NRU 304
「AIOps とアラート設計の基本」

June 7, 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。

① 画面下
「Q&A」をクリック！

② こちらにご質問をご記入し、
「送信」をクリックしてください！

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

New Relic 株式会社

技術統括 テクニカルサポート部

三井 翔太 / Shota Mitsui

Senior Technical Support Engineer

→ HAクラスター製品のQAエンジニア

→ 国内SIer AWSインフラエンジニア（構築・運用設計）

→ 国内SIer AWS再販顧客向けのテクニカルサポート

→ 2022年8月～ New Relic テクニカルサポート

得意カテゴリ Infrastructure, Alerts & AI

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
15:15-15:40	座学(2)	New Relicのアラート機能
15:40-15:50	ハンズオン(0)	環境を確認する
15:50-16:10	ハンズオン(1)	アラートを作成する
16:10-16:20	座学(3)	New Relicのアラート分析支援機能
16:20-16:30	ハンズオン(2)	New Relicのアラート分析支援ウォークスルー
16:30-16:45	座学(4)	AIOpsの意義
16:45-16:55	ハンズオン(3)	AIOpsを使った異常検知と原因分析
16:55-17:00		まとめ、アンケートご記入

new relic

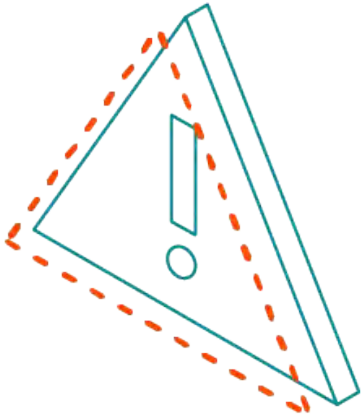
座学(1)
ユーザー視点のアラート

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)

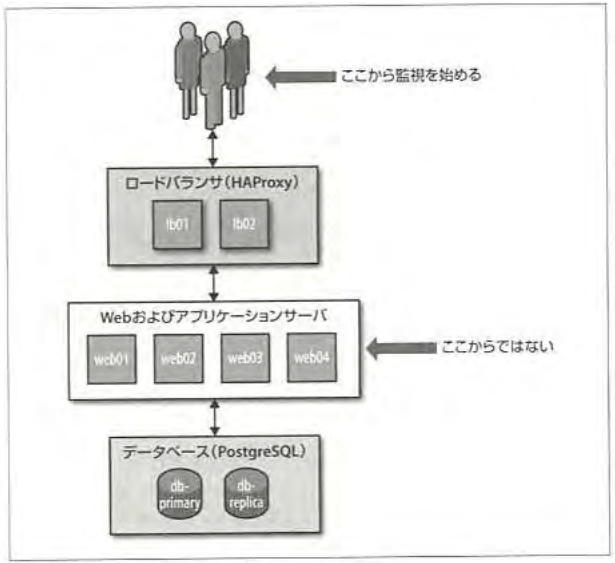
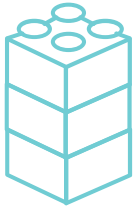


図2.1 できるだけユーザに近いところから監視を始める

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

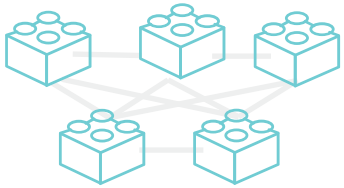


基盤

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



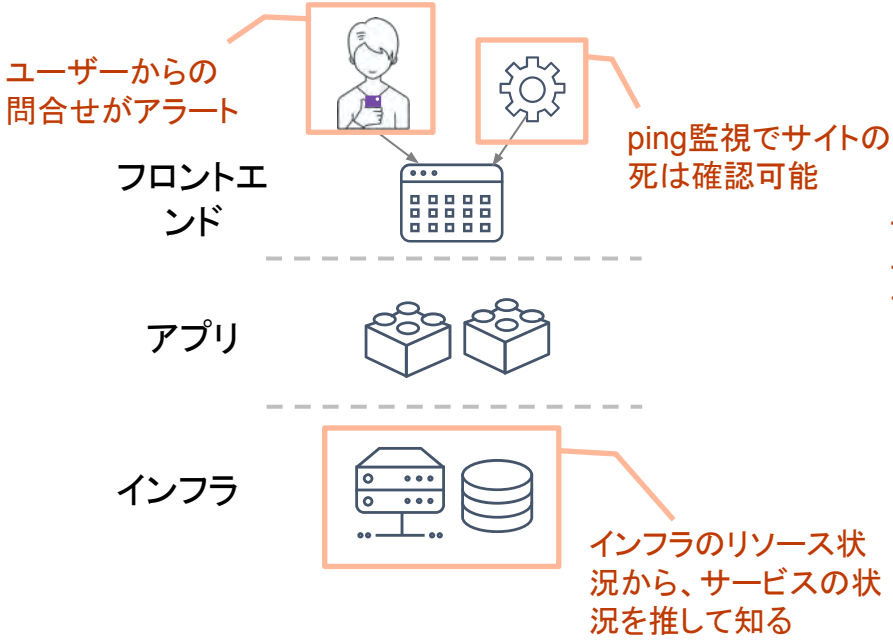
リソース抽象化
(仮想化、コンテナ等)

基盤

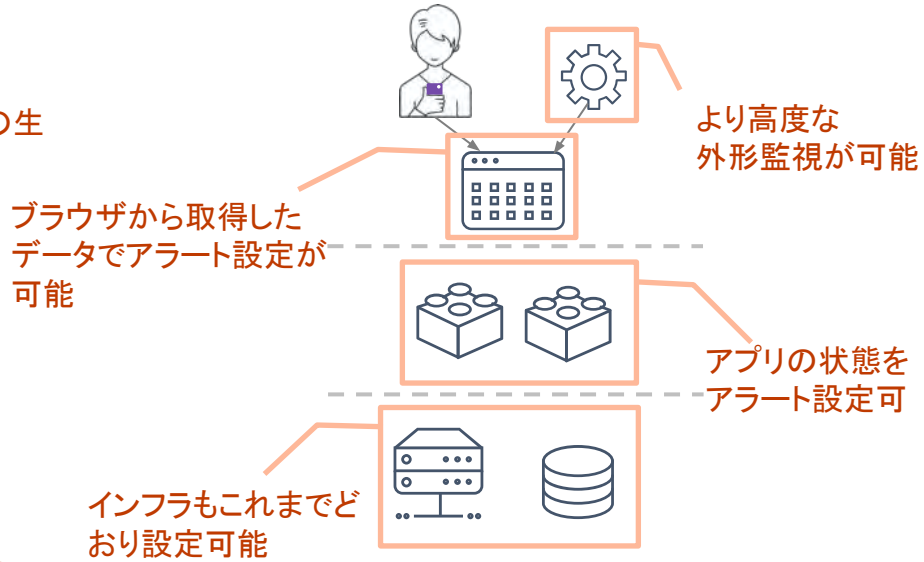
アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

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	Apdex	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 - 15:40 (25min)

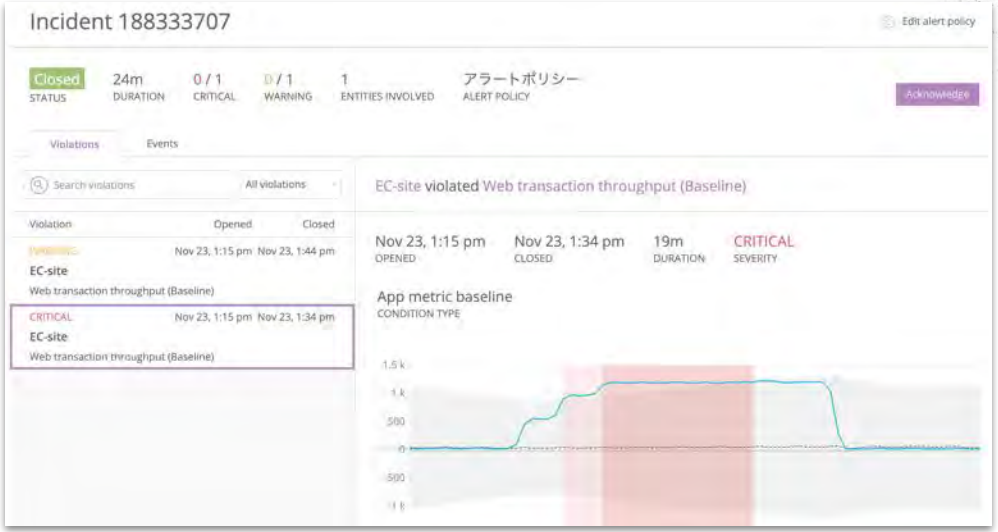
new relic

New Relicのアラート機能

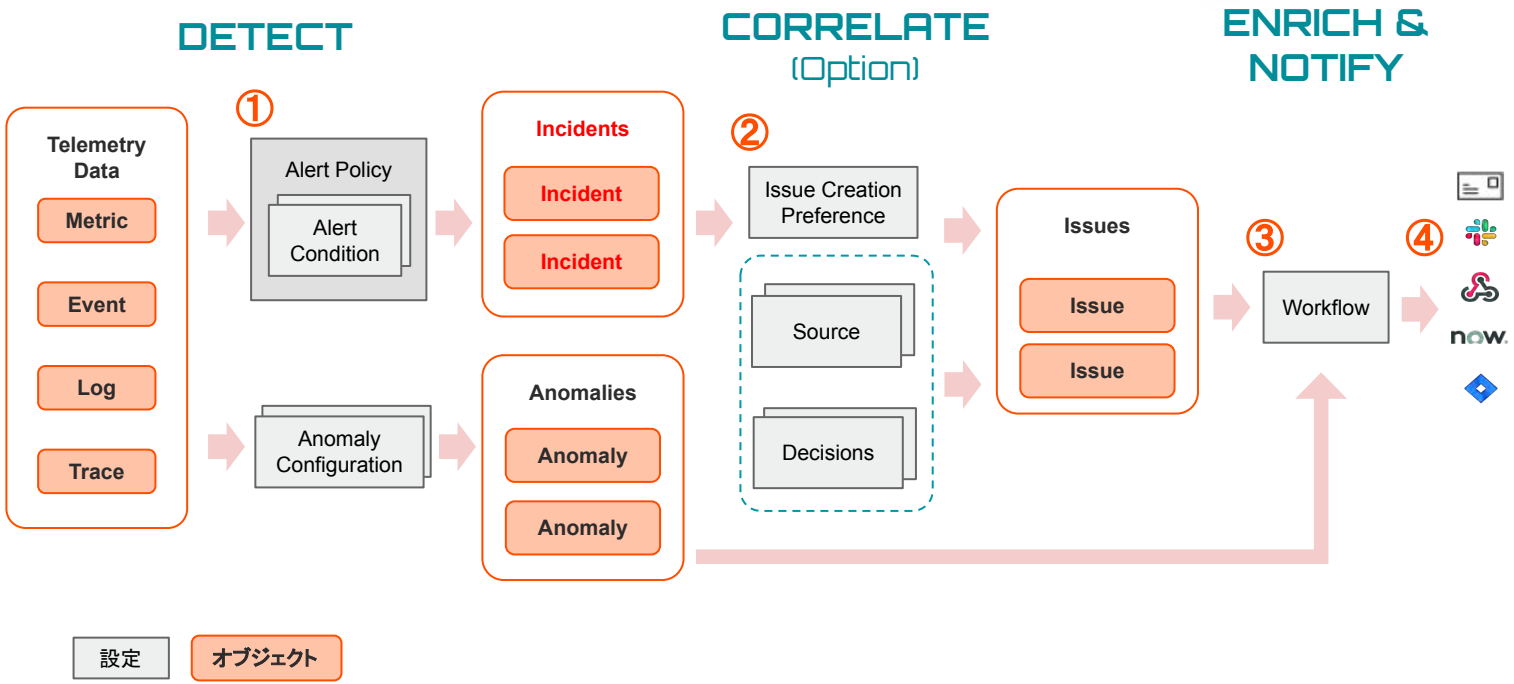
New Relicがリアルタイムに**収集しているデータ**を使って、アラートを設定することが可能

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

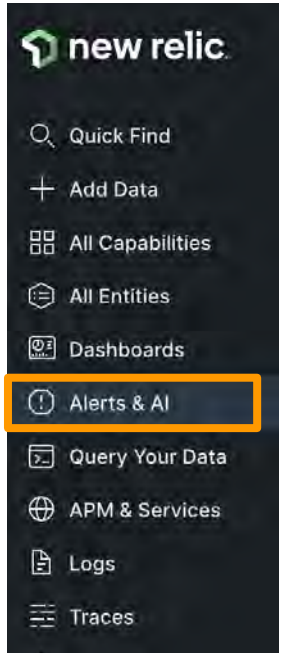
※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説していきます

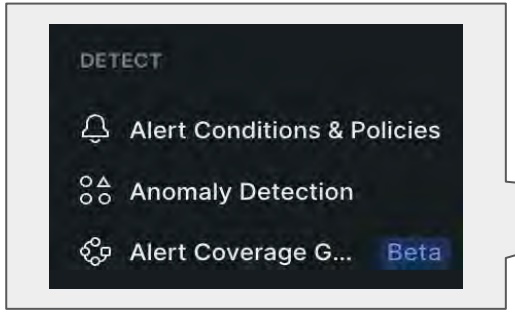


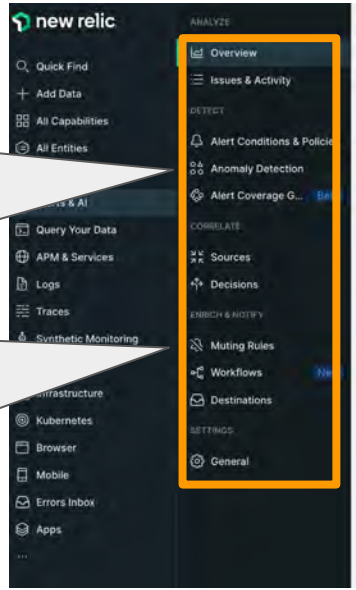
New Relicのアラート構造全体像

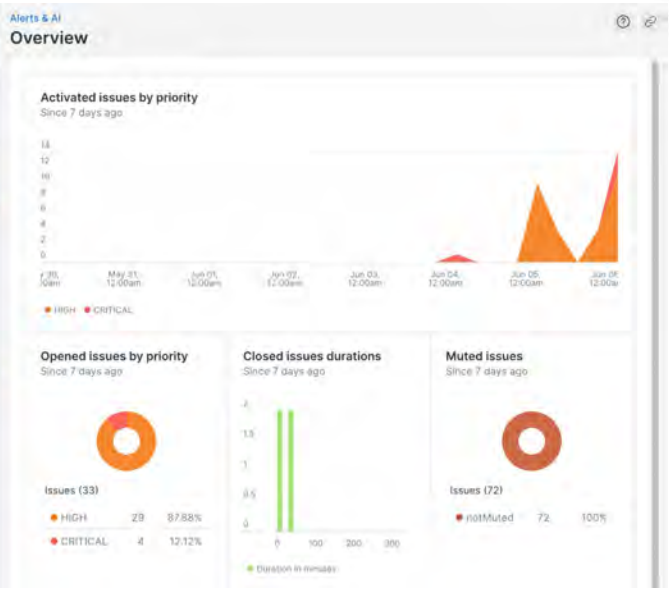


アラート機能の全体UIと重要メニュー









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

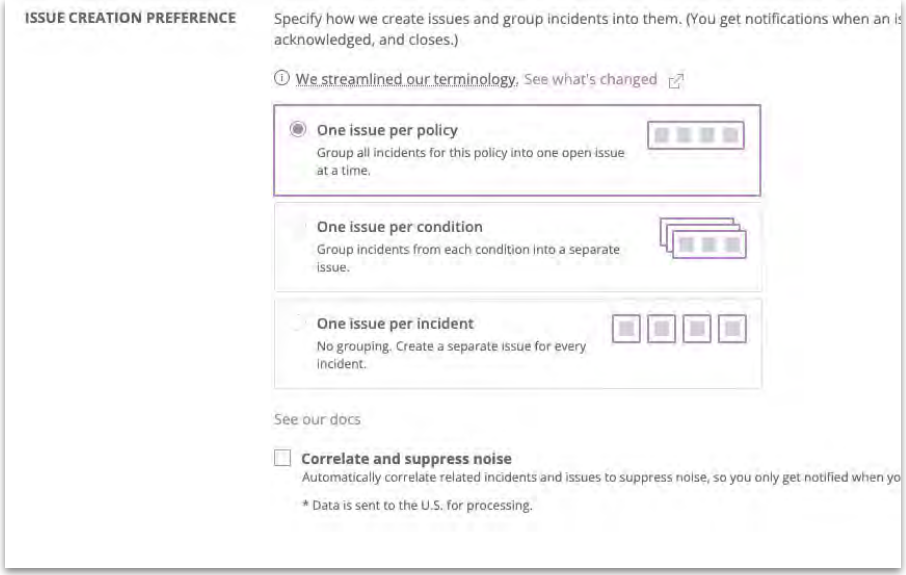
アラート対象や閾値、集計方法の定義

Incident

Alert Conditionで検出した個々の違反

Issue

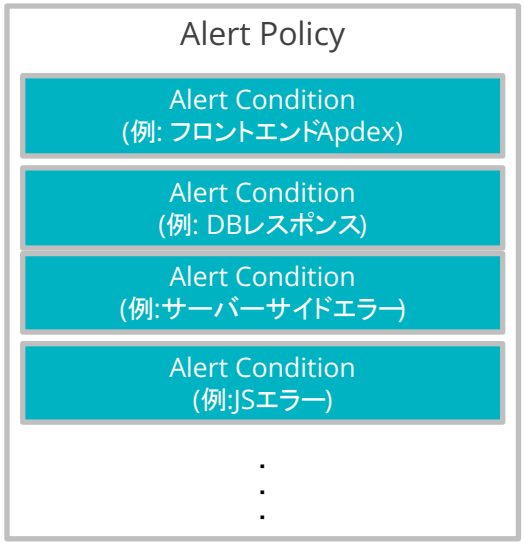
一つ以上のIncidentが示す、発生中の問題
実際の通知はIssueに対して行われる

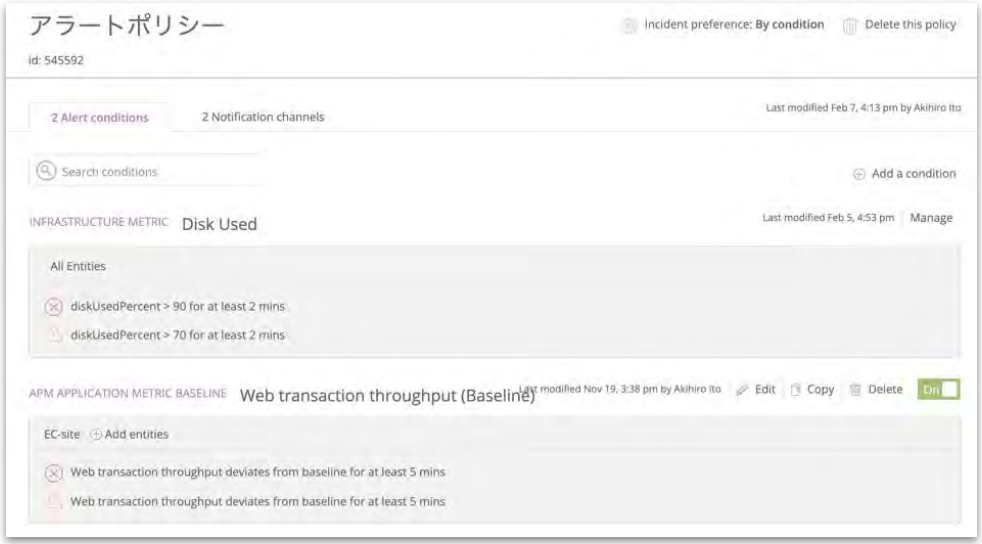


New Relic アラートの構成要素1: Alert Policy

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)

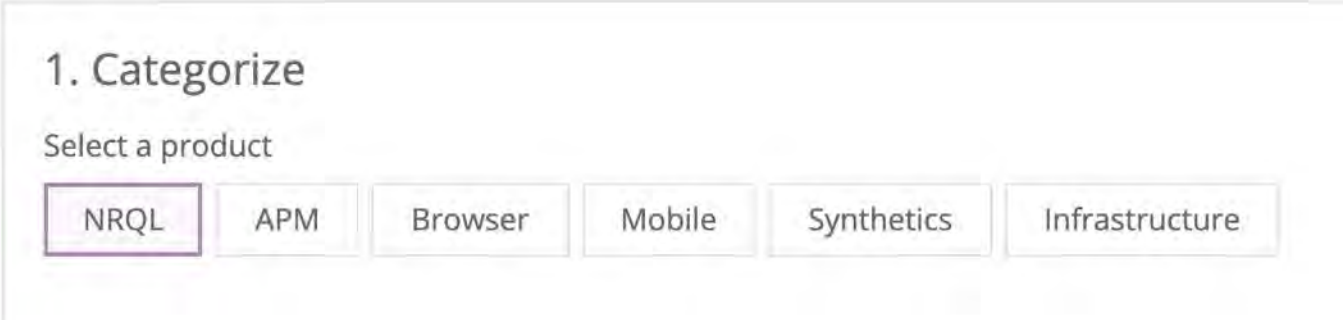
New Relic アラートの構成要素2: Alert Condition

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

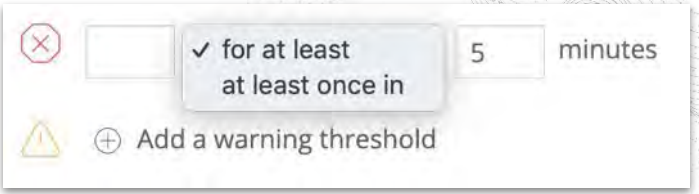


New Relic アラートの構成要素2: Alert Condition

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(Dynamic) * baseline	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) (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) (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) (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

- Additional settings > custom violation 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)
- Additional settings > 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 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)

