

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

Taku Oguchi Mar 17, 2022

©2008–20 New Relic, Inc. All rights reserved



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)



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)AlOpsの意義
16:10 – 16:25	ハンズオン(2)AlOps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AlOps機能
16:35 – 16:50	ハンズオン(3) AlOps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



ユーザー視点のアラート

©2008–20 New Relic, Inc. All rights reserved

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



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



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

アラートのこれまでと、New Relicを使ったこれから



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の アラート機能

©2008–20 New Relic, Inc. All rights reserved

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

アラートポリ	シー	💮 Incident preference: By condition 🍈 Delete	e this policy
d: 545592			
2 Alert conditions	2 Notification channels	Last modified Feb 7, 4:13 pr	n by Akihiro Ito
Search conditions		⊕ Add	a condition
NFRASTRUCTURE METRIC	Disk Used	Last modified Feb 5, 4:53 pm	Manage
All Entities			
<pre>diskUsedPercent ></pre>	0 for at least 2 mins 0 for at least 2 mins		
PM APPLICATION METRIC	3ASELINE Web transaction throughput (Baselin ^{e)t modified}	d Nov 19, 3:38 pm by Akihiro Ito 🧳 Edit 🗇 Copy 📋 Delet	te On
EC-site \oplus Add entities			
Web transaction th	oughput deviates from baseline for at least 5 mins oughput deviates from baseline for at least 5 mins		

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)

INCIDENT PREFERENCE

Specify how incidents should be created when conditions in this alert policy are violated. (Notifications are sent only when an incident opens, is acknowledged, and closes.)

۲	By policy All violations within this policy will be grouped into a single incident, only one open incident at a time for this alert policy
0	By condition
	All violations within a condition in this policy will be grouped into a single incident; only one incident at a time per alert condition
	By condition and signal
	A unique incident will open for every violation of a condition in this

Learn more about incident preference

Connect to Incident Intelligence

Automatically correlate related incidents and issues to suppress noise, so you only get notified when you need to take action.

* Data is sent to the U.S. for processing.

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



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 <u>https://docs.newrelic.com/docs/alerts-applied-intelligence/new-reli</u> <u>c-alerts/alert-conditions/create-baseline-alert-conditions</u>	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



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

2. Select entities		
3. Define thresholds		
When target application		
Apdex \checkmark	has an apdex score	below \sim
for at least V	5 minutes	
🛆 🕀 Add a warning threshold		
Condition name		
Apdex (Low)		

New condition

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

Apde	ex score	0.88 [0.37] APP SERVER	0.81 [1.7] BROWSER
0.9			
0.85	\sim		
0.8			
0.75	V		
1.4	11:10 AM	11:20 AM	11:30 AM

Application server

Apdex T is the response time threshold value for Apdex. Apdex T is the response time below which a user is satisfied with the experience. The default Apdex T threshold for an application server is 0.5 seconds. Apdex T applies to web transactions only.

Apdex T $_{?}$

0.37 seconds

Please input a decimal or whole number only.

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)





ハンズオン(1) アラートを作成する

30

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。 <u>https://login.newrelic.com/login</u> 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			



手順·解説

ハンズオン(1) 25min

©2008–20 New Relic, Inc. All rights reserved

ハンズオン(1)アラートを作成する

• Alert & Al メニューを開きます。

O New	Relic ONE™ All acc	ccounts ~								lilii Query your	data 🔡 Ap	ops Quick sta	rt 🧲	83% Q 0	2 F 🕗
Home	Explorer Brows	vse data	Dashboard	Is Alerts & Al	APM	Browser	Infrastructure Lo	gs Mobile	Synthetics	More	·	ć	ြ Share	+ Create a workload (i) +	Add more data
₹	entityType = Servi	vice x	Add more fi	lters										E List & Navigator	00 Lookout
YOUF	SYSTEM			Name 🗘			Account 🗘	End User 🗘	Page Vi 🔇)Respon 🗘	Throug 🗘	Error Ra 🗘		Activity stream	▼ Filters ×
000	All entities (318)		ž	7 🔳 EC-site			NewRelic	312.818 ms	···11 page/s	5 79.409 ms	…3 req∕min	0 %		Warning violation closed	10:21 am
⊕	APM/Services (5)		ž	🗧 📕 New Relic	Pet Clinic		New Relic	488.935 ms	1.74 page/s	s 17.314 ms	575 req/min	0 %		EC-site	10.51 am
	Hosts (2)		z	7 🔳 FoodMe			New Relic	1083.486 ms	…94 page∕s	s 10.001 ms	851 req/min	0 %		HttpDispatcher requests_pe deviated from the baseline minutes on 'EC-site'	er_minute for at least 5
\heartsuit	Containers (3)		ž	T = test-001			NewRelic		s	- 0 s	0 req/min	0 %			
	Mobile applications	s (0)	T.	7 ■ ap-001			NewRelic				-	×		Warning violation opened	10:29 am
	Browser applications	ns (3)												HttpDispatcher requests_pe	r_minute
è	Synthetic monitors ((8)	<											minutes on 'EC-site'	
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。

