New Relic

New Relic University

NRU 304 New Relic ハンズオン : Alert & AIOps

Taku Oguchi

Mar 17, 2022

Taku Oguchi

Solution Consultant
New Relic 株式会社

Enterprise Mobility Management and App Development
Independent Consultant

Senior Producer
Tigerspike

Solution Expert (Enterprise Sales)
Apple · Full-time

System Engineer (Financials Vertical / Infrastructure)
Hitachi · Full-time

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

https://newrelic.co.jp/webinar/nrb-newrelic-essentials

・ダッシュボードワークショップ (NRQL入門編に相当)

https://newrelic.co.jp/resources/webinars/nru-201

アジェンダ

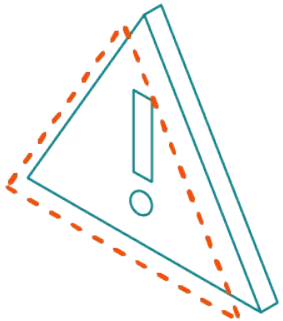
時間(目安)	内容
15:00 – 15:15	座学(1)ユーザー視点のアラート
15:15 – 15:30	座学(2)New Relicのアラート機能
15:30 – 15:55	ハンズオン(1)アラートを作成する
15:55 – 16:10	座学(3)AIOpsの意義
16:10 – 16:25	ハンズオン(2)AIOpsを使った異常検知と原因分析 (前編)
16:25 – 16:35	座学(4)New RelicのAIOps機能
16:35 – 16:50	ハンズオン(3) AIOpsを使った異常検知と原因分析 (後編)
16:50 – 17:00	まとめ、アンケートご記入

New Relic®

ユーザー視点のアラート

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

重要なのは、”**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**”を設定すること

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

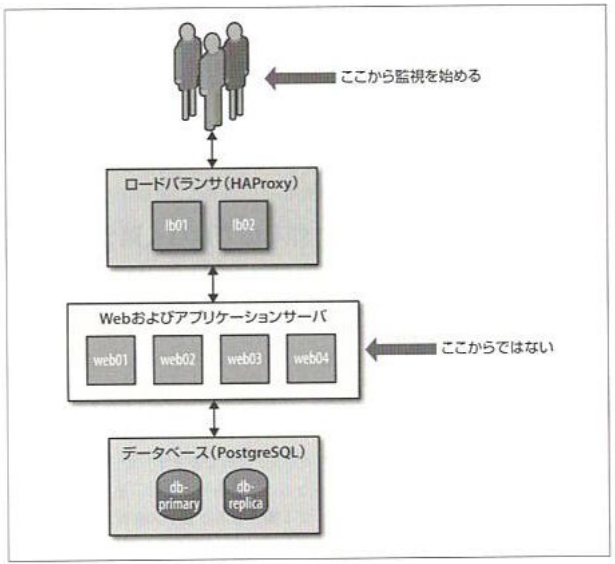


図2-1　できるだけユーザに近いところから監視を始める

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。”

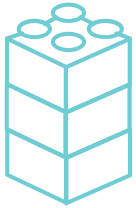
“ユーザー視点優先の監視によって、個別のノードを気にすることから解放されます。”

出典: 入門監視 (Oreilly, 2019)

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

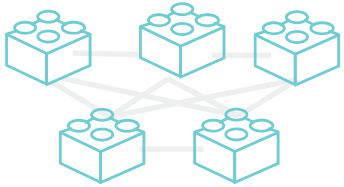


基盤

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

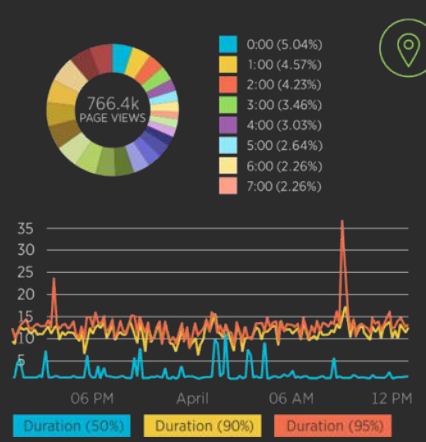


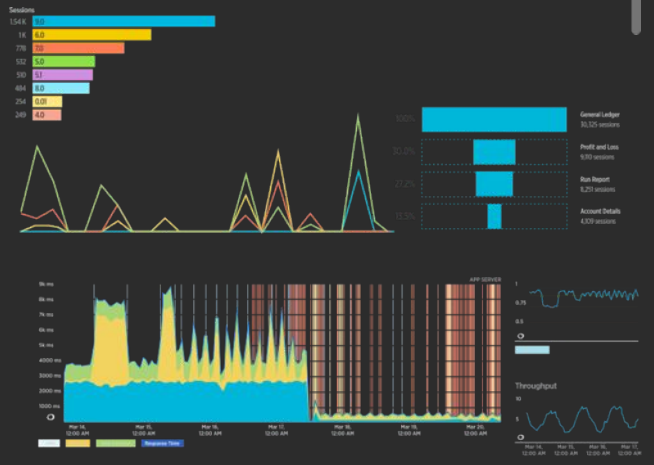
リソース抽象化
(仮想化、コンテナ等)

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

今のシステムに合わせたアラート変革を！



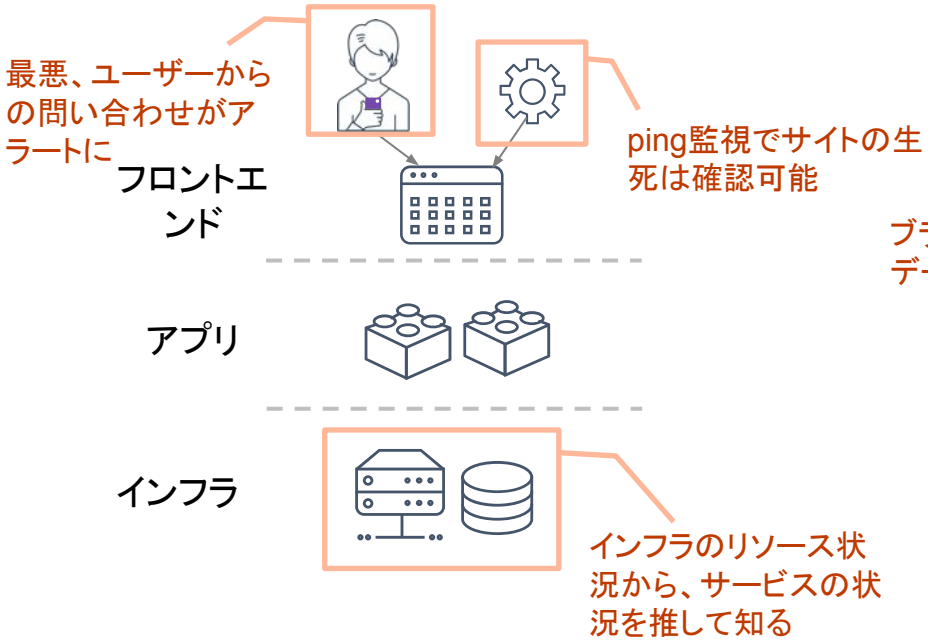


New Relic を使えば簡単に始められます

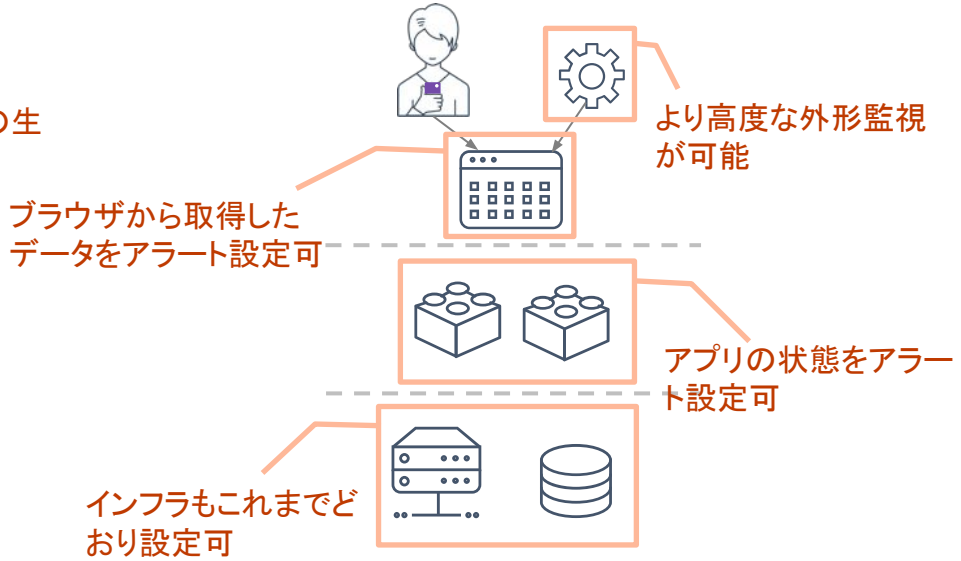
New Relic.

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	サイトがエラーを返す	サイトの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

New Relic®

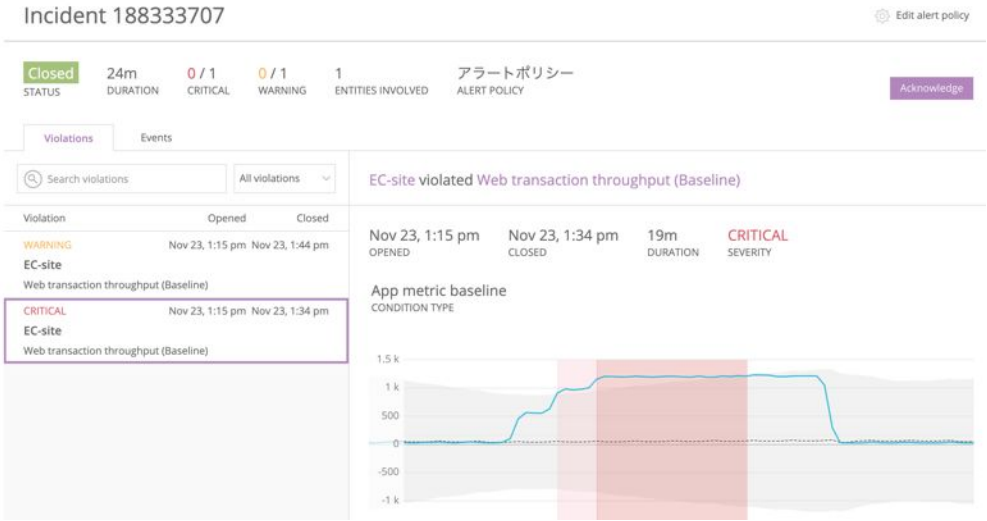
New Relicの
アラート機能

New Relic のアラート機能

New Relicが収集しているありとあらゆるデータを使って、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

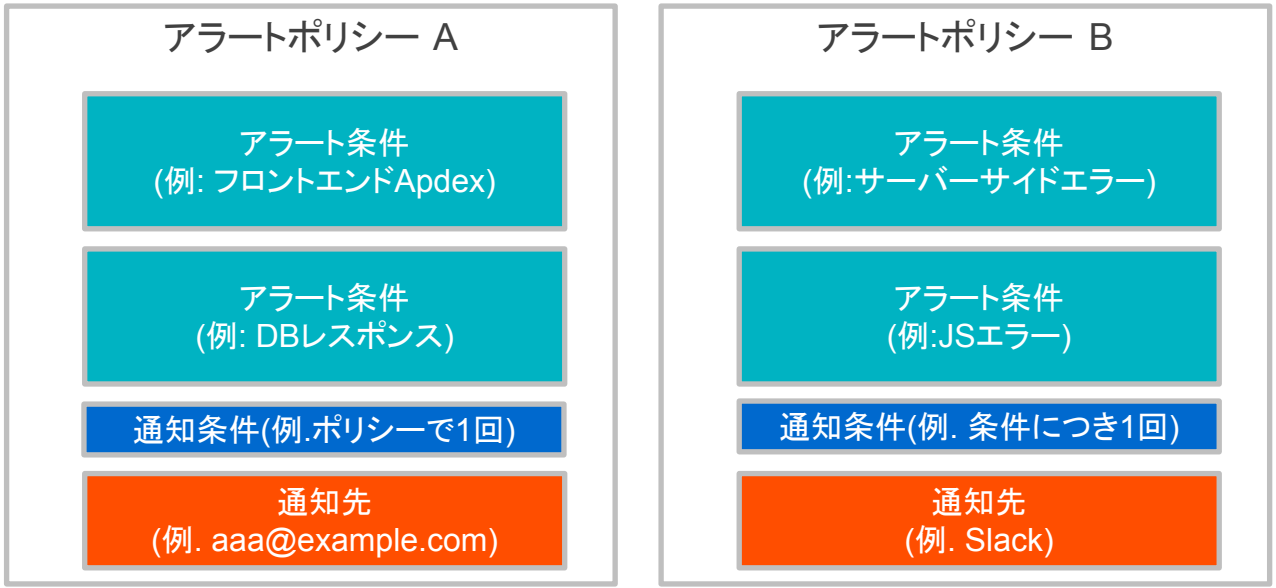
※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説していきます



New Relicのアラート構造を理解する

New Relic のアラートは、アラートポリシーという器に以下の要素を内包した構造となっている

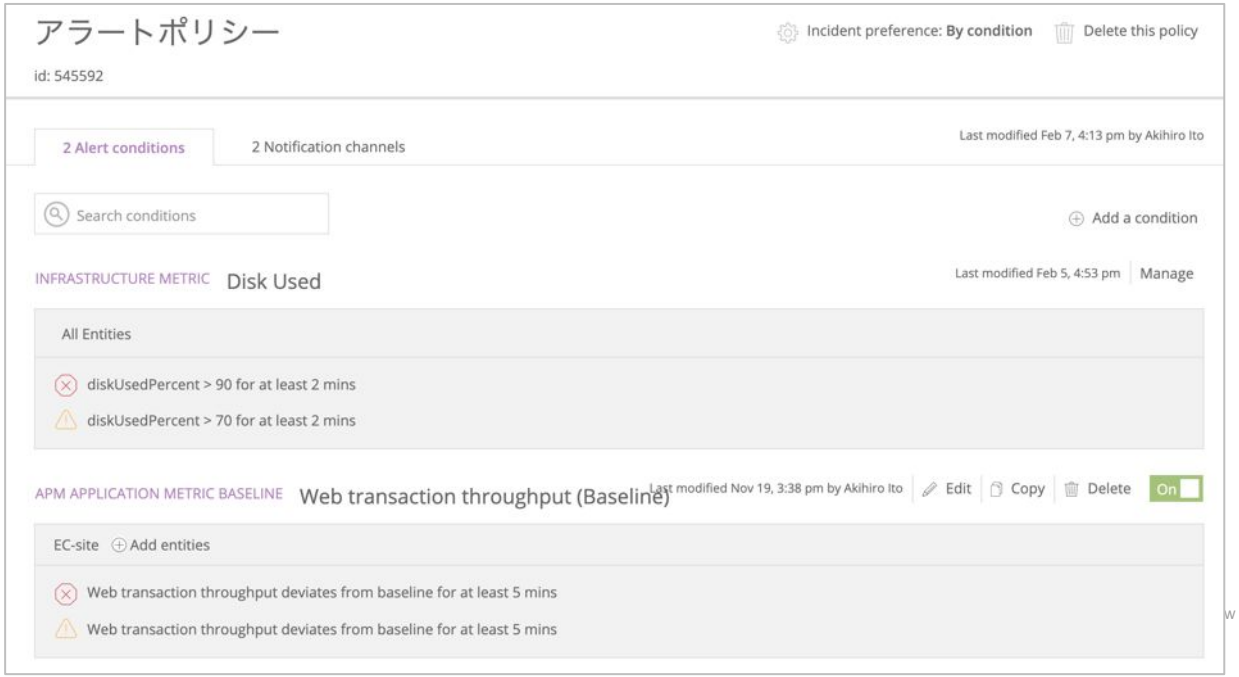
- アラート条件
- 通知条件
- 通知先



New Relic アラートの構成要素①アラートポリシー

アラートポリシーは、複数のアラート条件を内包し、送信先を制御できる機能

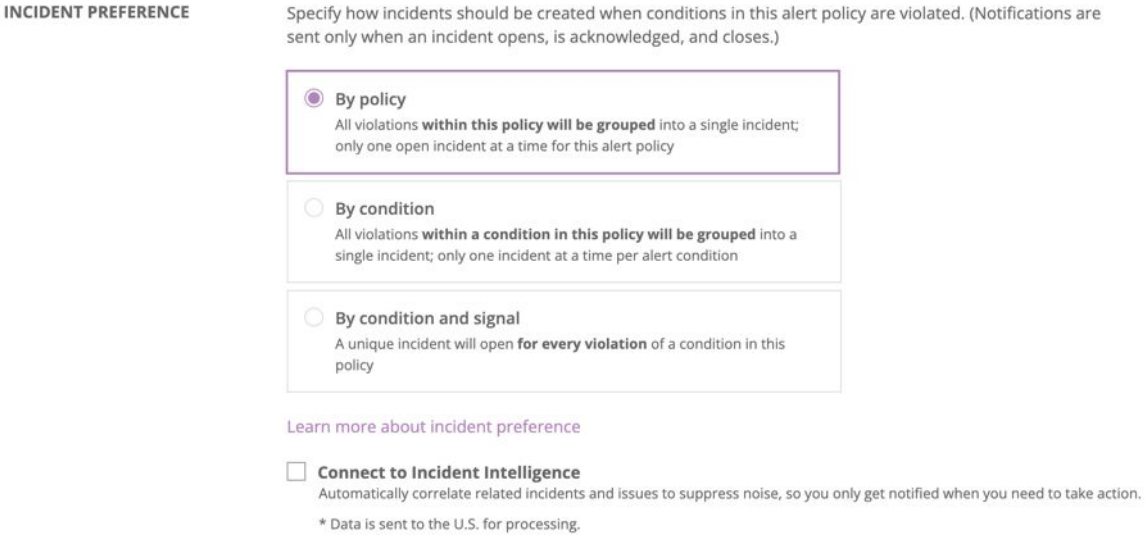
通常、送信先やアラートの目的別にポリシーを分けることが多い



New Relic アラートの構成要素②通知条件

New Relicはアラート条件にしたがって Incidentを起票し通知を行うが、Incidentを起票す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通知条件(続き)

通知条件ごとのIncidentの起票粒度について

例. 1つのアラートポリシーに2つのアラート条件を設定し、すべてのアラート条件が 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	Incidentの起票粒度	この例で起票されるIncident
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通知先

Incident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おり、これをアラートポリシーに登録すると、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

Email

Webhooks

Pager Duty

Slack

OpsGenie

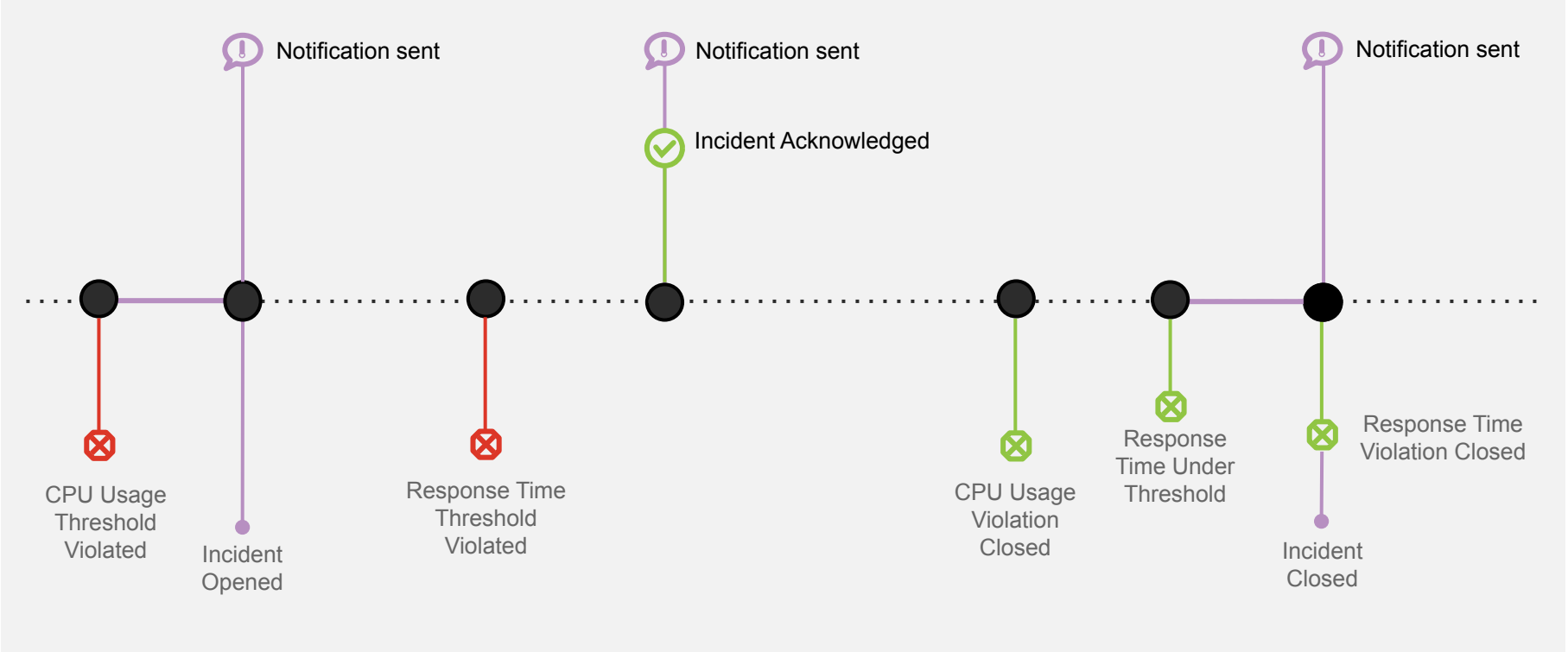
Hipchat

Campfire

VictorOps

補足: Incidentのライフサイクルと通知タイミング

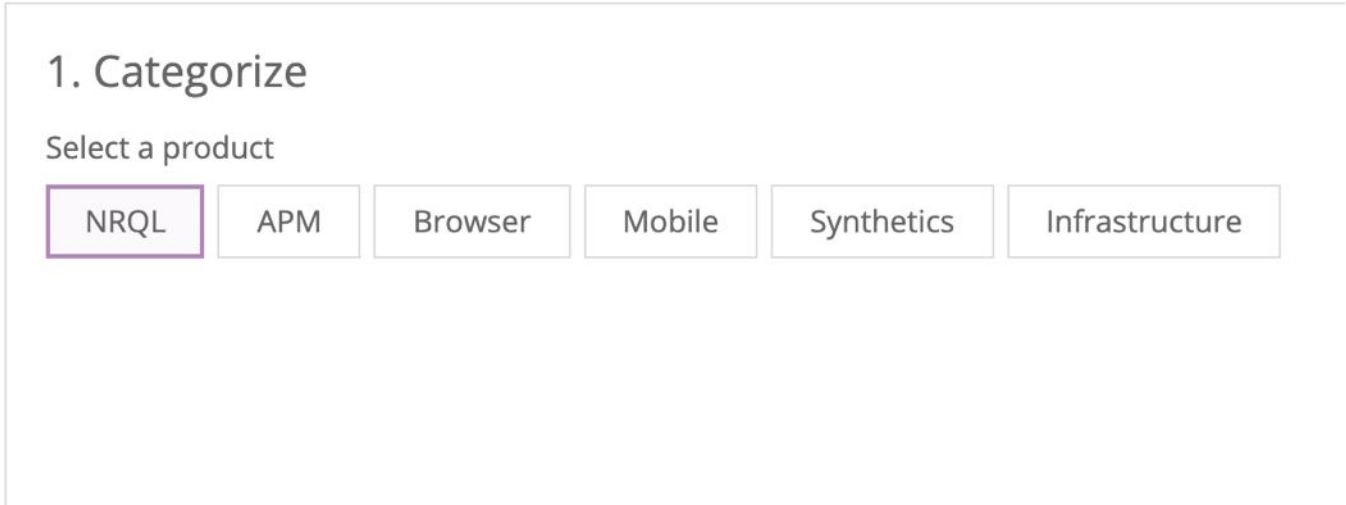
- Incidentの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く



New Relic アラートの構成要素④アラート条件

New Relicが収集しているデータを使って、アラート条件を作成できる

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アラート条件を作成することも可能



New Relic アラートの構成要素④アラート条件(続き)

- アラートのしきい値設定は 2種類から選択可能 (UI上は3種類ありますが 1つは廃止予定)

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)	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④アラート条件(続き)

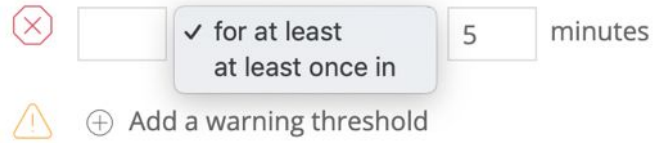
しきい値を超過した場合のアラート発報タイミング

- **For at least xx minutes**

しきい値をxx分継続して超過した場合のみアラートが発報される

- **at least once in xx minutes**

しきい値を1回でも超過した場合にアラートが発報される

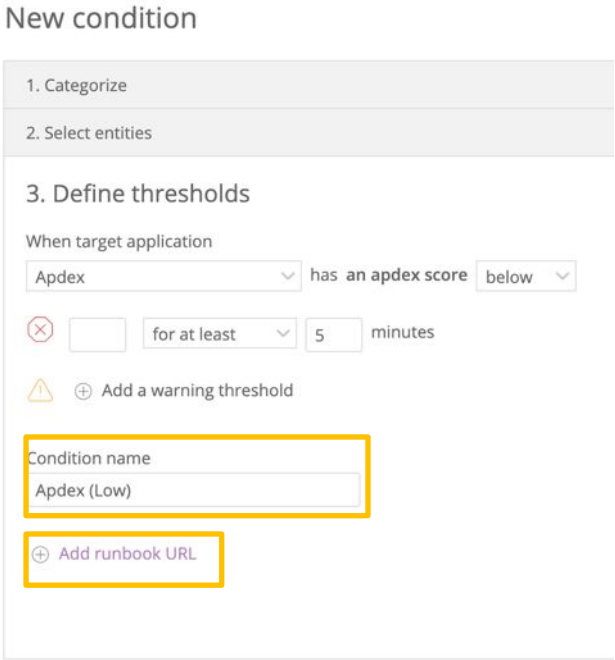


アラート条件はCriticalとWarning(オプション)2種類を作成できるが、通知が飛ぶのは Criticalの場合のみ(WarningはUI上で確認できる)

New Relic アラートの構成要素④アラート条件(続き)

