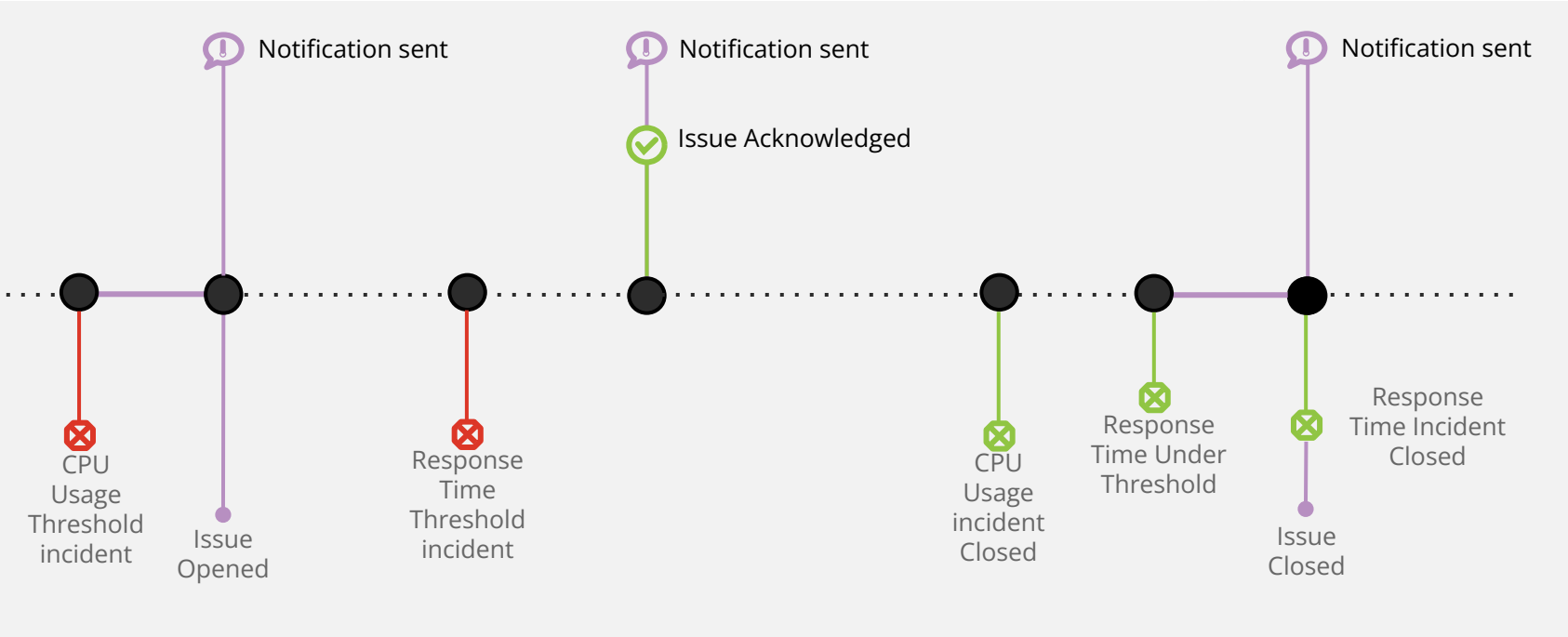
- Workflows変数を用いて、柔軟に標題や内容のカスタムができます
  - 補足: custom violation descriptionとは別の情報付加機能となります。
- “{{“と入力することで、Workflows変数の補完機能を活用できます。



Workflows variables:
https://docs.newrelic.com/docs/alerts-applied-intelligence/applied-intelligence/incident-workflows/custom-variables-incident-workflows/

補足: Issueのライフサイクルと通知タイミング

Issueの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く

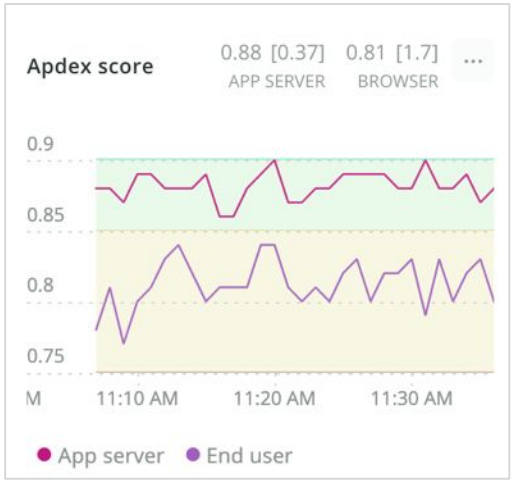


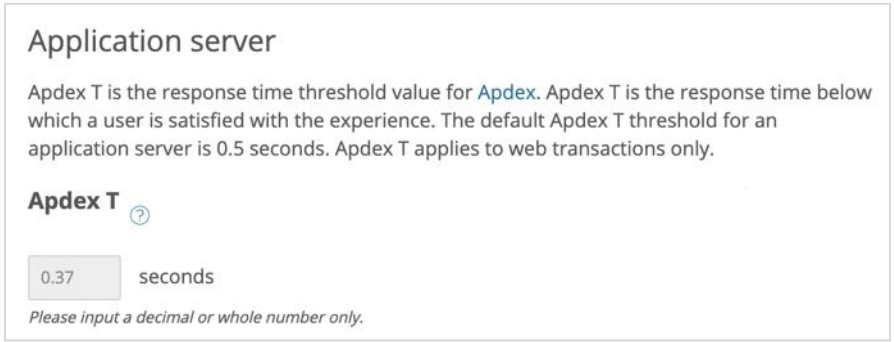
new relic

補足: アラートを設定する前にやること

Apdex Tの値を適切に設定する

- Apdexはパフォーマンスに対するユーザーの満足度を示す指標
- 特にフロントエンドはエンドユーザー側のノイズに影響されやすいため、単純な応答時間の平均よりも有用な場合が多い

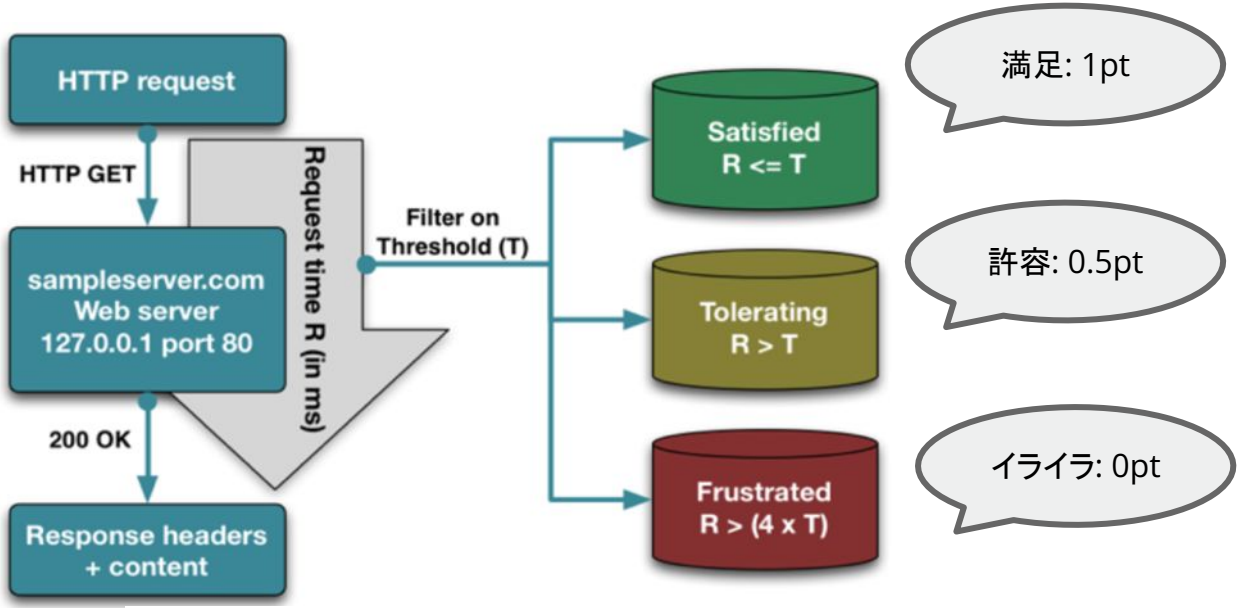




補足: Apdex T値について

それを満たせばユーザーが満足すると想定される、最大応答速度

APMおよびBrowserのアプリケーションごとに設定可能 (Application Settingsメニュー)



$$Apdex\ Score = \frac{1 \times \text{Satisfied件数} + 0.5 \times \text{Tolerating件数} + 0 \times \text{Frustrated件数}}{\text{Satisfied件数} + \text{Tolerating件数} + \text{Frustrated件数}}$$

今回監視対象のサイト

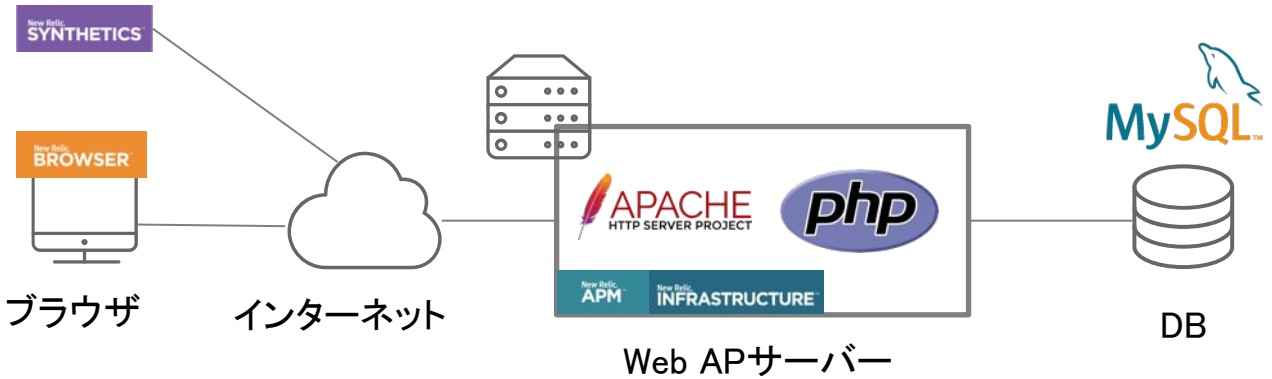
[NRUジェラートショップ](ECサイト)

このハンズオンでは、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
モニタリング対象にしています。

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

今回の環境の監視構成

- New Relic:
  - 外形監視, フロントエンド(ブラウザ), アプリケーション、インフラ
- Zabbix:
  - インフラ



ハンズオン(0)
環境を確認する

15:30 - 15:40 (10min)

ハンズオン環境について

New Relic にログインしてください。

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

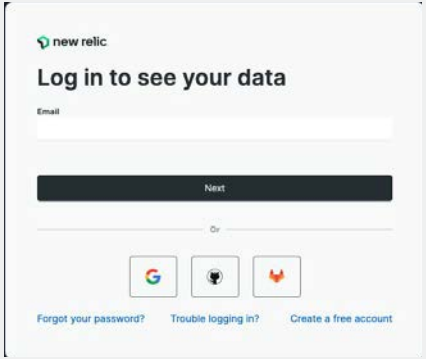
- ユーザー: **japan-handson+nru@newrelic.com**
- パスワード: **oSz6nrupas**
  (オー、エス、ゼット、ロク、エヌ、アール、ユー、ピー、エー、エス)

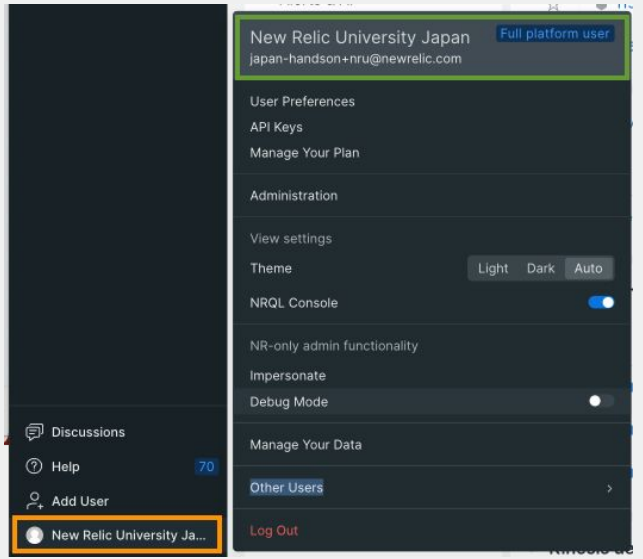
ユーザー名が “**New Relic University Japan**” であることをご確認ください

[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。
プライベートブラウジングをお使いください。

また、ブラウザは下記のいずれかをご利用ください。

- 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



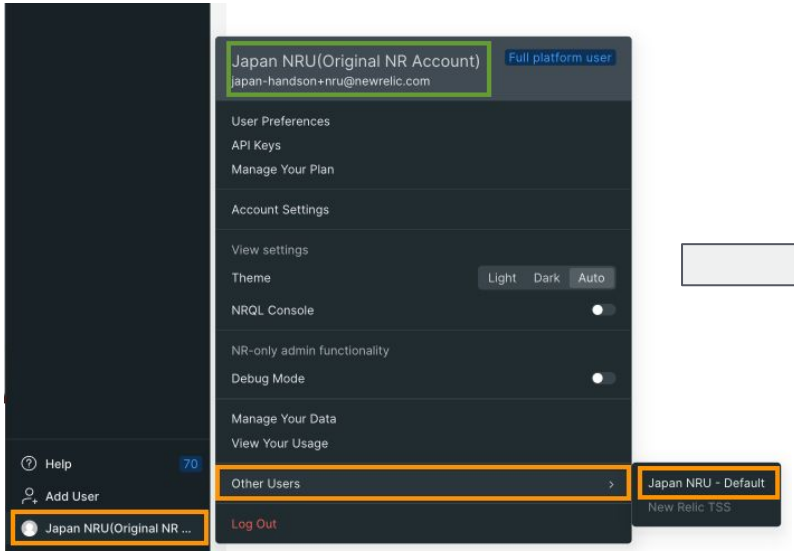


ログイン後のアカウントの切り替え

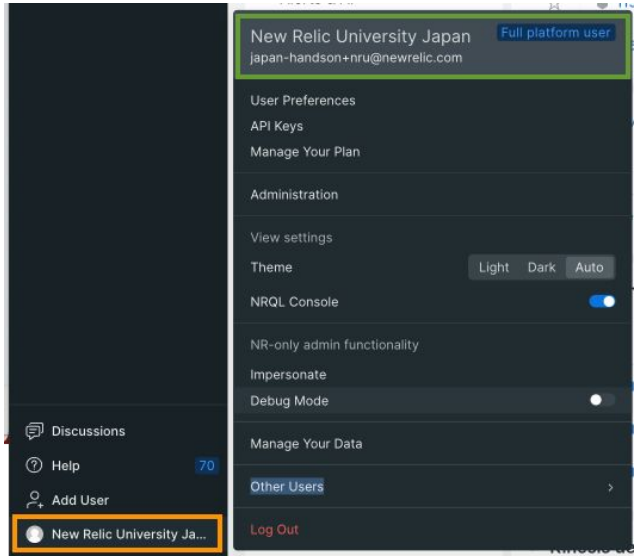
“Japan NRU(Original NR Account)” の場合は

以下の操作にて、ユーザーの切り替えをお願いします
ユーザー名 > Other Users > “Japan NRU”
再度パスワードを入力し、ユーザーの切り替えを実施ください。

“**Japan NRU (Original NR Account)**” ではなく



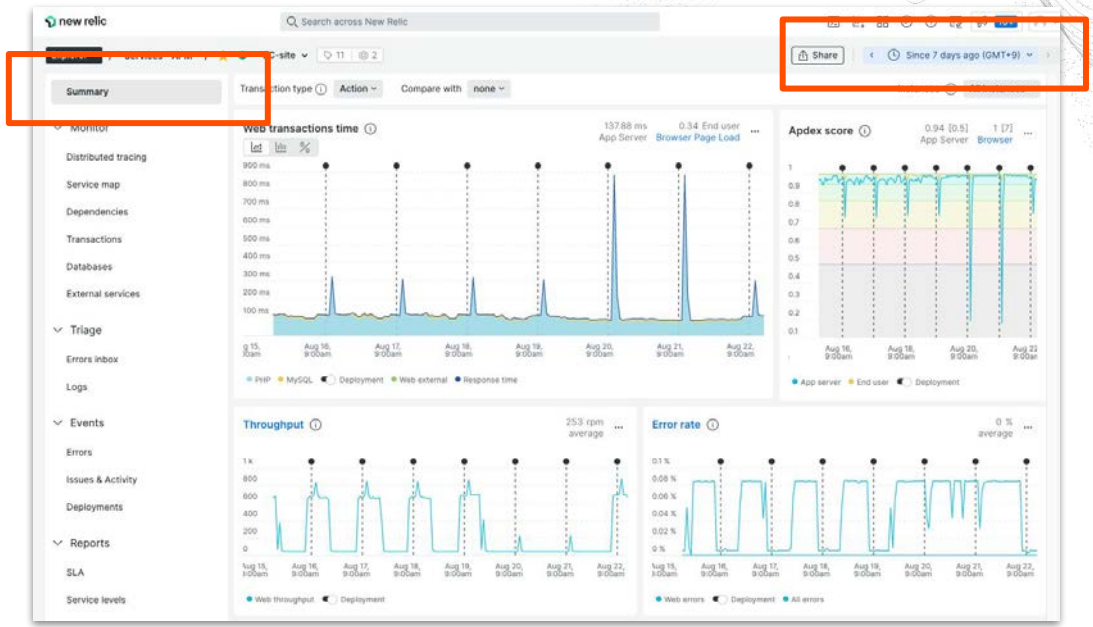
ユーザー “**New Relic University Japan**” を利用します



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。

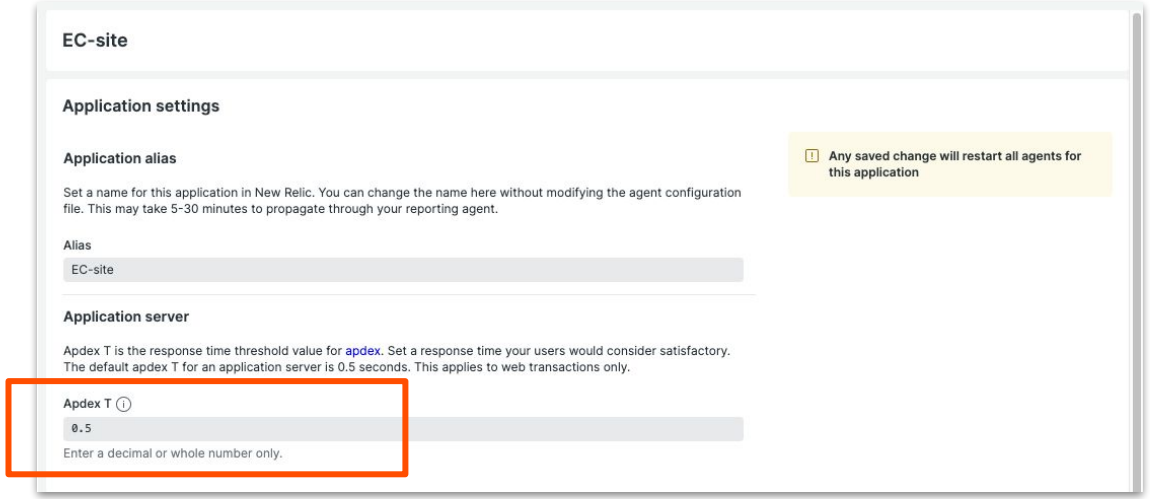


new relic

ハンズオン(0) Apdex Tの設定箇所の確認

変更は行わない!!!