O New Relic ONE™	Account: 2511671 - Nev	vRelicUniversity-Japan 🗸						
Home Explorer	Q, Search		PM Brows	er Infrastru	cture Logs	Mobile Synt	he	
	Most recent							
Overview	NewRelicUniversity-Japan 2511671		rcidents Anomalies					
ALERTS	NewRelicUniversity-Ja New Relic TSS	pan-Dora 3139014 1336182						
Incidents			.r any attribut	e or value.				
Events Policies		Opened violati Since 3 days ago	ons by pric	rity				
Notification channe	els	1 0.8						
Muting rules		0.6 0.4						
PROACTIVE DETECTION	DN	0.2 0						
Settings		Apr 23, 03:00 PM	Apr 23, 09:00 PM	Apr 24, 03:00 AM	Apr 24, 09:00 AM	Apr 24, 03:00 PM	Relic, Inc. All rights reserved	New Relic. 37

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。

O New Relic ONE™ Account: 2511671 - New	RelicUniversity-Japan 🗸
Explorer Browse data Dashboards Alerts	s & Al Errors Inbox APM Browser Infrastructure Logs Mobile Syn
ANALYZE	😇 \vee Search for any attribute or value.
Overview	Opened violations by priority
Issues & activity	Since 3 days ago
DETECT	10 8
Alert conditions (Policies)	°
Anomaly detection	2
CORRELATE	Dec 13, Dec 13, Dec 13, Dec 13, Dec 14, 03:00 AM 09:00 AM 03:00 PM 09:00 PM 03:00 AM

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。

Explorer Browse data Dashboards Ale	rts & Al Errors Inbox APM Browser Infrastructure Logs Mob	le Synthetics More 🗸 🖉			⊡ ⁷ Co	opy permalink 🛛 🗸
ANALYZE	Search policies		(+ New alert polic	y Browse pr	e-built alerts
Overview						
lssues & activity	Policy		Channels 🗘	Open incidents 🗘	Last of the content o	
DETECT	アラートポリシー	2	2	0	Apr 20, 2:01 am	Ŵ
Alert conditions (Policies)	インシデントインテリジェンス	1	0	0	5:52 am	1
Anomaly detection	ダッシュボードハンズオン用アラートポリシー	1	0	0	3:17 pm	Ŵ

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。

Create alert policy

 <u>New Relic アラートの構成要素②通知条件 (続き)</u>を参考に好みの「INCIDENT PREFERENCE」を 選択してください。

LERT POLICY NAME	Give your policy a concise and descriptive name.
	参加著名 アラートポリシー
ICIDENT PREFERENCE	Specify how incidents should be created when conditions in this alert policy are violated. (Notifications are sent only when an incident opens, is acknowledged, and closes.)
	By policy All violations within this policy will be grouped into a single incident; only one open incident at a time for this alert policy
	By condition All violations within a condition in this policy will be grouped into a single incident; only one incident at a time per alert condition
	By condition and signal A unque incident will open for every violation of a condition in this policy
	Learn more about incident preference

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。

iorei browse data basilboari	Aleris & Al	Arm browser initiastructure Logs moune 5	nuneucs more v 2	ЕЗ соруренналик	
nomaly detection	(Search c	hannels		+ New notification channel	
DRRELATE					
ources	Туре	Channel name	 Policy subscriptions 		
cisions	SLACK	NRU-Slack	1	面	
RICH & NOTIFY	USER		0		
ting rules	USER		0		
hways	USER		1		
stinations	USER	NRU-User <japan-handson+2021@newrelic.com></japan-handson+2021@newrelic.com>	0		
TINGS					
eral					
RTS (CLASSIC)					
nts					

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。

Create a new notification channel	Create a new notification channel			
Channel details	Channel details			
Select a channel type	Select a channel type			
select a channel type. \sim	Email V			
🚳 Campfire	Email			
Email	mail@Address.com			
Q HipChat	Include JSON attachment			
OpsGenie Create channel	Cancel Create channel			
od PagerDuty	©2008–20 New Relic, Inc. All rights reserved O New Relic. 42			

ハンズオン(1)アラートを作成する(オプション)