効果的な通知を送るためのプラクティス

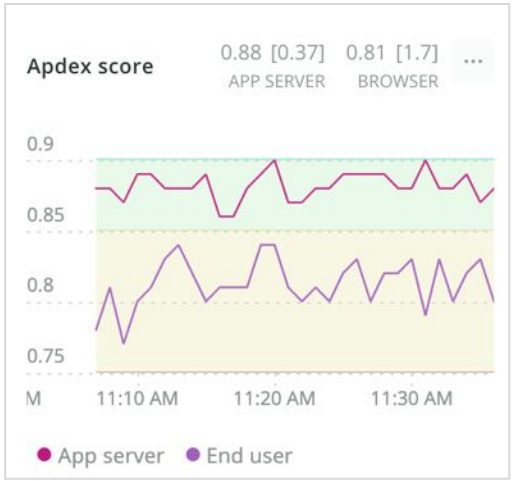
- “Condition name”がそのまま通知の際のタイトルになるため、なるべく何が起こってるかがわかりやすい名前をつける (右画像は悪い例)、日本語可
- Runbook URLを設定することにより、アラート発報時に対応手順へのリンクにすぐにアクセスすることが可能

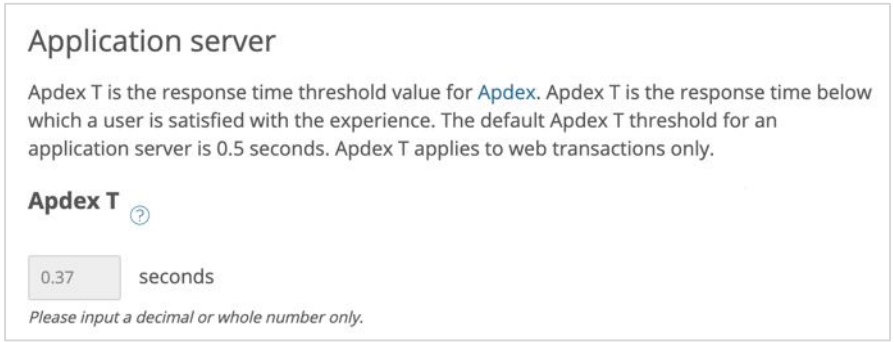


アラートを設定する前にやること

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

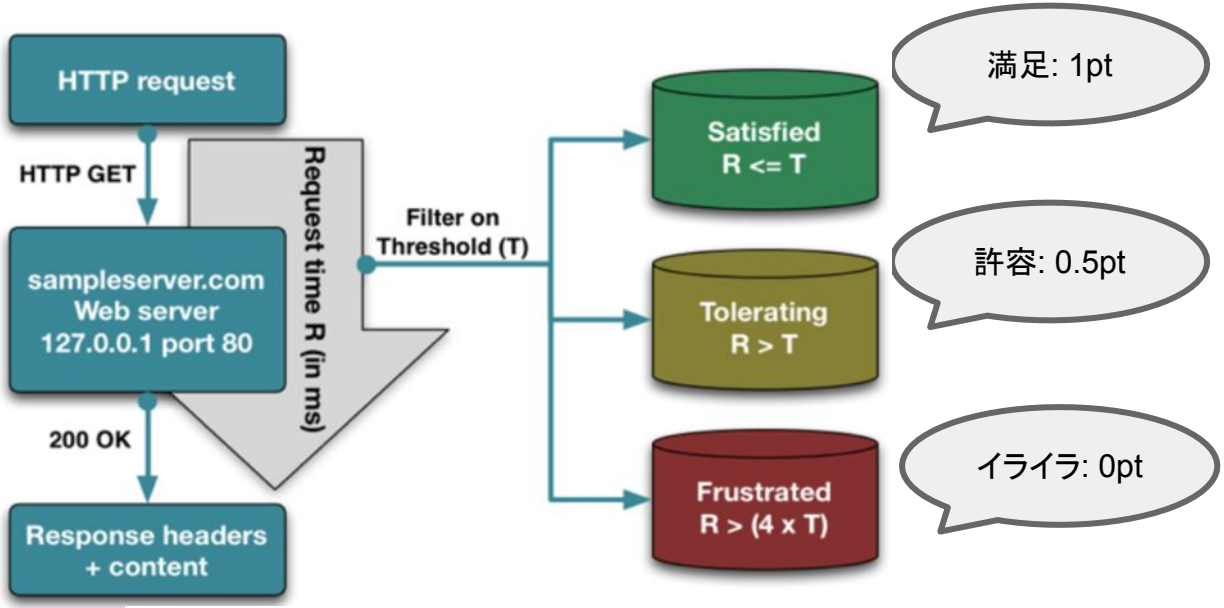




Apdex T値について

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)



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

New Relic®

ハンズオン(1)
アラートを作成する

ハンズオン(1)アラートを作成する

[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)
※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。

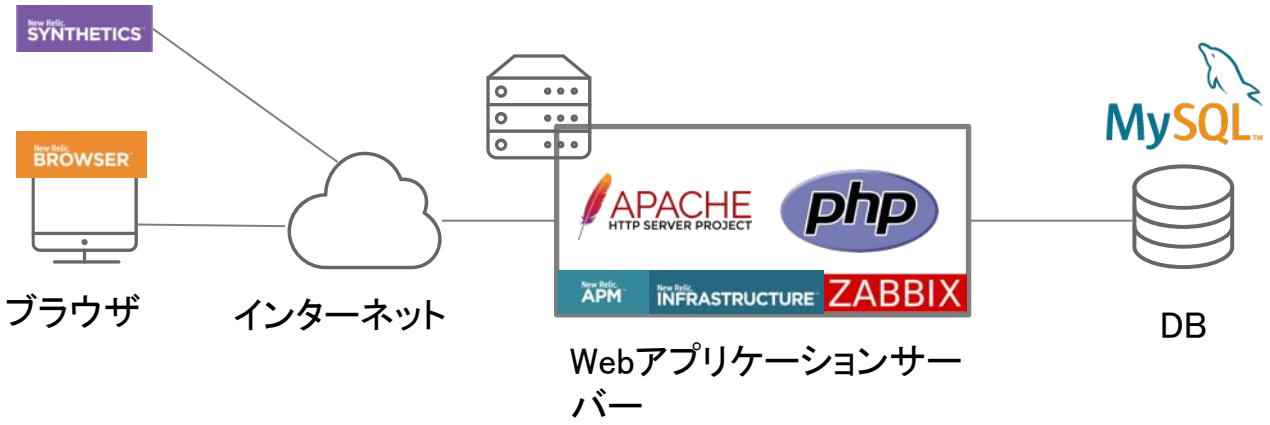
今回監視対象のサイト

[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

今回監視対象の監視構成

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(1)アラートを作成する

[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	サイトがエラーを返す	サイトの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

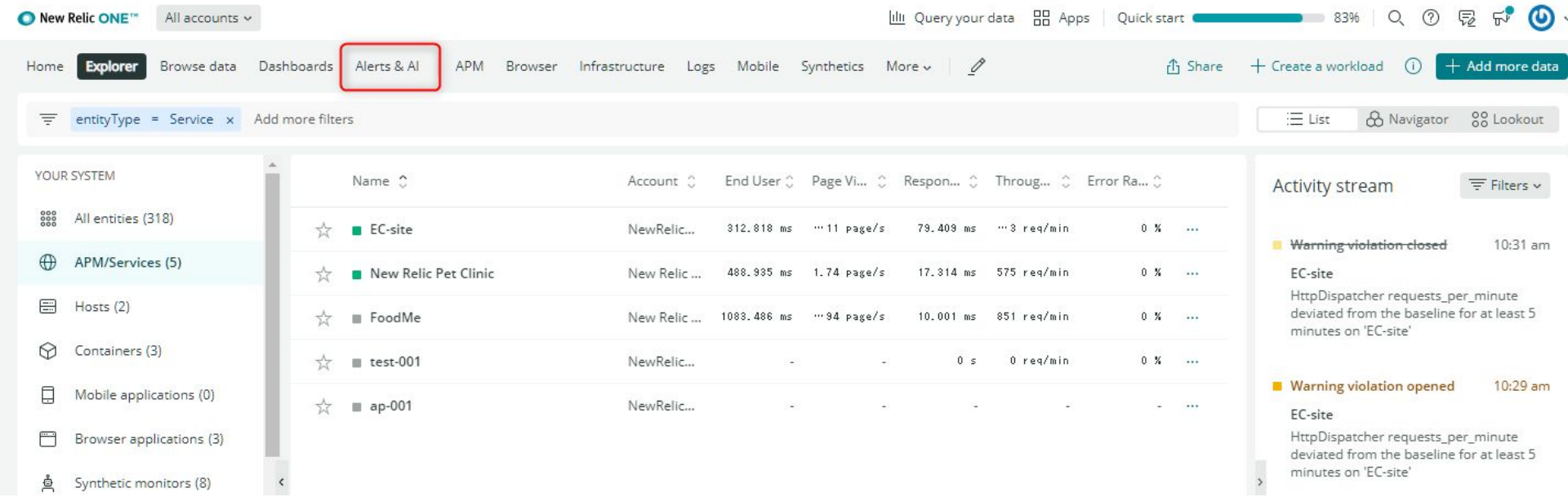
New Relic®

手順・解説

ハンズオン(1)　25min

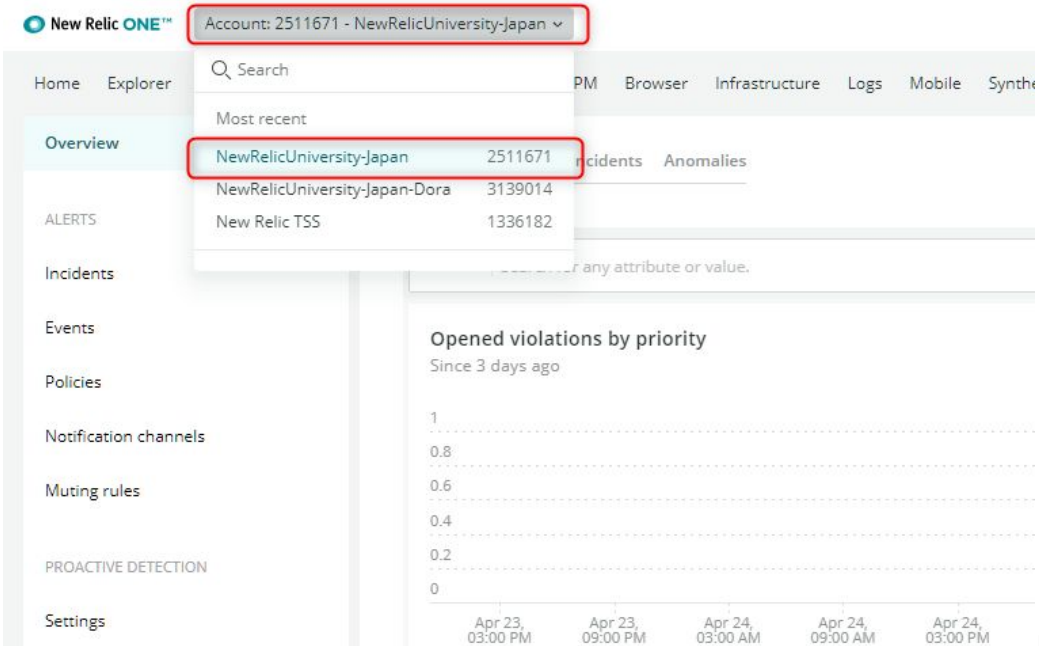
ハンズオン(1)アラートを作成する

- Alert & AI メニューを開きます。



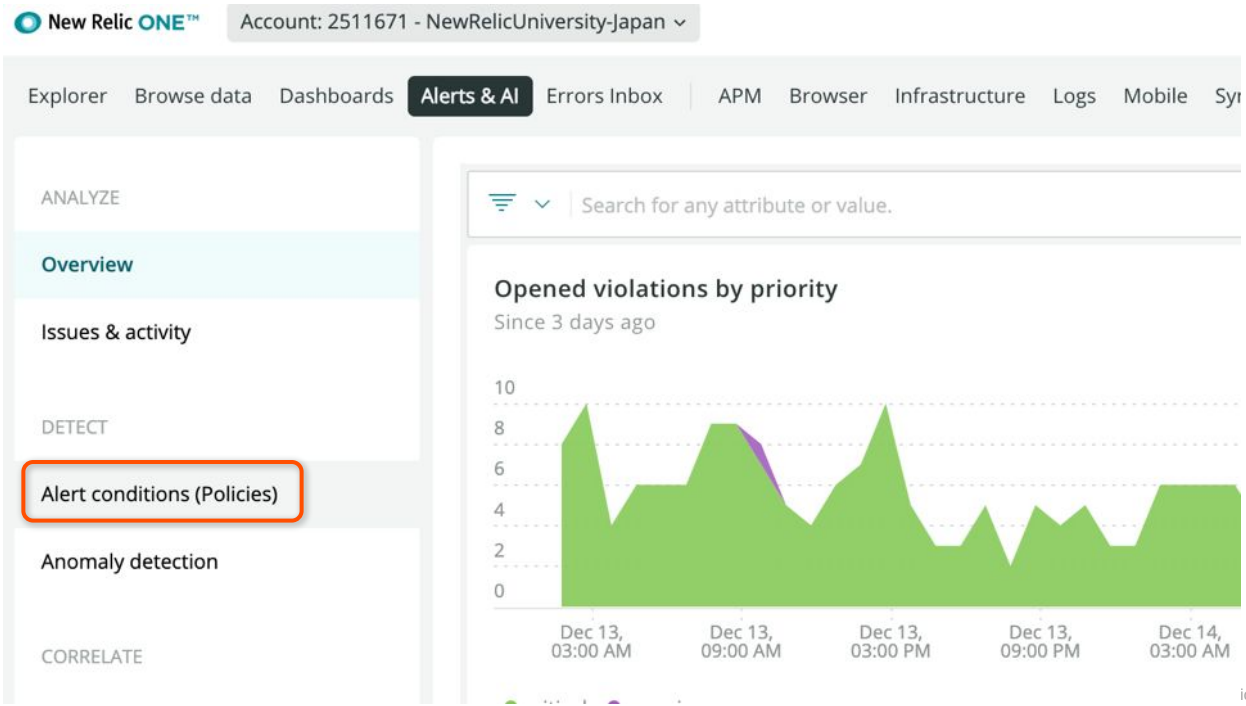
ハンズオン(1)アラートを作成する

- ハンズオンAccountでは複数のNew Relic Accountが参照できます。「ID:2511671 NewRelicUniversity-Japan」のAccountを選択してください。



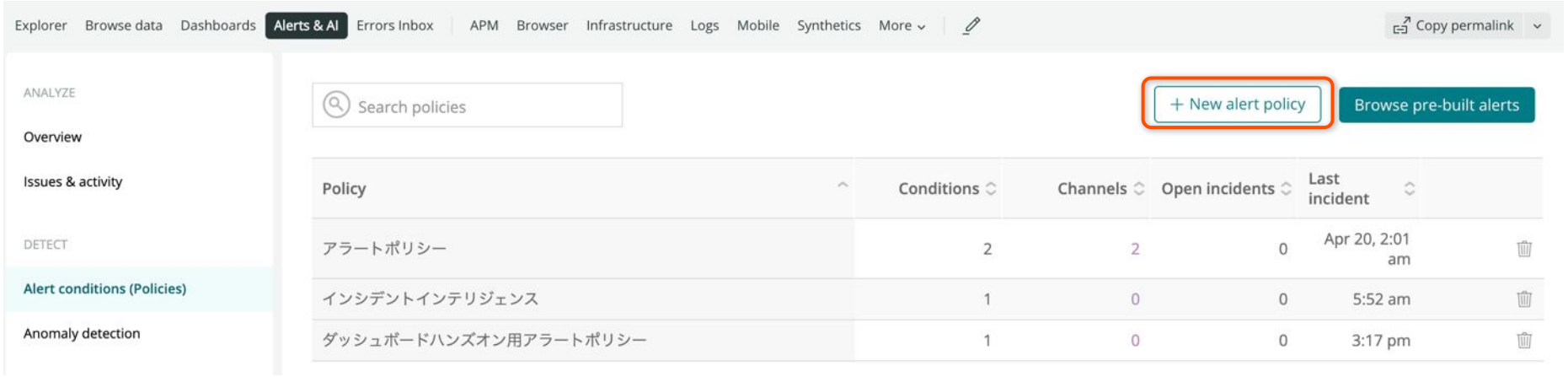
ハンズオン(1)アラートを作成する

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



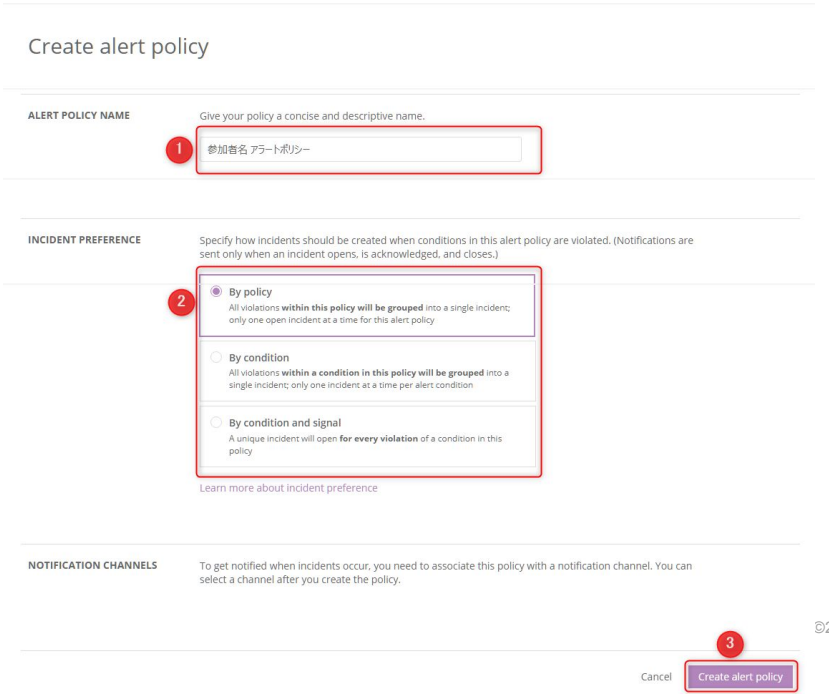
ハンズオン(1)アラートを作成する

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



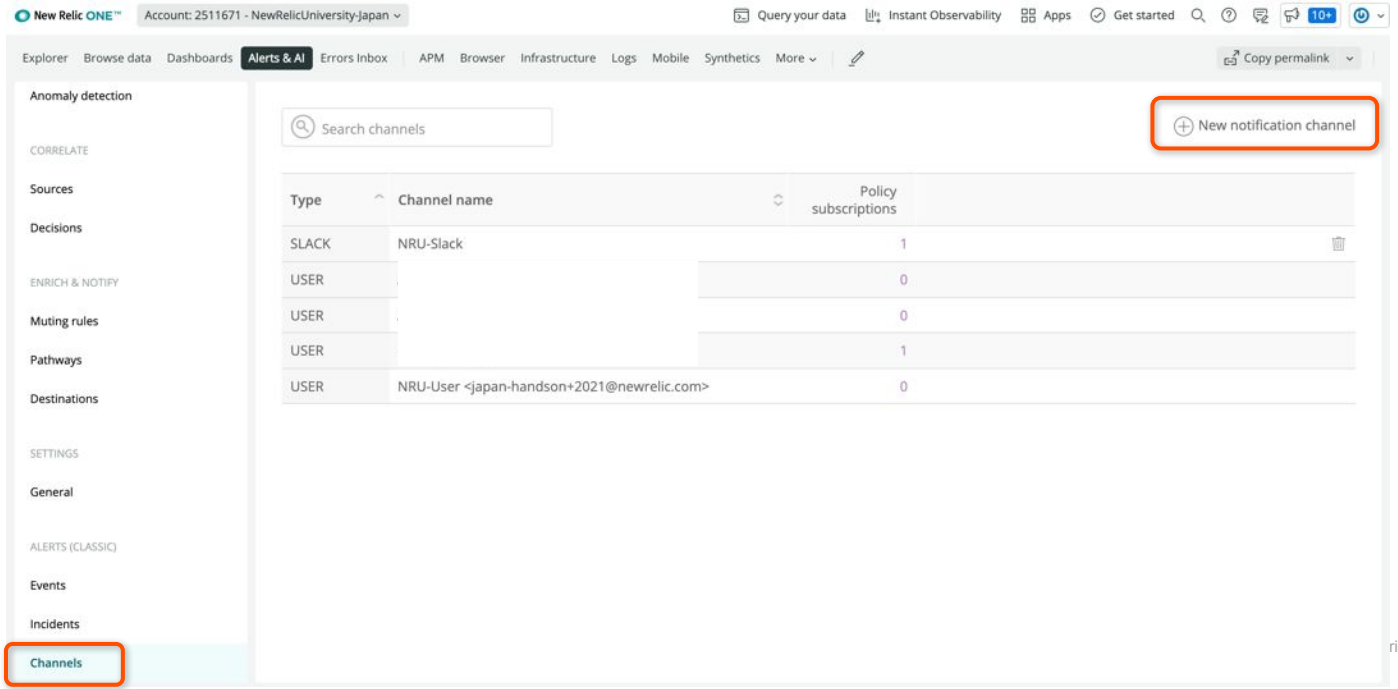
ハンズオン(1)アラートを作成する

- 自分用とわかりやすい名前を付けて AlertPolicyを作成します。
- New Relic アラートの構成要素②通知条件 (続き) を参考に好みの「INCIDENT PREFERENCE」を選択してください。



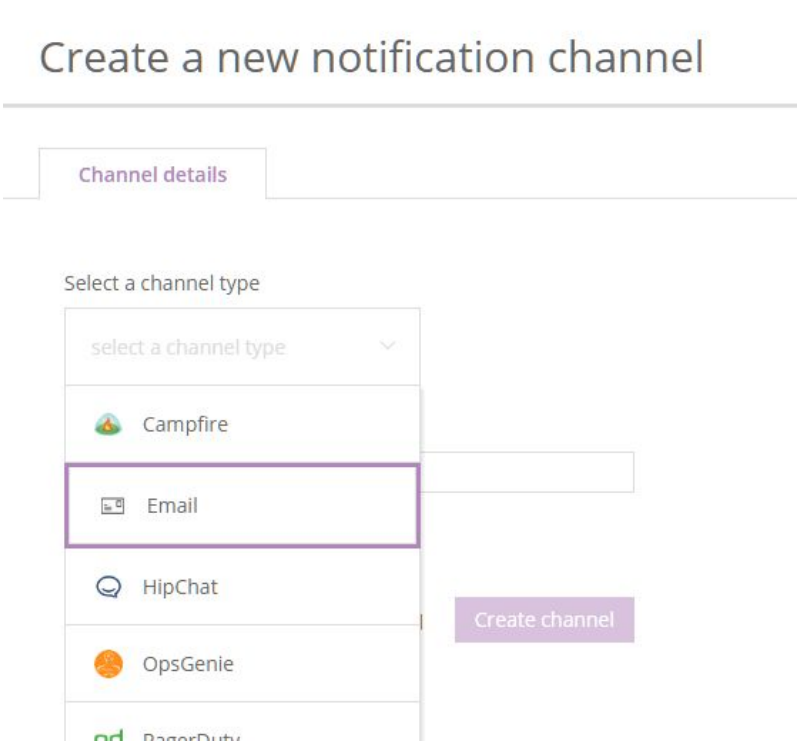
ハンズオン(1)アラートを作成する（オプション）

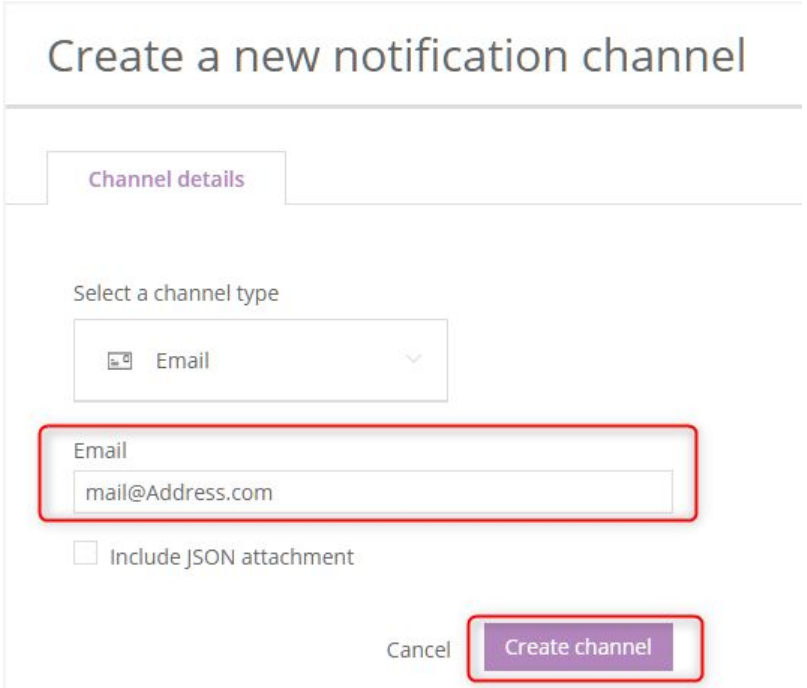
- （オプション）mail通知したい場合だけ設定します。
- 「Channels」を開き「＋ New notification channel」をクリックします。



ハンズオン(1)アラートを作成する（オプション）

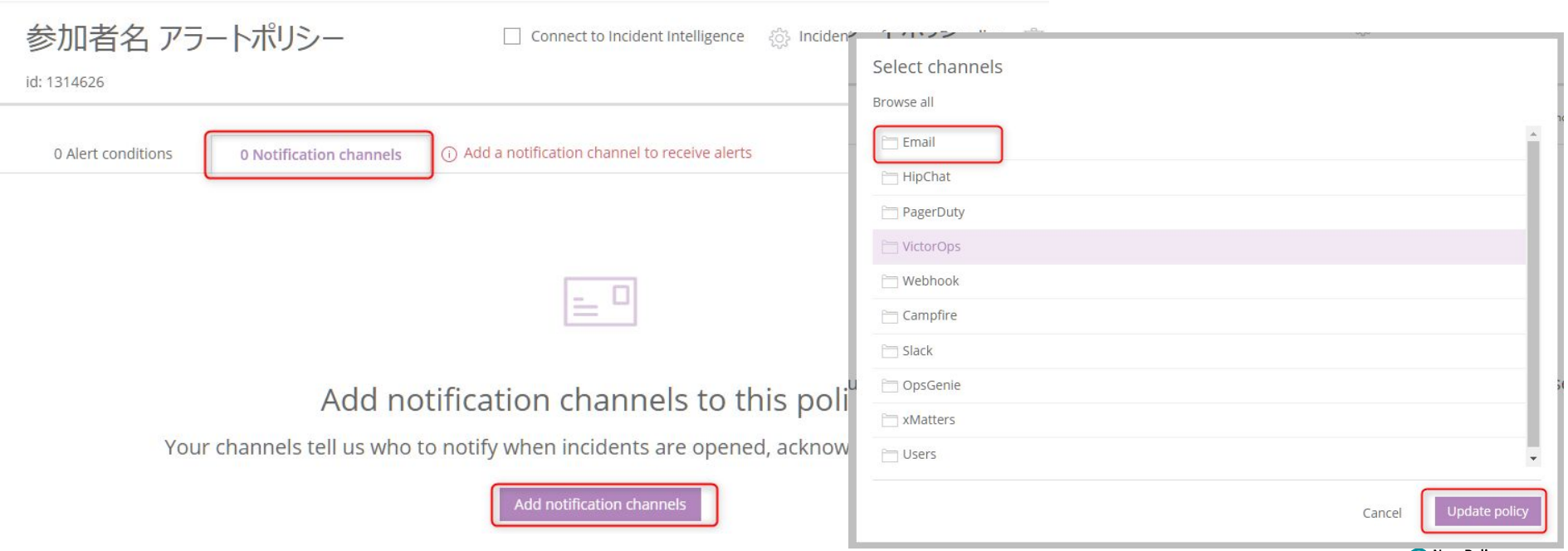
[Enail]を選択し自分の mail Addressを入力して「Create Channel」をクリックします。





