new relic

NRU 304
「AIOps とアラート設計の基本」

February 15, 2023

15:00より開始致します。しばらくお待ちください。

音声が聞こえづらい場合は退出、再入室をお試しください。

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

New Relic 株式会社
技術統括 コンサルティング部

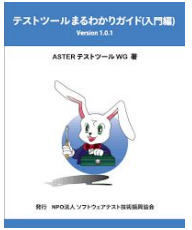
中島 良樹

SIerにて、さまざまなお客様のシステム開発やプロジェクトマネージャに従事。品質課題の改善を目的として主にWebシステムの負荷テストや機能テストの自動化を取り入れる。

外資テストツールベンダーに転職し、より多くのエンジニアにテスト自動化を取り入れてもらうべくプリセールスやコンサルティング業務を担当。

その後、データマネジメントベンダーにてデータ連携やデータ活用におけるプリセールスを担当。

開発や運用フェーズにおける自動化や効率化向上提案の経験を経て2022年より現職。



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.

本日のゴール

- New Relicを使ってより**ユーザー体験に近い指標**でアラートを設定する手法を学ぶ
- New Relicを使って**AIOpsを実現する手法**を学ぶ

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)

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
15:15-15:35	座学(2)	New Relicのアラート機能
15:35-15:45	ハンズオン(0)	環境を確認する
15:45-16:05	ハンズオン(1)	アラートを作成する
16:05-16:15	座学(3)	New RelicのAIOps機能
16:15-16:30	ハンズオン(2)	AIOpsを使った異常検知と原因分析
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 (応用編)
16:55-17:00		まとめ、アンケートご記入

new relic

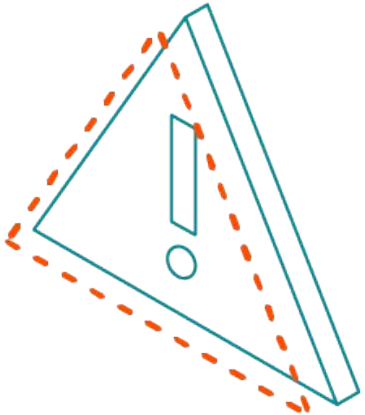
座学(1)
ユーザー視点のアラート

15:00 - 15:15 (15min)

new relic

突然ですが

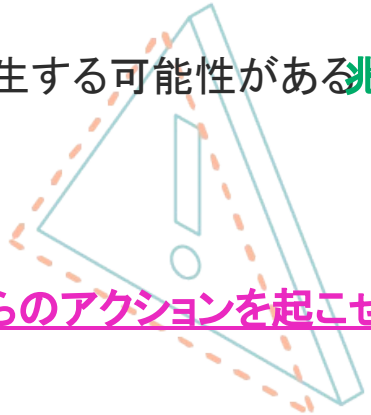
- どんなアラートを設定していますか？



アラートを設定する目的

対象システムが以下のような観点で対応が必要であることを知るための**通知を得るため**に行う

1. システムの停止、またはパフォーマンスの悪化が発生し、**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可能性がある**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)

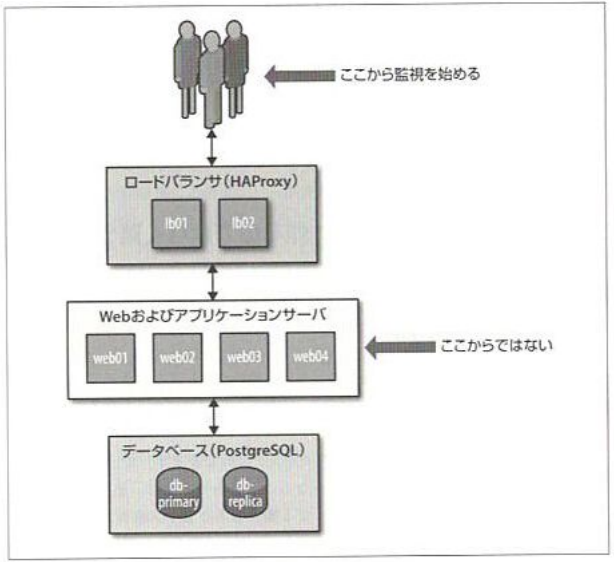
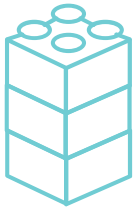


図2-1　できるだけユーザに近いところから監視を始める

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

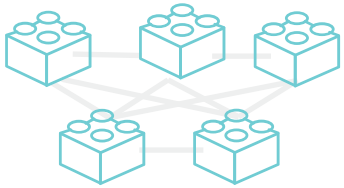


基盤

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



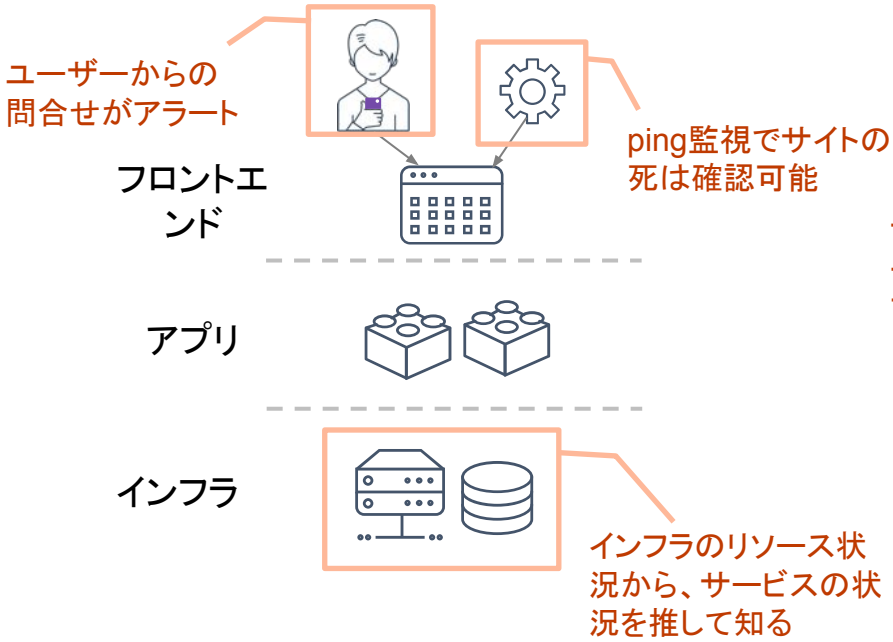
リソース抽象化
(仮想化、コンテナ等)

基盤

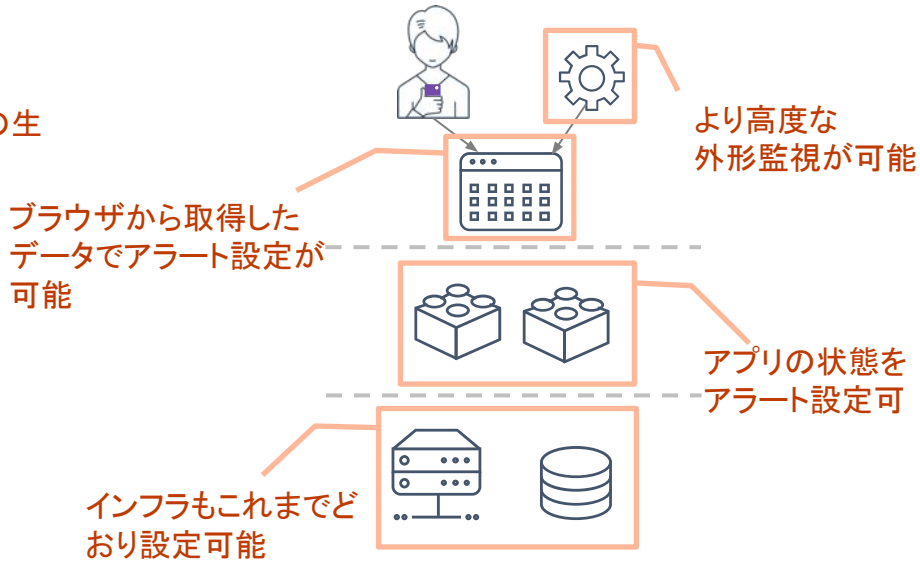
アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

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 - 15:35 (20min)

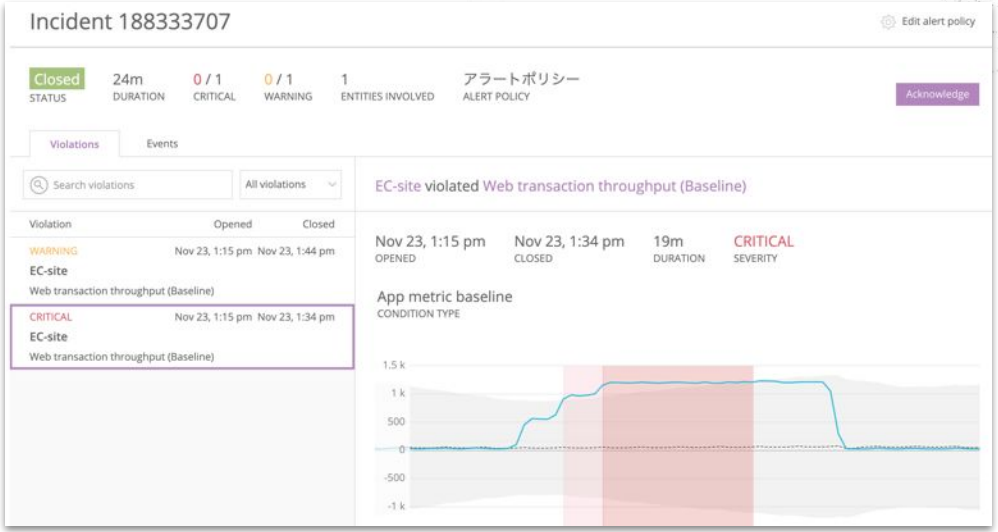
new relic

New Relicのアラート機能

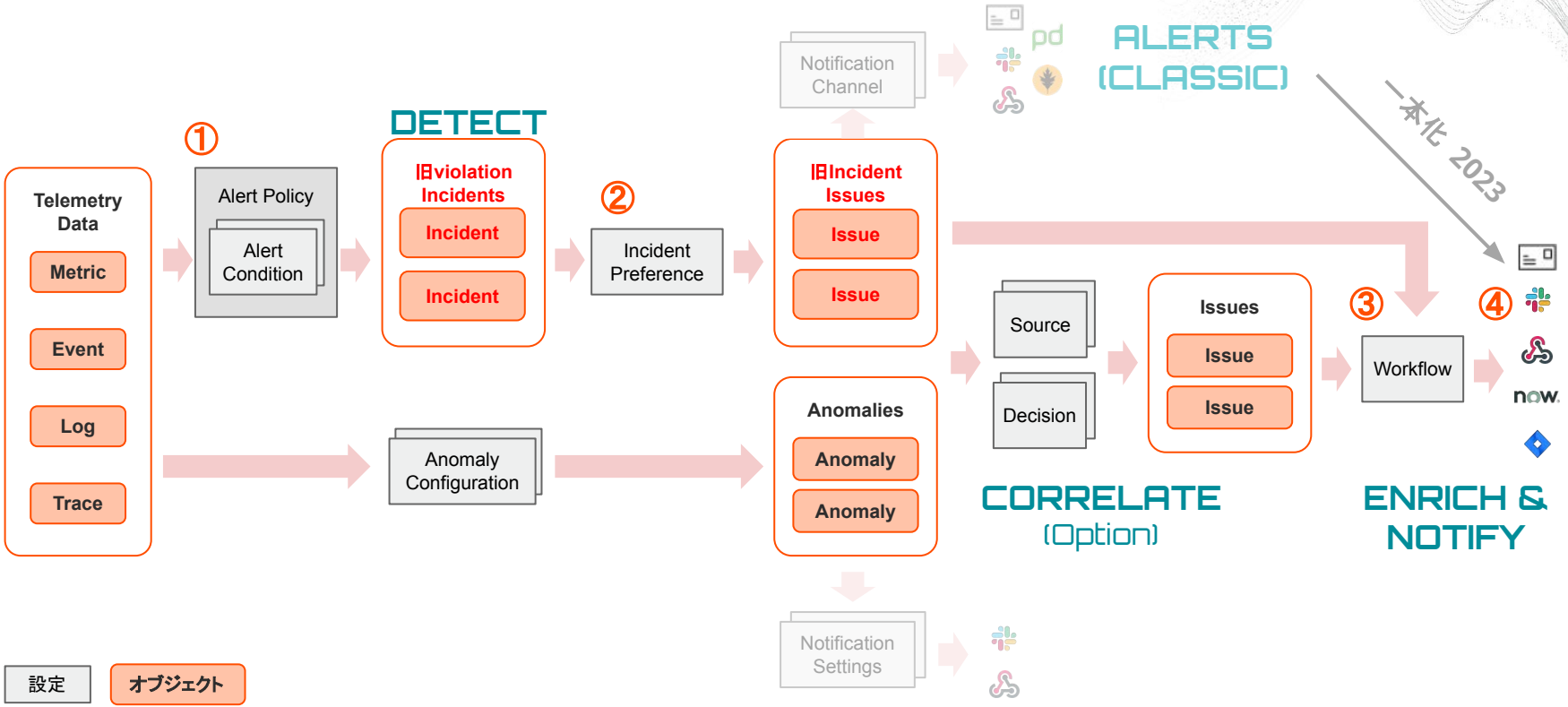
New Relicが**収集しているデータ**を使って、アラートを設定することが可能

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

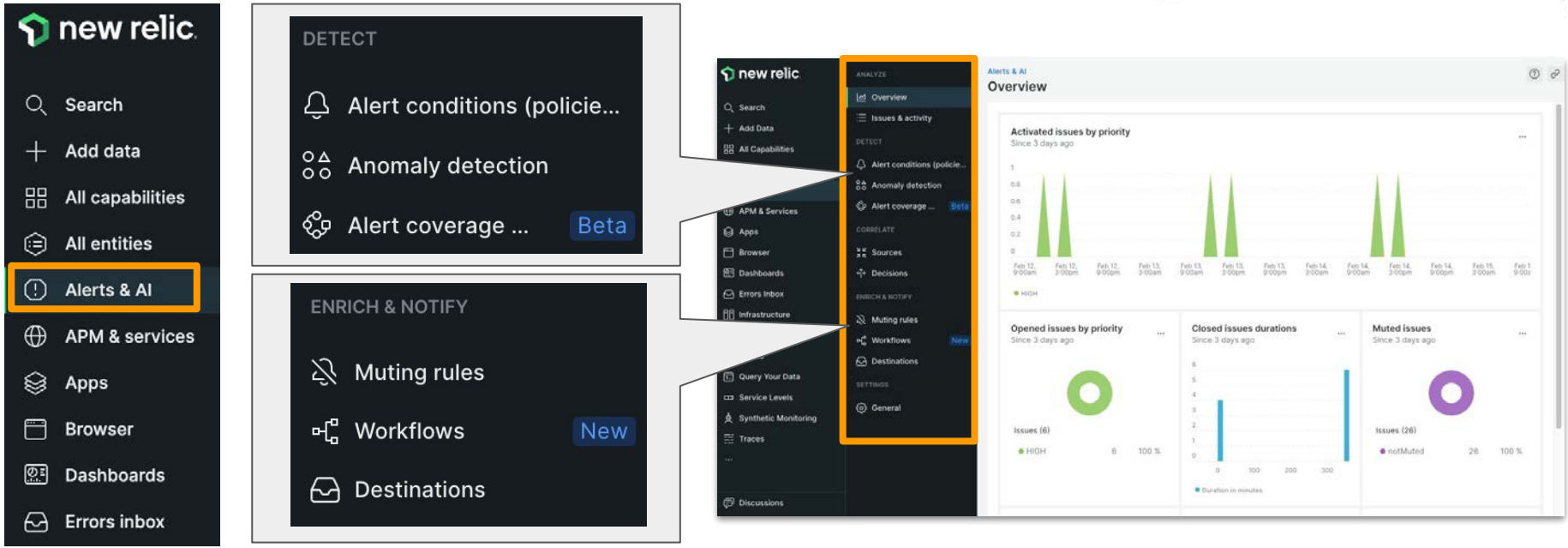
※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説していきます



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

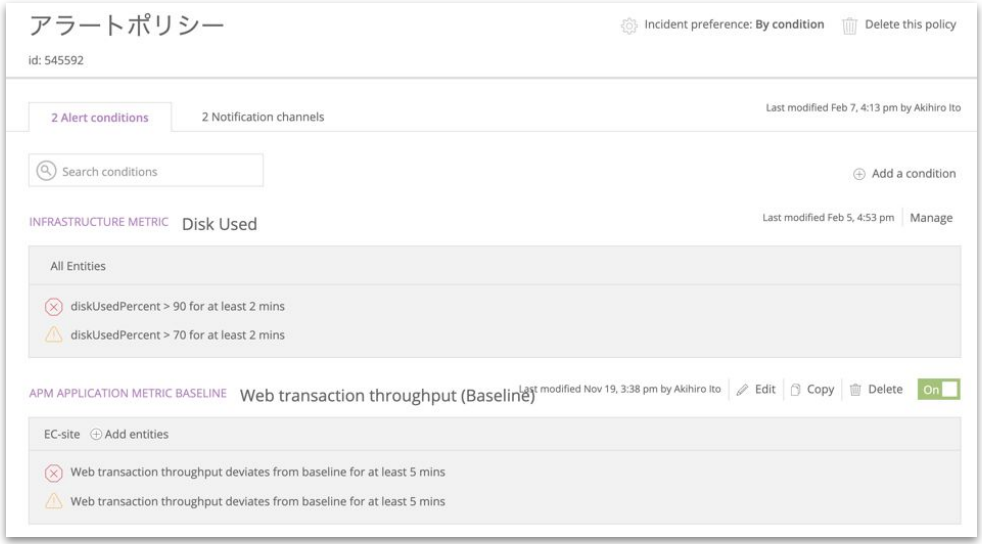


new relic

New Relic アラートの構成要素1: Alert PolicyとAlert Condition

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は複数のAlert Conditionを内包し、送信先を制御できる

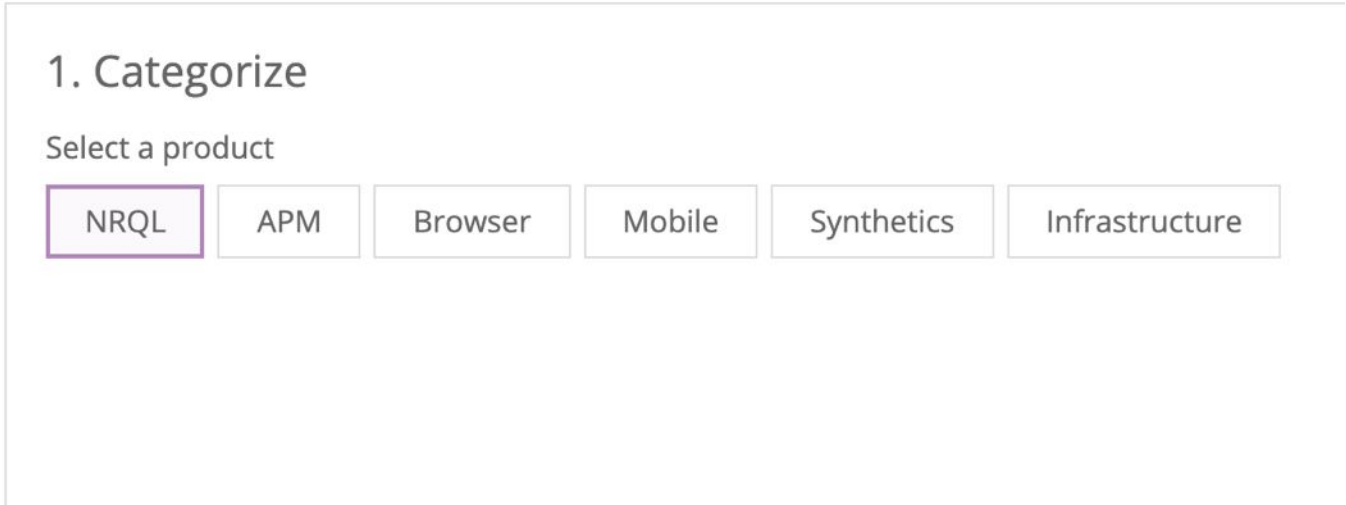
通常、送信先やアラートの目的別にポリシーを分けることが多い



New Relic アラートの構成要素1: Alert PolicyとAlert Condition

New Relicが収集しているデータを使って、Alert Conditionを作成できる

機能(例. APM, Browser等)ごとに簡単にアラートを作れる機能を持つ他、**汎用的なNRQL**を使い、自分でクエリを書いて細かなAlert Conditionを作成することも可能



New Relic アラートの構成要素1: Alert Policyと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1: Alert PolicyとAlert Condition

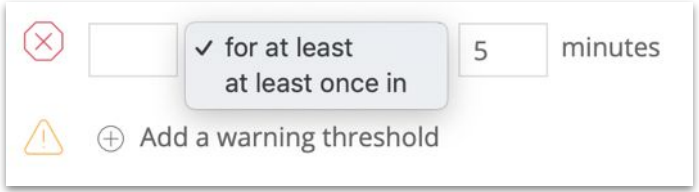
しきい値を超過した場合のアラート発報タイミング

- **For at least xx minutes**

  しきい値をxx分継続して超過した場合のみ Incidentが起票される

- **at least once in xx minutes**

  しきい値を1回でも超過した場合に Incidentが起票される



Alert ConditionはCriticalとWarning(オプション)2種類を作成可能

その他条件の設定に関する詳細は以下参照:
https://newrelic.com/jp/blog/how-to-relic/alert-configuration-guidance

New Relic アラートの構成要素1: Alert PolicyとAlert Condition

効果的な通知を送るためのプラクティス

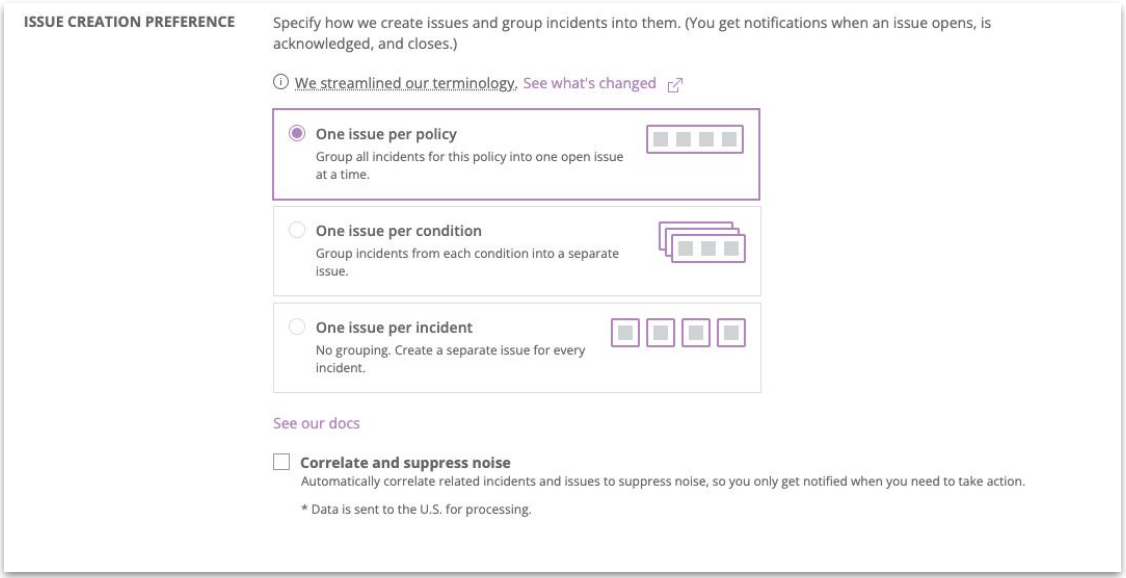
- Additional settingsのcustom violation descriptionから発報されるアラートに詳細な情報を付加する様に設定することが可能 (参考情報)
- Additional settingsのRunbook URLを設定することにより、
  アラート発報時に対応手順へのリンクにすぐにアクセスすることが可能

New Relic アラートの構成要素2: Incident Preference 1/2

New RelicはAlert Conditionの閾値を超過した場合はIncidentを起票する

Incident Preferenceの設定によって、Issueを起票する（Incidentをまとめる）粒度を設定できる

※アラートポリシーを作成する際に設定(後で編集可)



New Relic アラートの構成要素2: Incident Preference 2/2

Issueの起票粒度について

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

- フロントエンドのJSエラー率上昇(対象サイトは1つ)
- サーバーサイドのエラー率上昇 (対象アプリケーションは3つ)

設定名	Issueの起票粒度	この例で起票されるIssue
By Policy	ポリシーごと	1つ (ポリシー全体で1つ)
By condition	アラート条件ごと	2つ (JSエラーで1つ, サーバーサイドエラーで1つ)
By condition and signal	アラート条件と、その条件の対象となるエンティティ(構成要素)ごと	4つ (JSエラーで1つ, サーバーサイドエラーで3つ)

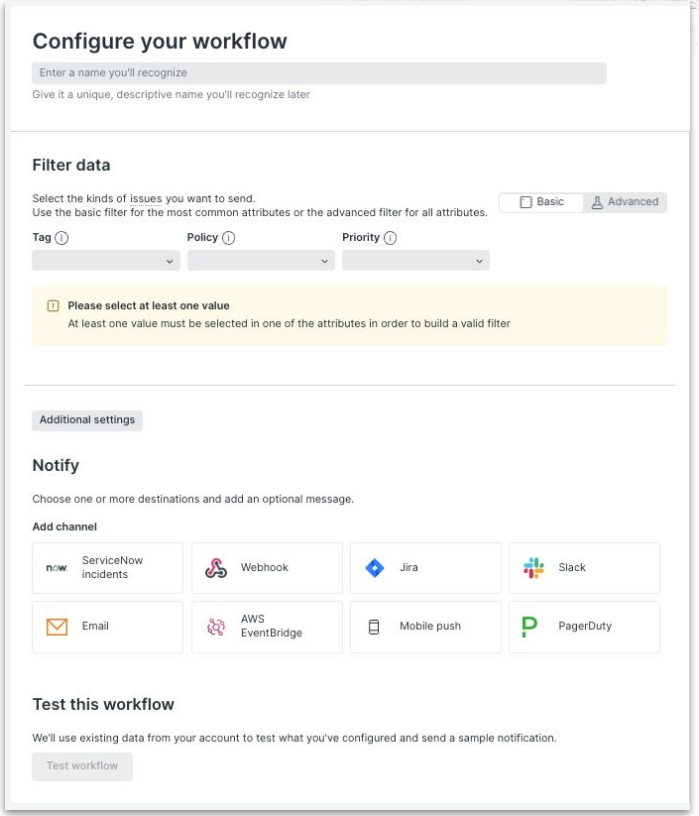
New Relic アラートの構成要素3: Workflows

Issueが起票された際に所定のデータを付与したり、
通知先（Destination）と関連づけて対象 Issueを
どこに通知するのかをマッピングする機能

Filter data

- どのIssueとマッピングするかを定義する

- **Enrich**
  - Issue対象のEntityに関する付加情報を付与する
- **Mute issues**
  - Muting Rulesが設定されていた場合の
    挙動について定義する
- **Notify**
  - 通知先のDestinationを選択
- **Test workflow** (重要)
  - このworkflowの通知テストを実行