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

参加者名 アラートポリシー	🗌 Connect to Incident Intelligence 🛛 👸 Inciden	「「 1 ハンン - "	-
id: 1214626		Select channels	
10, 1514020		Browse all	
	udd a potification channel to receive alerts	Email ^	
U Notification channels	and a notification channel to receive alerts	HipChat	
		PagerDuty	
		TictorOps	
		C Webhook	
		Campfire	
		Slack	
Add notific	sation channels to this poli	C OpsGenie	
Add Hotine	ation channels to this poli	T xMatters	
Your channels tell us who to not	otify when incidents are opened, acknow	🗁 Users 👻	
	Add notification channels	Cancel Update policy	

ハンズオン(1)アラートを作成する

[再揭]

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。

O New Relic ONE™ Account: 2511	671 - NewRelicUniversity-Japan 🗸 🔟 Query your data 🔡 Apps 🛛 Quick start 💶 🔤
Home Explorer Browse data	Dashboards 🗛 Alerts & Al APM Browser Infrastructure Logs Mobile Synthetics More 🗸 🧷
Overview	参加者名 アラートポリシー Connect to Incident Intelligence 🔅 Incident preference: By
ALERTS	id: 1314626
Incidents	
Events	0 Alert conditions 0 Notification channels (i) Add a notification channel to receive alerts
Policies	
Notification channels	
Muting rules	503
PROACTIVE DETECTION	
Settings	This policy doesn't have any conditions
INCIDENT INTELLIGENCE	Alert conditions are the criteria for creating incidents.
Decisions	Notifications are sent when incidents are created.
Sources	Create a condition ed
Destinations	

New Relic. 46

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。

New condition



(X)

Cance

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。

2. Select a monitor					
Search monitors					
Select:	,	View: /	Al <mark>l</mark> (4)	Selected (1)	Unselected (3)
C EC-Cube-TOP					
C EC-CUBE-Ping					
EC-CUBE-Checkout					
EC-CubeAdministrationPage					
	✓ Back to Name and Cate	gorize		Next, defin	e thresholds

ハンズオン(1)アラートを作成する①

New condition

• 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。

1. Categorize	Synthetics - Single failure
2. Select monitor	1 monitor
3. Define thresholds A violation occurs whenever a monitor fails a check	
Name this condition わかりやすい通知名	
Add runbook URL	

(∞) Cancel

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。

参加者名 アラートポリシー ^{id: 1314626}	Connect to Incident Intelligence 👸 Incident preference: By policy 🔟 Delete this policy	
1 Alert condition 0 Notification channels	Add a notification channel to receive alerts Last modified 7:37 am by NRU-Use	er
 Search conditions SYNTHETICS MONITOR FAILURE わかりやすい通知名 EC-CUBE-Checkout Monitor check failure 	Add a condition Last modified 8:05 am by NRU-User Copy Delete On]

(+) Add a condition

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。

参加者名アラ	ートポリシー	Connect to Incident Intelligence 🎲 Incident prefer	ence: By policy Delete this policy
id: 1314626			
1 Alert condition	0 Notification channels	① Add a notification channel to receive alerts	Last modified 7:37 am by NRU-User
Search conditions			① Add a condition
SYNTHETICS MONITOR FAI	LURE わかりやすい通知名	Last modified 8:05 am by NRU-User	Edit 🖸 Copy 🔟 Delete On
EC-CUBE-Checkout			
🛞 Monitor check failur	re		
			Add a condition

ハンズオン(1)アラートを作成する②

• Categories を設定します。

New condition

NRQL APM Browser Mobile Plugins Synthetics	Infrastructure

 \otimes Cancel

Next, select entities

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。

2. 1 entity selected	
Search browser applications	
Select: All (1) None	View: All (1) Selected (1) Unselected (0)
	< Back to Name and Categorize Next, define thresholds

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。

3. Define thresholds	EC-site \vee
When target browser application	4
End User Apdex \checkmark has an apdex score below \checkmark	
Ø 0.7 at least once in ∨ 5 minutes	0.8
· · · · · · · · · · · · · · · · · · ·	0.6
Add a warning threshold 🕀 🕀	0.4
Condition name	0.2
名前を追記 End User Apdex (Low)	0
	03:00 AM 04:00 AM 05:00 AM 06:00 AM 07:00 AM 08:00 AM
Add runbook URL	• Apdex • Critical threshold • Critical violation
	K Back to Select entities Create condition

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。

2 Alert conditions	0 Notification channels () Add	d a notification channel to receive alerts	Last modified 7:37 am by NRU-User
Search conditions			① Add a condition
APM BROWSER APPLICATIO	N METRIC 名前を追記 End User	r Apdex (Low)	Edit 🖸 Copy 🛍 Delete On
EC-site ① Add entities			
End User Apdex < 0 \triangle \oplus Add a warning the	7 at least once in 5 mins reshold		
SYNTHETICS MONITOR FAIL	URE わかりやすい通知名	Last modified 8:05 am by NRU-User 🧳	Edit 🗇 Copy 🍿 Delete On
EC-CUBE-Checkout			
🛞 Monitor check failur			