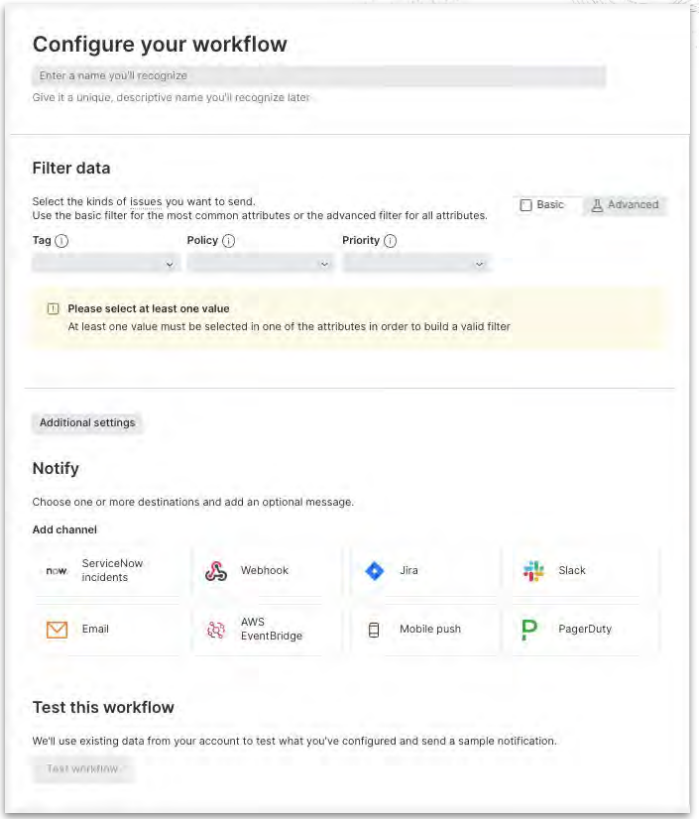
Muting Rulesが設定されていた場合の挙動の設定

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

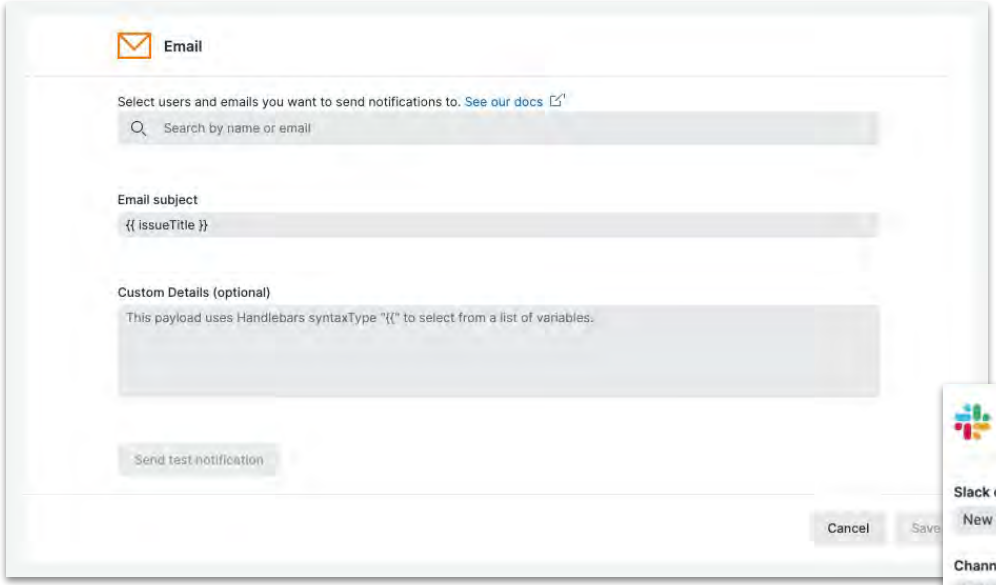
シンプルな通知

Email　Slack　Mobile push

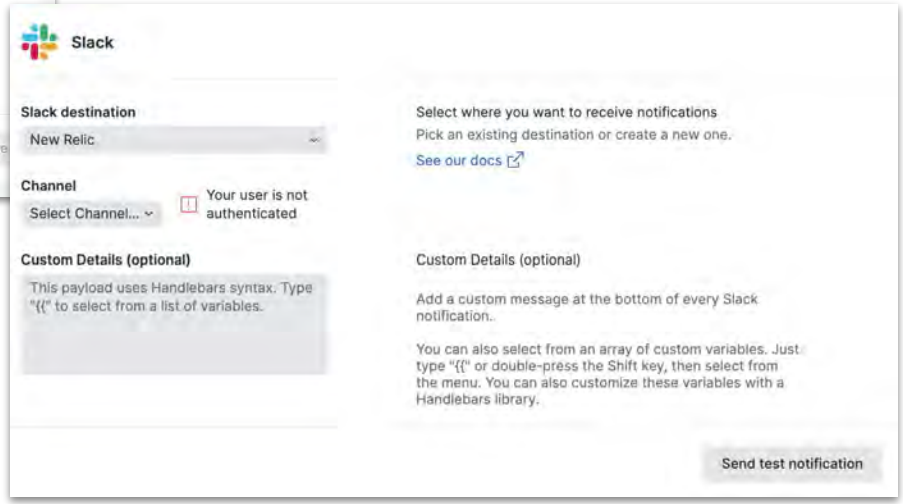
連携サービスへの通知

Webhooks　servicenow　PagerDuty　JIRA　Amazon EventBridge

New Relic アラートの構成要素4: Destinations



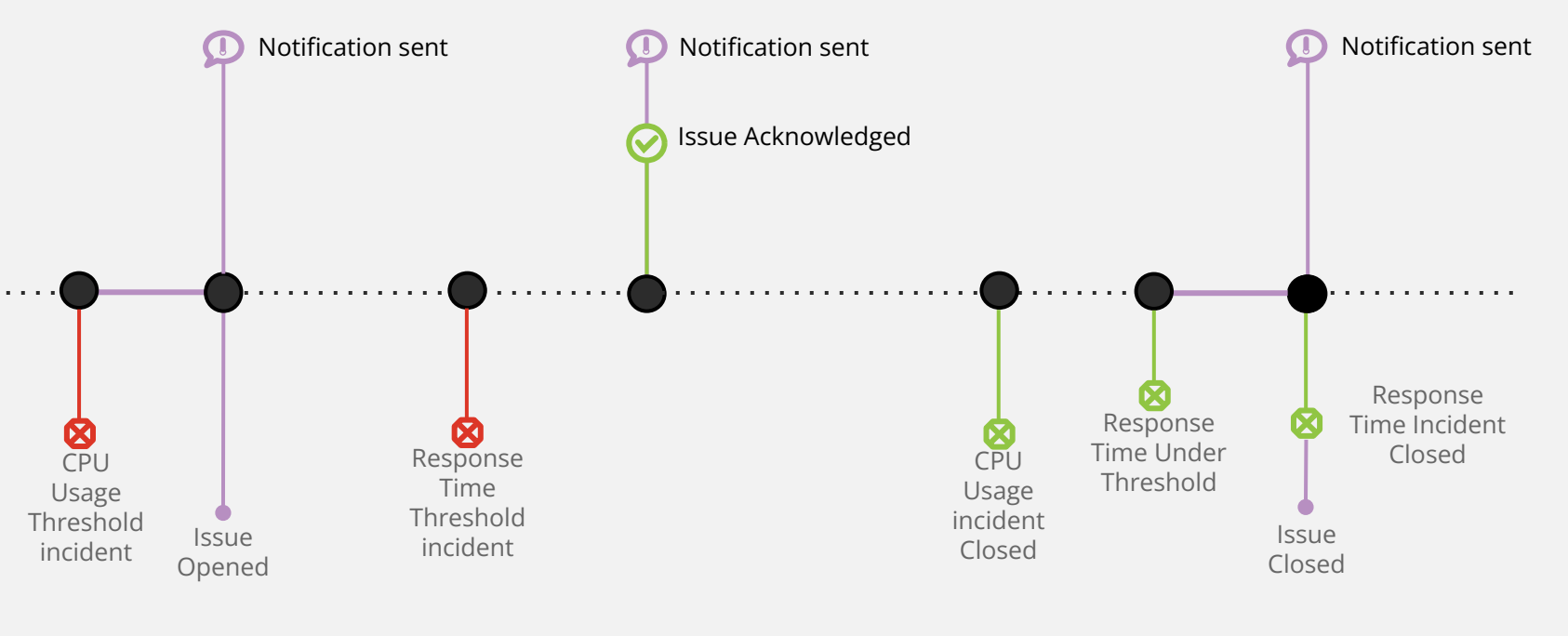
- Workflows変数を用いて、柔軟に標題や内容のカスタムができます
  - 補足: custom violation descriptionとは別の情報付加機能となります。
- “{{“と入力することで、Workflows変数の補完機能を活用できます。



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

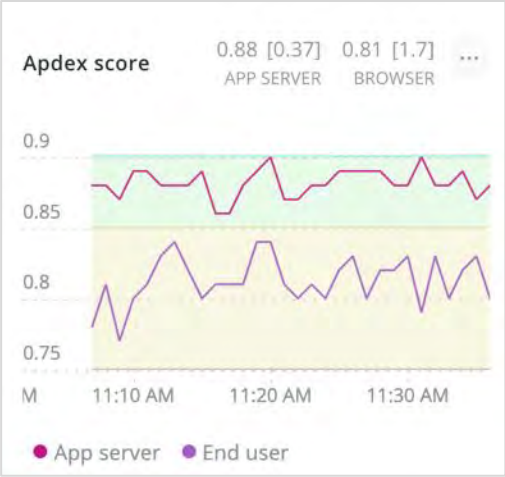


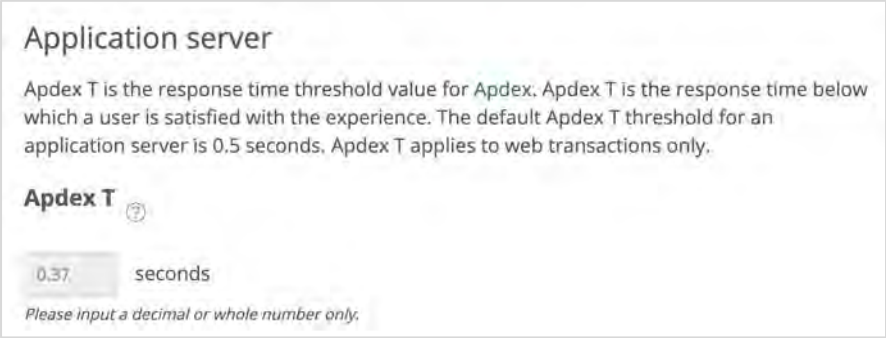
new relic

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

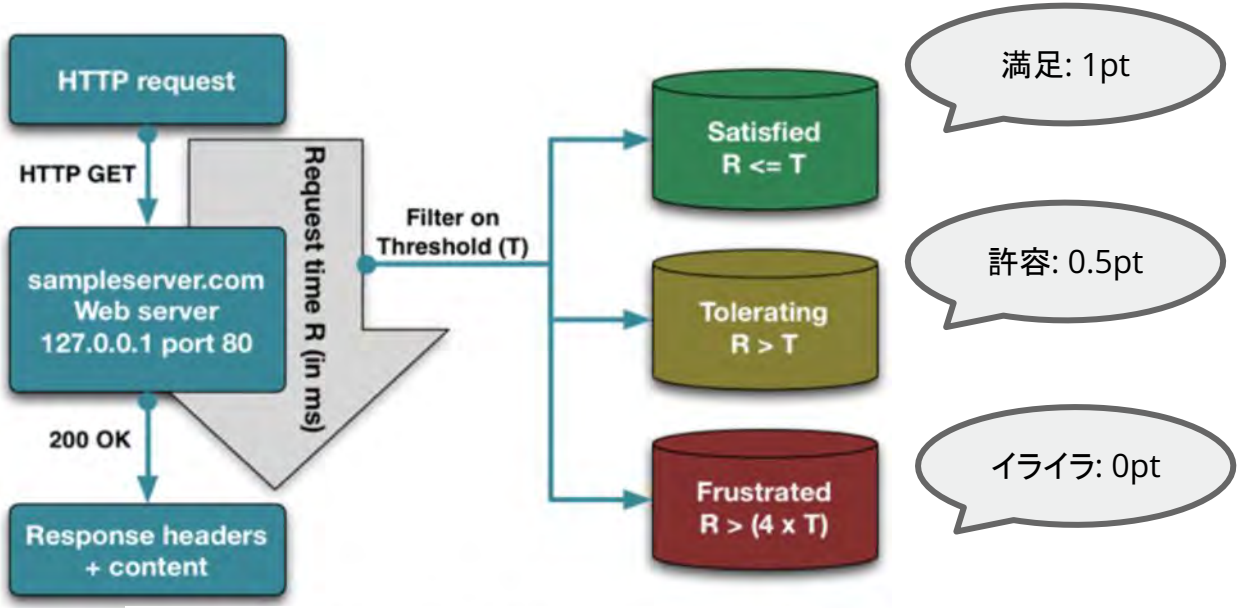




補足: Apdex T値について

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

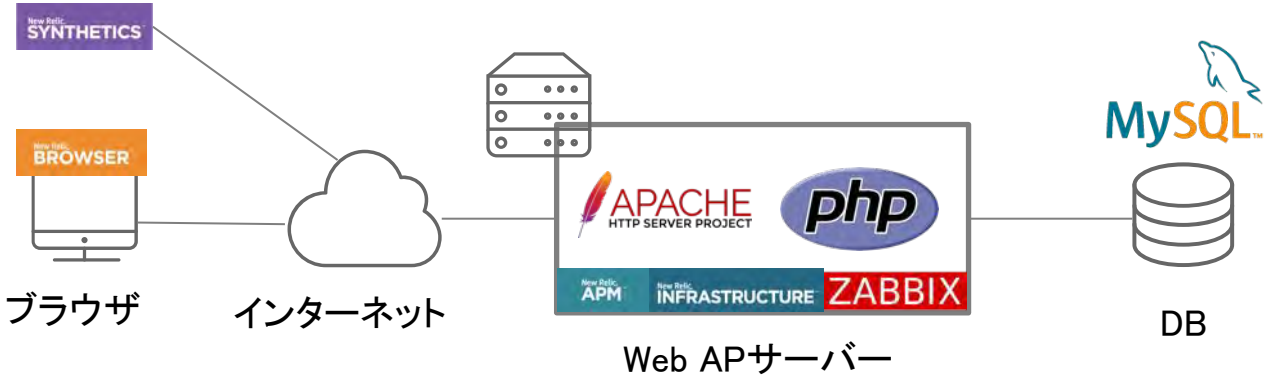
[NRUジェラートショップ](ECサイト)

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

15:40 - 15:50 (10min)

ハンズオン環境へのログイン方法

IMPORTANT

[準備]
New Relicにログインしてください。https://login.newrelic.com/login

- 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)

※本ハンズオンセミナーでは、2つのNew Relicアカウントにログインします。
ユーザー名とパスワードは共通です。
スムーズに切り替えを行うためにログイン時に [Remember my email]にチェックをつけてください
ログイン切り替えは次項参照。

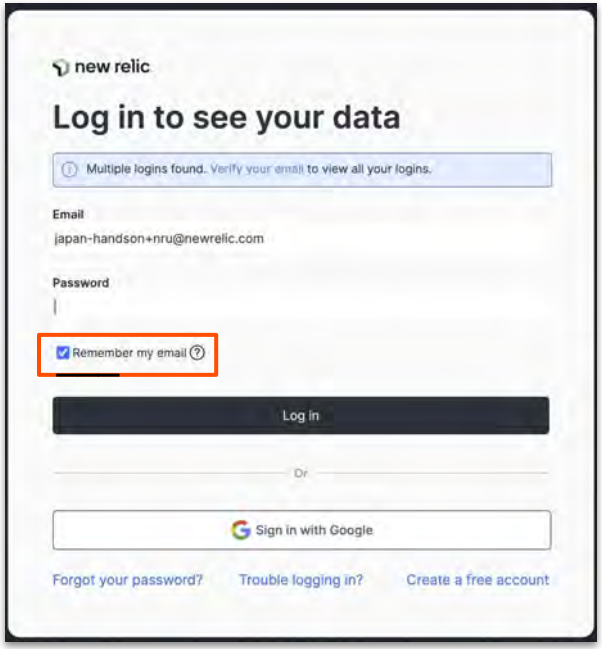
※普段NewRelicをお使いの方はセッションが残っている場合がありますのでプライベートブラウジングをお使いください。

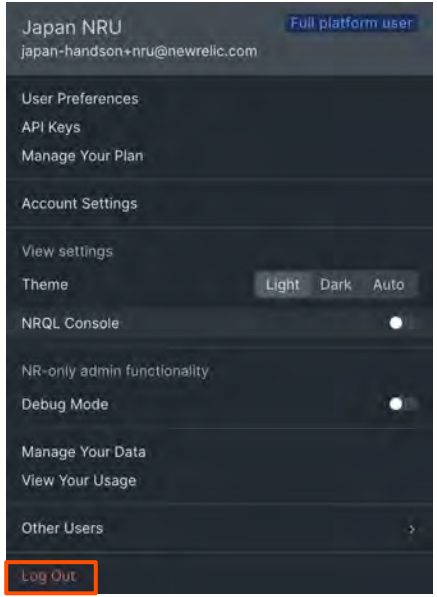
- Chrome:シークレットウィンドウ
- Firefox:プライベートウィンドウ
- Edge:InPrivate ウィンドウ
- IE: New Relicの一部機能はIEをサポートしていません。上記のいずれかのブラウザをご利用ください。

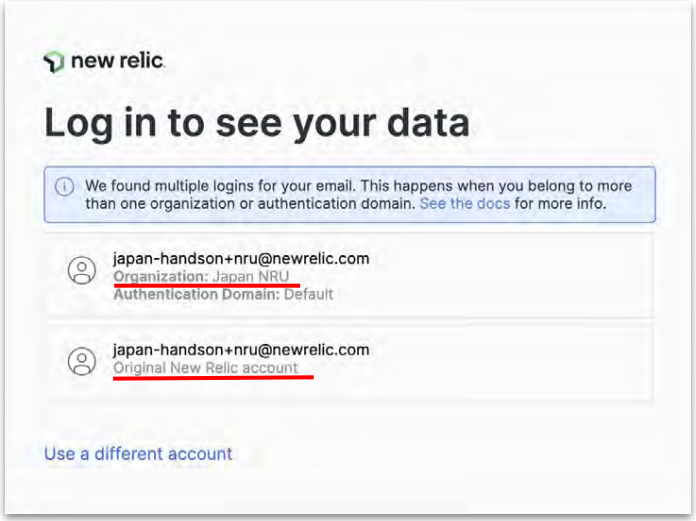
ログインするNew Relicアカウントを切り替える

IMPORTANT

ログイン時に[Remember my email]にチェックをつけておくと、
Log outした際に次にどこのアカウントにログインするか選択する画面が表示されるようになります。



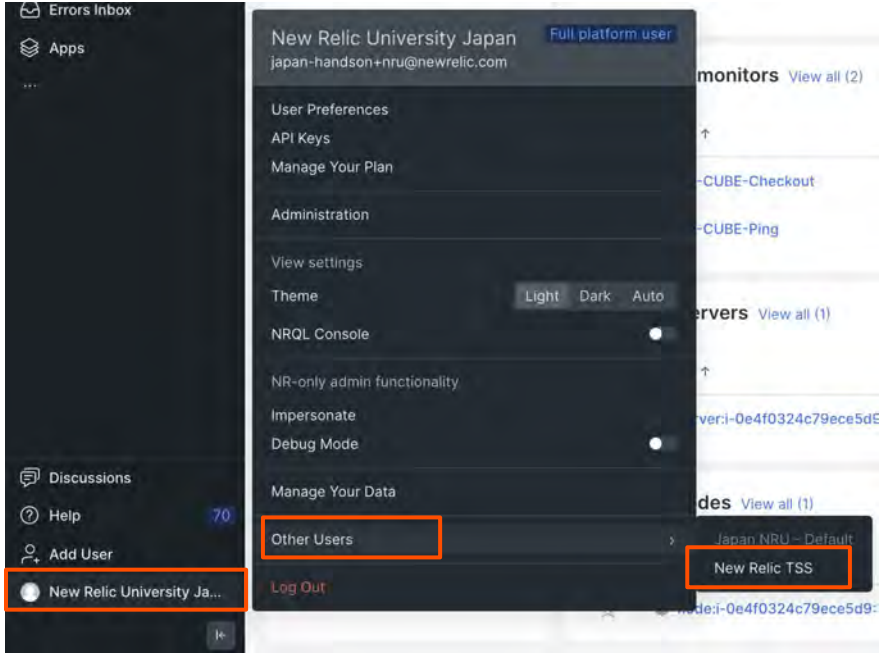


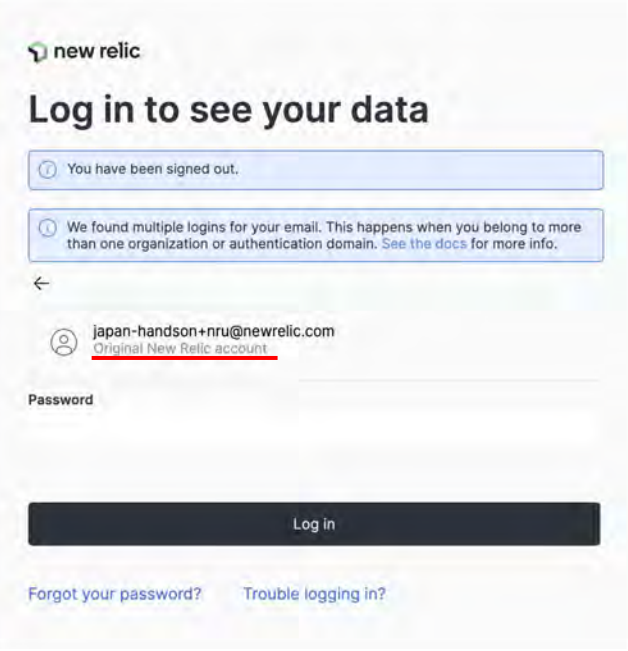


ログインするNew Relicアカウントを切り替える

IMPORTANT

同じメールアドレスでログインしているアカウント間は、直接切り替えも可能です。
（画面遷移が異なるだけで、結果は一回ログアウトする場合と同じです。）





ハンズオン(0) 2つのアカウントにログインする

IMPORTANT

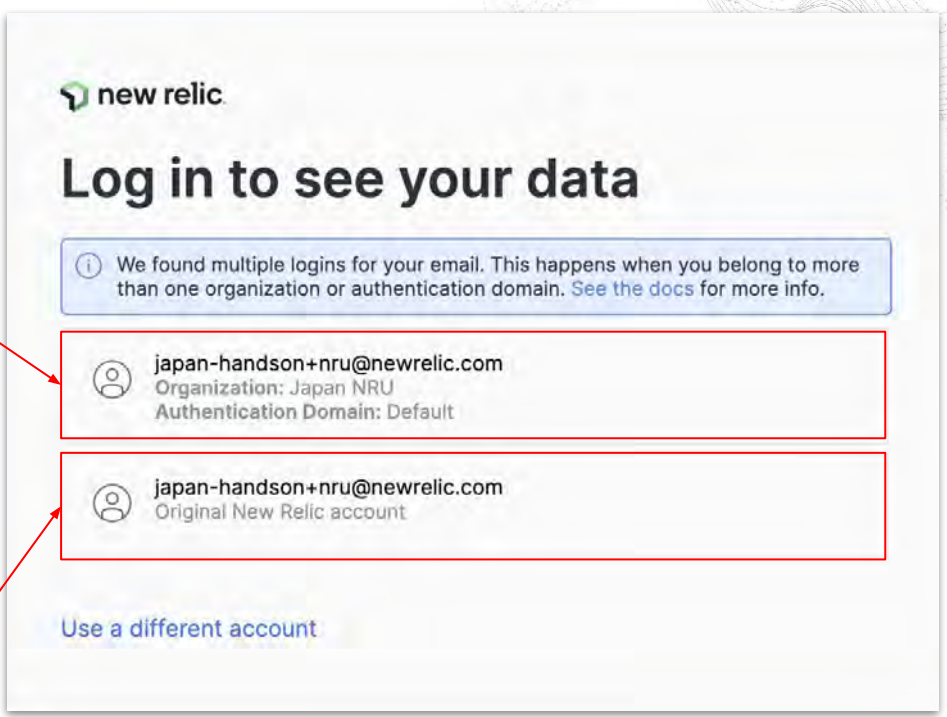
ログアウトすると、アカウントが選択できる
パスワードは共通： oSz6nrupas

Organization: Japan NRU

- 設定変更を伴うハンズオンはこちらのアカウントで実施します。

Original New Relic account

- いくつかのサンプルデータが入っています。UI上でデータを確認する一部ハンズオンで、こちらのアカウントを使用します。
- Other Users の切替先に New Relic TSS と表示されているのも本アカウントです。

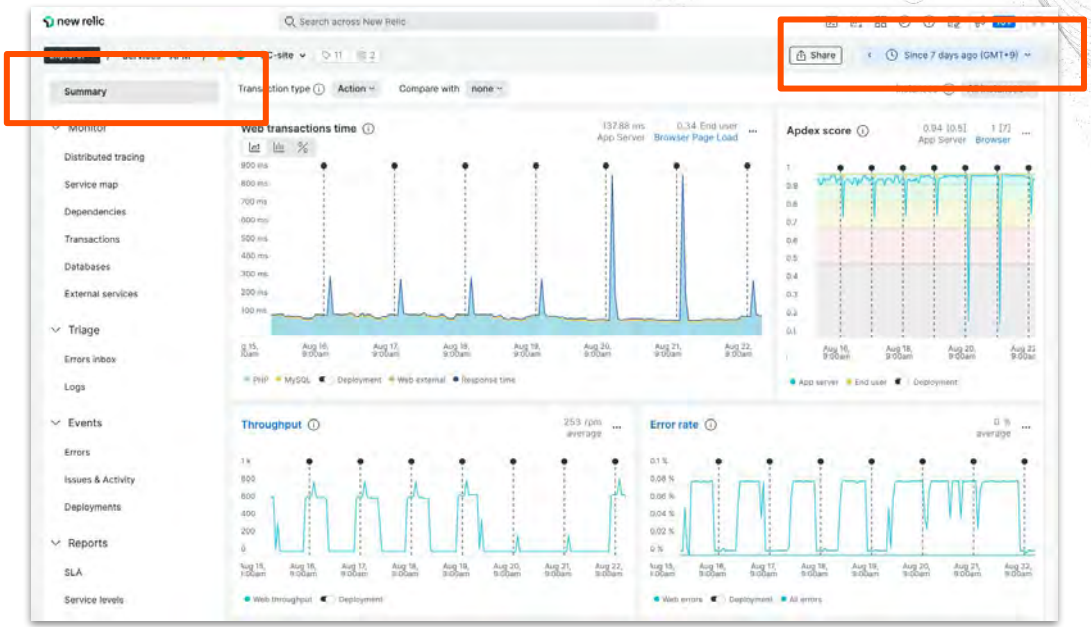


操作アカウント: Japan-NRU

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。



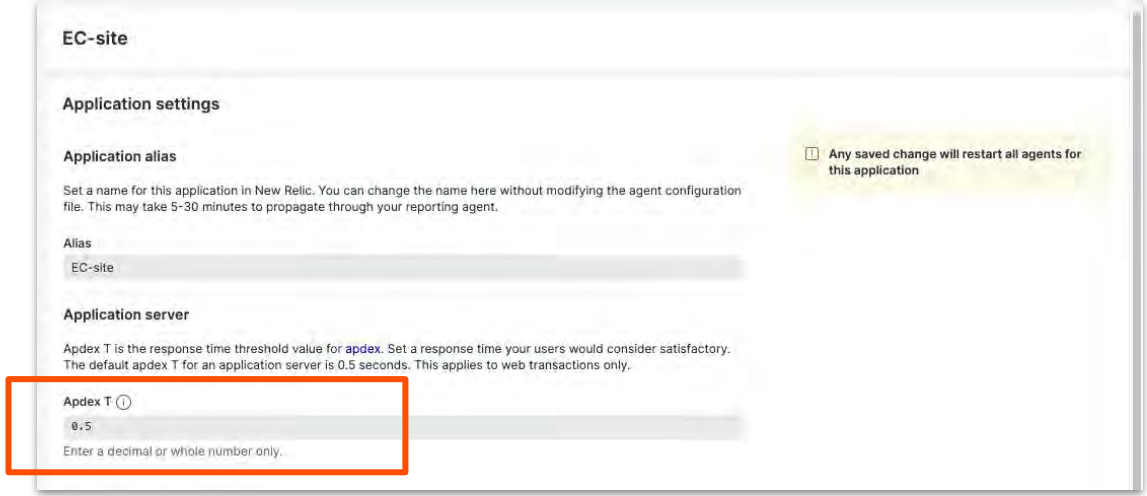
new relic

操作アカウント: Japan-NRU

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。



new relic

ハンズオン(1)
アラートを作成する

15:50 - 16:10 (20min)

今回の環境の監視構成

[前提]

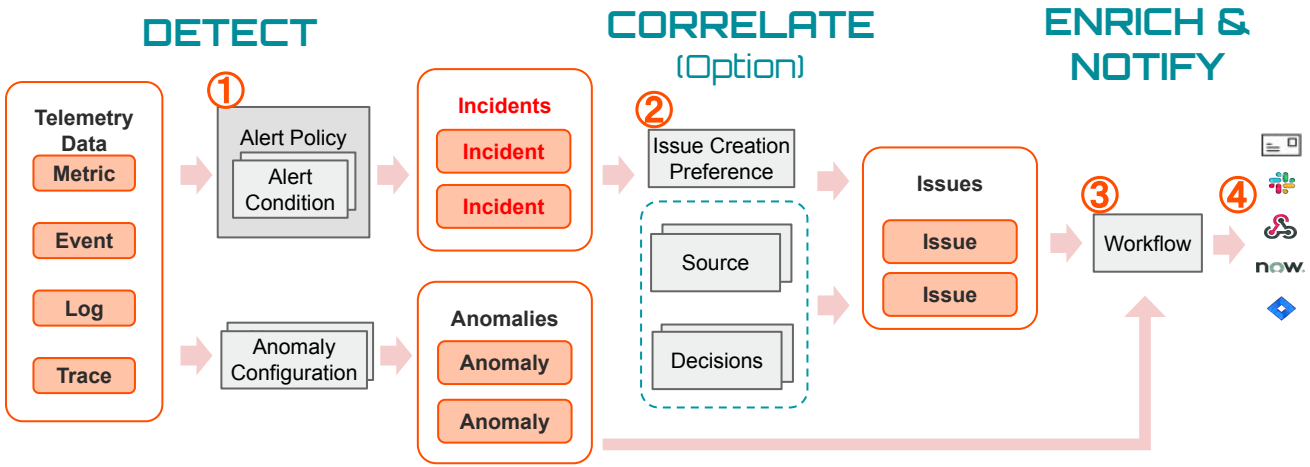
今回は**赤字**のアラートを設定してみます。

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	**Apdex**	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