New Relic アラートの構成要素4: Destinations

Issueのライフサイクルに応じた通知を受けることができる

デフォルトで各New Relic ユーザーは利用できる通知先として登録されている

Workflowsと関連づけると、以下の形式で通知される

- 登録メールアドレスに対する通知
- New Relicモバイルアプリ経由での通知

その他、追加で利用可能な通知先一覧は以下のとおりとなります

servicenow

Webhooks

JIRA

Slack

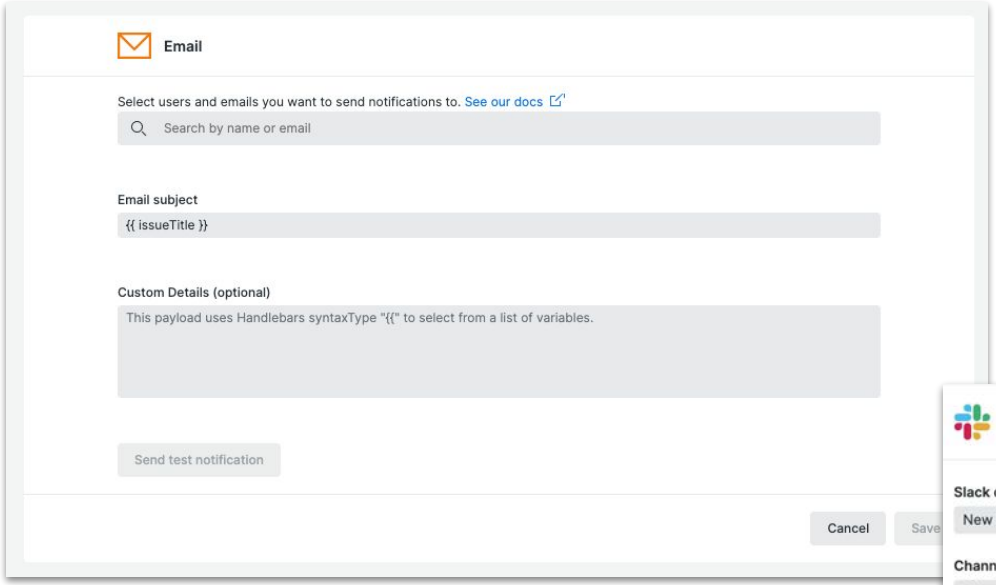
Email

Amazon EventBridge

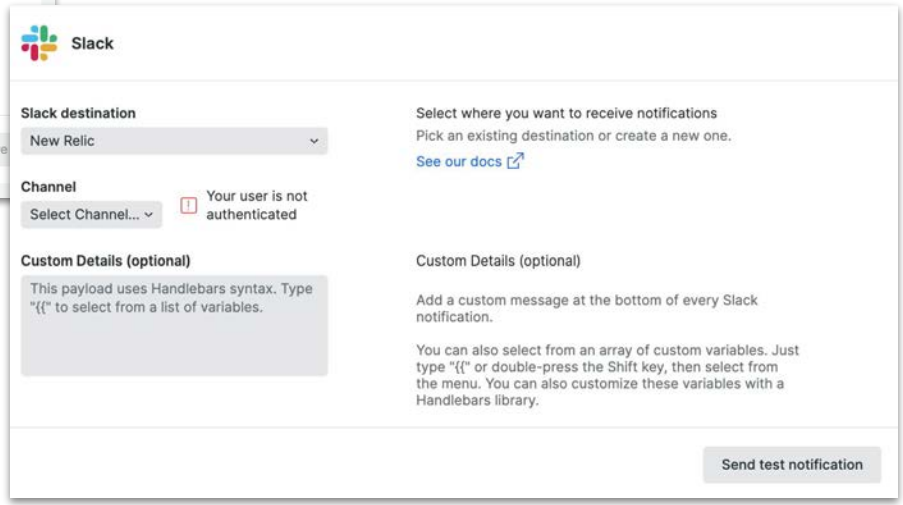
Pager Duty

Mobile push

重要: Email / Slack 内容の設定画面



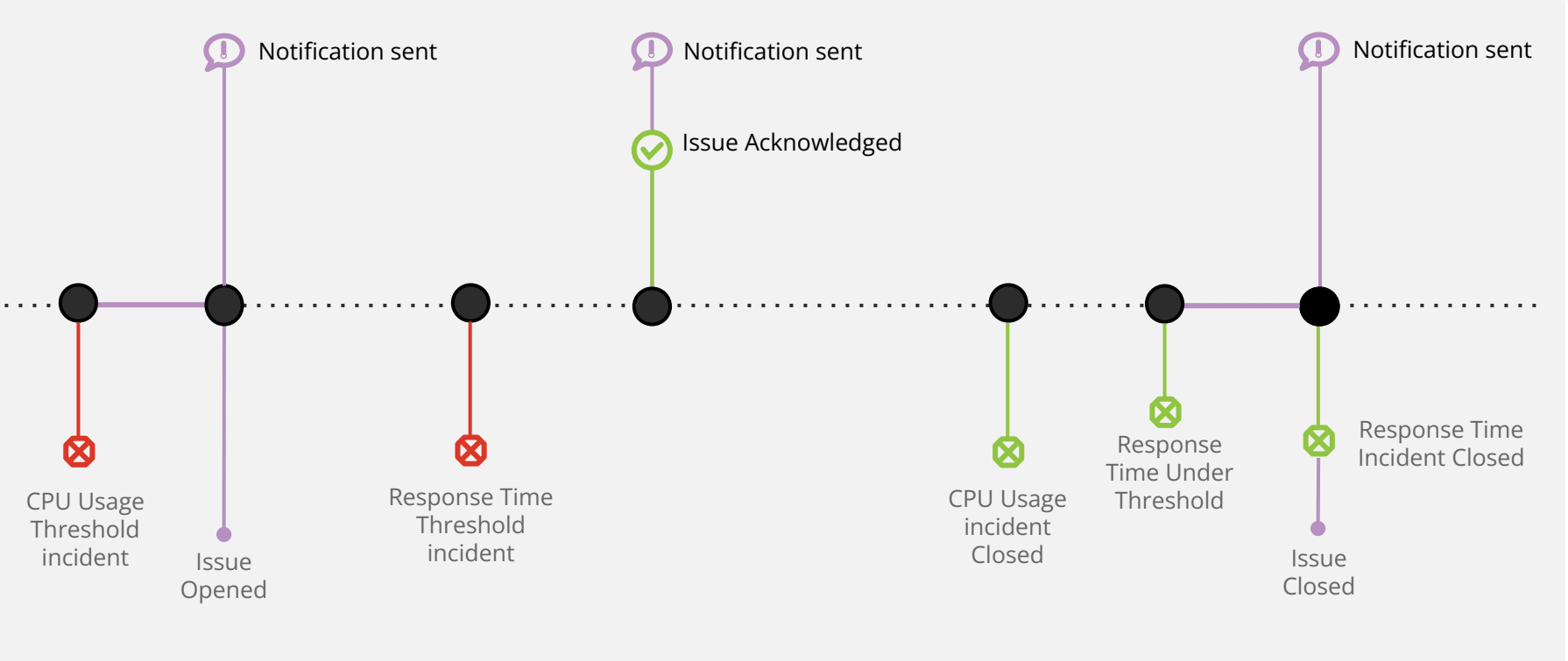
- Workflows変数を用いて柔軟に標題や内容のカスタムができるようになりました。
  - 補足: custom violation descriptionとは別の情報付加機能となります。
- “{{“と入力することで、Workflows変数の補完機能を活用できます。



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

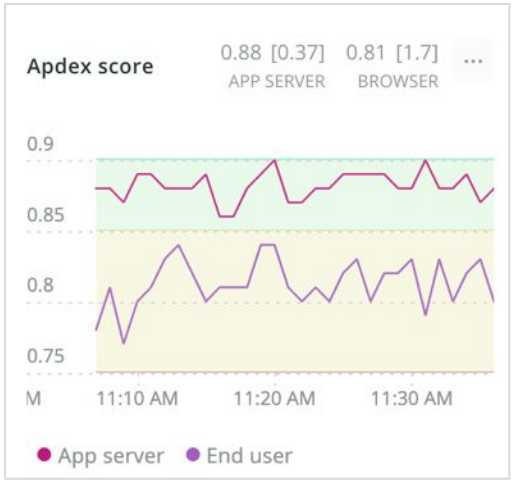
Issueの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く

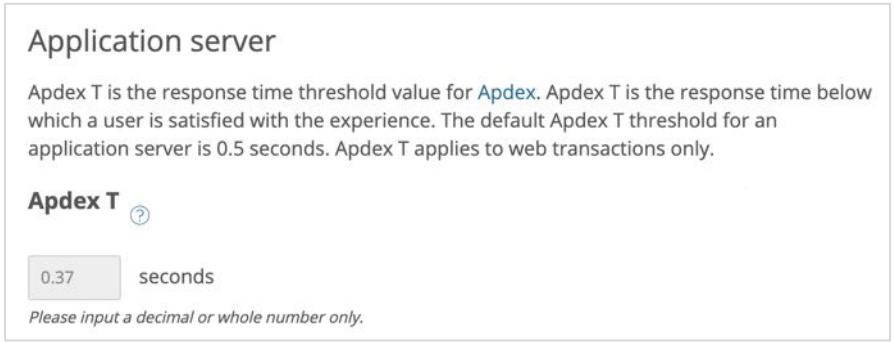


アラートを設定する前にやること

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

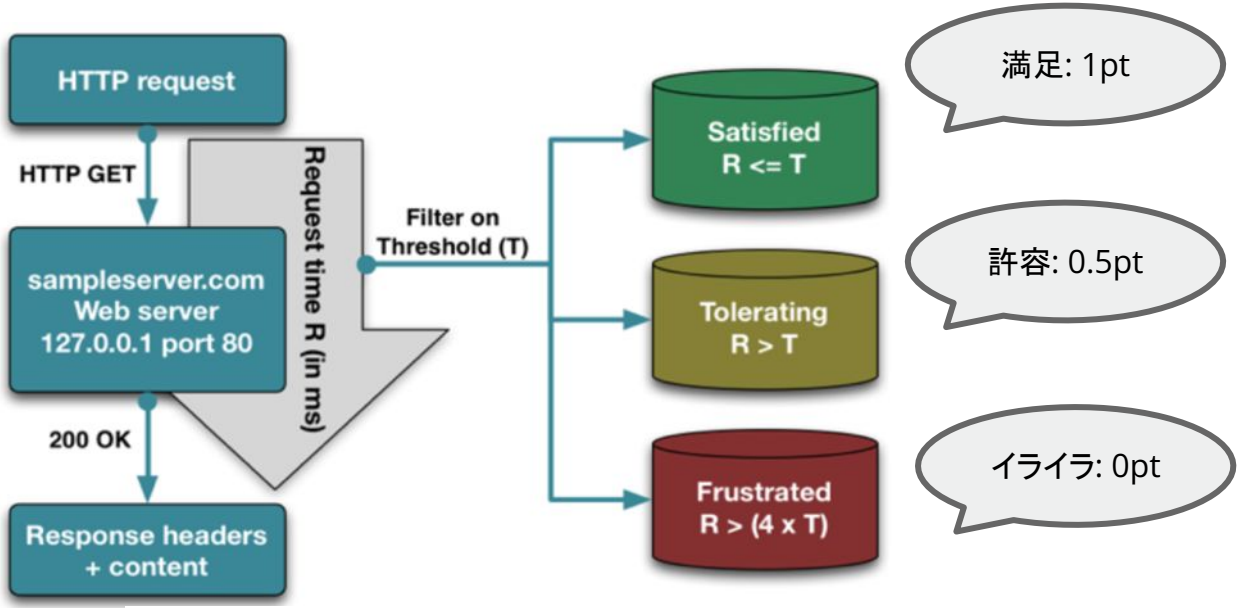




Apdex T値について

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)



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

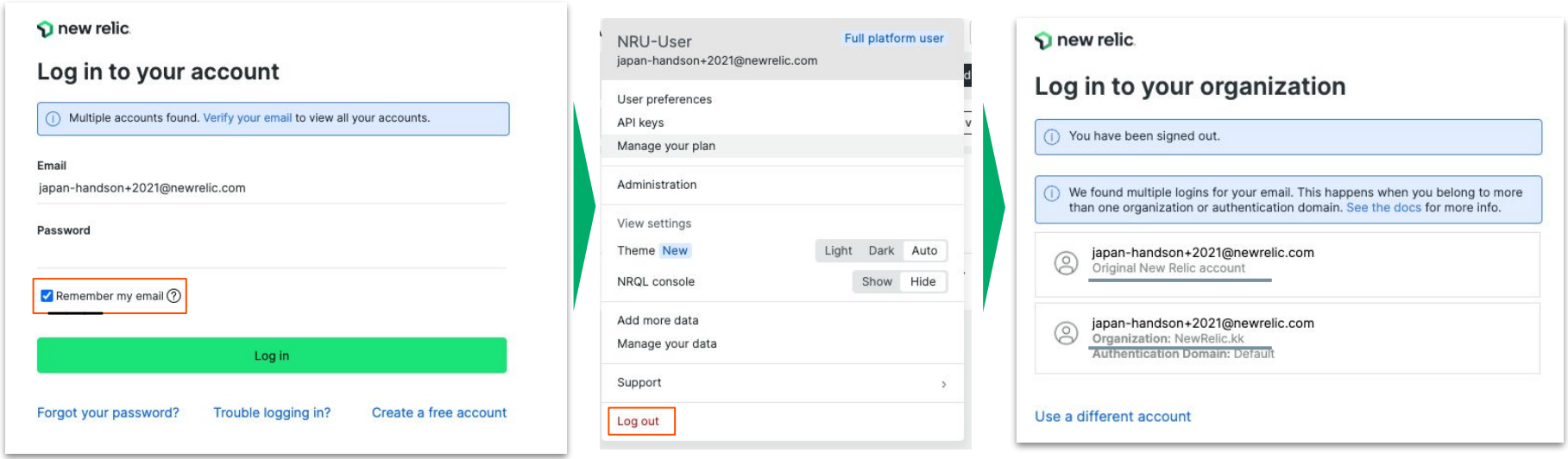
ハンズオン(0)
環境を確認する

15:35 - 15:45 (10min)

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。
詳細はブログを参照



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+2021@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。
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。

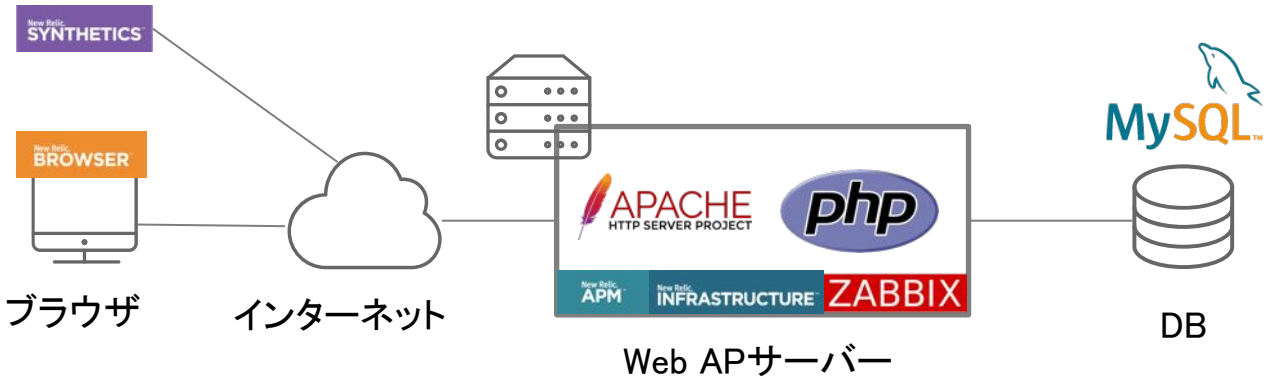
今回監視対象のサイト

[NRUジェラートショップ](ECサイト)

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

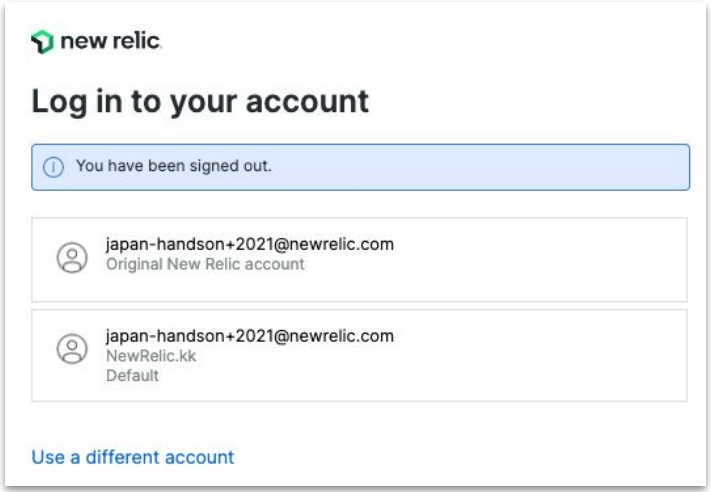
今回の環境の監視構成

- 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) 2つのアカウントにログインする

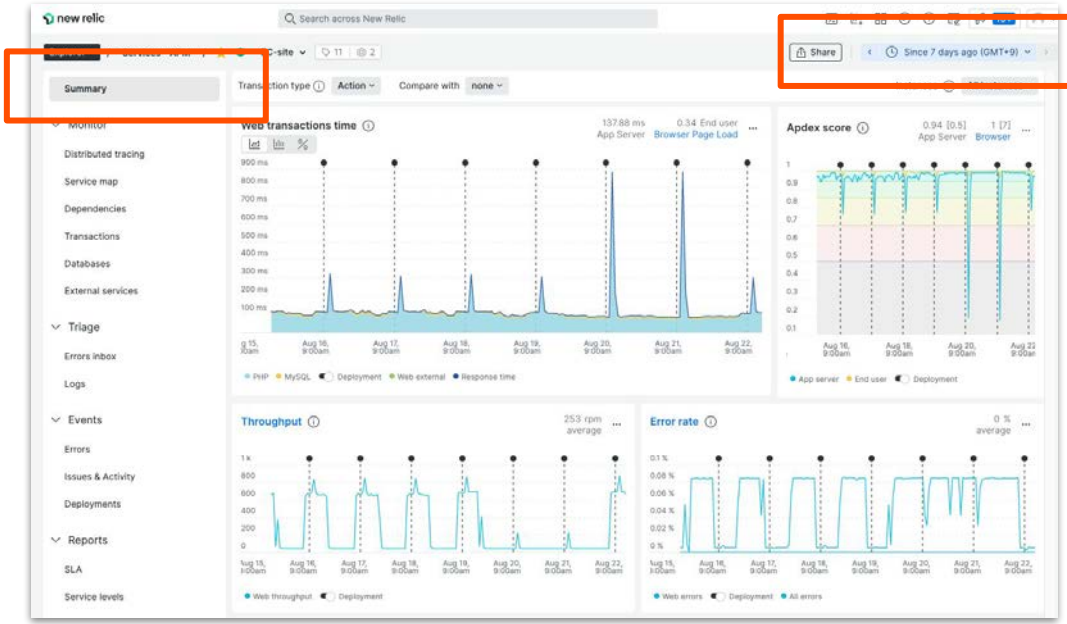
- ログイン先のアカウントを切り替えて確認頂くハンズオンが後半に予定されています。
- こちらの手順に従って、事前作業を行ないます。



ハンズオン(0) FSO 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。

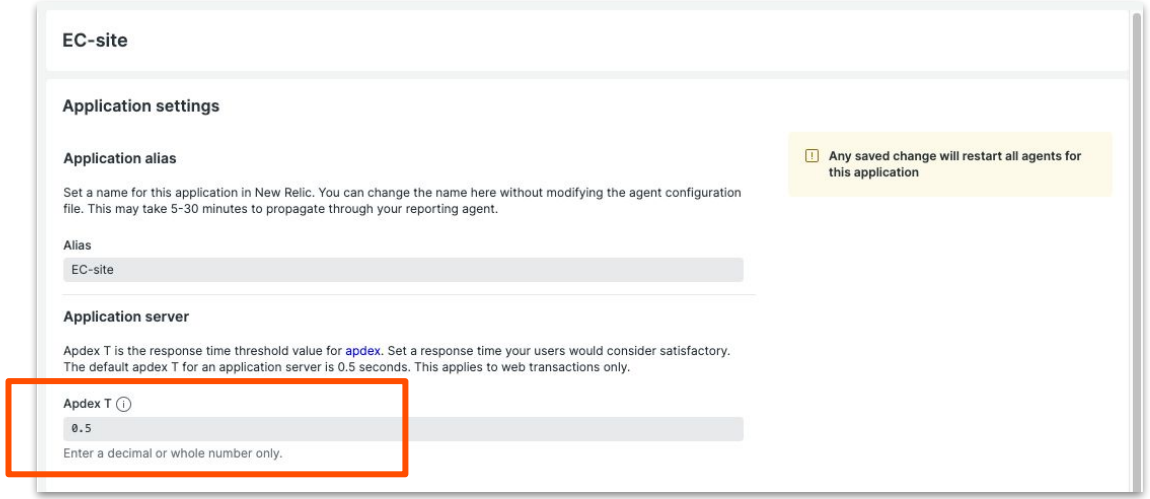


new relic

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。



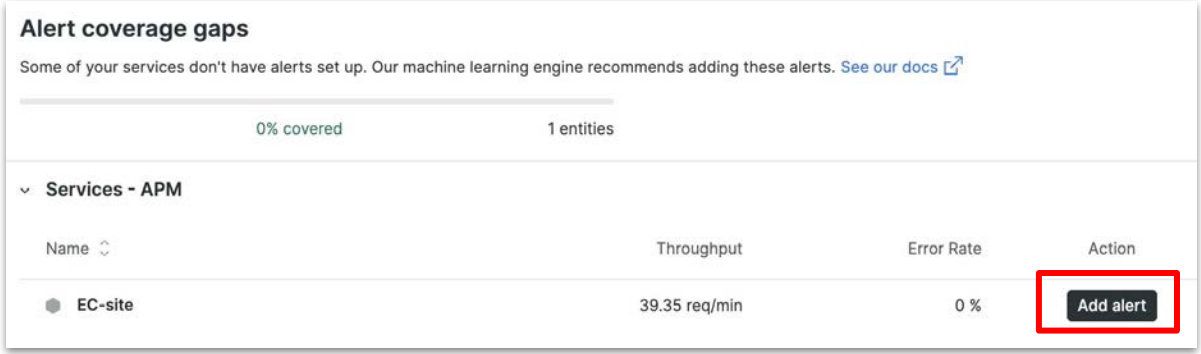
new relic

ハンズオン(0) Alerts & AIの確認

変更は行わない!!!

詳細については、後ほどご説明します。

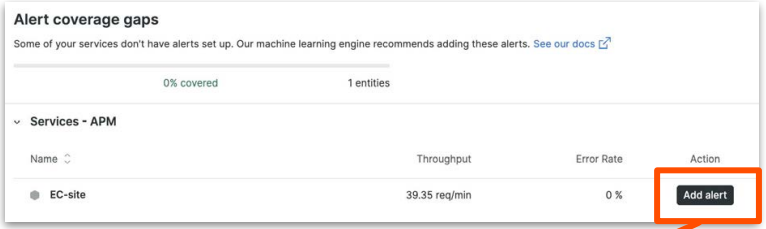
- Alert coverage gaps (Beta)にアクセスします。 Alerts & AI → Alert coverage gaps
- EC-siteのAdd alertボタンを押します。



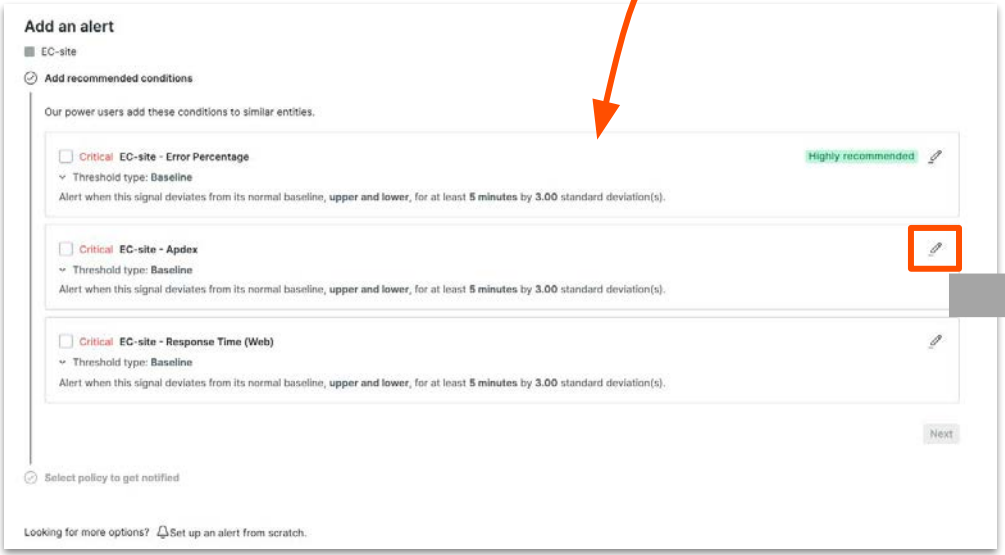
- 表示される一覧の中の任意の 1つを選び、鉛筆アイコンをクリックします。
- (後ほど説明します。)アラートに関する設定 (condition)のUIが表示されます。
  - **表示を確認したら、保存などは一切行わずに、設定の UIを閉じてください。**

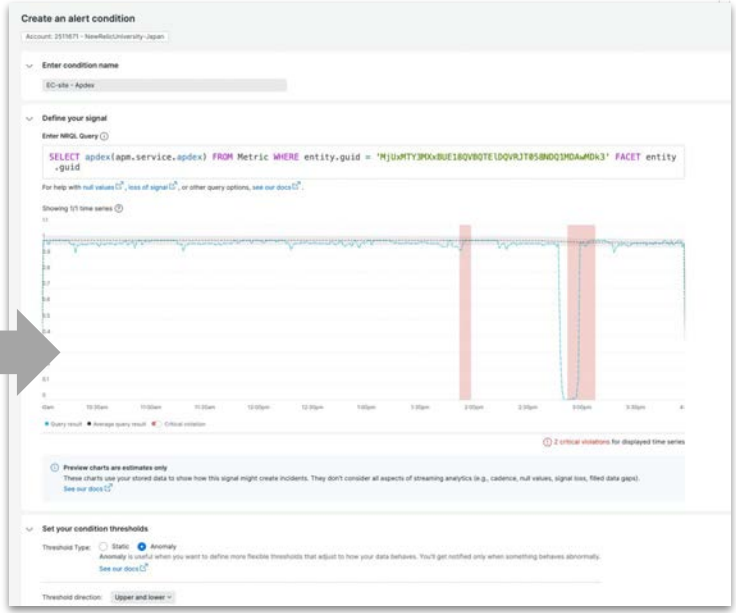
new relic

ハンズオン(0) Alerts & AIの確認



変更は行わない!!!





new relic

ハンズオン(1)
アラートを作成する

15:45 - 16:05 (20min)

今回の環境の監視構成

[前提]