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。



Add runbook URL

59

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。
 - ✓ Define your signal

What's possible with NRQ	L Alerting 🗸						
ignal loss violations and fille howing 1/1 time series ⑦	ed data gaps are curren	tly not reflected in the	e chart. See our c	locs 🖓			
.9							
.4					 	<u>.</u>	
.9							
4							
9							
.4							
			^				
0.571							







©2008–20 New Relic, Inc. All rights reserved

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



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





AIOpsのアプローチ

複数の事象を自動で関連付け、



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



ハンズオン(2) AIOpsを使った異常検知 と原因分析(前編)

©2008-20 New Relic, Inc. All rights reserved
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AlOps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のうちーつを選択
 - 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AlOps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AlOps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AlOps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。



手順·解説

ハンズオン(2) 15min

©2008–20 New Relic, Inc. All rights reserved

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。

O New Relic ONE™ Account: 2511671 - N	ewRelicUniversity-Japan 🗸	🕞 Query your data 🔤 Instant Observability 🔡 Apps 🥥 Get start	ed Q @ 💀 🔂 💽 🤇
Explorer Browse data Dashboards	erts & AI Errors Inbox APM Browser Infrastructure Logs M	tobile Synthetics More -	Copy permalink ∽
ANALYZE	アラートポリシー	Connect to Incident Intelligence 💮 Incident preference: By cond	ition 👘 Delete this policy
Overview	id: 545592		
Issues & activity	2 Al us on distance 2 Matification shapped	Last modif	ied Feb 7, '20 7:13 am by Akihiro Ito
DETECT	2 Alert conditions 2 Notification channels		
Alert conditions (Policies)	Search conditions		\oplus Add a condition
Anomaly detection	ADM ADDUCATION METDIC DASSURE MALL AND A	Laet modified Mar 30, 3:05 am by Akihiro Ito 🖉 Edit	Copy in Delete
CORRELATE	EC-site	on throughput (Baseline)	
Sources		for a bread for all an	
Decisions	Web transaction throughput deviates from baseline	for at least 5 mins	
ENRICH & NOTIFY			
Muting rules	INFRASTRUCTURE METRIC Disk Used	Last modifi	ed Feb 5, '20 7:53 am Manage
Pathways	All Entities		
Destinations	kUsedPercent > 90 for at least 2 mins		
CETTINPE	Aiski IsedPercent > 70 for at least 2 mins		d

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。

O New Relic ONE	Account: 2511671 - NewRelicUniversity-Ja	ipan ~		E Q	uery your data 네냐 Instant Observability	🗄 Apps ⊘ Get s	tarted O 🕜	R R 10+ (e	
Explorer Browse d	data Dashboards Alerts & Al Errors In	box APM Browse	r Infrastructure L	ogs Mobile Synthetics	More - 🏼 🦉	Copy permalink	~ (C) Since 3 days ago 🐱	2	
ANALYZE	Issues Incide	ents Anomalies								
Overview		Q. Search or click the dro	pdown for options							
Issues & activity										
DETECT	8 6 4									
Alert conditions (Po	olicies) 0									
Anomaly detection	Dec 12, 09:00 PM	Dec 13, Dec 13, 03:00 AM 09:00 AM	Dec 13, 03:00 PM	Dec 13, Dec 14, 09:00 PM 03:00 AM	Dec 14, Dec 14, Dec 14, 09:00 AM 03:00 PM 09:00 PM	Dec 15, Dec 15, 03:00 AM 09:00 AM	Dec 15, 03:00 PM	Dec 15, Dec 09:00 PM 03:01		
CORRELATE	Network transition	affic 🧧 Cpu usage								
Sources	STATE	NAME	ENTITY TYPE	SIGNAL		START	DURATION	CONFIGURATION		
Decisions	Open	ip-172-31-26	Host	Cpu usage	111	27m ago	5	Host		
ENRICH & NOTIFY	Open	ip-172-31-26	Host	Cpu usage		27m ago		Host		
Muting rules	Closed	ip-172-31-26	Host	Network traffic		27m ago	12m	Host		
Destinations	Closed	ip-172-31-26	Host	Cpu usage		27m ago	12m	Host	served	O New Relic
									SCIVEU	V new Keit.