- 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。
- Settings → Applicationを選択します。



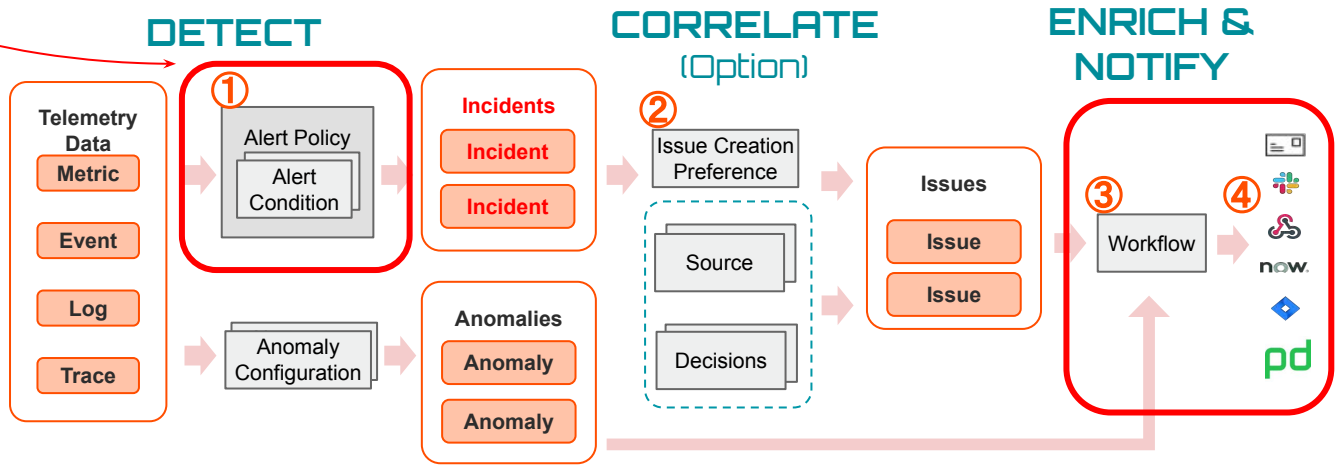
ハンズオン(1)
アラートポリシー・ワークフローを作成する

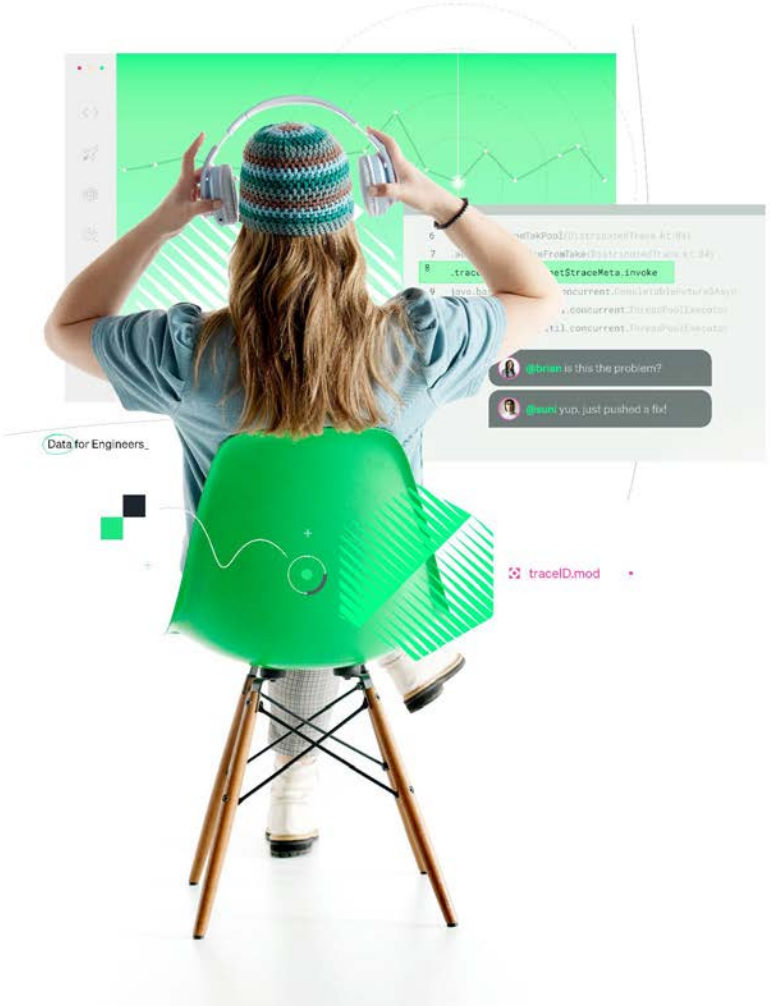
15:40 - 16:00 (20min)

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を作成する

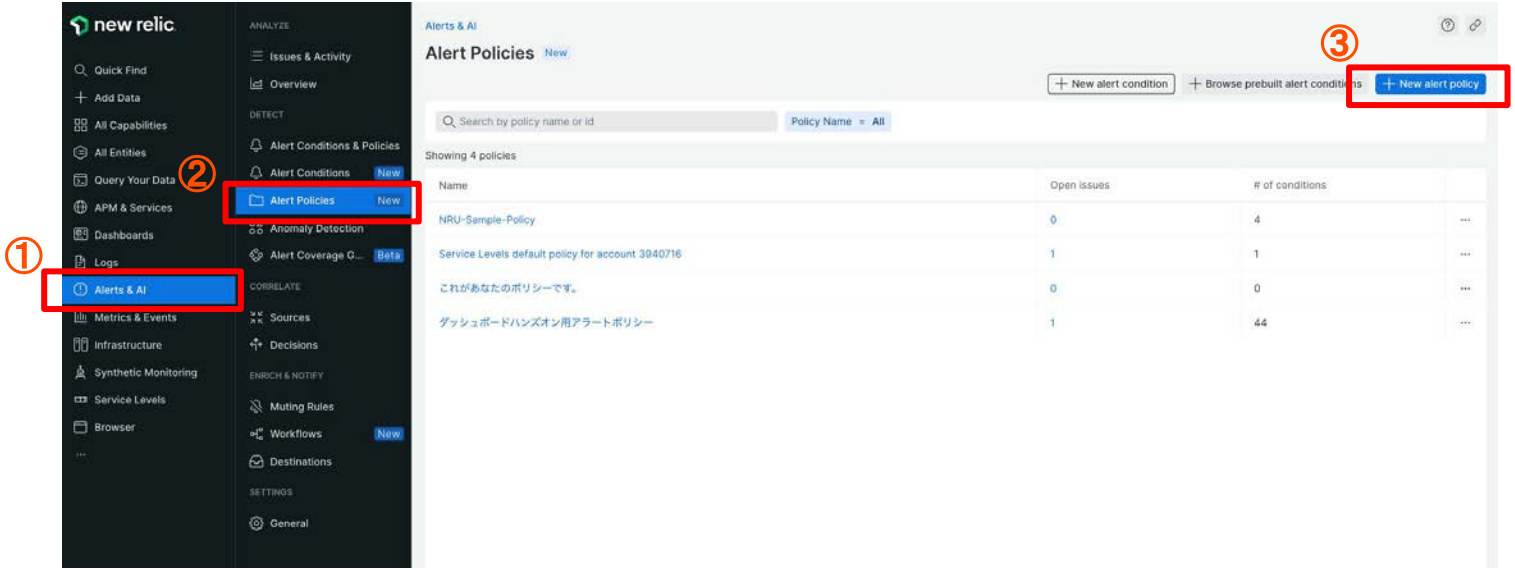



Data for Engineers_
@brian is this the problem?
@suni yup, just pushed a fix!
traceID.mod

手順・解説

ハンズオン(1-1) Alert policyを作成する 1/2

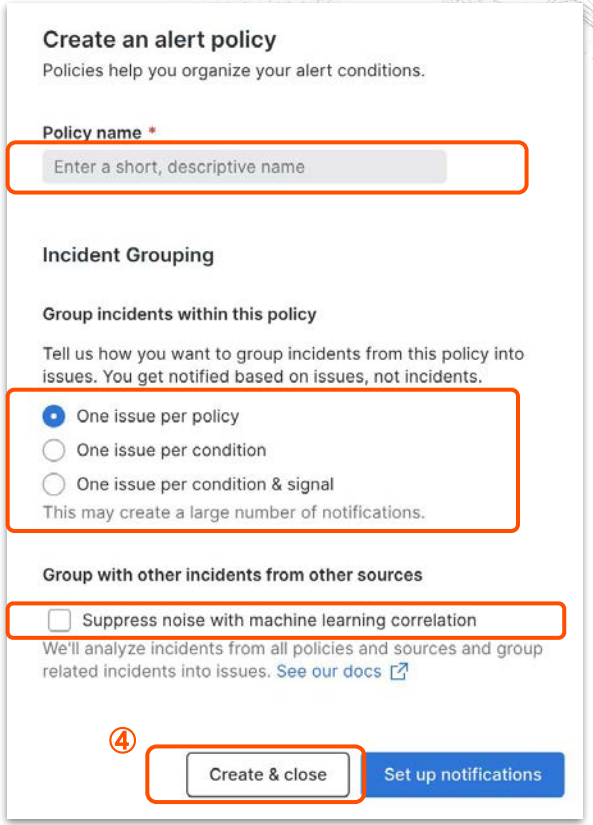
1. Alerts&AI メニューを開きます。
2. Alert Policies を開きます。
3. [+New alert policy] を選択して、新しいAlert Policyを作成します。



ハンズオン(1-1) Alert policyを作成する 2/2

1. 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
2. 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
3. [Suppress noise...]をチェック
4. [Create & close] をクリックします

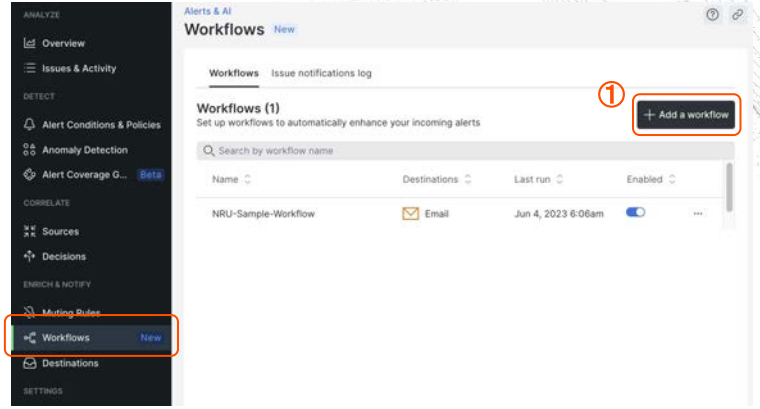
ウィザードでの一括作成もできますが、今回は各コンポーネントを手動で作成したいため、ここでは **Alert policyのみ**を作成します

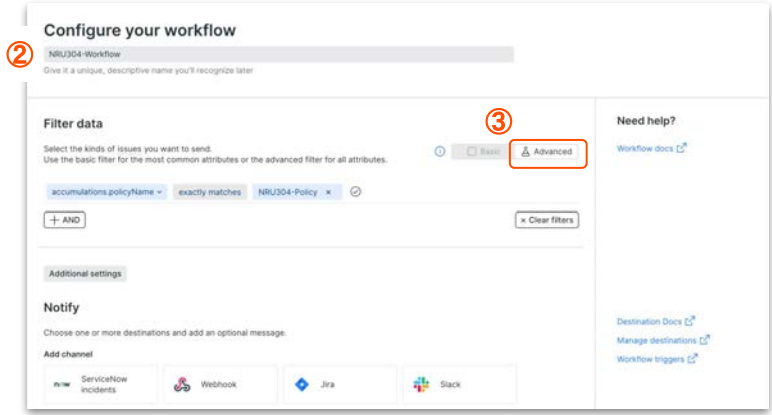


ハンズオン(1-2) Workflowを作成する 1/6

1. Alerts & AI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

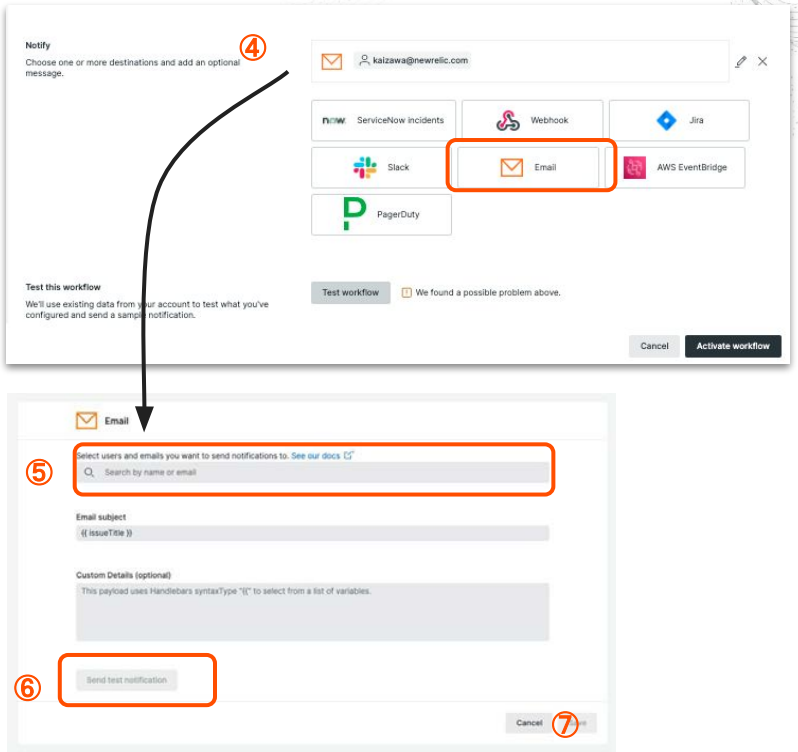
補足: 上記3番の設定はBasicでも可能ですが、より柔軟な設定を行う場合にはAdvancedを活用します。





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。
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



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。

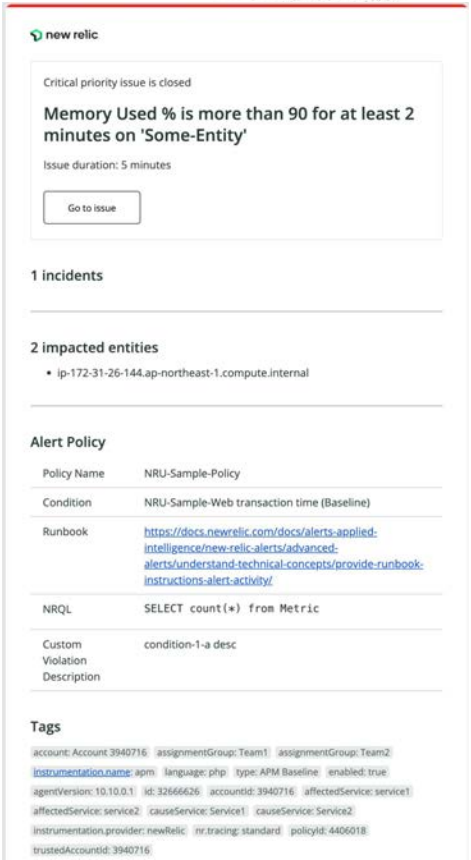
- Policy名やCondtion名は確認できますか？
- Runbook URLはどこに記載されていますか？
- Tagsというセクションには、どのような情報が含まれ ていますか？

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。



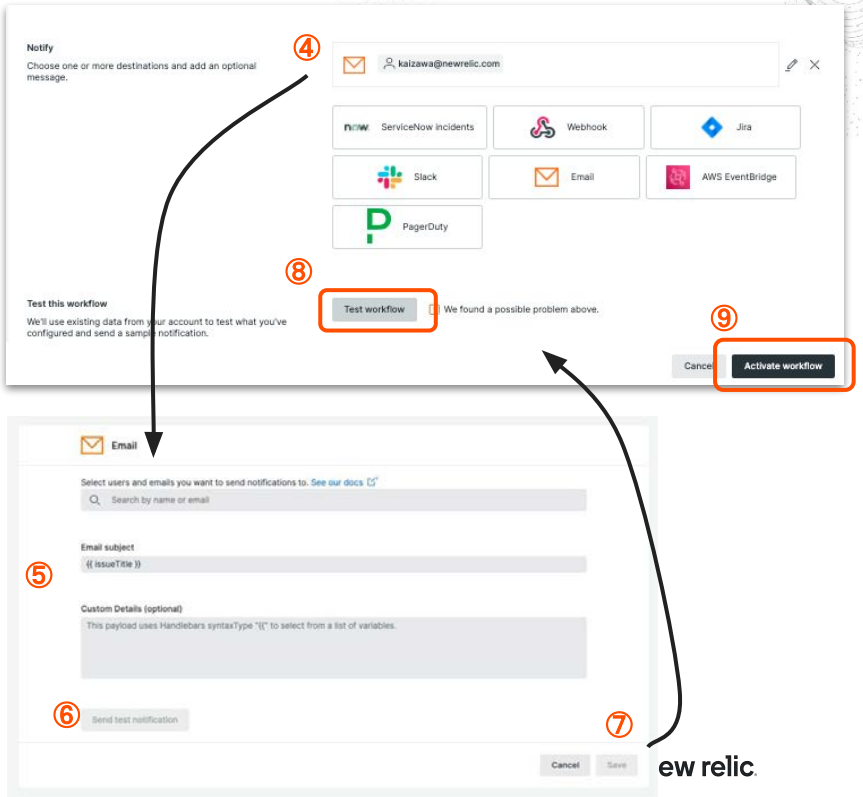
new relic

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)

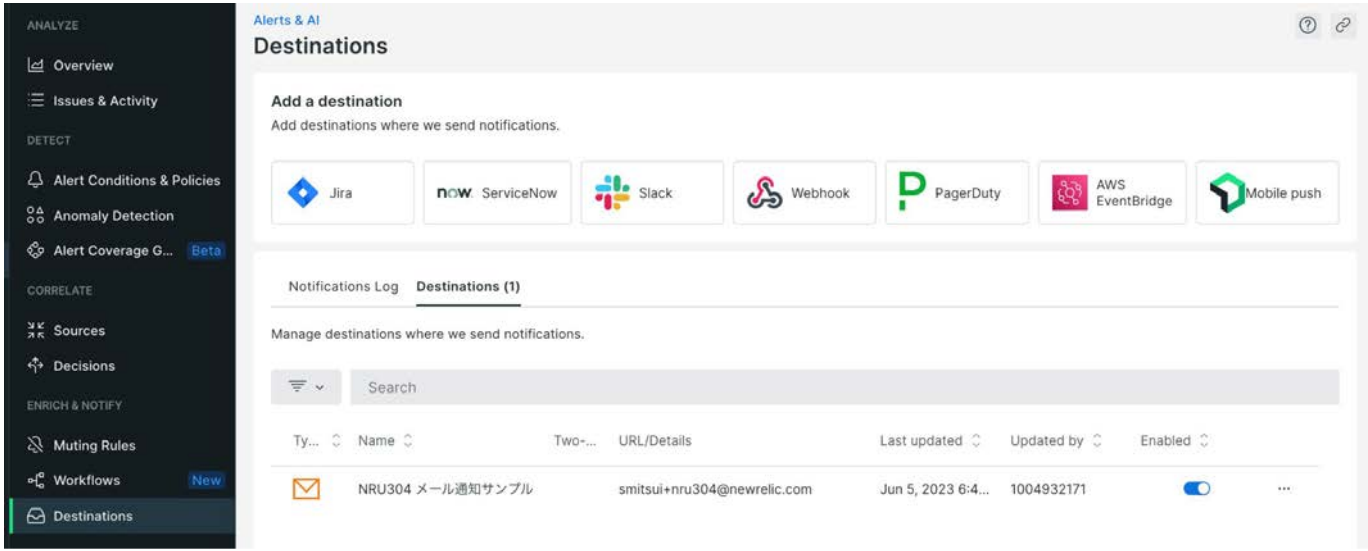
9. Activate workflowボタンをクリックし、設定を保存します



ハンズオン(1-2) Workflowを作成する 5/6

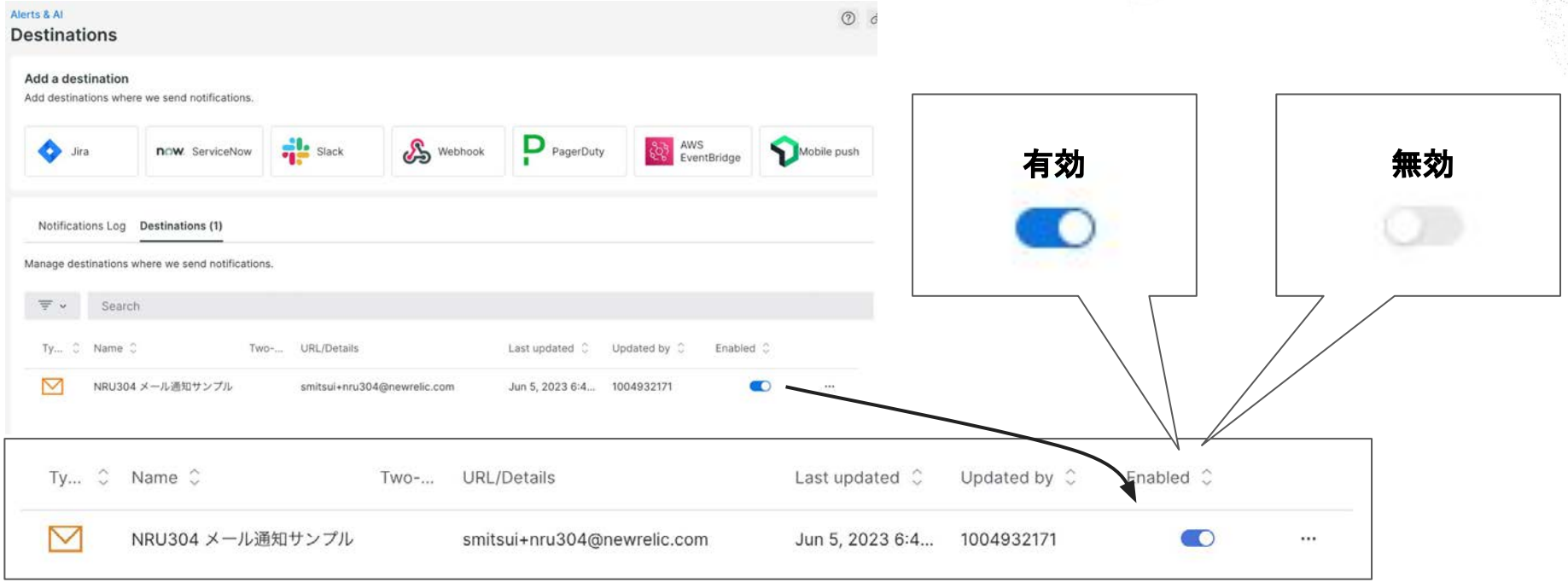
Workflows内でEmailを追加すると、Destinationも自動的に作成されます。

Alerts & AI > 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 - 16:15 (15min)

new relic

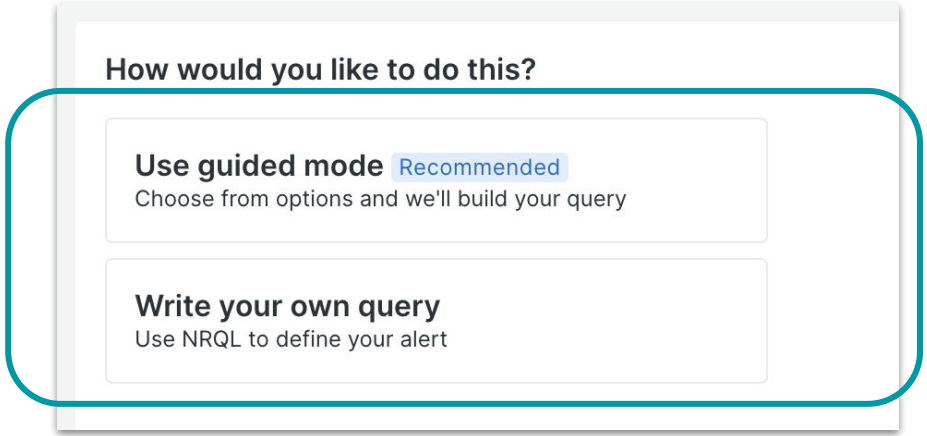
New Relic アラートの構成要素2: Alert Condition

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

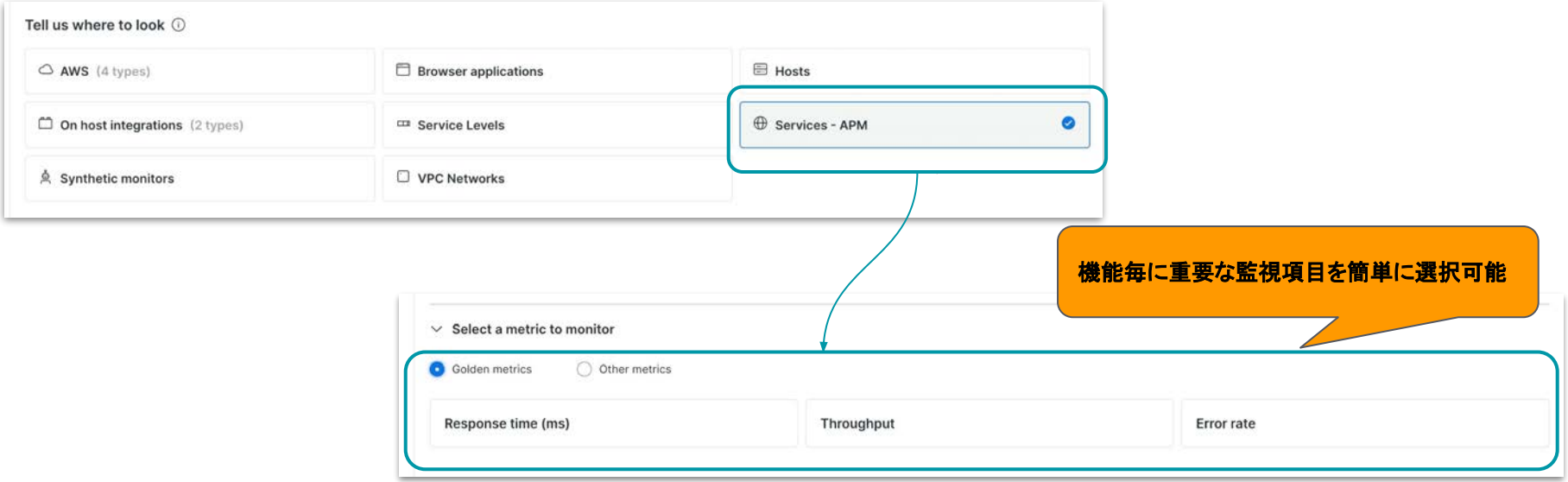
機能（例. APM, Browser等）ごとに用意されたプリセットから簡単にアラートを作れるほか、