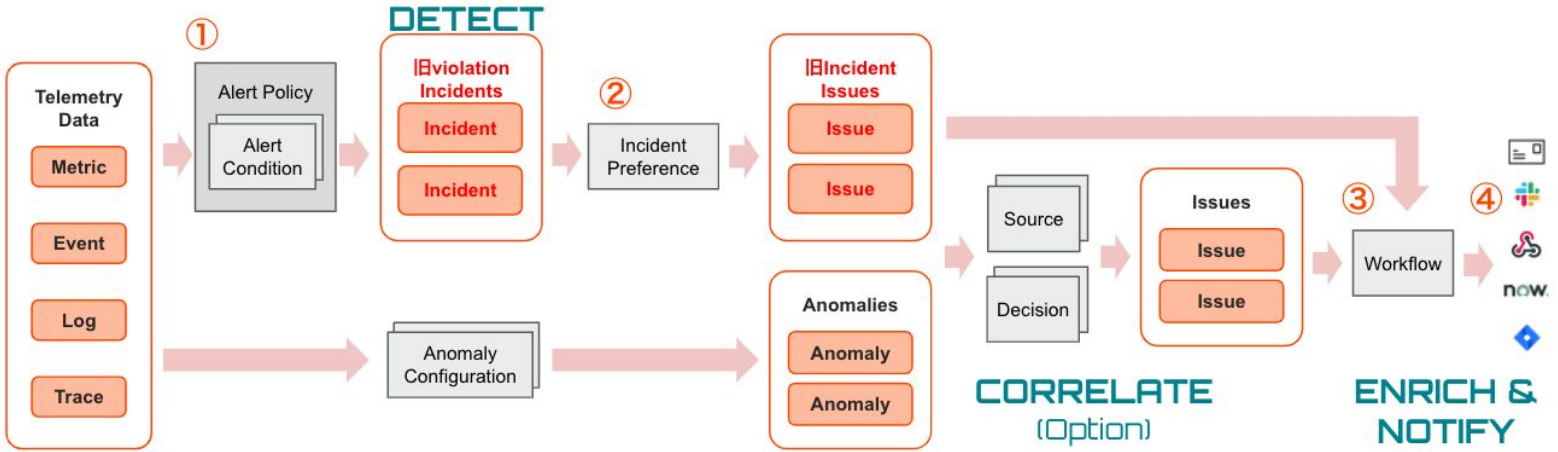
今回は**赤字**のアラートを設定してみます。

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. Workflowsを作成する

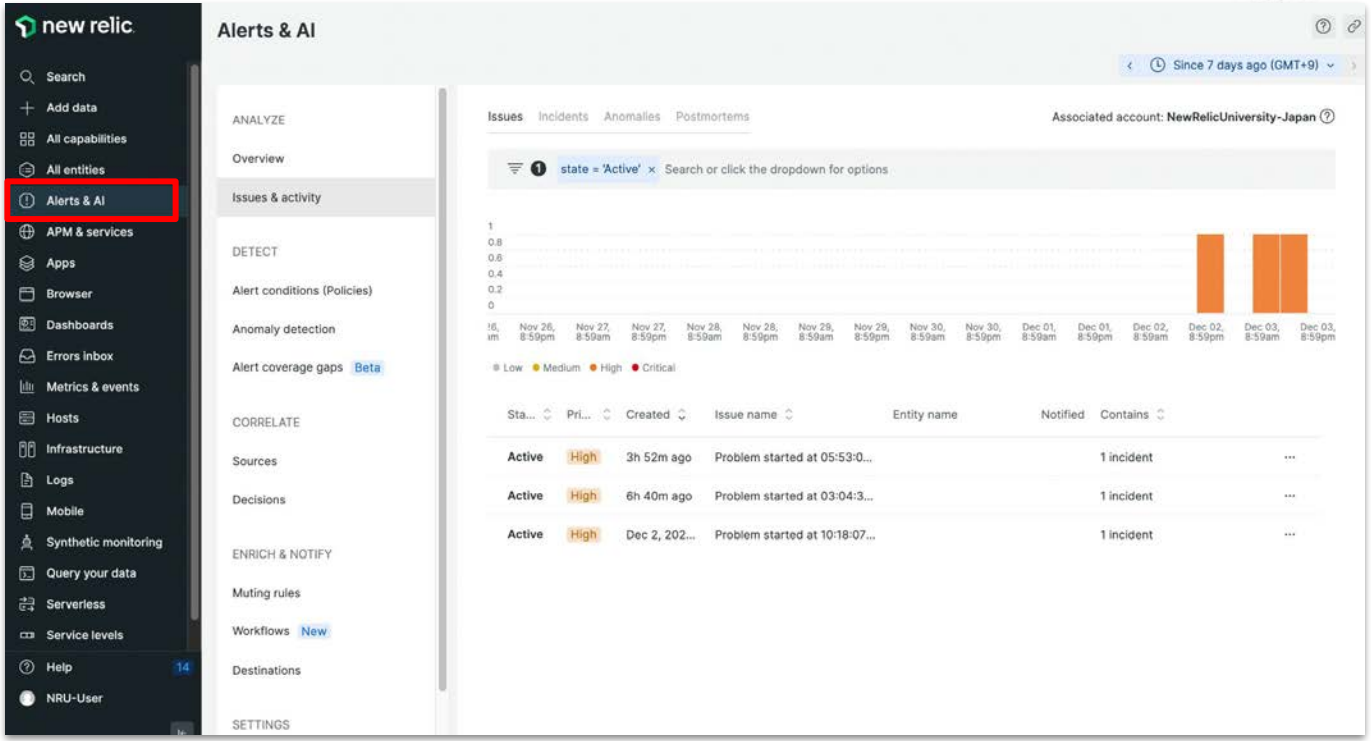


手順・解説

使用アカウント：NewRelic.kk
（ログイン先選択はこちら参照）

ハンズオン(1)-1 Alert policyを作成する 1/4

- Alerts & AI メニューを開きます。

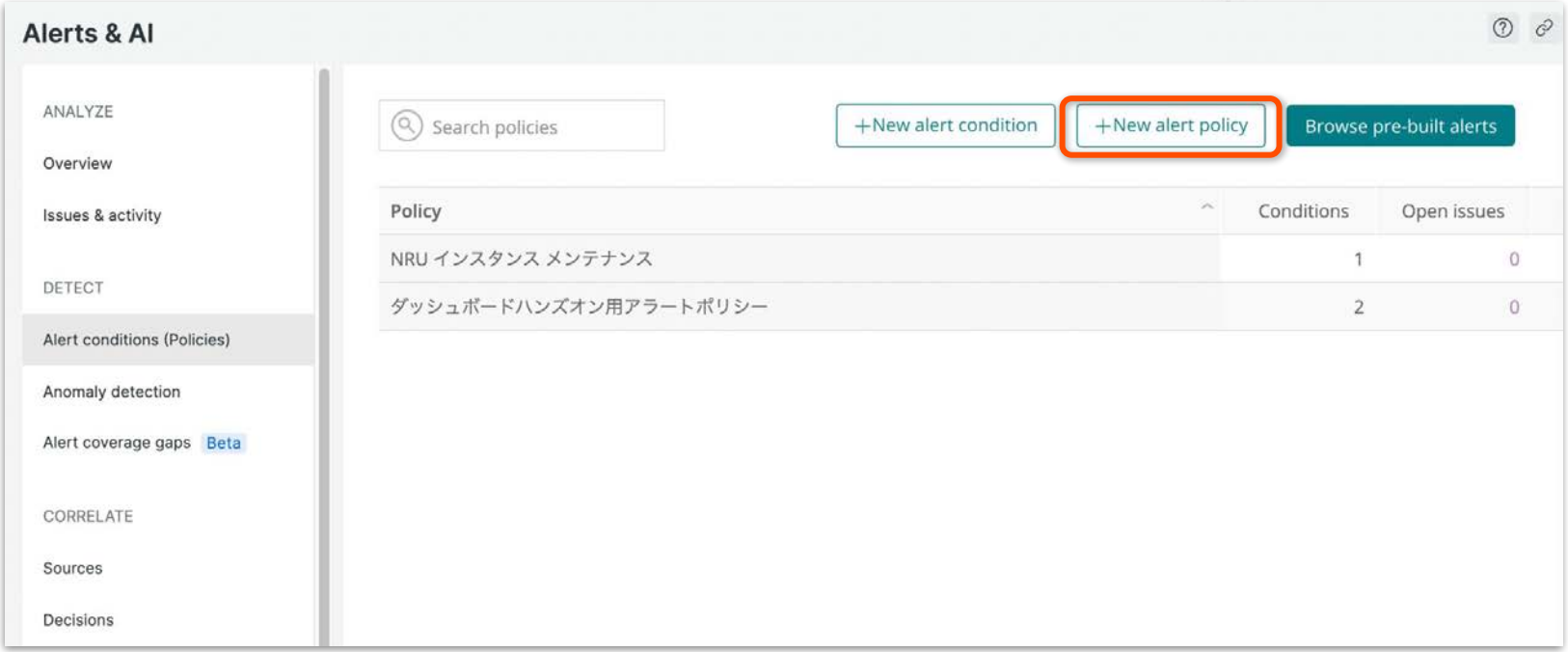


ハンズオン(1)-1 Alert policyを作成する 2/4

- 「Alert conditions (Policies)」をクリックします。

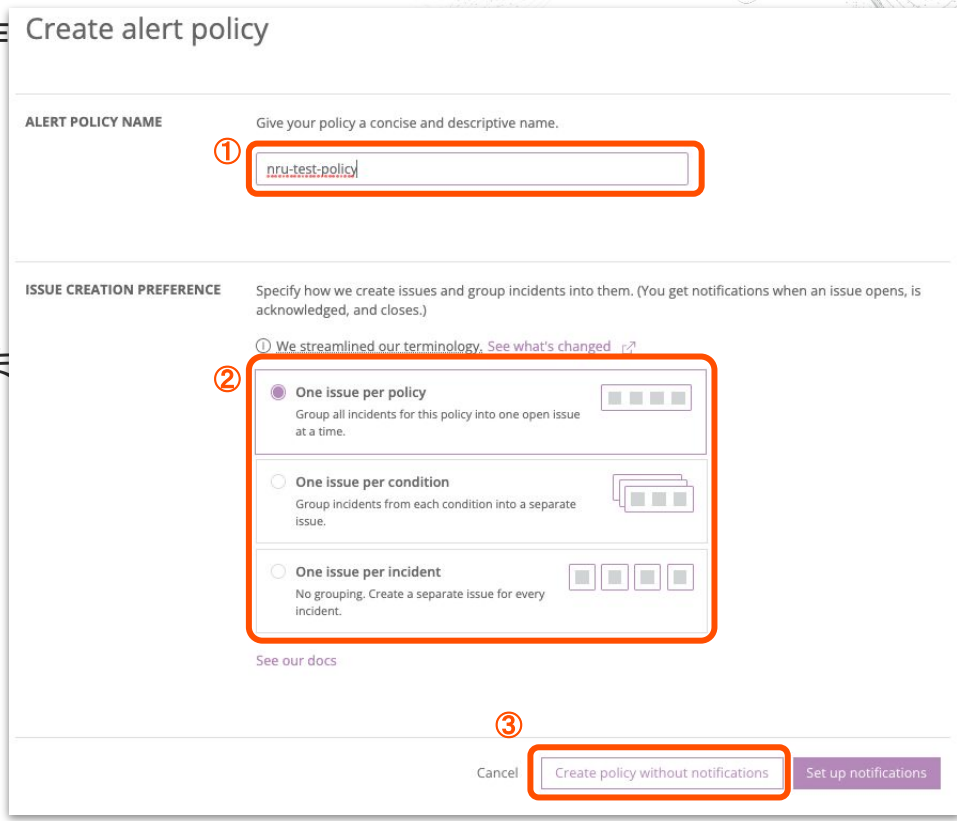
ハンズオン(1)-1 Alert policyを作成する 3/4

- 「＋ New alert policy」をクリックして新しい Policyを作成します。



ハンズオン(1)-1 Alert policyを作成する 4/4

1. 自分用と判断できる名前を付けて AlertPolicyを作成します
2. New Relic アラートの構成要素② Incident Preference 1/2 を参考に、好みの「INCIDENT PREFERENCE」を選択してください
3. [Create policy without notifications]をクリックします
    a. あえてすべての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 Alert Conditionを作成する 1/18

[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)-2 Alert Conditionを作成する 2/18

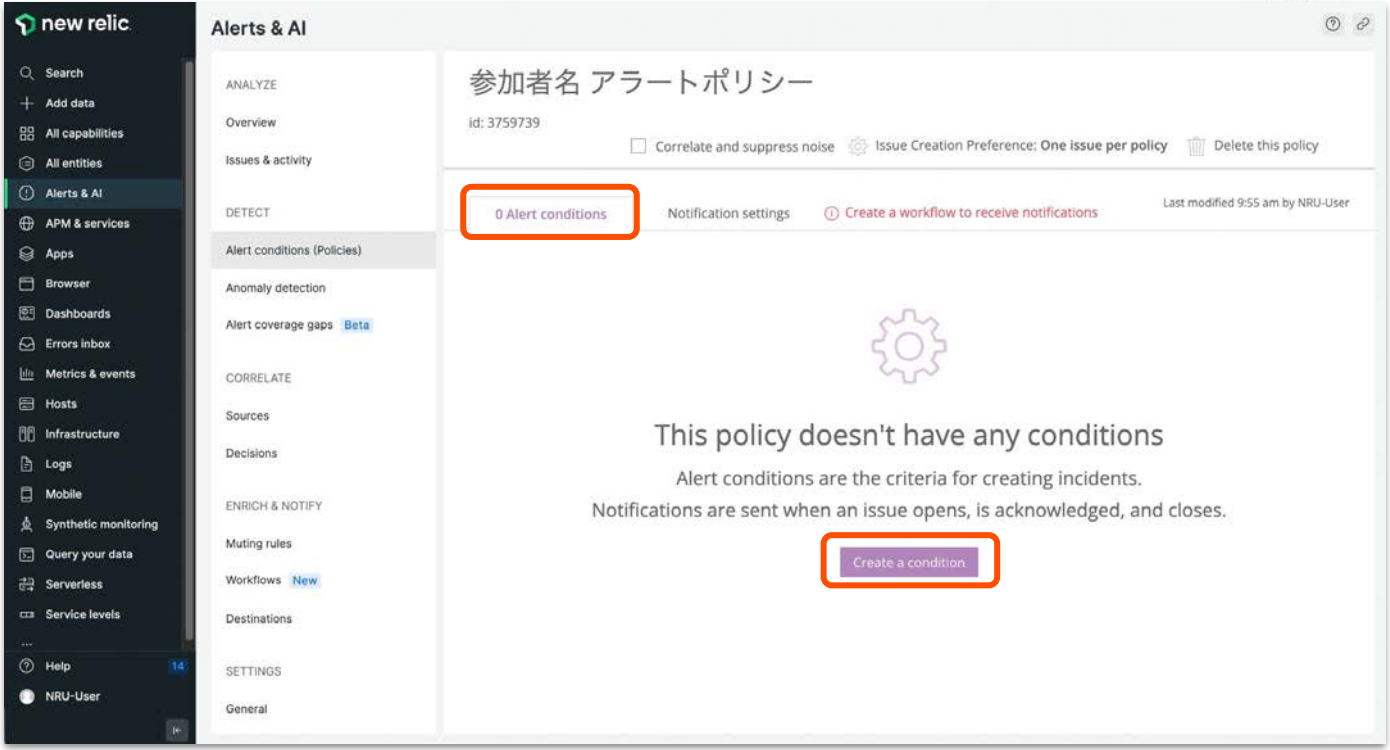
- 新規Alert Conditionの追加

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)

ハンズオン(1)-2 Alert Conditionを作成する 3/18

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



ハンズオン(1)-2 Alert Conditionを作成する 4/18

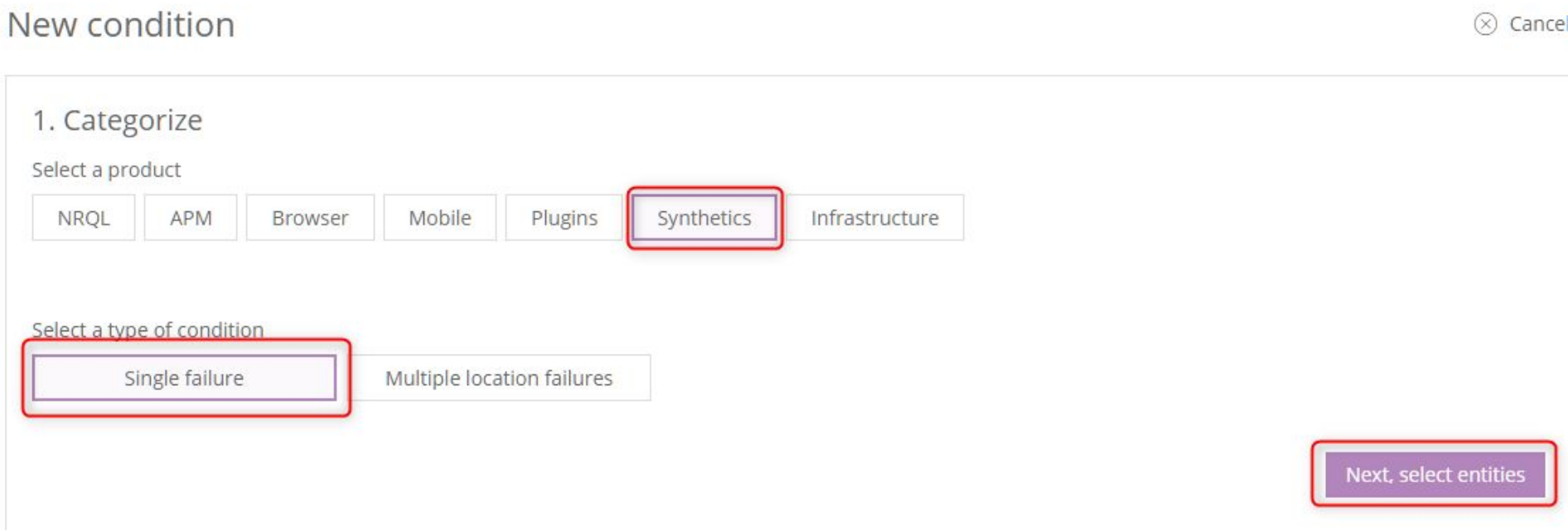
- 外形監視:チェックエラー
- 監視設定は次のようにしてください。

1. **Categories**
   a. Synthetics –> Single failure

2. **Select a monitor**
   a. EC-CUBE-Checkout

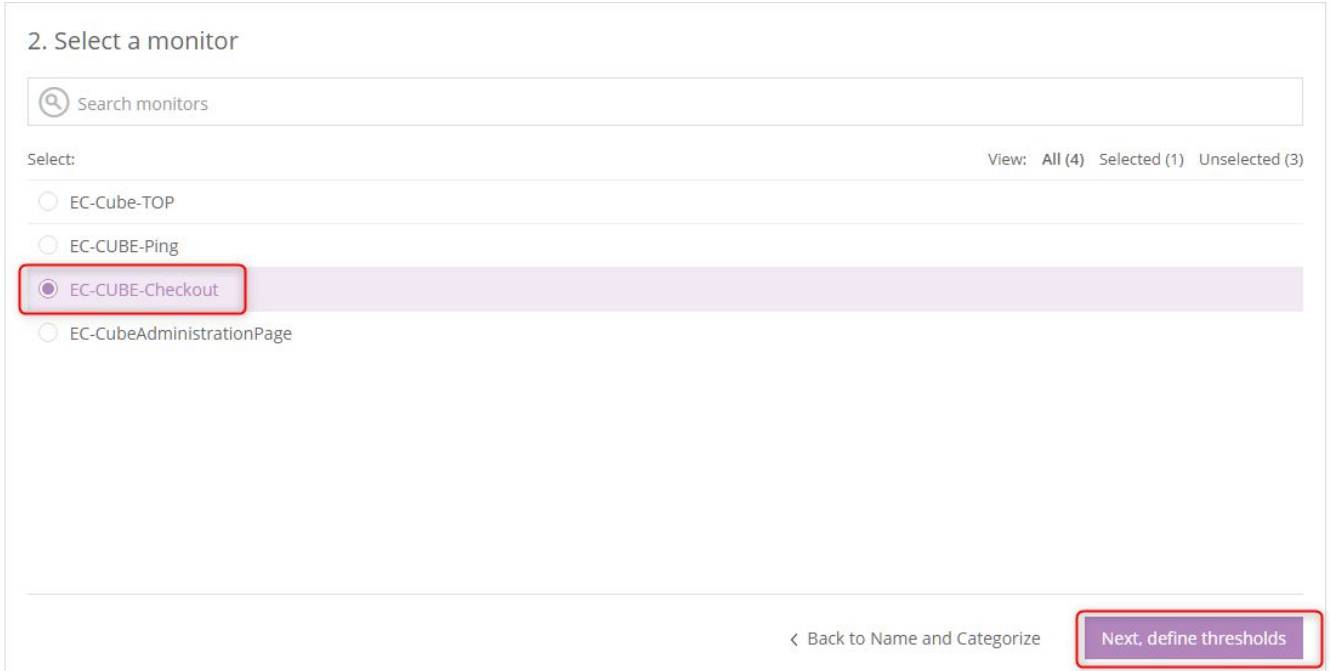
ハンズオン(1)-2 Alert Conditionを作成する 5/18

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



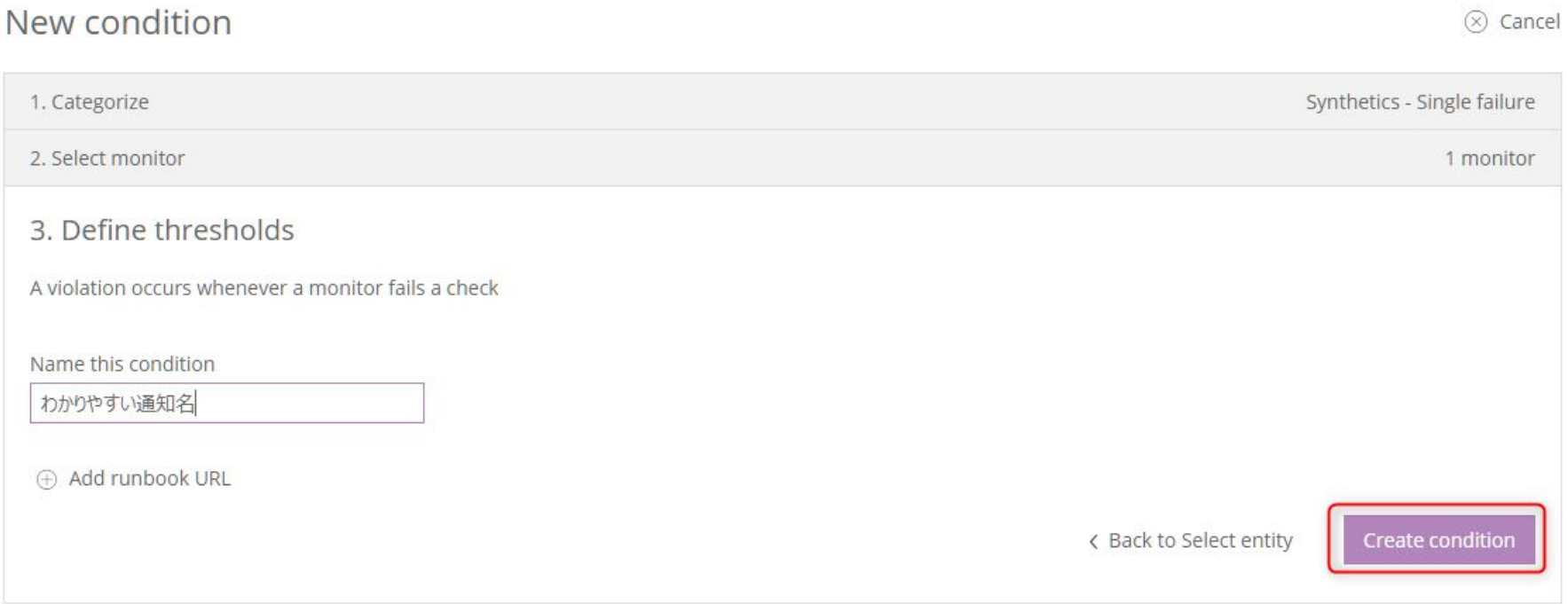
ハンズオン(1)-2 Alert Conditionを作成する 6/18

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



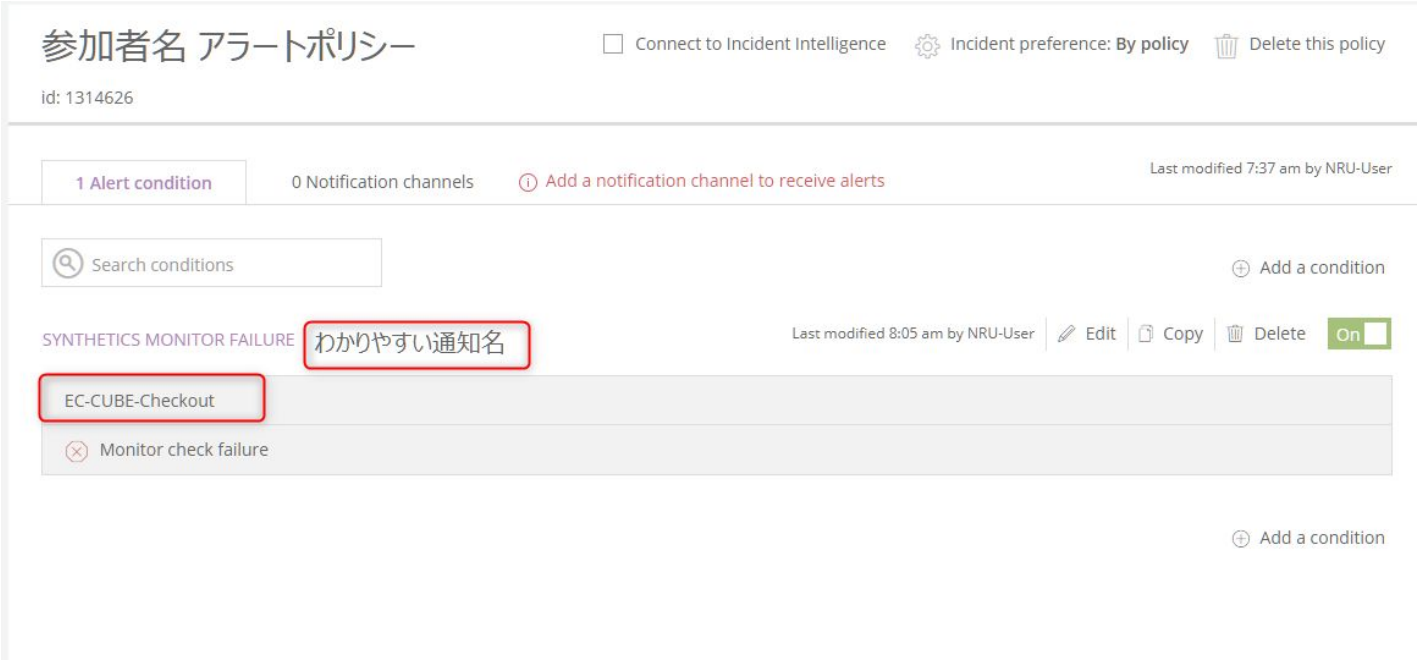
ハンズオン(1)-2 Alert Conditionを作成する 7/18

- 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。



ハンズオン(1)-2 Alert Conditionを作成する 8/18

- 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(1)-2 Alert Conditionを作成する 9/18

- **新規Alert Conditionの追加**

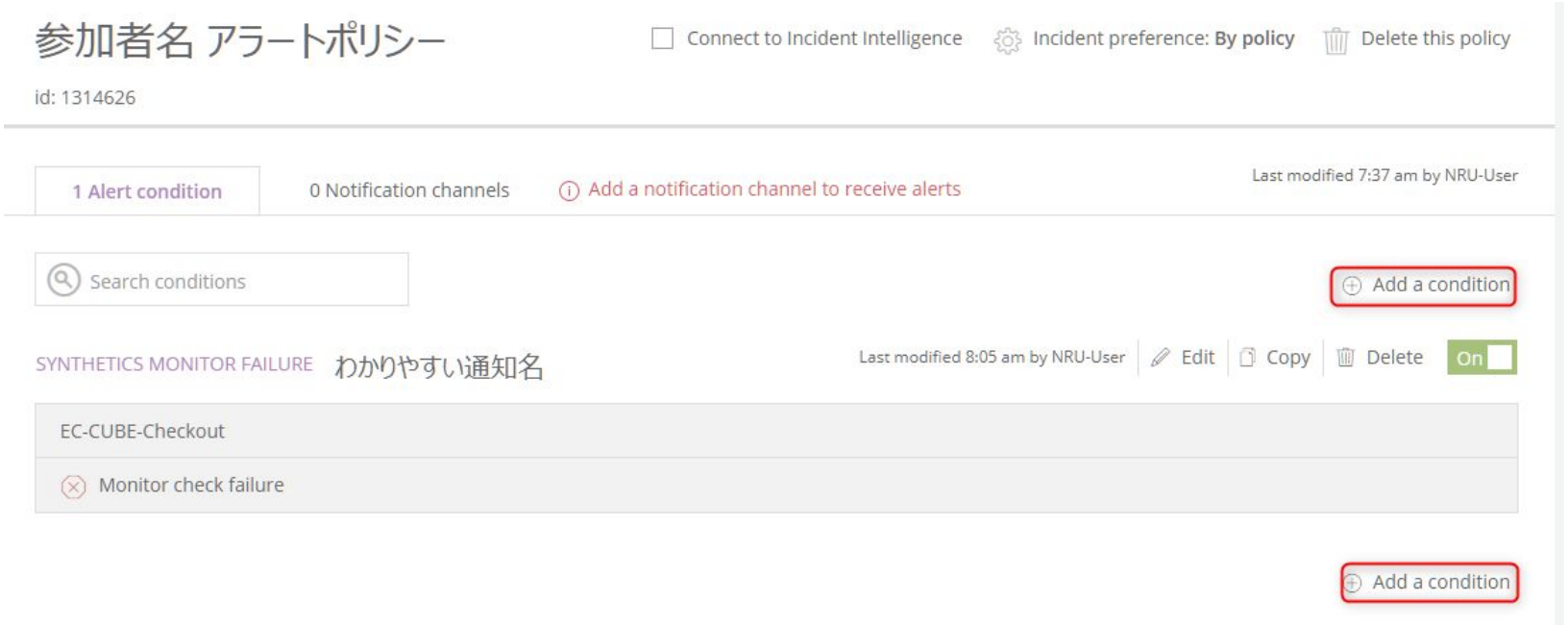
②フロントエンド: Apdex(静的)