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。

New Relic ONE" Account: 2511671 - Ne	ewRelicUniversity-Japan	¥.	
Explorer Browse data Dashboards Ale	erts & Al Errors Inbox	APM Browse	r Infrastructure L
ANALYZE	Issues Incidents	Anomalies	
Overview		earch or click the dro	pdown for options
Issues & activity			
DETECT	8		
Alert conditions (Policies)	0		
Anomaly detection	c 08, Dec 09, 10 PM 09:00 AM	Dec 09, Dec 09:00 PM 09:0	10, Dec 10, 0 AM 09:00 PM
CORRELATE	 Network traffic 	• Cpu usage	
Sources	STATE	NAME	ENTITY TYPE
Decisions	Closed	ip-172-31-26	Host
ENRICH & NOTIFY	Closed	ip-172-31-26	Host
Muting rules			
Pathways	Closed	ip-172-31-26	Host
Destinations	Closed	ip-172-31-26	Host

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。

● New Relic ONE [™] All accounts ~		<u>lılı</u> Quer	ry your data 🔡 Apps 🛛 Quick start 💶 🔤	— 83% 🔍 🕐 🗟 式 🕑 ~
Home Explorer Browse data Dashboa	ards Alerts & Al APM Browser Infrastruct	rure Logs Mobile Synthetics More -	<u>_</u> /	ြံ Share
Overview	3 active sources			•
ALERTS	1 policy connected (1), 1 endpoint	connected 🛛 🔿 3 configurations connected		
Incidents		n.		
Events	Available sources			
Policies				-
Notification channels	O Alerts	pd PagerDuty	(I) REST API	
Muting rules	1 active policy		1 active endpoint	
PROACTIVE DETECTION	Ingest your existing alert policies for	Ingest incidents from PagerDuty for real- time correlations so you can respond and	Use REST endpoint to easily ingest	
Settings	correlations to gain actionable insights and cross-source visibility of your stack.	solve issues faster.	monitoring data for correlations from any other tool, including homegrown solutions.	
INCIDENT INTELLIGENCE			Last incident: Apr 26, 2021 15:00:10	
Decisions			Prometheus	
Sources	Anomalies	Splunk	4 Alertmanager	
Destinations	3 active configurations	Splunk allows you to collect analyze and	Prometheus is an open-source systems	
Pathways	Ingest anomalies that have been configured in Proactive Detection to provide additional	search machine data that is generated by your infrastructure logs.	monitoring and alerting toolkit.	
System settings	visibility and context.			

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。

Associated account: NewRelicUniversity-Japan (?)

New Relic Alerts source When connected policies generate activity, we'll automatically correlate it to filter out noise, add context, and identify issues. You'll get fewer notifications and have more information, so you can solve problems faster.	NEW RELIC IS CONNECTED
POLICIES (1)	+ Add a policy
POLICY 🗘	ACCOUNT 🗘
インシデントインテリジェンス ピュ	NewRelicUniversity-Japan

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。

			Select the New Relic Alerts policie	es you want to connect ⑦				
ccount	All	~	Q Search policies					
					View: A	All (4)	Selected (2)	Unselected
	POLICY 🗘			ACCOUNT NAME 👙				
\checkmark	インシデントインテリジェンス ピ			NewRelicUniversity-Japan				
	アラートポ リシー <u>Ŀ</u> ?			NewRelicUniversity-Japan				
	ダッシュボードハンズオン用アラートポリシー ピ			NewRelicUniversity-Japan				
	参加者名 アラートポリシー ピー			NewRelicUniversity-Japan				

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。



New Relic Alerts source

When connected policies generate activity, we'll automatically correlate it to filter out noise, add context, and identify issues. You'll get fewer notifications and have more information, so you can solve problems faster.

NEW RELIC IS CONNECTED



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。

Explorer Browse data Dashboards	Alerts & Al Errors Inbox APM Browser In
ANALYZE	We'll analyze up to 1,000 events per merepresentative for more subscription o
Overview	100
Issues & activity	
DETECT	
Alert conditions (Policies)	New Relic Alerts sou
Anomaly detection	When connected policies generate a filter out noise, add context, and ide
CORRELATE	and have more information, so you
Sources	
Decisions	

O New Relic ONE™

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。

Anomaly detection settings

We automatically detect anomalies that you can query and add to dashboards. Use this page to adjust which anomalies you see, where you see them, and whether you get notified. For more info or help with querying, see our docs 🖸

Visibility

We display anomalies in the activity stream and Al overview. Use the button below to adjust what you see.