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 アラートの構成要素2: Golden signal or Metric

Golden Signalをベースにそれぞれの機能に合わせて、ガイド付きで簡単にアラート条件を作成



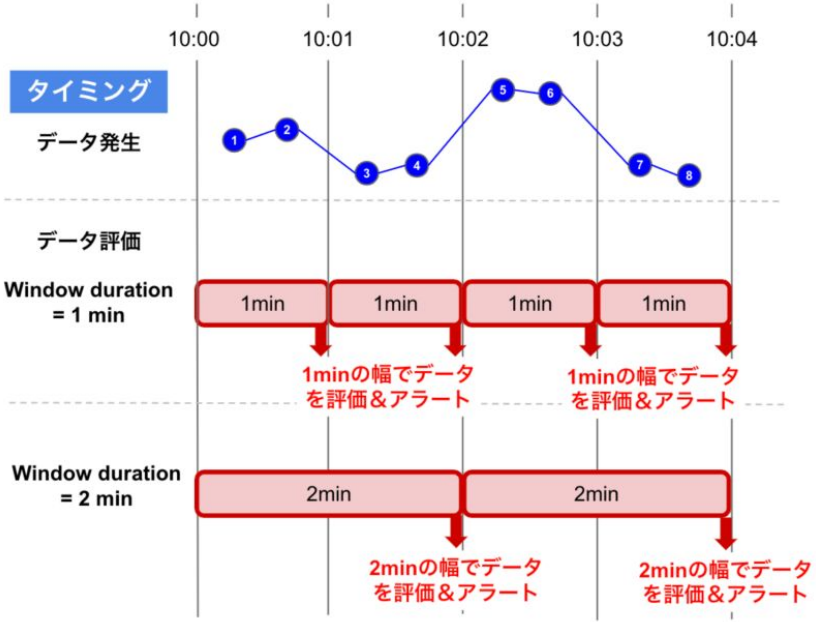
new relic

New Relic アラートの構成要素2: Windows Duration

アラート条件ごとに、この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。

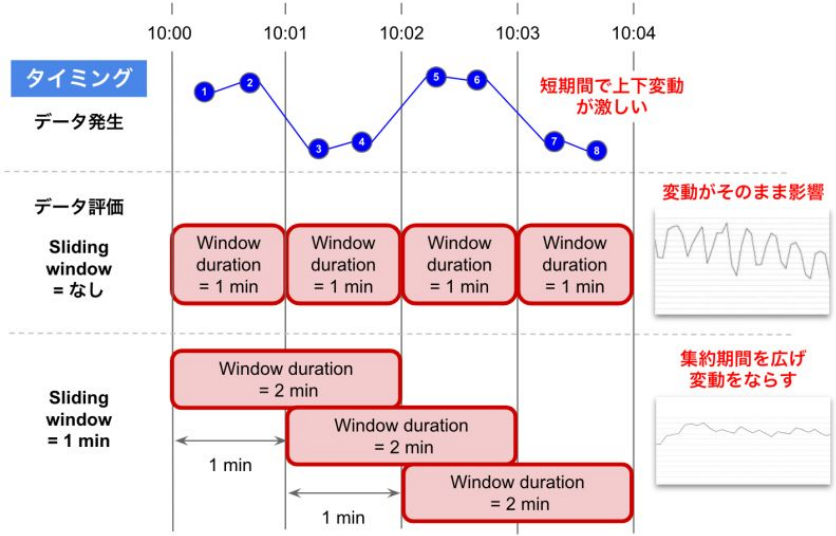


new relic

Sliding Window(オプション)

通常、集計ウィンドウの期間は互いに重なりません。

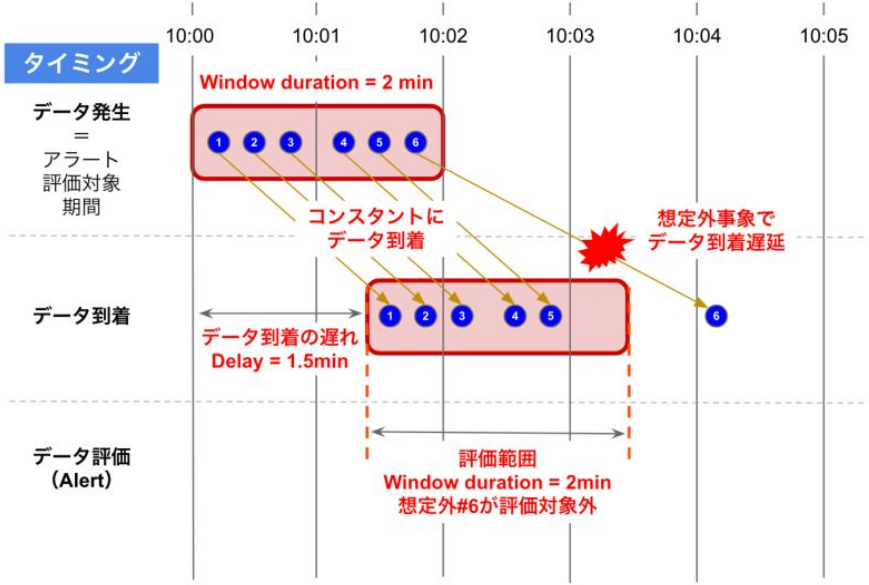
Sliding Windowオプションを有効にすると、指定した時間分スライドさせた複数の集計ウィンドウが並行して開かれるため、よりきめ細かい集計結果を得ることができます。



new relic

New Relic アラートの構成要素2: Streaming method

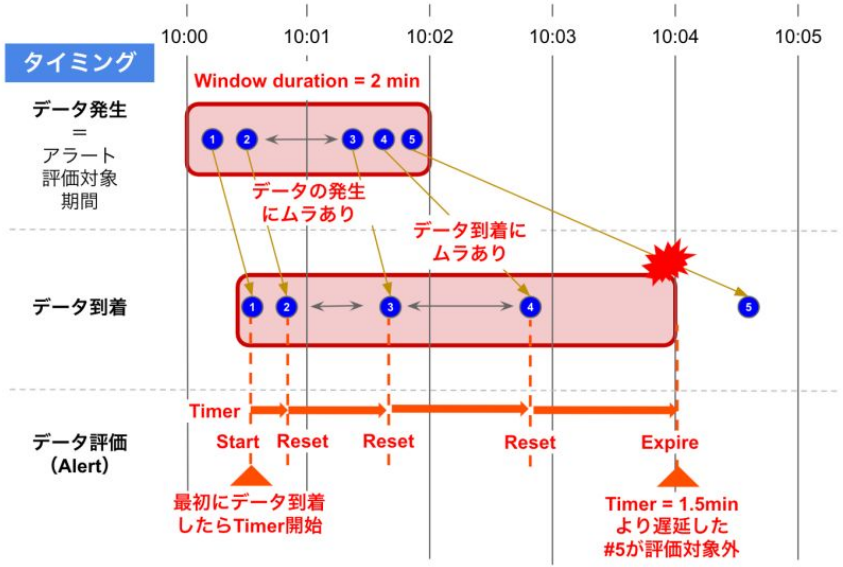
- Event Flow
  頻繁かつ一定間隔で発生するデータに対するアラート設定に最適な方式です。
  許容される遅延時間（Delay）よりも後に続くデータが到着すると、集計ウィンドウが閉じられます。



new relic

New Relic アラートの構成要素2: 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。



new relic

New Relic アラートの構成要素2: Streaming method

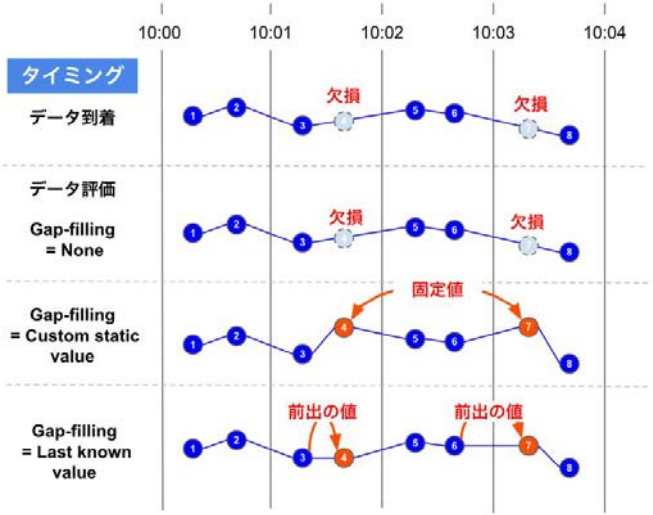
- Cadence
  Cadenceは、データのタイムスタンプではなく、New Relic内部のシステムクロックに基づいて、一定の間隔で集計を行う方法です。多くのケースでは Event FlowまたはEvent Timerが適していますが、モバイル端末やブラウザから送信されるイベントのように、ユーザー端末の時刻設定に影響されて、タイムスタンプに一貫性がないデータを対象にする場合には、Cadenceが有効です。

補足: Gap-filling strategy

- Gap-filling strategy

集計結果が存在しない集計ウィンドウ（ギャップ）を検出した場合に0、任意の値、直前の集計結果のいずれかで、その期間の集計結果を埋めることができます。

ただし、集計結果が存在しないことを検出してギャップを埋めることができるのはNRQLクエリのWHERE句に該当する集計対象データが新たに到着したタイミングであり、集計対象データが存在しない状況をリアルタイムで検出して置換するものではない点に留意してください。



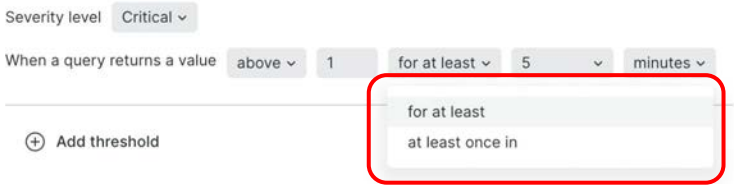
new relic

New Relic アラートの構成要素2: Alert Condition

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/docs/alerts-applied-intelligence/new-relic-alerts/alert-conditions/create-baseline-alert-conditions	エラー発生割合がいつもよりも増加した

New Relic アラートの構成要素2: Alert Condition



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

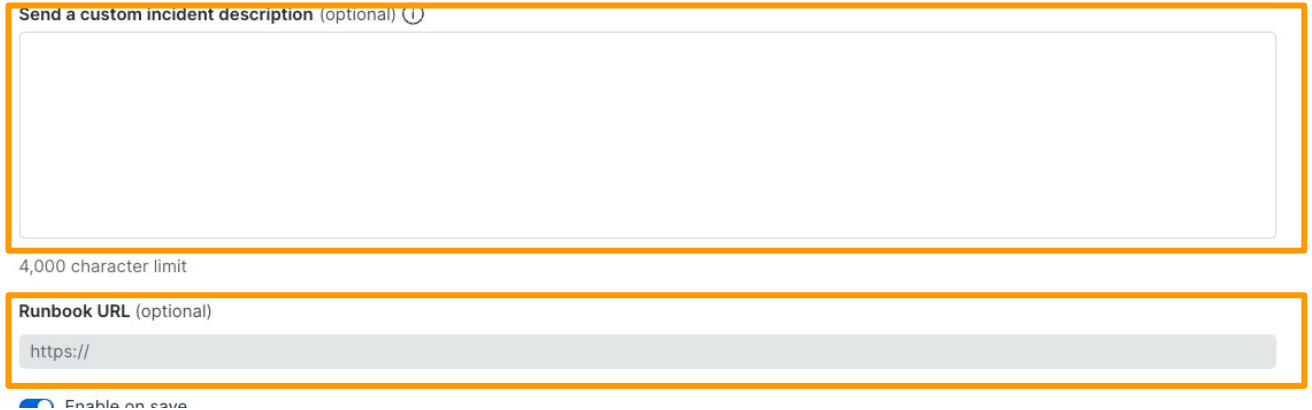
その他、アラート設定に関する詳細は以下もご参照ください:

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 アラートの構成要素2: Alert Condition