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

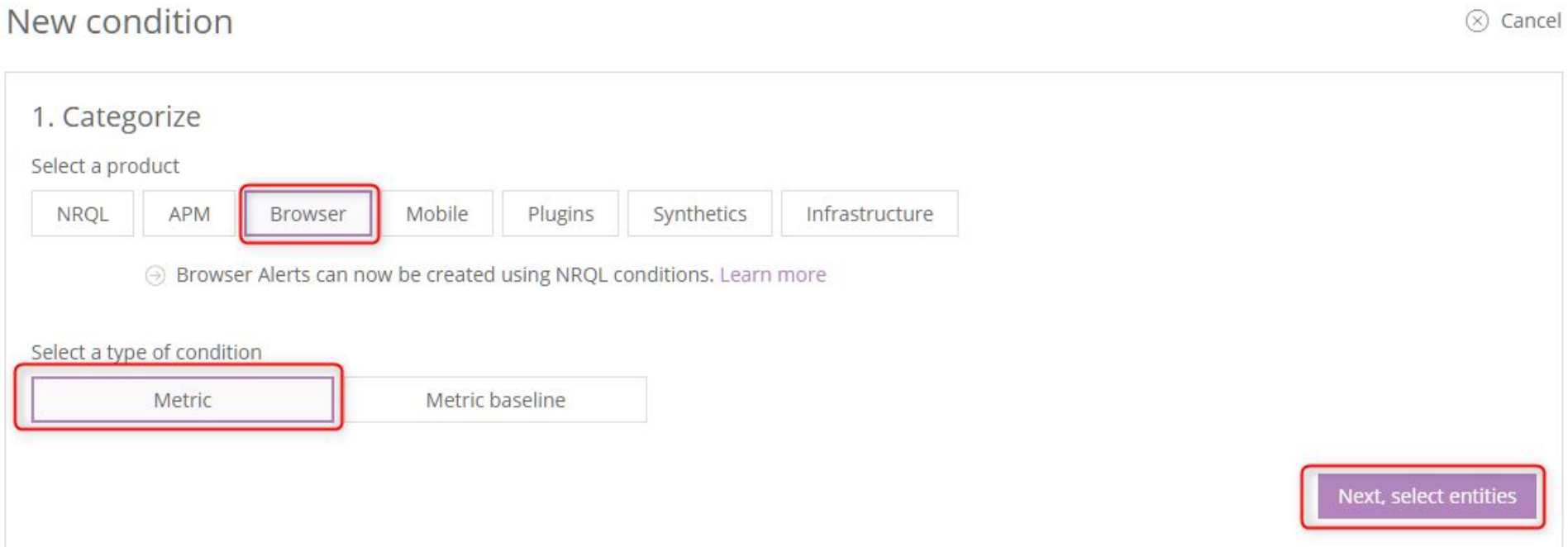
ハンズオン(1)-2 Alert Conditionを作成する 10/18

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



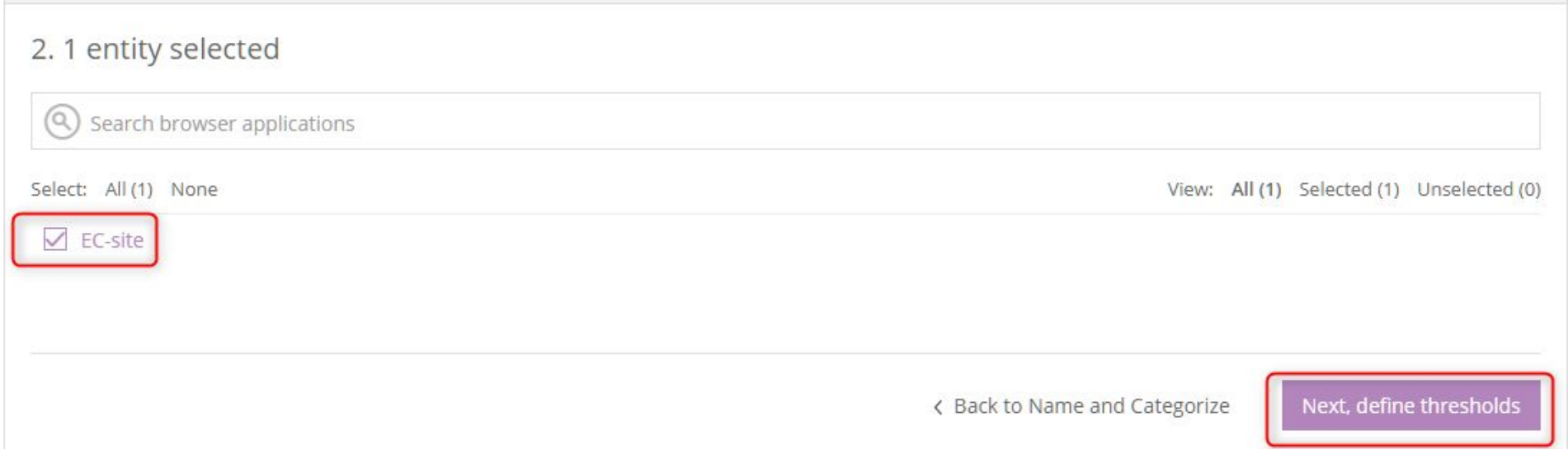
ハンズオン(1)-2 Alert Conditionを作成する 11/18

- Categories を設定します。



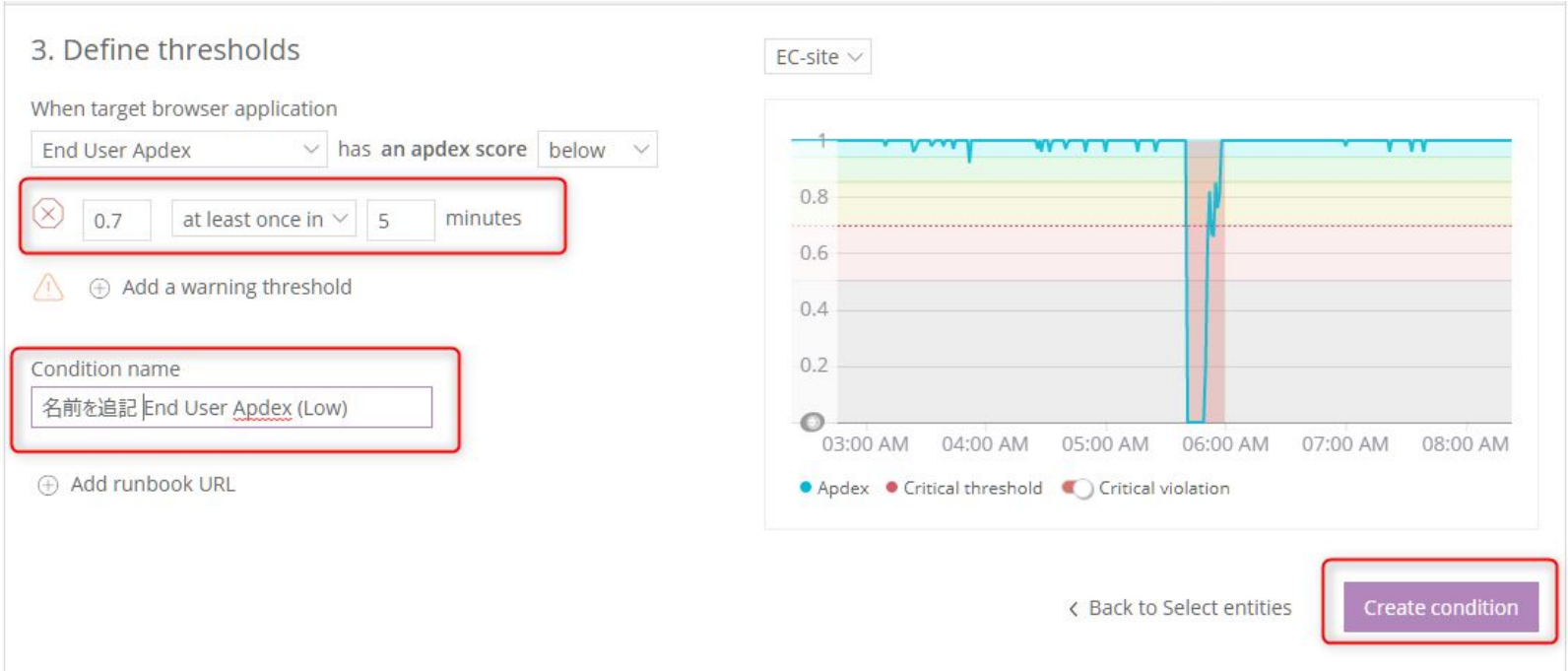
ハンズオン(1)-2 Alert Conditionを作成する 12/18

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



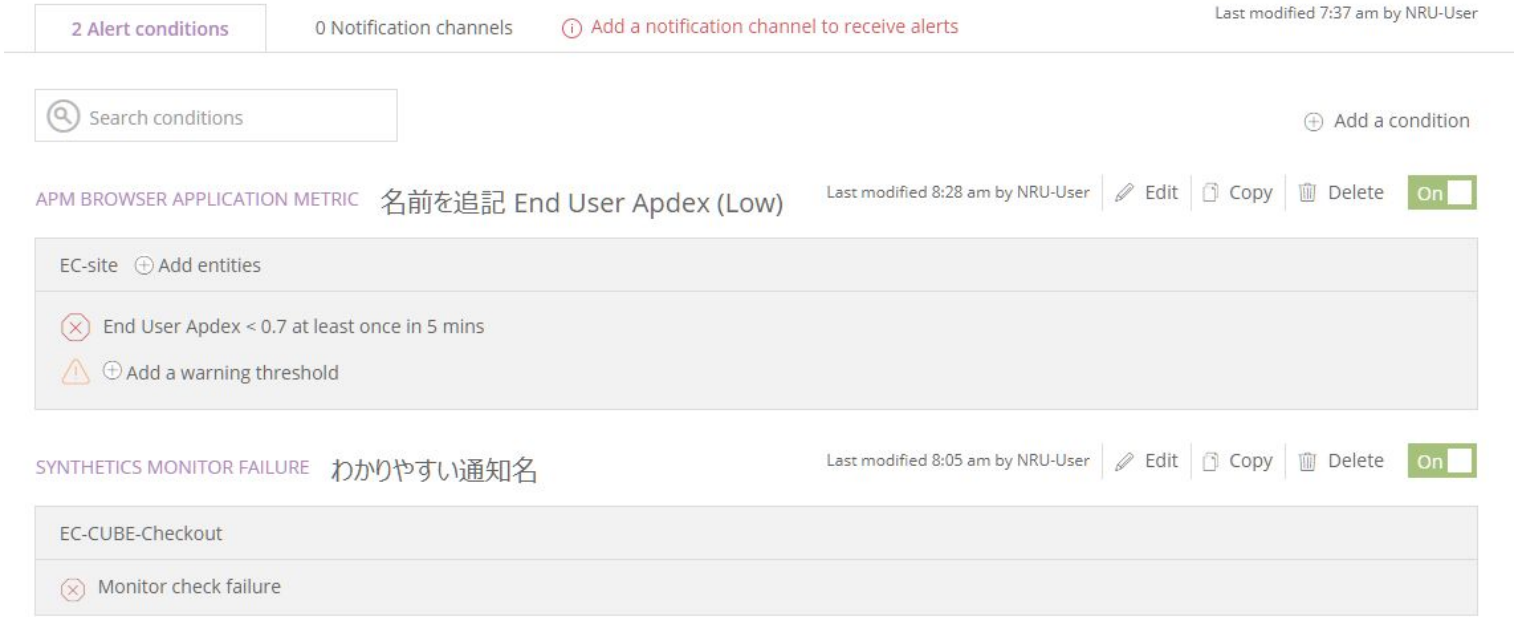
ハンズオン(1)-2 Alert Conditionを作成する 13/18

- Thresholds を設定しわかりやすい名前を設定します。



ハンズオン(1)-2 Alert Conditionを作成する 14/18

- 2つめのconditionが作成されました。



ハンズオン(1)-2 Alert Conditionを作成する 15/18

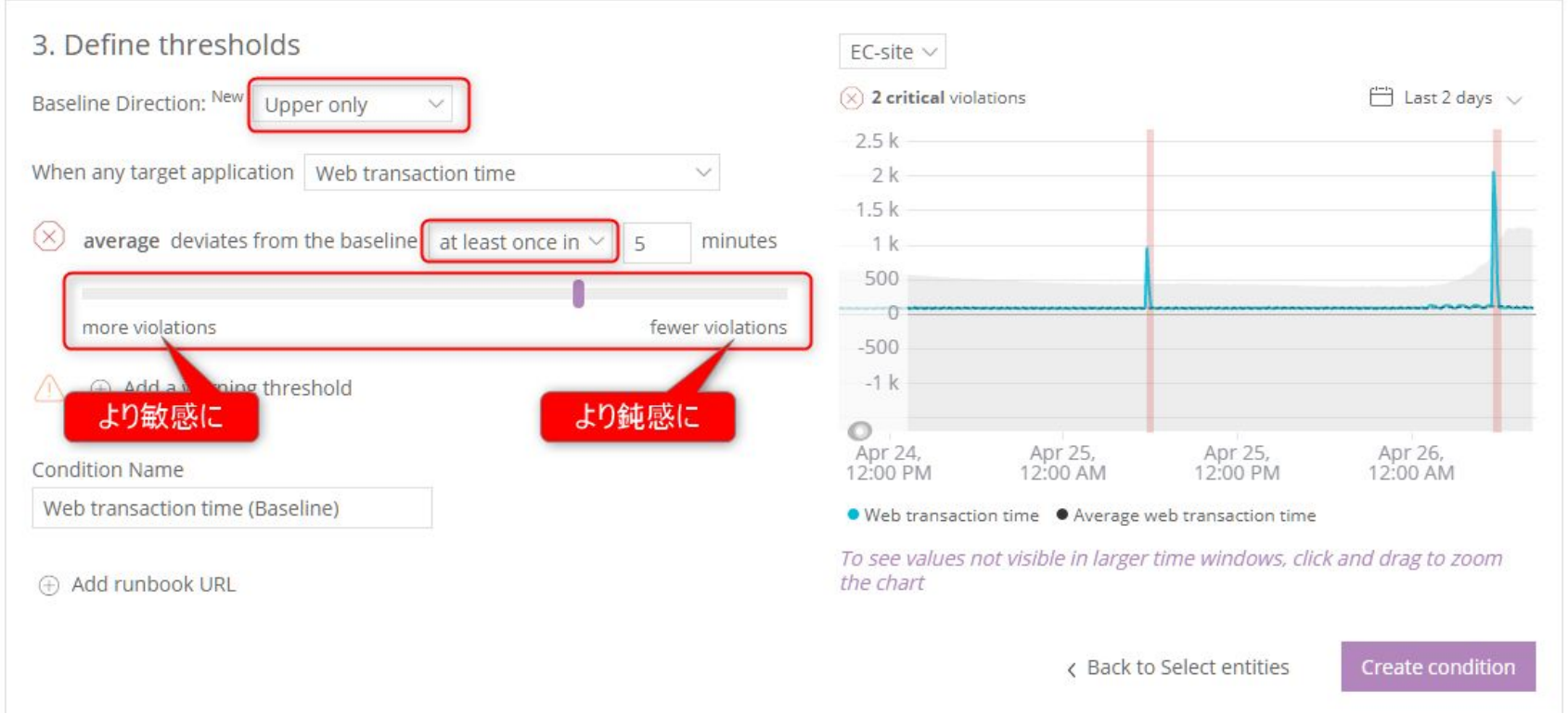
- **新規Alert Conditionの追加**
  ③アプリケーション : 応答時間(動的)

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

ハンズオン(1)-2 Alert Conditionを作成する 16/18

- 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。



ハンズオン(1)-2 Alert Conditionを作成する 17/18

- **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. **Enter NRQL query**

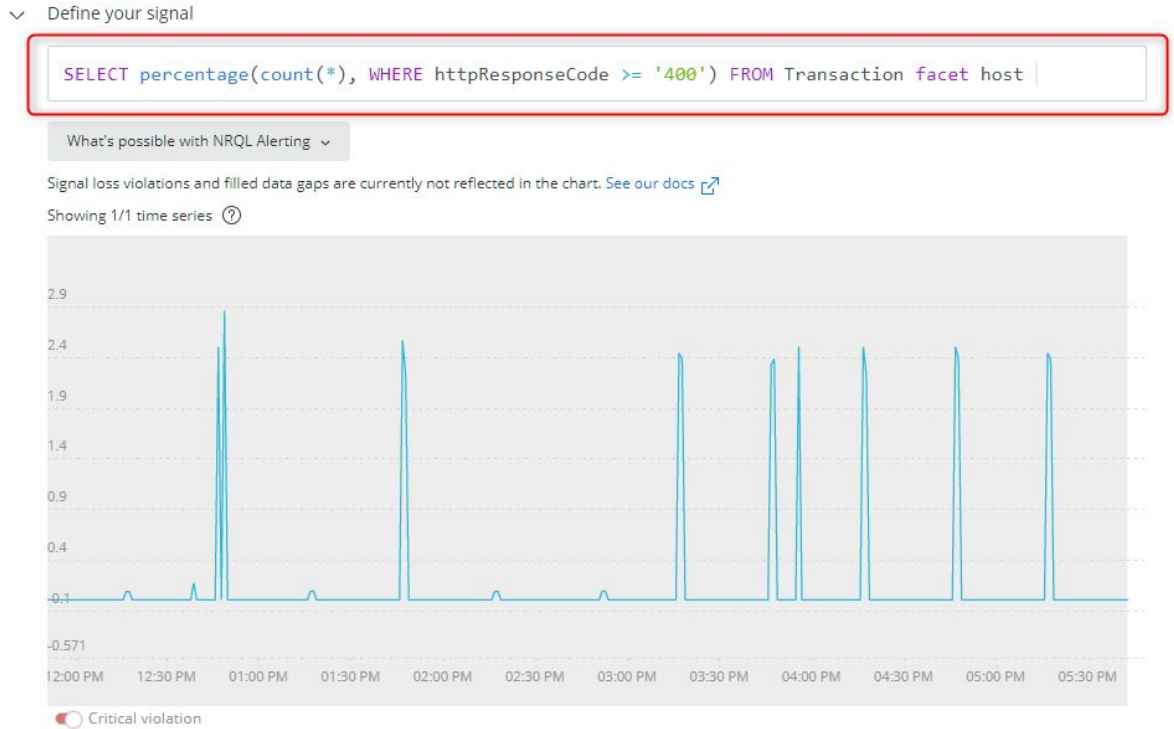
```
SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction facet host
```

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

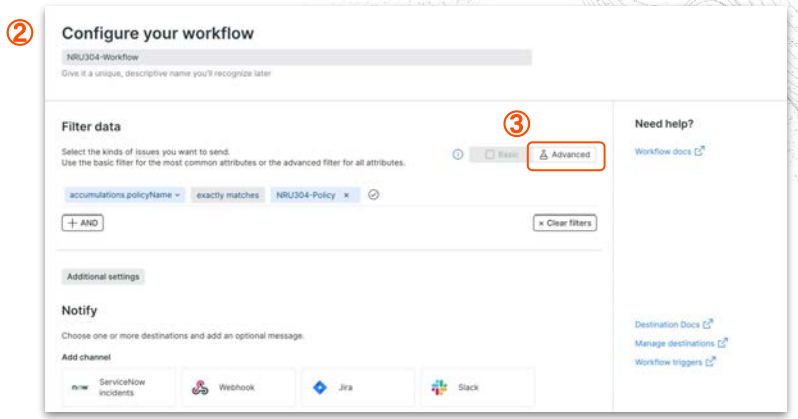
ハンズオン(1)-2 Alert Conditionを作成する 18/18

- NRQLを入力すると自動的に参考となる Chartが表示されます。



ハンズオン(1)-3 Workflows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workflows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

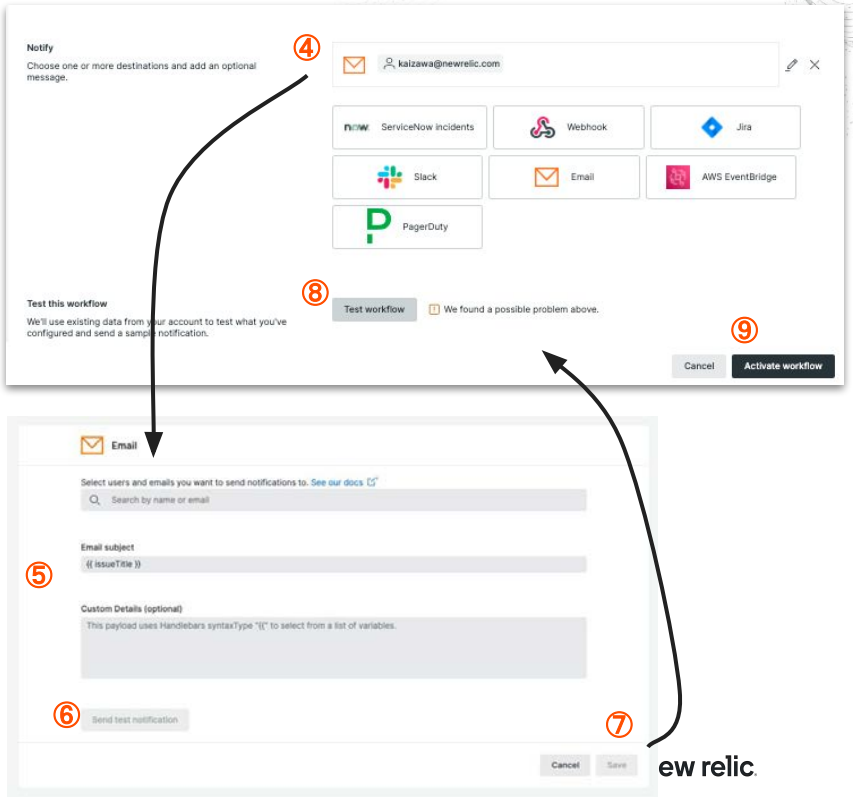


次のスライドに進みます

ハンズオン(1)-3 Workflowsを作成する 2/6

4. Notify: Emailを選択します **(重要)**
5. メール送信内容を設定します
   a. 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、指定したメールアドレスに通知メールが届くかを確認します
   a. メール内容を確認します
      i. Policy名やCondtion名は確認できますか？
      ii. Runbook情報URLはどこに記載されていますか？
      iii. Tagsというセクションはありますか？

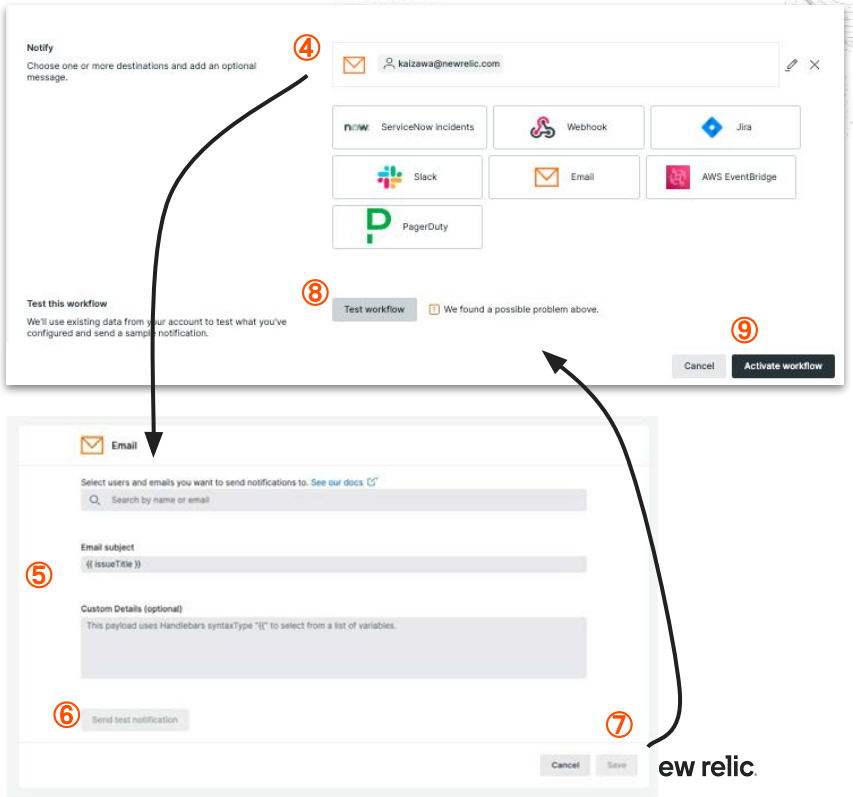
次のスライドに進みます



ハンズオン(1)-3 Workflowsを作成する 3/6

6. Send test notificationボタンをクリックし、指定したメールアドレスに通知メールが届くかを確認します
   b. 無事に手元に届いたことを確認の後に、⑤に戻り、Email subjectやCustom Detailsを変更します。再度Send test notificationをクリックし、どのようにメールの中身が変わるかを確認します。(色々試してみて下さい。)
      i. 補足: 環境変数を利用する際は、"{{"と入力して開始して下さい。
7. Saveボタンを押します

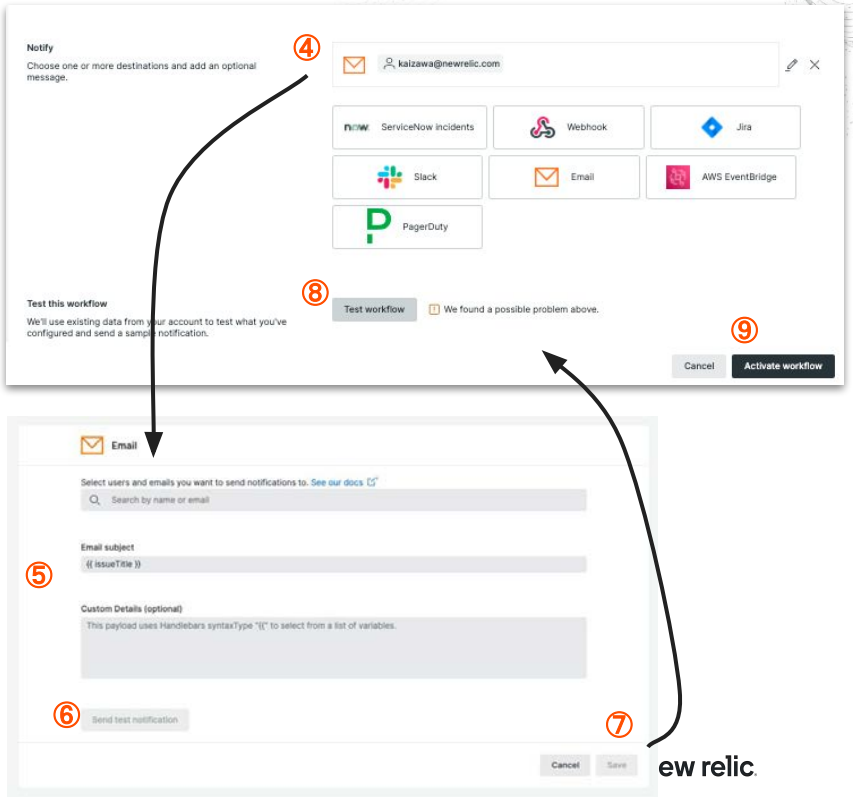
次のスライドに進みます



ew relic

ハンズオン(1)-3 Workflowsを作成する 4/6

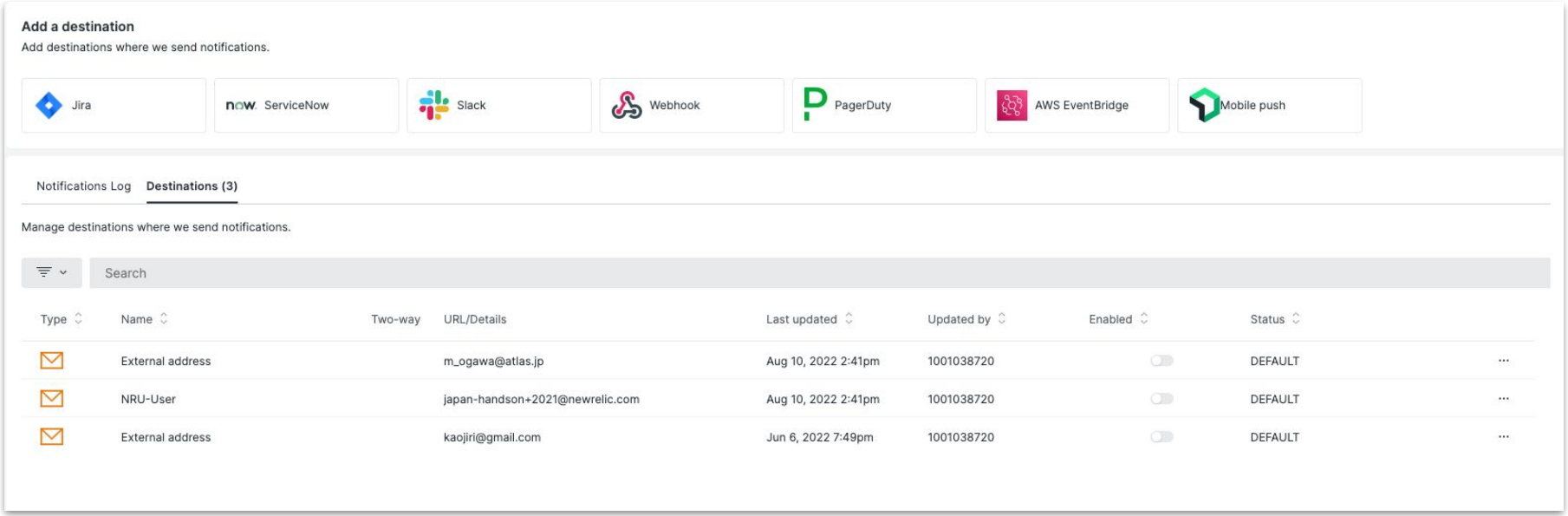
8. Test workflowボタンを押し、テスト用メール内容を確認してください。
   b. 先程のテスト用メールとどの様な違いがあるかを確認してください
9. Active workflowボタンをクリックし、設定を保存します