Anomaly visibility preferences

Notifications

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

+ Add a configuration

Q Search configurations

Configuration name 🔅



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。

New Proactive Detection configuration
1. Make this configuration easy to identify 自分名前
2. What account do you want to use?
Account: 2511671 - NewRelicUniversity-Japan 🗸
3. What applications and services do you want to include? (Select up to 1,000)
Q Search in this table
All (1) Selected (1/1) Unselected (0)
Name
EC-site

telic, Inc. All rights reserved **O New Relic.** 90

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。

 Veb throughput Non-web through Error rate 	should we monitor fo Web response time put Von-web response ti	r anomalies?
 Slack 	u want to receive notif re detect to NRDB, which means y Webhook	ications? ou can query them and view them in the anomalies tab.
 6. Do you want Correlate with other ale Cancel 	to correlate anomalie:	s from this configuration? ⑦

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。

Anomaly detection settings

We automatically detect anomalies that you can query and add to dashboards. Use this page to adjust which anomalies you see, where you see them, and whether you get notified. For more info or help with querying, see our docs C³

Visibility

We display anomalies in the activity stream and Al overview. Use the button below to adjust what you see.

Anomaly visibility preferences

Notifications

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

Q Search configurations

Configuration name 💲	Applications 👙	Account 🗘	Last updated 🗘	Destination \Diamond
自分名前	1	NewRelicUniversity-Japan	Apr 26, 2021 7:11pm	
sasaki-test	1	NewRelicUniversity-Japan	Apr 22, 2021 7:16pm	

+ Add a configuration

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。

3 active sources () 2 policies connected (), 1 endpo	int connected () 4 configurations connected	
ilable sources Alerts Catting alert policies for correlations to gain actionable insights and cross-source visibility of your stack.	PagerDuty Ingest incidents from PagerDuty for real- time correlations so you can respond and solve issues faster.	REST API 1 active endpoint Use REST endpoint to easily ingest monitoring data for correlations from any other tool, including homegrown solutions. Last Incident: Apr 26, 2021 15:00:10
Anomalies	Splunk	Prometheus Alertmanager

served 🔘 New Relic. 93

参考 Zabbixの連携

(1) .

• API URLとAPI TokenをコピーしてZabbixに登録します。

Get data from REST API



New Relic Web Collector for REST API https://collectors.signifai.io/v1/incidents	Ê
New Relic Security Token for REST	
Bearer	Ê

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。

	alen_subject	{ALERT.SUBJECT}
Zabbix 5.0	event_id	{EVENT.ID}
٩	event_nseverity	{EVENT.NSEVERITY}
◎ 監視データ ~	event_recovery_status	{EVENT.RECOVERY.STATUS}
·	event_recovery_value	{EVENT.RECOVERY.VALUE}
11. レポート ~	event source	
🔧 設定 🗸	even_source	
管理 ^	event_tags	{EVENT.TAGS}
一般設定	event_time	{EVENT.TIME}
プロキシ	event_update_status	{EVENT.UPDATE.STATUS}
ユーザーグループ	event_value	{EVENT.VALUE}
1-4-	host_name	{HOST.HOST}
メティアタイプ スクリプト	new_relic_bearer	Bearer eyJ0eXAiOiJKV1QiLCJhbGci
≠ 2 −	new_relic_proxy_url	
ባ ታ ポート	Dew relic url	https://collectors.signifai.jo/v1/inciden
Share		inspendenterer er ginnande er medeen
? ヘルプ	urgency_for_average	2
▲ ユーザー設定	urgency_for_disaster	1
<u> </u>	urgency_for_high	2

-

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。

ン 実行内容				
ルトのアクション実行ステップの間隔	1h			
シテナンス中の場合に実行を保留				
実行内容	ステップ 詳細	開始時刻	継続期間	アクション
	ユーザーグループにメッセージを送信: New Relic via New Relic Incident Intelligence 追加	র বর্ণার	標進	変更 削除
復旧時の実行内容	詳細	アクション		
	ユーザーグループにメッセージを送信: New Relic via New Relic Incident Intelligence 追加	変更 削	除	
更新時の実行内容	詳細	アクション		
	ユーザーグループにメッセージを送信: New Relic via New Relic Incident Intelligence 追加	変更 削	除	

ed 🔘 New Relic. 96



New RelicのAlOps機能

©2008–20 New Relic, Inc. All rights reserved

New Relic AlOpsによるインシデント対応フロー



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②: Proactive Detectionによる異常の通知