ハンズオン(1)アラートを作成する（オプション）

- 自分のポリシーを開き、「Notification channel」から先ほど登録したEmailを紐付けます。



ハンズオン(1)アラートを作成する

[再掲]

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	サイトがエラーを返す	サイトの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	**①チェックエラー**		
フロントエンド	**②Apdex**	JSエラー		
アプリケーション	Apdex **③応答時間**	**④4xx, 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

- **新規アラート条件の追加**

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

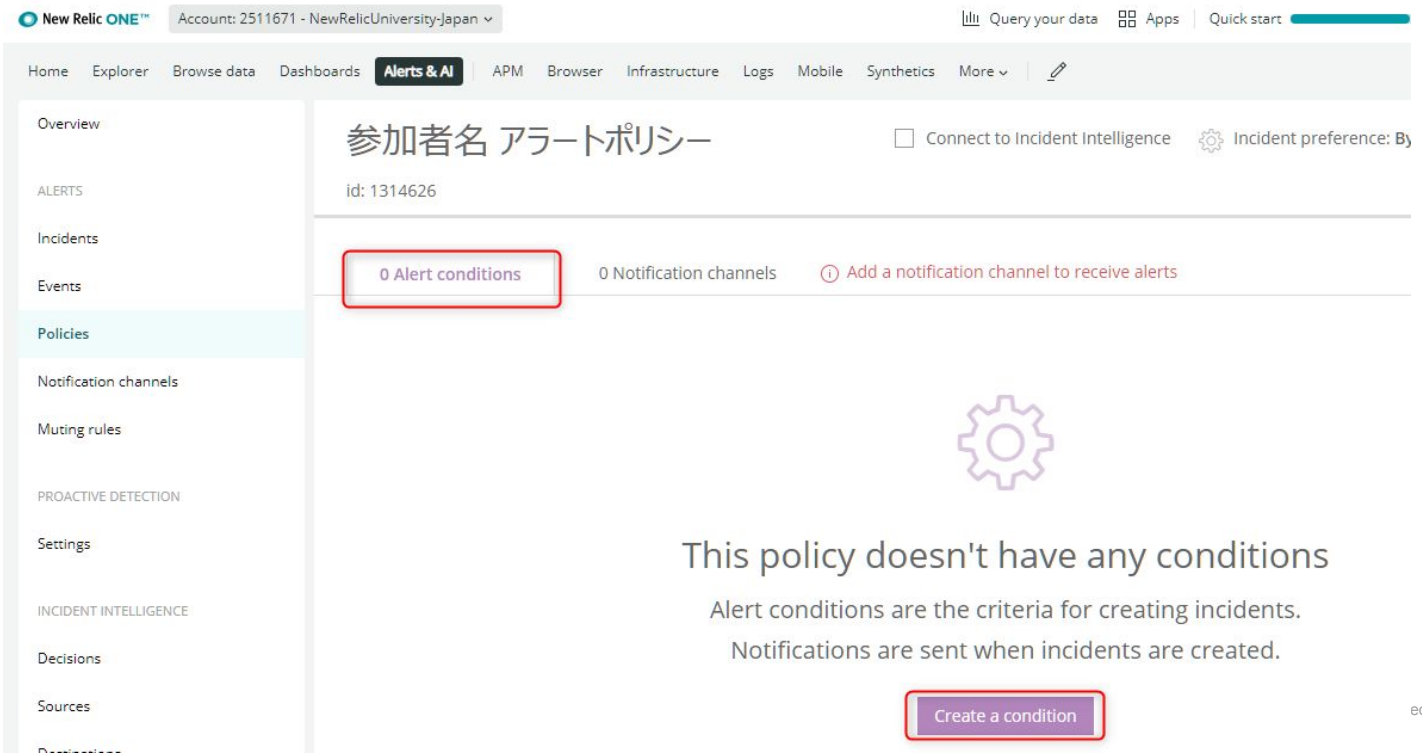
②フロントエンド: Apdex(静的)

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(ホスト間での外れ値)

ハンズオン(1)アラートを作成する①

- 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)アラートを作成する①

- 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

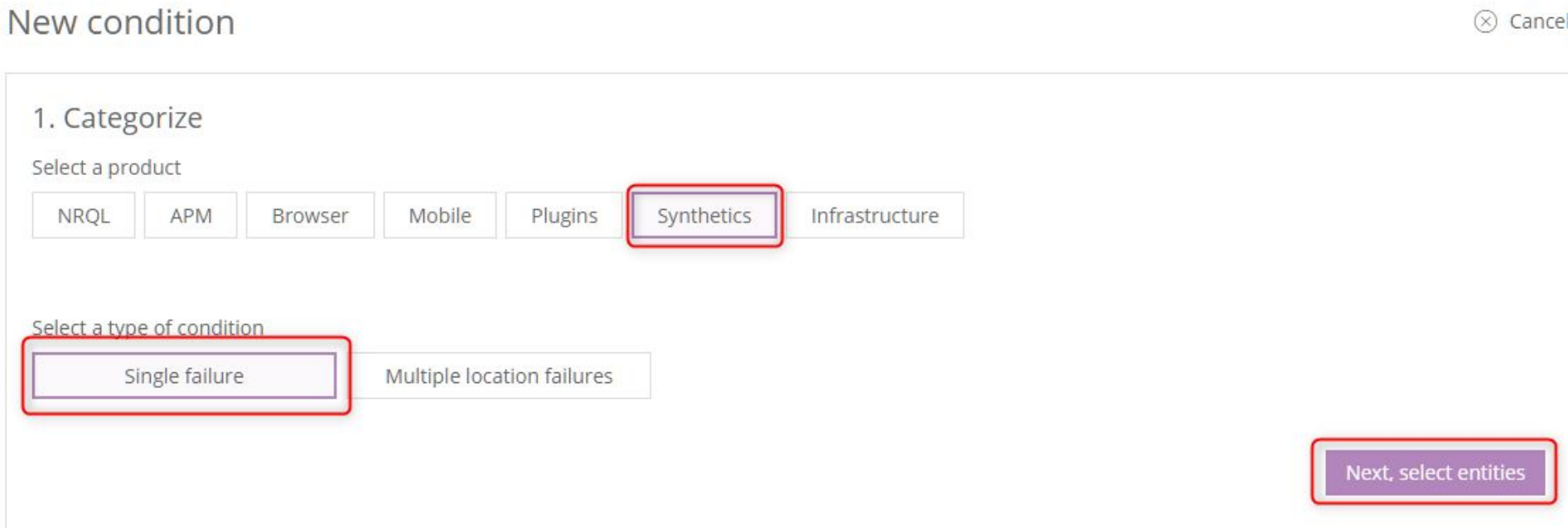
Synthetics –> Single failure

2. Select a monitor

EC-CUBE-Checkout

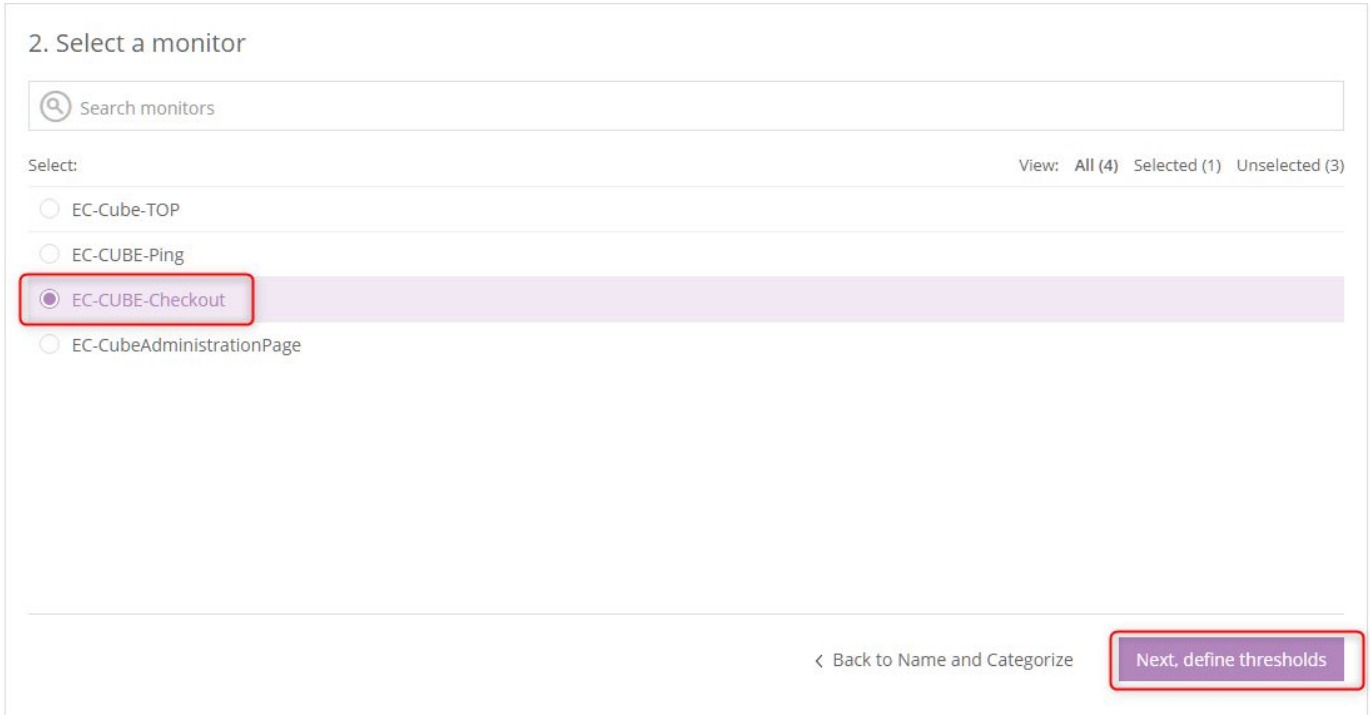
ハンズオン(1)アラートを作成する①

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



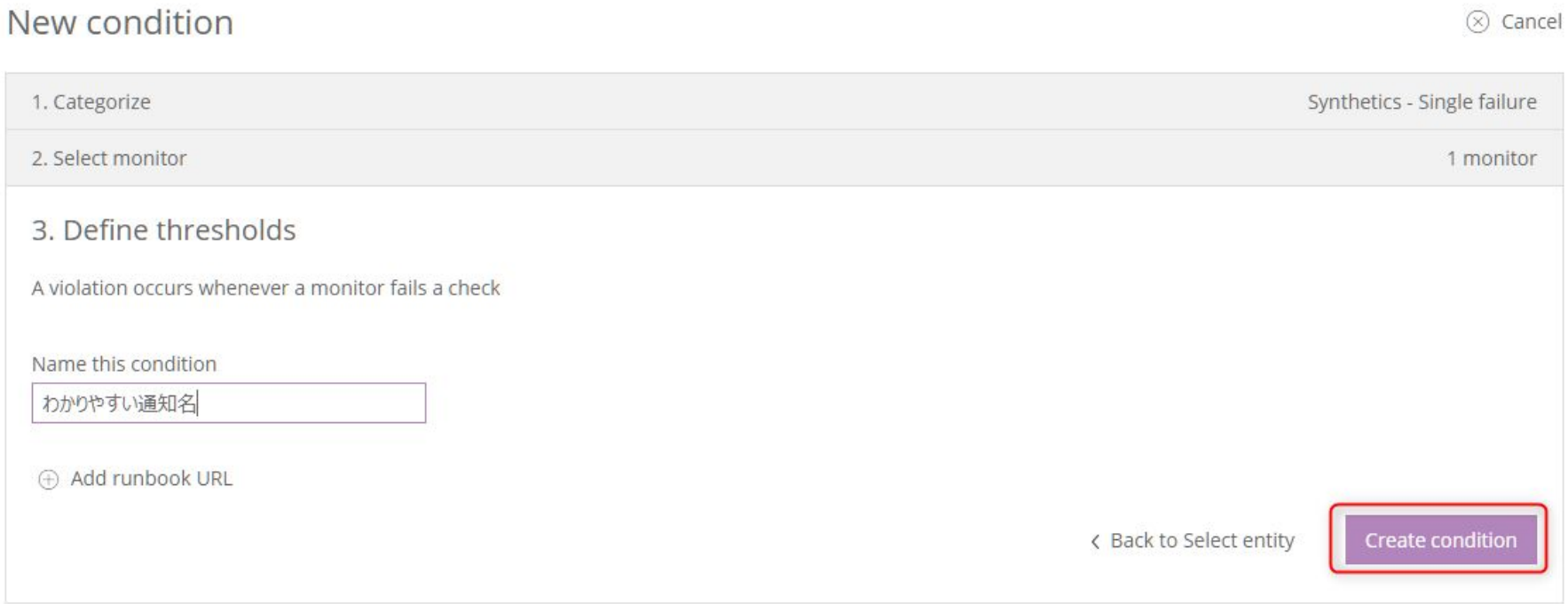
ハンズオン(1)アラートを作成する①

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



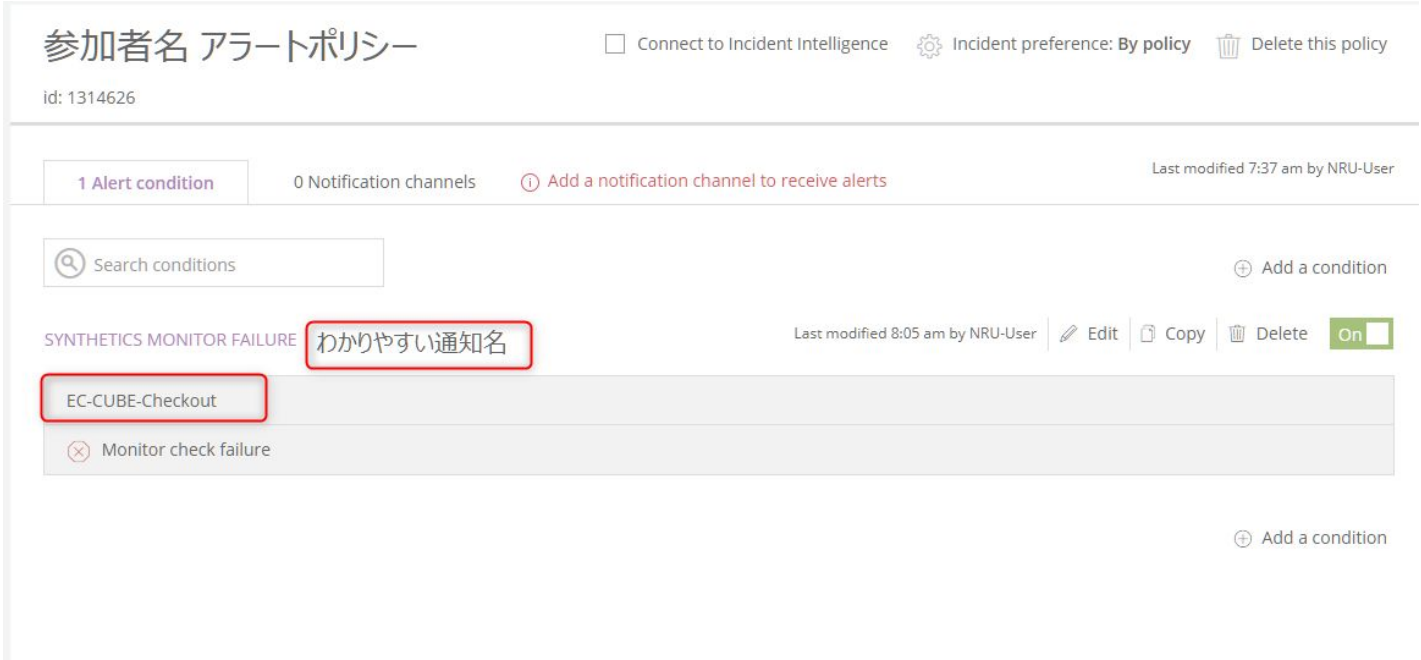
ハンズオン(1)アラートを作成する①

- 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)アラートを作成する①

- 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)アラートを作成する②

- **新規アラート条件の追加**

②フロントエンド: Apdex(静的)