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



ハンズオン(2)
アラートコンディションを作成

16:15 - 16:30 (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

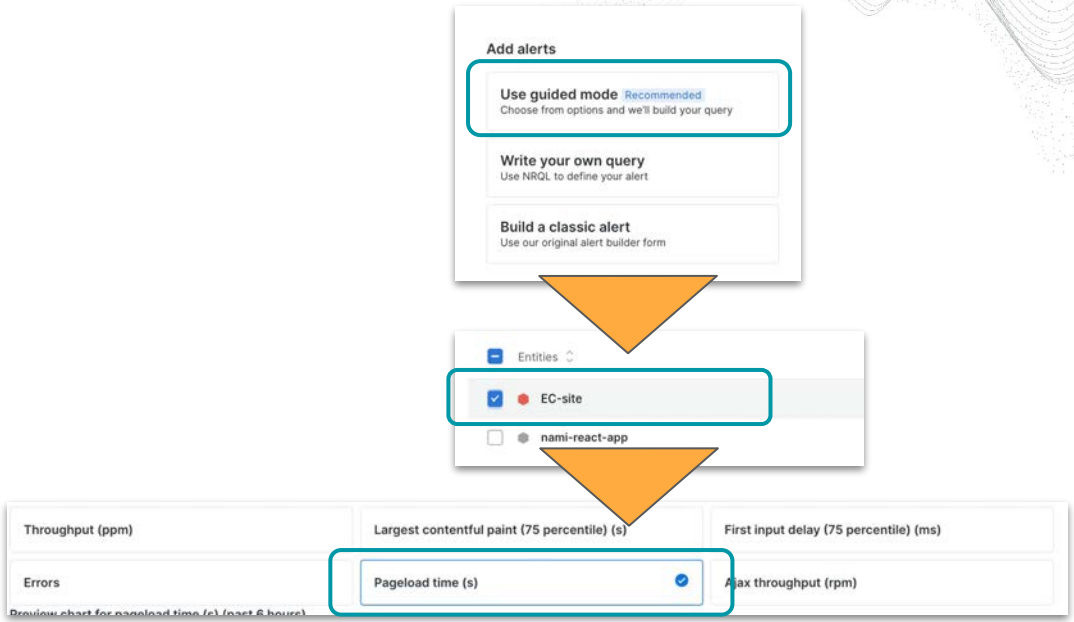
ハンズオン(2-1) Alert Conditionを作成する 2/21

- **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

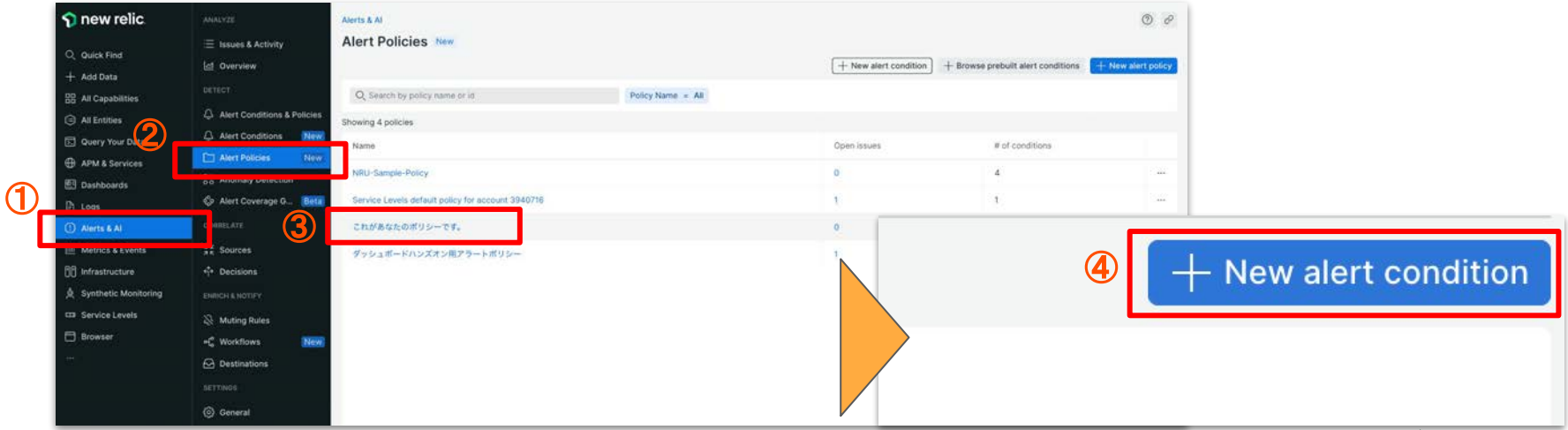


Condition名は適切なものを各自設定してください

（例：NRU304-yourname-NRQL-pageloadtime）

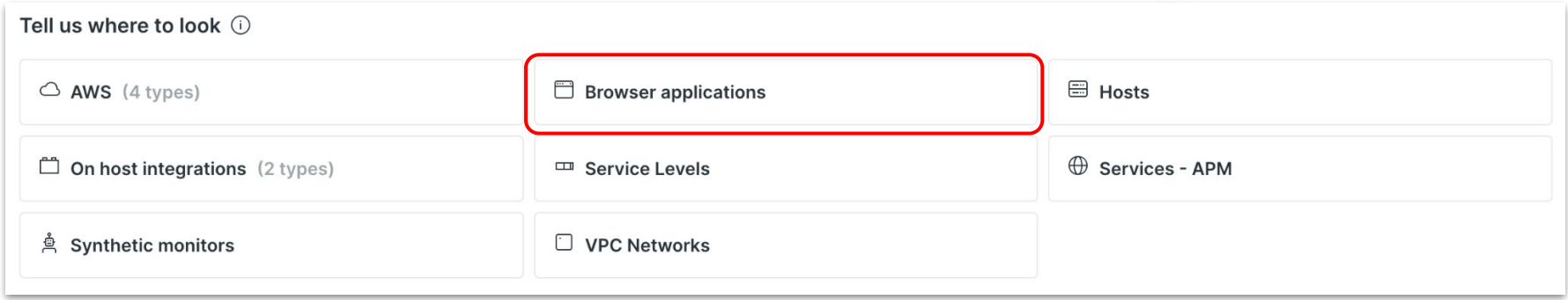
ハンズオン(2-1) Alert Conditionを作成する 3/21

1. Alerts&AI 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。



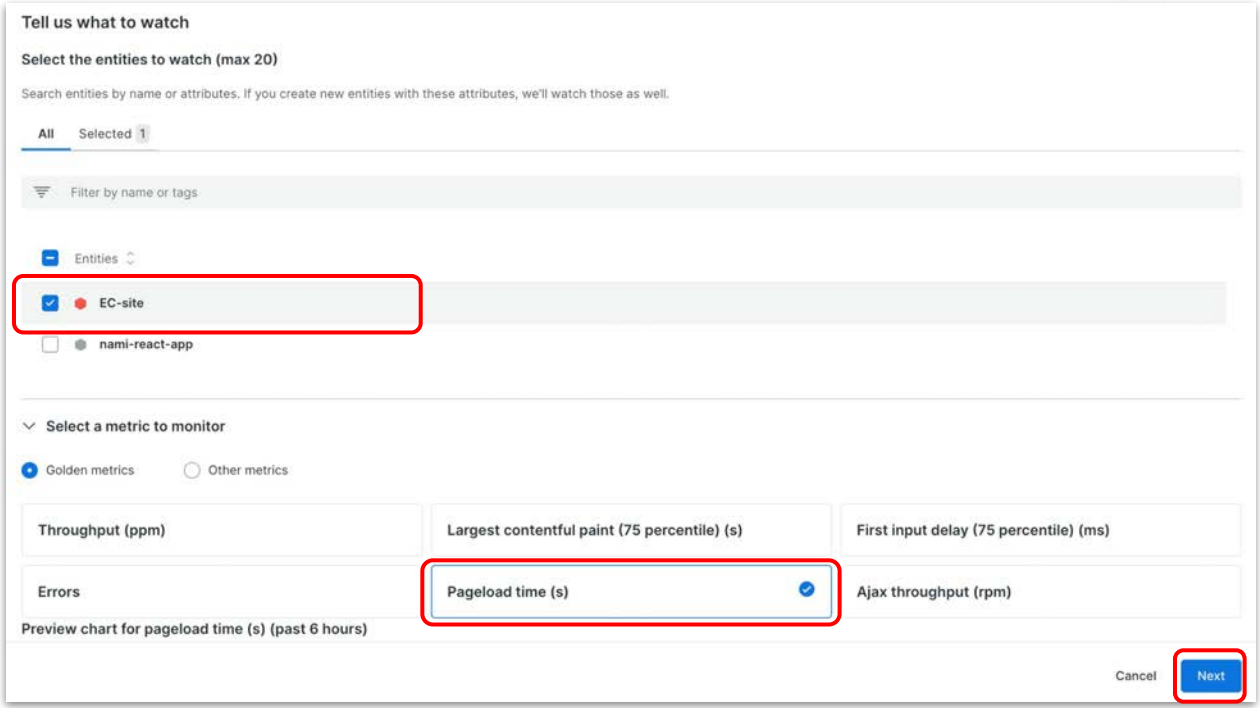
ハンズオン(2-1) Alert Conditionを作成する 4/21

- 「Browser applications」を選択し、設定画面を進みます。



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。



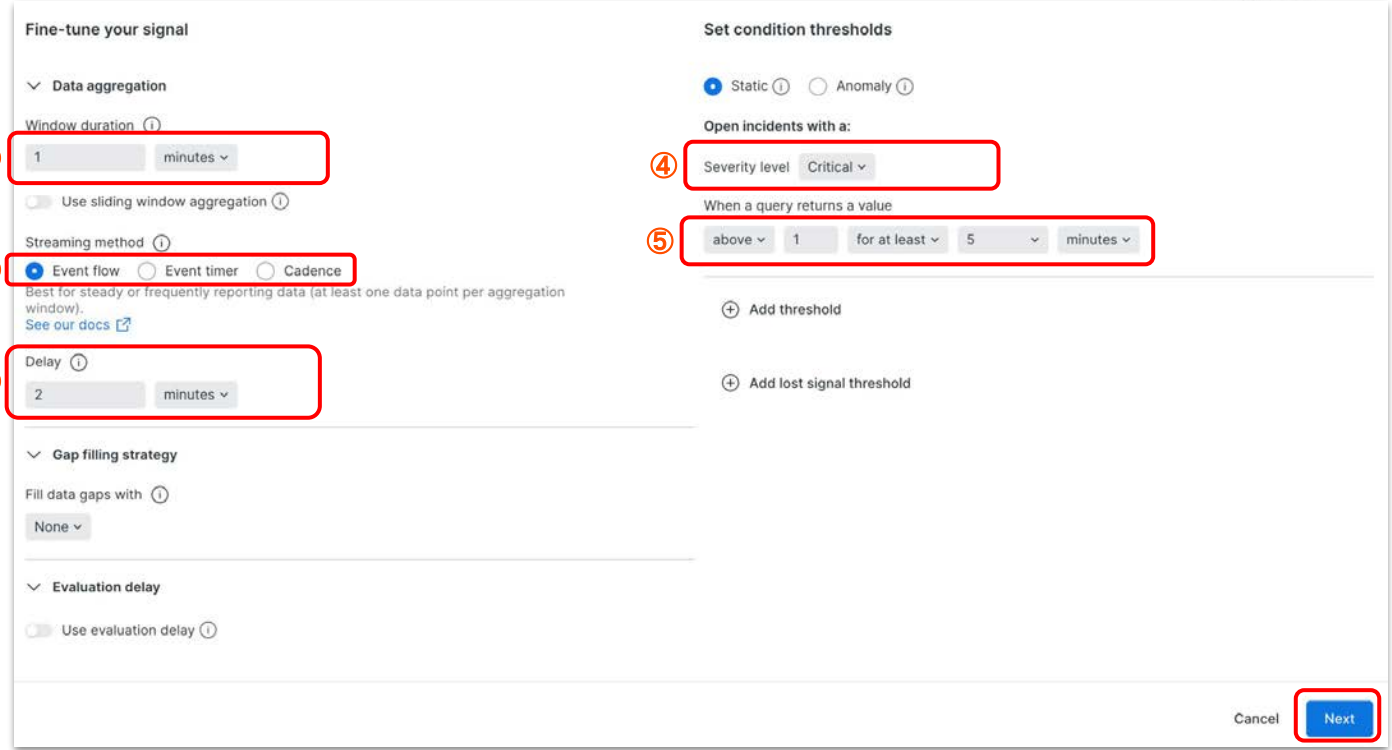
ハンズオン(2-1) Alert Conditionを作成する 6/21

- 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. **Severity level**
   a. Critical
5. **When a query returns a value**
   a. above 1 for at least 5 minutes

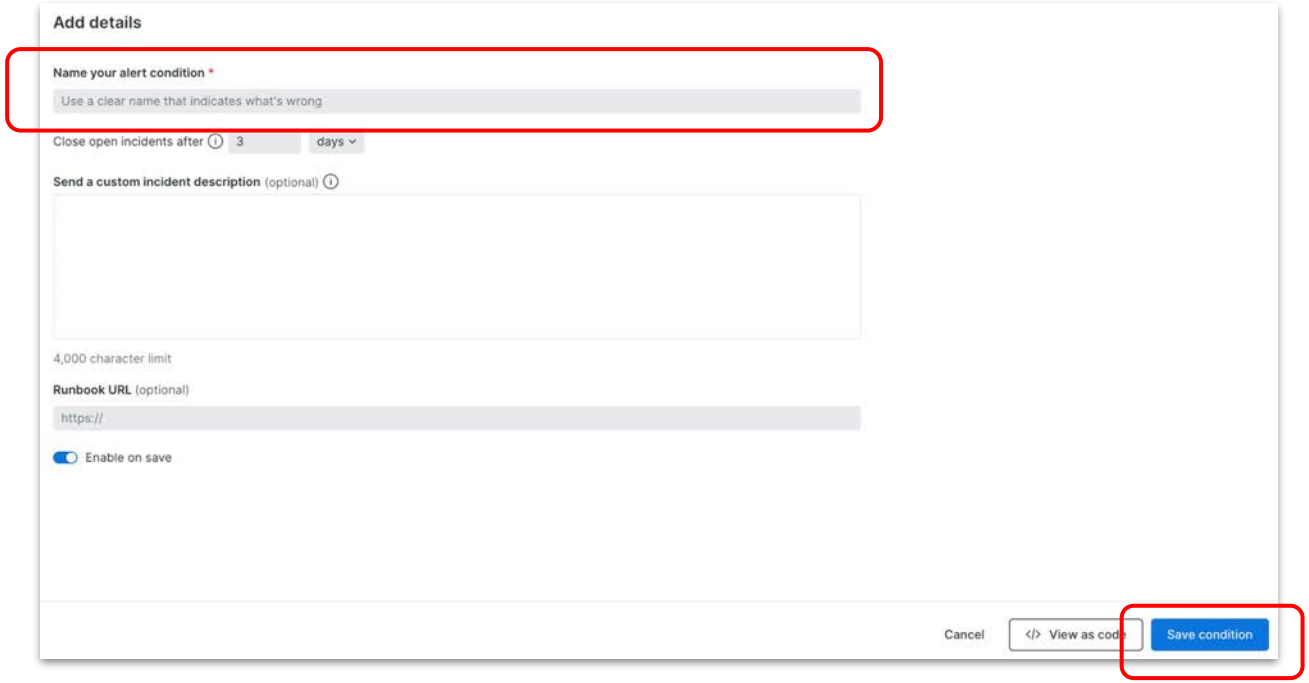
ハンズオン(2-1) Alert Conditionを作成する 7/21

- それぞれ 設定を確認し「Next」をクリック。



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。

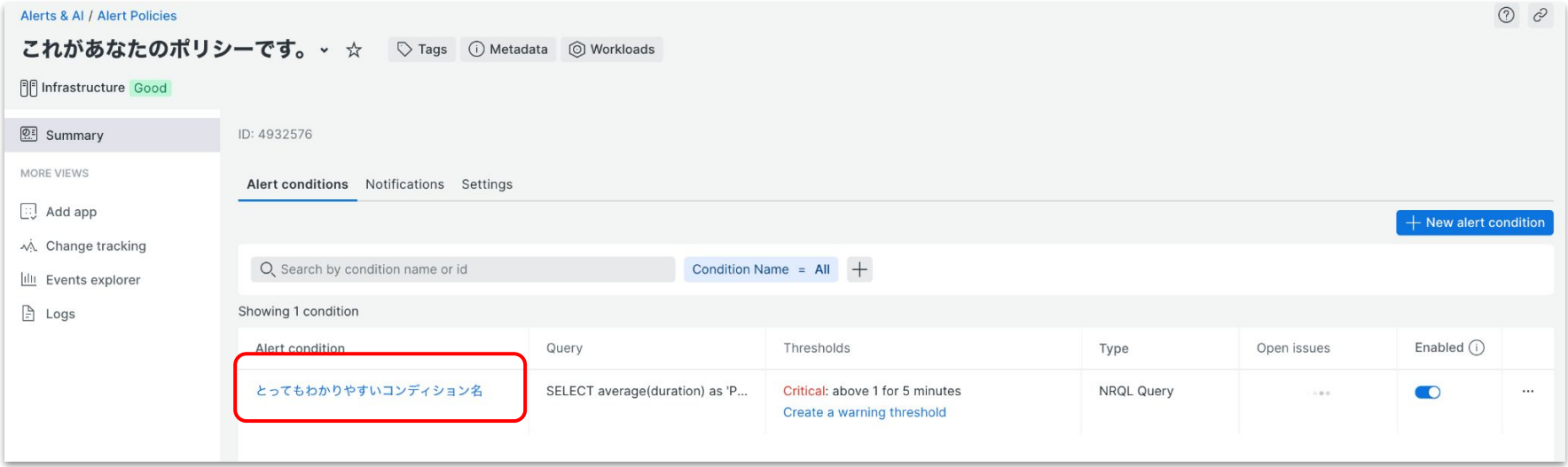


ハンズオン(2-1) Alert Conditionを作成する 9/21

- 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。

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**

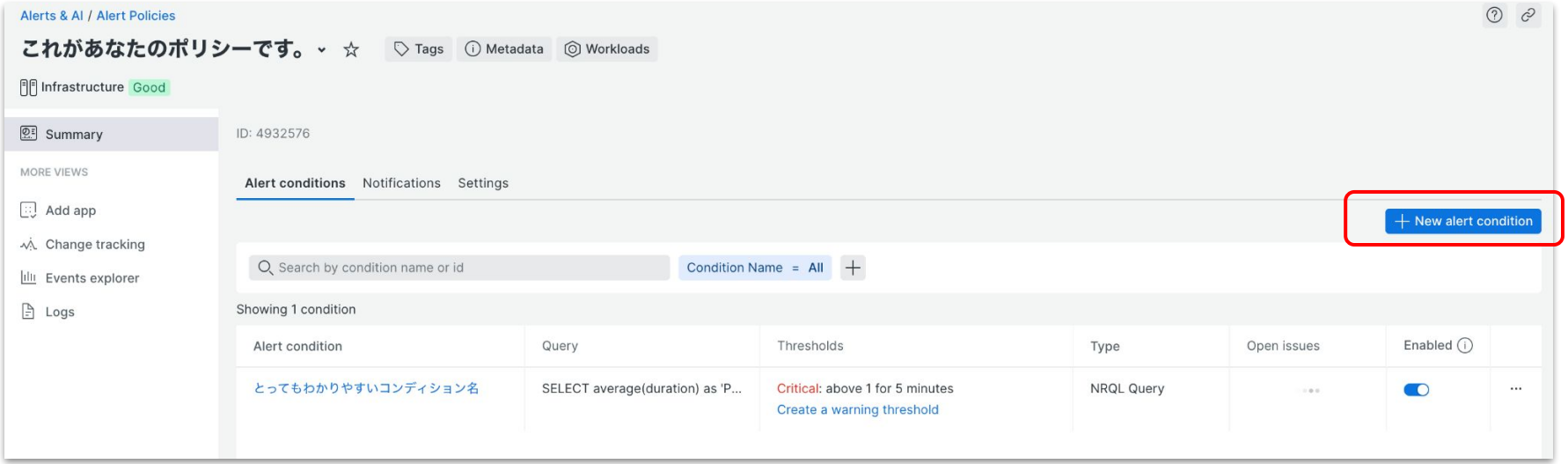
```
SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction FACET host
```

Condition名は適切なものを各自設定してください

（例：NRU304-yourname-NRQL-ErrorResponse）

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。

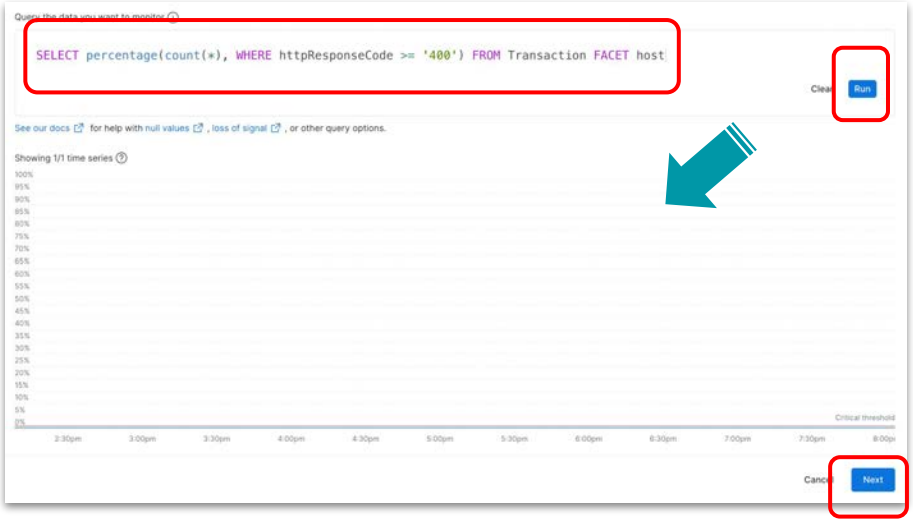


ハンズオン(2-1) Alert Conditionを作成する 13/21

- 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。

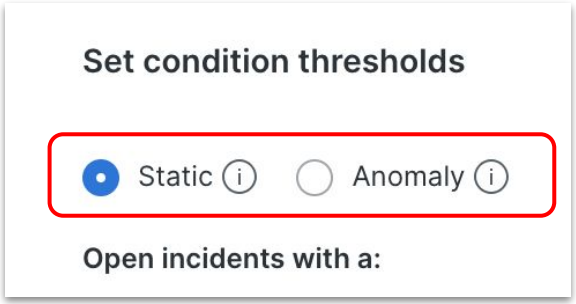
  SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction FACET host

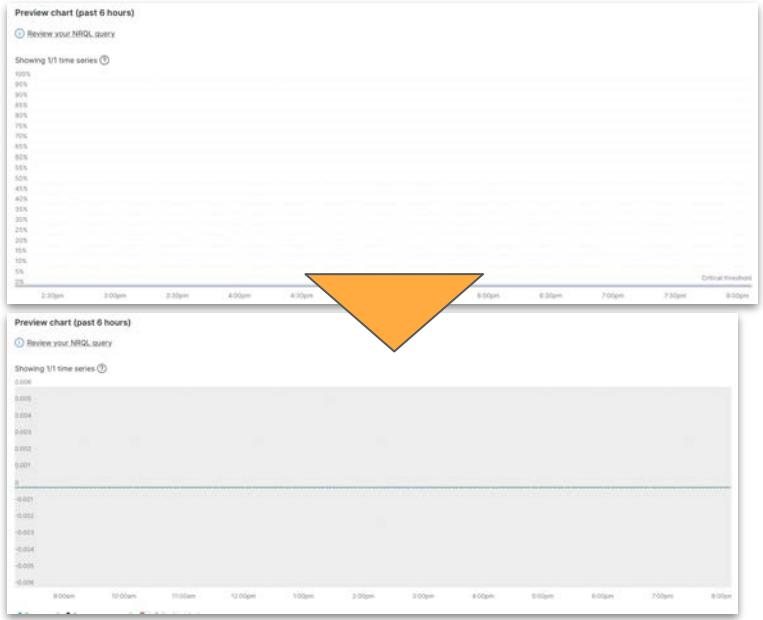
- クエリ実行後、直近の状態を示す参考チャートが表示されることを確認し、Nextをクリックする。



ハンズオン(2-1) Alert Conditionを作成する 14/21

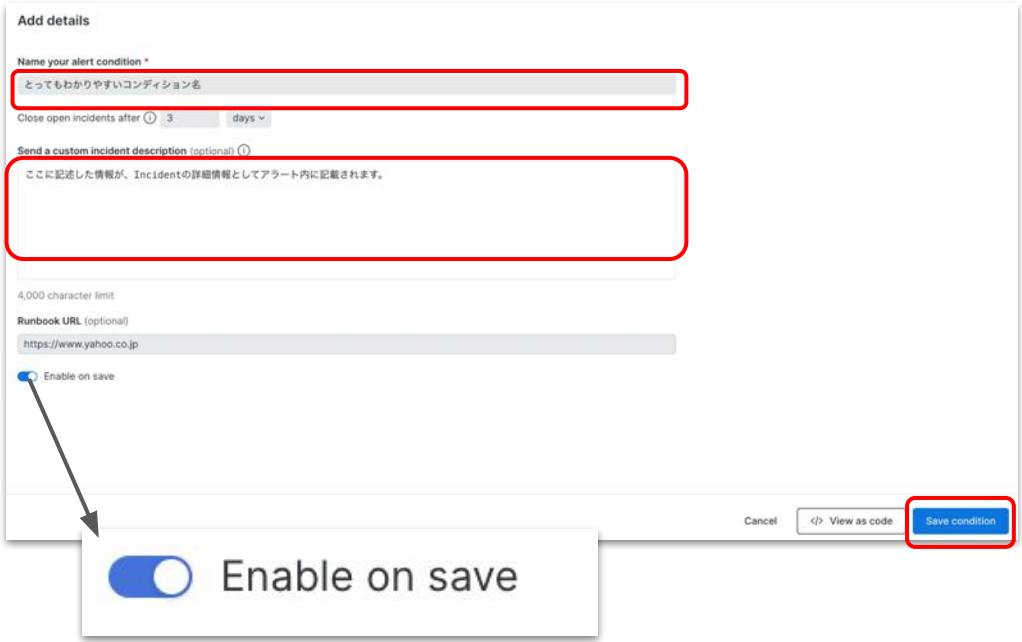
- Fine-tune your signalはすべて初期値のままNextをクリックします。
- 補足: もし時間がある場合は、閾値条件の設定項目にある「Static」を「Anomaly」に変更した場合、チャートがどのように変更されるかを確認してください。





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。
- 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

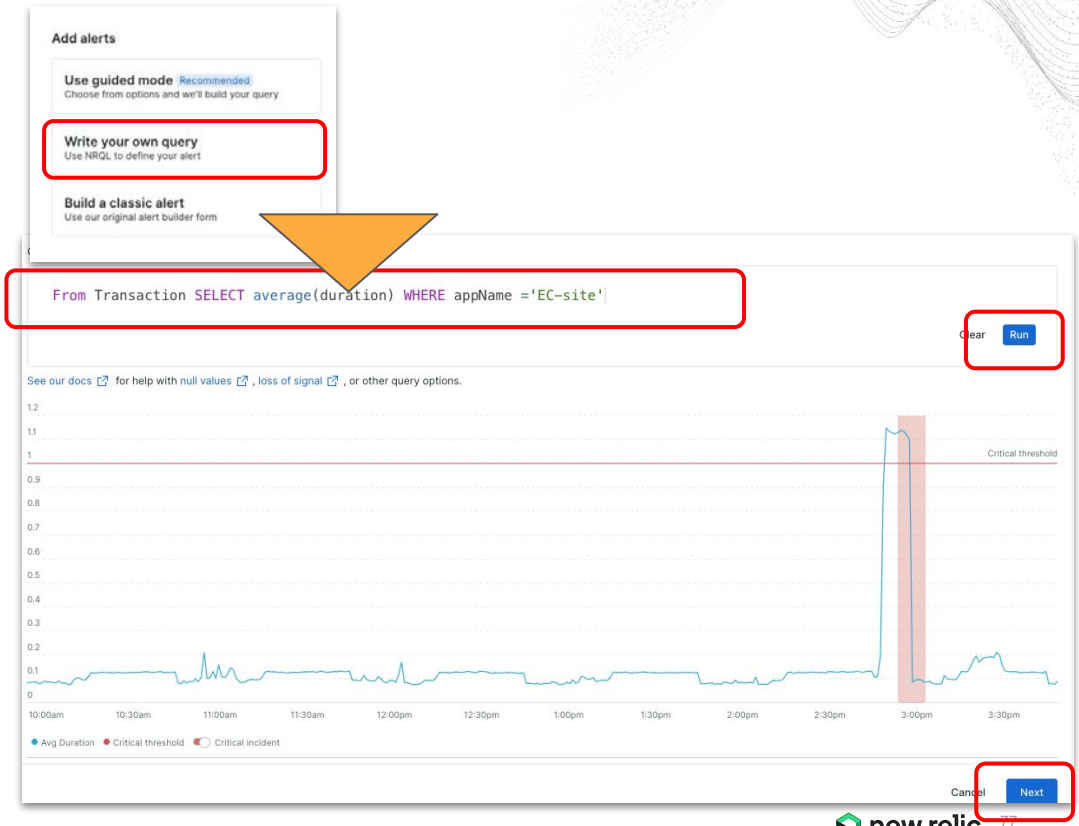
（例：NRU304-yourname-transaction-time-baseline）

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。

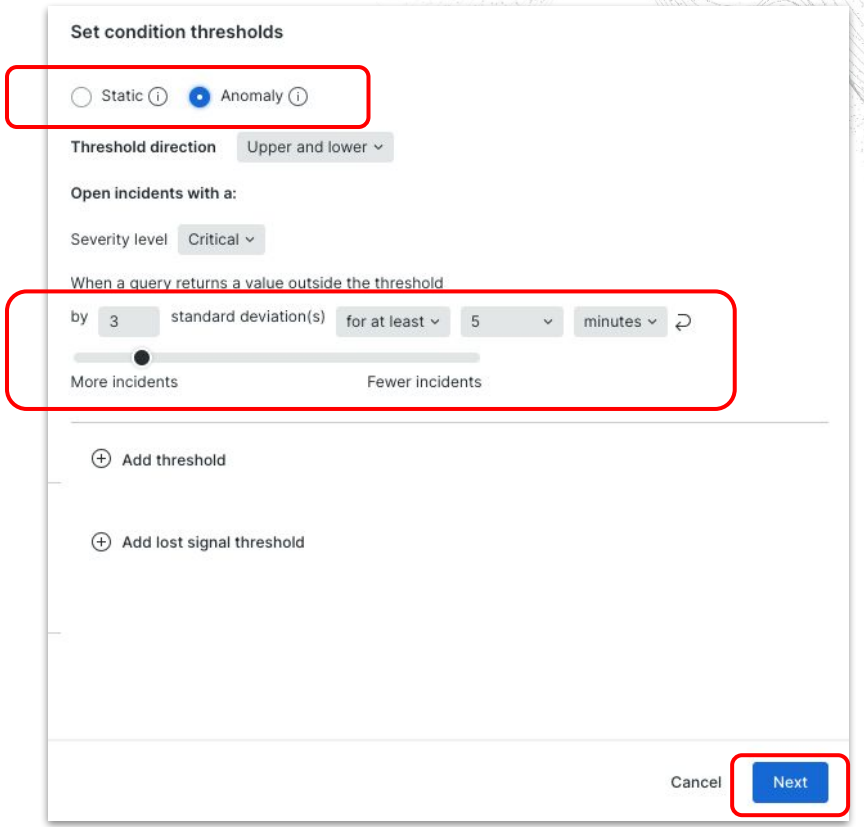
  From Transaction SELECT average(duration) WHERE appName ='EC-site'