検知③: Lookoutによる異常の可視化と探索





診断①: Correlationによるアラート統合とノイズの削減





診断②: Correlationによる根本原因の示唆



		嘎 合 Share ×
Control Critical //eb response time > 700 milliseconds for at least 10 minu s c o pd → 100 milliseconds for at least 10 minu	tes on 'Plan Service'	() 24m Mar 15, 11:57am
Issue summary		er ^
Analysis summary ② Golden signals: Latency ゆ ☆ ③ Related components: Applicatio	n 学 ①	I responders the transformation of transformation of the transformation of transformati
Impacted entities (1) 🛞 1 Application		
Plan Service		* Deployment events 🔍 Anomaly overview 🕀 Entity overview
Root cause analysis Deployment events (3)	Error logs (3)	Attributes to investigate (3)
3 Deployments ③ Last 12h	errorlogs	
Deployment Im after issue created Application: Plan Service Deployer: graphweit/eliclo.ordemo.com Revision: Horth:: Floring bad query	Concernant 15, 111/Barri Uniti Mar 15, 111/Barri Colore Mar 15, 111/Barri Uniti Mar 15, 111/Barri Uniti Mar 15, 111/Barri Uniti Mar 15, 111/Barri Colore Mar 15, 111/Barri Uniti Mar 15, 111/Barri M	Plan Service Database Hurston (ms) factored by Datastore type and Table and Operation 60 k 50 k 40 k 20 k 20 k
Deployment Im after issue created Application: Plan Service Deploying space-titletics.org Revision: Hoth:: Floing bad query Possible cause: Due to provinity to issue creation	Conservation	Plan Service Database duration (ms) faceted by Datastore type and Table and Operation 60% 40% 40% 40% 40% 40% 40% 40% 40% 40% 4

対処: ITSMツールと連携しアクションを実行



O New Relic ONE**			•) 🖮 部 9、 ⑦	R P () ·
Home Explorer Browse data	Dashboards Alerts & Al APM Browser	Infrastructure Logs Mobile Synthetics More -	9		1 Share
Overview	Pathways			+ Ac	id a pathway
ALERTS	Your nathways tell us when and when	are you want to receive correlated issues			
Incidents	four patiways ten us when and whe	ere you want to receive correlated issues.			
Events	NAME 0	DESTINATION	FILTERS		ċ
Policies	SNOW Pathway	RP Incident Intelligence to SNOW Webhook			
Notification channels	ServiceNow-ABC	🚓 Incubator - ServiceNow Test			
Muting rules	Only Warning Alerts	🚓 Webhook.Site	1		
PROACTIVE DETECTION	Default route	pd Al Demo Service +1	B		
Settings	Incubator to Events API	Unknown			
	SNOWDemoPathway	now DemoSNOWChannel	Remove pathway	🖉 Ediegathway	
INCIDENT INTELLIGENCE	Incubator : All Events	Unknown			
Decisions					
Sources					
Destinations					
Pathways					
System settings					

104



ハンズオン(3)AlOpsを使った異常検知と原因分析(後編)

©2008–20 New Relic, Inc. All rights reserved

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 ● New Relic ONE[™] Account: 1336182 - New Relic TSS ~ Explorer Browse data Dashboards Alerts & Al Error

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



手順·解説

ハンズオン(3) 15min

©2008–20 New Relic, Inc. All rights reserved

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



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

● New Relic ONE [™] All accounts	5 w	🔟 Query your data 🗄 Apps 🛛 Quick start 🛑 💶 \min 🖉 🕄 83% 🔍 🕐 🛒 🕐 🗸
Home Explorer Browse data	Dashboards Alerts & Al APM Browser Infrastructure Logs Mobile	Synthetics Lookout 見終わったらxを押して閉じます
Application golden Comparing the last 5 minutes Last updated 5:00 am \bigcirc ~	■ EC-site appName ∨ Explore app C ² Response time	Performance Abnormal history Correlations Profile Traces Other performance indicators for EC-site各タブをクリックしてどのような情報が
② Decreased ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Comparing the last 5 minutes to the preceding 60 minutes 180% higher than the preceding 60 minutes Decreased Increased	Top transactions by percent of wall clock time 2k 1.5k
	Last 5 minutes average 227.192	1.k
	Preceding 60 minutes minute average 81.026	500
	Preceding 60 minutes minute standard dev 14.834	0 01:00 PM 01:10 PM 01:20 PM 01:30 PM 01:50 PM 01:50 PM C
New Relic Pe	Apr 27, 3:59 - 4:59am compared to 1 hour earlier	 WebTransaction/Action/block_search_product WebTransaction/Action/block_cart WebTransaction/Action/block_cart WebTransaction/Action/block_cart Critical Violation Top errors by error class 1
	 Avg Newrelic goldenmetrics.apm.application.response Time Ms Previous Avg Newrelic goldenmetrics.apm.application.response Time Ms 	0.8
	Last 5 minutes compared to	eserved 🔘 New Relic. 112