1. Categories

Browser –> Metric

2. Select entities

EC-site

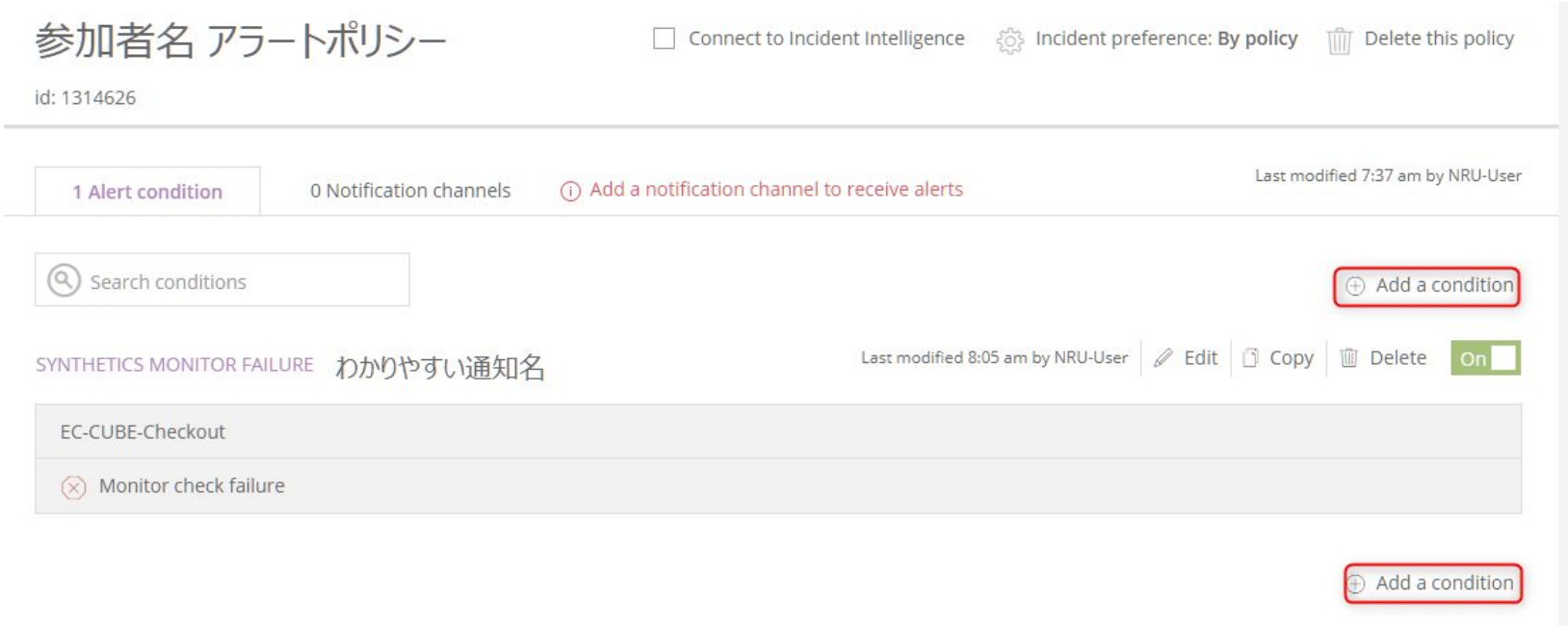
3. Define thresholds

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

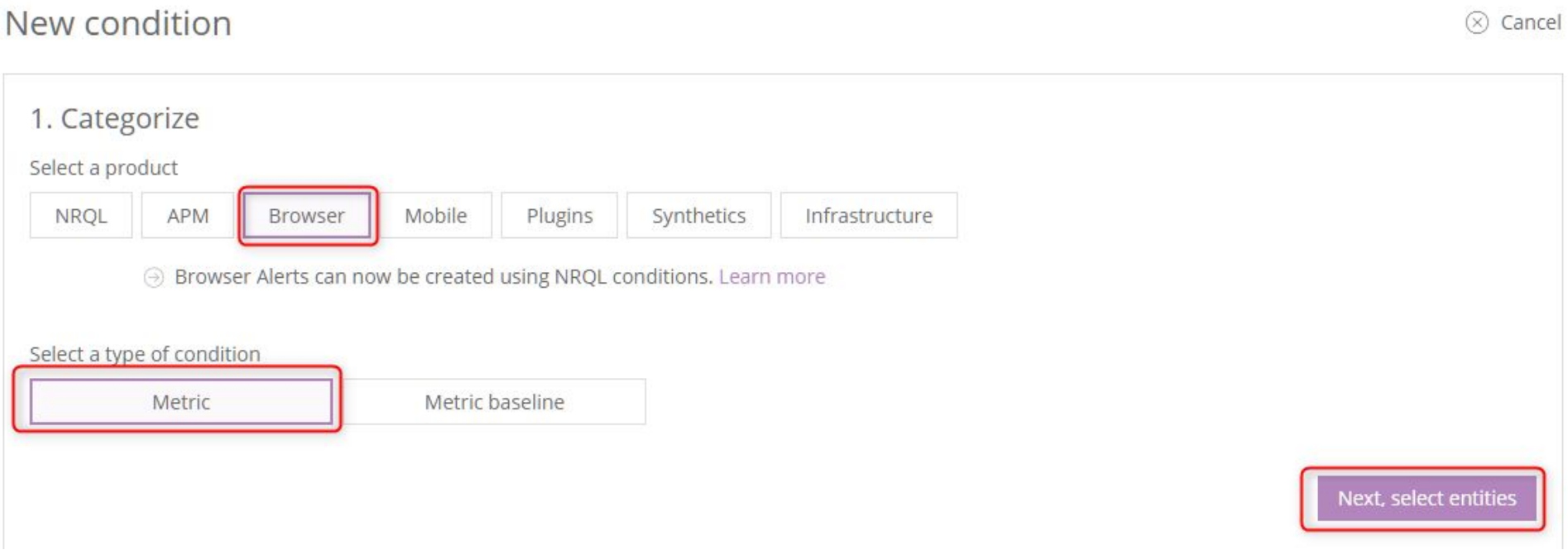
ハンズオン(1)アラートを作成する②

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



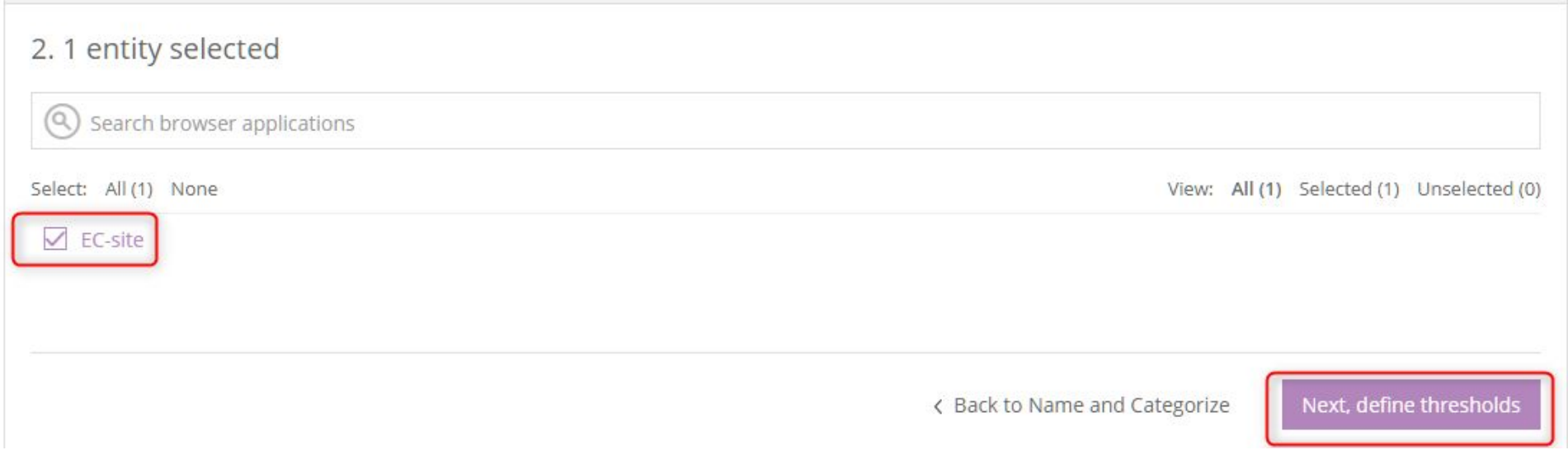
ハンズオン(1)アラートを作成する②

- **Categories** を設定します。



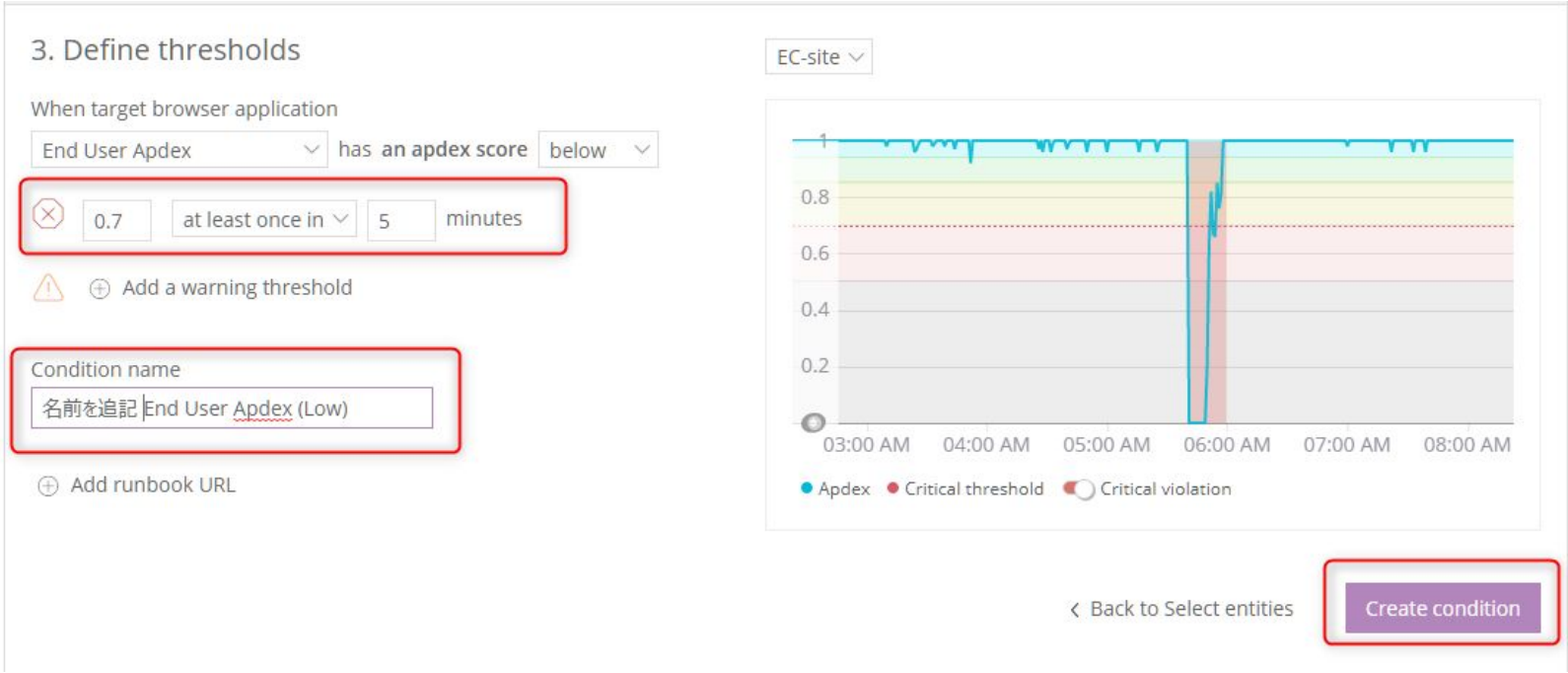
ハンズオン(1)アラートを作成する②

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



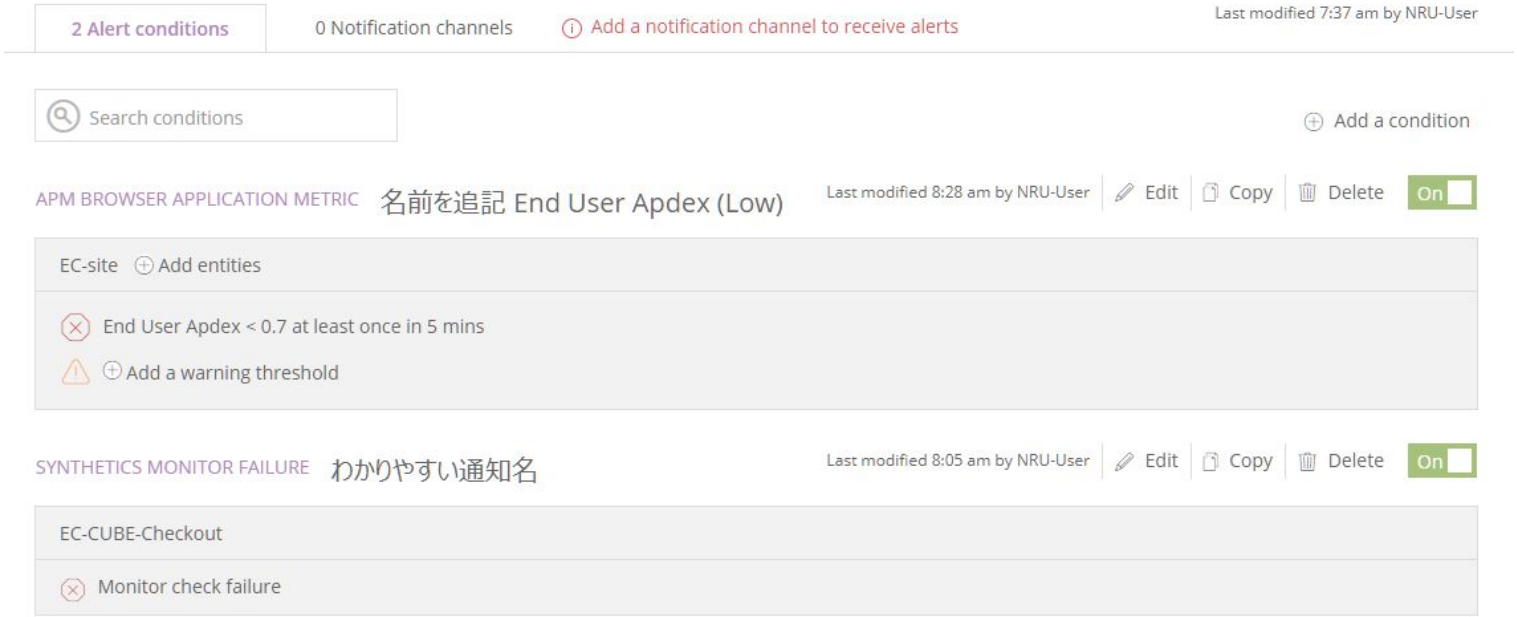
ハンズオン(1)アラートを作成する②

- **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)アラートを作成する②

- 2つめのconditionが作成されました。



ハンズオン(1)アラートを作成する③

- **新規アラート条件の追加**

③アプリケーション : 応答時間(動的)

1. Categories

APM –> Application metric baseline

2. Select entities

EC-site

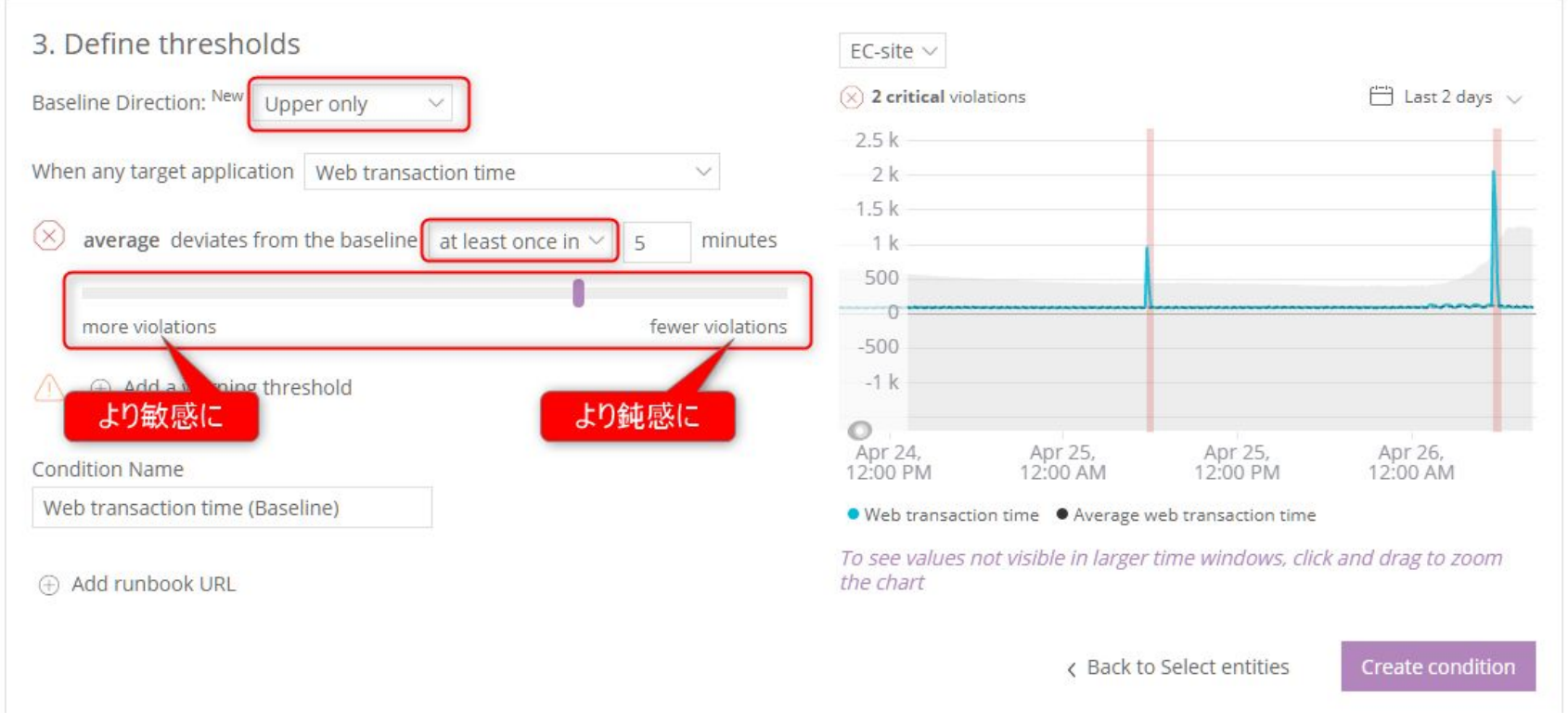
3. Define thresholds

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)アラートを作成する③

- 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)アラートを作成する④

- **新規アラート条件の追加**

④アプリケーション : 4xx,5xxエラー(ホストごとに評価)

1. Categories

NRQL

2. Enter a NRQL query and thresholds

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

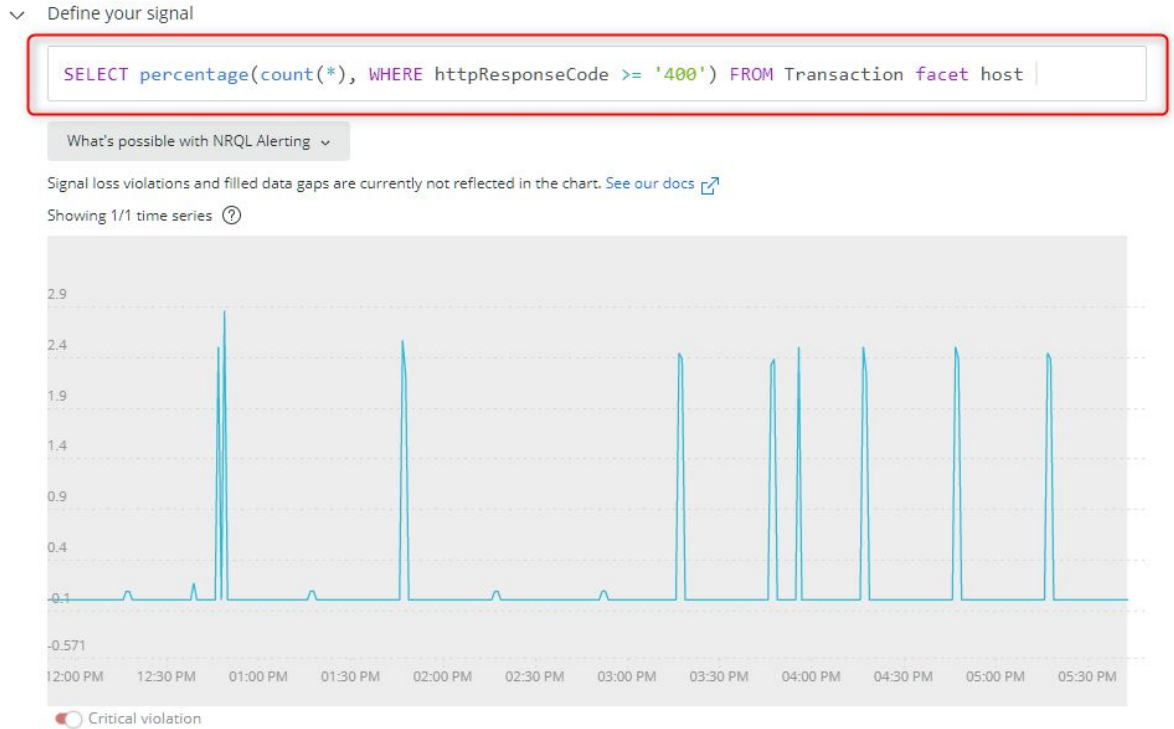
3. Define thresholds

Critical: 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)アラートを作成する④

- NRQLを入力すると自動的に参考となる Chartが表示されます。



New Relic®

AIOpsの意義

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

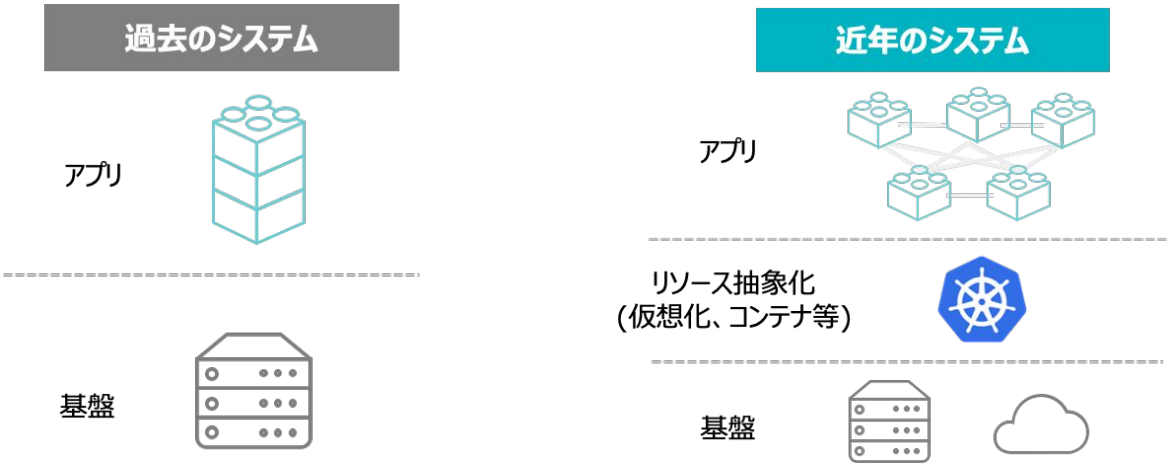
AIOpsとは、IT運用プロセスを自動化するためにビッグデータと機械学習を紐付けたものであり、以下のような機能を含む:

- イベントの相関分析
- 異常検知
- 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

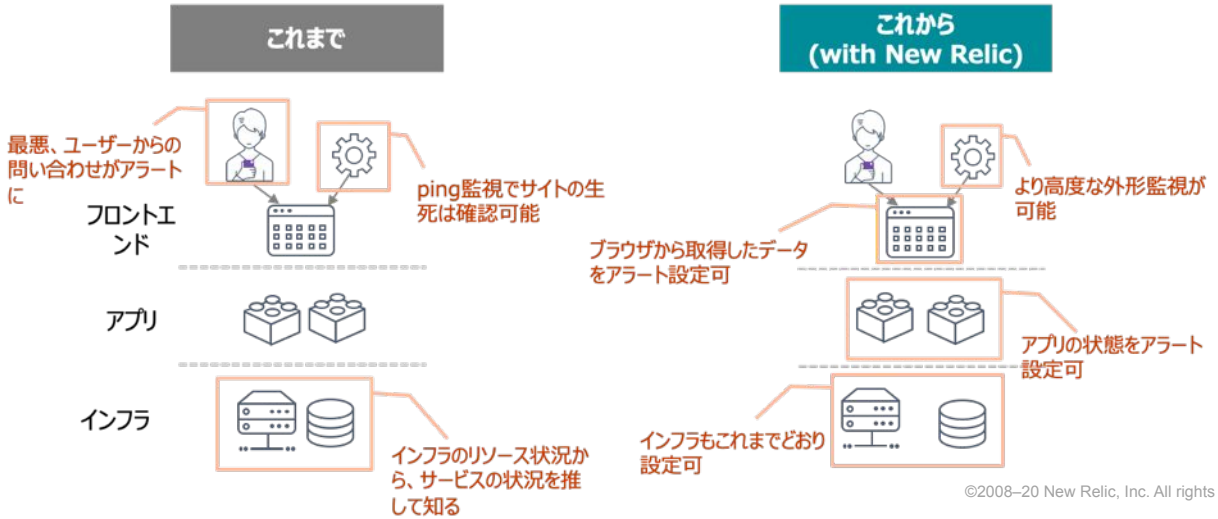
監視対象となるコンポーネントの絶対数が増えると同時に、コンポーネント同士の関連性がより複雑に



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

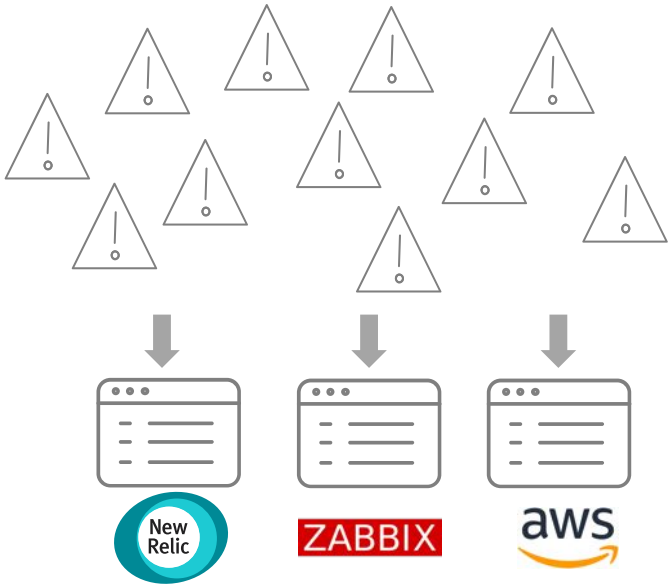
New Relicのようなオブザーバビリティプラットフォームによって、サービスを構成する様々なコンポーネントから多種多様なデータを取得できるように



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

気づけない

Actionableな監視

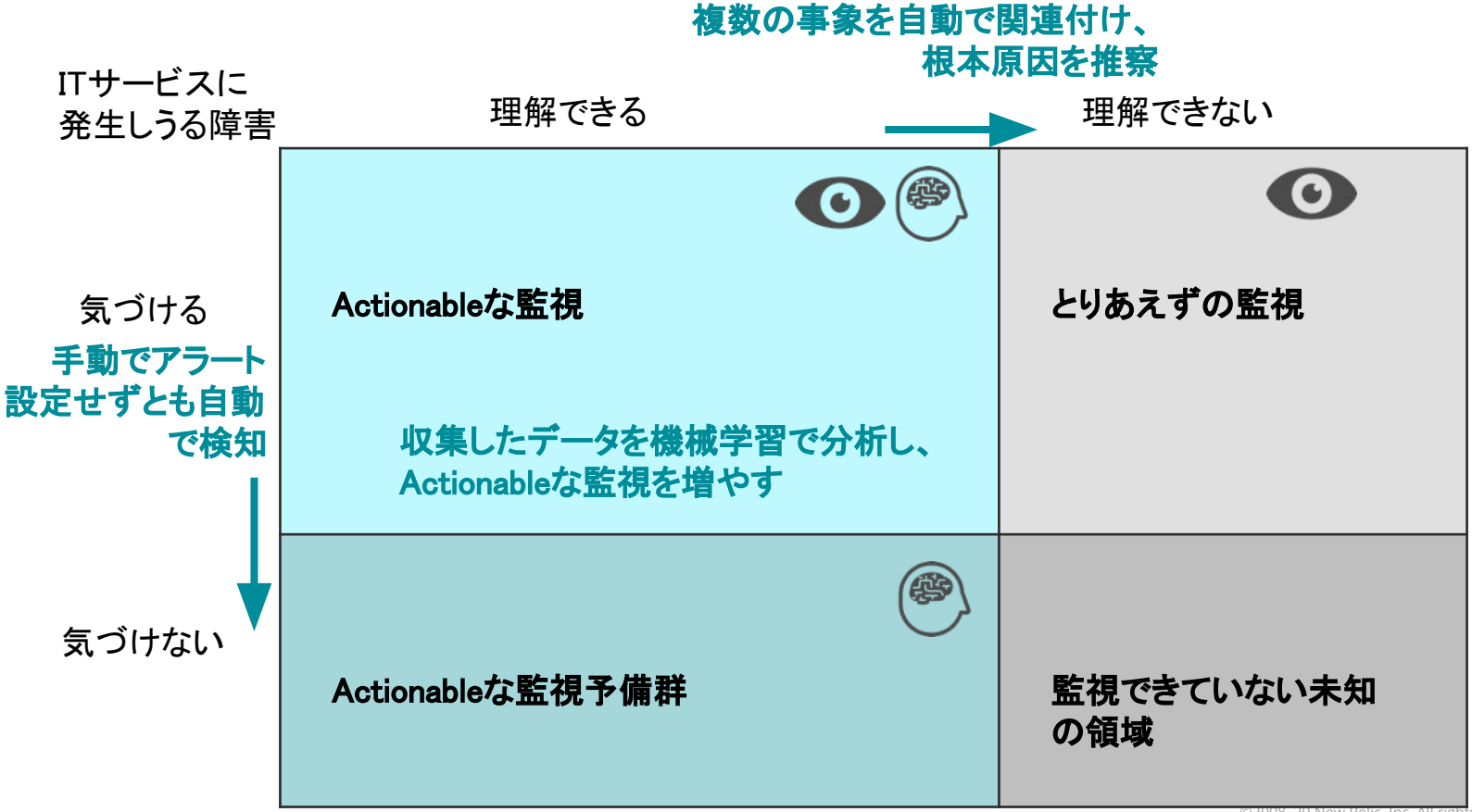
人力でこの面を増やすのは困難

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



AIOpsによってサービスの信頼性を高める

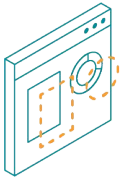
アラートを1つ1つ網羅的に
設定するのか問題

[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

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**



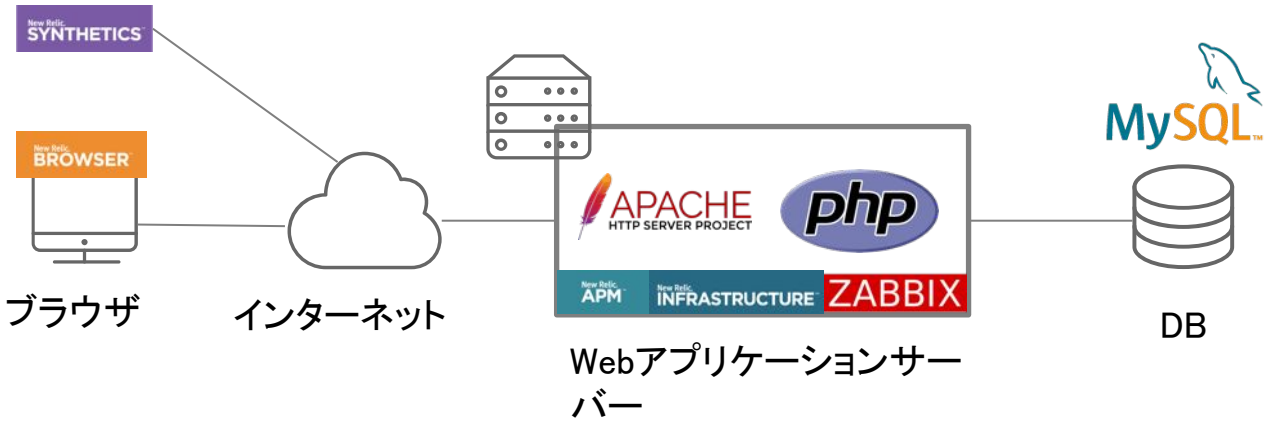
複数の事象を自動で関連付け、根本原因を推察

New Relic®

ハンズオン(2)
AIOpsを使った異常検知と原因分析(前編)

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. 異常を自動検知する

[目的]New RelicのAIOpsによる異常検知によって、何が検知できているかを確認しましょう

Alerts&AI -> Issues&activity -> Anomalies を選択

- 過去に発生したAnomalyのうち一つを選択
  - 何のAnomaly(異常)が発生しているでしょうか
  - 発生したAnomalyに関連する他のメトリックはありますか？

ハンズオン(2)

2. 様々なソースのアラートをまとめる (1)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 -> Sourceを選択
- 左上のAlertsを選択し、Add a policyを押す
- ハンズオン(1)で作成した自分のアラートポリシーを選択し、Connect

ハンズオン(2)

2. 様々なソースのアラートをまとめる (2)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以下のSettings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

ハンズオン(2)（参考）

2. 様々なソースのアラートをまとめる (3)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APISecurityTokenを利用してJavaScript から送信することができます。