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. Alert Condition（4つ）を作成する
3. Workflowを作成する



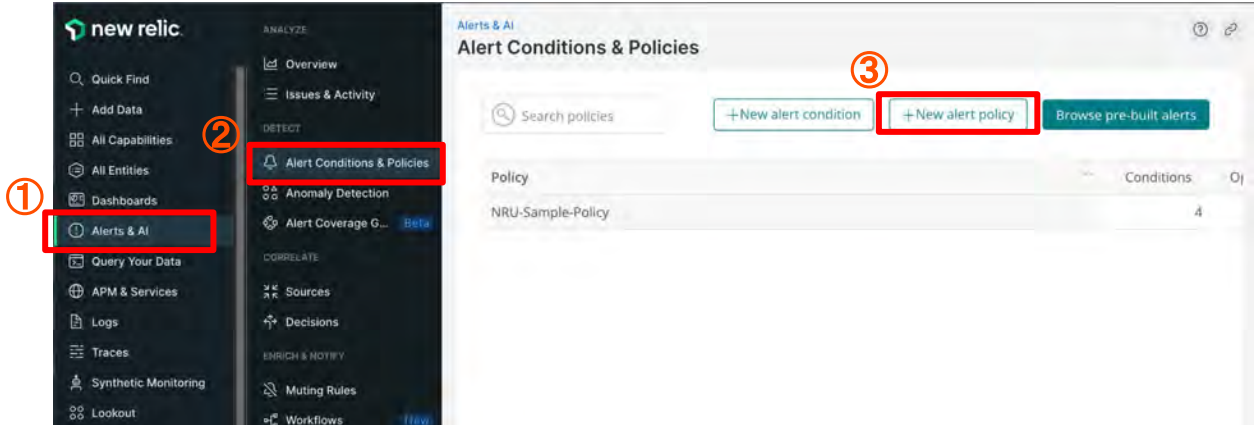
手順・解説

使用アカウント：Japan-NRU
（ログイン先選択はこちら参照）

操作アカウント: Japan-NRU

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 Conditions & 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。

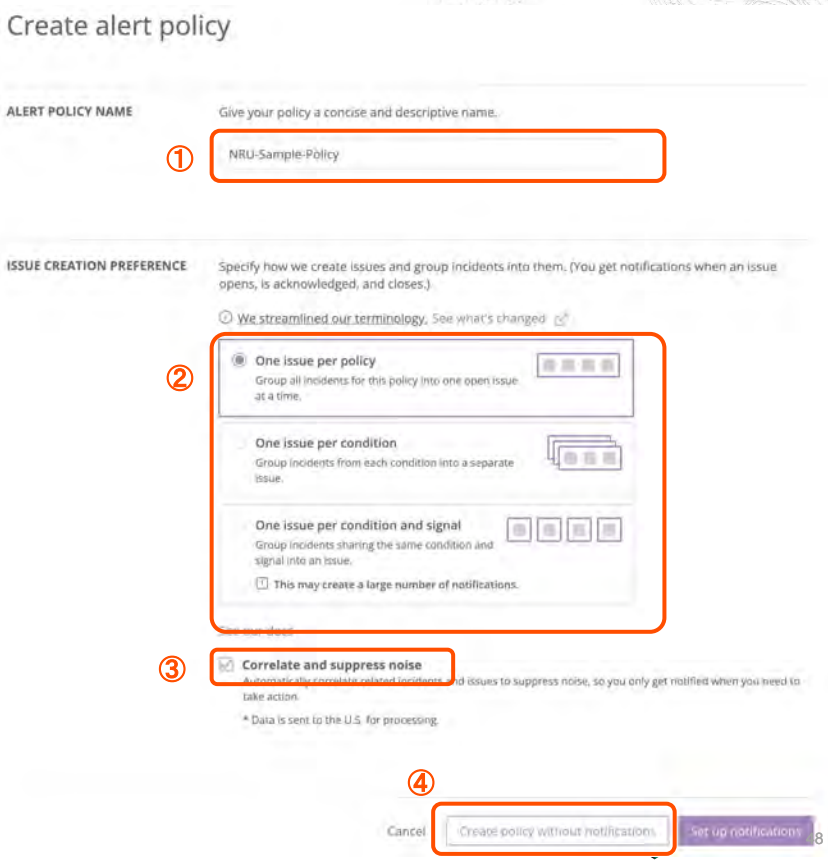


操作アカウント: Japan-NRU

ハンズオン(1-1) Alert policyを作成する 2/2

1. Alert Policy名には、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「Issue Creation Preference」を選択してください
3. [Correlate and suppress noise]をチェック
4. [Create policy without notifications] 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



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 1/20

[前提]

今回は**赤字**のアラートを設定してみます。

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	**Apdex**	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

操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 2/20

- 新規Alert Conditionの追加

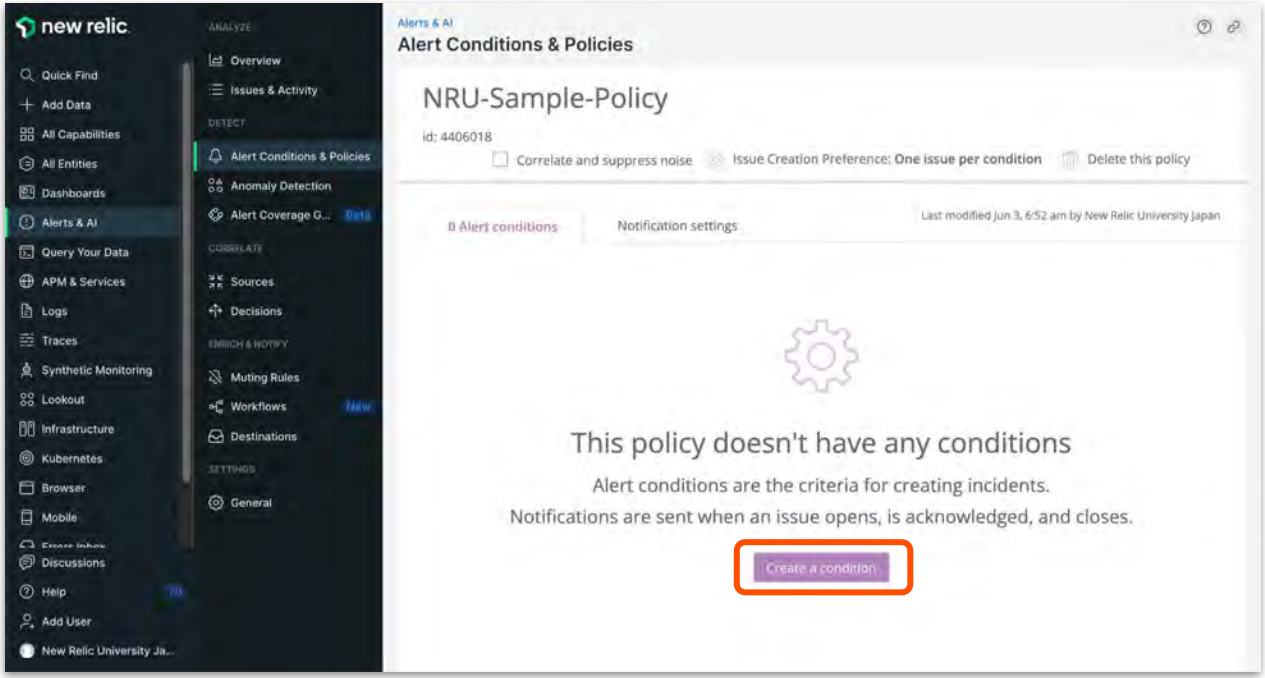
4つのアラートを順番に設定していきます

1. 外形監視:チェックエラー
2. フロントエンド: Apdex(静的)
3. アプリケーション: 応答時間(動的)
4. 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)

操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 3/20

- Policyを作成したら「Create a condition」からconditionを作成します。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 4/20

- 外形監視:チェックエラー
- 監視設定は次のようにしてください。

1. **Categories**
   a. Synthetics → Single failure
2. **Select a monitor**
   a. EC-CUBE-Checkout

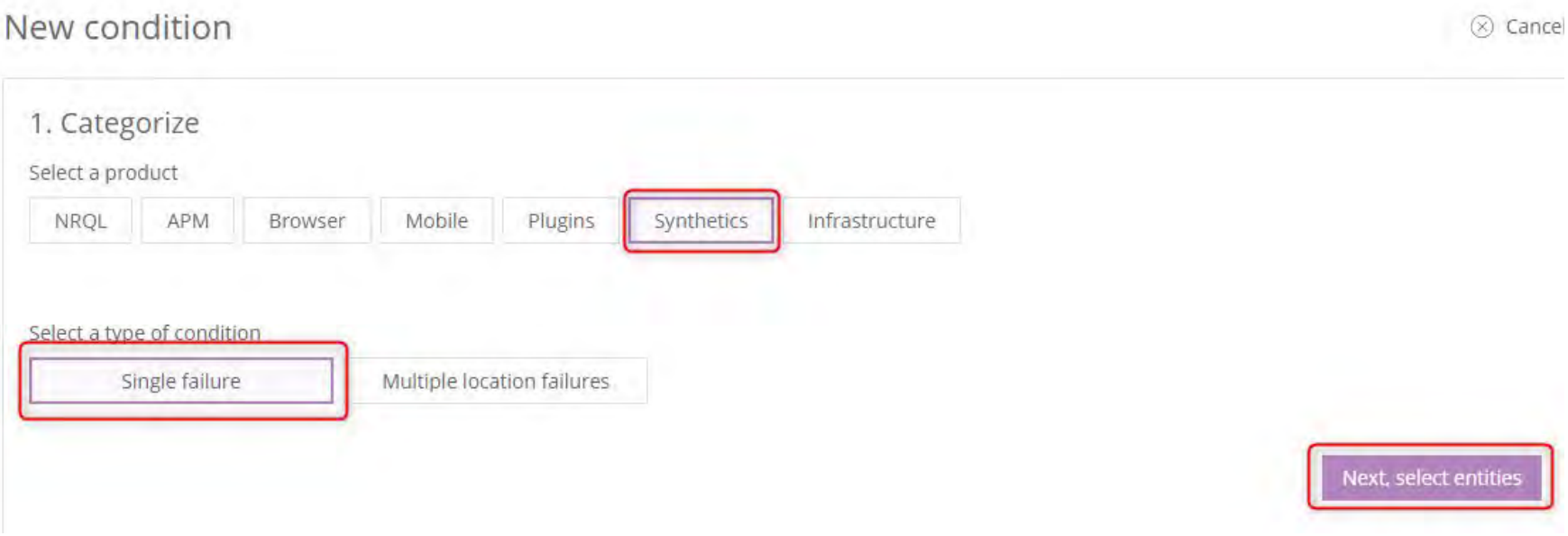
Condition名は適切なものを各自設定してください

（例：NRU304-yourname-Synthetics-Failure）

操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 5/20

- Categories を選択し、「Next, select entities」をクリックします。



操作アカウント: Japan-NRU

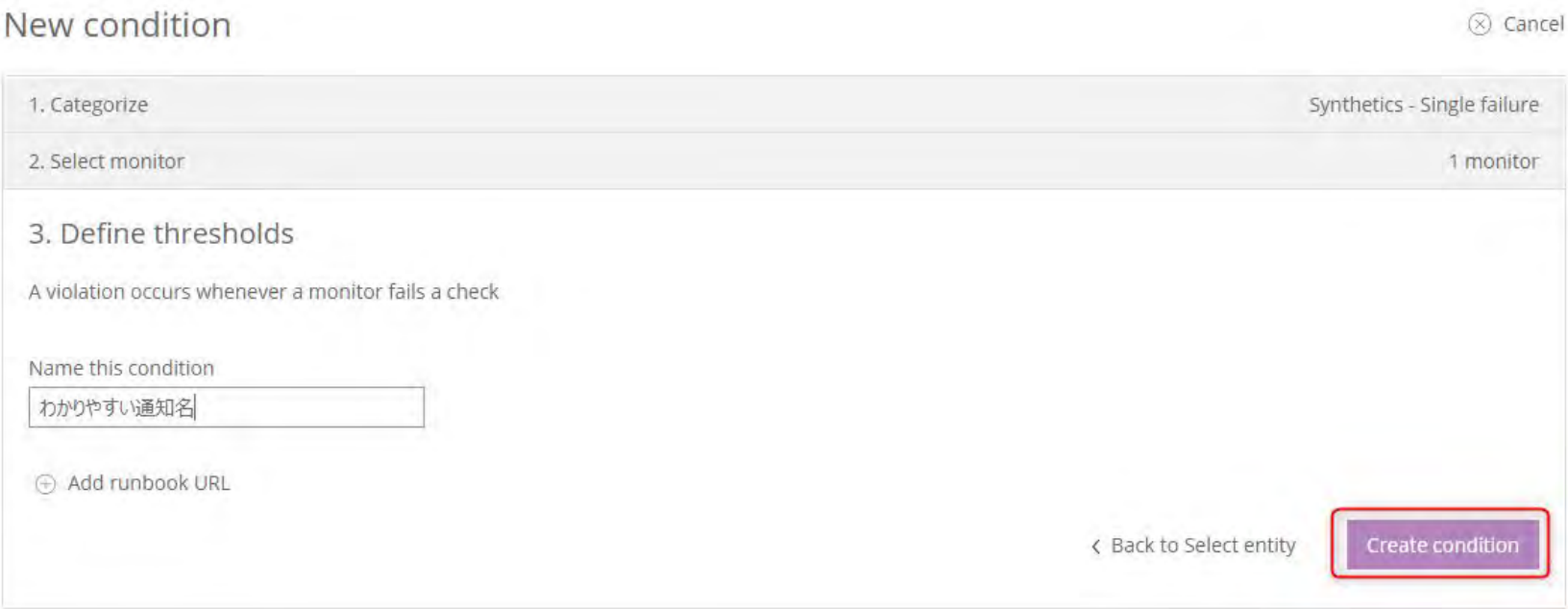
ハンズオン(1-2) Alert Conditionを作成する 6/20

- Select a monitor で「EC-CUBE-Checkout」を選択し「Next, define thresholds」をクリックします。

操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 7/20

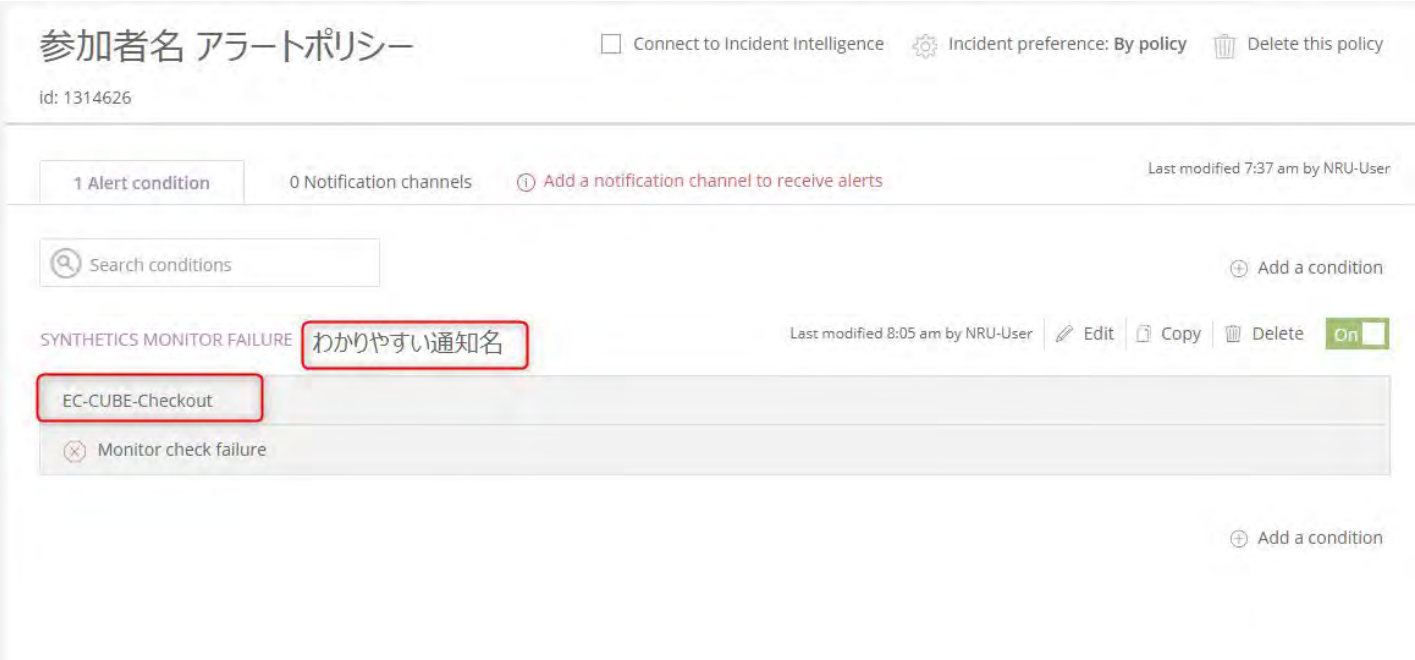
- コンディション名にわかりやすい名前を入力して 「Create condition」をクリックします。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 8/20

- 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。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 9/20

- **新規Alert Conditionの追加**

②フロントエンド: Apdex(静的)

1. **Categories:**
   a. Browser → Metric
2. **Select entities:**
   a. EC-site
3. **Define thresholds**
   a. Critical: End User Apdexが5分間に1度でも(at least once)0.7を下回ったら(below)

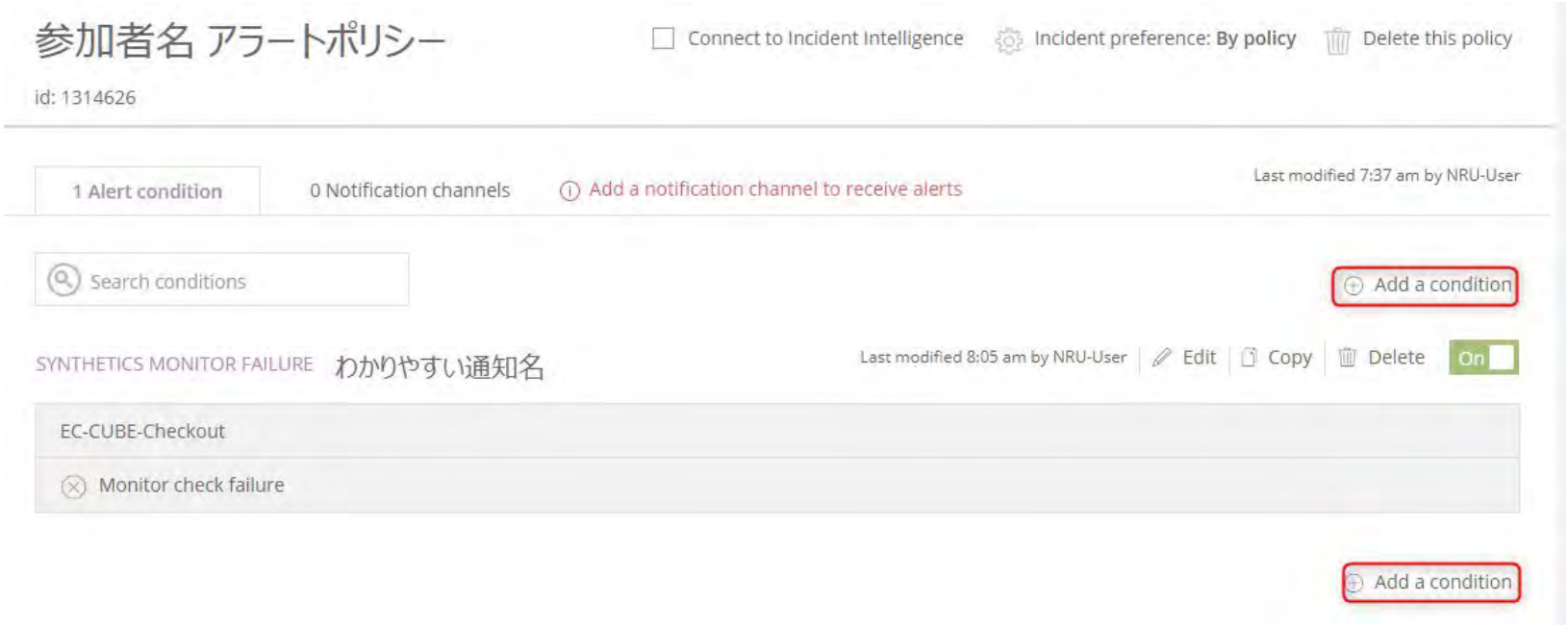
Condition名は適切なものを各自設定してください

（例：NRU304-yourname-End User Apdex）

操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 10/20

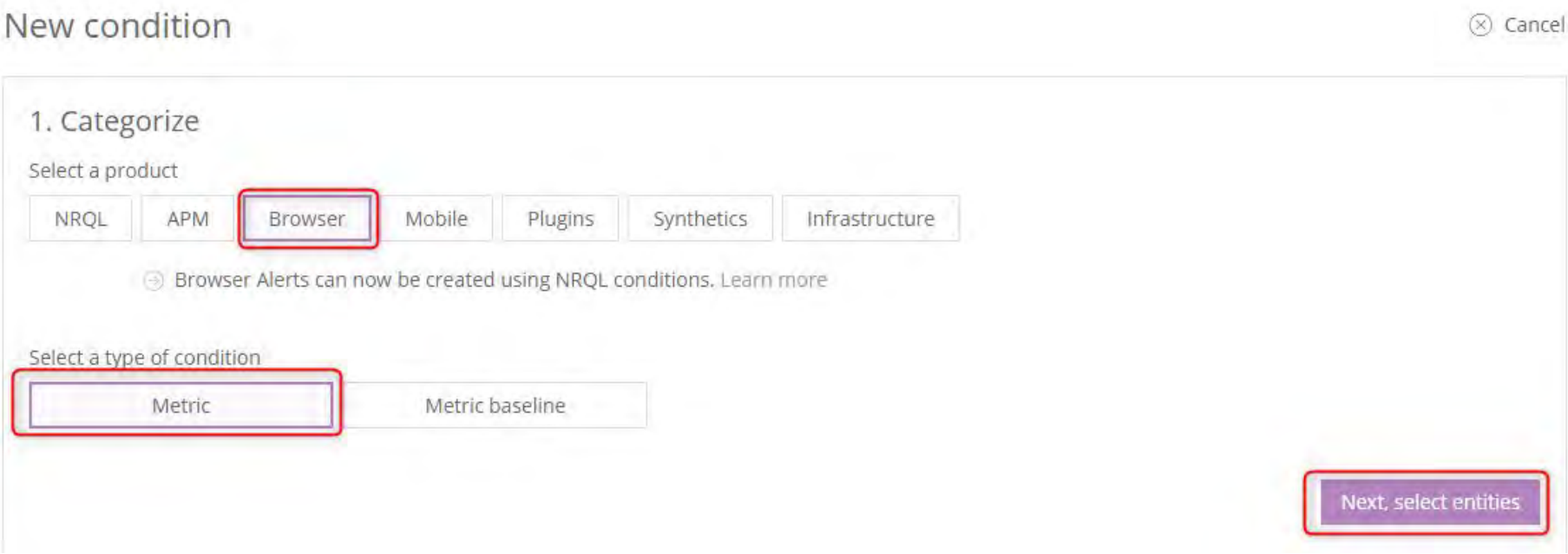
- 「＋ Add a condition」をクリックすればPolicyにconditionを追加できます。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 11/20