- 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。
  - Fine-tune your signalの値は初期値のままにする。
- 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

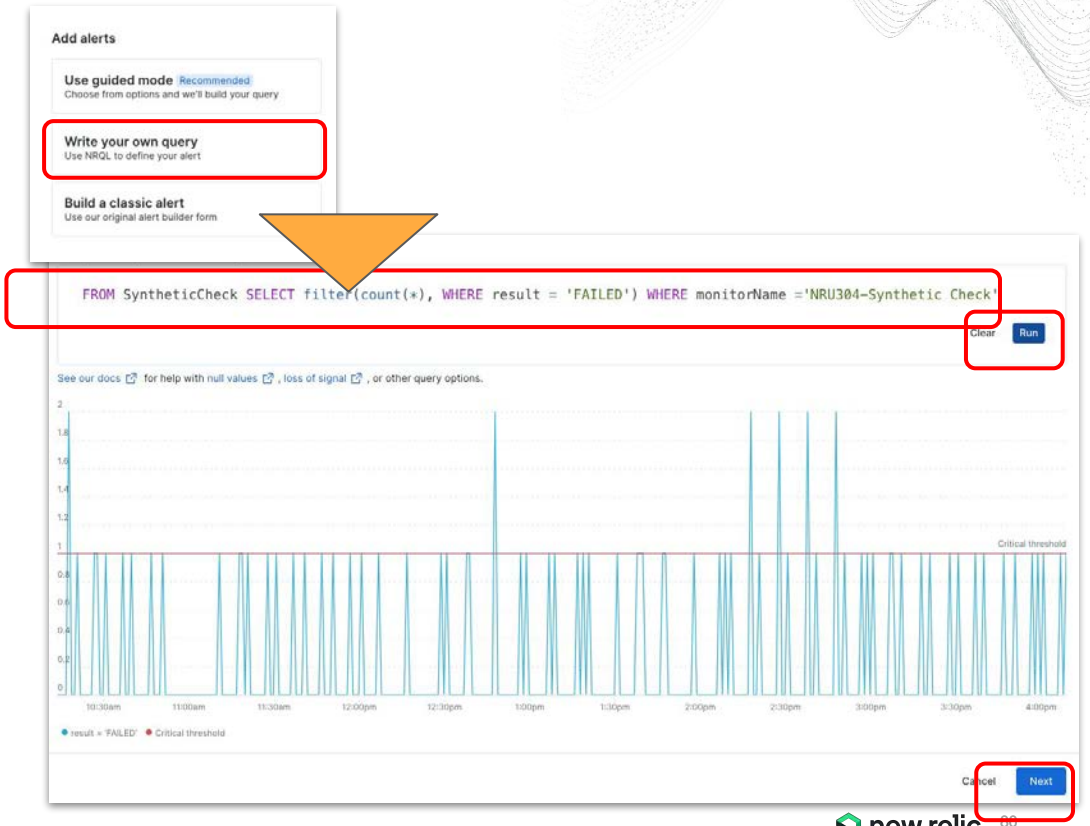
（例：NRU304-yourname-synthetics-check）

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。

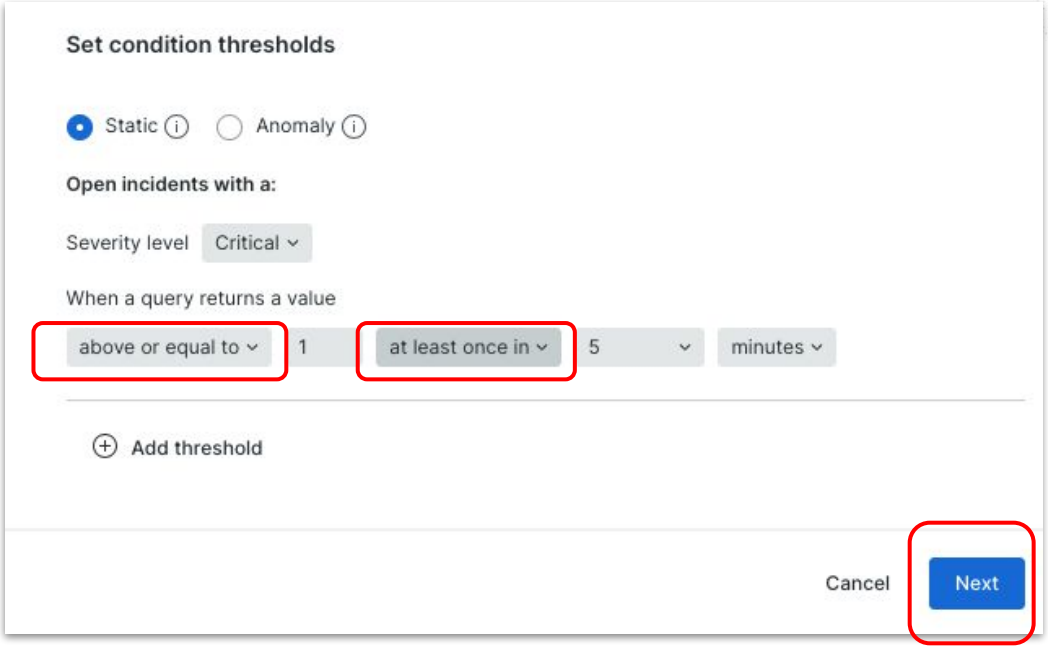
  FROM SyntheticCheck SELECT filter(count(*), WHERE result = 'FAILED') WHERE monitorName ='NRU304-Synthetic Check'