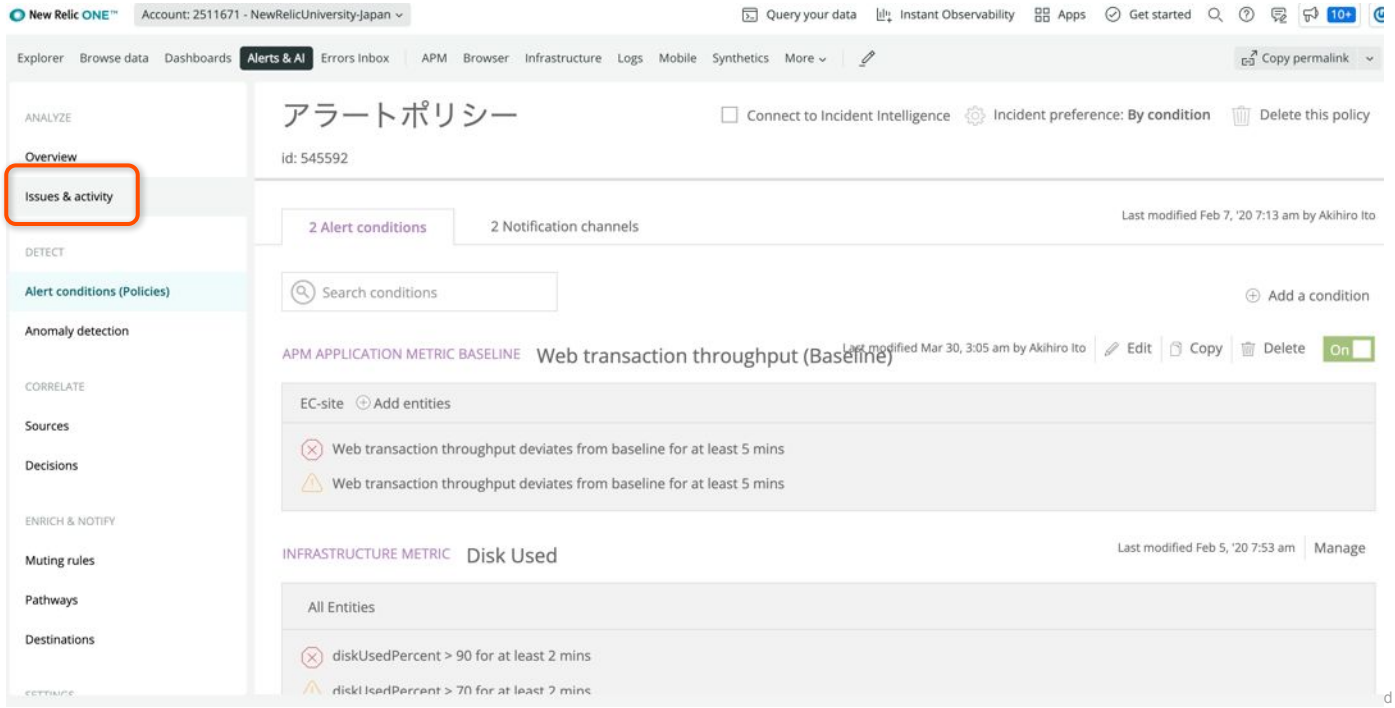
New Relic®

手順・解説

ハンズオン(2) 15min

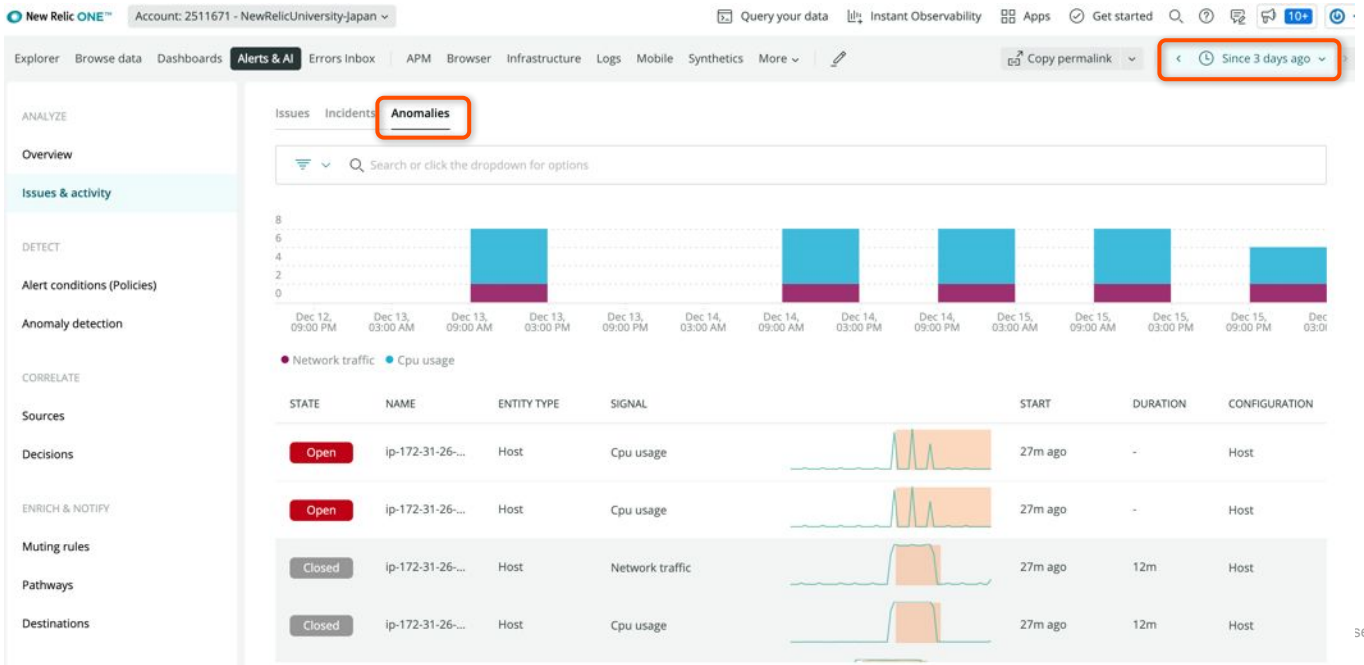
ハンズオン(2)異常を自動検知する

- 「Issues & activity」をクリックします。



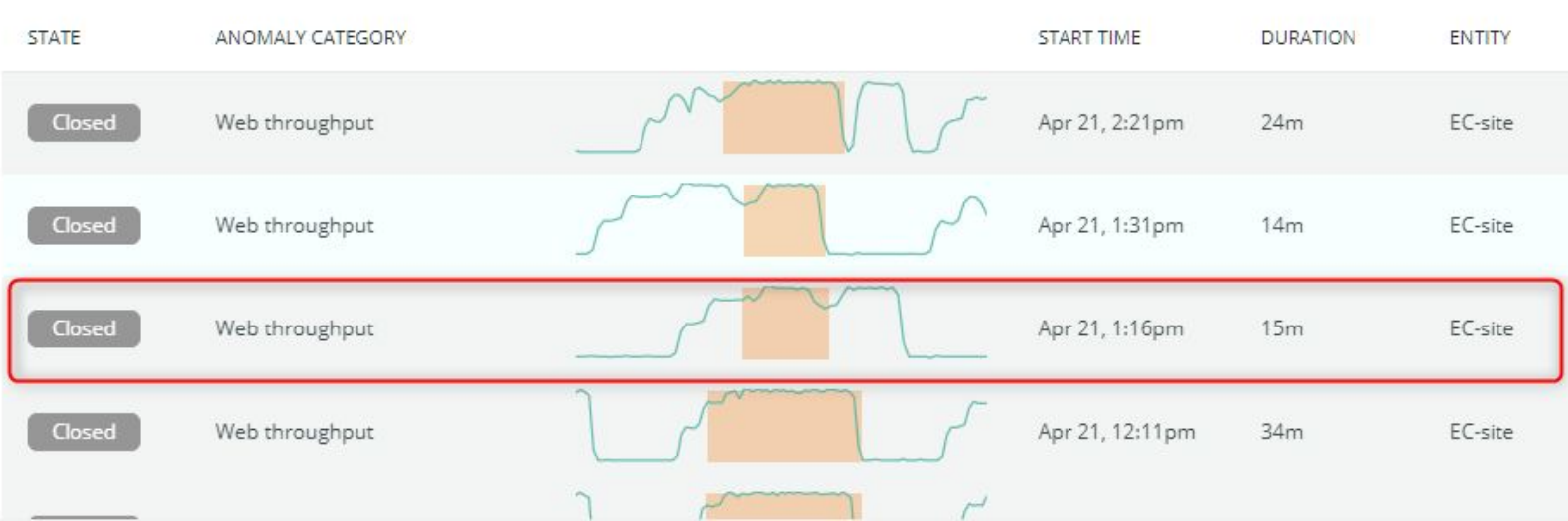
ハンズオン(2)異常を自動検知する

- Anomalies タブをクリックします。
- データが表示されない場合は表示期間を延ばしてみてください。



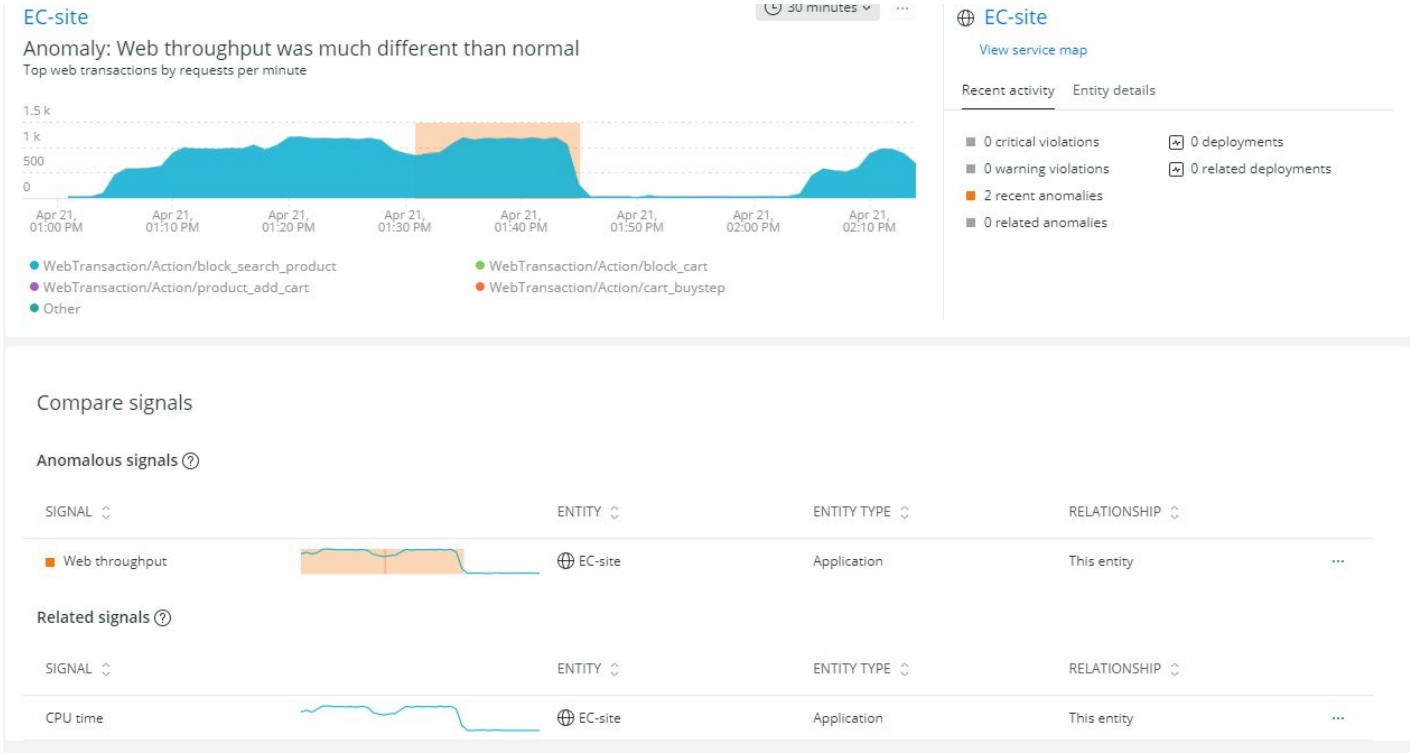
ハンズオン(2)異常を自動検知する

- 自動的に検知された値のいずれかをクリックします。



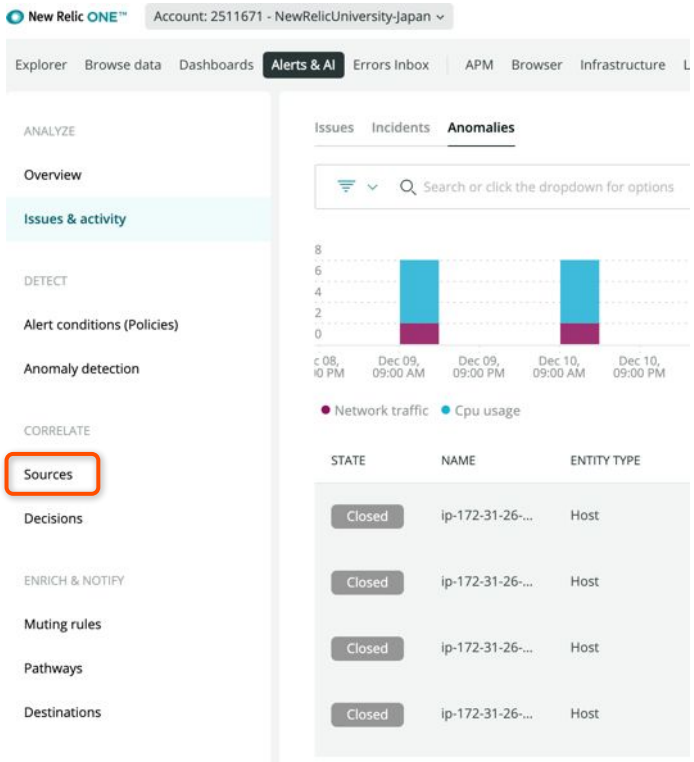
ハンズオン(2)異常を自動検知する

- Anomalyの詳細ではその異常が検知されたときに、同時に変化していた値などを確認することができます。



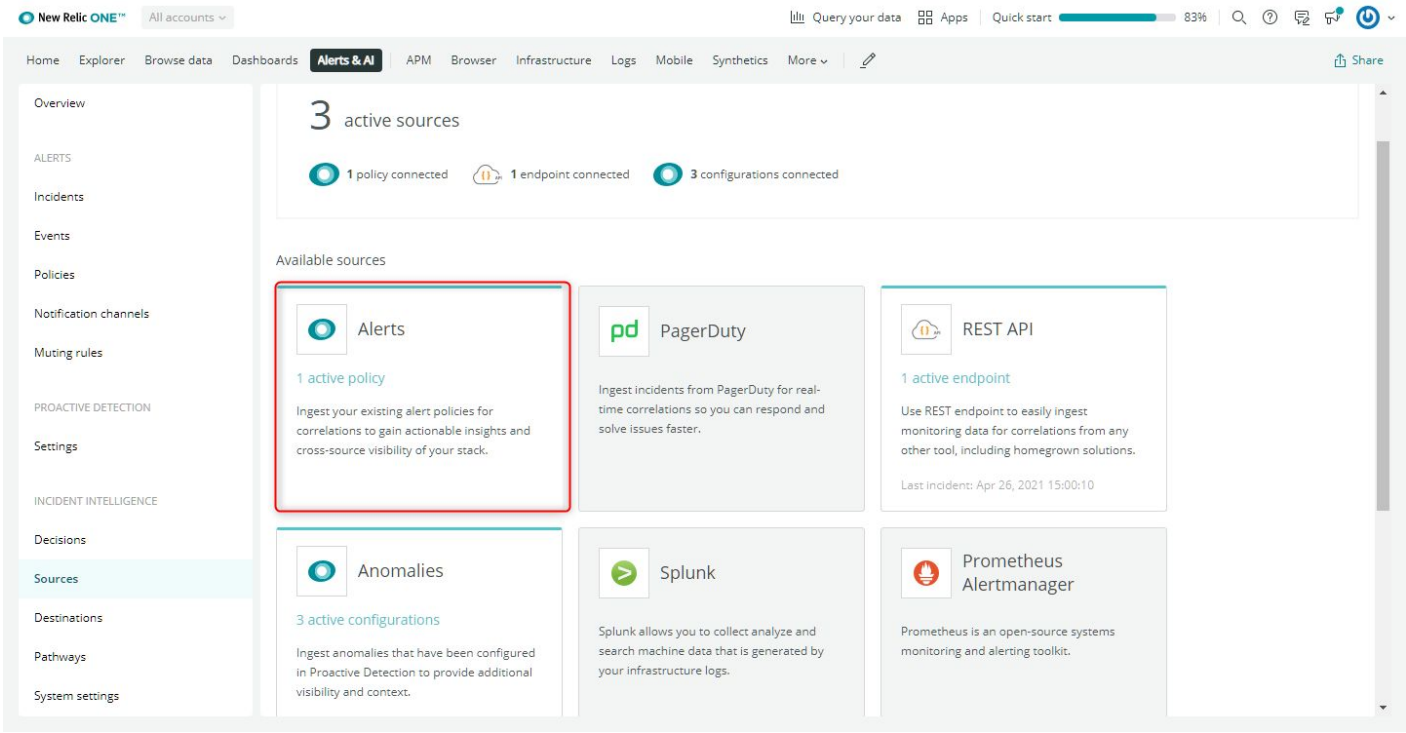
ハンズオン(2)様々なソースのアラートをまとめる(1)

- 「Sources」をクリックします。



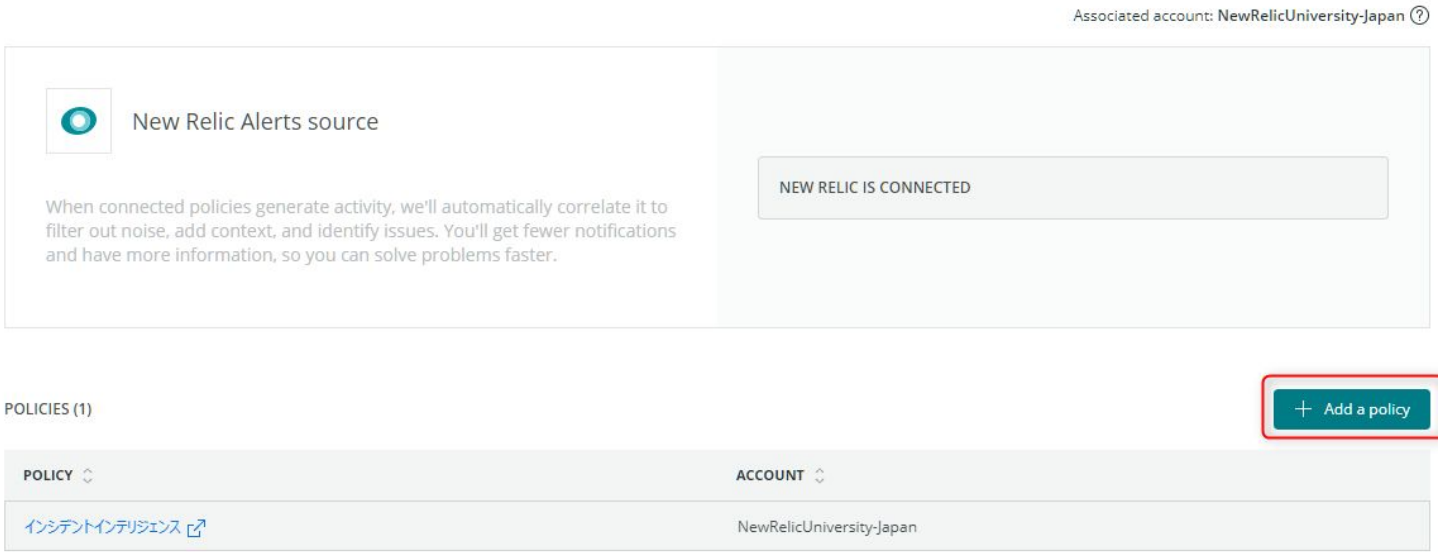
ハンズオン(2)様々なソースのアラートをまとめる(1)

- 「Alerts」カードをクリックします。



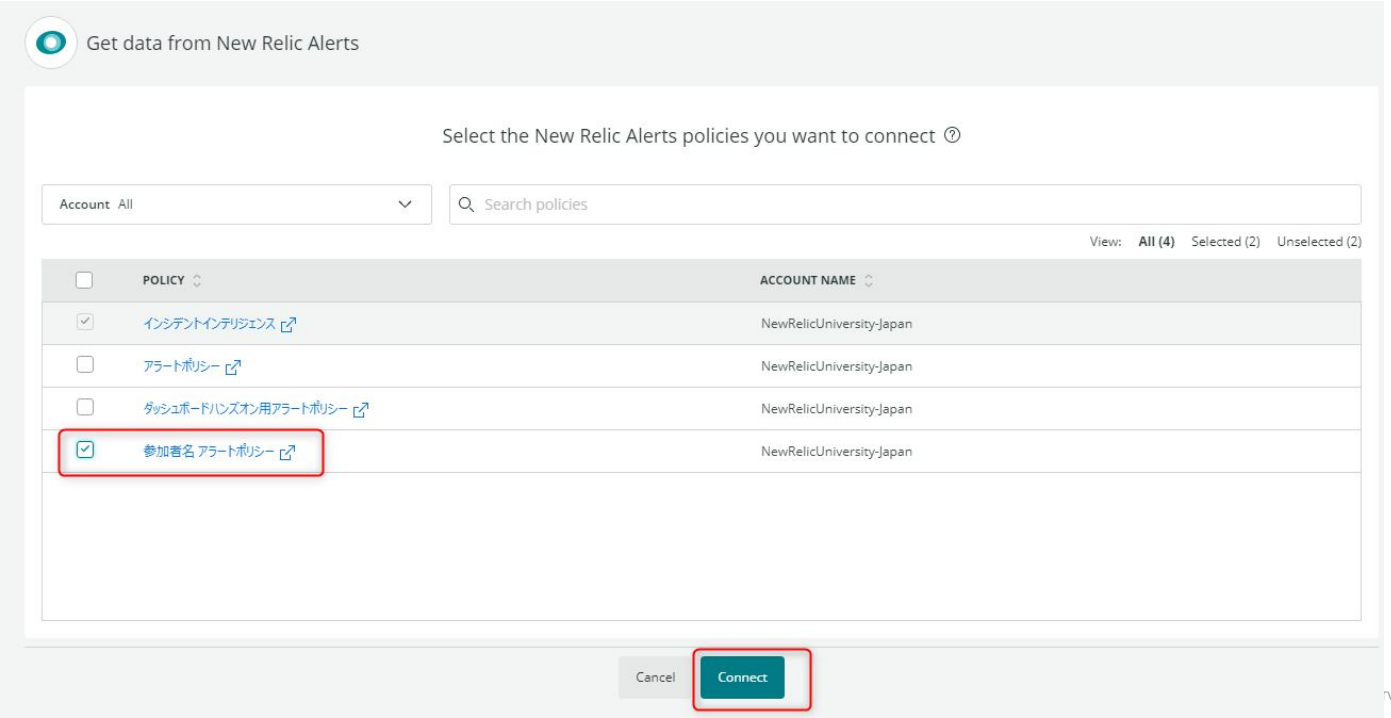
ハンズオン(2)様々なソースのアラートをまとめる(1)

- 「＋ Add a policy」ボタンをクリックします。



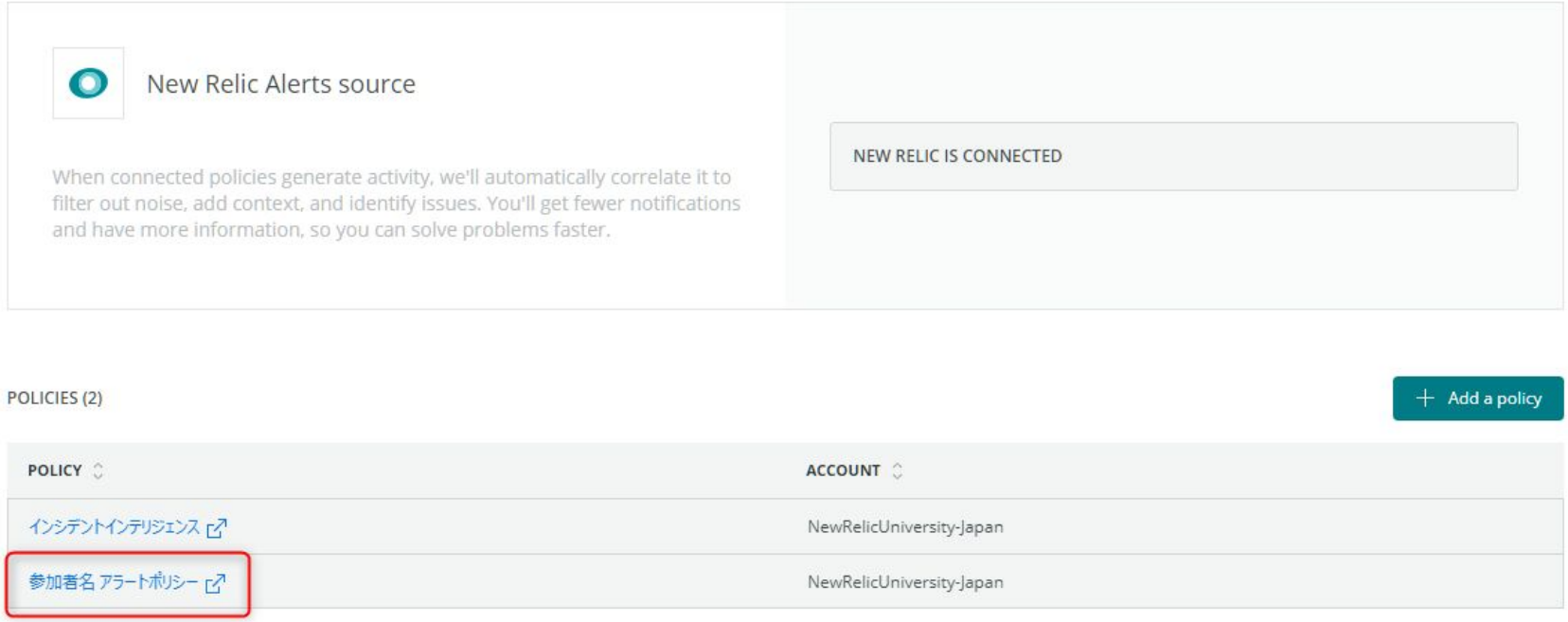
ハンズオン(2)様々なソースのアラートをまとめる(1)

- 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。



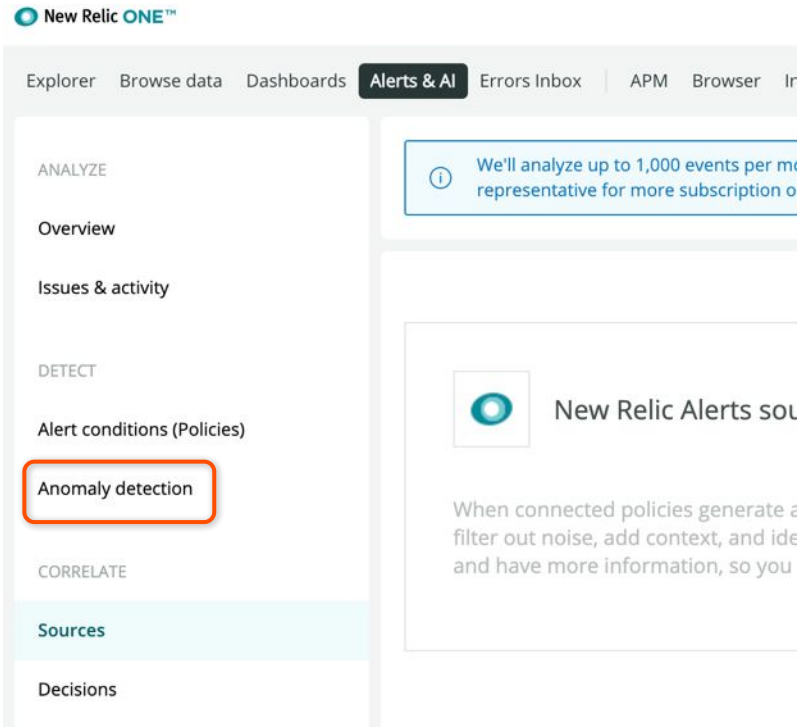
ハンズオン(2)様々なソースのアラートをまとめる(1)

- 自分のPolicyが追加された事を確認します。



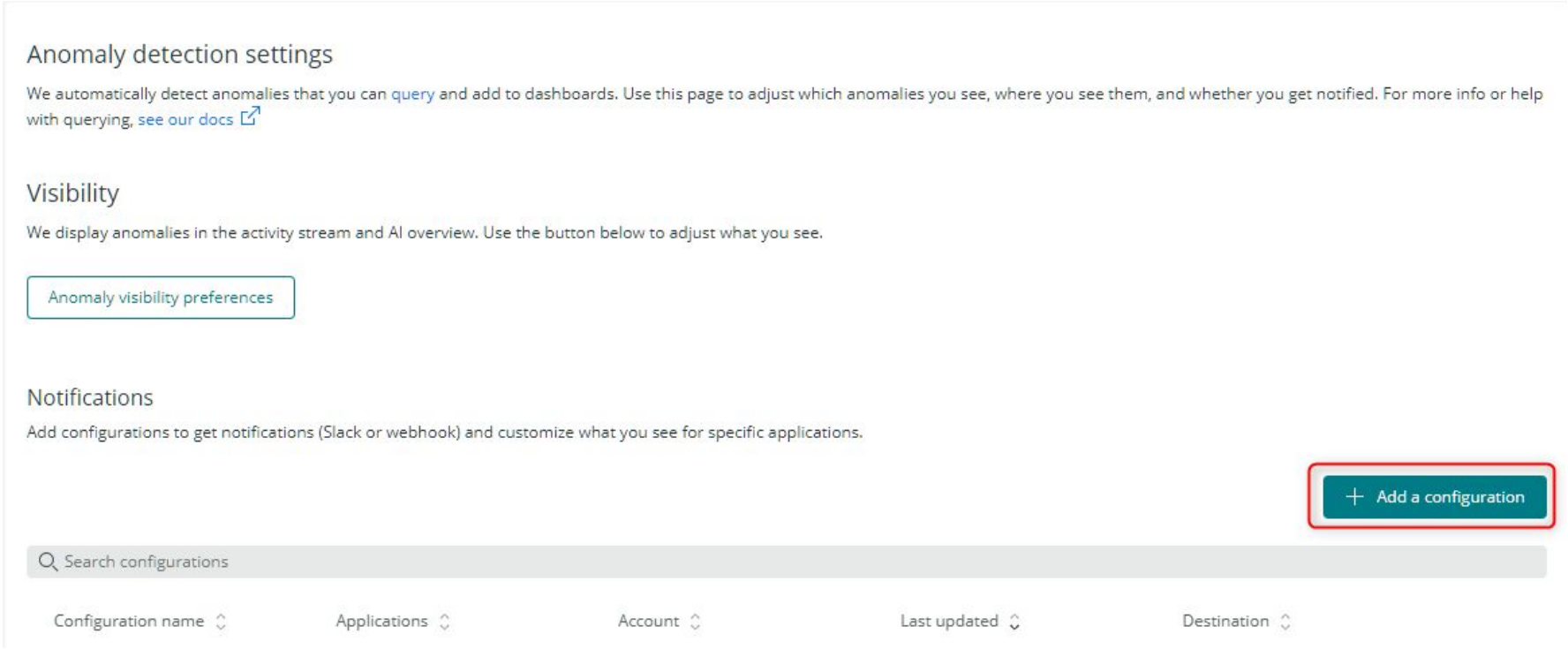
ハンズオン(2)様々なソースのアラートをまとめる(2)