- Categories を設定します。



操作アカウント: Japan-NRU

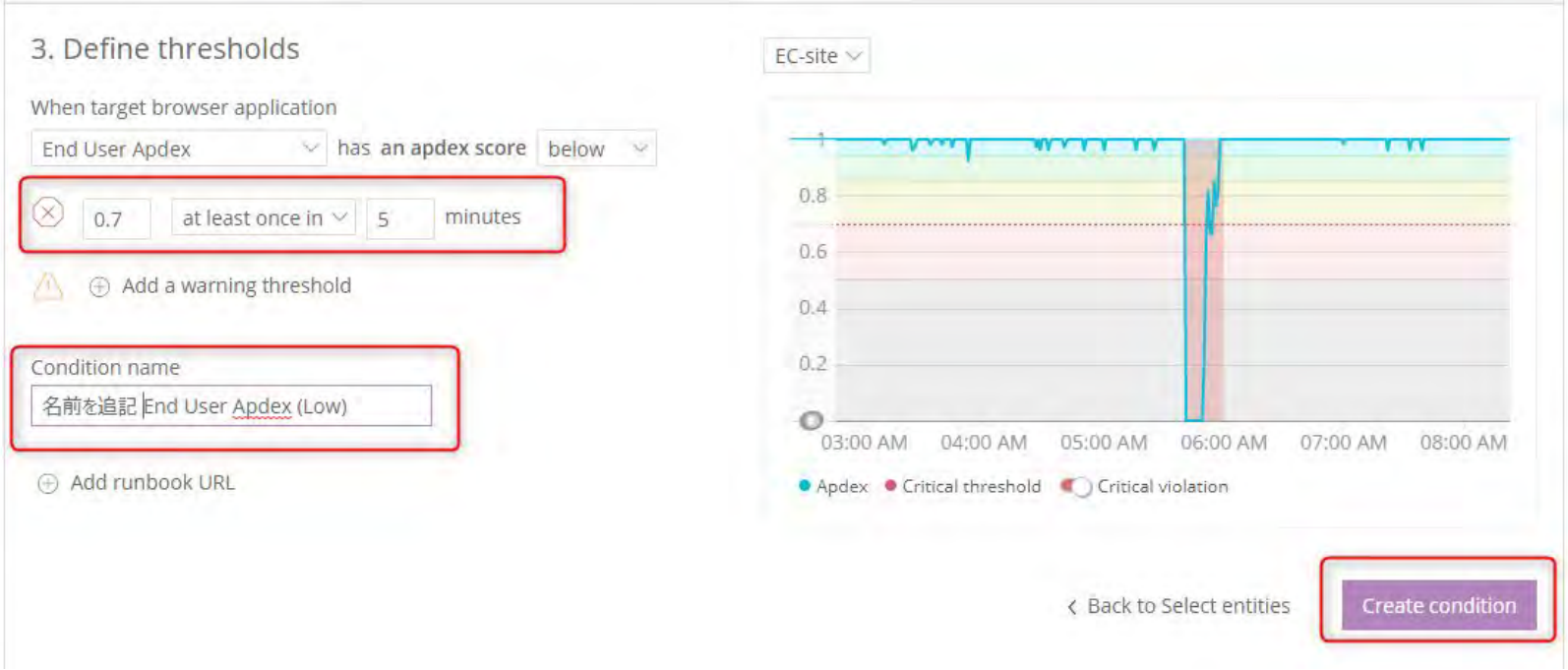
ハンズオン(1-2) Alert Conditionを作成する 12/20

- Select entities で対象にするアプリケーションを選択します。

操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 13/20

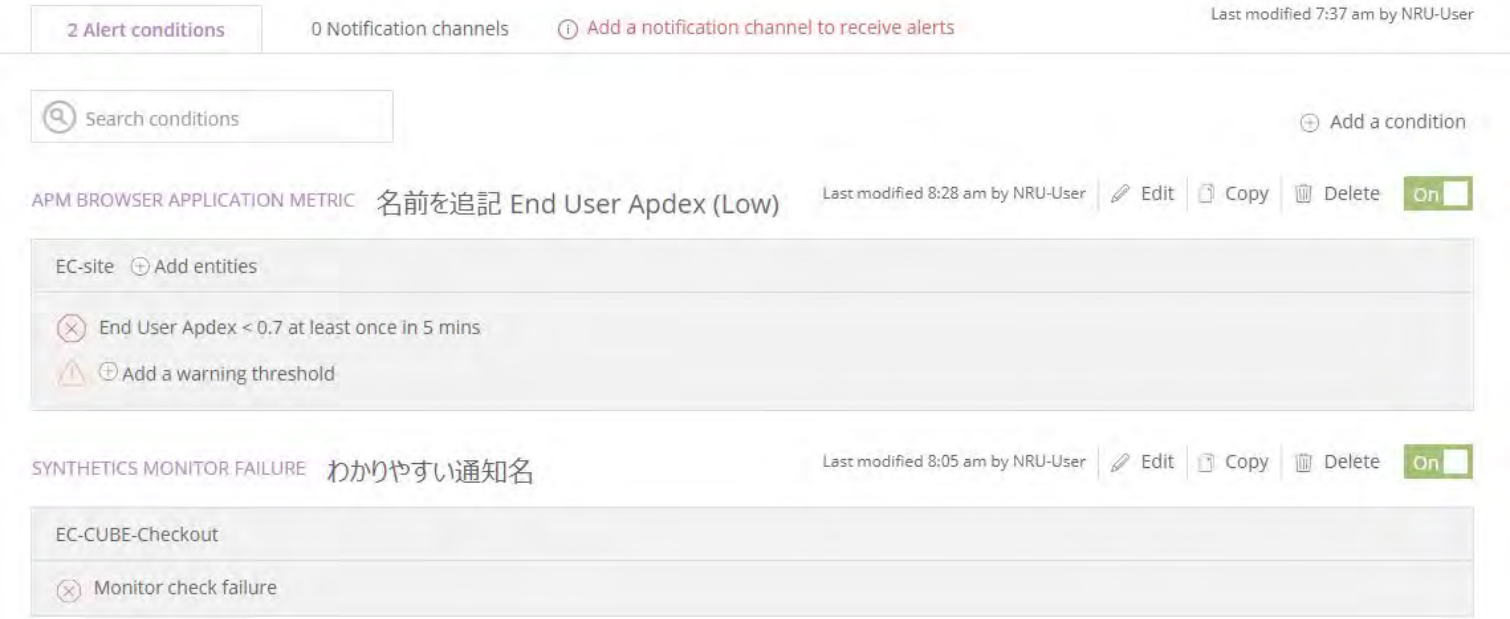
- Thresholds を設定しわかりやすい名前を設定します。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 14/20

- 2つめのconditionが作成されました。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 15/20

- **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. APM → Application metric baseline
2. **Select entities**
   a. EC-site
3. **Define thresholds**
   a. 次ページ参照

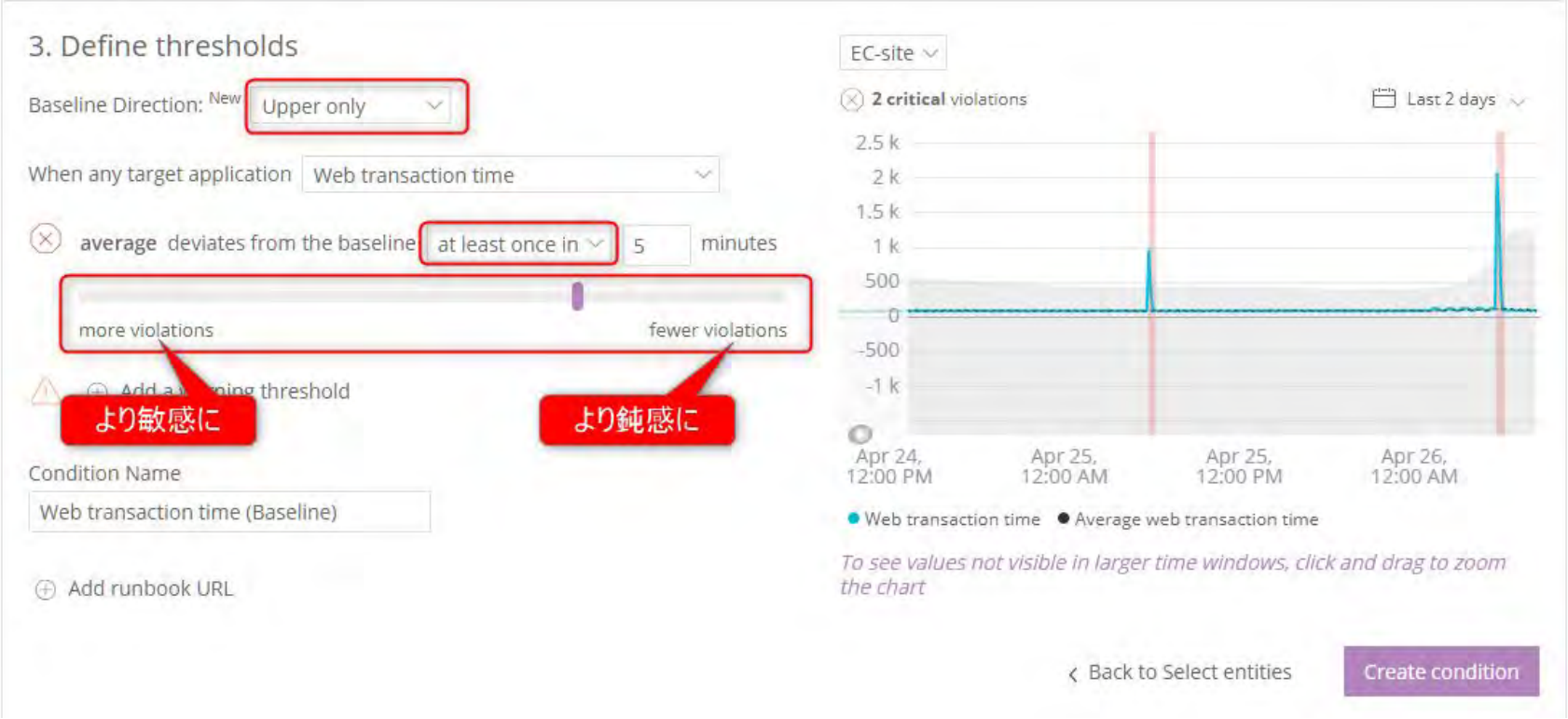
Condition名は適切なものを各自設定してください

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

操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 16/20

- ベースラインアラートではスライドバーで感度が変化します。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 17/20