- 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。
  - Fine-tune your signalの値は初期値のままにする。
  - 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'
```

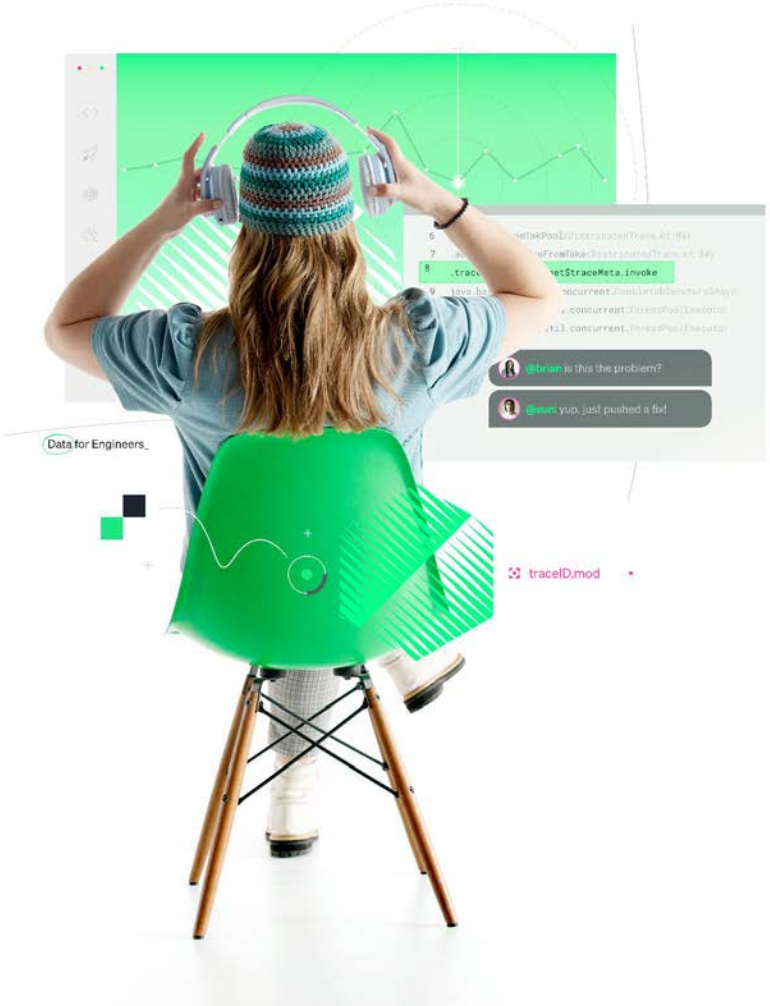
その場合**filter**関数の中で絞り込むことで評価対象にすることができます

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

参考：Example: null value returned

ハンズオン(3)
発生したアラートの確認

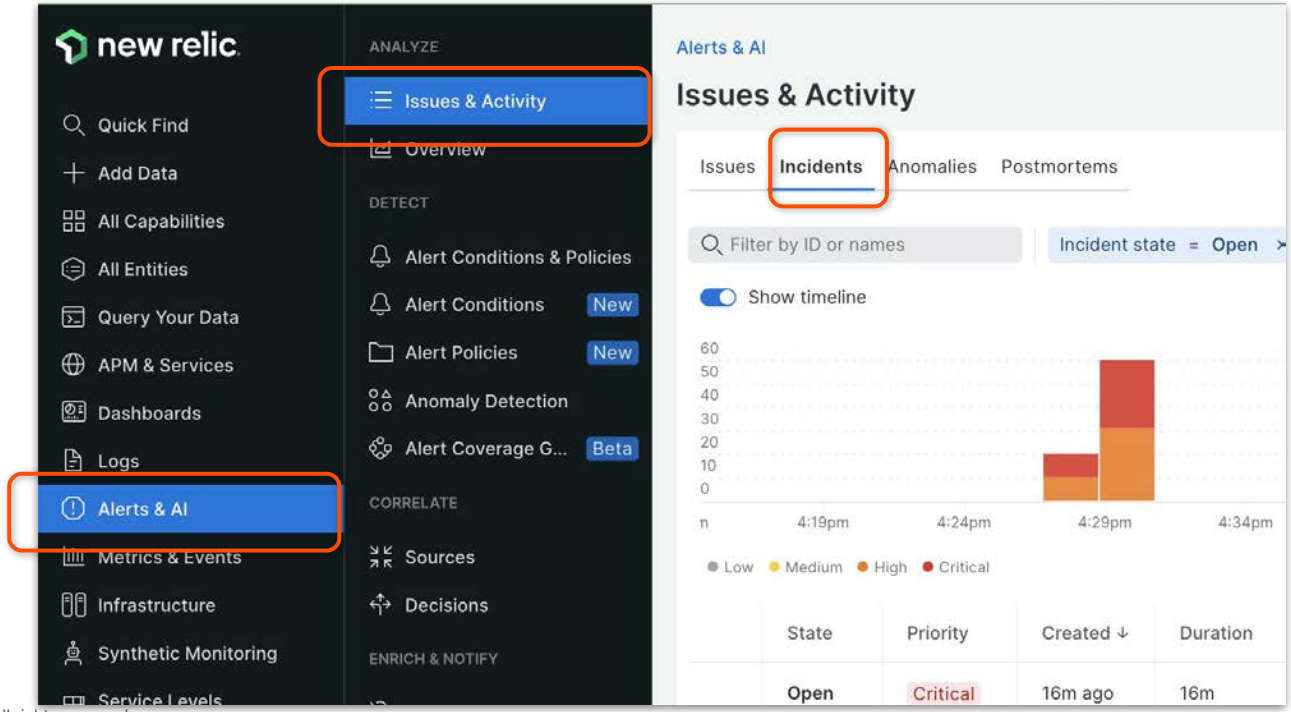
16:30 - 16:40 (10min)


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

手順・解説

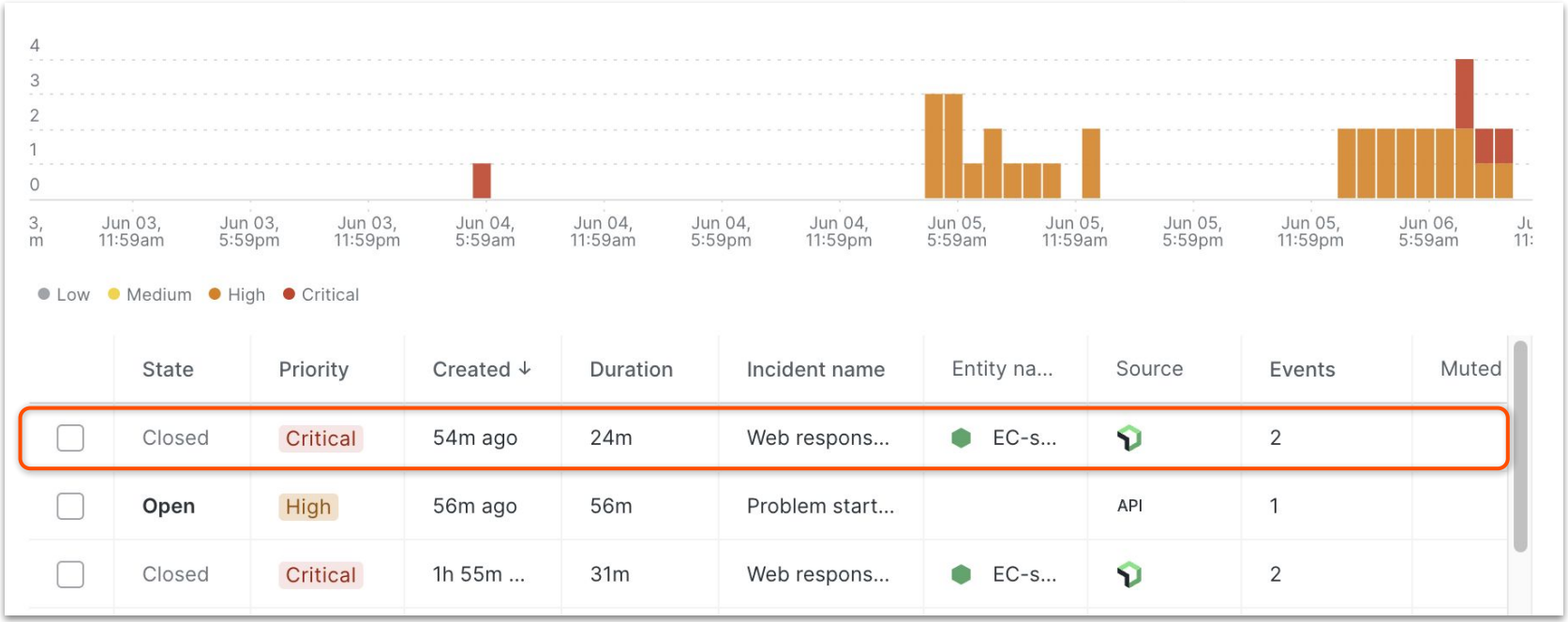
ハンズオン(3-1) 個々のアラートを確認する 1/3

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



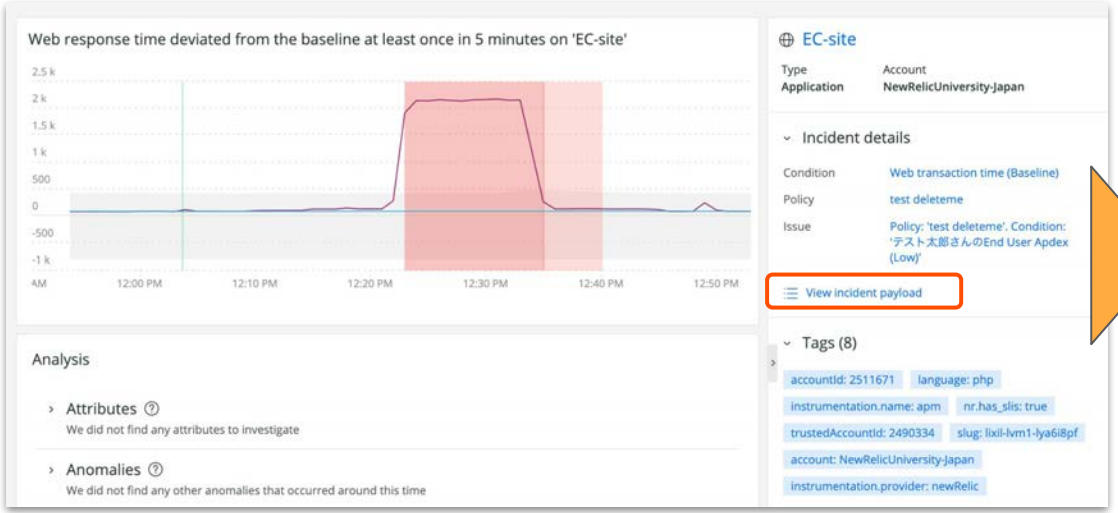
ハンズオン(3-1) 個々のアラートを確認する 2/3

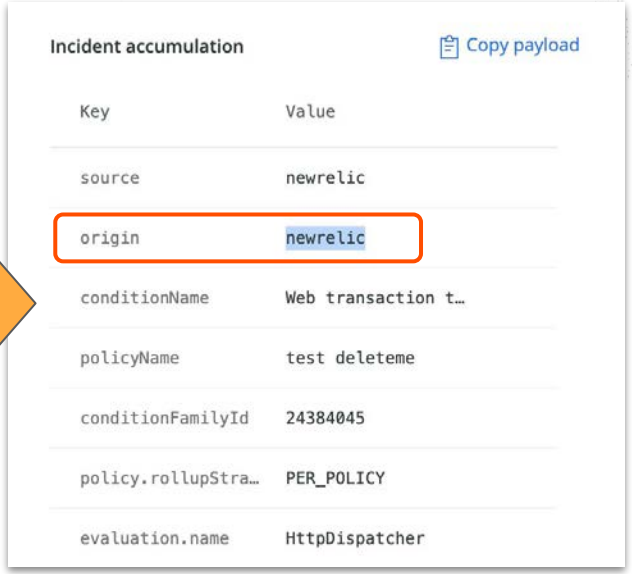
- Incidentをクリックします。



ハンズオン(3-1) 個々のアラートを確認する 3/3

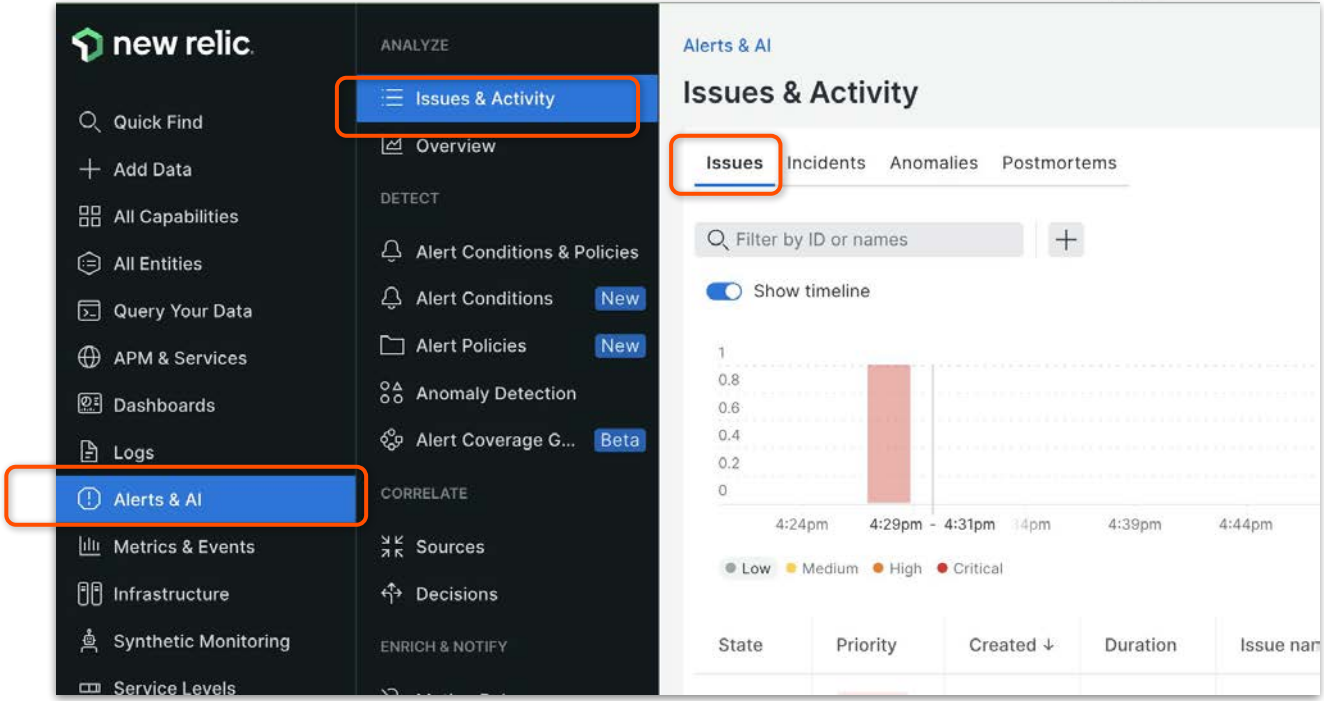
- Origin Key の値を確認することで、どのツールによって判定されたアラートかを確認することができます。





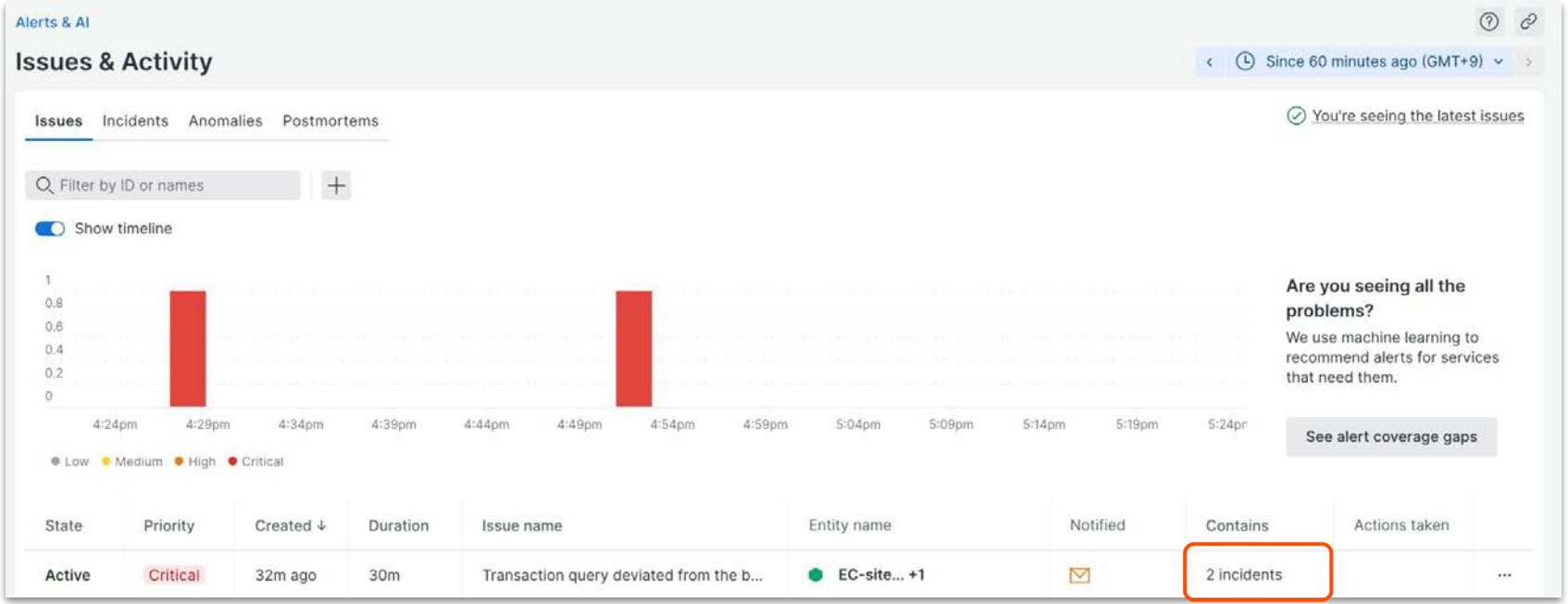
ハンズオン(3-2) 複数のアラートを紐付けトラブルシューティングに役立てる 1/5

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



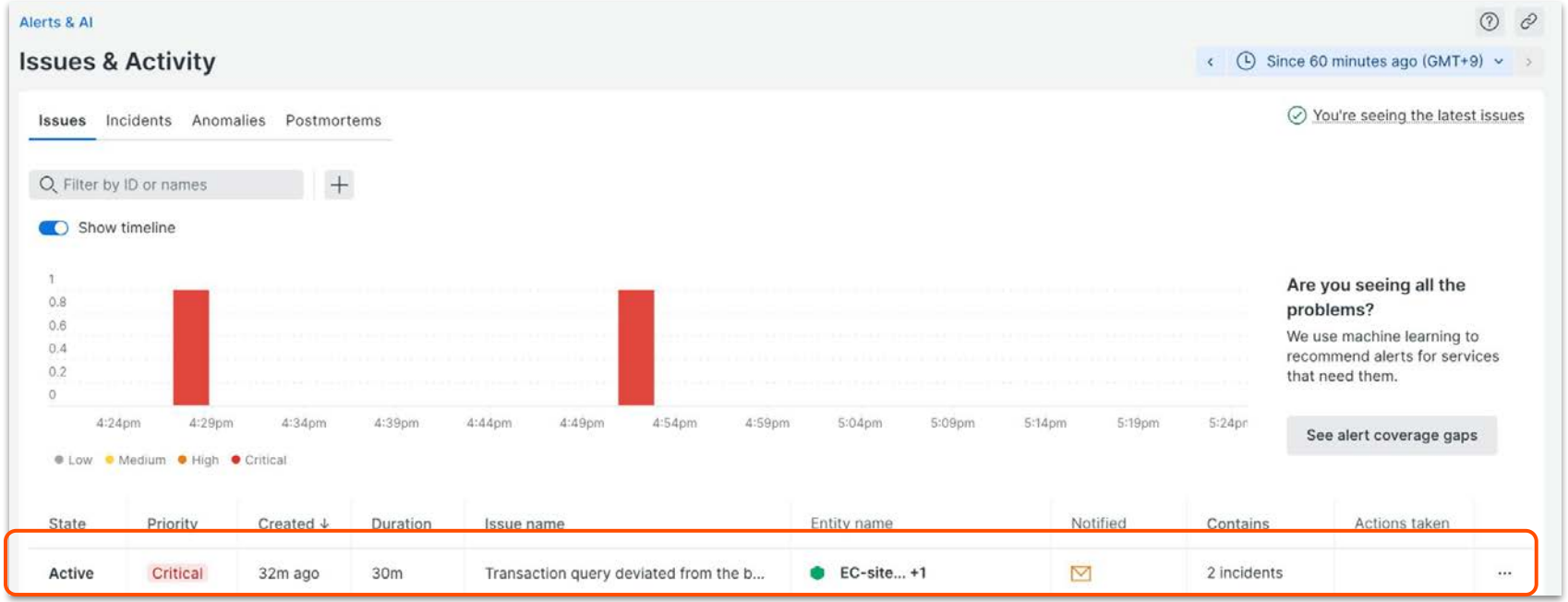
ハンズオン(3-2) 複数のアラートを紐付け トラブルシューティングに役立てる 2/5

- 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。



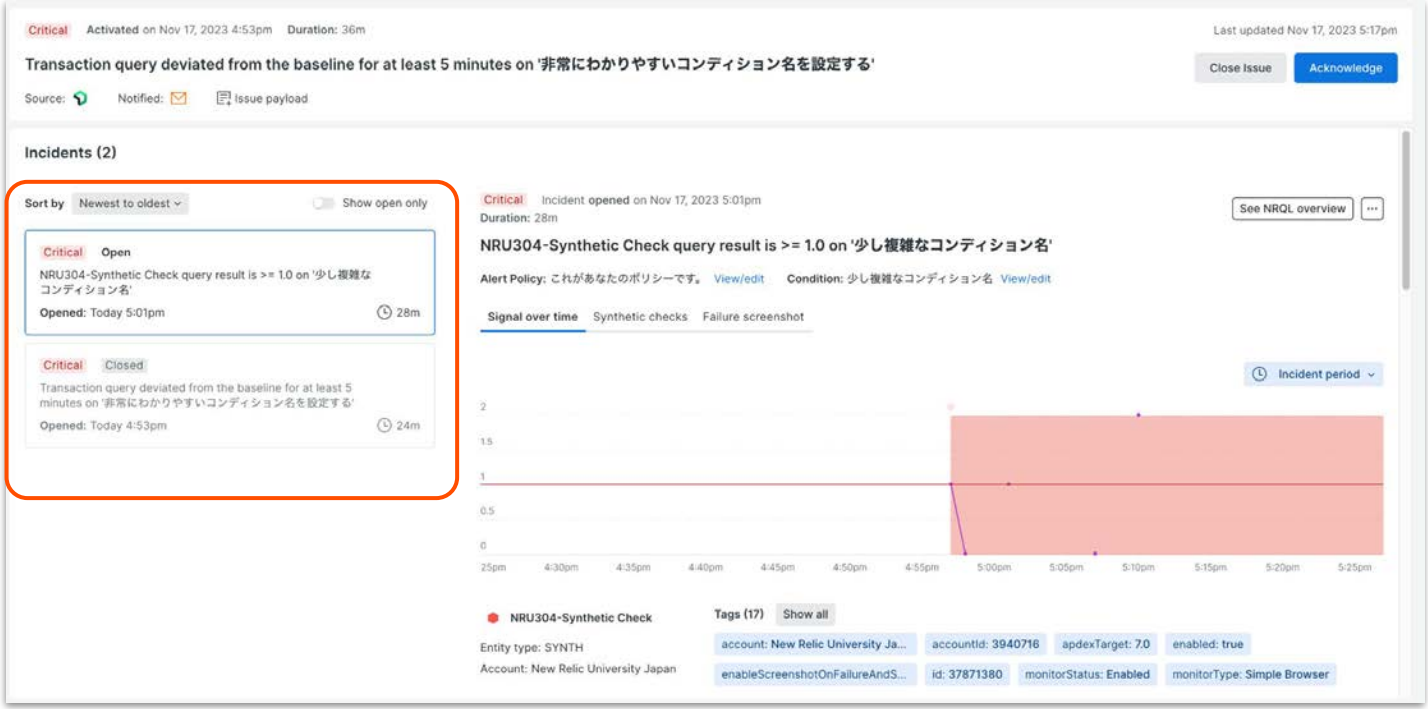
ハンズオン(3-2) 複数のアラートを紐付けトラブルシューティングに役立てる 3/5

- Issueをクリックすると詳細が表示されます。



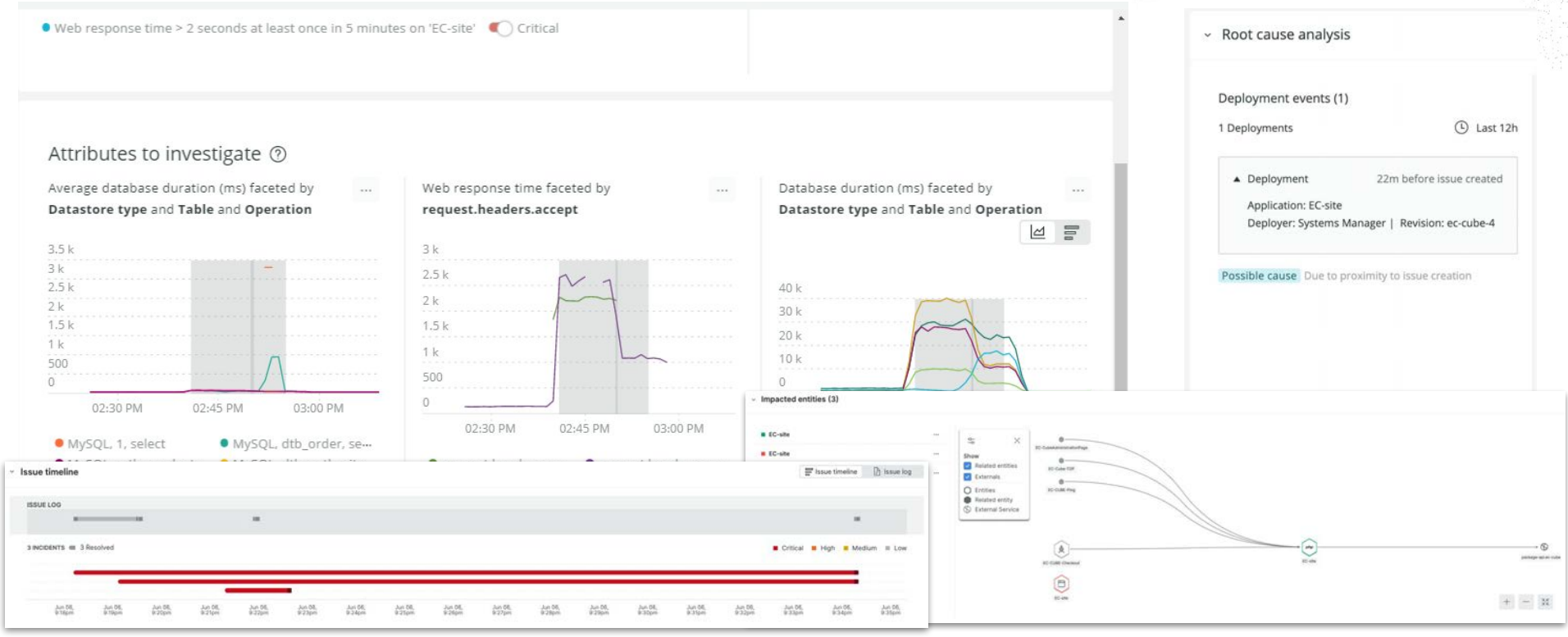
ハンズオン(3-2) 複数のアラートを紐付けトラブルシューティングに役立てる 4/5

- 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



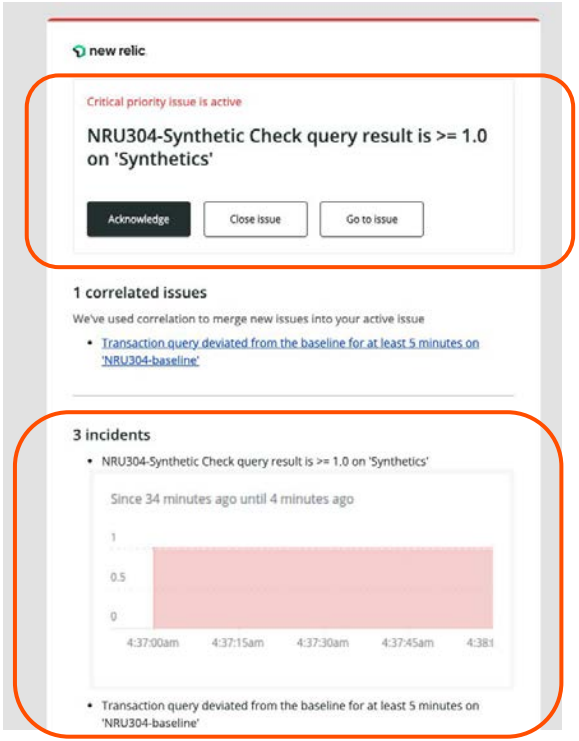
ハンズオン(3-2) 複数のアラートを紐付けトラブルシューティングに役立てる 5/5

- 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

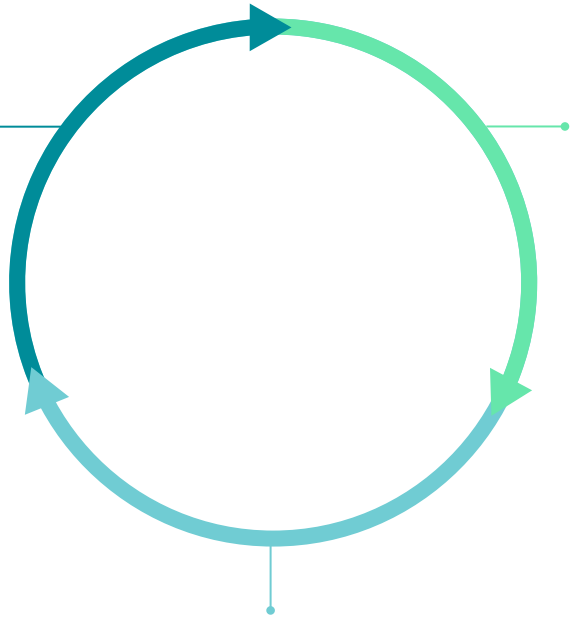


new relic

座学(4)
New Relicのアラート分析支援機能とAIOpsを使った異常検知

16:40 - 16:55 (15min)

New Relic AIOps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おこす

検知1: 重要な指標に対する手動アラートによる気づき

検知

手動 | 異常検知 (通知) | 異常検知 (探索)

↓

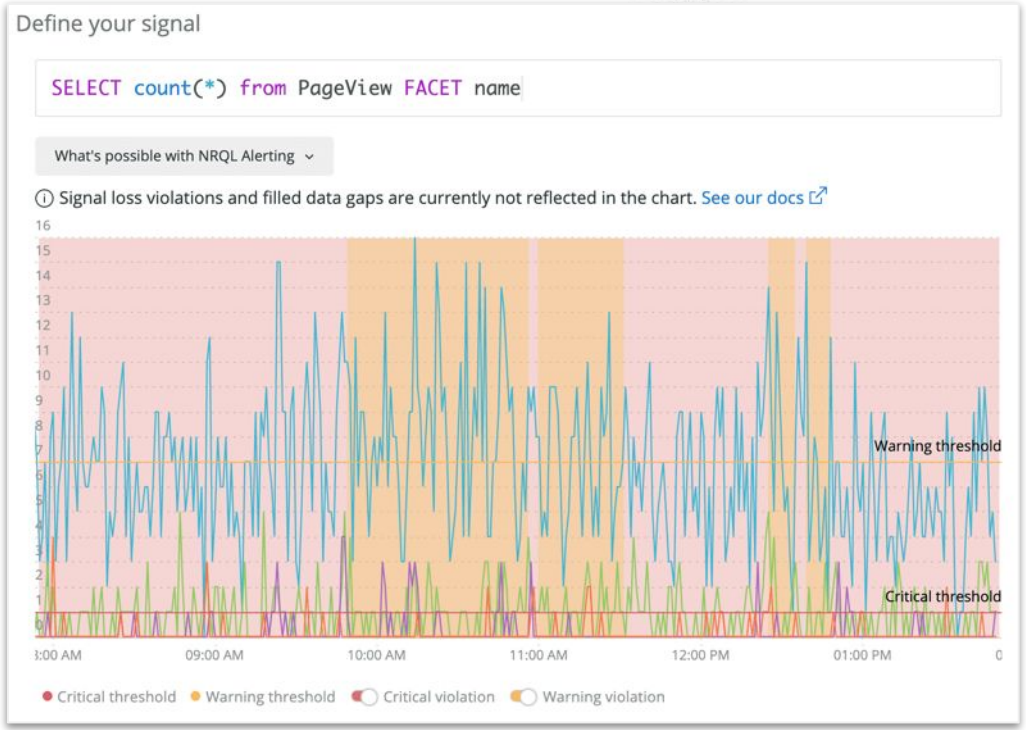
診断

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)



検知2: Anomaly Detectionによる異常の通知

検知

手動　**異常検知（通知）**　異常検知（探索）

↓

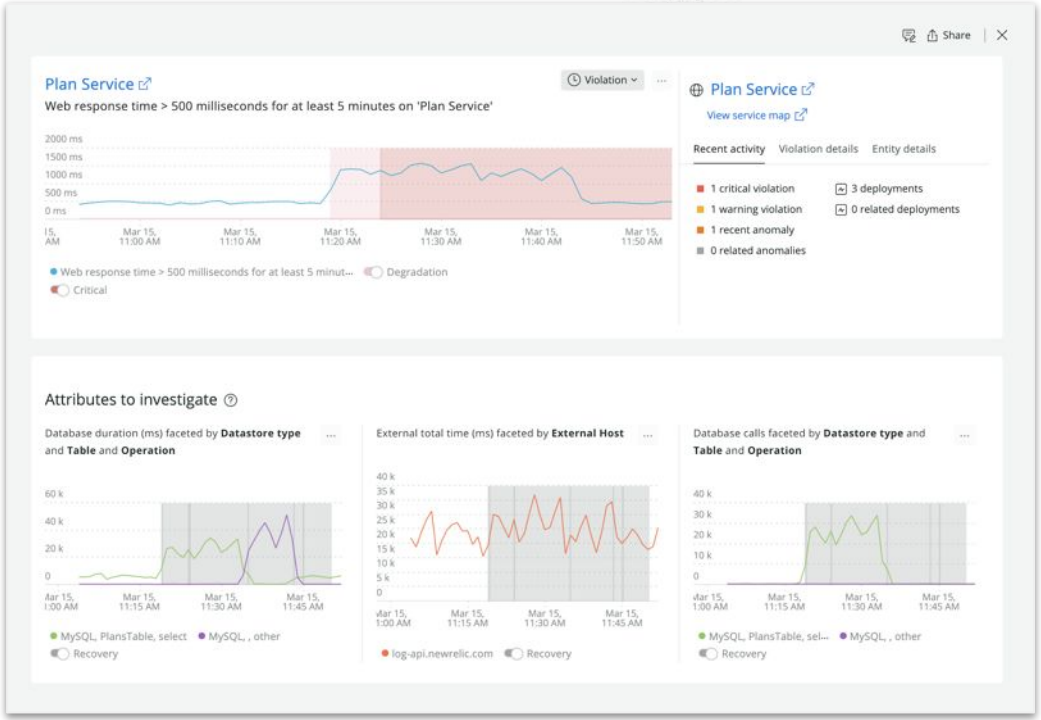
診断

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）



検知3: Lookoutによる異常の可視化と探索

検知

手動

異常検知
(通知)

**異常検知
(探索)**

↓

診断

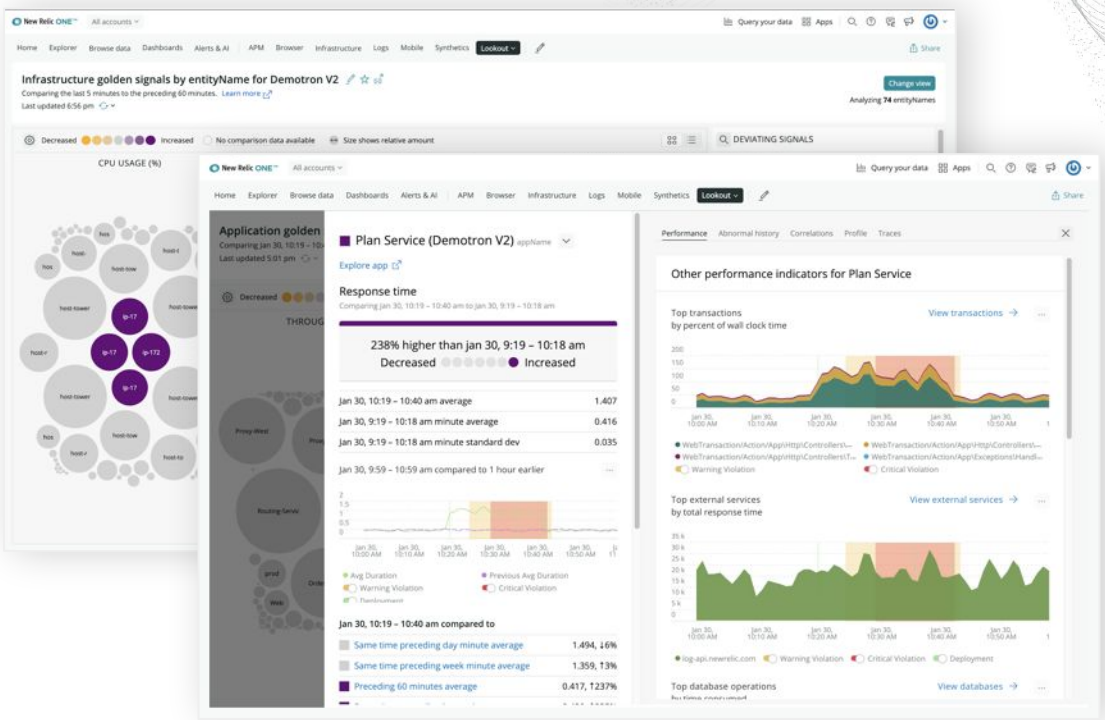