- 「Anomaly detection」をクリックします。



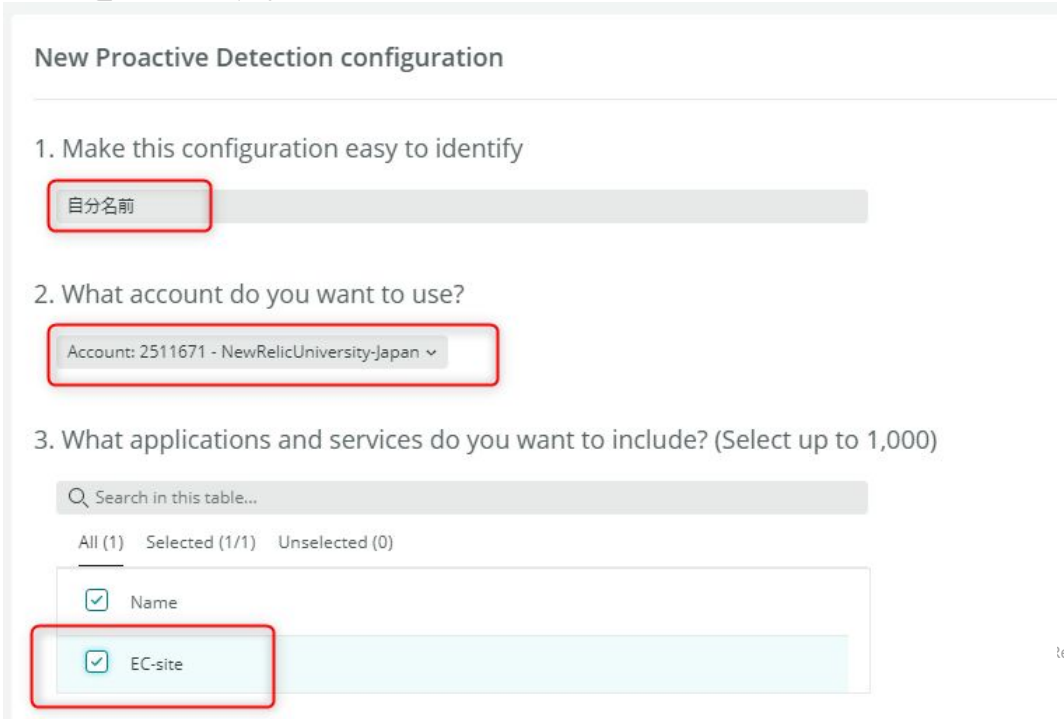
ハンズオン(2)様々なソースのアラートをまとめる(2)

- 「＋ Add a Configuration」ボタンをクリックします。



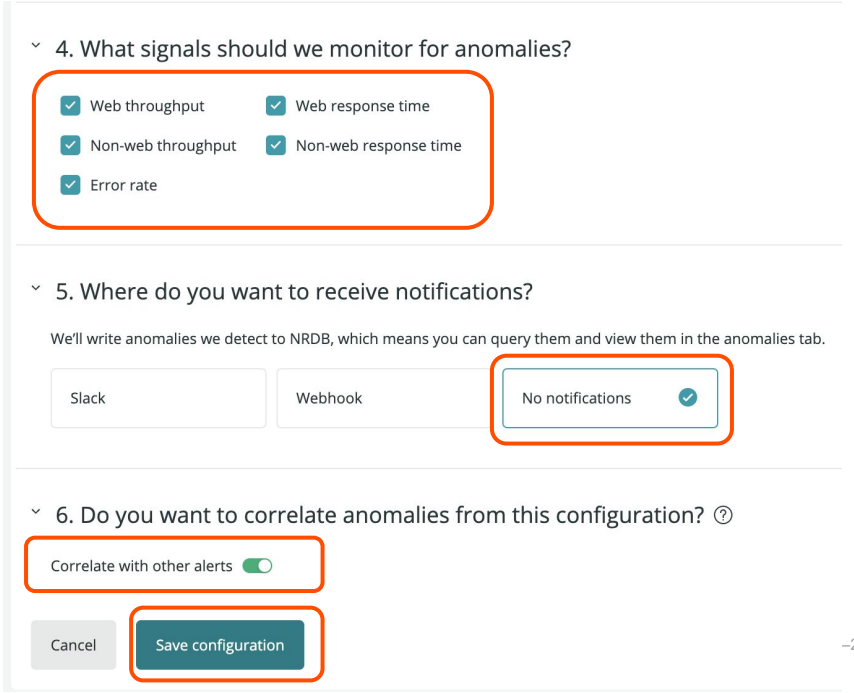
ハンズオン(2)様々なソースのアラートをまとめる(2)

- 「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。



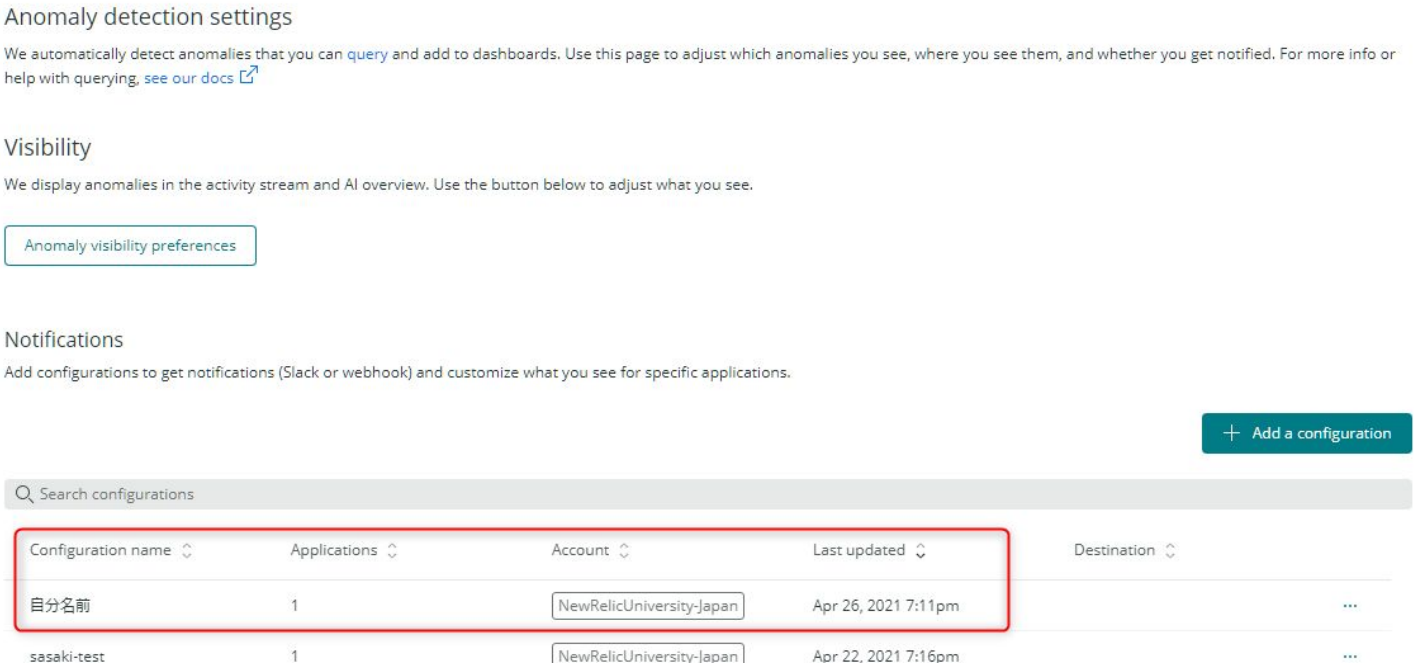
ハンズオン(2)様々なソースのアラートをまとめる(2)

- 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。



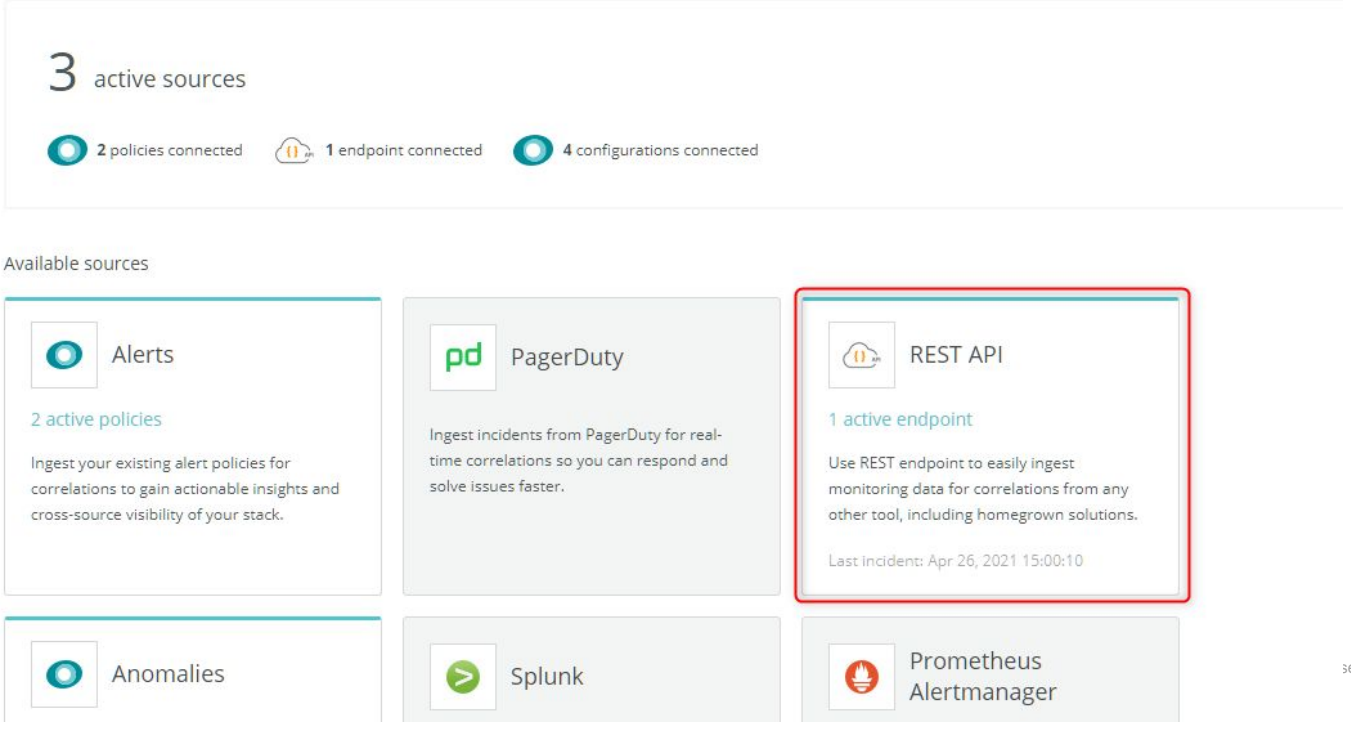
ハンズオン(2)様々なソースのアラートをまとめる(2)

- 設定が追加されたことを確認します。



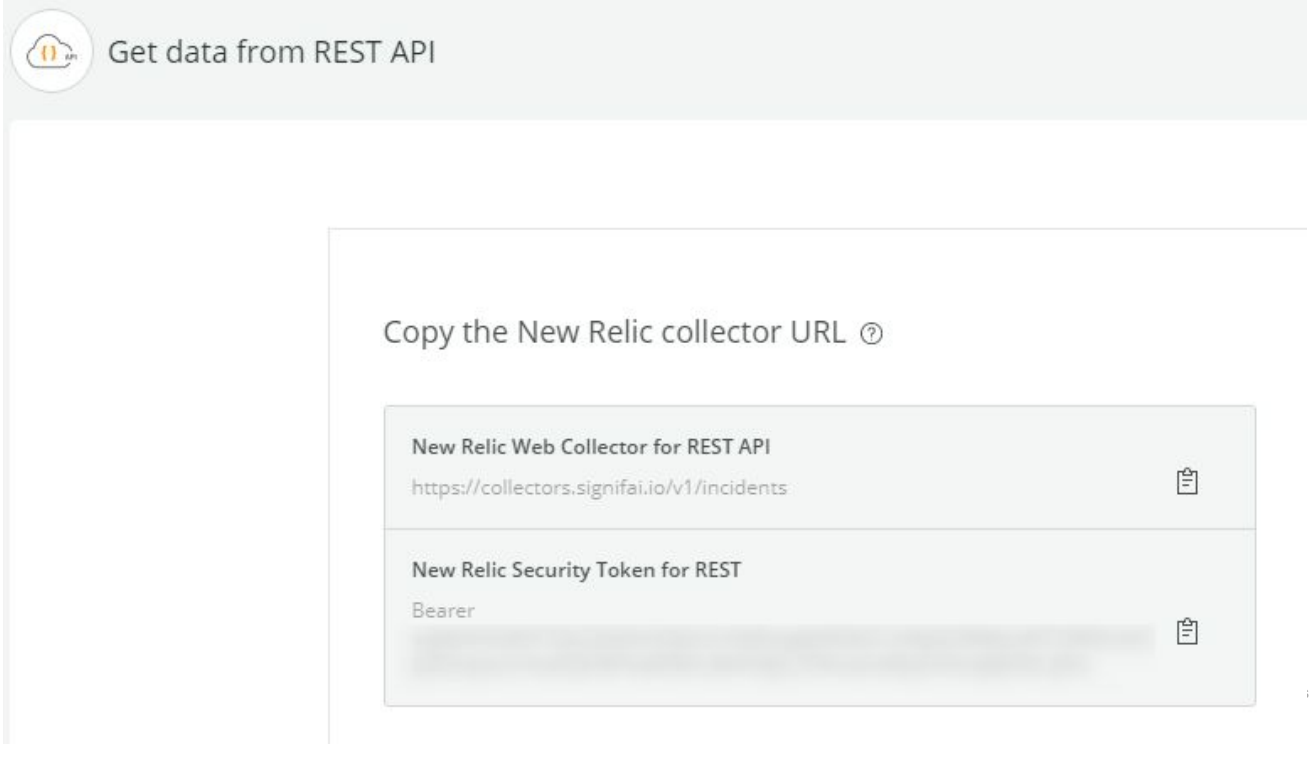
参考 Zabbixの連携

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



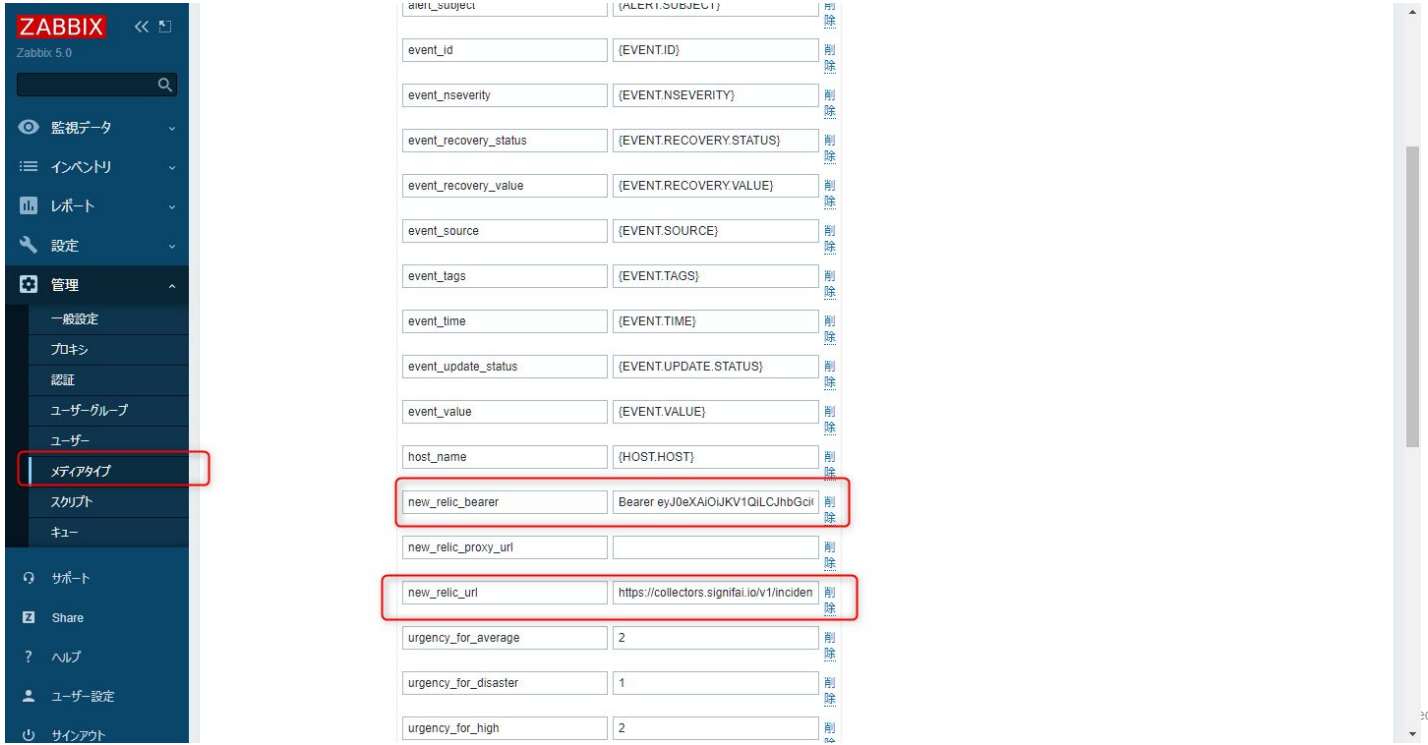
参考 Zabbixの連携

- API URLとAPI Tokenをコピーして Zabbix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。



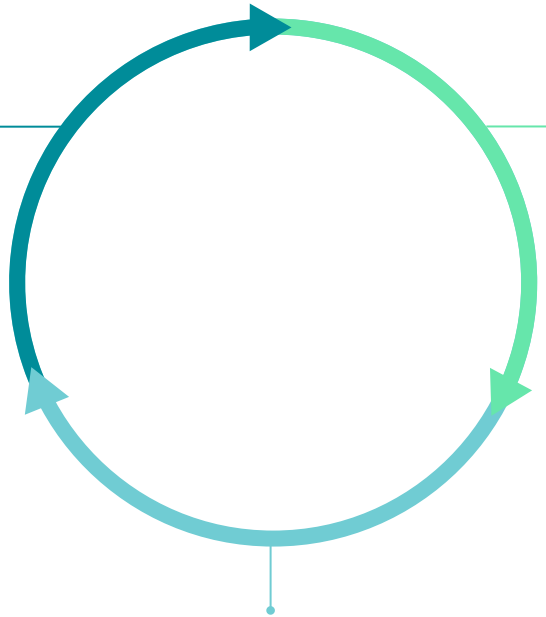
参考 Zabbixの連携

- 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。

New Relic®

New RelicのAIOps機能

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)

分析

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）

⬇

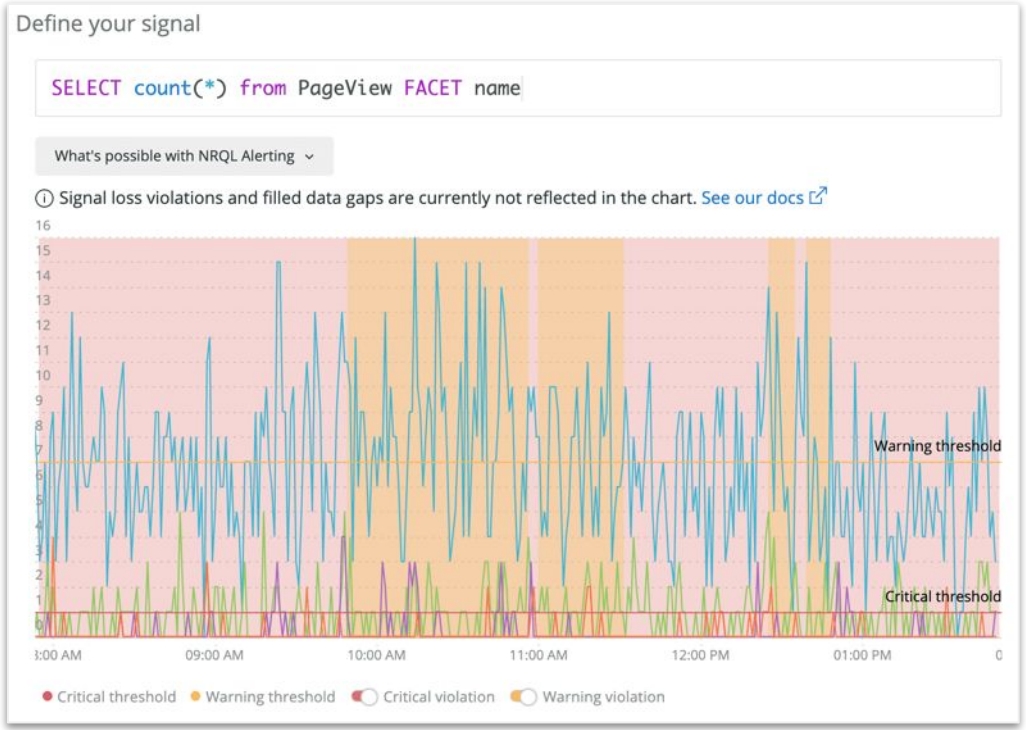
診断

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: Proactive 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）