- **新規Alert Conditionの追加**

④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
```

3. **Set your condition thresholds**
   a. Threshold type: Staticで適宜好きな値(%)を設定してください

Condition名は適切なものを各自設定してください

（例：NRU304-yourname-NRQL-ErrorResponse）

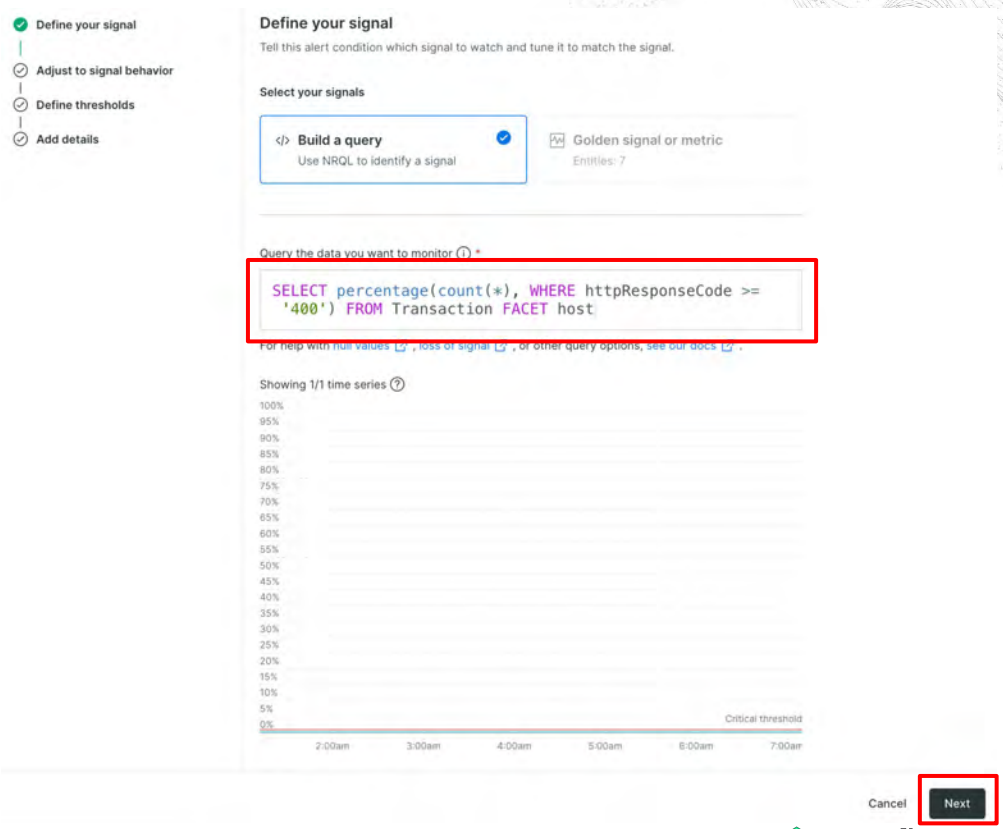
操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 18/20

- カテゴリにNRQL を選択すると右の画面に遷移します。
- クエリ入力欄に次の NRQLクエリをコピー＆ペーストして、Nextをクリックします。

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

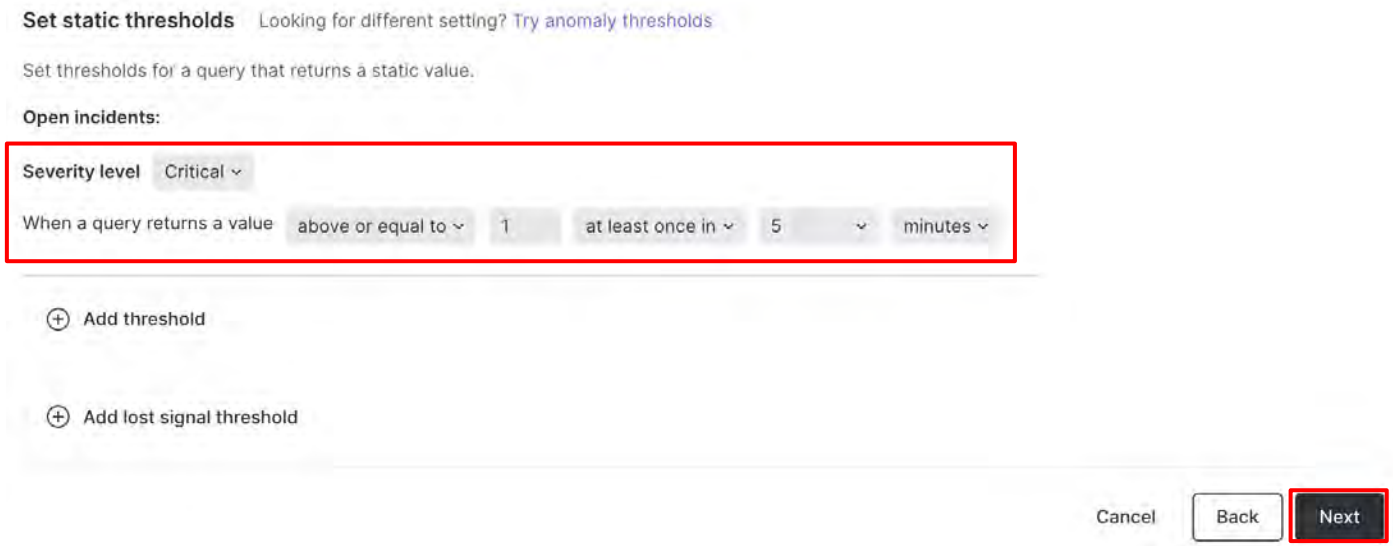
- クエリを入力すると、直近の状態を示す参考チャートが表示されます。



操作アカウント: Japan-NRU

ハンズオン(1-2) Alert Conditionを作成する 19/20

- Adjust to signal behaviorはすべて初期値のまま Nextをクリックします。
- 閾値設定は任意ですが、以下を参考に設定してみてください。



操作アカウント: Japan-NRU

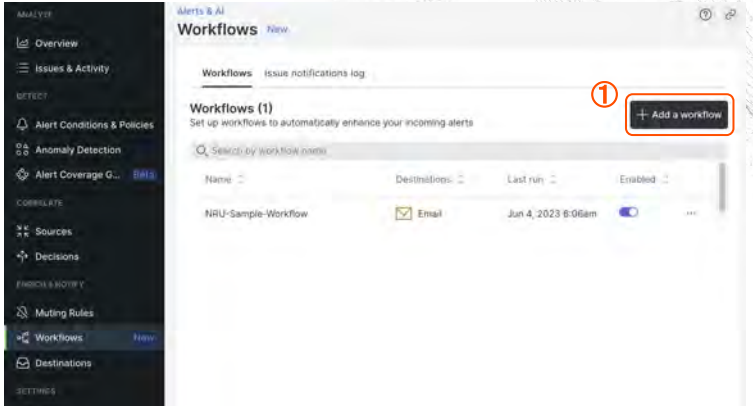
ハンズオン(1-2) Alert Conditionを作成する 20/20

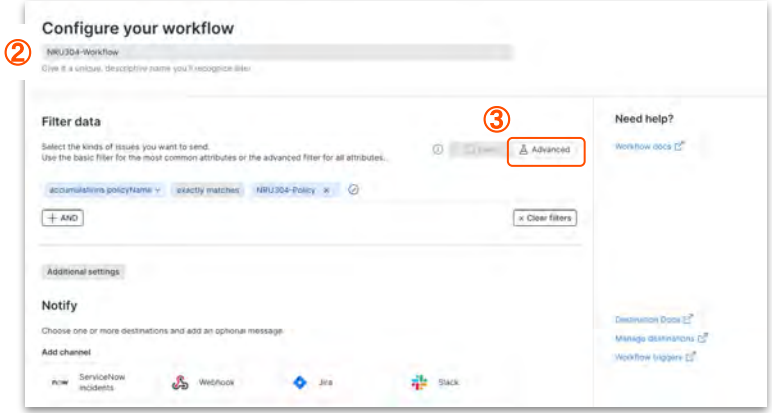
- 任意のAlert Condition名を設定します。
- Custom incident descriptionとRunbook URLはオプションです。何か思いついた内容を記載してみてください。
- Enable on saveが図の状態になっていることを確認し、Save conditionをクリックします。
- 設定確認画面が表示されるので、Closeをクリックして閉じます。

操作アカウント: Japan-NRU

ハンズオン(1-3) 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

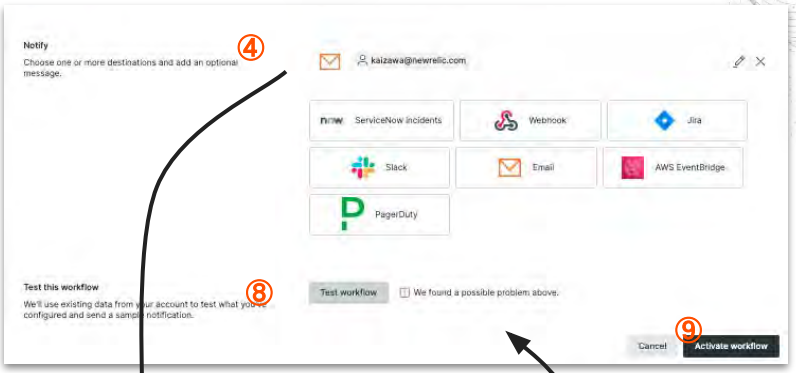




操作アカウント: Japan-NRU

ハンズオン(1-3) 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



new relic

操作アカウント: Japan-NRU

ハンズオン(1-3) Workflowを作成する 3/6

受信したテストメールを確認します。

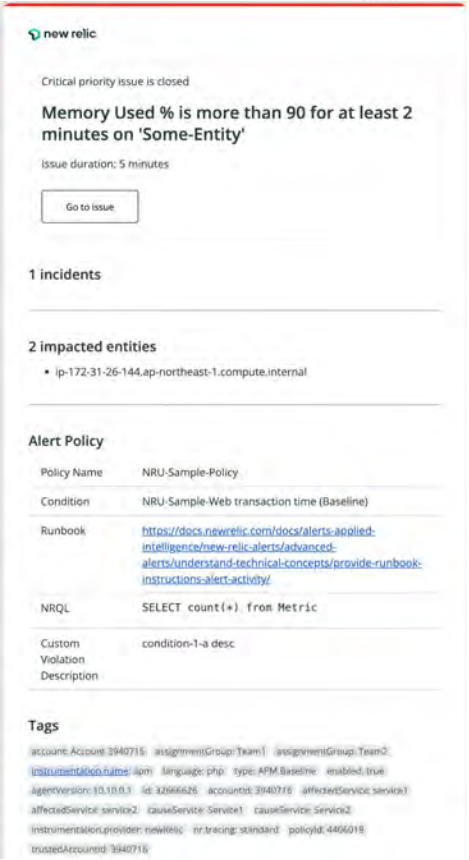
- Policy名やCondtion名は確認できますか？
- Runbook URLはどこに記載されていますか？
- Tagsというセクションには、どのような情報が含まれ ていますか？

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。

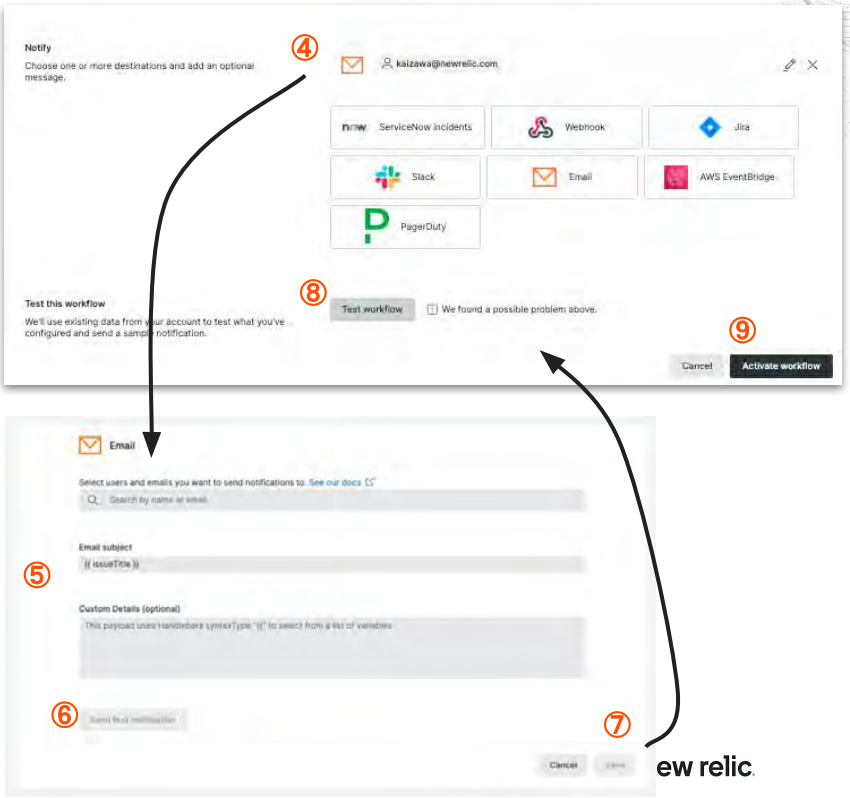


new relic

操作アカウント: Japan-NRU

ハンズオン(1-3) Workflowを作成する 4/6

8. Test workflowボタンを押し、テスト用メール内容 を確認してください。
   b. 先程のテスト用メールとどの様な違いがあるかを確認してください
9. Activate workflowボタンをクリックし、設定を保存します



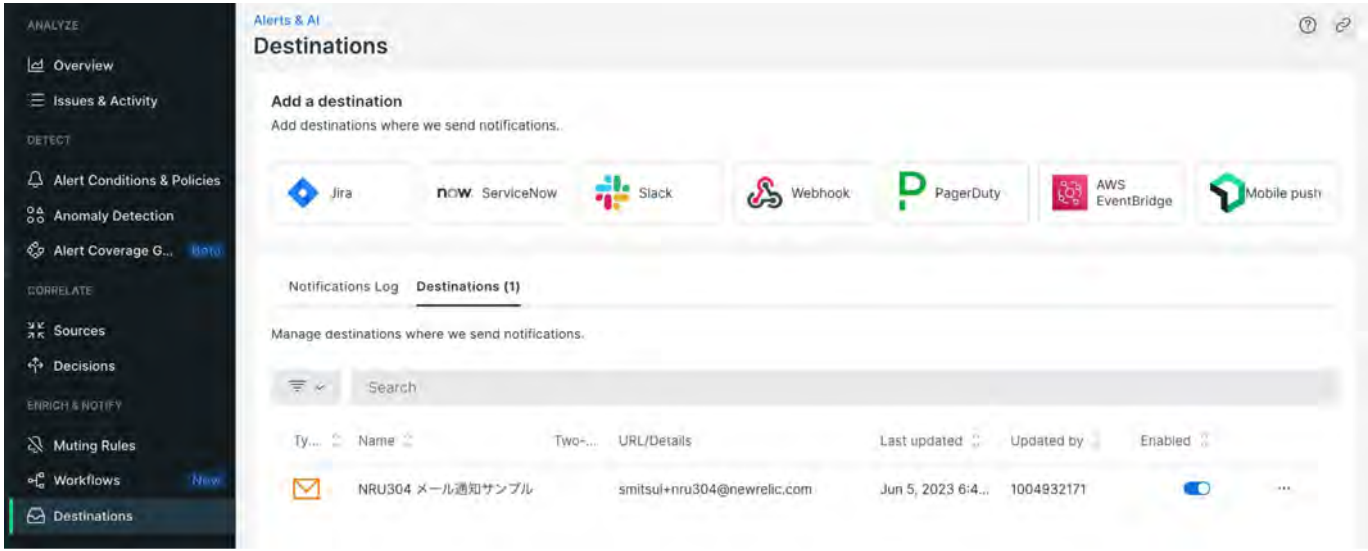
ew relic

操作アカウント: Japan-NRU

ハンズオン(1-3) 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。

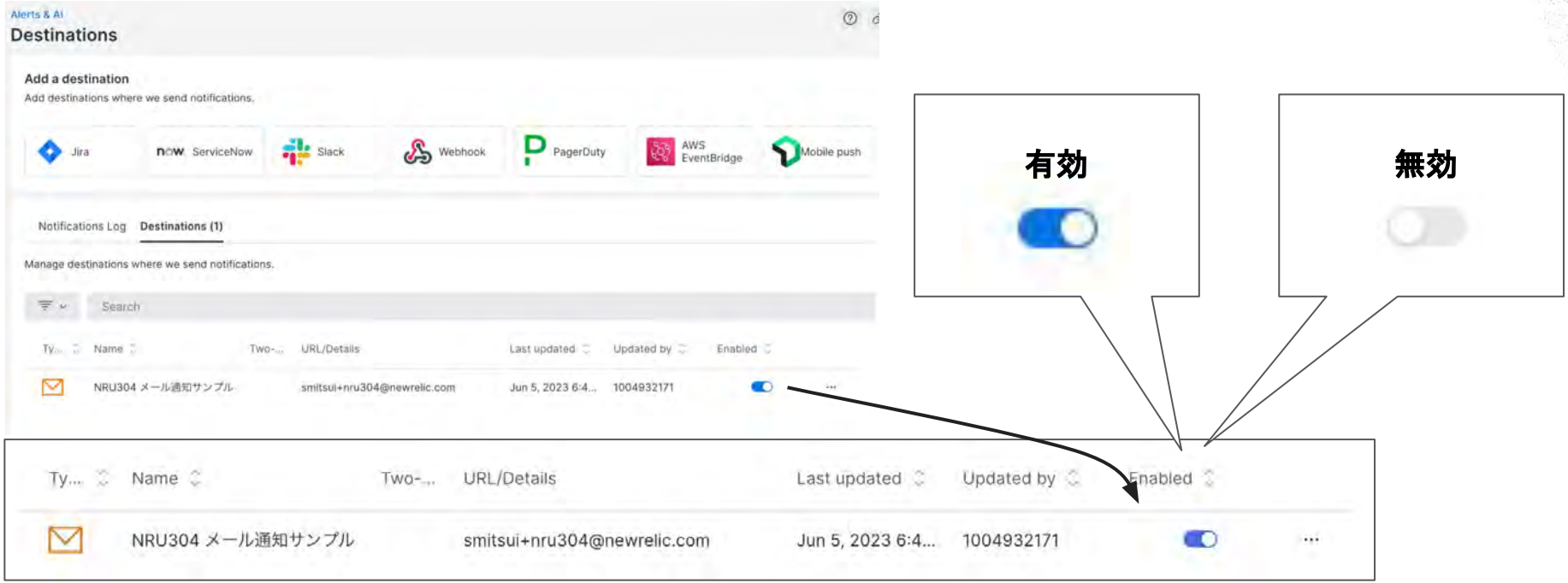
Alerts & AI > Destinationsで、ご自身のメールアドレスが追加されていることを確認します。



操作アカウント: Japan-NRU

ハンズオン(1-3) Workflowを作成する 6/6

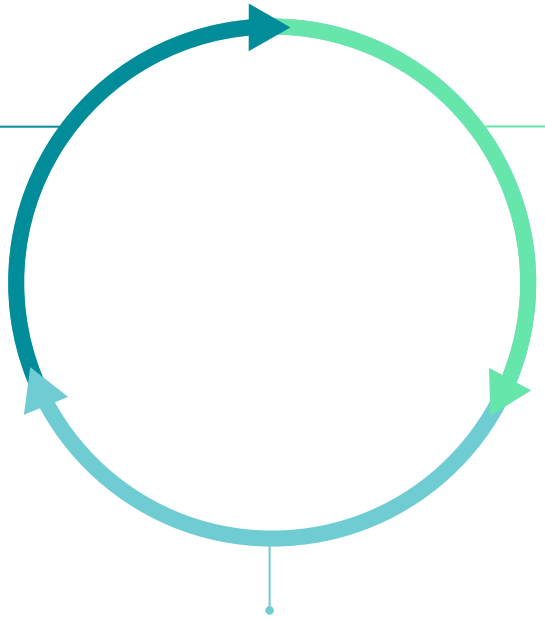
メール通知をこのセッション中に無効にしたい場合、Enabledトグルボタンを無効化して下さい。



座学(3)
New Relicのアラート分析支援機能

16:10 - 16:20 (10min)

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)

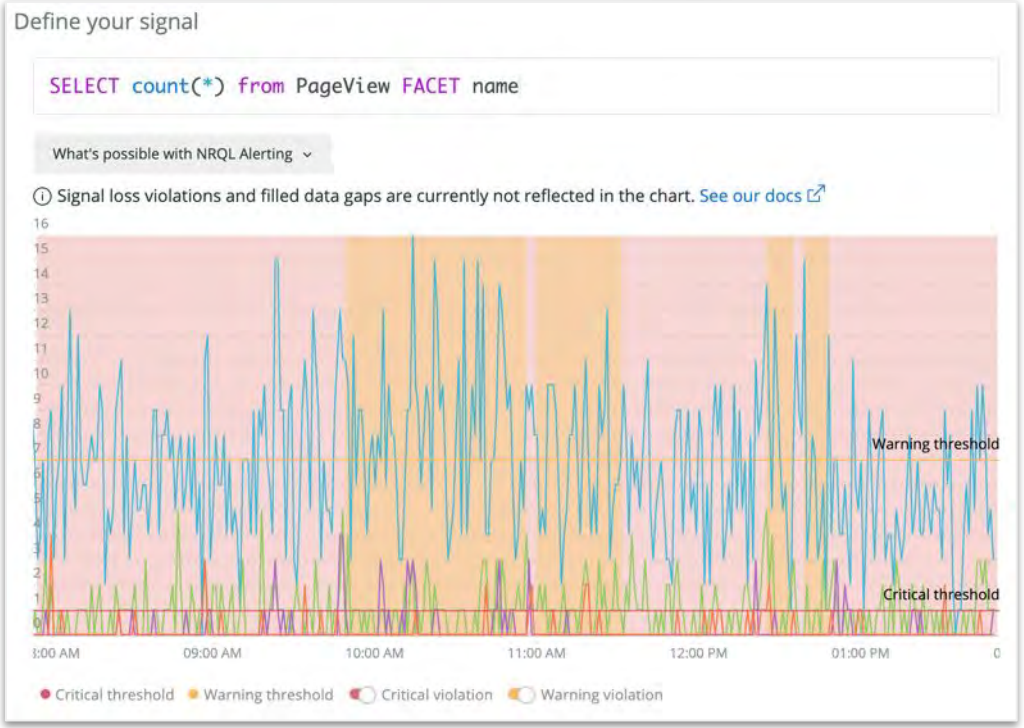
診断

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)

↓

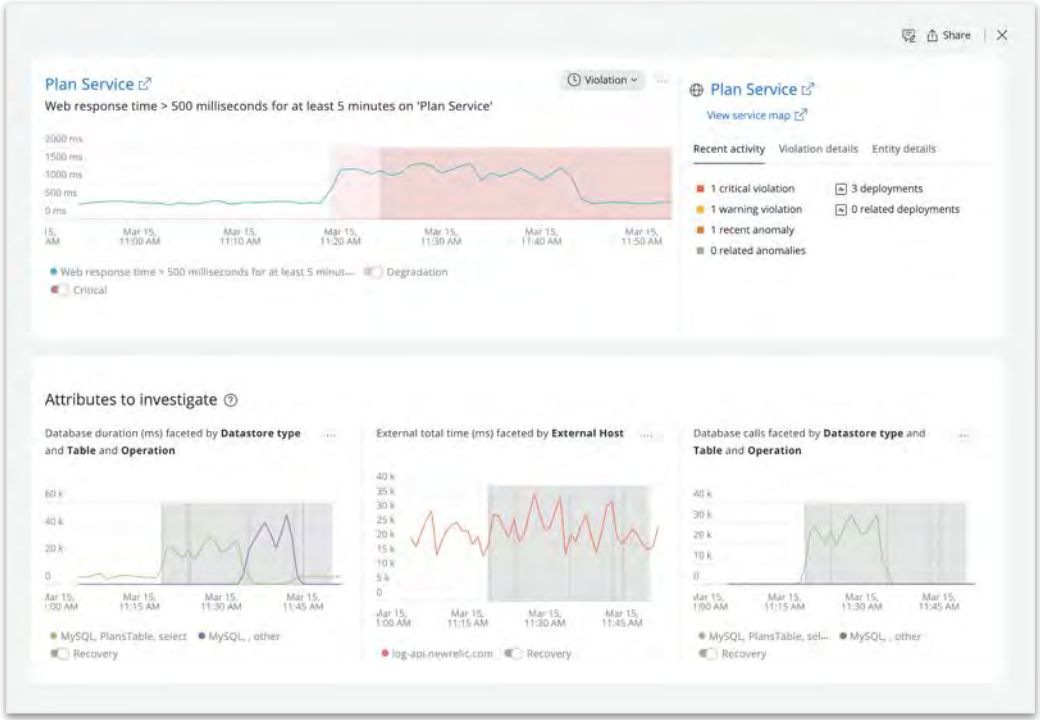
診断

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)**

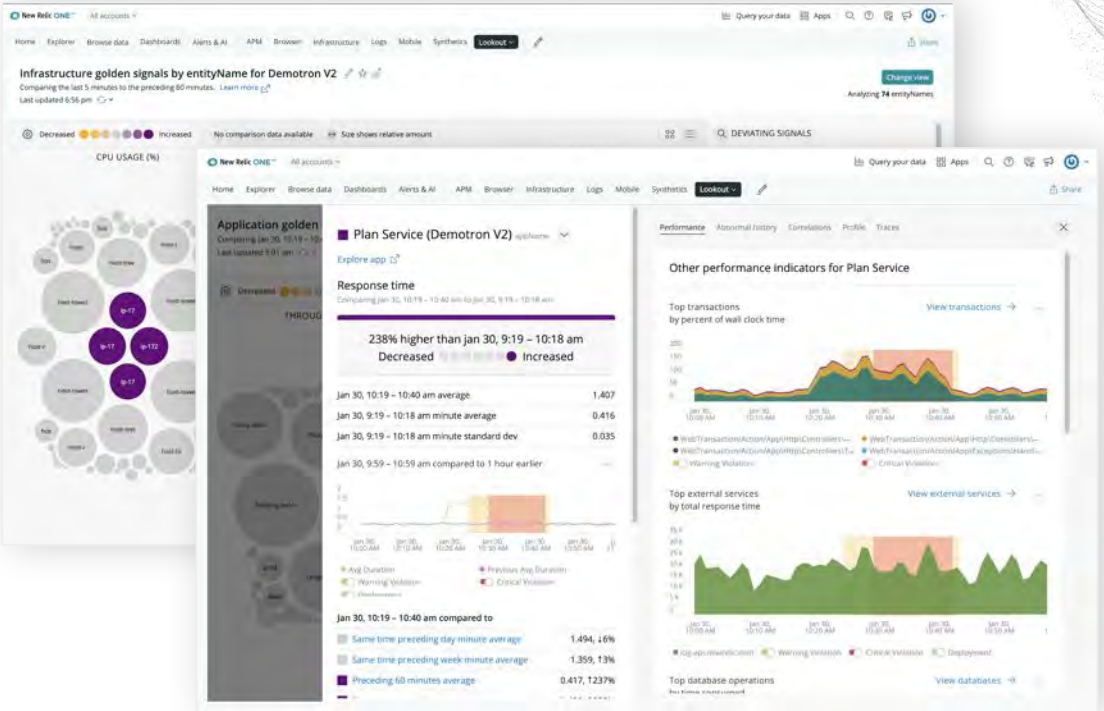
診断

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

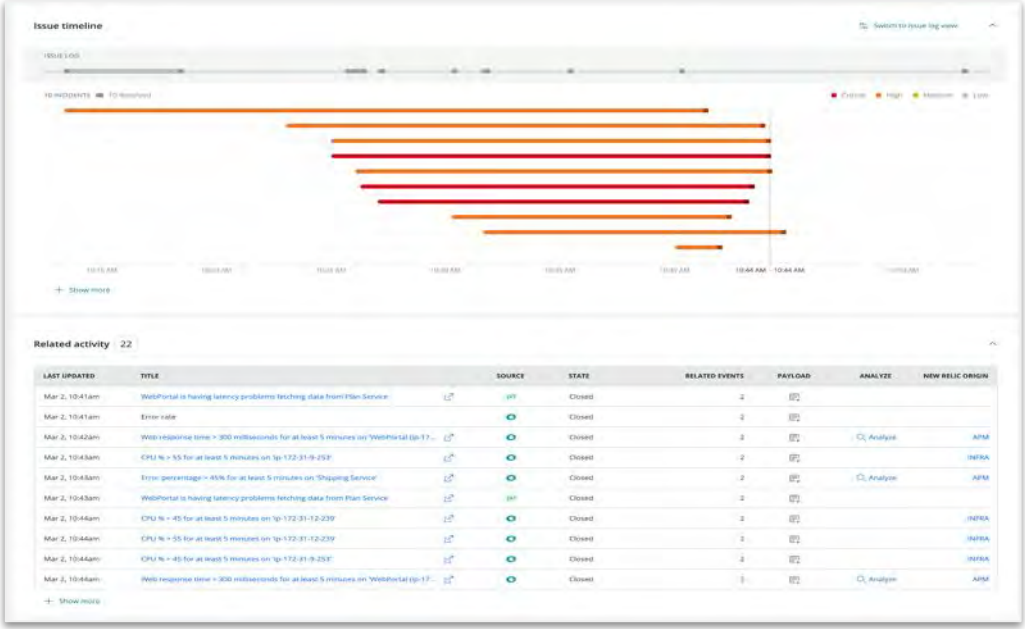
イベントの相関分析

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

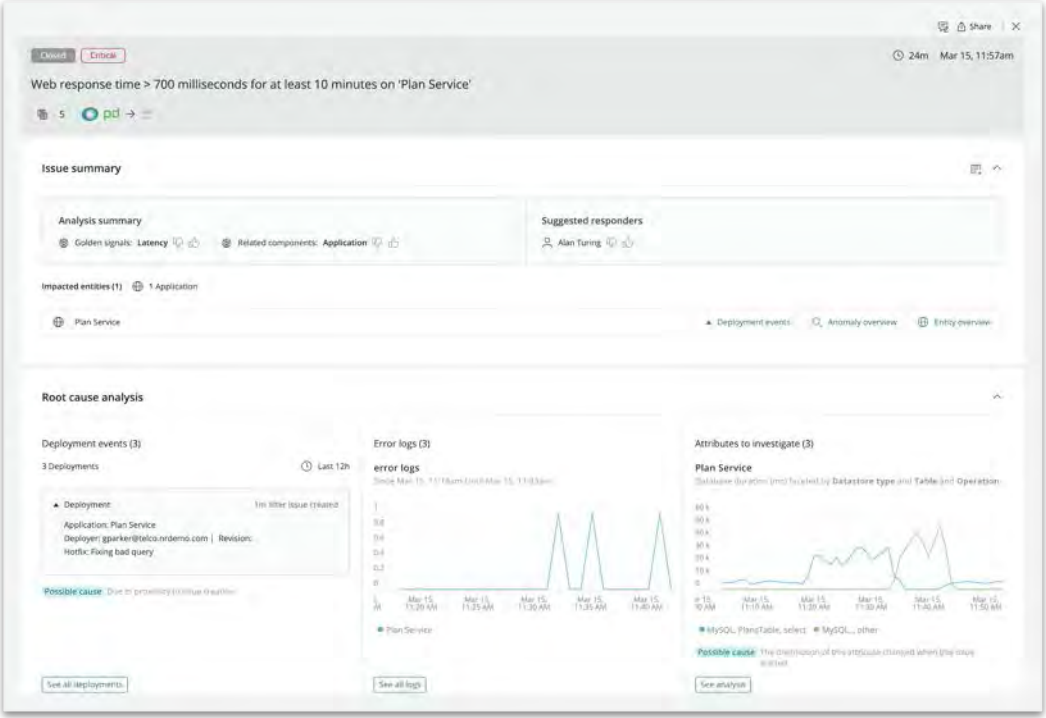
イベントの相関分析

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

検知

手動

異常検知
(通知)

異常検知
(探索)

↓

診断

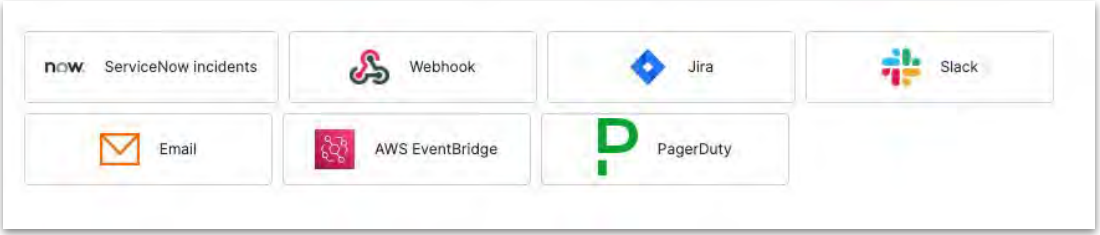
イベントの相関分析

根本原因分析

↓

対処

(外部ITSMツール: Servicenow, Pagerduty等)



ハンズオン(2)
アラート分析支援機能
ウォークスルー

16:20 - 16:30 (10min)

操作アカウント: Original New Relic Account (New Relic TSS)

ハンズオン(2-1) 異常を可視化する

[目的]
New Relicの異常検知の仕組みを使い、異常を可視化する機能を学びましょう

- Topメニューの”More”から”Lookout”を選択