ハンズオン(1)-3 Workflowsを作成する 5/6

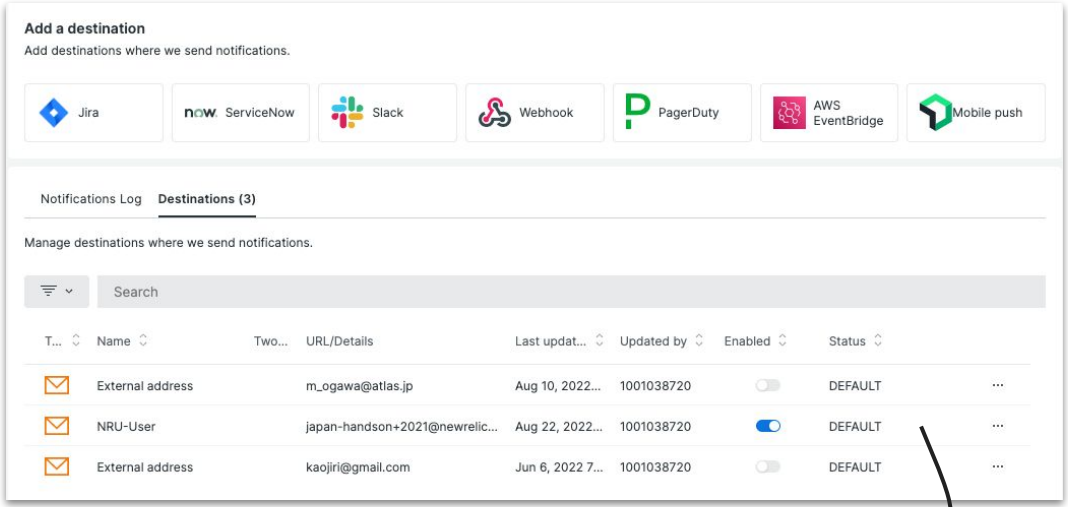
Workflows内でEmailを追加すると、Destinationも自動的に作成されます。

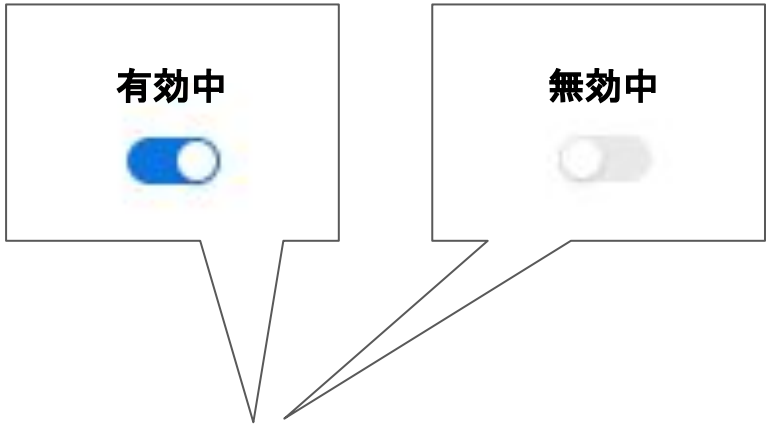
Alerts & AIメニューのDestinationsをクリックし、External addressとしてご自身のメールアドレスが追加されていることを確認します



ハンズオン(1)-3 Workflows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。



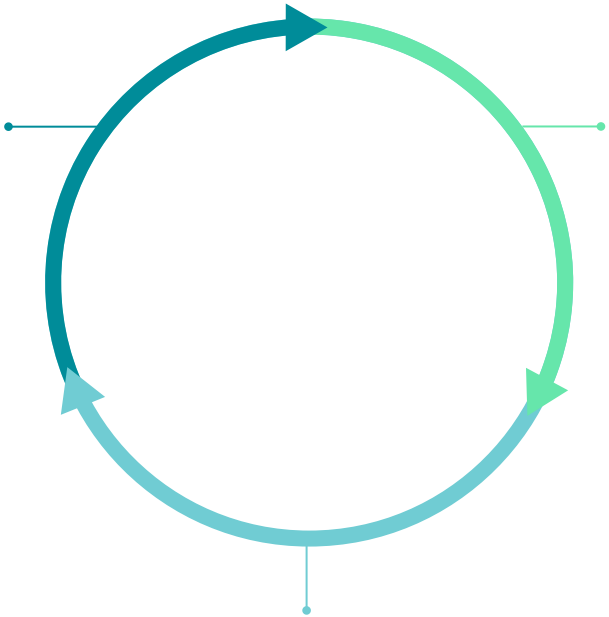


座学(3)
New RelicのAIOps機能

16:05 - 16:15 (10min)

new relic

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)

⬇

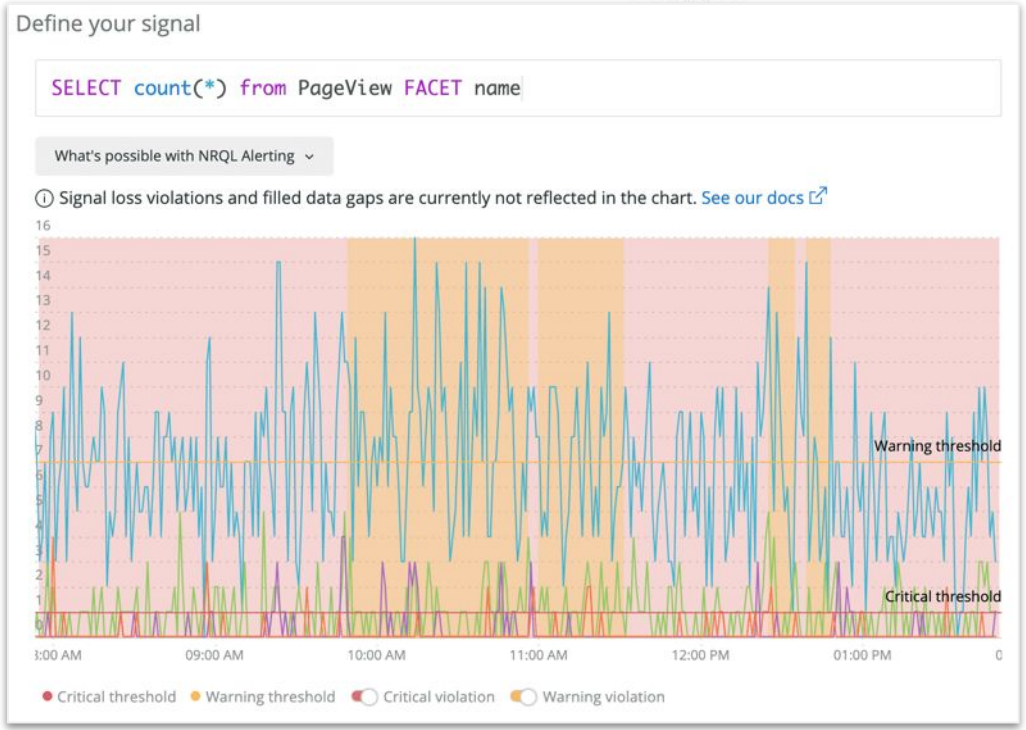
診断

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)

↓

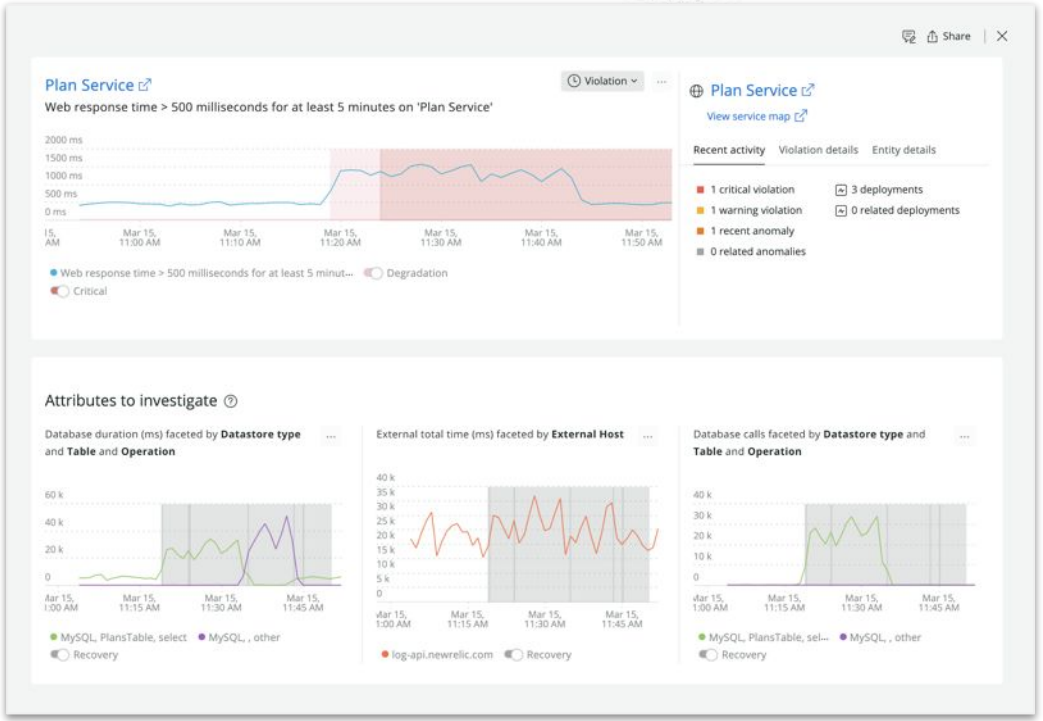
診断

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

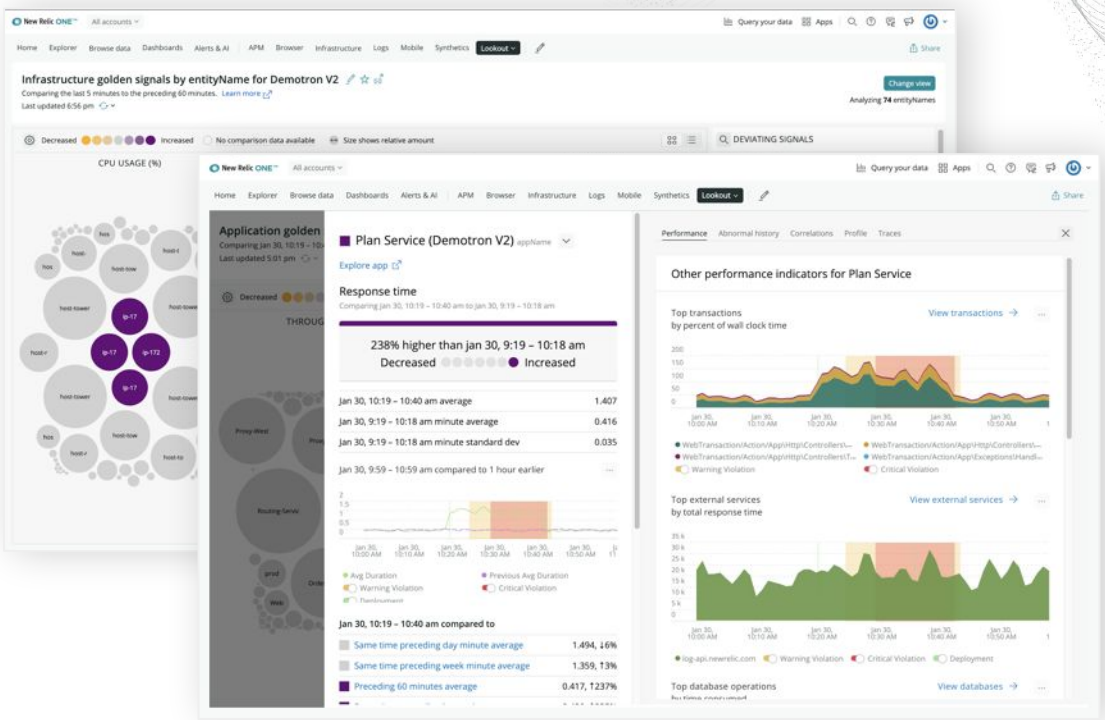
イベントの相関分析

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

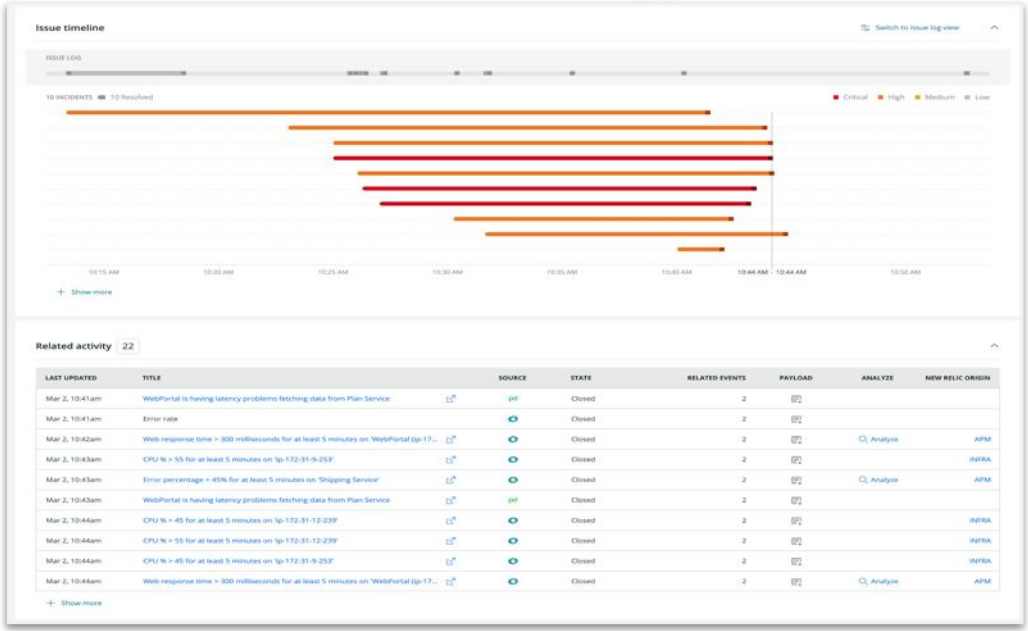
イベントの相関分析

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

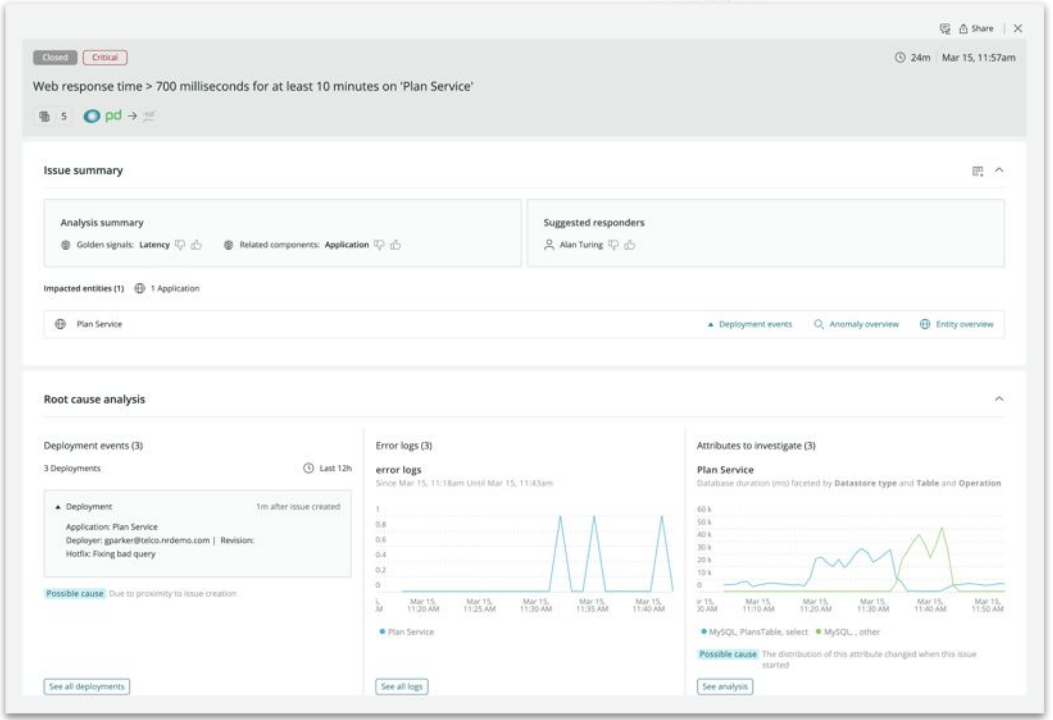
イベントの相関分析

根本原因分析

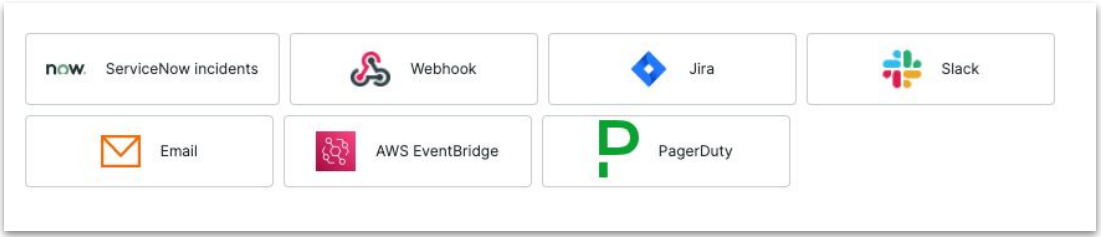
↓

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



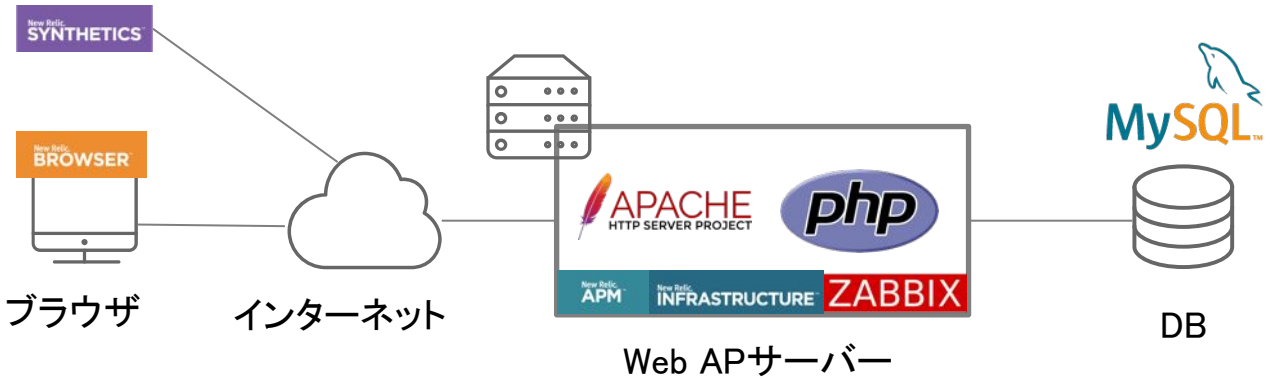
ハンズオン(2)
AIOpsを使った異常検知と原因分析

16:15 - 16:30 (15min)

※使用アカウント：NewRelic.kkとOriginal newrelic account
（ログイン先選択はこちら参照）

今回の環境の監視構成(再掲)

- 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(2)

1. 異常を可視化する

[目的]
AIOps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）

ハンズオン(2)

2. 個々のアラートを確認する

[目的]
AIOps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、Open中のアラートを確認する
  - 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

ハンズオン(2)

AIOps:イベントの相関分析

AIOps:根本原因分析

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]
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

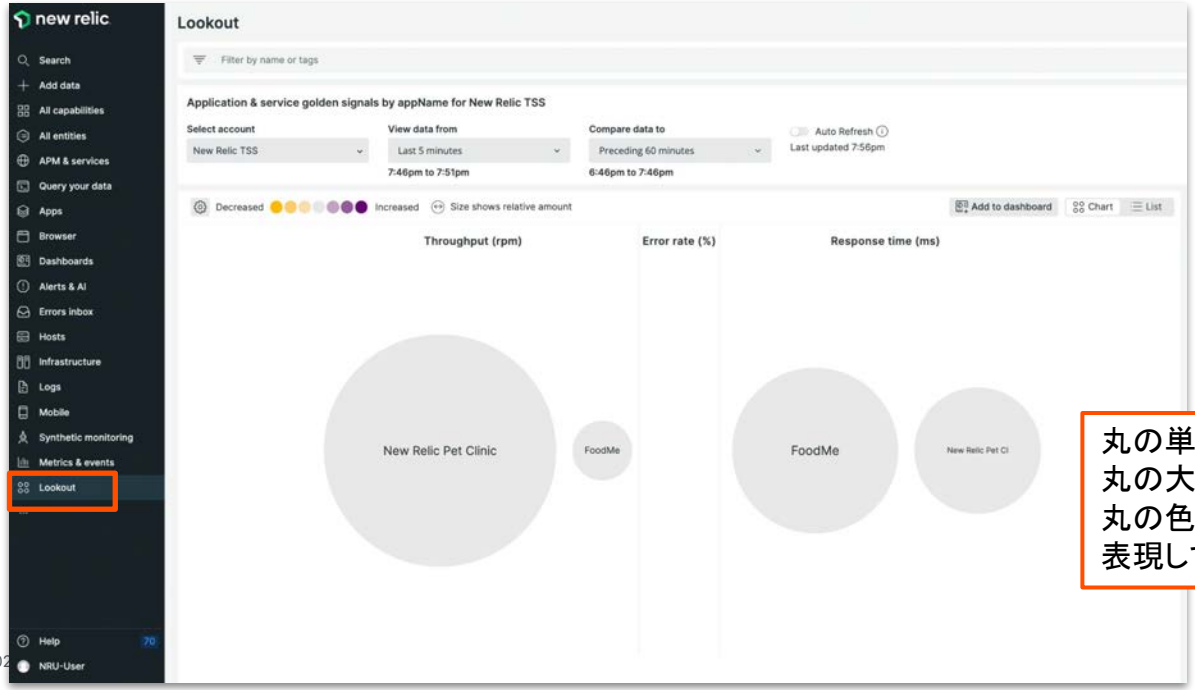
- Alerts&AI -> Overview -> Issueで、Active中のIssueを確認する
  - それぞれ、どのようなアラートが紐付いているかを確認しましょう
  - Root cause analysisにどのような項目が書かれているでしょうか

手順・解説

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

ハンズオン(2)異常を可視化する

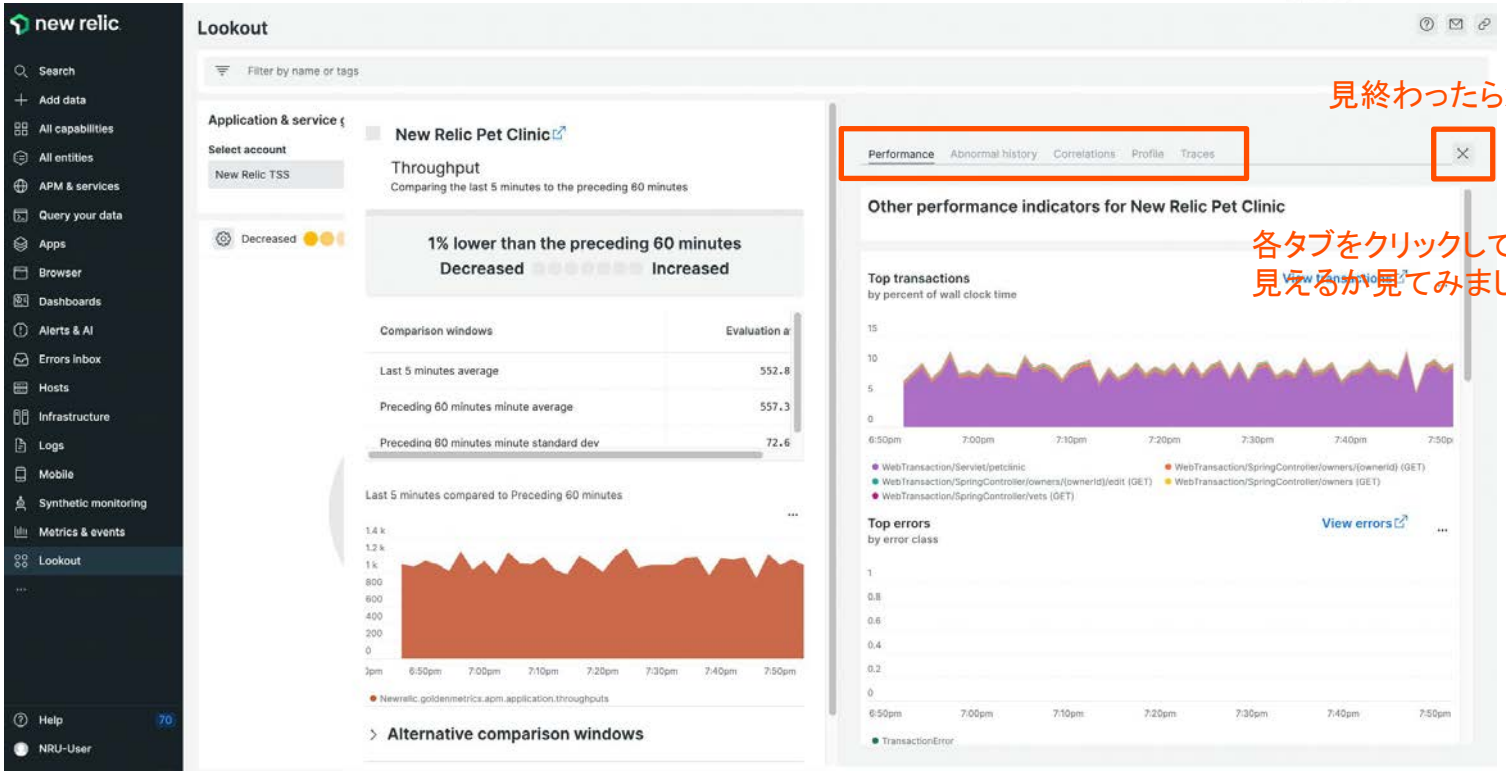
- 「Original New Relic account」側にログインします（詳細手順は こちら）
- メニューから「Lookout」をクリックし、現れた画面上でサービスの現状を読み解きましょう



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(2)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