↓

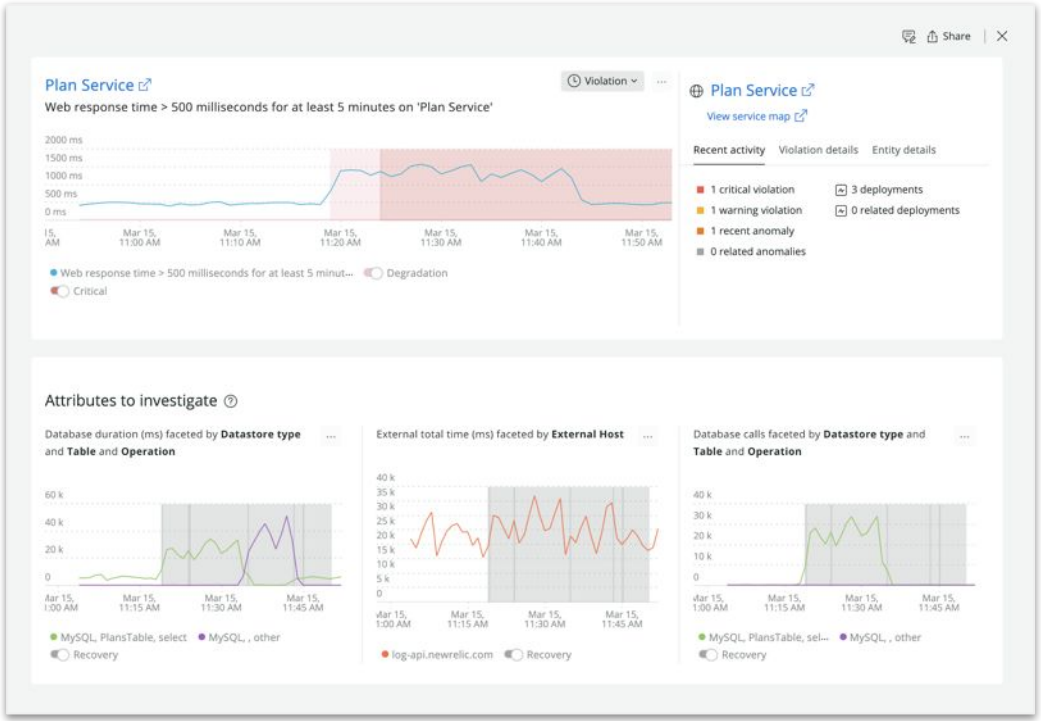
診断

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

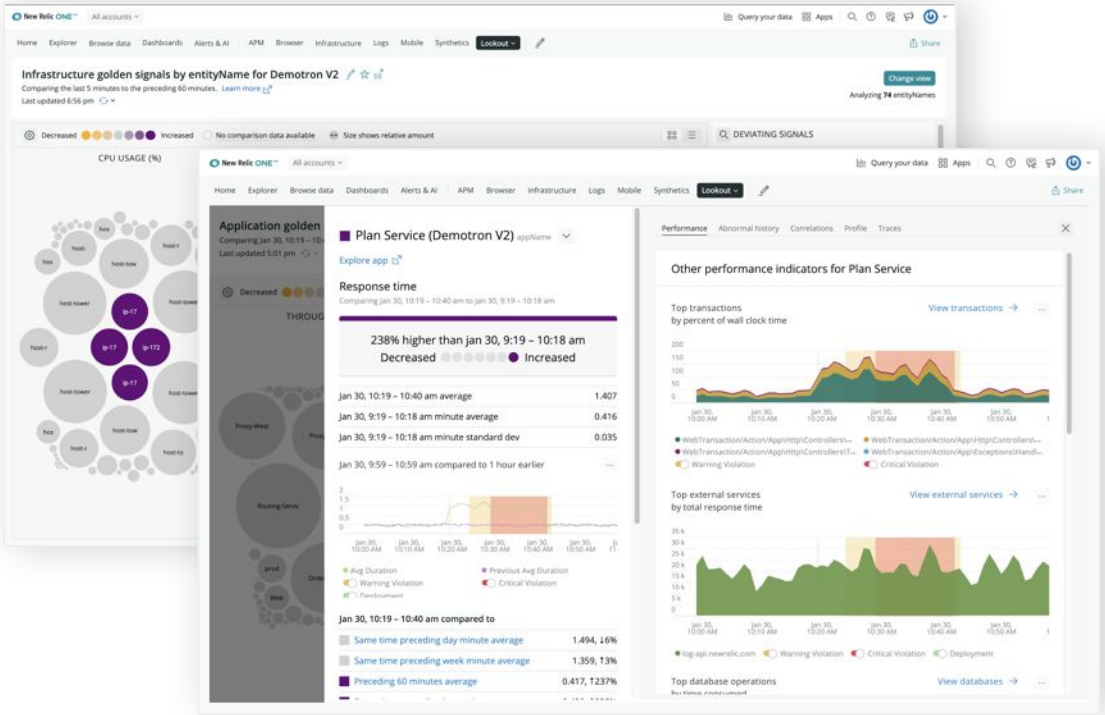
イベントの相関分析

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）

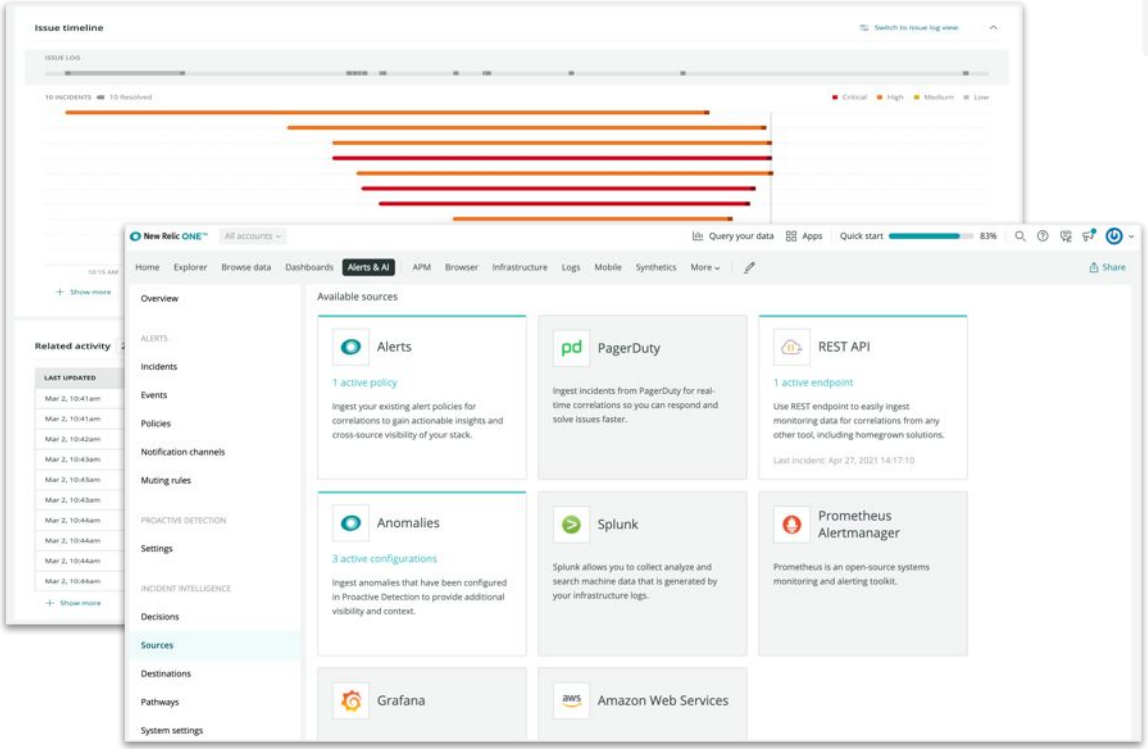
診断

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）

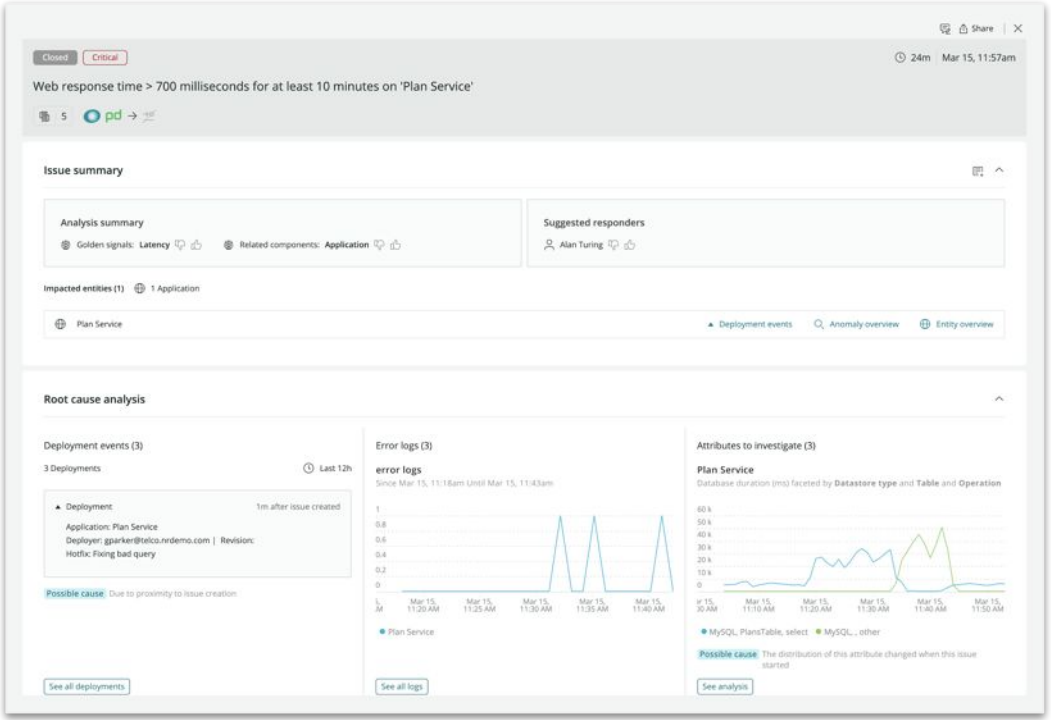
診断

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）

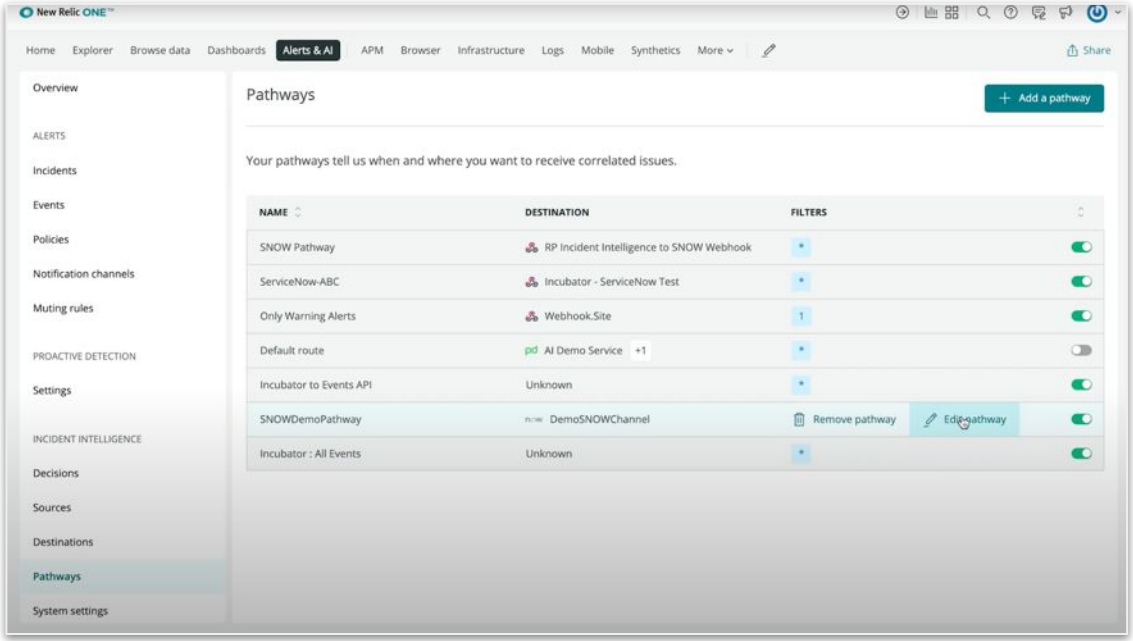
診断

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）

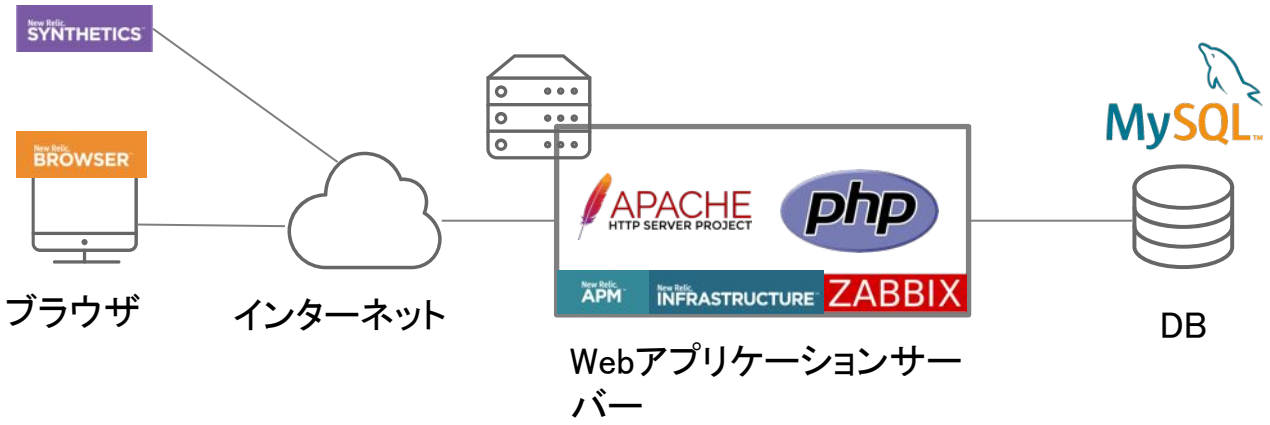


New Relic®

ハンズオン(3)
AIOpsを使った異常検知と原因分析(後編)

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



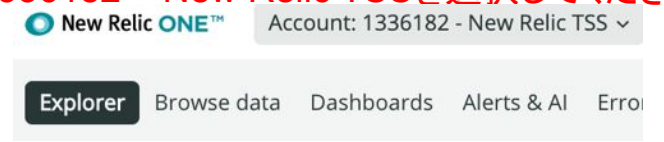
ハンズオン(3)

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、画面左上のアカウント選択メニューから
Account: 1336182 – New Relic TSSを選択してください



ハンズオン(3)

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(3)

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

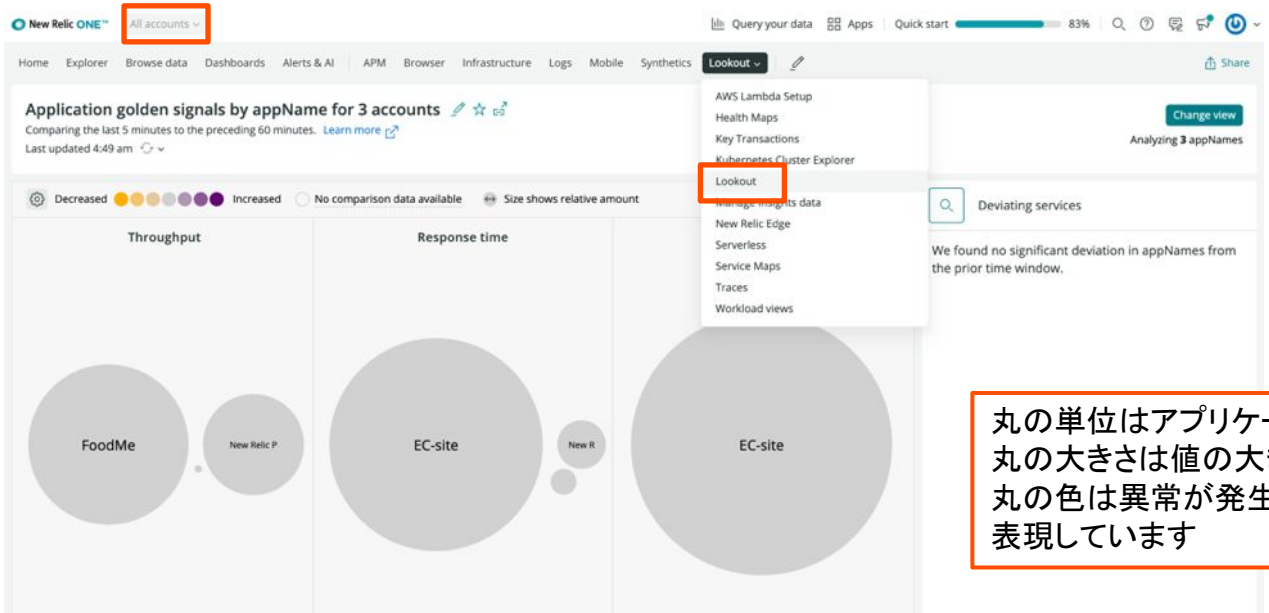
New Relic®

手順・解説

ハンズオン(3)　15min

ハンズオン(3)異常を可視化する

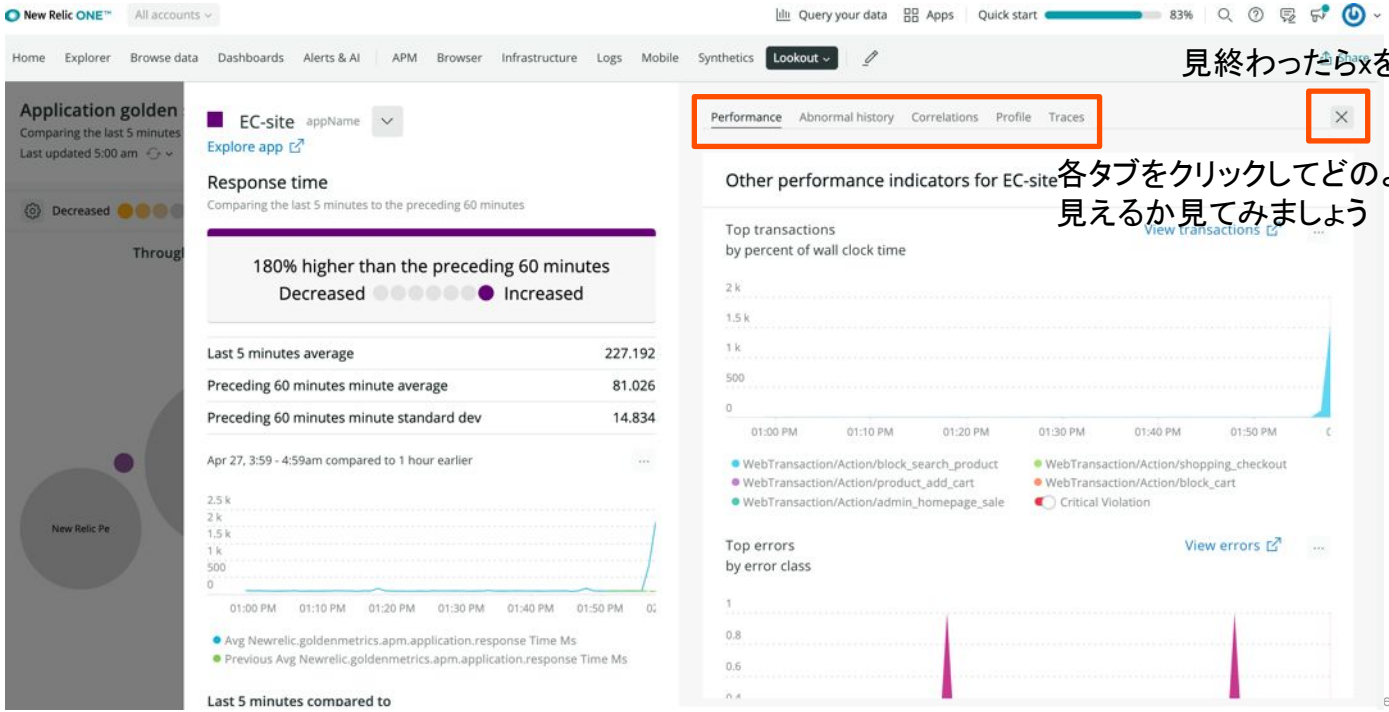
- 画面左上のアカウント選択メニューからAccount: 1336182 – New Relic TSSを選択
- トップメニューの「More」->「Lookout」をクリックし、現れた画面上でサービスの現状を読み解きましょう



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(3)異常を可視化する

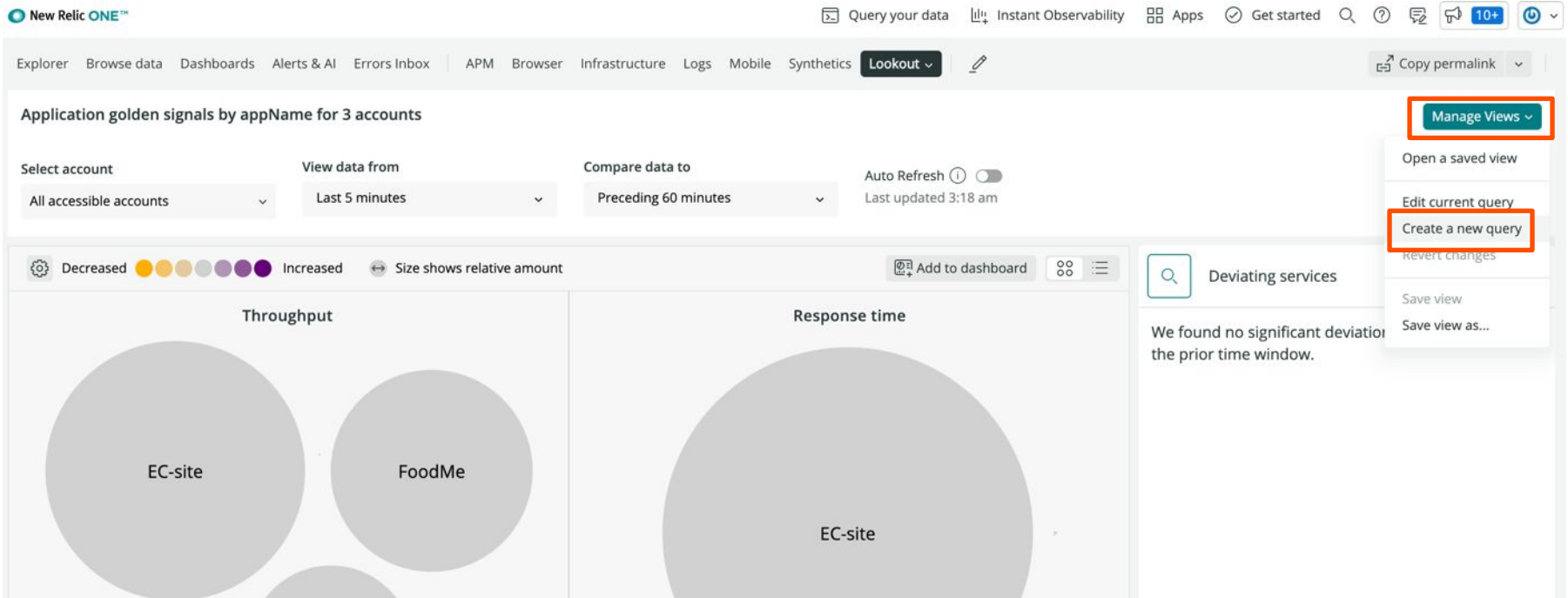
- 気になる○(丸)を選択し、どのような変化が生じているか、詳細を確認します



ハンズオン(3)異常を可視化する

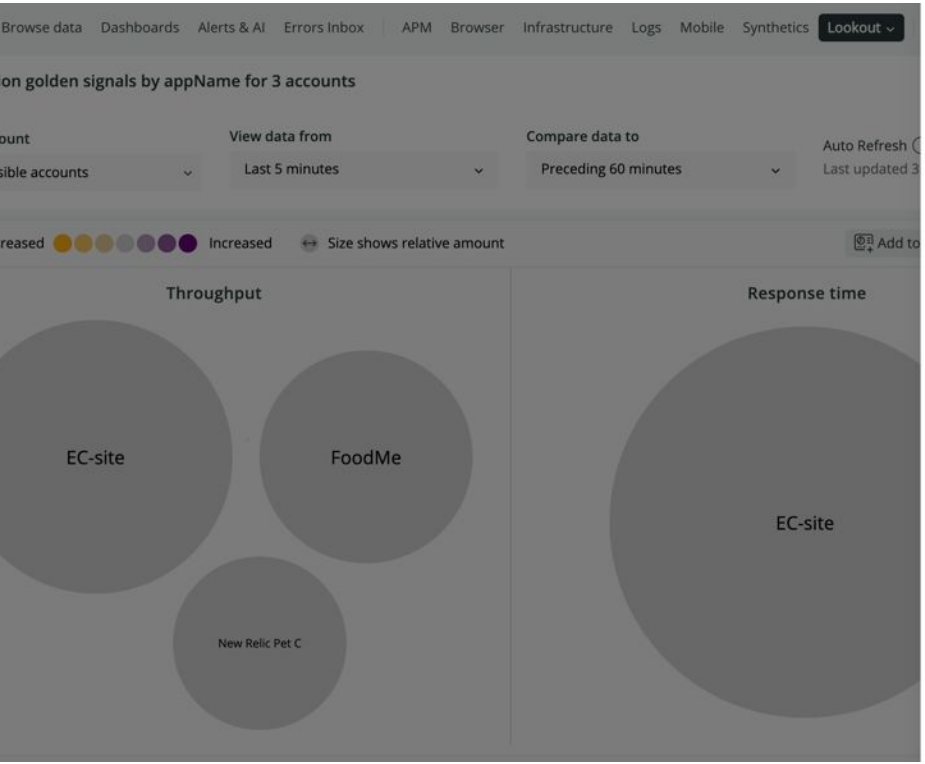
- カスタムのビューを作成します

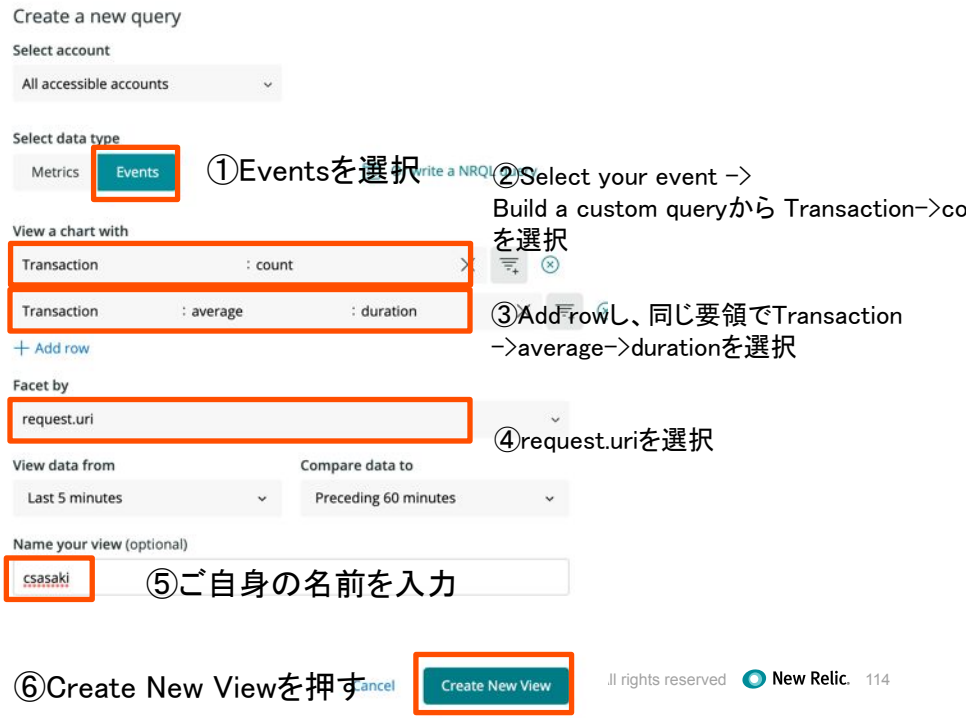
Manage Views -> Create a new queryを選択



ハンズオン(3)異常を可視化する

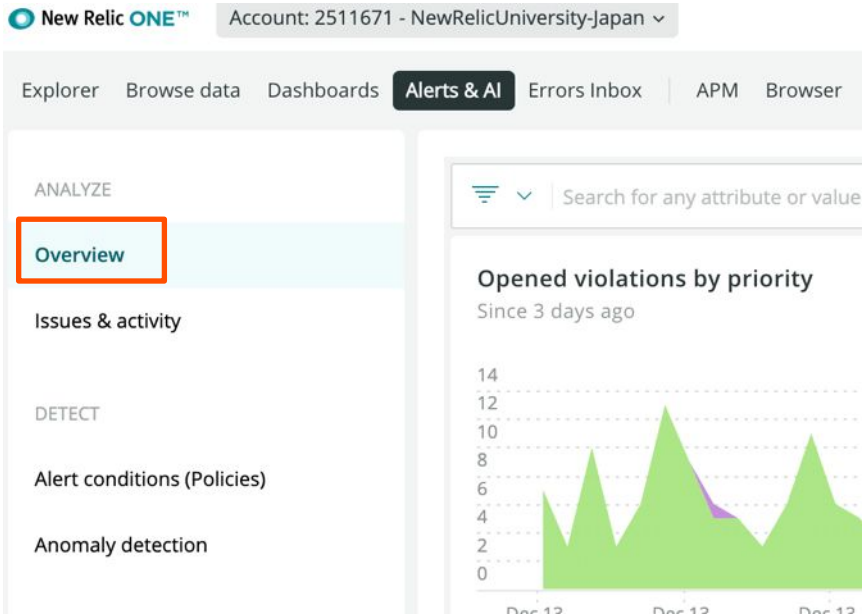
- カスタムのビューを作成します(続き)。作成後の画面から詳細分析ができます。
  この手順によりアクセス先URLごとでのレスポンスの多さと速さの大きさ、変化率が可視化できます。