  - 何が表示されているか確認しましょう
  - 目的に応じたカスタムのビューを作ってみましょう

注: Lookoutを見るときだけ、「Original New Relic account」にログインしてください
（詳細はこちら）

操作アカウント: Japan-NRU

ハンズオン(2-2) 個々のアラートを確認する

[目的]
New RelicのAlerts & AIに送られたアラートを把握します (後続の演習の事前確認)

- Alerts & AI → Overview → Incidentsで、個々のIncidentの詳細を確認する
  - 画面上部のフィルター設定で、Open中以外のものも表示してみましょう
  - それぞれ、Originがなにかを確認しましょう
  - メッセージから、どのようなアラートかを推測してみましょう

操作アカウント: Japan-NRU

ハンズオン(2-3) 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

[目的]

ハンズオン(2-2)で確認した個々のアラートがどのように紐付けられ、分析されているかを確認しましょう

- Alerts&AI → Overview → Issueで、個々のIssueを確認する
  - Root cause analysisや、Impacted entitiesにはどのような項目が書かれているでしょうか

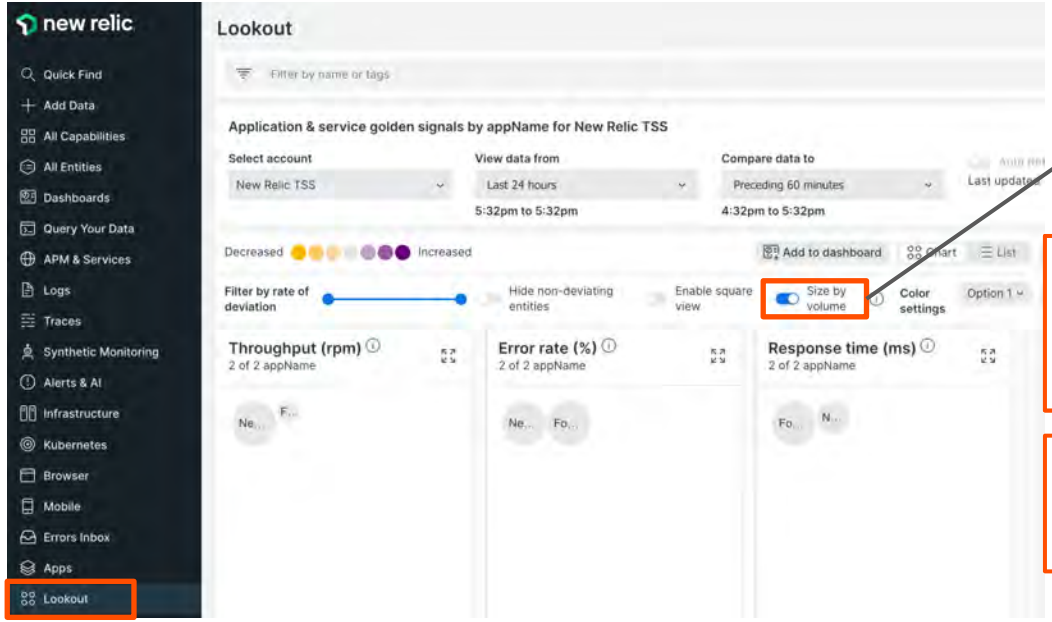
手順・解説

使用アカウント：Japan-NRUとOriginal New Relic Account
（ログイン先選択はこちら参照）

操作アカウント: Original New Relic Account (New Relic TSS)

ハンズオン(2-1) 異常を可視化する

- 「Original New Relic account」側にログインします（詳細手順は こちら）
- メニューから「Lookout」をクリックし、現れた画面上でサービスの現状を読み解きましょう



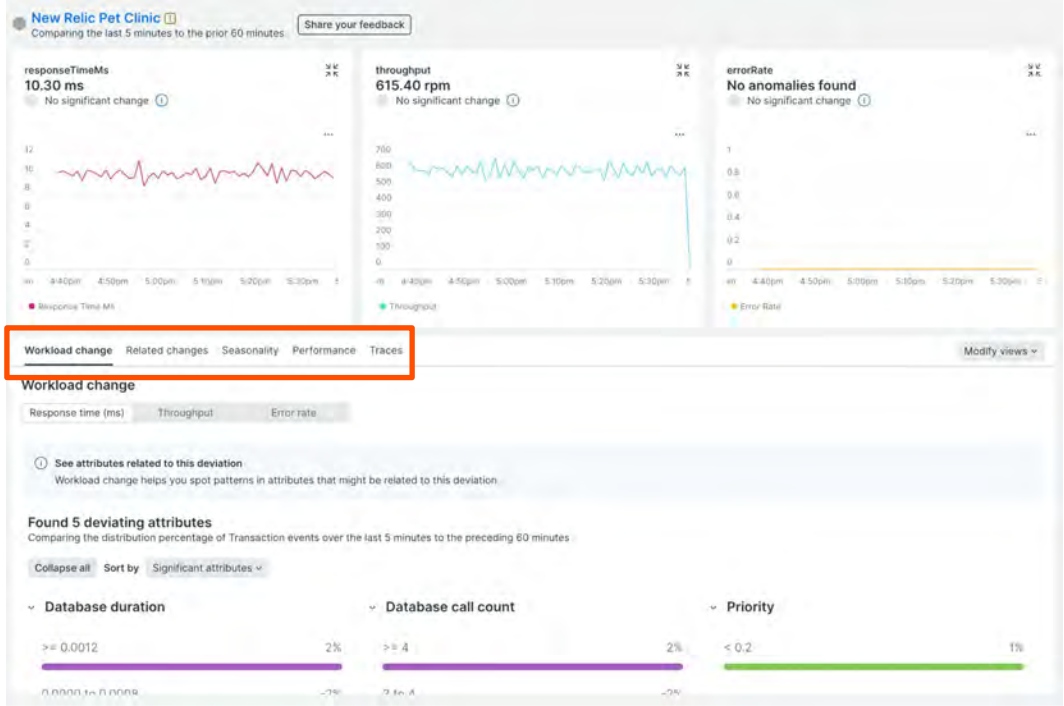
丸の単位はアプリケーション単位です
丸の大きさは値の大きさを、
丸の色は異常が発生しているかどうかを
表現しています

ハンズオン環境では大きな変化率を確認できない可能性があるため、その場合は後ほどデモ環境をお見せします

操作アカウント: Original New Relic Account (New Relic TSS)

ハンズオン(2-1) 異常を可視化する

- 気になる○(丸)を選択し、どのような変化が生じているか、詳細を確認します



各タブをクリックして、どのような情報が見えるか見てみましょう

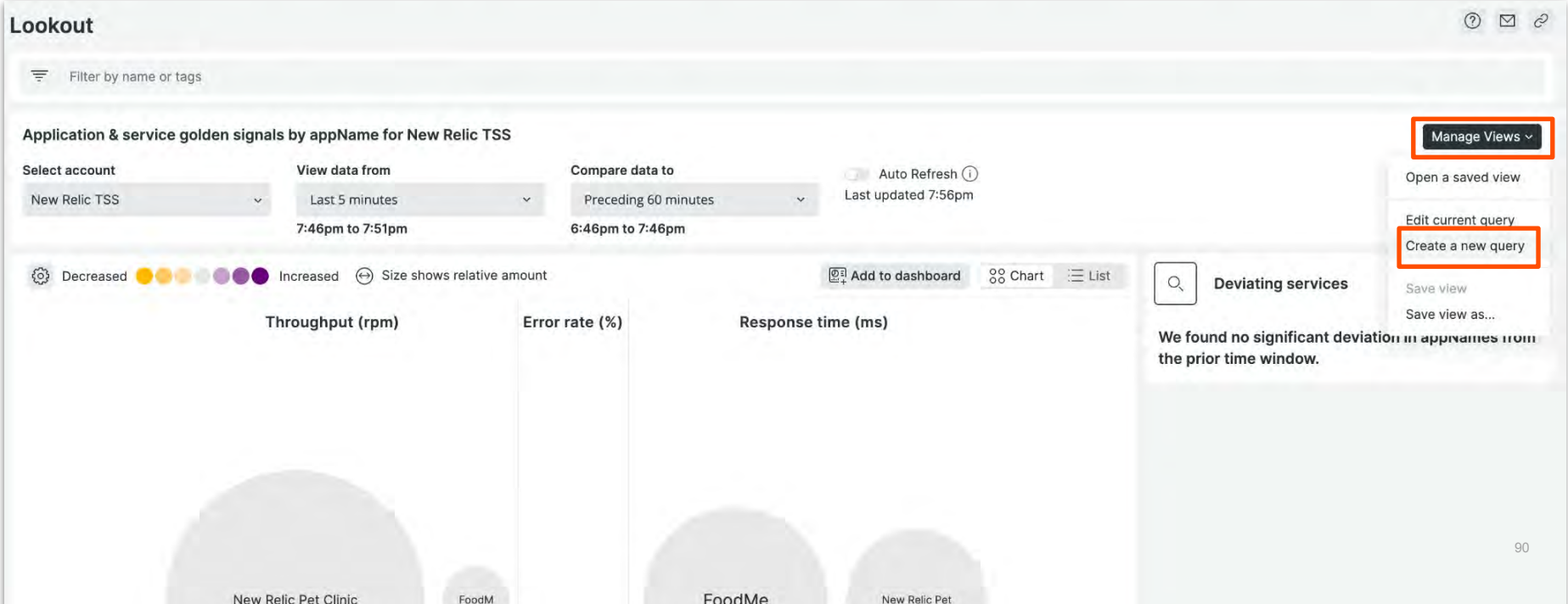
見終わったら右上のxをクリックします

操作アカウント: Original New Relic Account (New Relic TSS)

ハンズオン(2-1) 異常を可視化する

- カスタムのビューを作成します

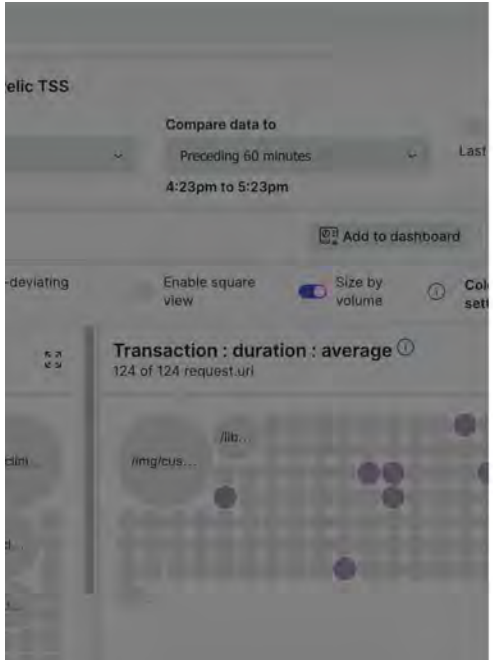
Manage Views → Create a new queryを選択

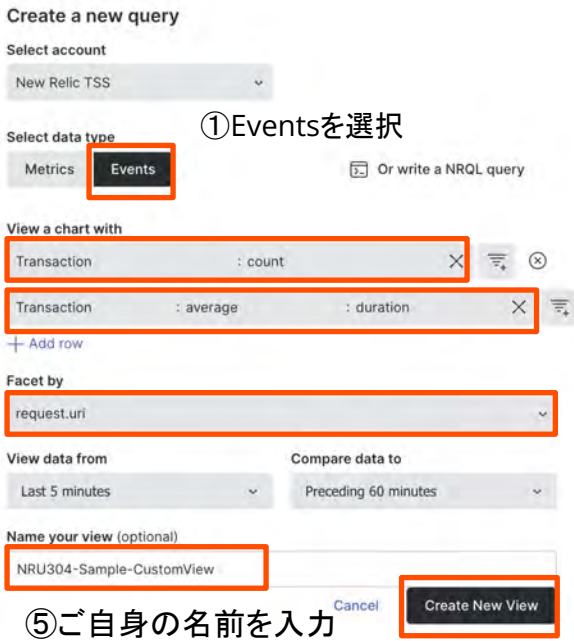


操作アカウント: Original New Relic Account (New Relic TSS)

ハンズオン(2-1) 異常を可視化する

- カスタムのビューを作成します(続き)。作成後の画面から詳細分析ができます。
  この手順によりアクセス先URLごとでのレスポンスの多さと速さの大きさ、変化率が可視化できます。





①Eventsを選択

②Select your event ->
Build a custom queryから
Transaction->countを選択

③Add rowし、同じ要領でTransaction
->average->durationを選択

④request.uriを選択

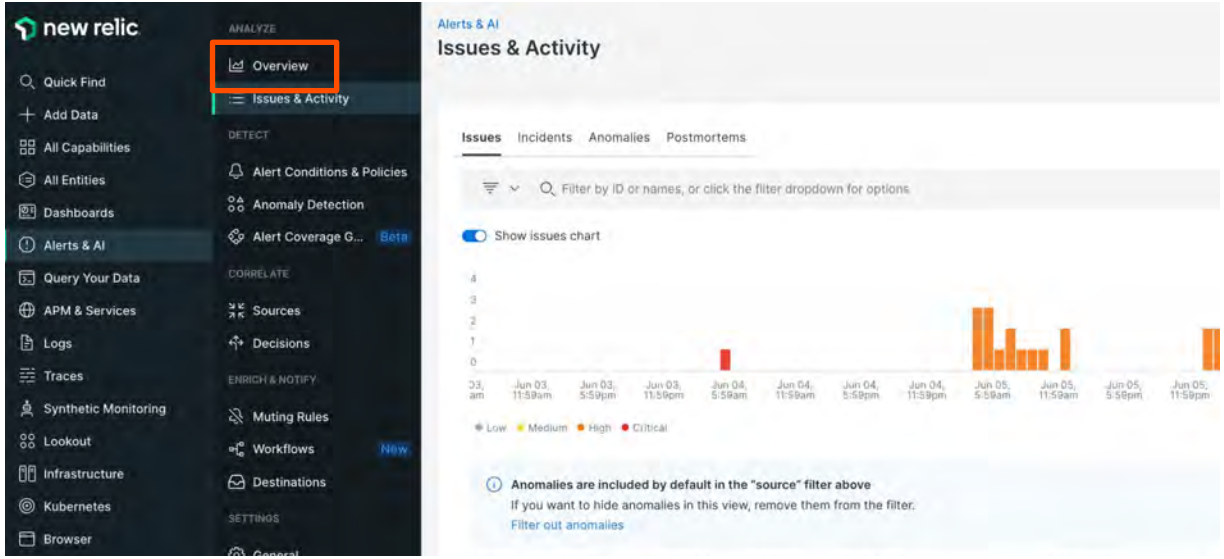
⑤ご自身の名前を入力

⑥Create New Viewをクリック

操作アカウント: Japan-NRU

ハンズオン(2-2) 個々のアラートを確認する

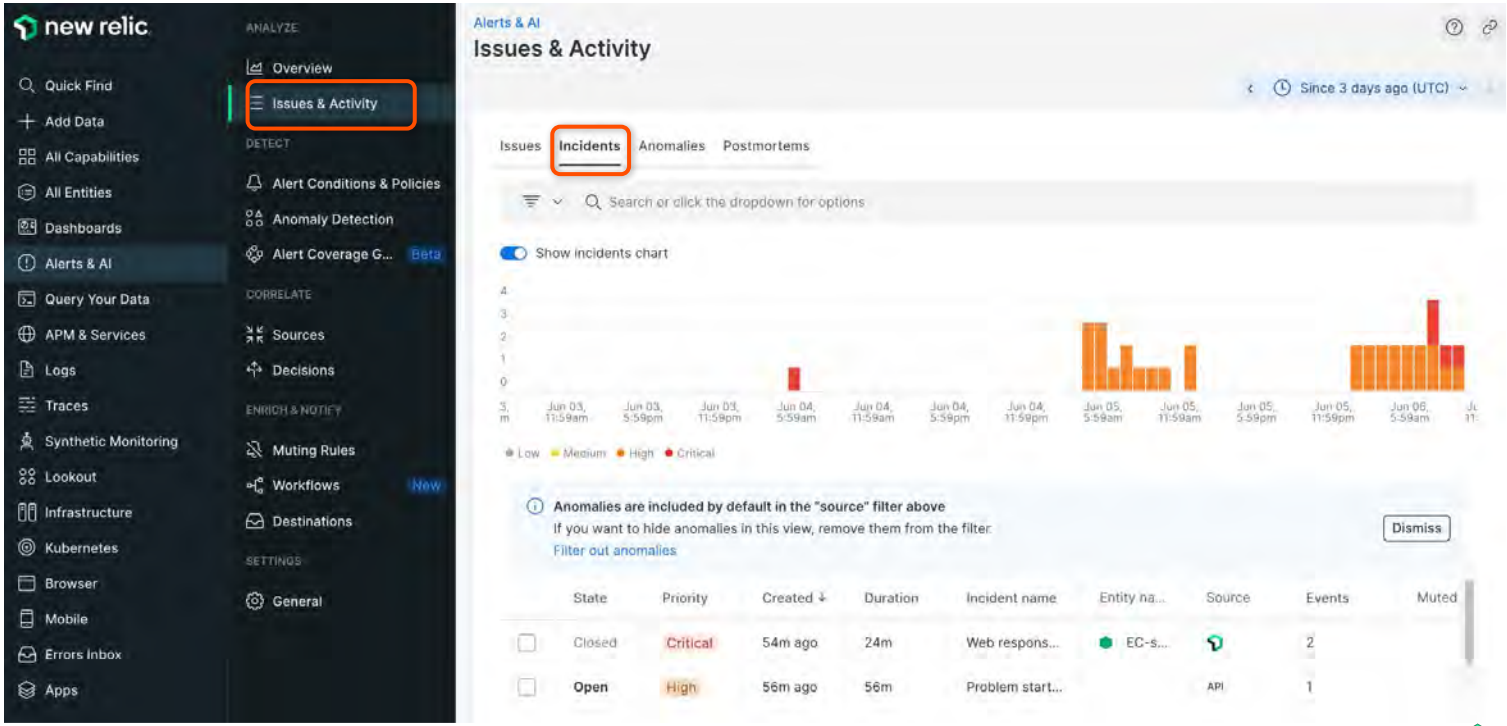
- 「Organization: Japan-NRU」アカウントにログインし直します
- Alerts & AI、[Overview]をクリックします



操作アカウント: Japan-NRU

ハンズオン(2-2) 個々のアラートを確認する

- 「Issues & activity」>「Incidents」タブをクリックします。



操作アカウント: Japan-NRU

ハンズオン(2-2) 個々のアラートを確認する

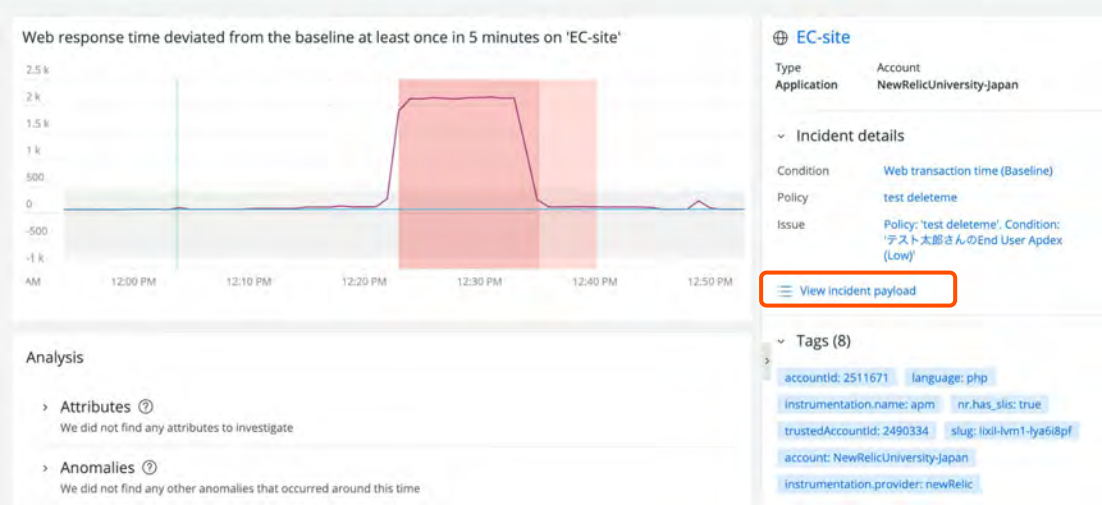
- Incidentをクリックします。

	State	Priority	Created ↓	Duration	Incident name	Entity na...	Source	Events	Muted
☐	Closed	Critical	54m ago	24m	Web respons...	EC-s...		2	
☐	**Open**	High	56m ago	56m	Problem start...		API	1	
☐	Closed	Critical	1h 55m ...	31m	Web respons...	EC-s...		2	

操作アカウント: Japan-NRU

ハンズオン(2-2) 個々のアラートを確認する

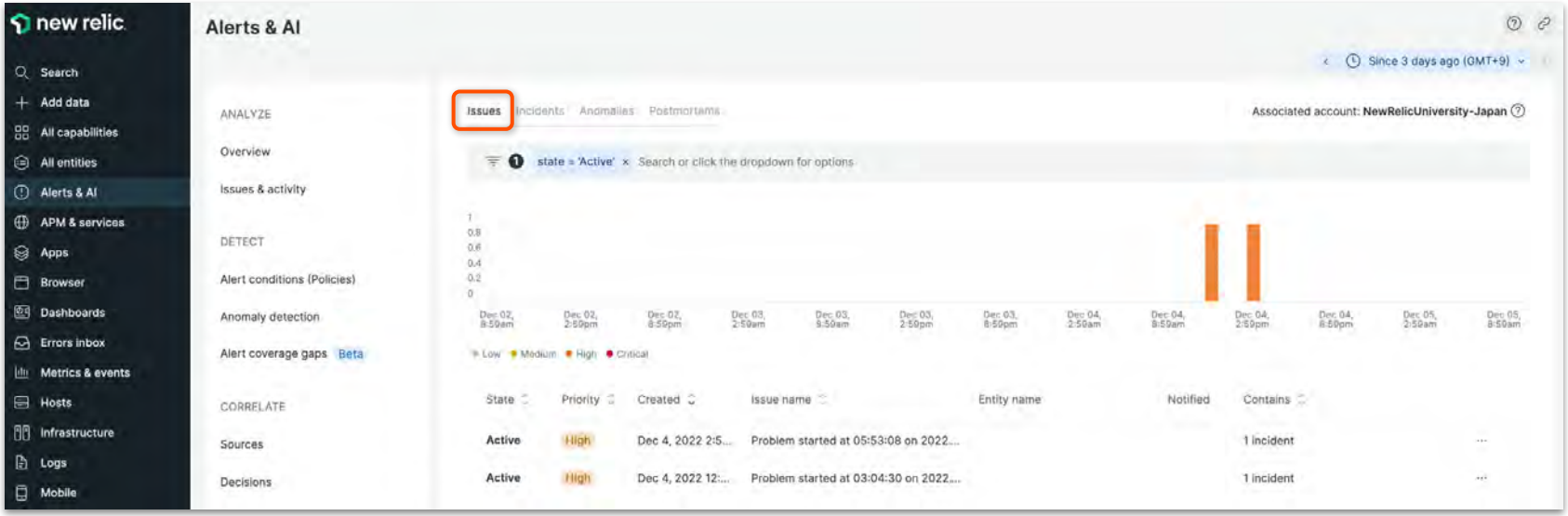
- Origin Key の値を確認することで、どのツールによって判定されたアラートかを確認することができます。



操作アカウント: Japan-NRU

ハンズオン(2-3) 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

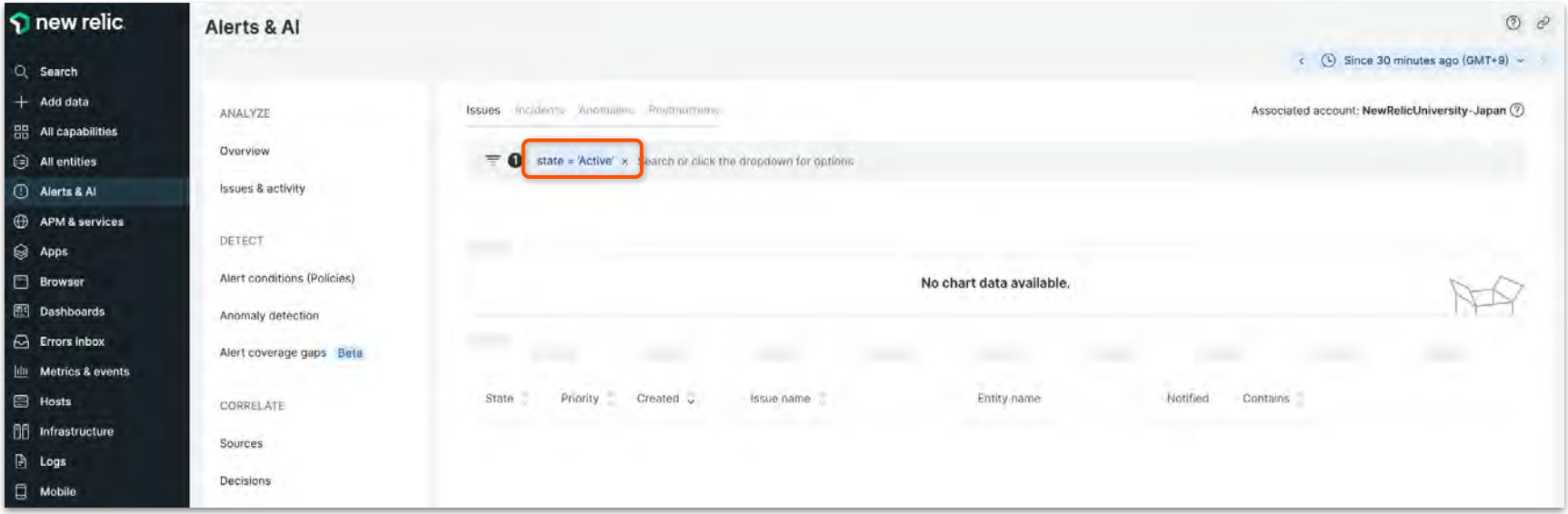
- 「Issues」タブをクリックします。



操作アカウント: Japan-NRU

ハンズオン(2-3) 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

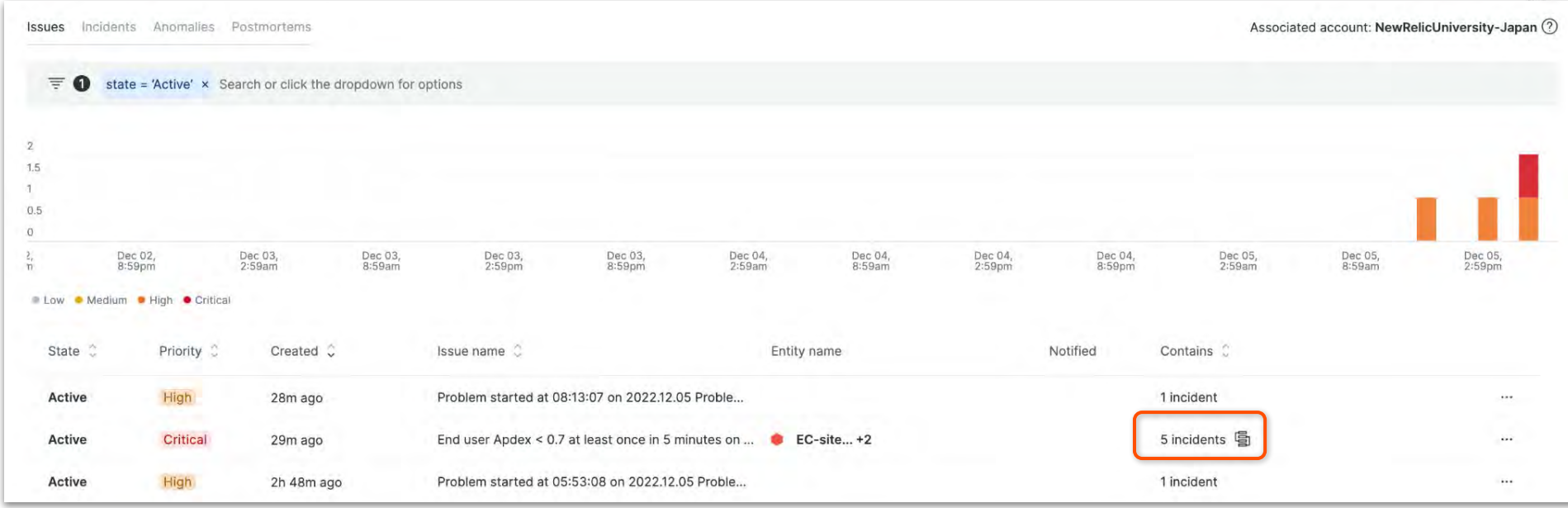
- オープン中のIssueが存在しない場合は「Active」フィルタを削除します。



操作アカウント: Japan-NRU

ハンズオン(2-3) 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

- 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。