イベントの相関分析

根本原因分析

↓

対処

(外部ITSMツール: Servicenow, Pagerduty等)



診断1: Correlationによるアラート統合とノイズの削減

検知

手動

異常検知
(通知)

異常検知
(探索)

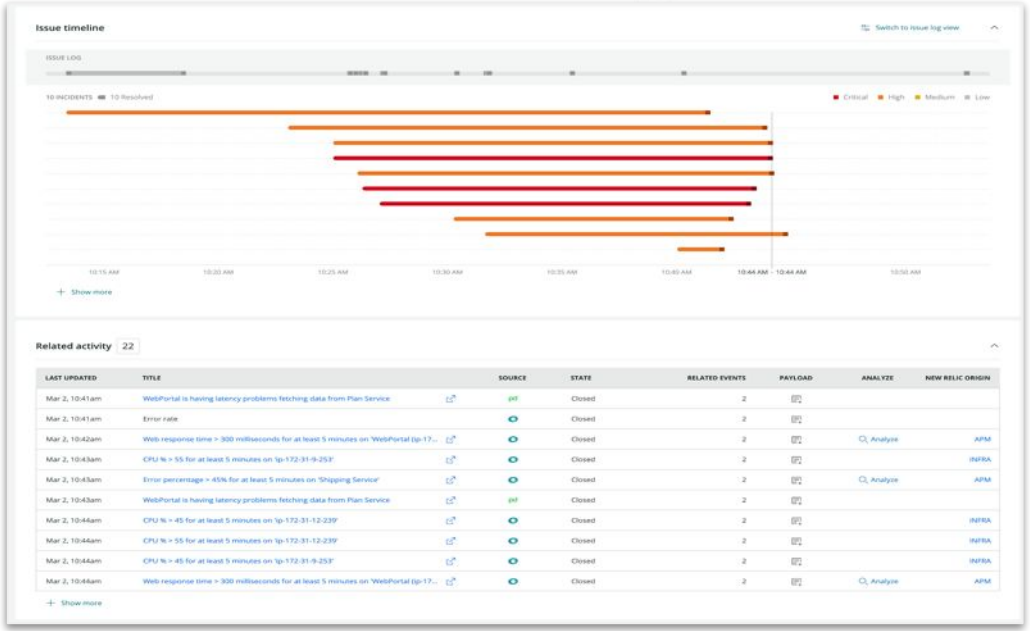
診断

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)



診断2: Correlationによる根本原因の示唆

検知

手動

異常検知
(通知)

異常検知
(探索)

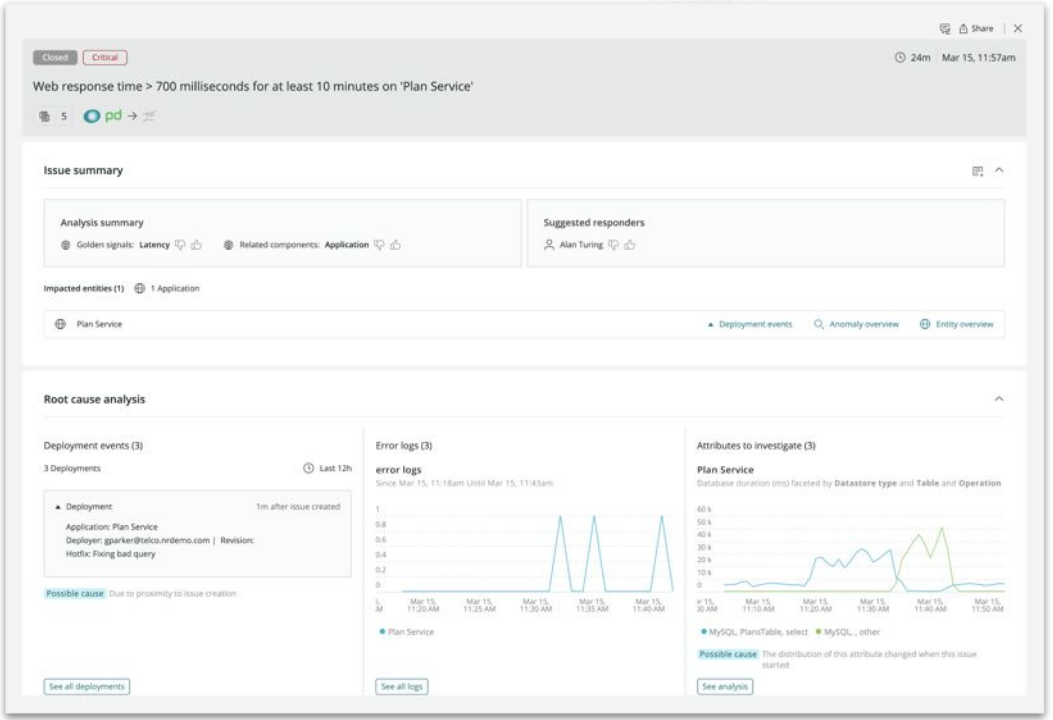
診断

イベントの相関分析

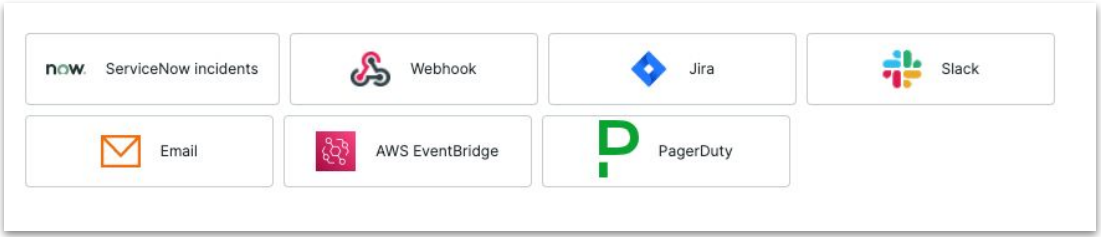
根本原因分析

対処

(外部ITSMツール: Servicenow, Pagerduty等)



対処: ITSMツールと連携しアクションを実行



ITサービスに発生しうる障害と監視の関連性

ITサービスに発生しうる障害	理解できる	理解できない
気づける	**Actionableな監視** 気づいたあとに正しく対処ができる (例. ユーザーが特定の機能を使えない)	**とりあえずの監視** 気づいても対処につなげられない (例.インフラのリソース使用率上昇)
気づけない	**Actionableな監視予備群** 障害発生して後手対応になったが、原因がわかったので次回から監視で気づける	**監視できていない未知の領域** 障害発生したが原因がわからず監視もできない

従来の監視のアプローチ

運用スペシャリストがログから気合いで分析
のちのち手順化

ITサービスに
発生しうる障害

	理解できる	理解できない
気づける 頑張ってすべての障害ポイントを洗い出す	**Actionableな監視** 努力と根性と属人性で Actionableな監視を増やす	**とりあえずの監視**
気づけない	**Actionableな監視予備群**	**監視できていない未知の領域**

AIOpsとは

ガートナーによる定義

https://www.gartner.com/en/information-technology/glossary/aiops-artificial-intelligence-operations

AIOpsとは、IT運用プロセスを自動化するためにビッグデータと機械学習を紐付けたものであり、以下のような機能を含む:

1. *異常検知*
2. *イベントの相関分析*
3. *根本原因分析*

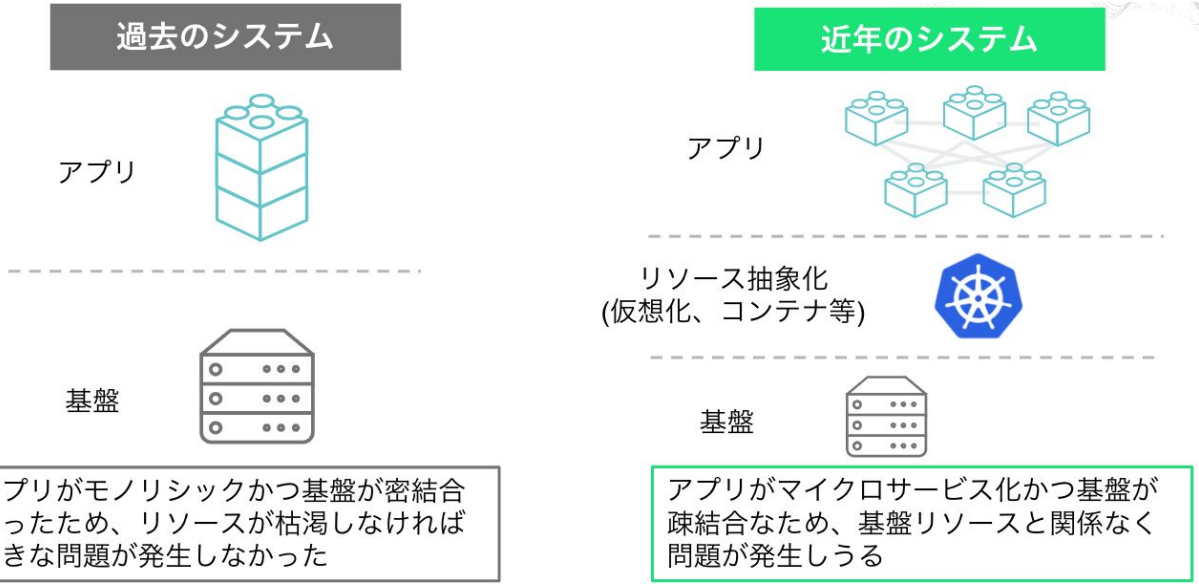
New RelicのAlerts & “**AI**”

→ **Applied Intelligence**
応用知能:機械学習によって得たデータを元に運用をアシスト

AIOpsが必要とされる背景

1. モノリスからマイクロサービスへ

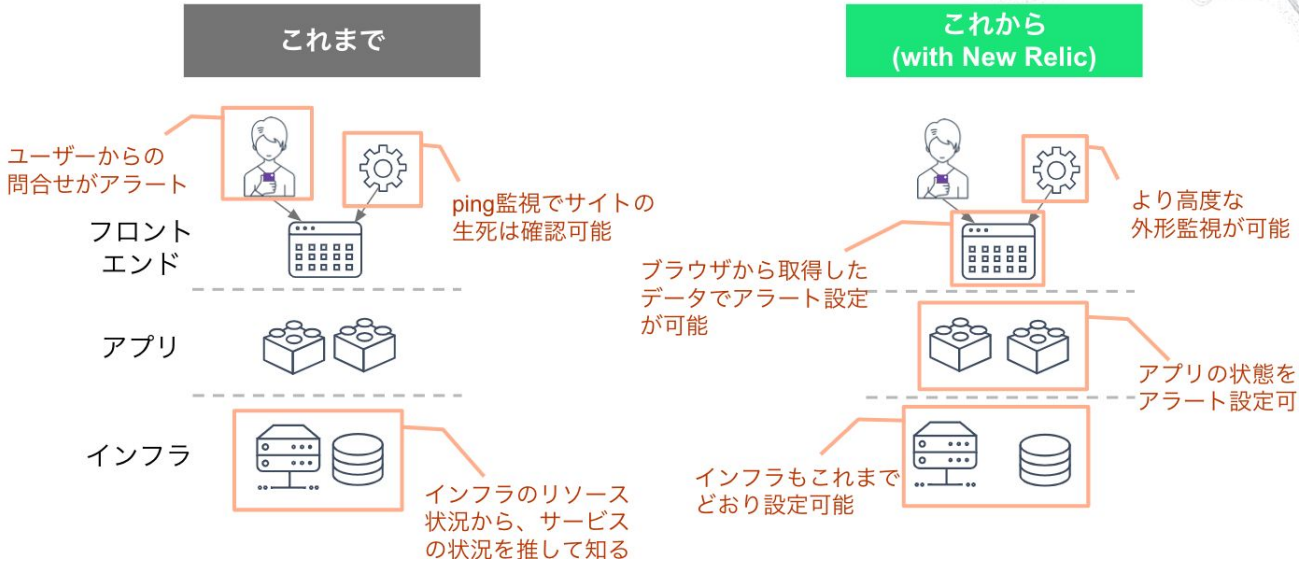
監視対象となるコンポーネントの絶対数が増えると同時に、コンポーネント同士の関連性がより複雑に



AIOpsが必要とされる背景

2. 捕捉できるデータの増加と多様化

New Relicのようなオブザーバビリティプラットフォームによって、サービスを構成する様々なコンポーネントから多種多様なデータを取得できるように



監視にまつわる新たな課題

アラートを1つ1つ網羅的に
設定するのか問題

大量のアラートをどう解釈してトラ
シューするのか問題

従来の監視の限界

ITサービスに
発生しうる障害

理解できる

理解できない

気づける

Actionableな監視

人力でこの面を増やすのは困難

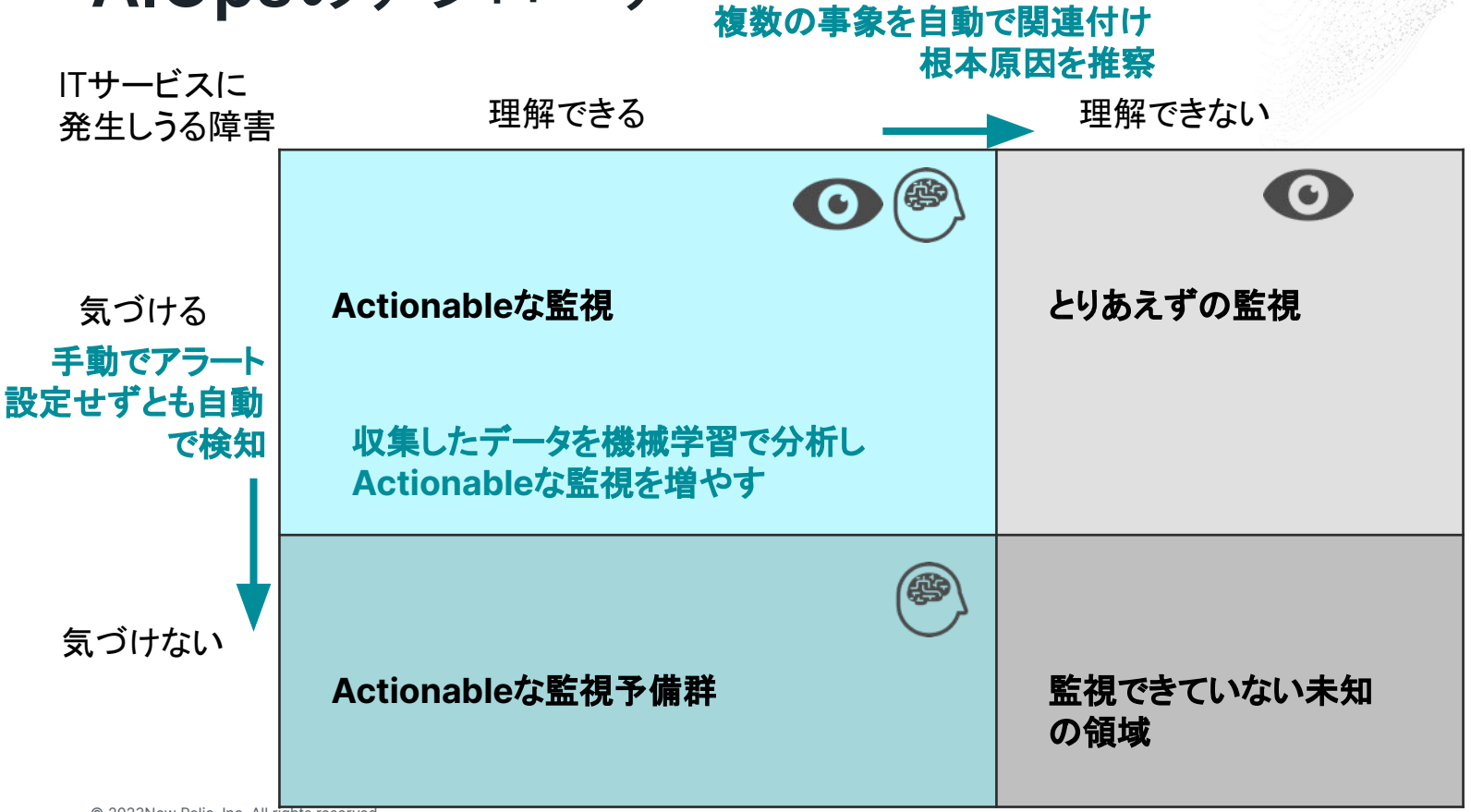
とりあえずの監視

気づけない

Actionableな監視予備群

監視できていない未知の領域

AIOpsのアプローチ



AIOpsによってサービスの信頼性を高める

アラートを1つ1つ網羅的に
設定するのか問題

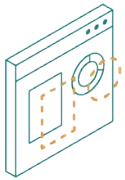
[解決するAIOpsの機能]
- 異常検知

手動でアラート設定せずとも自動で検知

Anomaly Detection
Alert coverage gaps

大量のアラートをどう解釈してトラ
シューするのか問題

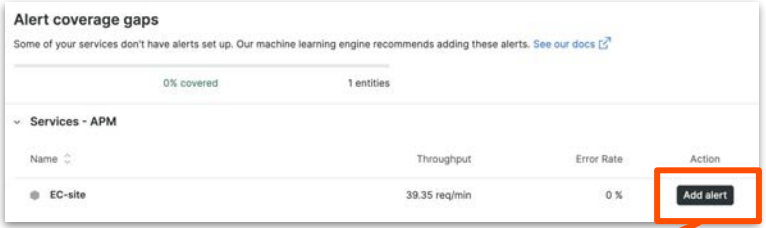
[解決するAIOpsの機能]
- イベントの相関分析
- 根本原因分析



複数の事象を自動で関連付け、根本原因を推察

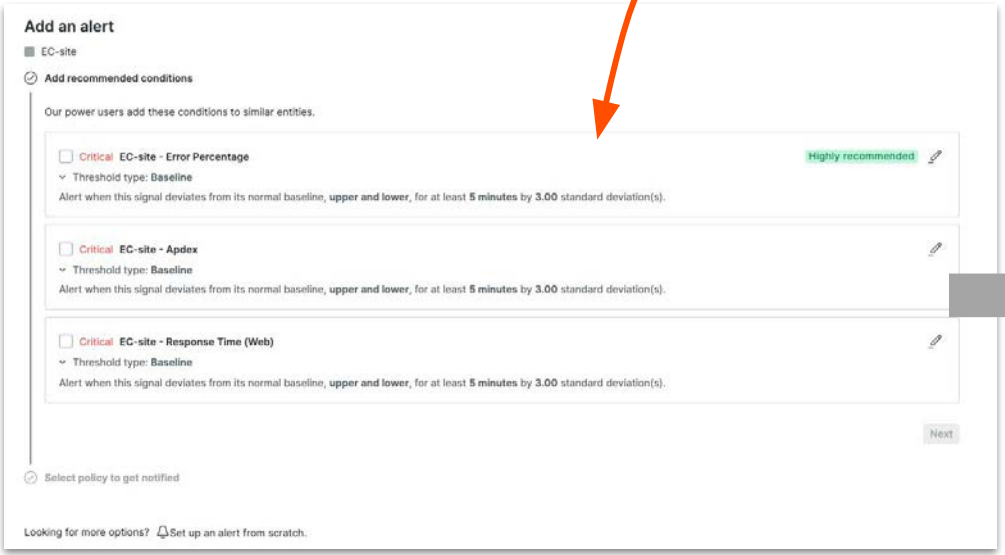
Correlation
Root Cause Analysis