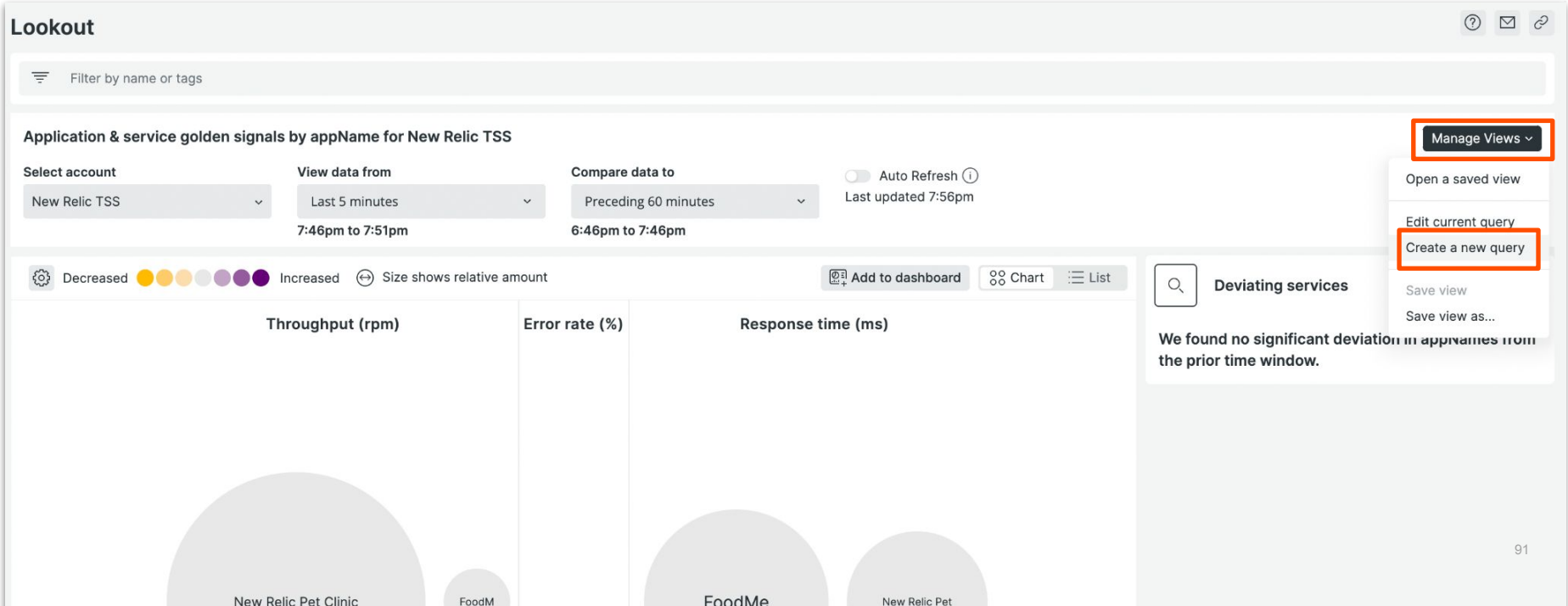
見終わったらxを押して閉じます

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

ハンズオン(2)異常を可視化する

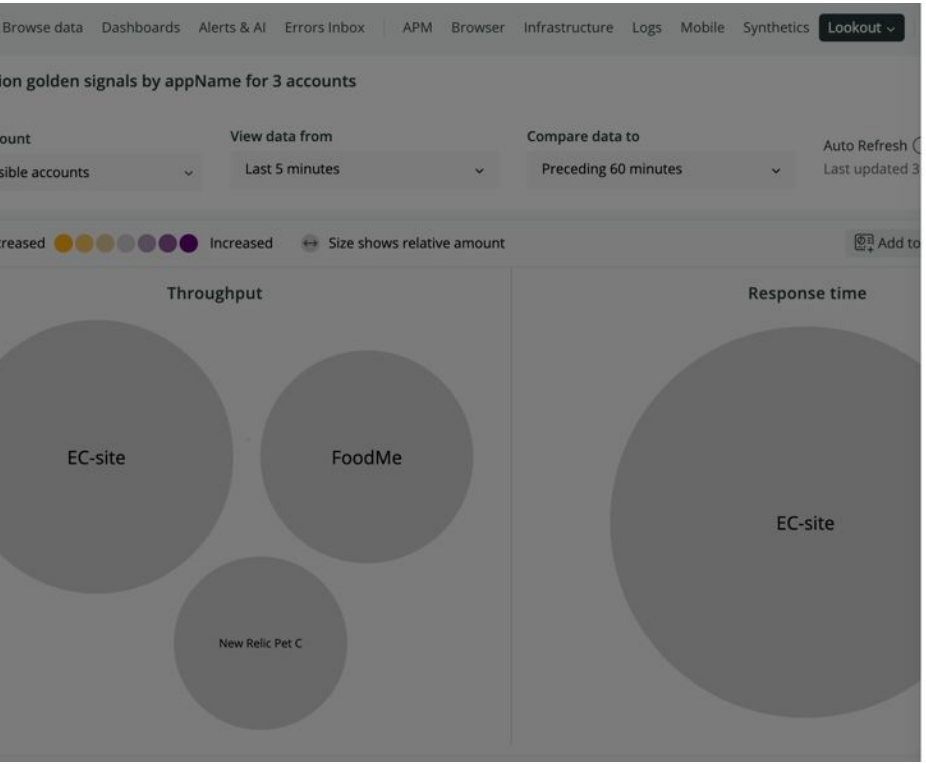
- カスタムのビューを作成します

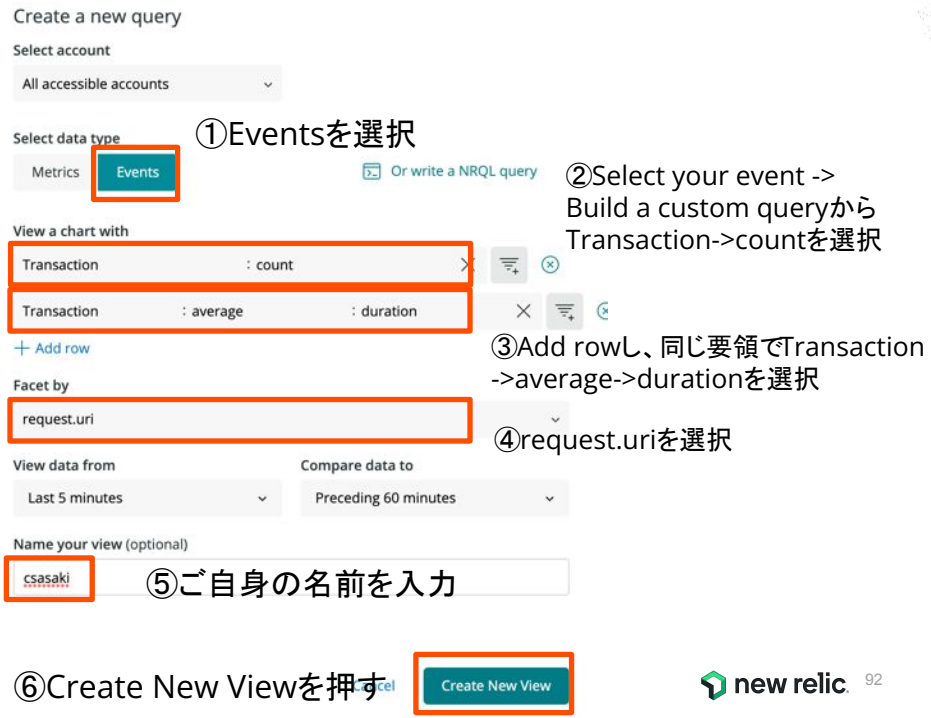
Manage Views -> Create a new queryを選択



ハンズオン(2)異常を可視化する

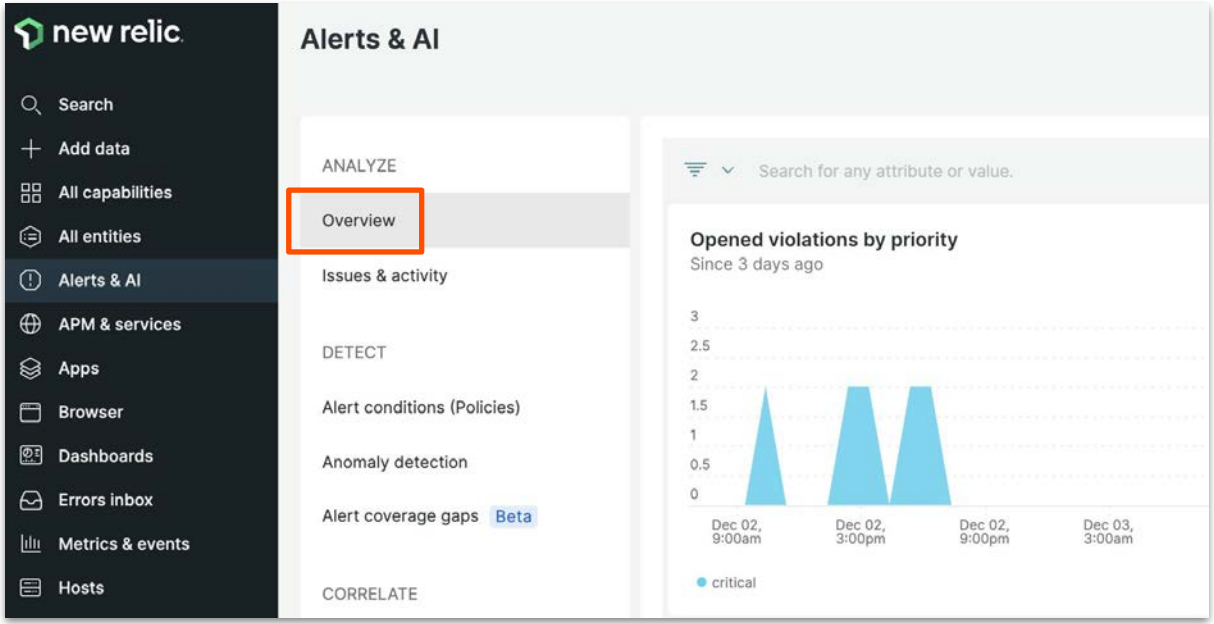
- カスタムのビューを作成します(続き)。作成後の画面から詳細分析ができます。
  この手順によりアクセス先URLごとでのレスポンスの多さと速さの大きさ、変化率が可視化できます。





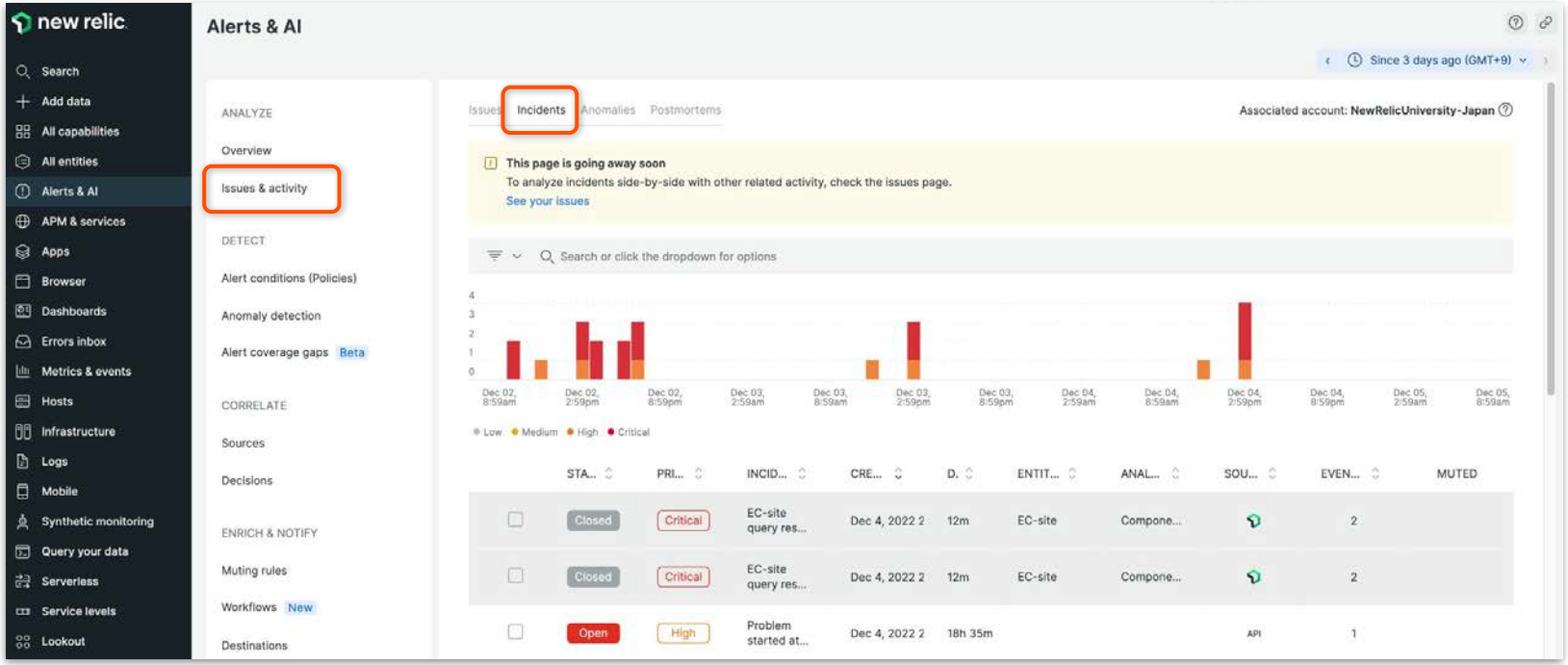
ハンズオン(2)個々のアラートを確認する

- 「Organization: NewRelic.kk」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



ハンズオン(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。

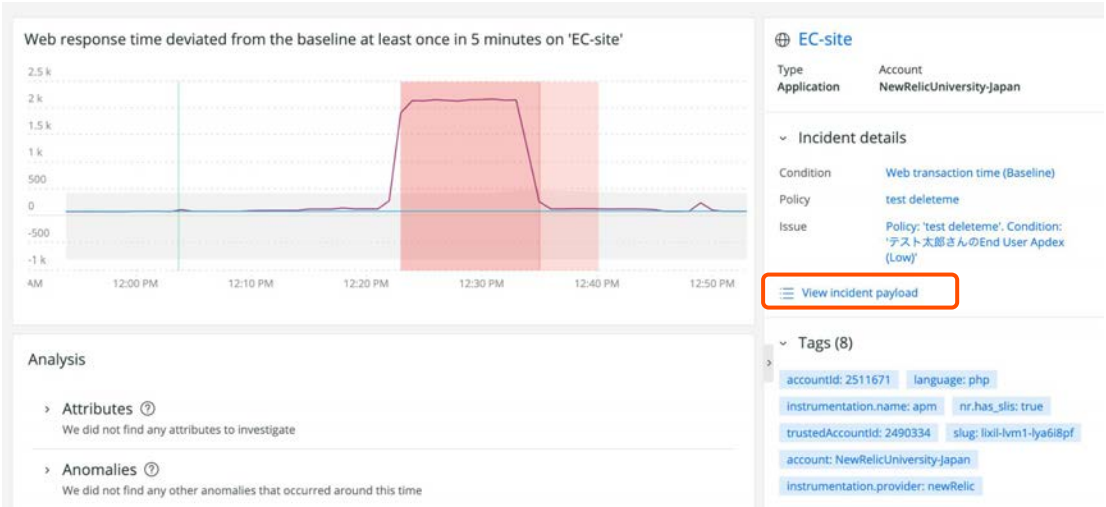


ハンズオン(2)個々のアラートを確認する

- 個々のIncidentをクリックします。

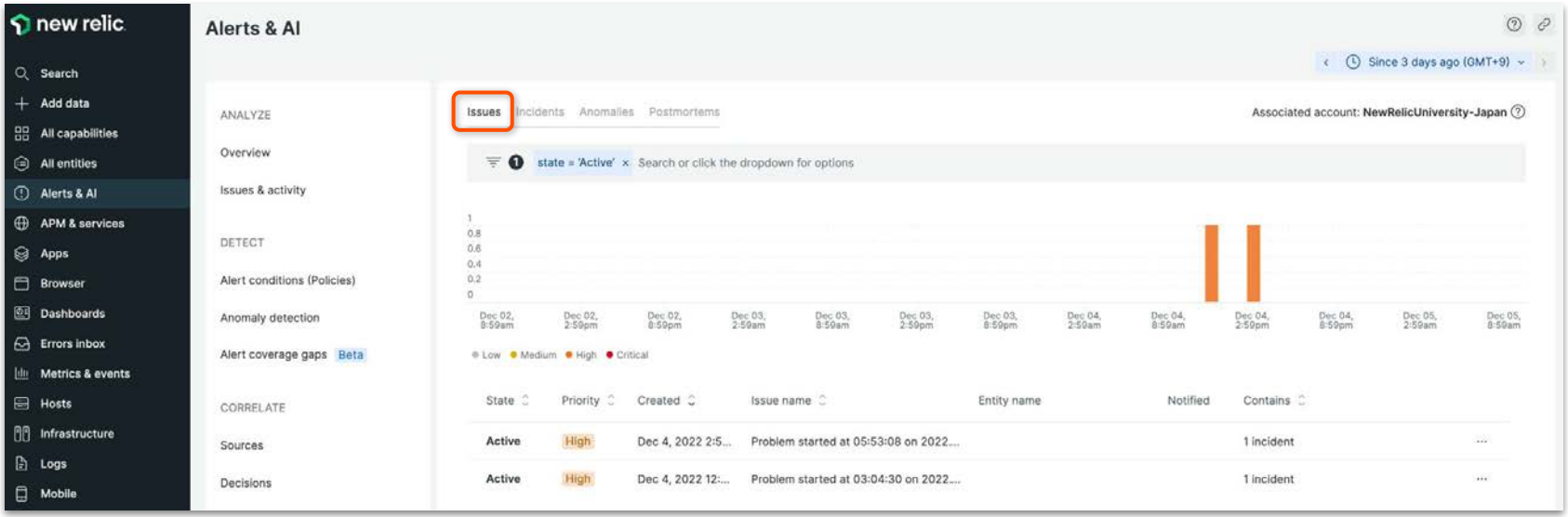
ハンズオン(2)個々のアラートを確認する

- 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。



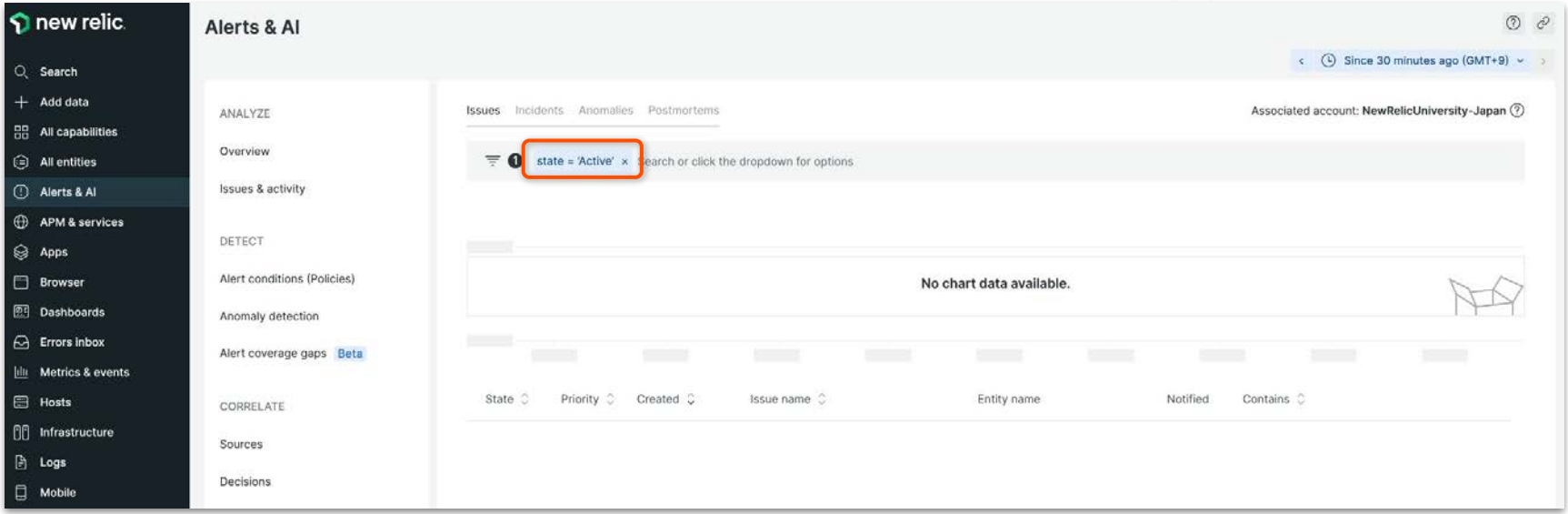
ハンズオン(2)複数のアラートを紐付けトラブルシューティングに役立てる

- 「Issues」タブをクリックします。



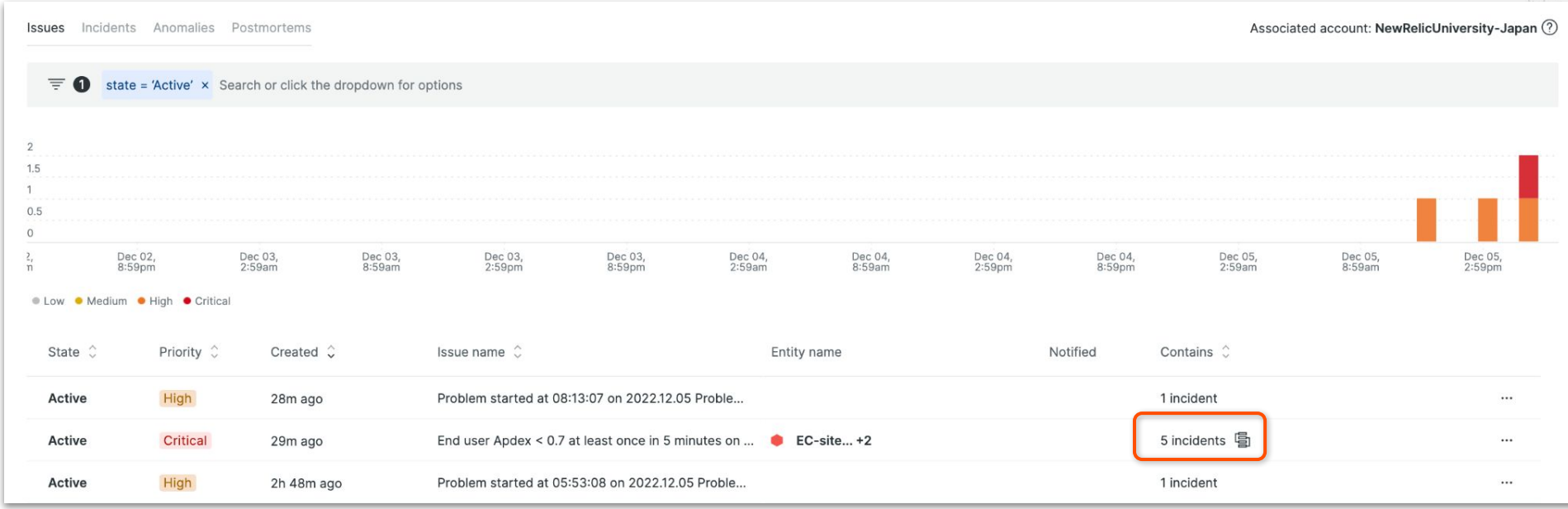
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- 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。



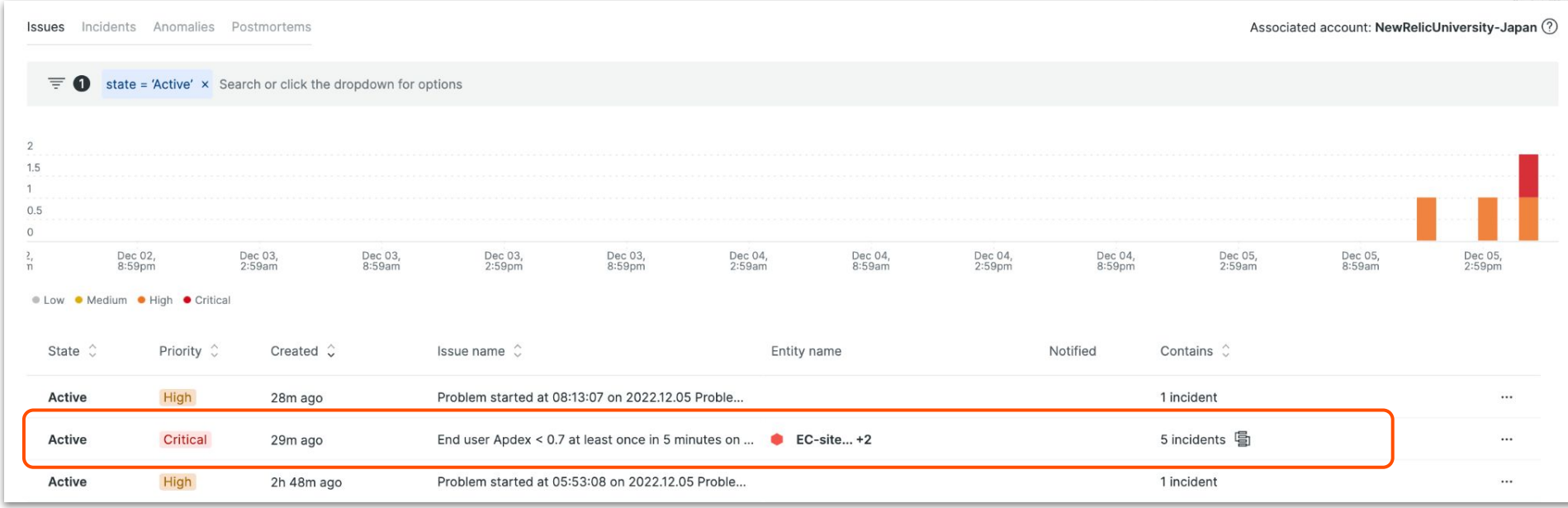
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- 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(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

- Issueをクリックすると詳細が表示されます。

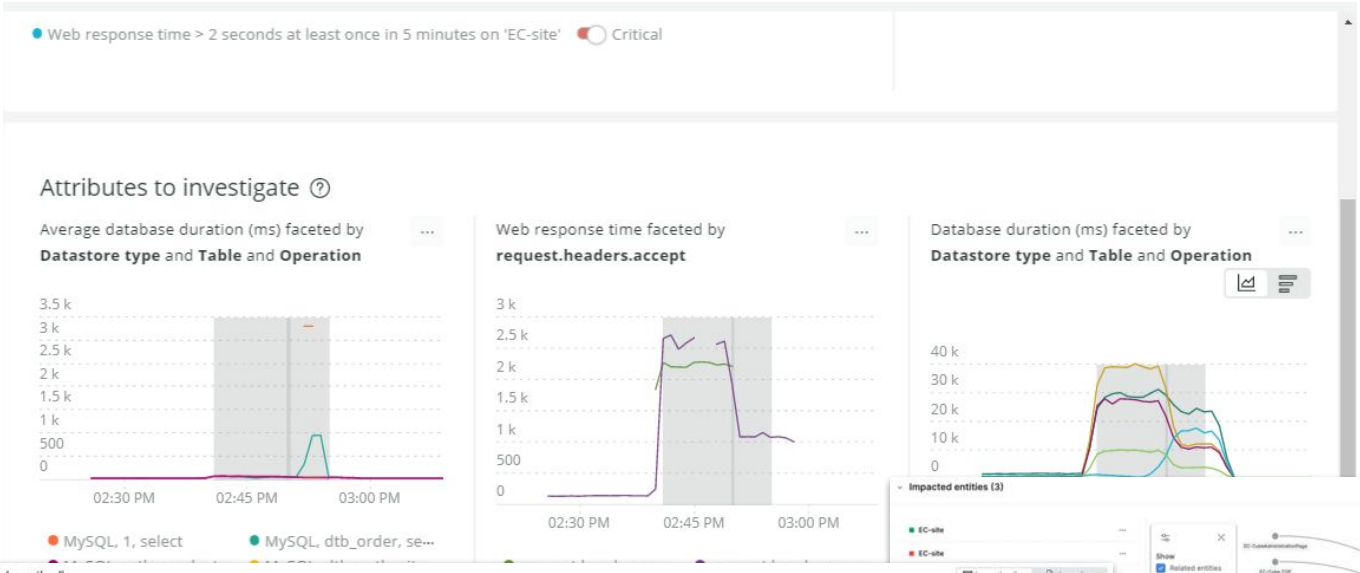


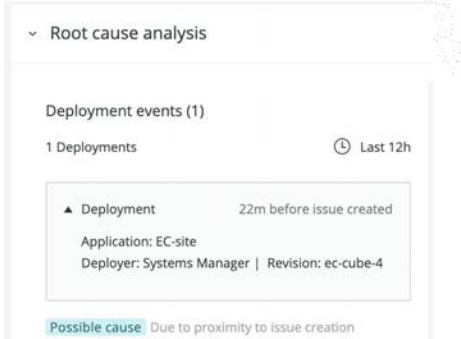
ハンズオン(2)複数のアラートを紐付けトラブルシューティングに役立てる

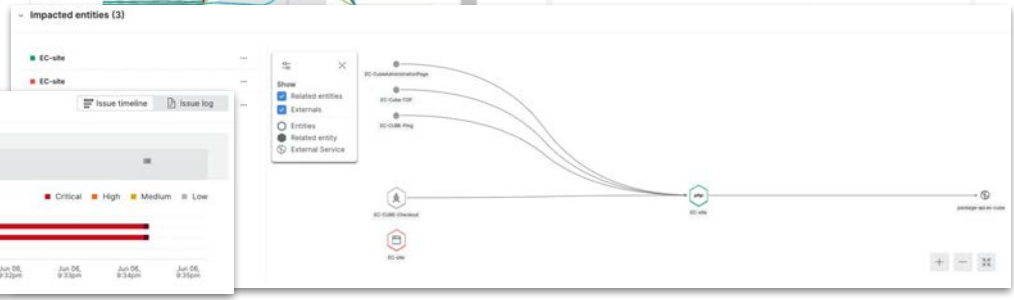
- どのIncidentがまとめられているのか確認することができます

ハンズオン(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

- 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

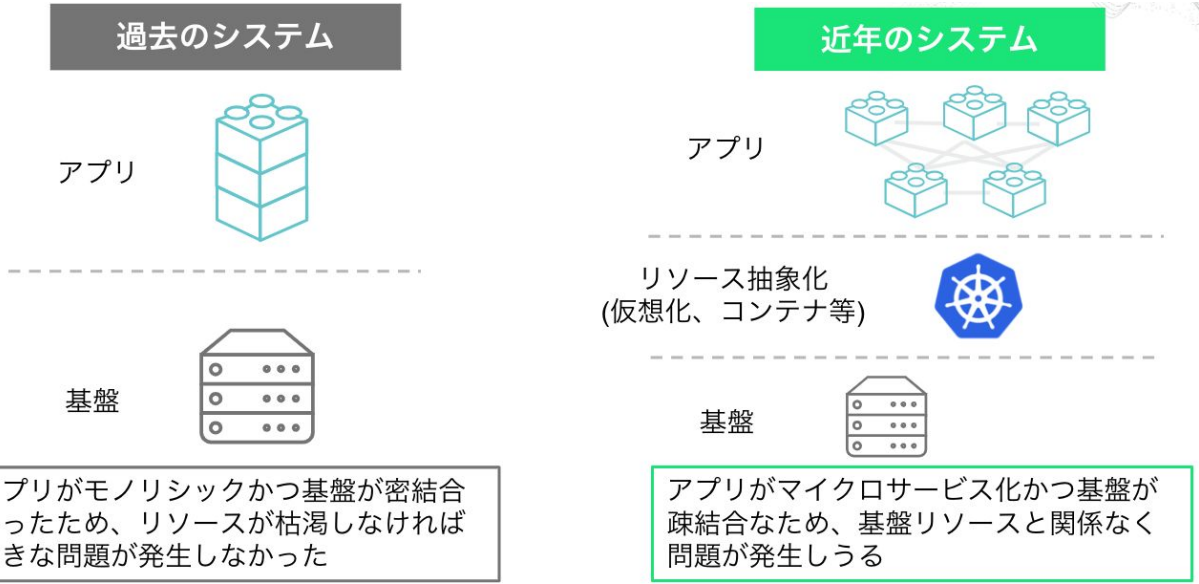
AIOpsとは、IT運用プロセスを自動化するためにビッグデータと機械学習を紐付けたものであり、以下のような機能を含む:

1. 異常検知
2. イベントの相関分析
3. 根本原因分析

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

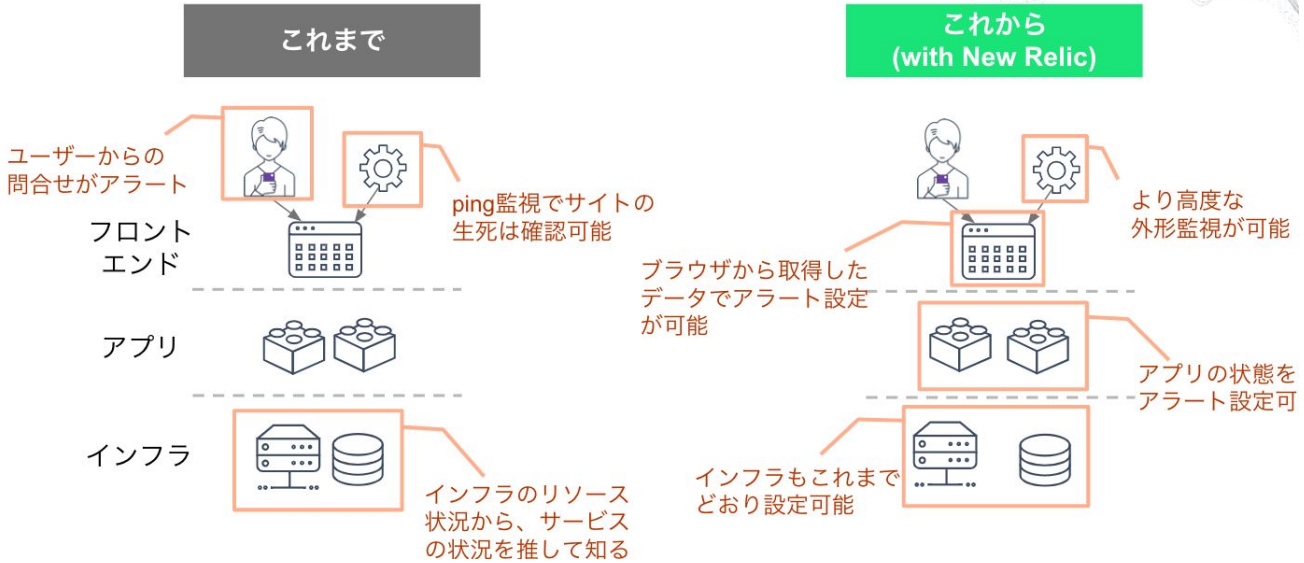
監視対象となるコンポーネントの絶対数が増えると同時に、コンポーネント同士の関連性がより複雑に



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

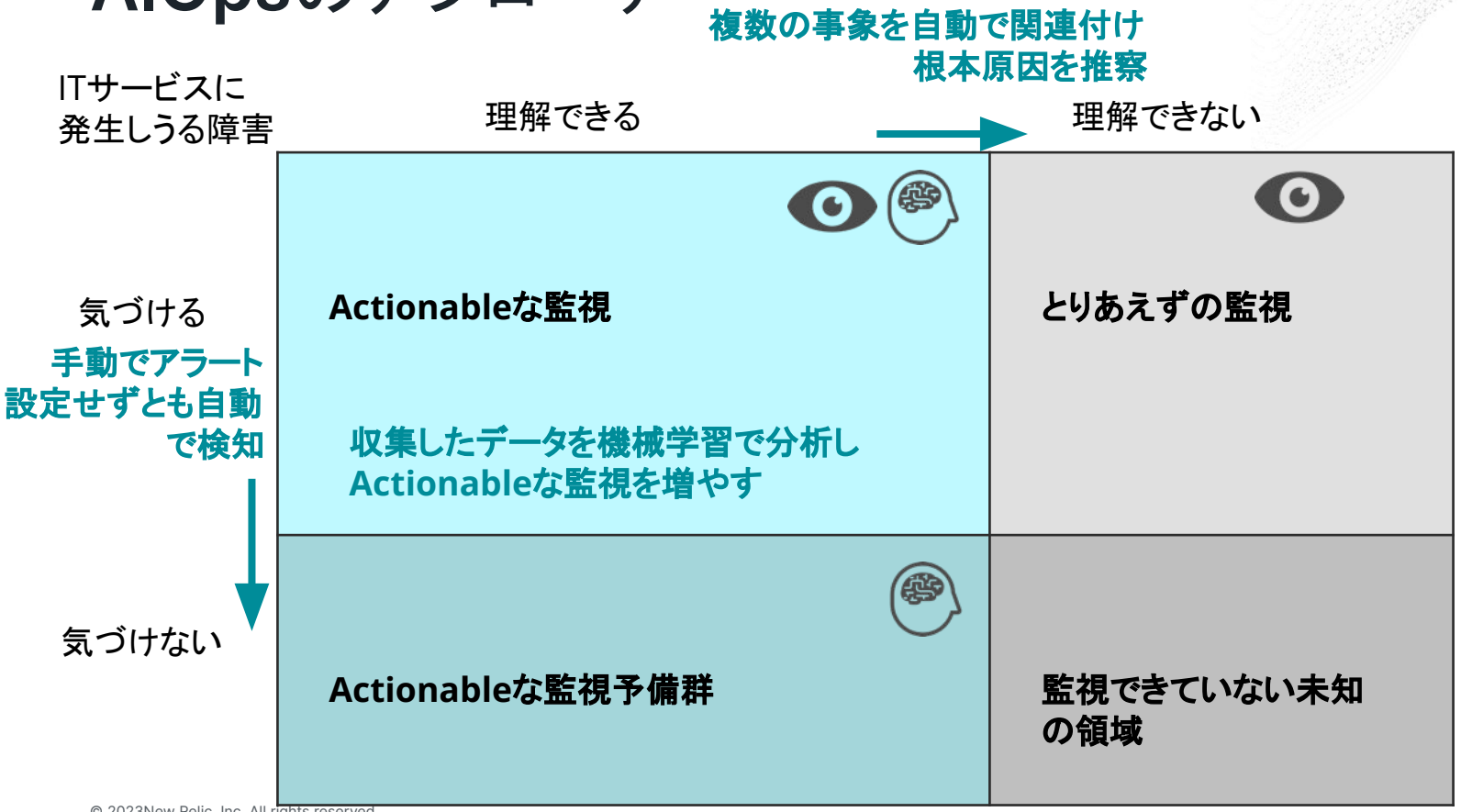
とりあえずの監視

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

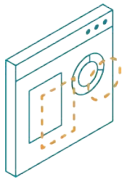
[解決するAIOpsの機能]
- 異常検知

手動でアラート設定せずとも自動で検知

Alert coverage gaps (BETA)

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

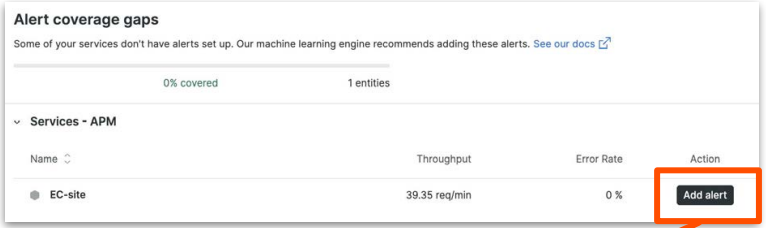
[解決するAIOpsの機能]
- イベントの相関分析
- 根本原因分析



複数の事象を自動で関連付け、根本原因を推察

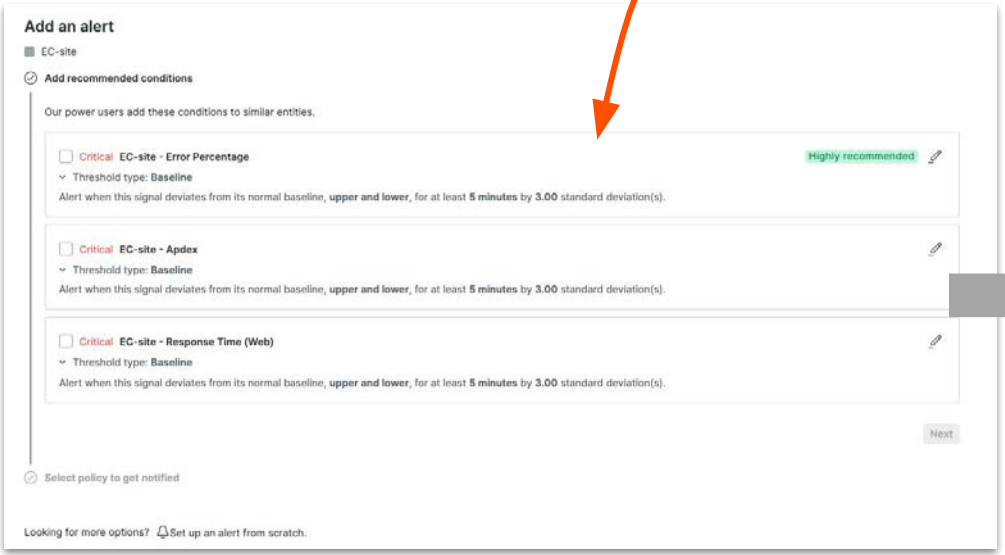
Anomaly Detection

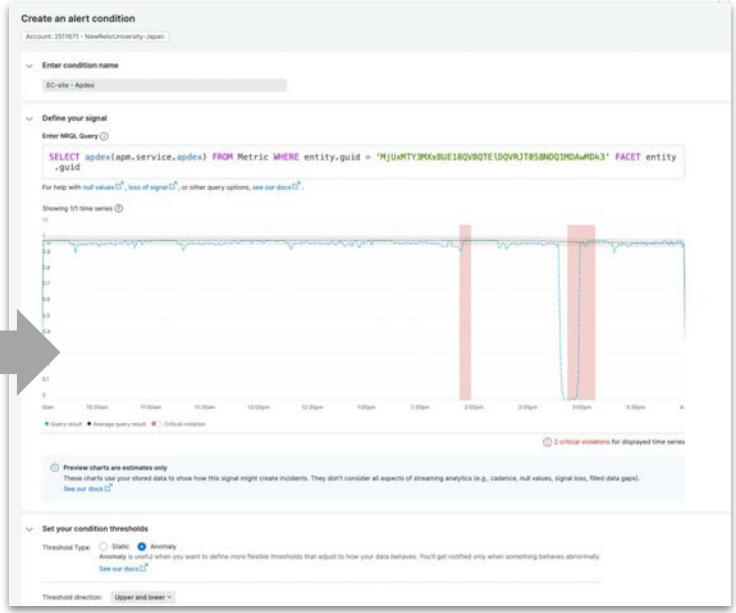
機能紹介: Alert coverage gaps



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。

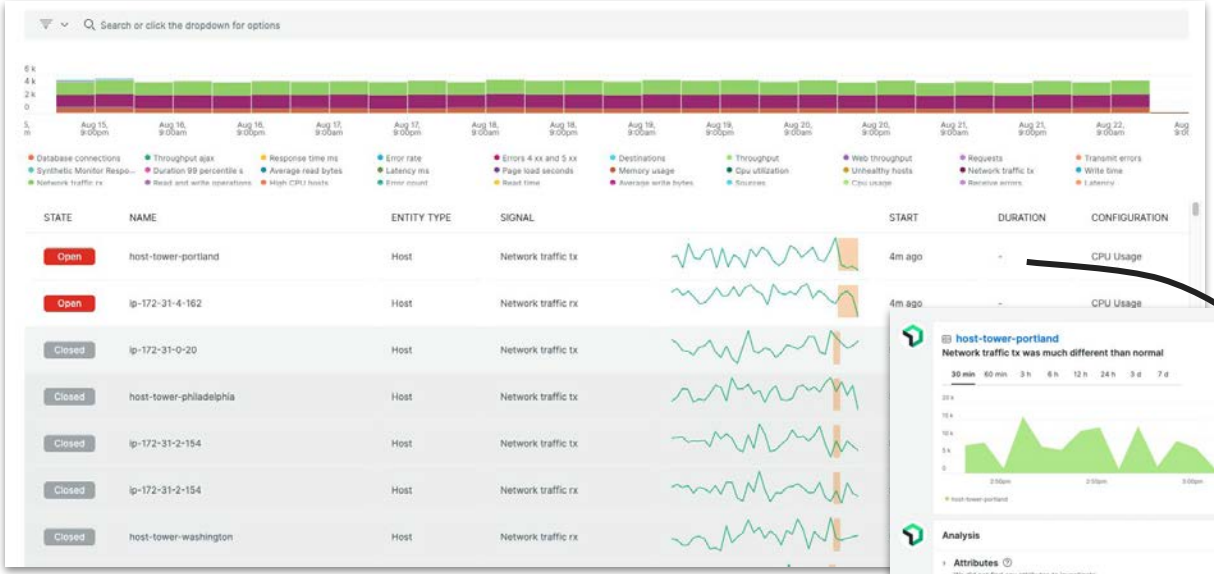




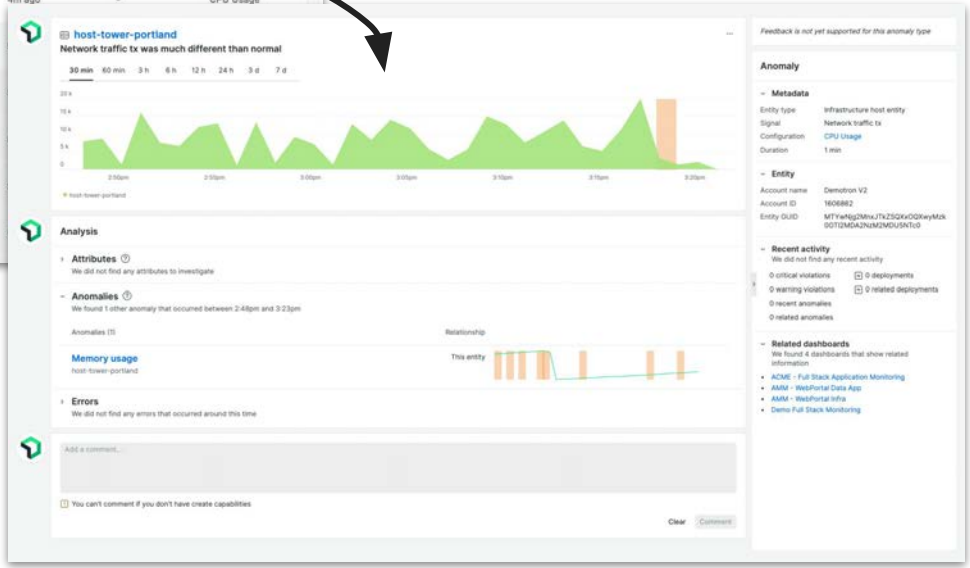
Alerts & AI -> Alert coverage gaps

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、他の監視entityのサポートを今後計画しています。



Alerts & AI -> Issues & activity -> Anomalies

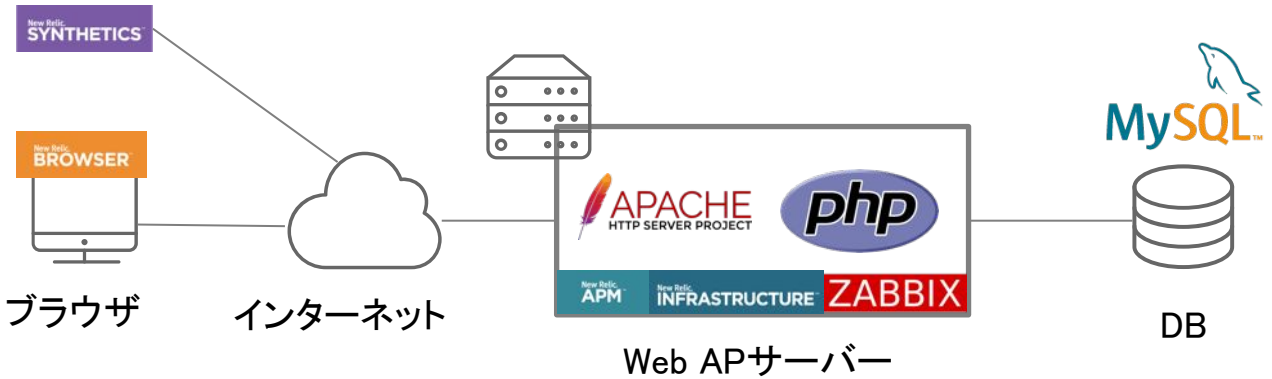
- 発生したAnomalyの1つを選択し、詳細を確認する

ハンズオン(3)
AIOpsを使った異常検知と原因分析(応用編)

16:45 - 16:55 (10min)

今回の環境の監視構成(再掲)

- 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(3)

3-1 様々なソースのアラートをまとめる : 通常のアラート

[目的]
アラートを相関分析できるよう、複数ソースのアラートを New RelicのAIOpsに取り込みましょう

- 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)

3-2 様々なソースのアラートをまとめる : 異常検知情報の接続

[目的]
アラートを相関分析できるよう、複数ソースのアラートを New RelicのAIOpsに取り込みましょう

- 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 NRU(2511671)、アプリはEC-site、No notification、Correlate with other alerts をオンにして[Save configuration]

ハンズオン(3)

3-3 様々なソースのアラートをまとめる : [参考情報] Zabbixからのアラート

[目的]
アラートを相関分析できるよう、複数ソースのアラートを New RelicのAIOpsに取り込みましょう

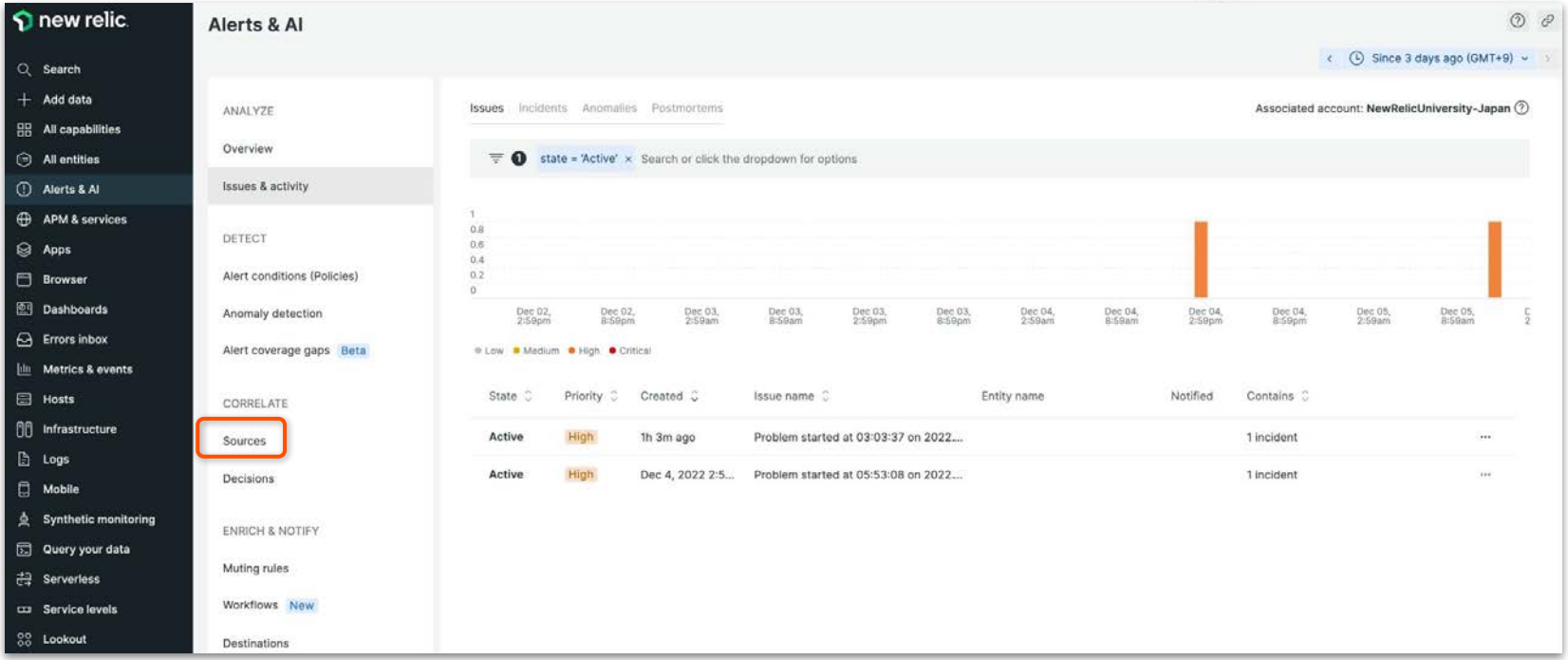
- Zabbix 5.0 以降で追加されたwebhook メディアタイプによって、ZabbixのAlertをNew Relci Incident Intelligence APIに通知することができます。
- Zabbix のMacroから値を受け取り、New Relic APIエンドポイントURLとInsights Insert Keyを利用してJavaScript から送信することができます。

手順・解説

使用アカウント：NewRelic.kk
（ログイン先選択はこちら参照）

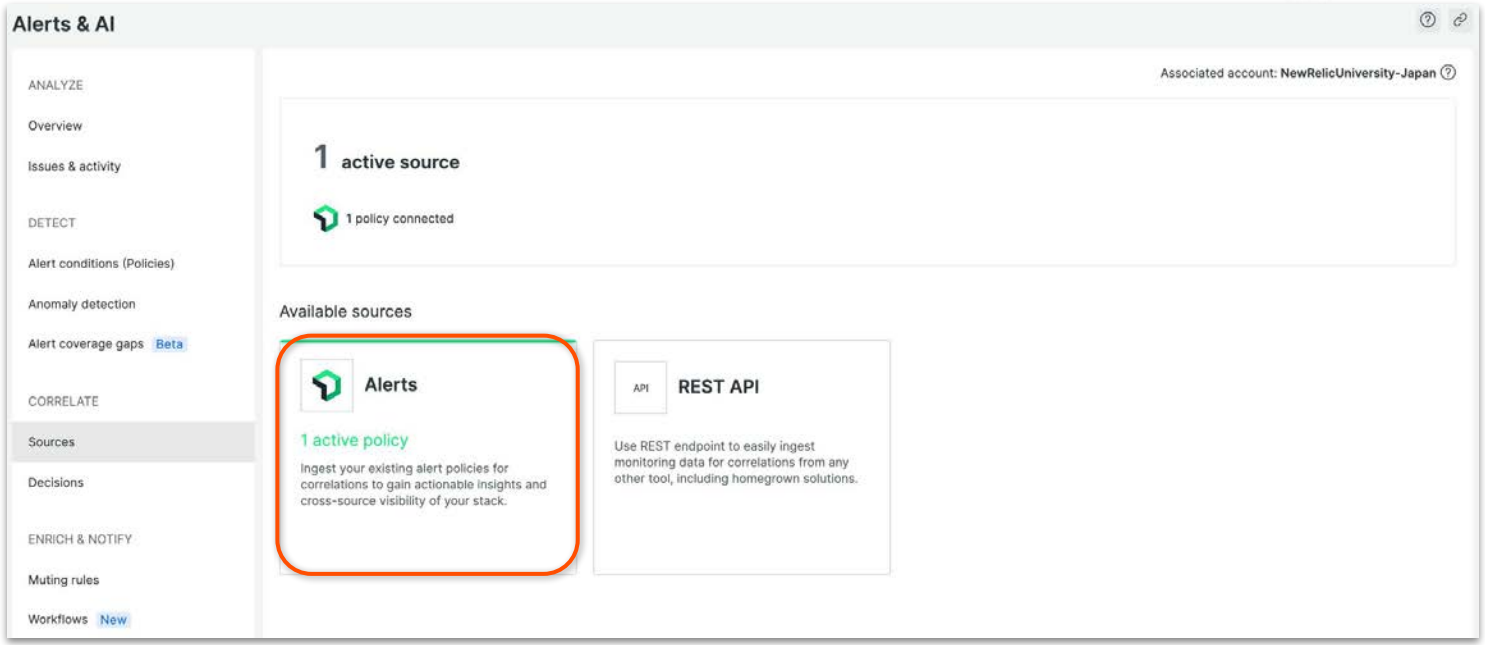
ハンズオン(3)様々なソースのアラートをまとめる(1)