操作アカウント: Japan-NRU

ハンズオン(2-3) 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

- Issueをクリックすると詳細が表示されます。

Issues Incidents Anomalies Postmortems

Associated account: NewRelicUniversity-Japan

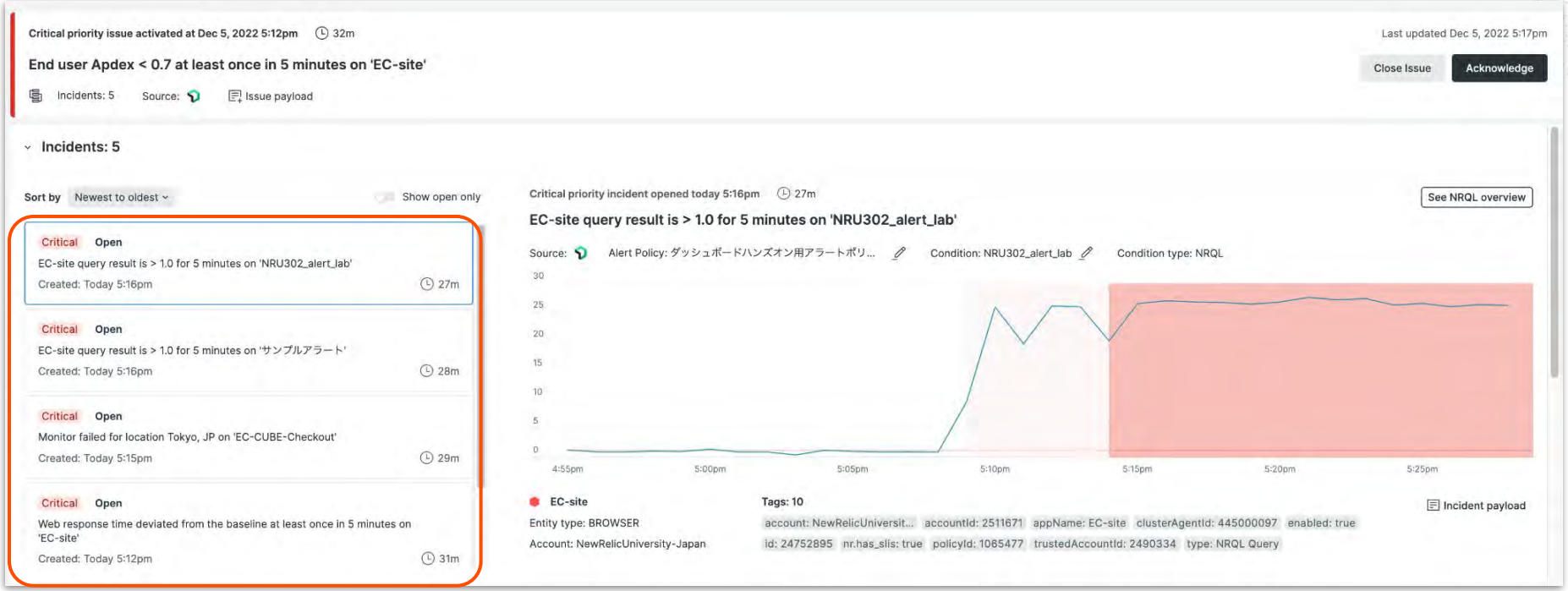
1 state = 'Active' × Search or click the dropdown for options

State	Priority	Created	Issue name	Entity name	Notified	Contains
Active	High	28m ago	Problem started at 08:13:07 on 2022.12.05 Proble...			1 incident
Active	Critical	29m ago	End user Apdex < 0.7 at least once in 5 minutes on ...	EC-site... +2		5 incidents
Active	High	2h 48m ago	Problem started at 05:53:08 on 2022.12.05 Proble...			1 incident

操作アカウント: Japan-NRU

ハンズオン(2-3) 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

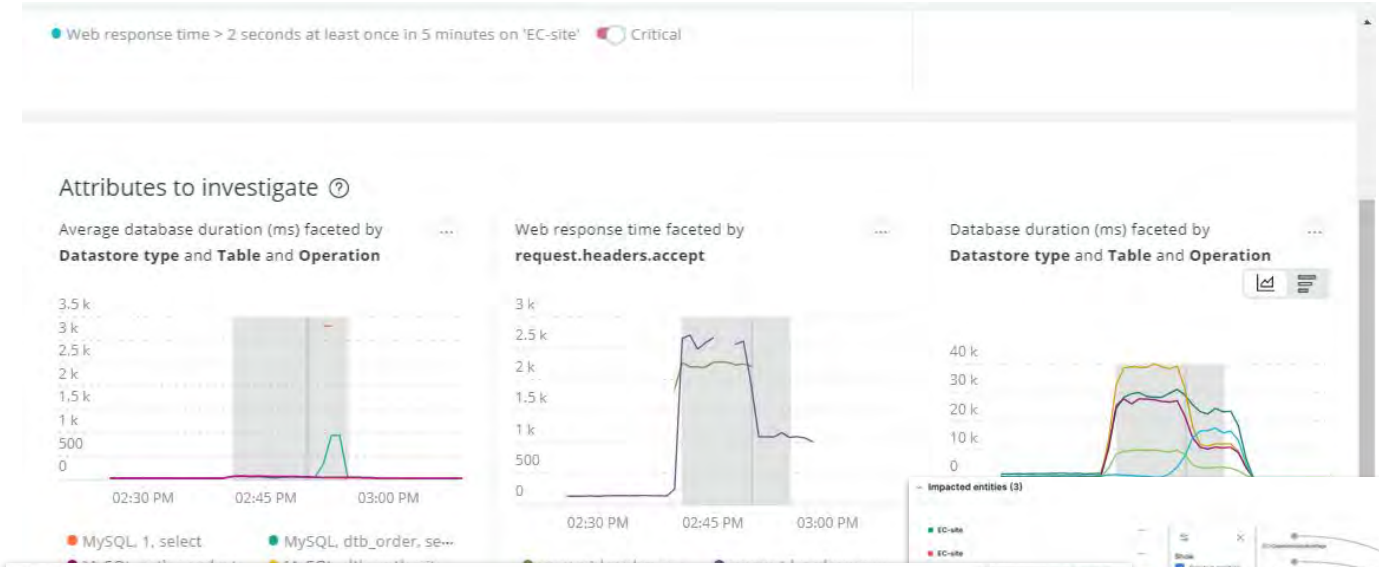
- どのIncidentがまとめられているのか確認することができます

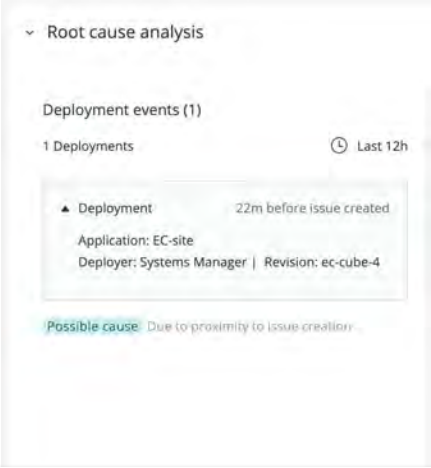


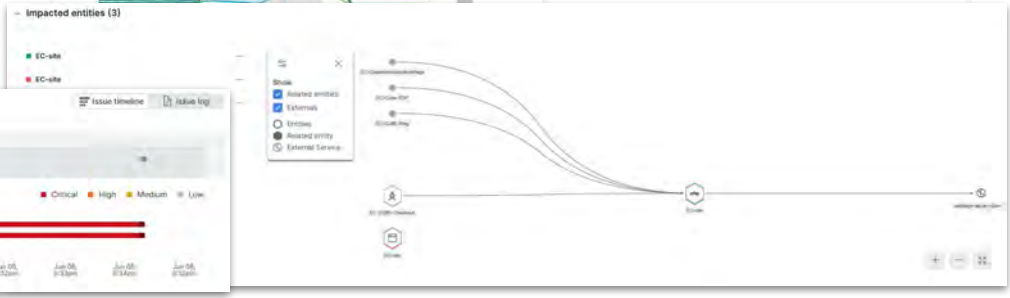
操作アカウント: Japan-NRU

ハンズオン(2-3) 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

- 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







座学(4)
AIOpsの意義

16:30 - 16:45 (15min)

new relic

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*

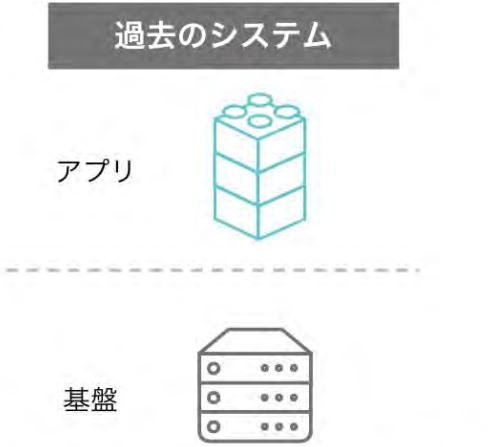
New RelicのAlerts & “**AI**”

→ **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

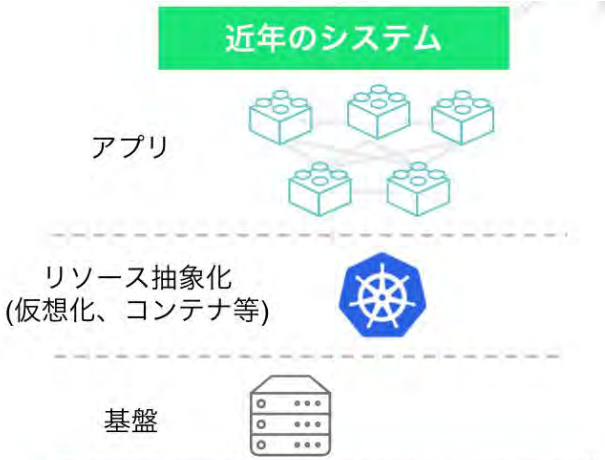
AIOpsが必要とされる背景

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



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

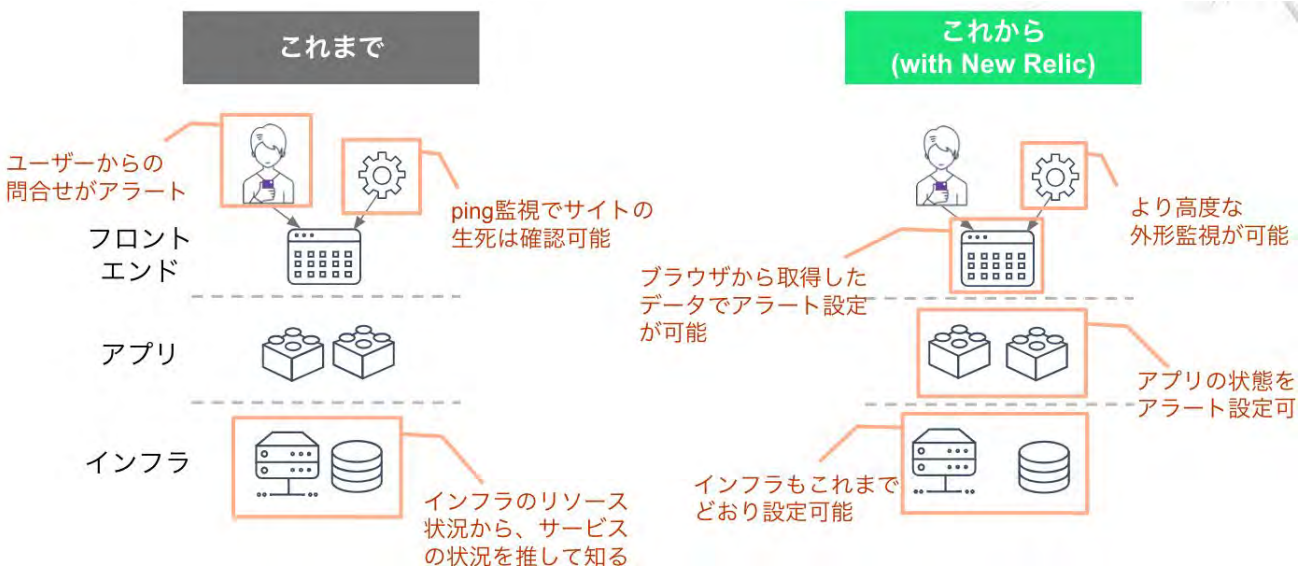


アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

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

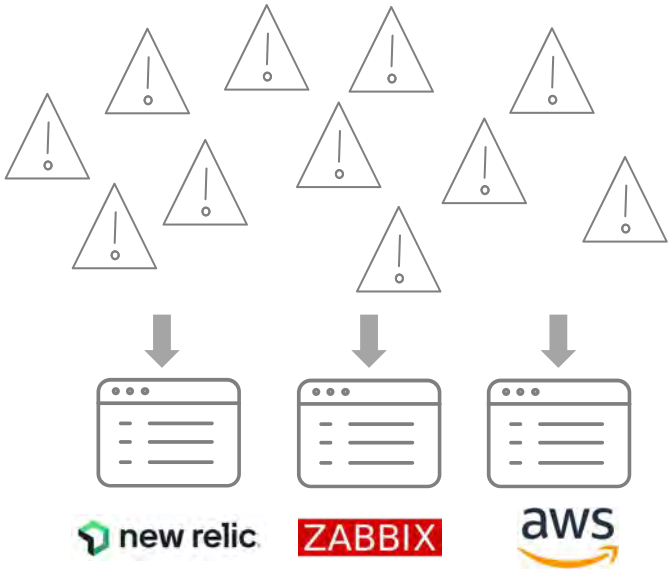
New Relicのようなオブザーバビリティプラットフォームによって、サービスを構成する様々なコンポーネントから多種多様なデータを取得できるように



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

気づけない

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**
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

複数の事象を自動で関連付け
根本原因を推察

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

手動でアラート
設定せずとも自動
で検知

気づけない

Actionableな監視 収集したデータを機械学習で分析し Actionableな監視を増やす	**とりあえずの監視**
Actionableな監視予備群	**監視できていない未知の領域**

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**

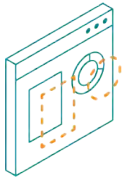
手動でアラート設定せずとも自動で検知

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]

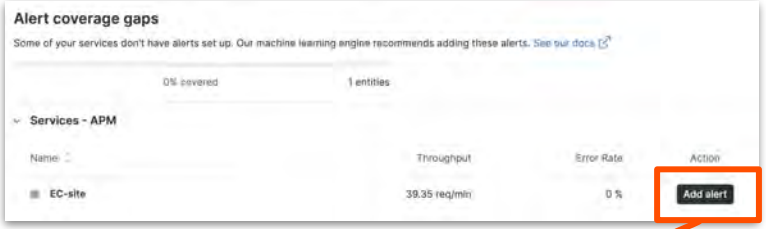
- **イベントの相関分析**
- **根本原因分析**



複数の事象を自動で関連付け、根本原因を推察

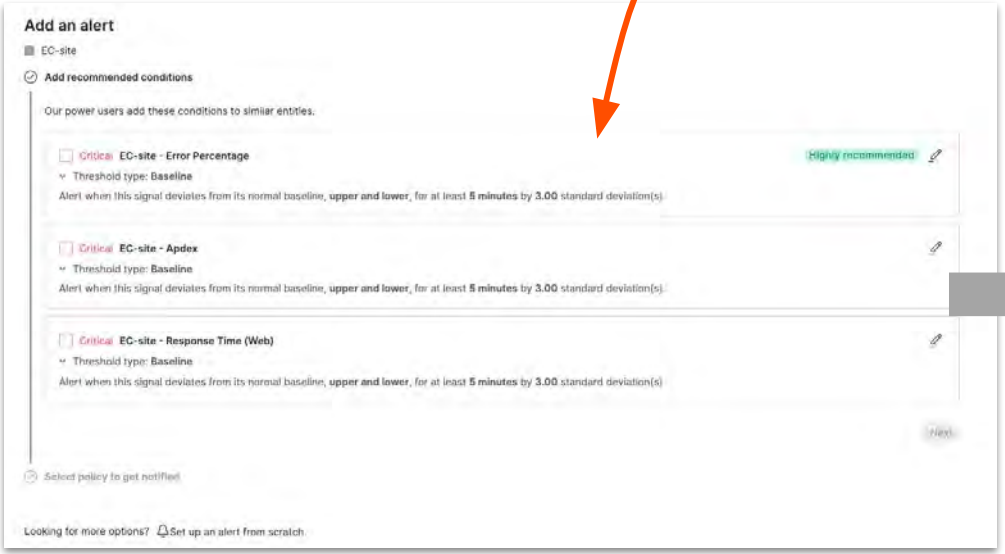
Correlation
Root Cause Analysis

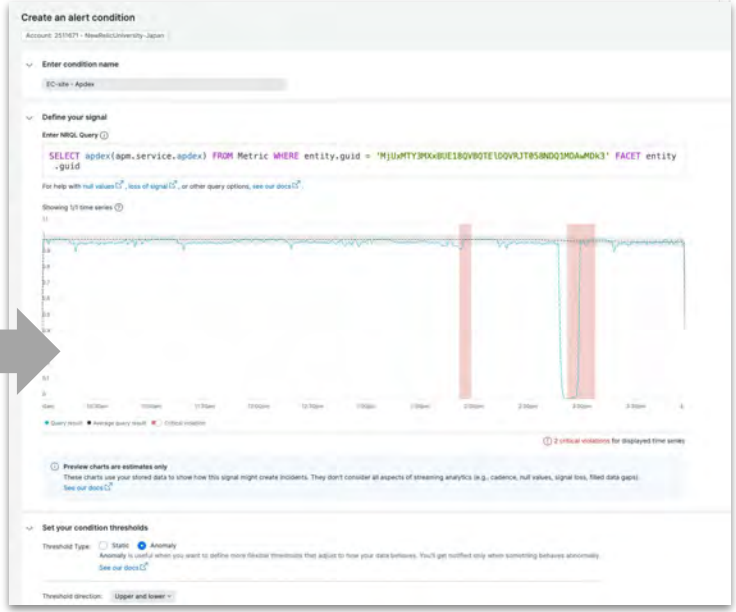
機能紹介: Alert coverage gaps



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。



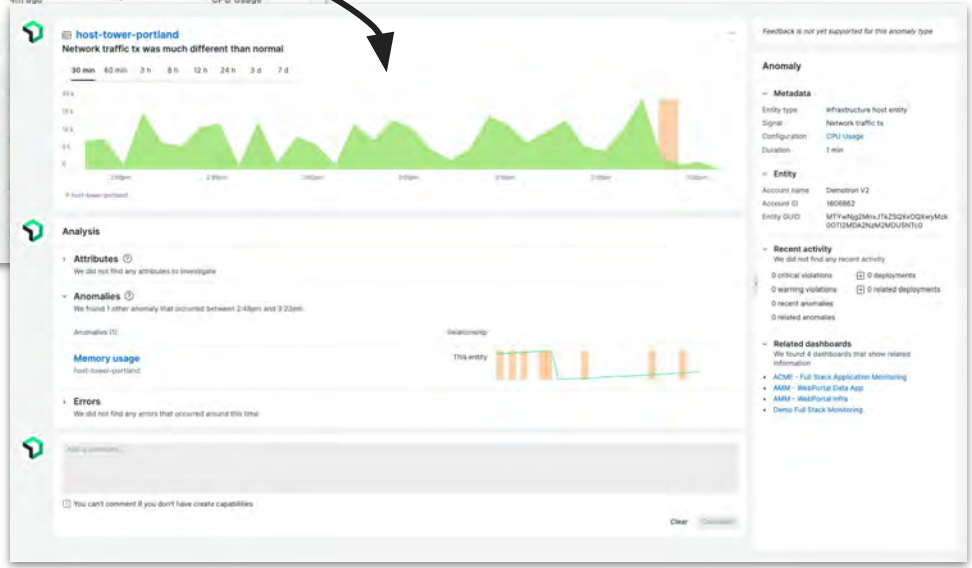


Alerts & AI → Alert coverage gaps

new relic

機能紹介: Anomaly Detection

現行では、APMのみの対応となっていますが、HOSTやBrowserなど、他のentityのサポートを今後計画しています。



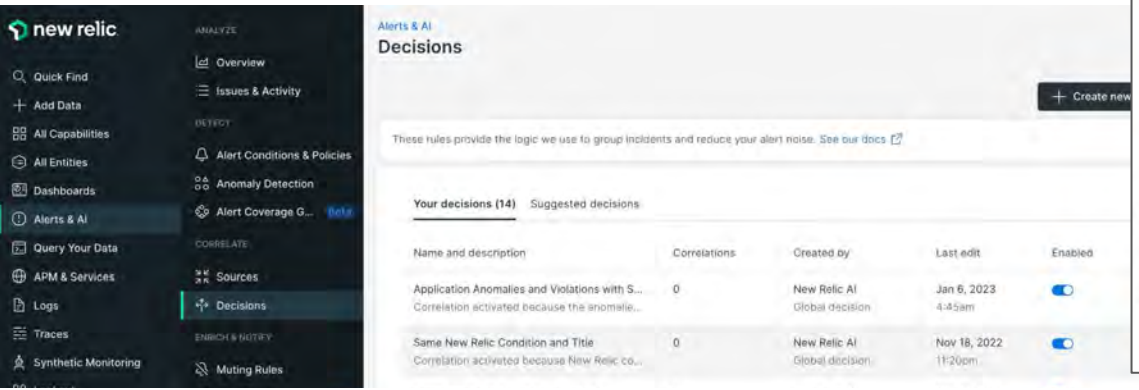
Alerts & AI → Issues & activity → Anomalies

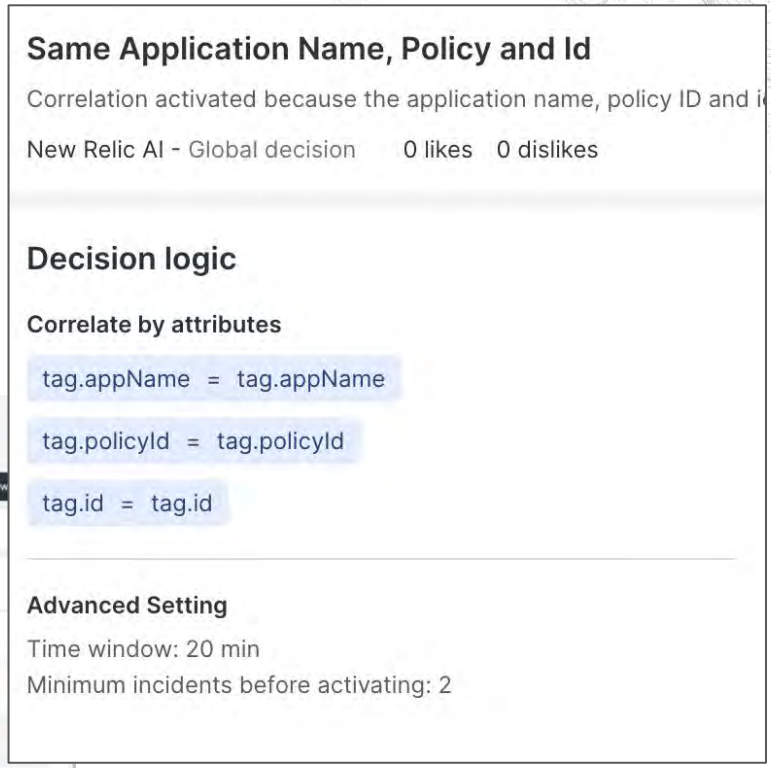
- 発生したAnomalyの1つを選択し、詳細を確認する

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

ハンズオン(3)
AIOpsを使った異常検知と原因分析

16:45 - 16:55 (10min)

操作アカウント: Japan-NRU

ハンズオン(3)

AIOps:異常検知

3-1 AIOpsの機能をセットアップする : 異常検知の設定

[目的]
異常検知を有効化しましょう