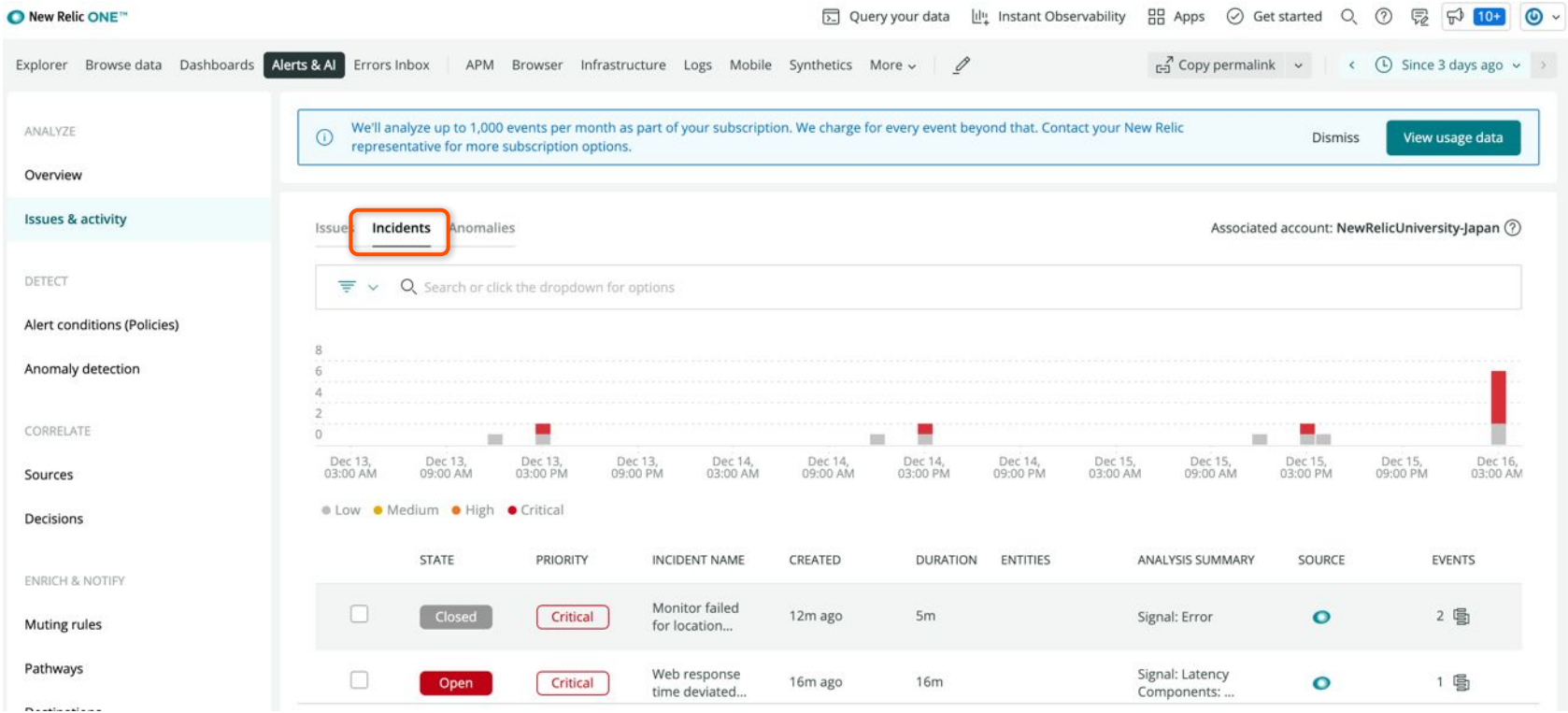
ハンズオン(3)個々のアラートを確認する

- Alerts&AIに戻り、画面左上のアカウント選択メニューから Account:2511671 NewRelicUniversity-Japanを選択
- 「Overview」をクリックします



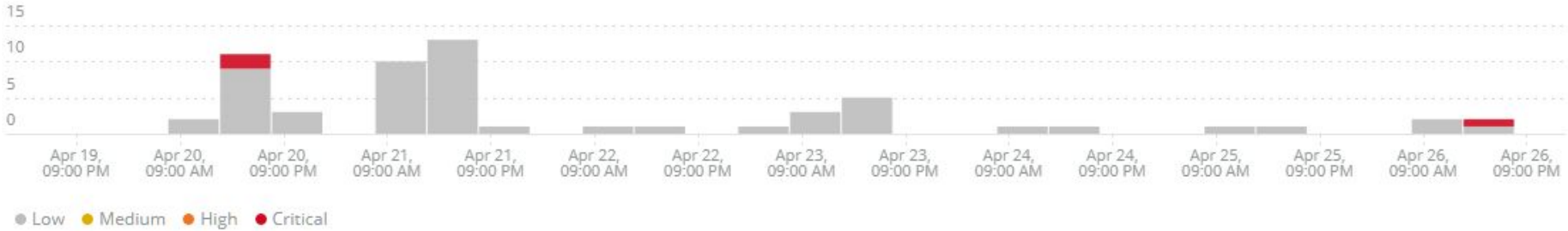
ハンズオン(3)個々のアラートを確認する

- 「Incidents」タブをクリックします。



ハンズオン(3)個々のアラートを確認する

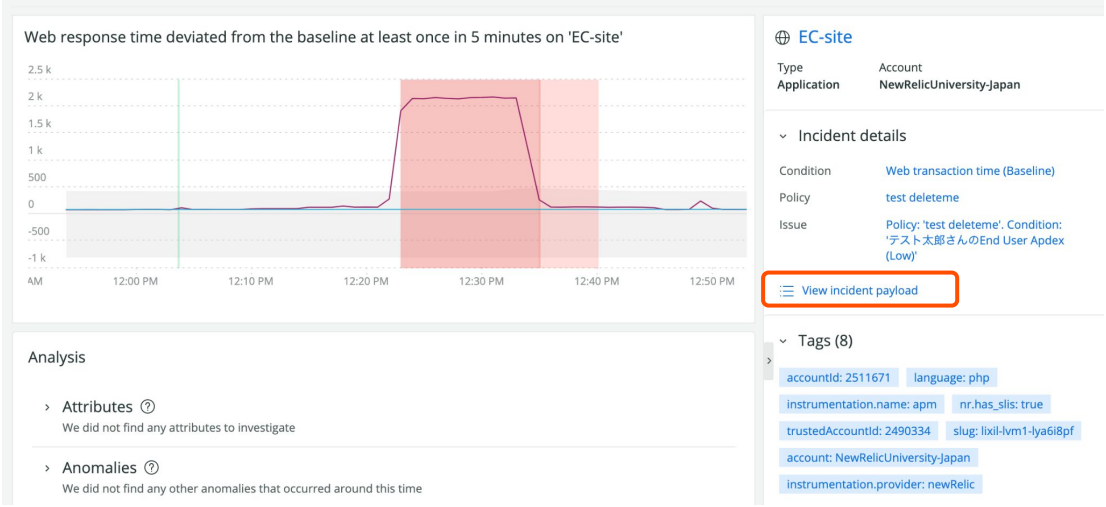
- 個々のIncidentをクリックします。



STATE	PRIORITY	INCIDENT NAME	CREATED	DURATION	ENTITIES	ANALYSIS SUMMARY	SOURCE	EVENTS
Closed	Low	[PROBLEM] Load average is too...	4h 49m ago	14m				2
Closed	Critical	Web response time > 2 secon...	4h 50m ago	12m	EC-site	Signal: Latency Components: ...		2
Closed	Low	[PROBLEM] ip-172-31-26-...	7h 30m ago	9m				2
Closed	Low	[PROBLEM] High	9h 5m ago	1m				2

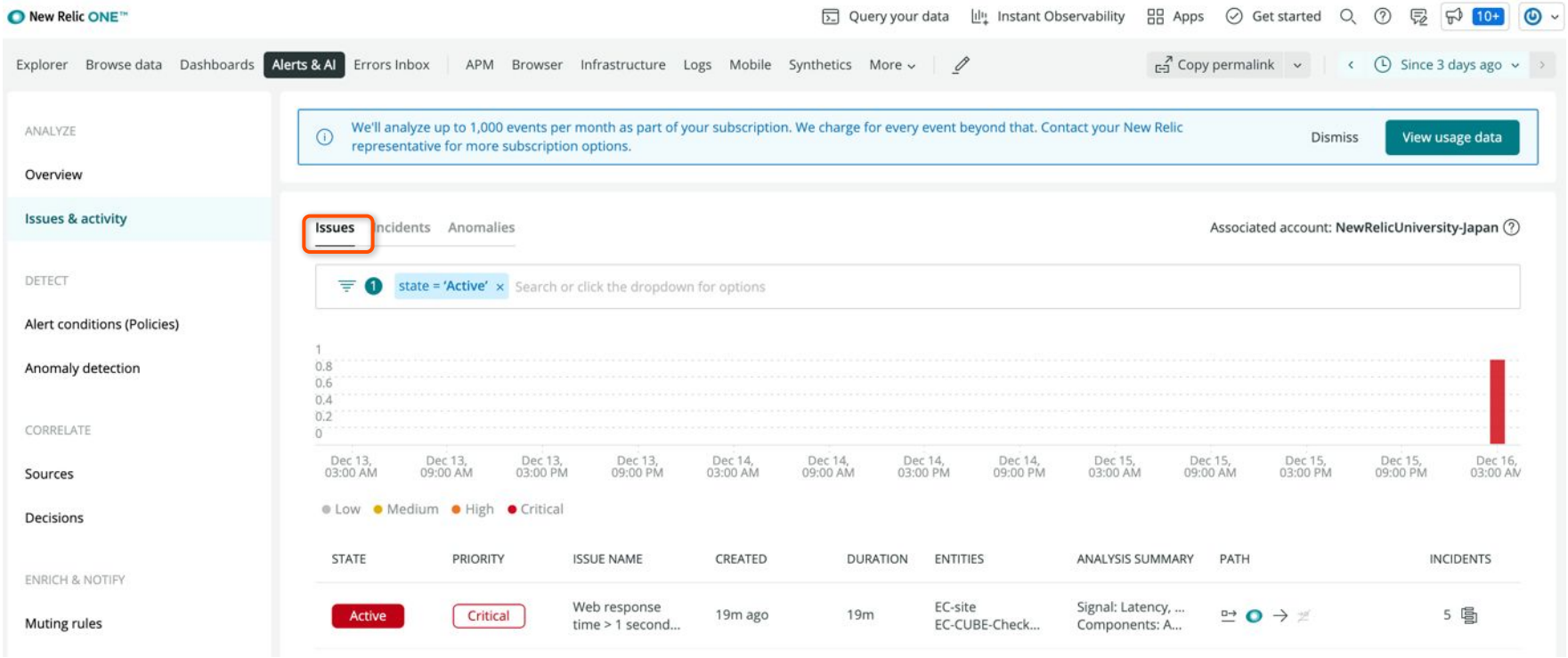
ハンズオン(3)個々のアラートを確認する

- 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。



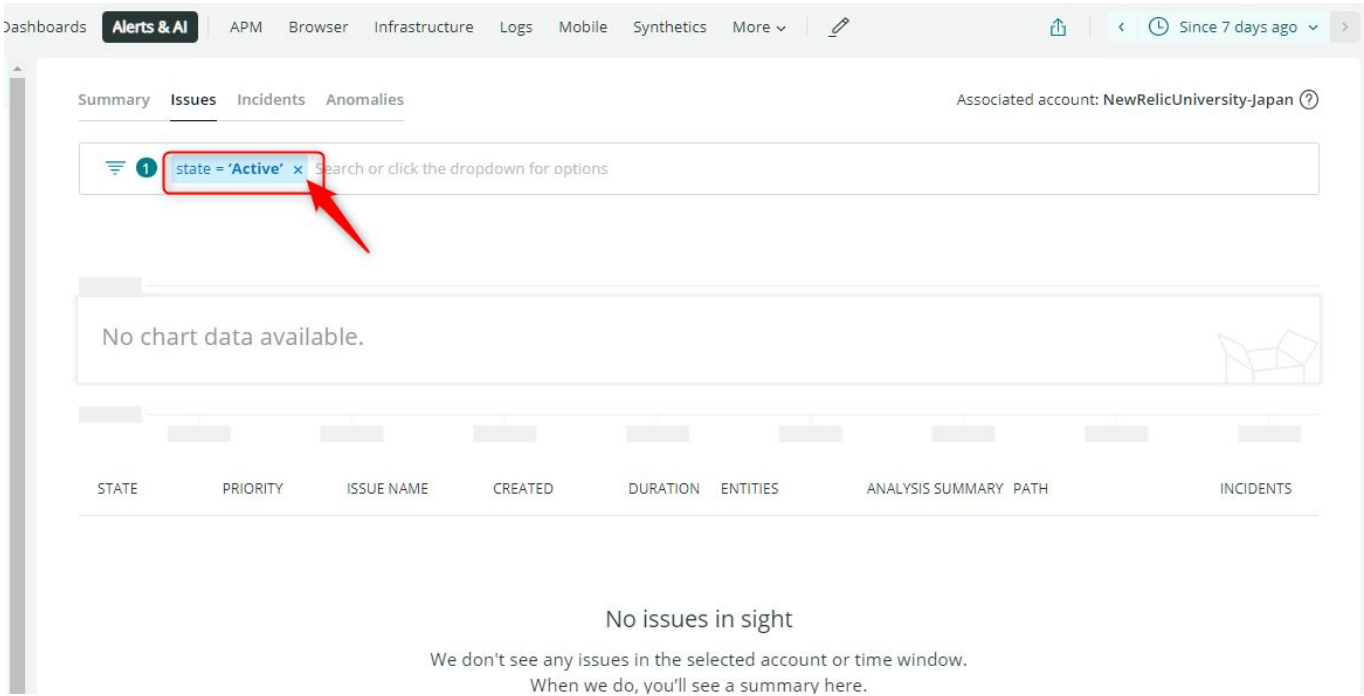
ハンズオン(3)複数のアラートを紐付け、トラブルシューティングに役立てる

- 「Issues」タブをクリックします。



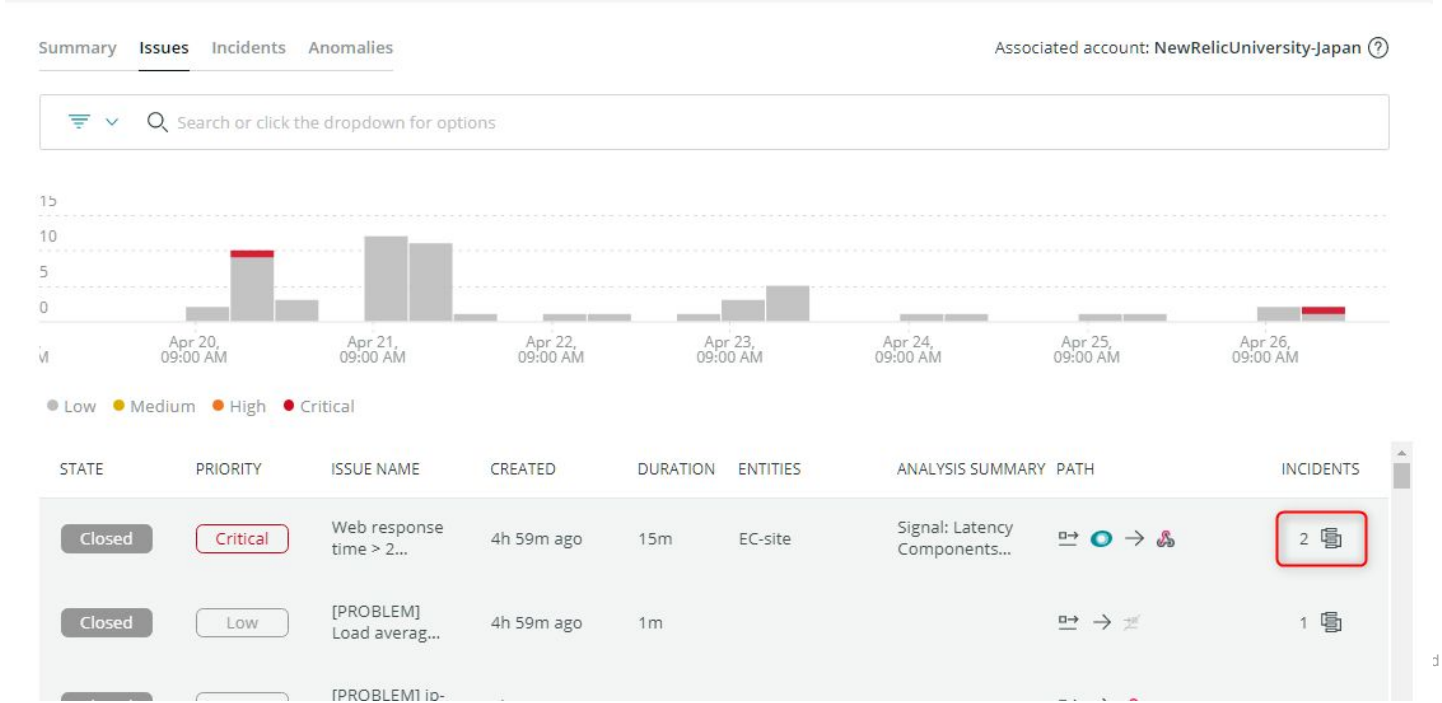
ハンズオン(3)複数のアラートを紐付け、トラブルシューティングに役立てる

- 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。



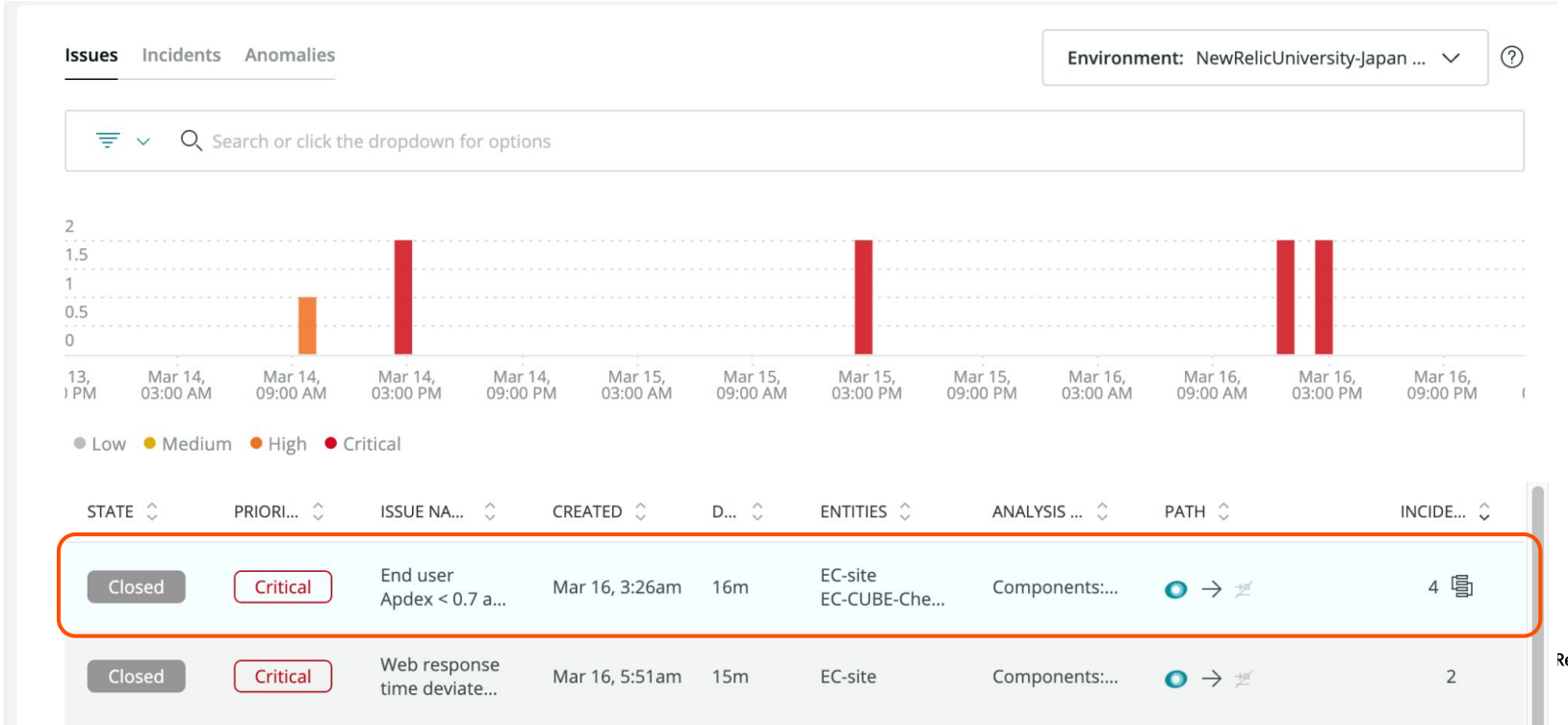
ハンズオン(3)複数のアラートを紐付け、トラブルシューティングに役立てる

- 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。

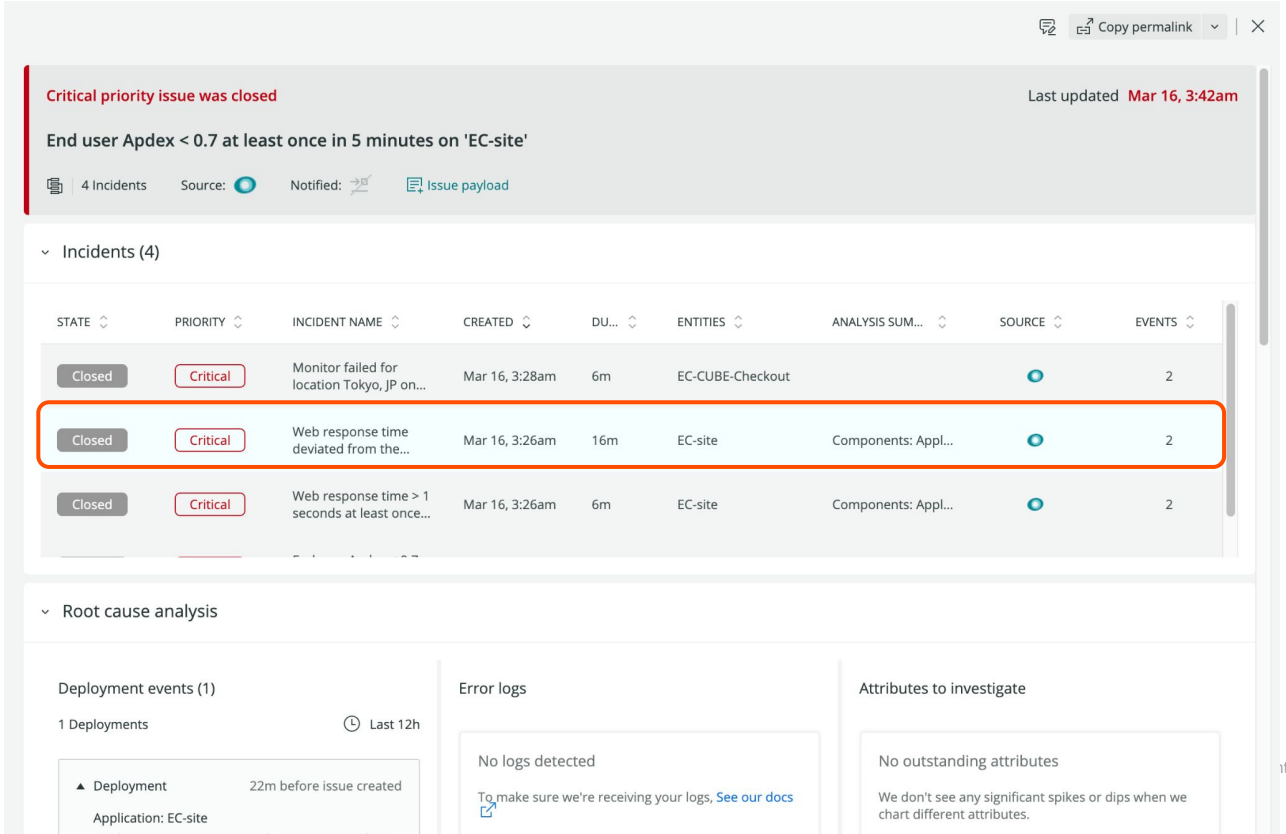


ハンズオン(3)複数のアラートを紐付け、トラブルシューティングに役立てる

- Issueをクリックすると詳細が表示されます。

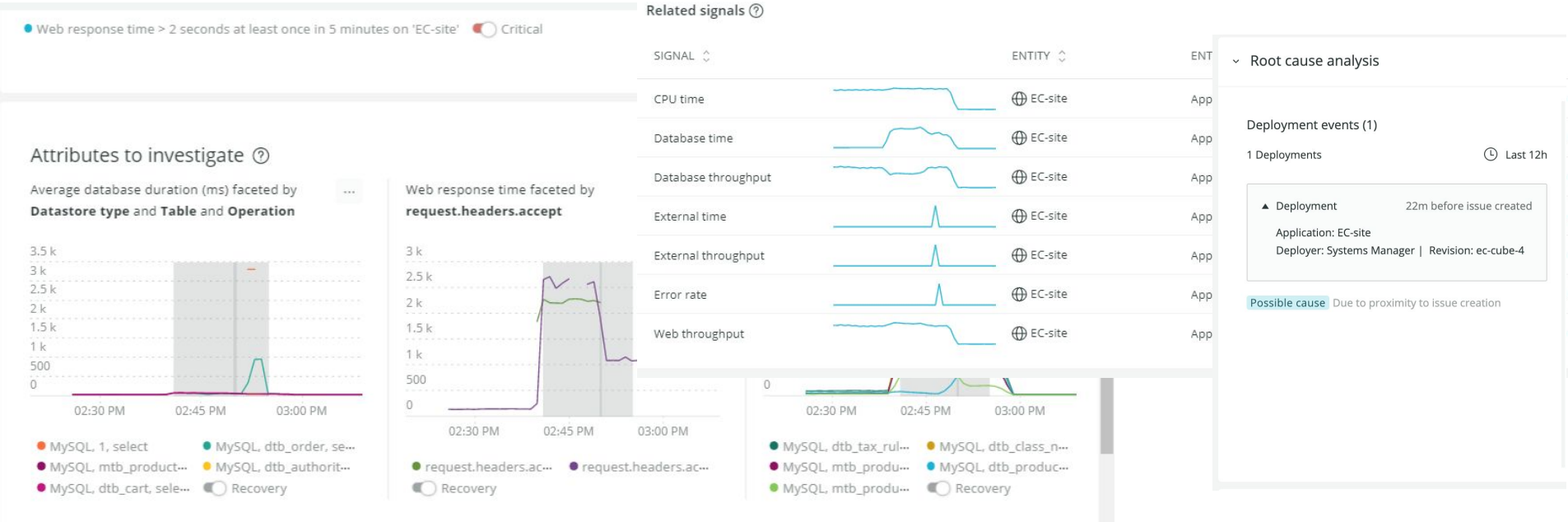


ハンズオン(3)複数のアラートを紐付け、トラブルシューティングに役立てる



ハンズオン(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

- さらにAnalyzeからNew Relci上のデータを分析することができます。

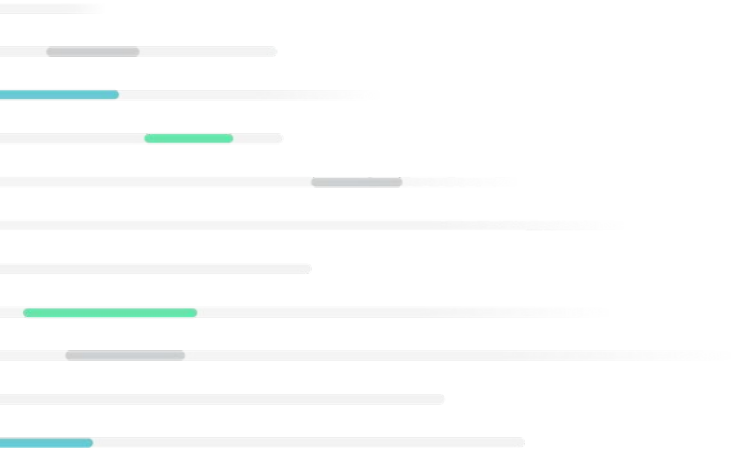


以上、お疲れさまでした

ご質問があればチャットにご記入ください

最後に

- アンケートへのご協力をお願いします！
  - もっと詳しい話を聞きたい方は、その旨アンケートにご記載ください



Thank You

New Relic.