- 「Sources」をクリックします。



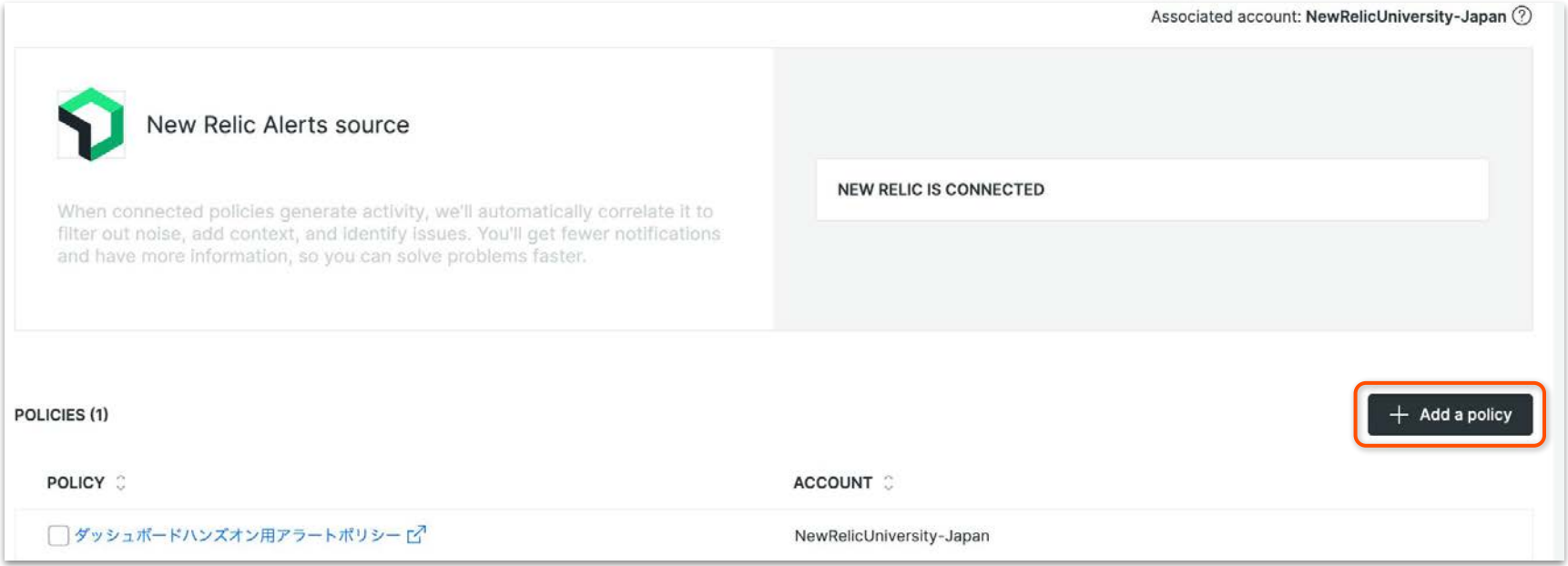
ハンズオン(3-1)様々なソースのアラートをまとめる

- 「Alerts」カードをクリックします。



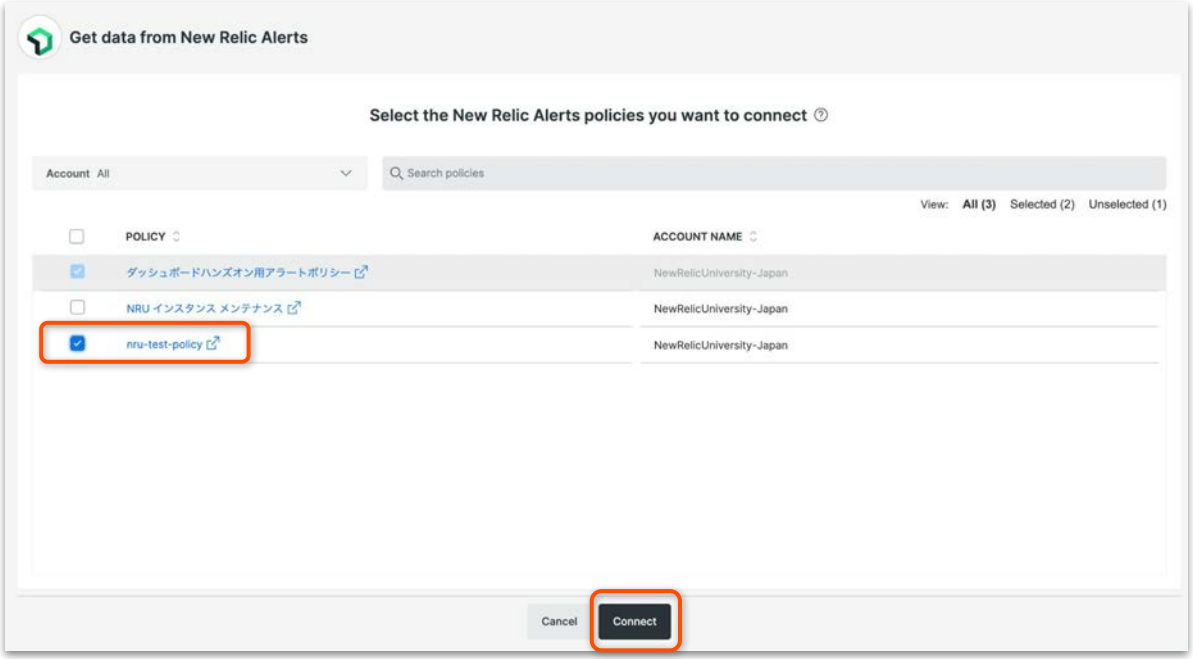
ハンズオン(3-1)様々なソースのアラートをまとめる

- 「＋ Add a policy」ボタンをクリックします。



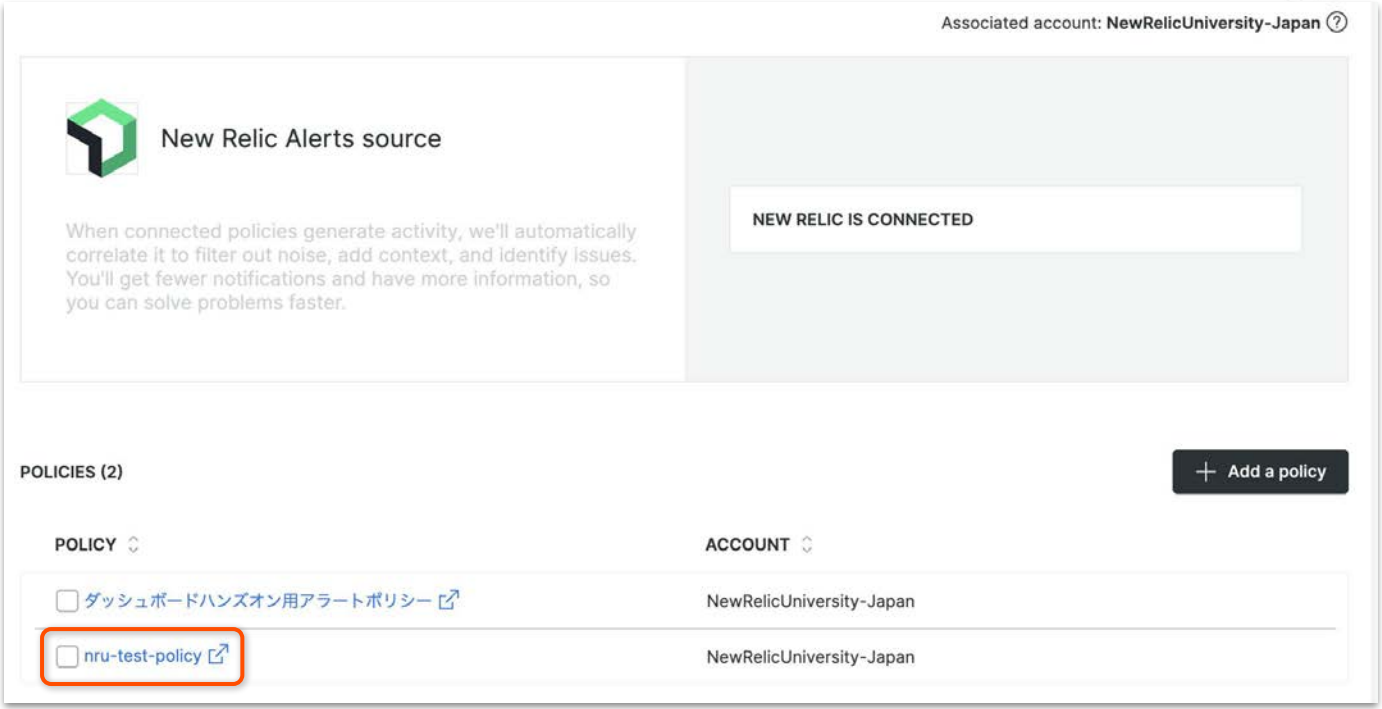
ハンズオン(3-1)様々なソースのアラートをまとめる

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



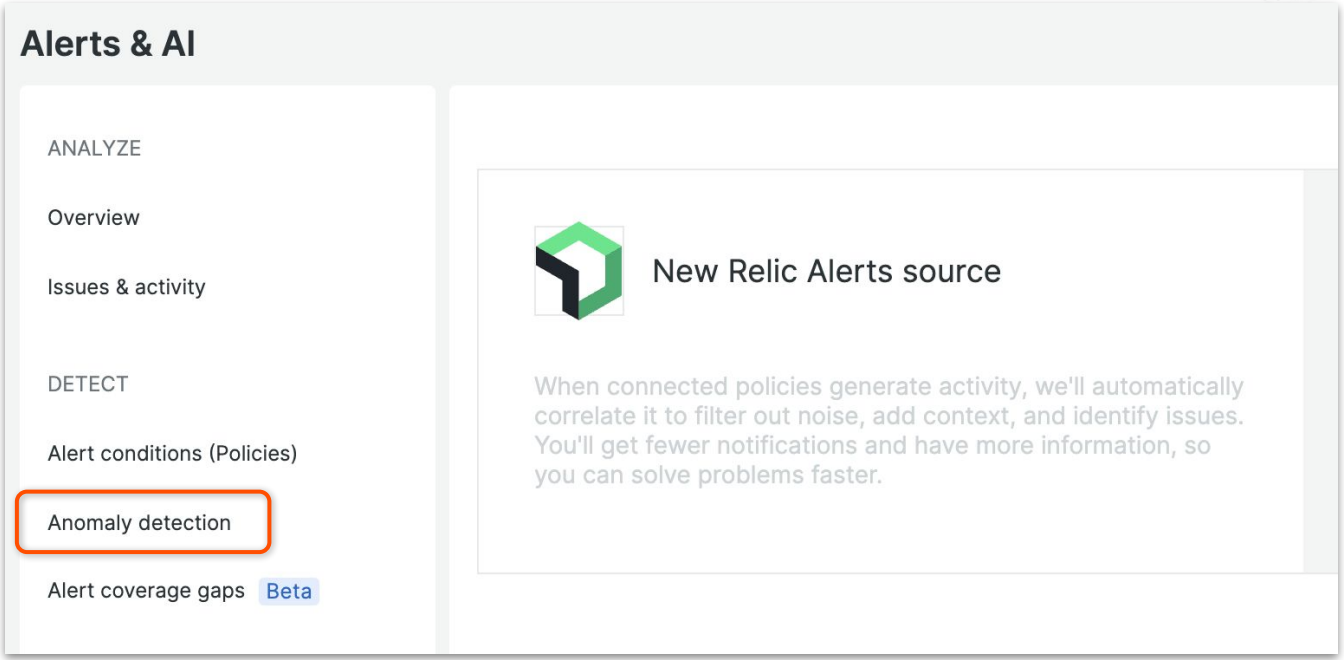
ハンズオン(3-1)様々なソースのアラートをまとめる

- 自分のPolicyが追加された事を確認します。



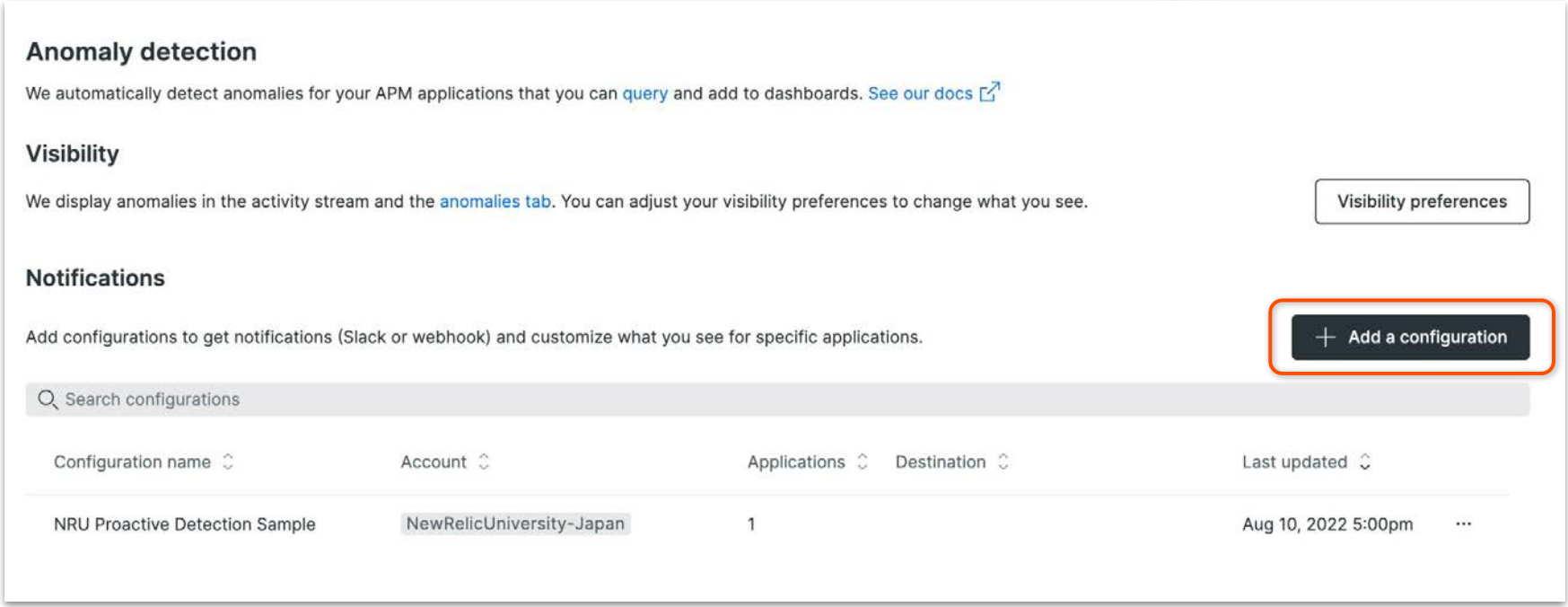
ハンズオン(3-2)様々なソースのアラートをまとめる

- 「Anomaly detection」をクリックします。



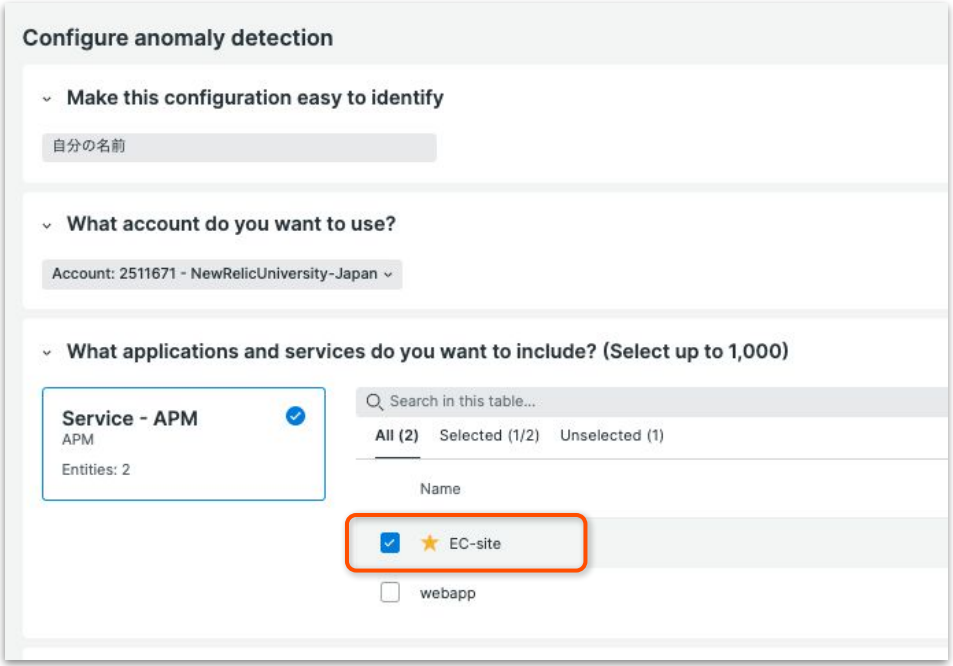
ハンズオン(3-2)様々なソースのアラートをまとめる

- 「＋ Add a Configuration」ボタンをクリックします。



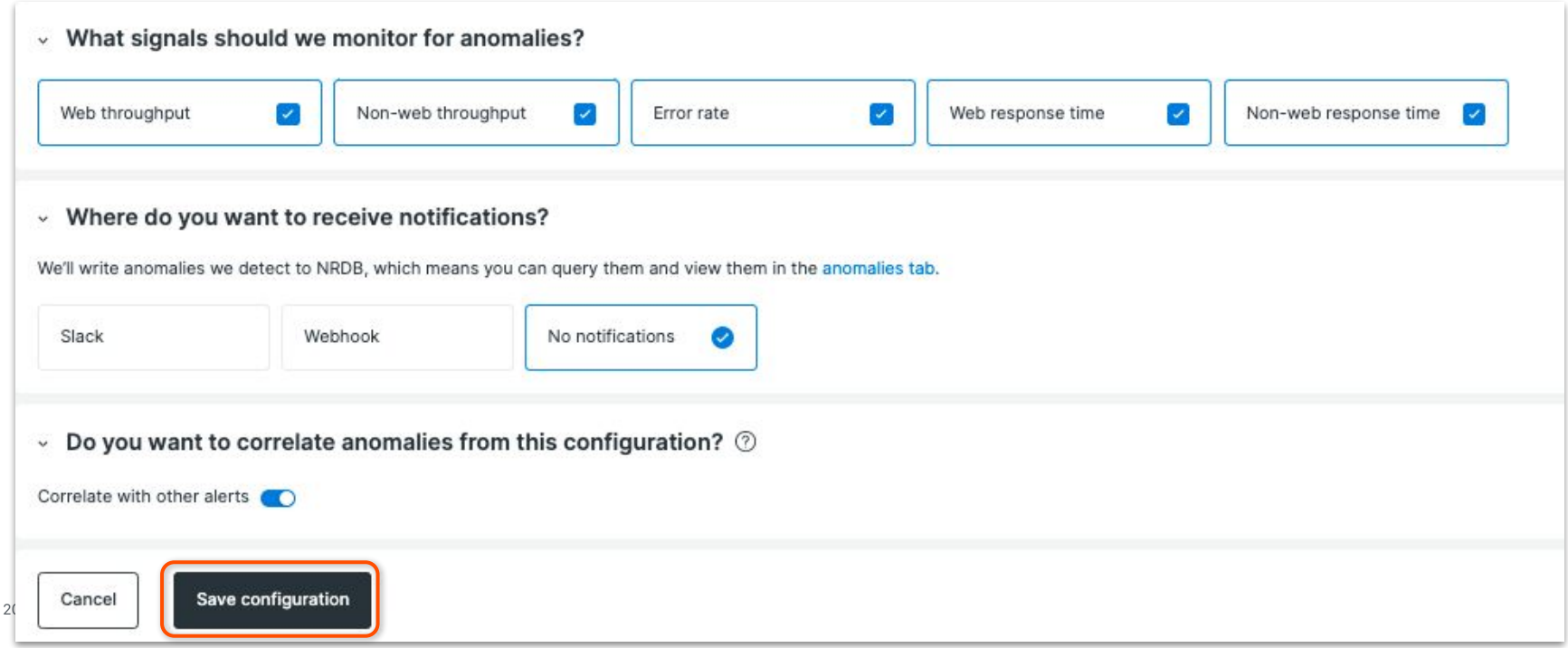
ハンズオン(3-2)様々なソースのアラートをまとめる

- 「設定名」に自分の名前を付け、Accountは「NewRelciUniversity-Japan」を選択します。
- 「EC-site」にチェックを入れます。



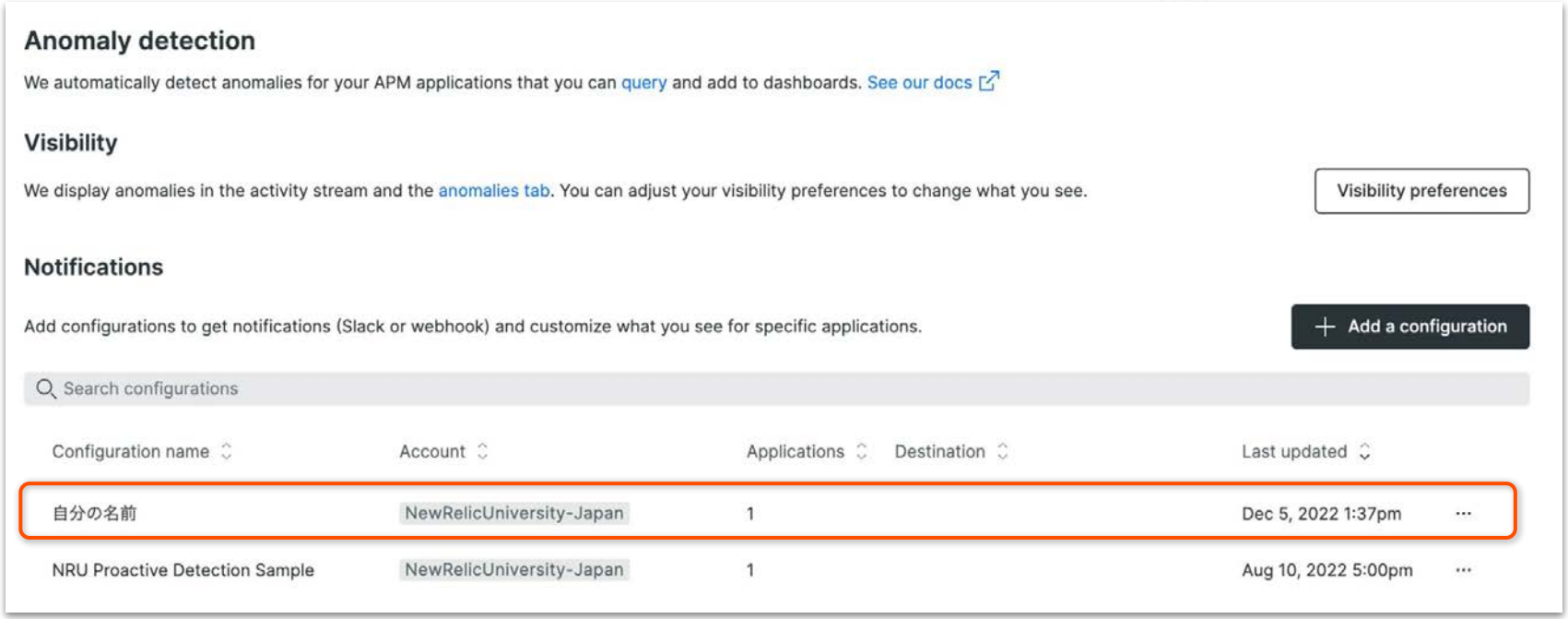
ハンズオン(3-2)様々なソースのアラートをまとめる

- 5カテゴリ全てにチェックをつけ、「 No notifications」を選択します。
- 「Correlate with other alerts」を有効にして「Save configuration」をクリックします。



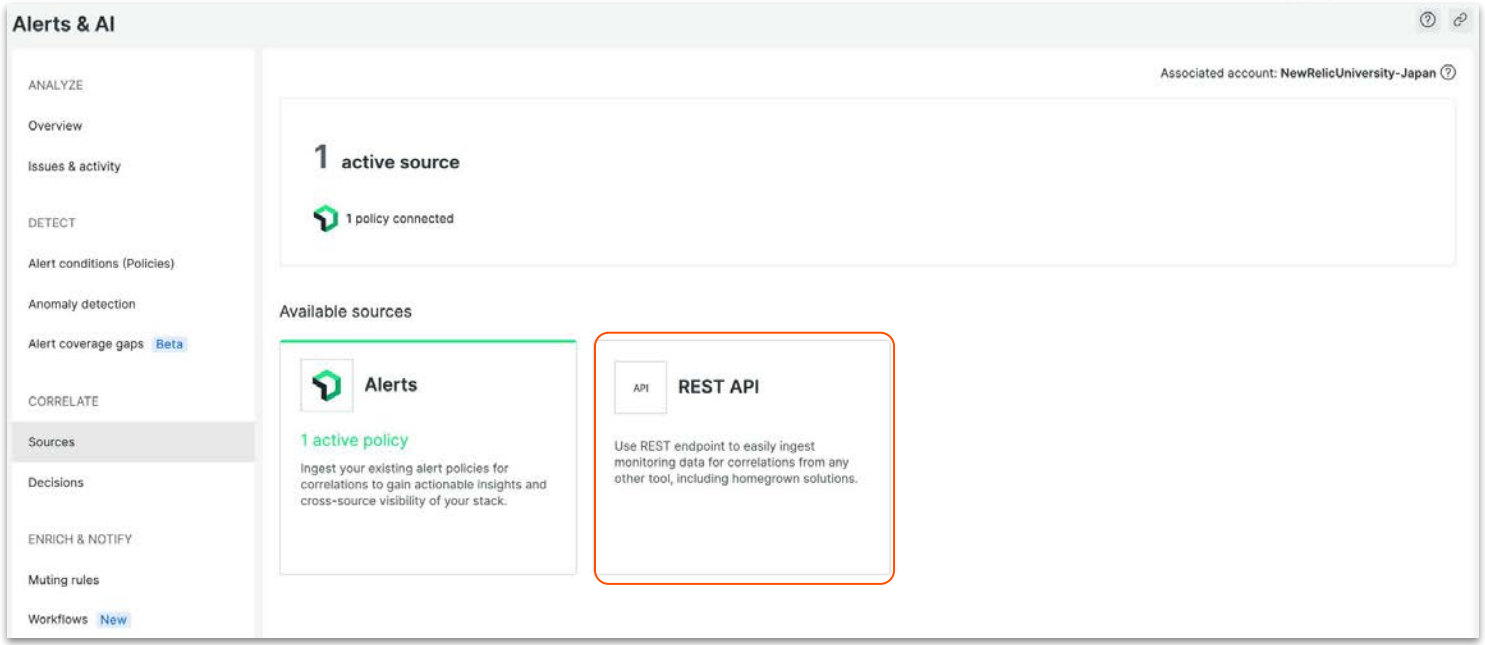
ハンズオン(3-2)様々なソースのアラートをまとめる

- 設定が追加されたことを確認します。



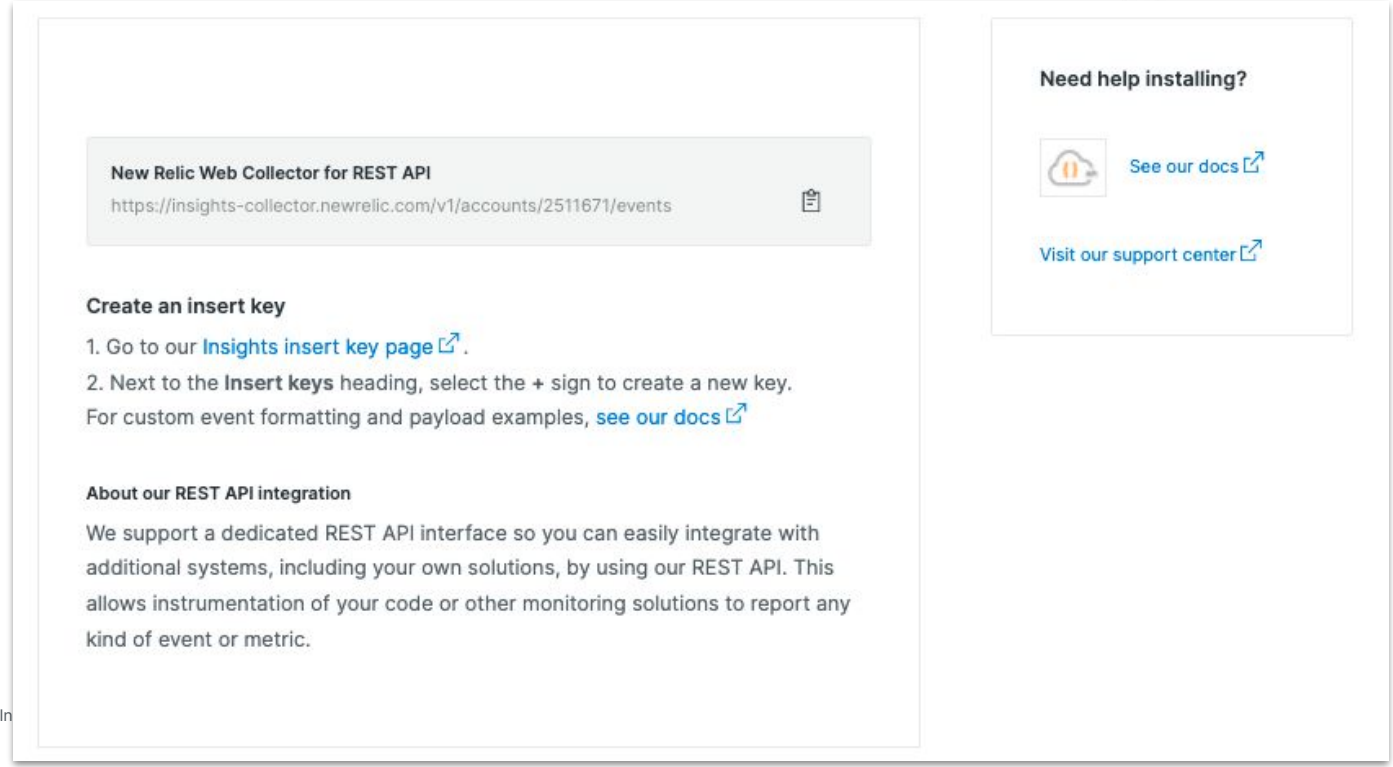
参考 Zabbixの連携

- ZabbixからIncident Intelligence への連携にはREST APIを利用しています。



参考 Zabbixの連携

- 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

- Incident Intelligence 用メディアタイプは現在プロトタイプです。

参考 Zabbixの連携

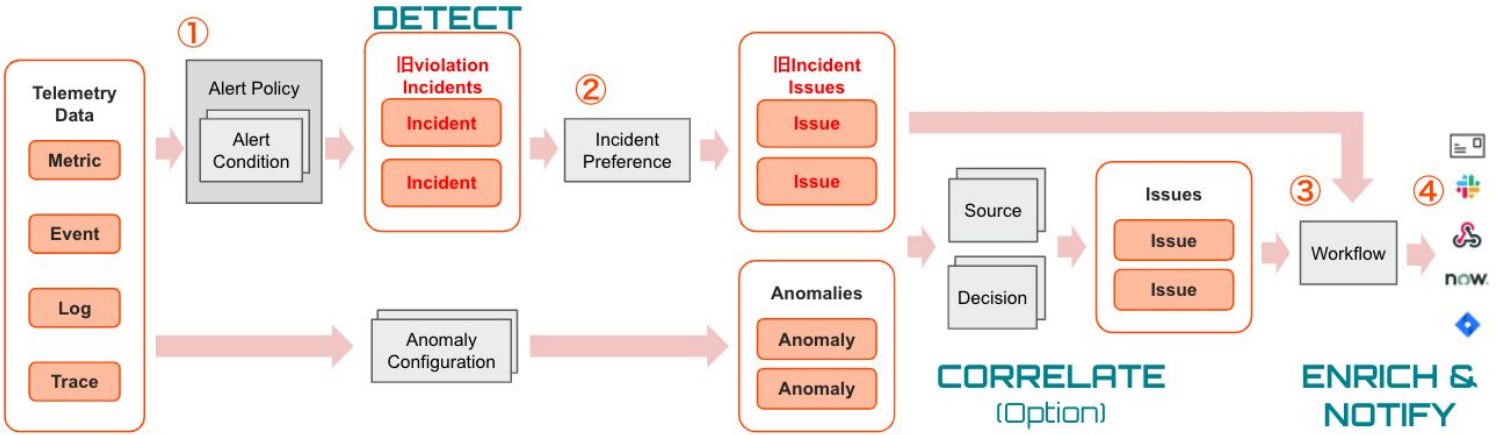
- Zabbixのトリガーアクションによってメディアタイプを呼び出して利用しています。

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**
  - インフラ監視はアンチパターン
- **New Relicのアラート構造と設定方法を理解しよう**



- **New Relicを使ってAIOpsを実現しよう**
  - Anomaly DetectionとCorrelation、Lookoutを使った異常検知

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.