- Alerts & AI → Anomaly Detectionを選択
- Add a configurationを押す
- 設定名は自分の名前、アカウントは New Relic University Japan(3940716)、アプリはEC-siteを選択
- Anomalies種別は全てチェック、通知は No notificationに設定して [Save configuration]

操作アカウント: Japan-NRU

ハンズオン(3)

AIOps:イベントの相関分析

3-2 AIOpsの機能をセットアップする : 相関分析の有効化

[目的]
AIOpsの機能を活用するため、作成したアラートポリシーの相関分析を有効化しましょう

- Alerts & AI → Sourcesを選択
- Alertsカードを選択
- [+ Add a policy]をクリックして自分が作成した Alert Policyを追加する

ハンズオン(3)

AIOps:イベントの相関分析

3-3 AIOpsの機能をセットアップする： New Relic以外のイベントデータを取り込む

（実際に手を動かすものではなく、スライドに目を通して頂ければ OKです）

[参考情報] Zabbixからのイベント取り込みの設定例

- Zabbix 5.0 以降で追加されたwebhook メディアタイプによって、ZabbixのAlertをNew Relci Incident Intelligence APIに通知することができます。
- ZabbixのMacroから値を受け取り、New Relic APIエンドポイントURLとInsights Insert Keyを利用してJavaScript から送信することができます。

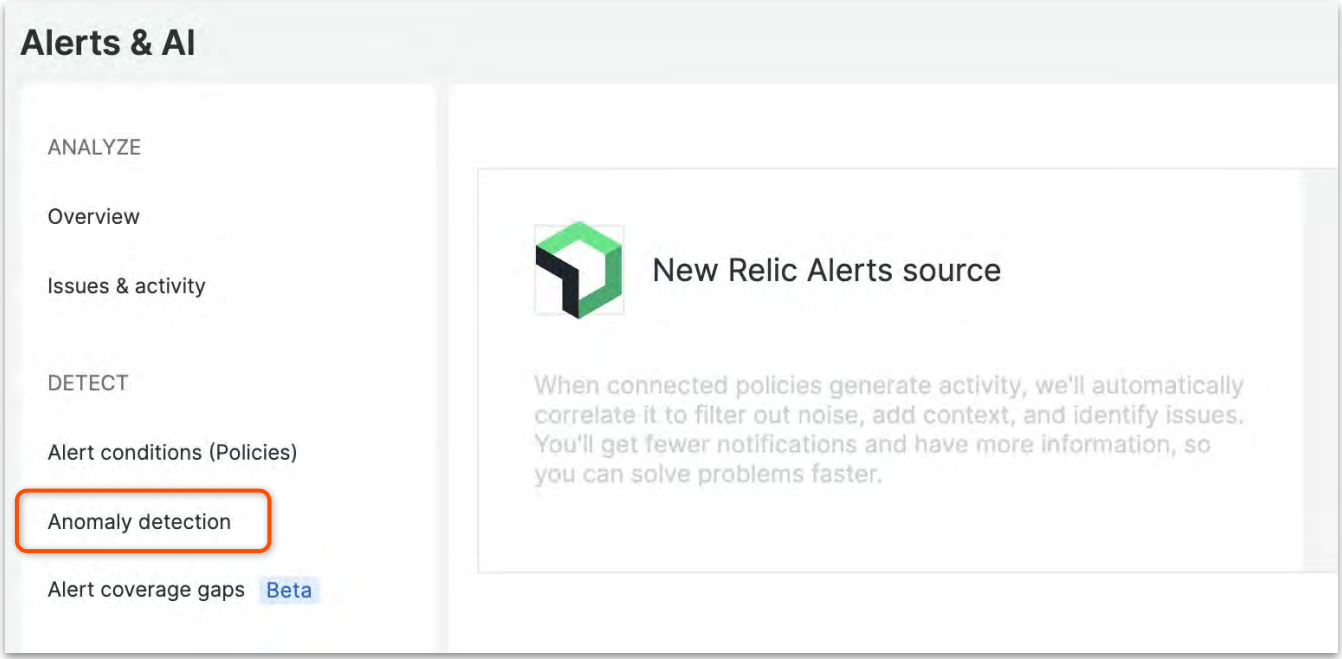
手順・解説

使用アカウント：Japan-NRU
（ログイン先選択は[こちら]参照）

操作アカウント: Japan-NRU

ハンズオン(3-1) AIOpsの機能をセットアップする

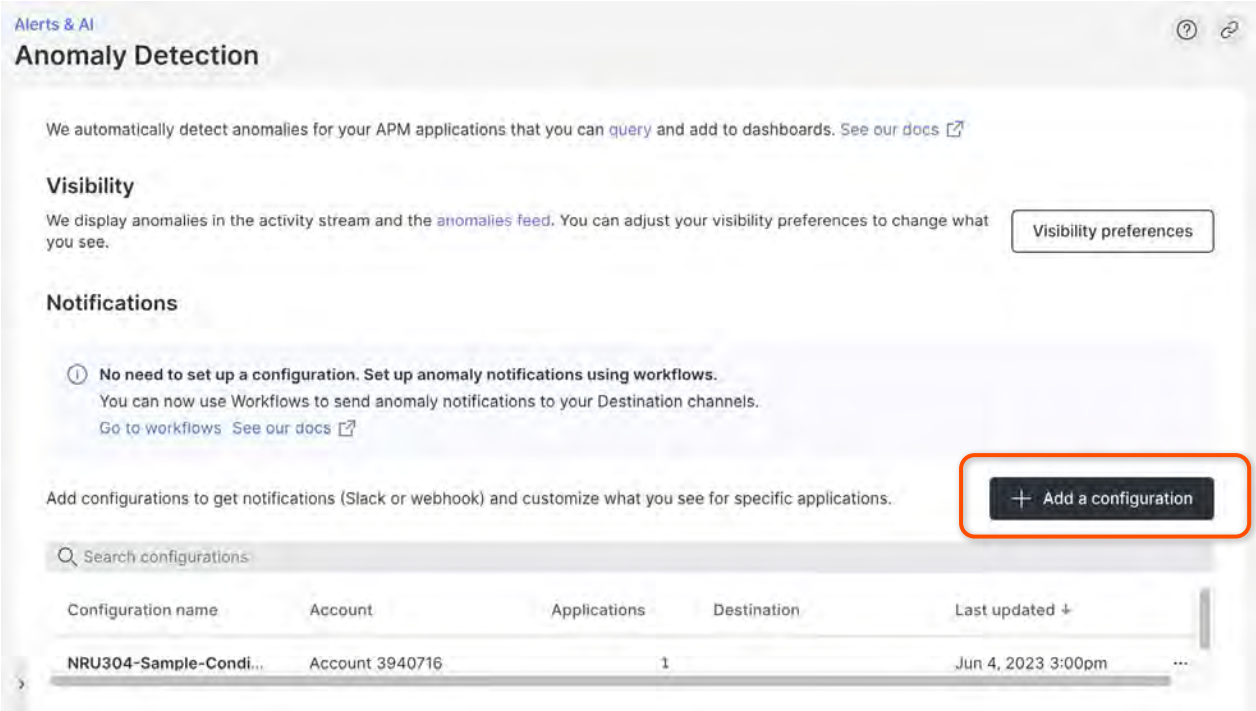
- Alerts&AI > Anomaly detection をクリックします。



操作アカウント: Japan-NRU

ハンズオン(3-1) AIOpsの機能をセットアップする

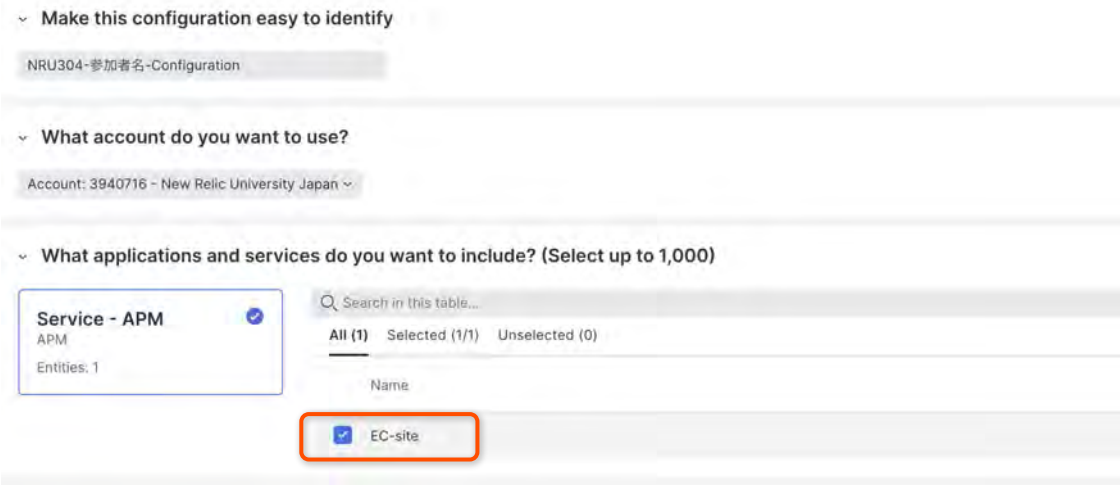
- [＋ Add a Configuration] ボタンをクリックします。



操作アカウント: Japan-NRU

ハンズオン(3-1) AIOpsの機能をセットアップする

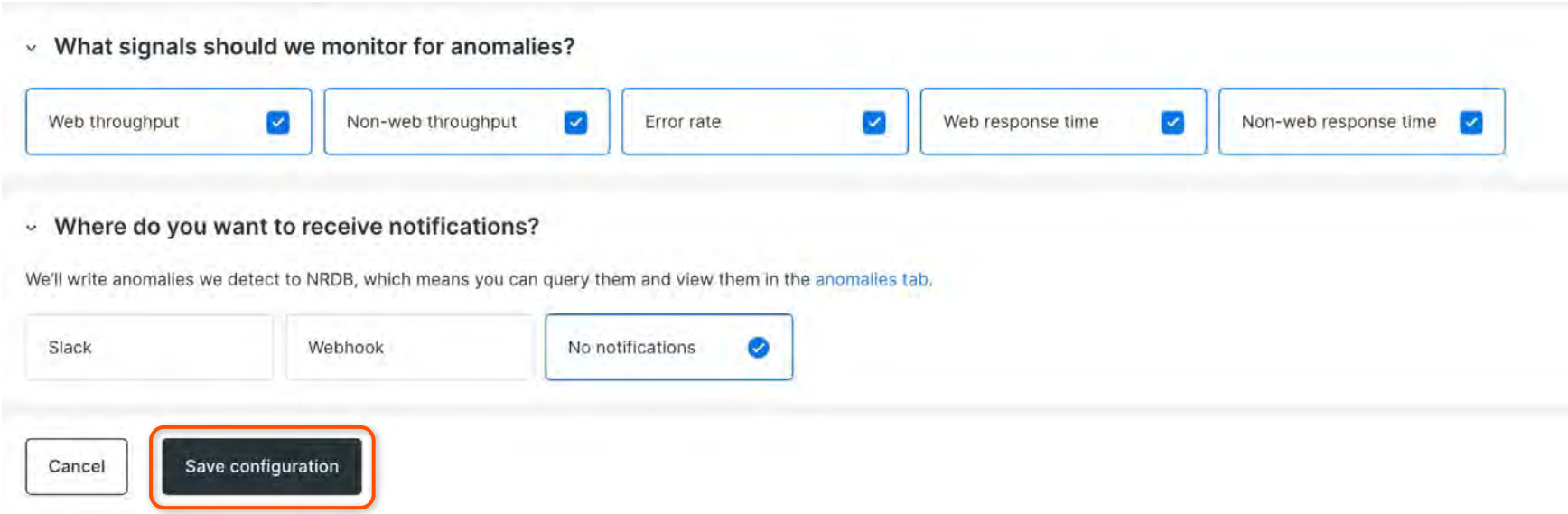
- 「設定名」には識別しやすい名前を設定します。
- Accountは「3940716 - New Relic University Japan」を選択します。
- 「EC-site」にチェックを入れます。



操作アカウント: Japan-NRU

ハンズオン(3-1) AIOpsの機能をセットアップする

- 5カテゴリ全てにチェックをつけ、「 No notifications」を選択します。
- 「Save configuration」をクリックします。



操作アカウント: Japan-NRU

ハンズオン(3-1) AIOpsの機能をセットアップする

- Anomaly設定の一覧に戻り、設定が追加されたことを確認します。

Add configurations to get notifications (Slack or webhook) and customize what you see for specific applications.

+ Add a configuration

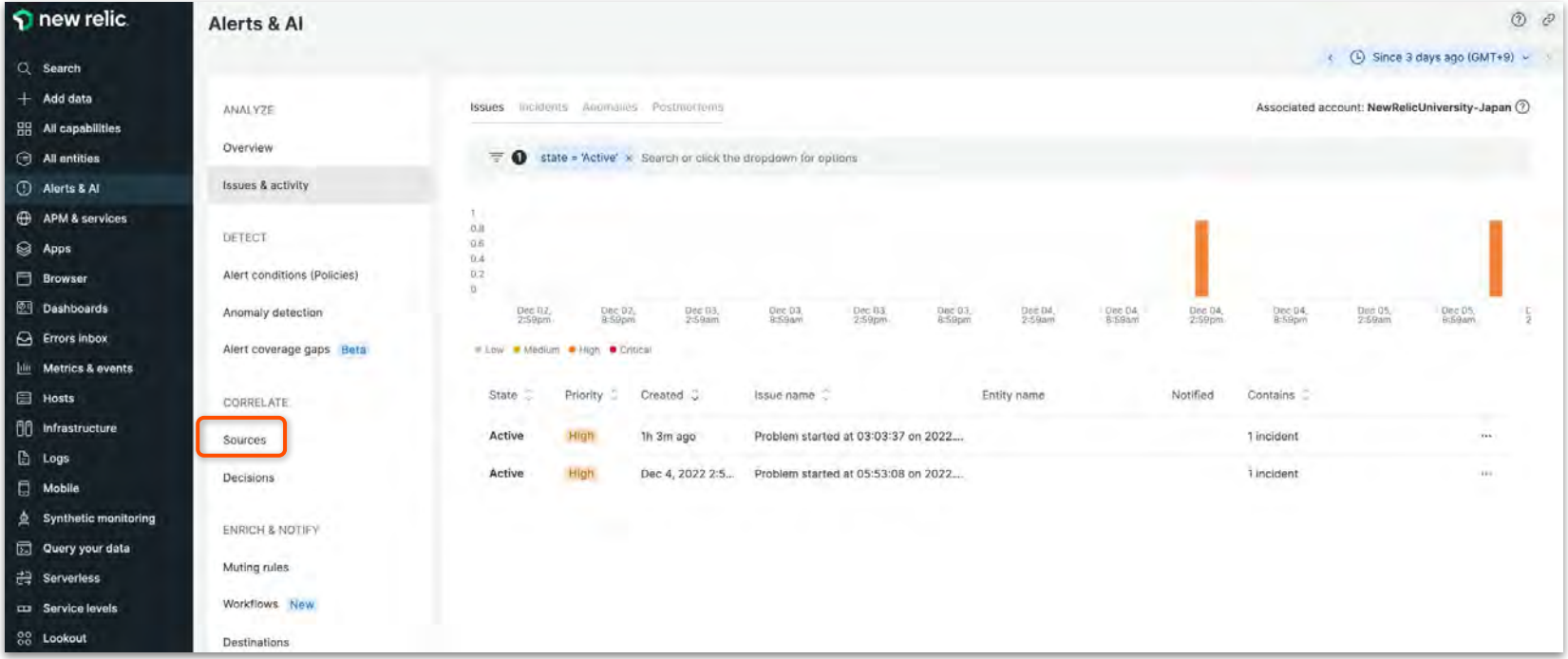
Search configurations

Configuration name	Account	Applications	Destination	Last updated ↓	
NRU304-参加者名-Configuration	New Relic University Japan	1		Jun 5, 2023 5:55am	···
NRU304-Sample-Condiguration	New Relic University Japan	1		Jun 4, 2023 3:00pm	···

操作アカウント: Japan-NRU

ハンズオン(3-2) AIOpsの機能をセットアップする

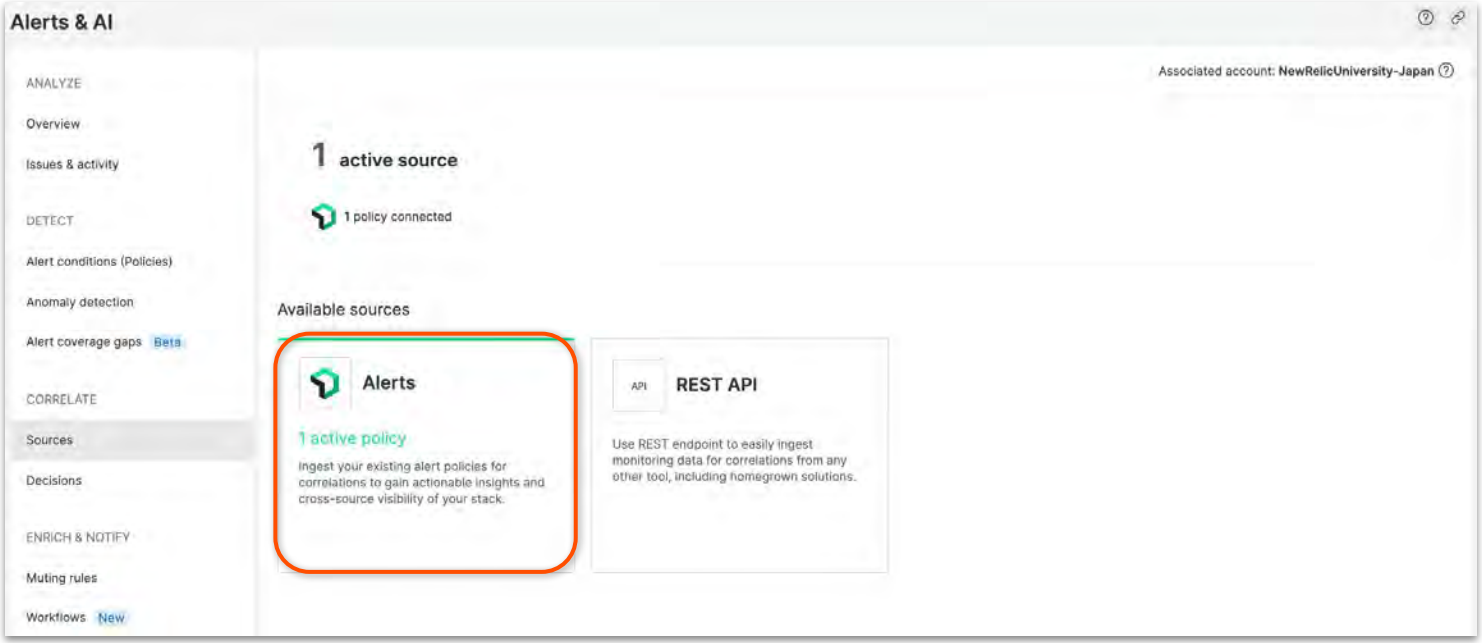
- 「Sources」をクリックします。



操作アカウント: Japan-NRU

ハンズオン(3-2) AIOpsの機能をセットアップする

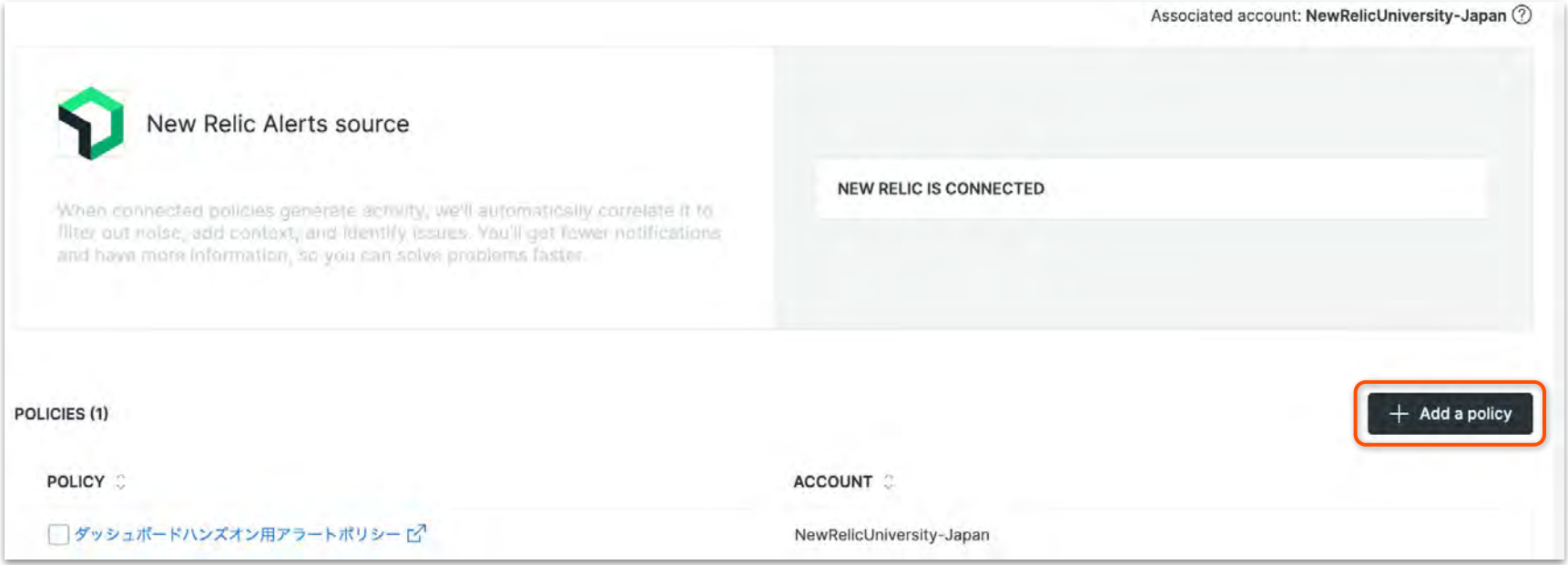
- 「Alerts」カードをクリックします。



操作アカウント: Japan-NRU

ハンズオン(3-2) AIOpsの機能をセットアップする

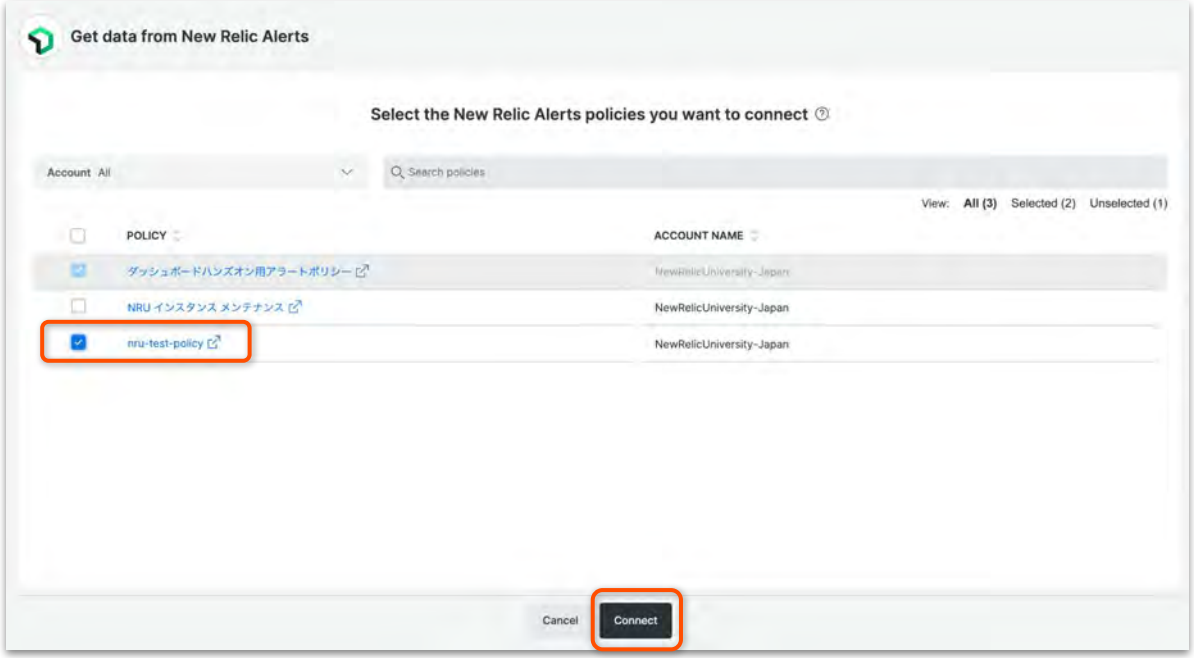
- 「＋ Add a policy」ボタンをクリックします。



操作アカウント: Japan-NRU

ハンズオン(3-2) AIOpsの機能をセットアップする

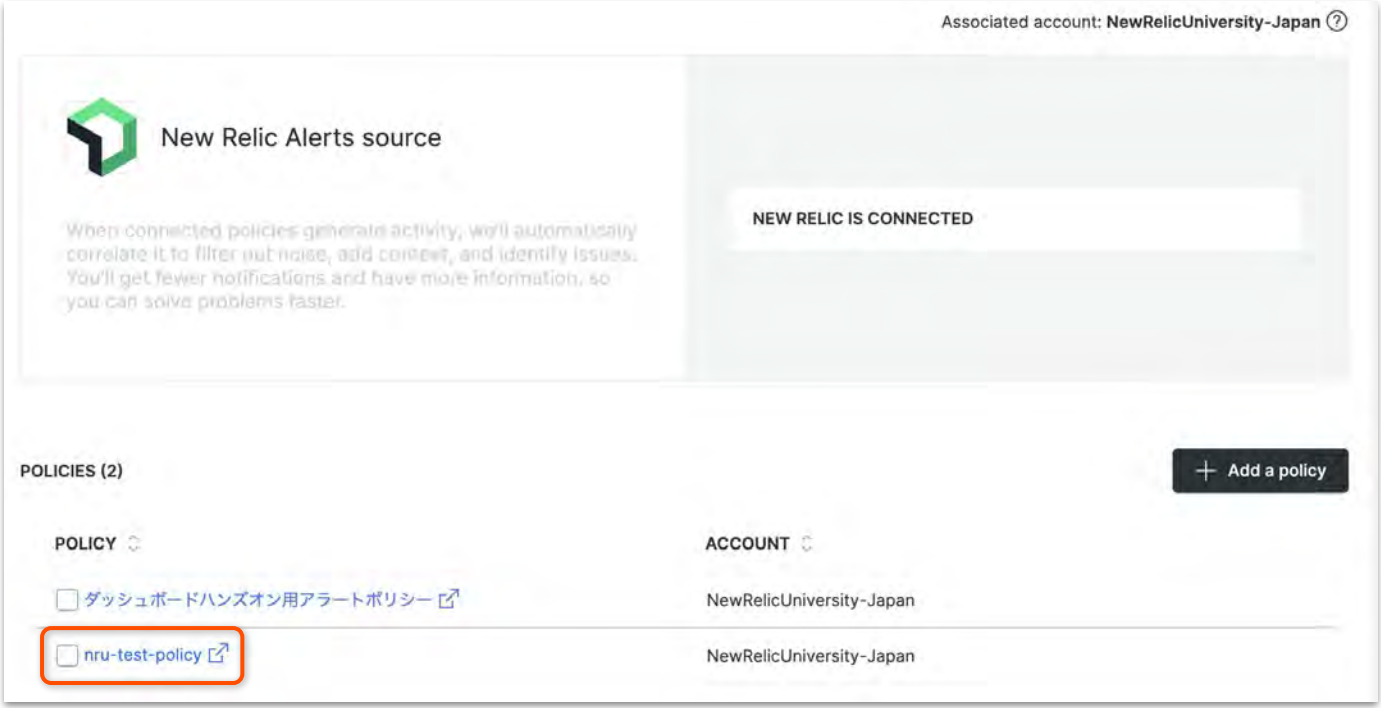
- ハンズオン（1）で作成した自分の Alert Policyにチェックを付けて「Connect」ボタンをクリックします。



操作アカウント: Japan-NRU

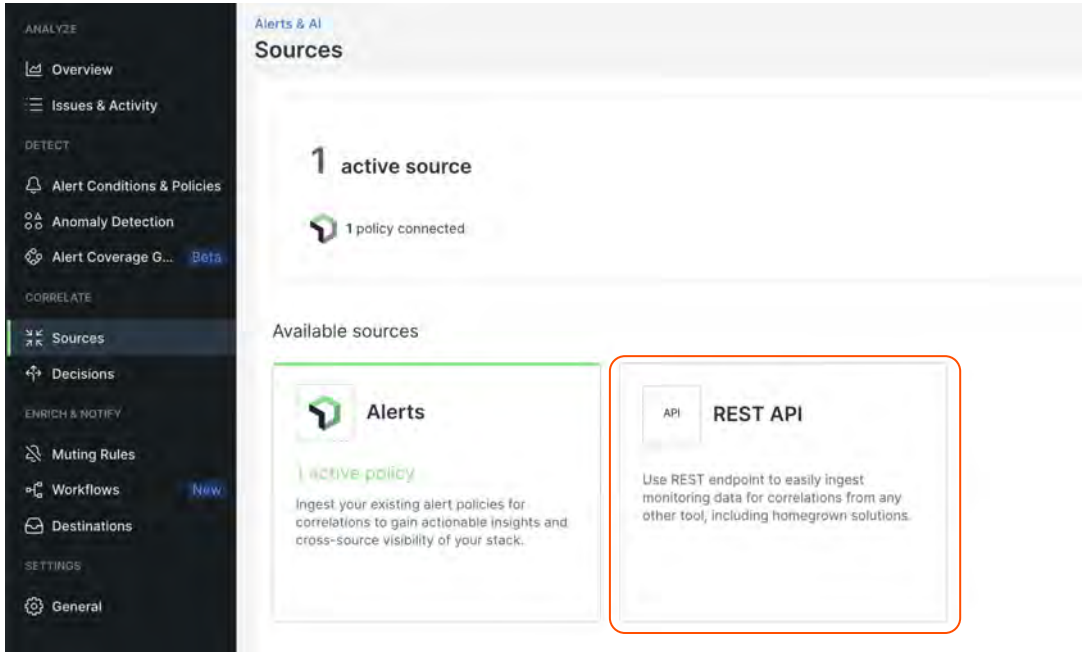
ハンズオン(3-2) AIOpsの機能をセットアップする

- 自分のPolicyが追加された事を確認します。



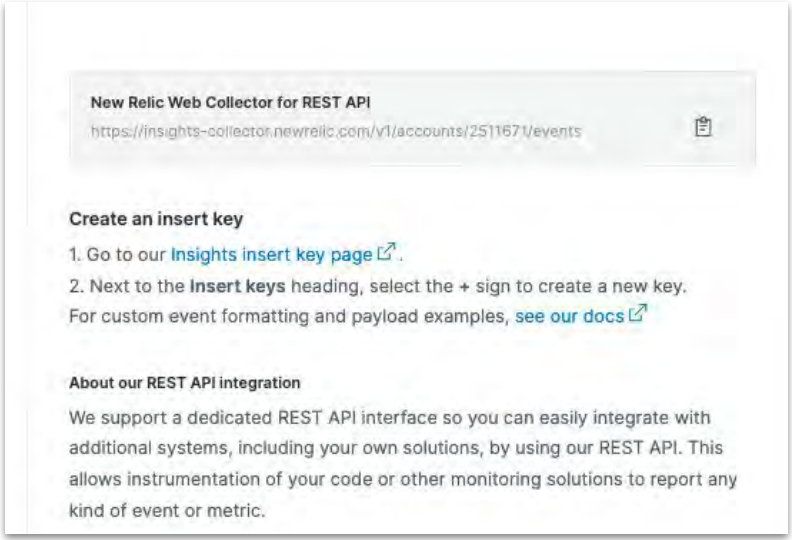
ハンズオン(3-3) 参考 Zabbixの連携1

- 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。



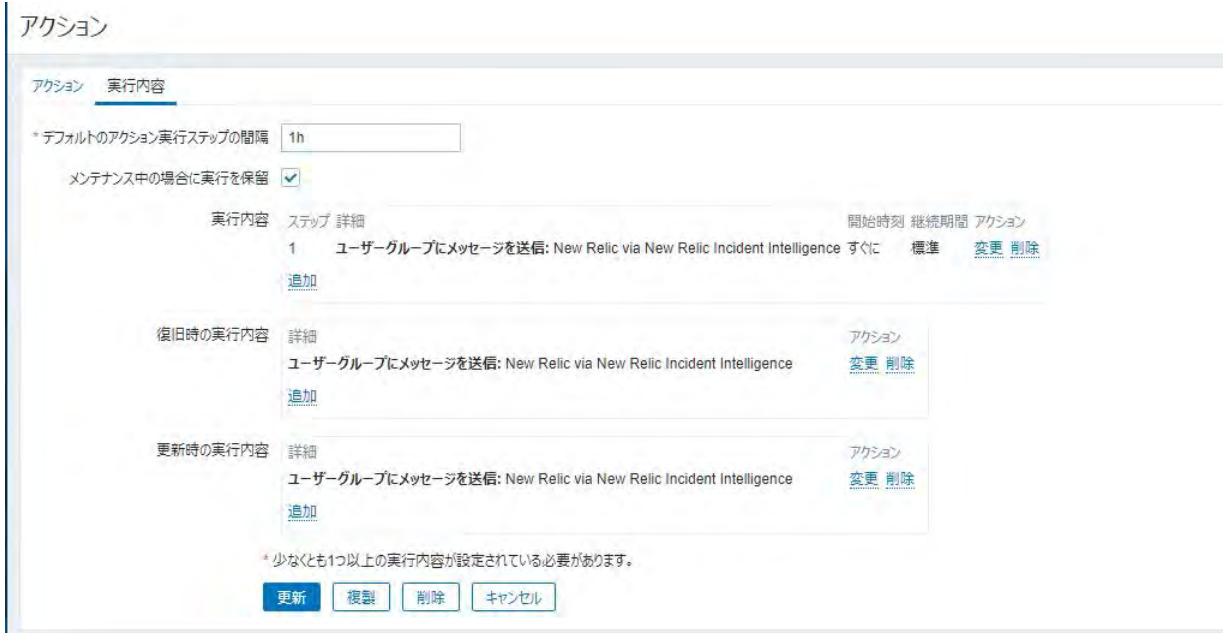
ハンズオン(3-3) 参考 Zabbixの連携2

- 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。



ハンズオン(3-3) 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。

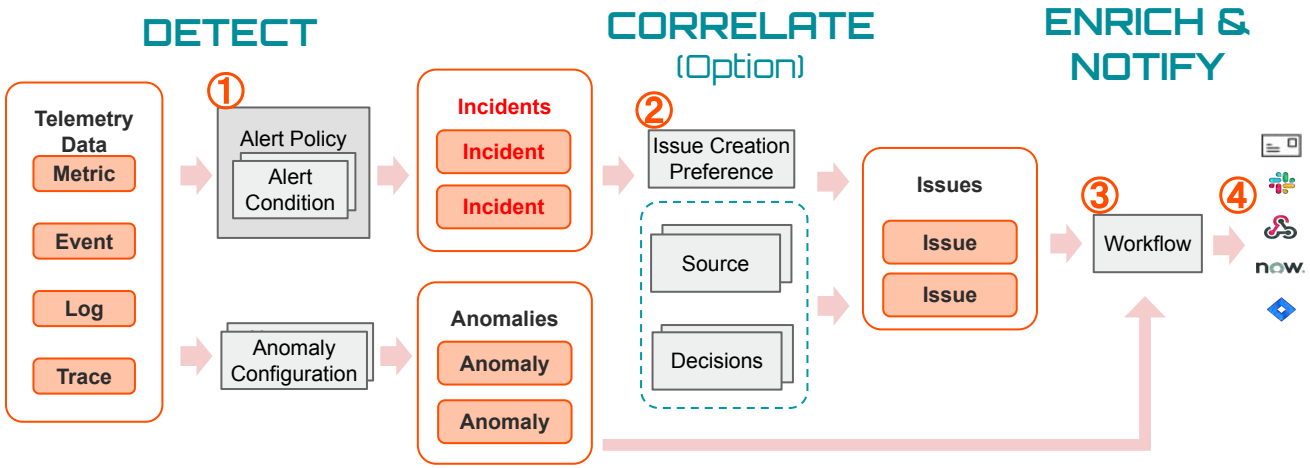


まとめ

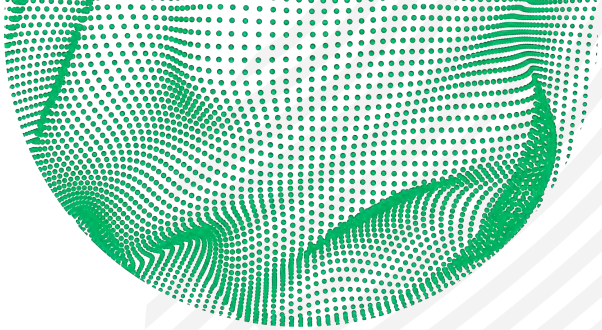
new relic

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

お疲れさまでした。

ご質問があればQ＆Aにご記入ください

アンケートにご協力お願いいたします

Thank you.