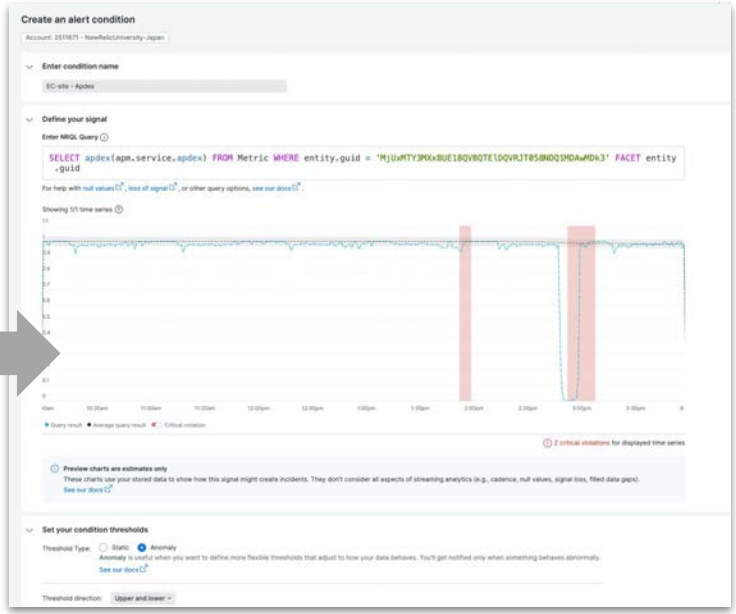
機能紹介: Alert coverage gaps



設定すべきアラートを通知します。

現行ではAPMのみを対象としています。

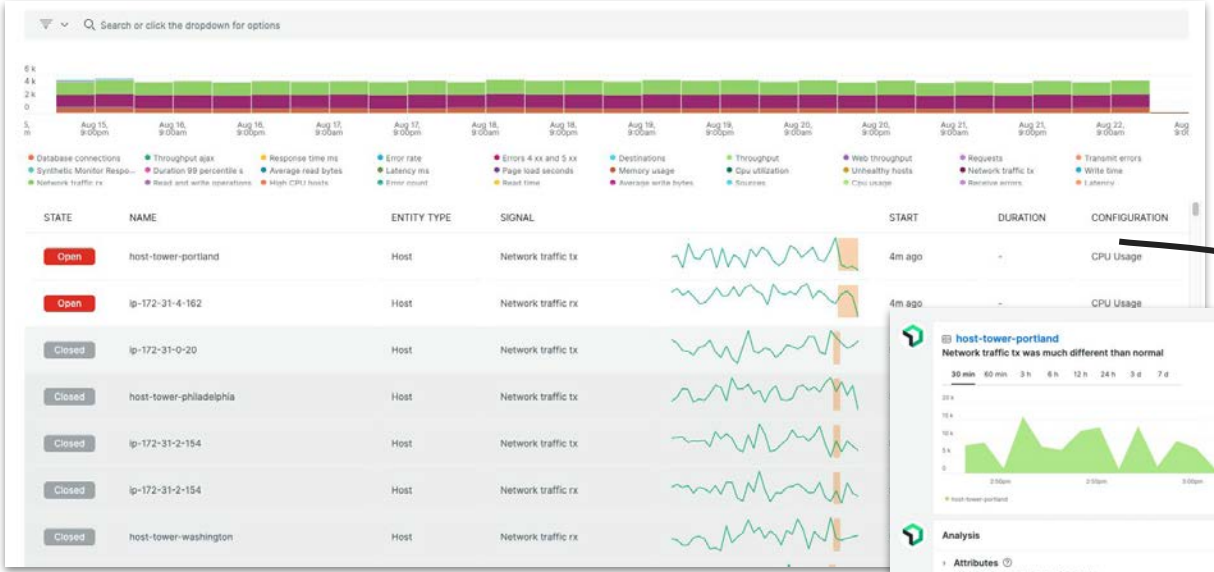


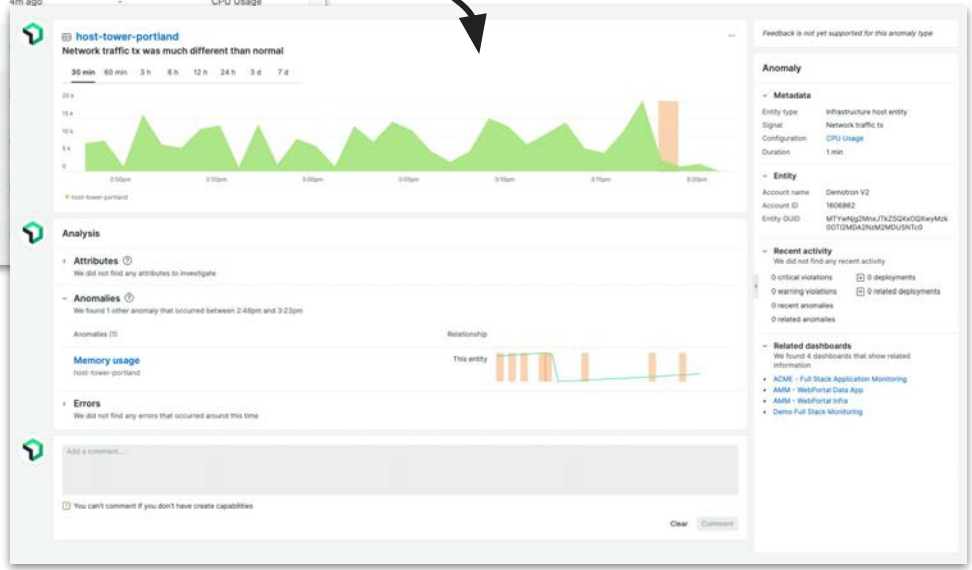


Alerts & AI → Alert coverage gaps

new relic

機能紹介: Anomaly Detection





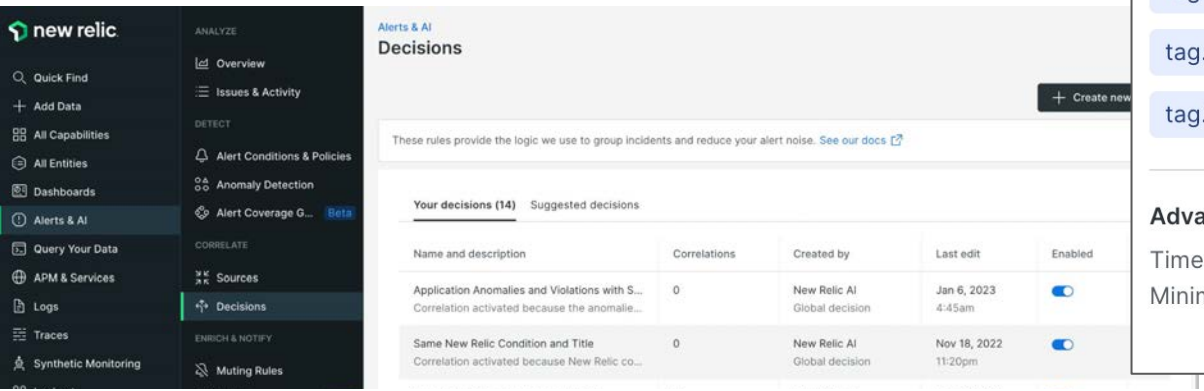
Alerts & AI → Issues & activity → Anomalies

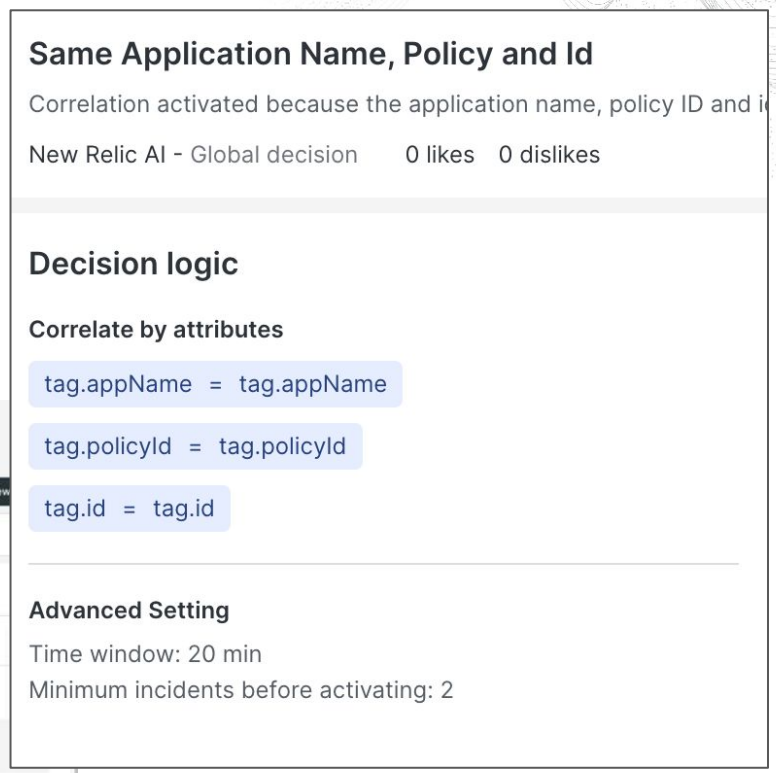
- 発生したAnomalyの1つを選択し、詳細を確認する

機能紹介: Correlate (Decisions)

Alerts & AI → 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

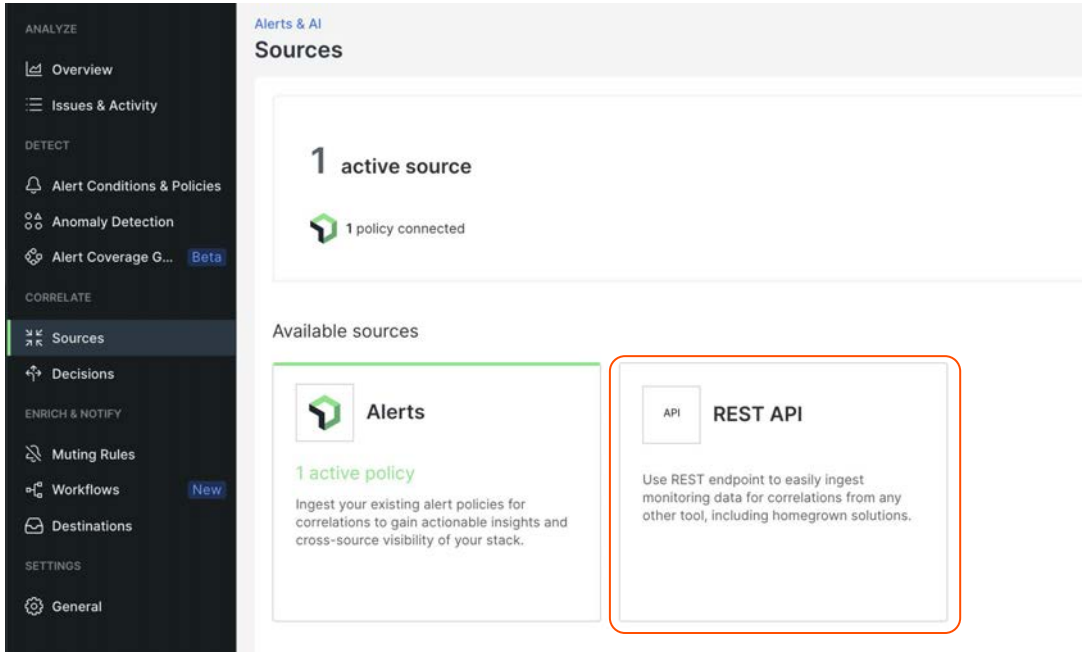




new relic

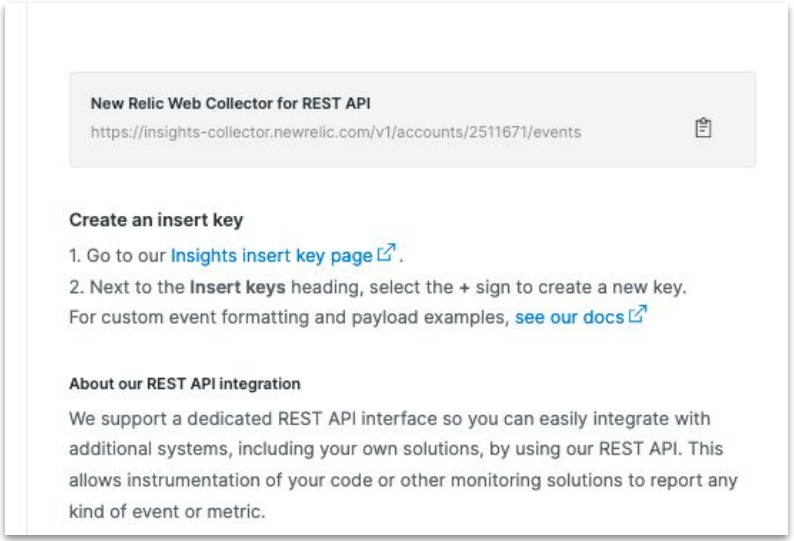
参考：Zabbixの連携1

- ZabbixからNew Relicへのアラート連携にはREST APIを利用しています。



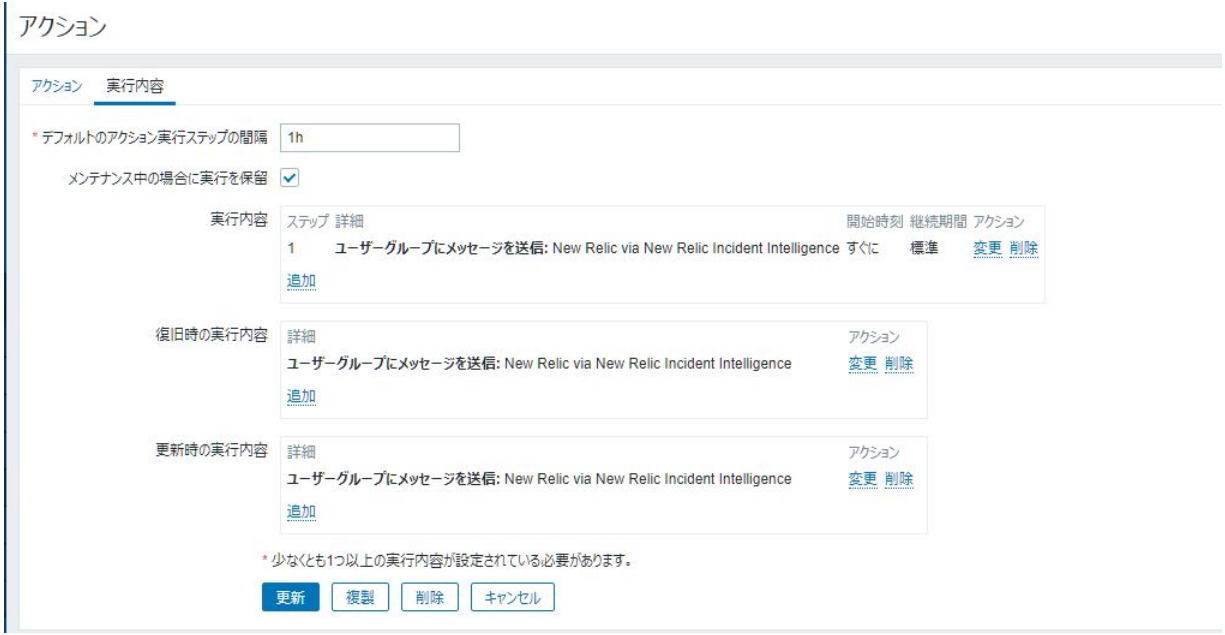
参考：Zabbixの連携2

- API URLとInsights Insert keyを作成し、それをコピーして Zabbix側に登録します。



参考：Zabbixの連携3

- ZabbixのトリガーアクションでメディアタイプNew Relic Incident Intelligenceを呼び出します。

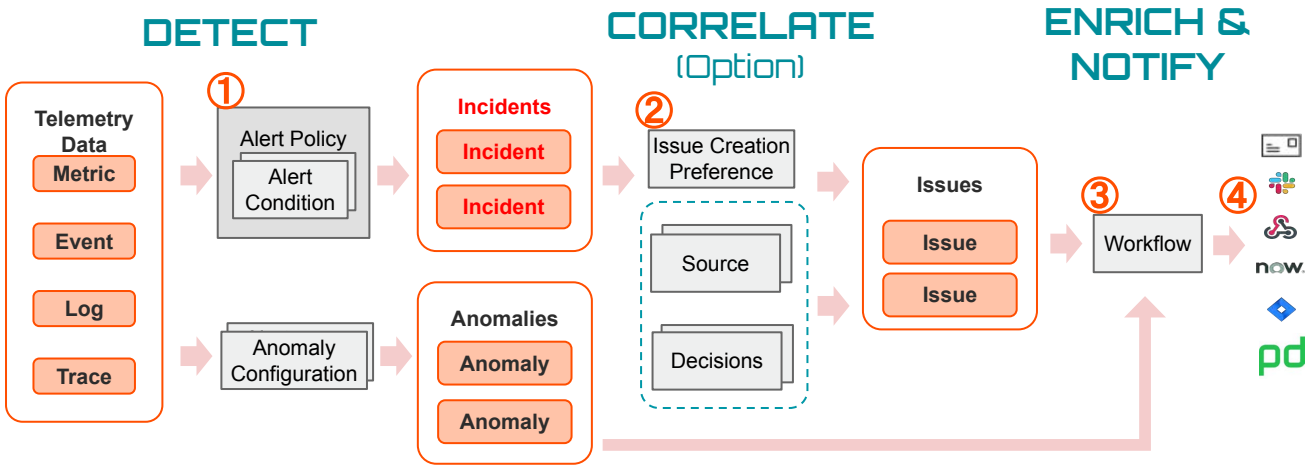


まとめ

new relic

まとめ

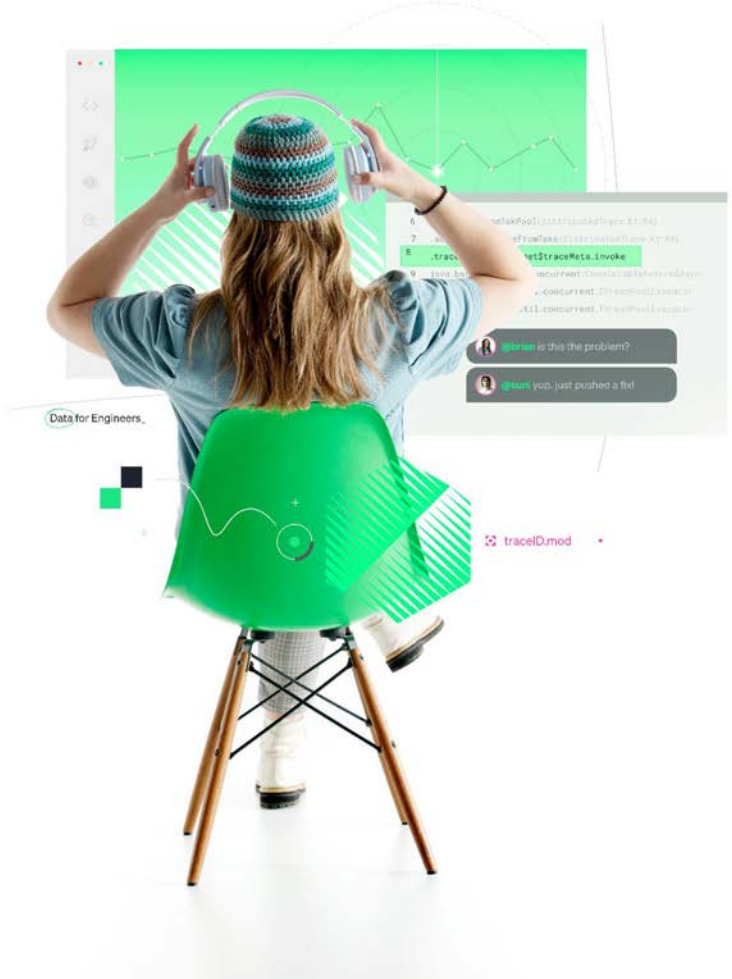
- **ユーザー体験に近い指標でアラートを設定しよう**
  - インフラ監視だけではサービスの異常に気付くには不十分
- **New Relicのアラート構造と設定方法を理解しよう**



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

new relic.

お疲れ様でした！



New Relicを個人で試してみよう。

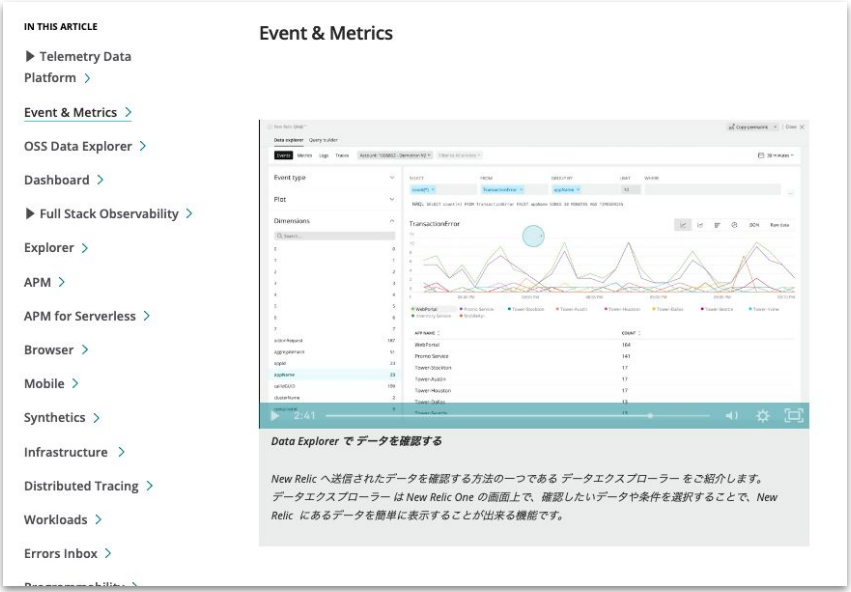
無料サインアップは https://newrelic.com/jp/sign-up-japan より
手順はこちら。

- 100GB/月まで一生無料
- New Relic の オブザーバビリティ機能を試せる
- FSOユーザー1名つき！
- クレジットカード不要

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 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

▸インストールガイド

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

▸オンデマンドセミナー (**practitioner**), (**nru101**)

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54の機能群を動画で説明

NRU201 Telemetry Data Platform

NRU202 Full Stack Observability

NRU203 Applied Intelligence

▸主要機能解説動画

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

▸開催スケジュール

Exam

資格を得る

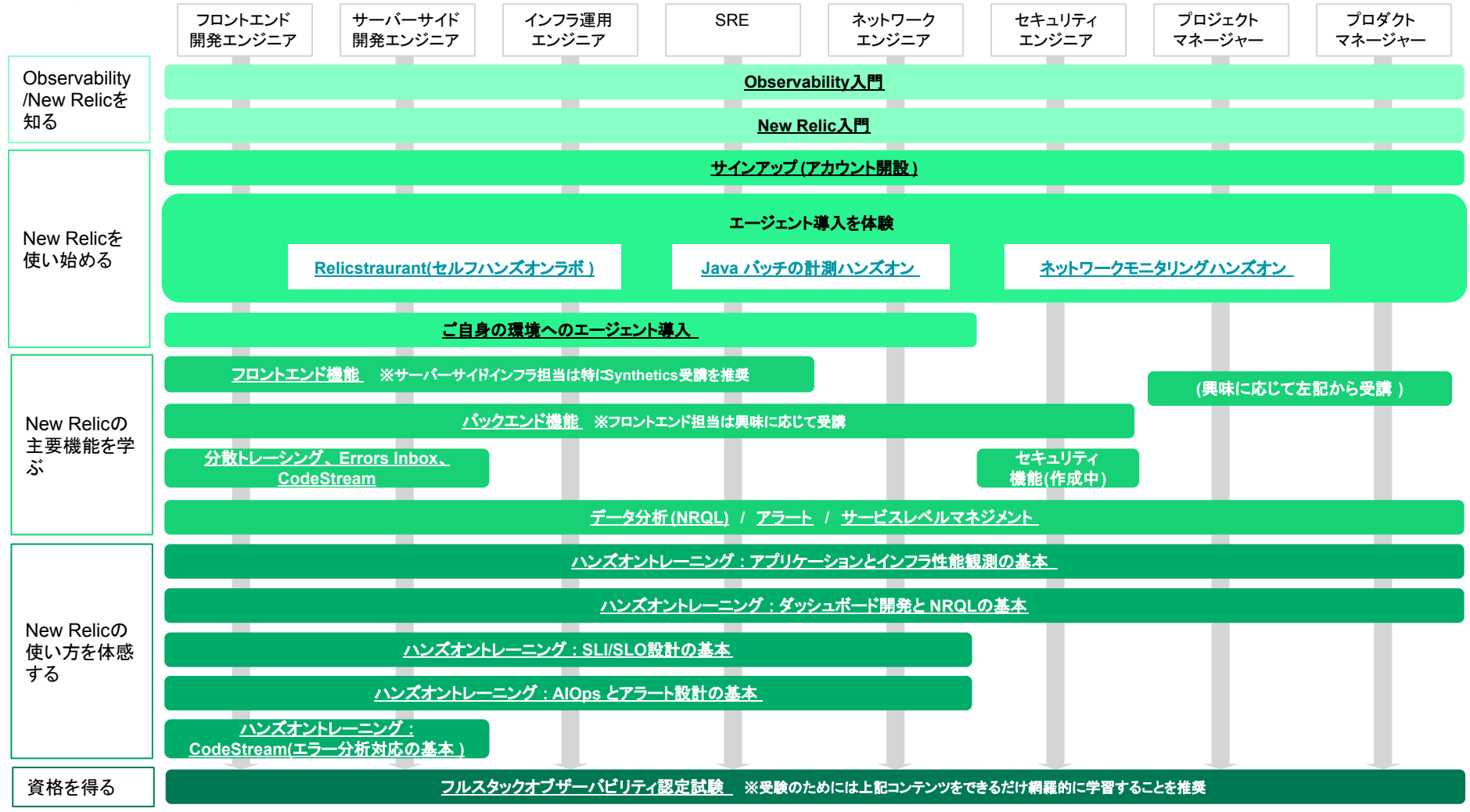
New Relicの知識を有していることを証明するための試験、合格すると資格バッジを授与

フルスタックオブザーバビリティ認定試験

▸受験サイト

new relic

ロール別 New Relic ラーニングパス



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。
(https://nrug.connpass.com/)

本当にお疲れさまでした。

new relic

最後となりますが、
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**アンケートにご記載**ください。

Thank you.