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。

rowse data Dashboards Alerts & Al Errors Inbox APM Browser	Infrastructure Logs Mobile Synth	etics Lookout ~			
			Create a new query		
n golden signals by appName for 3 accounts			Select account		
unt View data from	Compare data to	Auto Refresh (All accessible accounts	~	
ble accounts 🔍 Last 5 minutes 🗸	Preceding 60 minutes 🗸 🗸	Last updated 3	Select data type		
			Metrics Events	①Eventsを選択 ^{rite a} NR	୍2Select vour event ->
eased 🌒 🌒 🌒 🌒 🌒 🛑 Increased 🛛 🖶 Size shows relative amount		₫ Add to			Build a custom queryから Transaction->c
Throughput	Res	ponse time	View a chart with		を選択
			Transaction	: count >	≂₊ ⊗
			Transaction : aver	rage : duration	③Add rowし、同じ要領でTransaction
			+ Add row		->average->durationを選択
EC-site EoodMe			Facet by		
roodivie			request.un		④request.uriを選択
	1	EC-site	View data from	Compare data to	
			Last 5 minutes	 Preceding 60 minutes 	*
			Name your view (optional)		
New Relic Pet C			csasaki (5)ご	自身の名前を入力	
					Il rights reserved New Relic 114
			GUreate New	VIEWを押 fancel Creat	

ハンズオン(3)個々のアラートを確認する

- Alerts&All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。

O New Relic ONE™					▶ Que	ery your data 📗	1 Instant Ob	servability	∃ Apps ⊘ G	et started Q	0 2	F) <u>10+</u>
Explorer Browse data Dashboards	Alerts & Al Errors	Inbox APM	Browser Inf	rastructure Logs Mob	ile Synthetics	More 🗸 🖉		G	P Copy permali	nk 🗸 🤇	Since 3	days ago 🐱
ANALYZE	We'll a repres	nalyze up to 1,00 entative for mor	00 events per mo e subscription op	nth as part of your subscritions.	ption. We charge f	or every event bey	ond that. Con	tact your New R	Relic	Dismiss	View us	age data
Overview	-											
Issues & activity	Issues Inc	idents Anoma	lies						Associat	ed account: Ne	wRelicUniversi	ty-Japan ⑦
DETECT	₹ ~	Q Search or c	lick the dropdow	n for options								
lert conditions (Policies)												
Anomaly detection	8											
ORRELATE	4											
Sources	Dec 13, 03:00 AM	Dec 13, 09:00 AM	Dec 13, 03:00 PM	Dec 13, Dec 14, 09:00 PM 03:00 AM	Dec 14, 09:00 AM	Dec 14, 03:00 PM	Dec 14, 09:00 PM	Dec 15, 03:00 AM	Dec 15, 09:00 AM	Dec 15, 03:00 PM	Dec 15, 09:00 PM	Dec 16, 03:00 AM
Decisions	● Low ● M	/ledium 🥚 High	• Critical									
		STATE	PRIORITY	INCIDENT NAME	CREATED	DURATION	ENTITIES	ANA	LYSIS SUMMARY	SOURCE	EV	ENTS
Muting rules		Closed	Critical	Monitor failed for location	12m ago	5m		Sign	nal: Error	0	2	6
Pathways		Open	Critical	Web response	16m ago	16m		Sign	nal: Latency	0	1	5
De alle alle a		1.0		- une deviated				CON	inponents			

i**c.** 116

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。



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。



• 「Issues」タブをクリックします。

O New Relic ONE™					S. Query	your data <u>네</u> 晴 I	nstant Observability	🗄 Apps 🥥	Get started O	0 2	≓ <u>10+</u> @ ·
Explorer Browse data Dashboards Aler	ts & Al Errors Inbox	APM Brow	wser Infrastructure I	Logs Mobile	Synthetics Mor	re v 🖉		Copy perma	link v 🗸	C Since 3	days ago 🐱 🔿
ANALYZE	() We'll analyze representation	e up to 1,000 even ive for more subsc	ts per month as part of y ription options.	our subscriptior	n. We charge for e	very event beyond	d that. Contact your Ne	w Relic	Dismis	s View us	age data
Overview											
Issues & activity	Issues	s Anomalies						Associa	ited account: Ne	wRelicUniversit	ty-Japan 곗
DETECT	Ţ 1 state	e = 'Active' × Sea	rch or click the dropdow	n for options							
Alert conditions (Policies)											
Anomaly detection	1 0.8 0.6 0.4										
CORRELATE	0.2										
Sources	Dec 13, 03:00 AM 0	Dec 13, De 9:00 AM 03:0	c 13, Dec 13, 00 PM 09:00 PM	Dec 14, 03:00 AM	Dec 14, 09:00 AM	Dec 14, 0 03:00 PM 09	Dec 14, Dec 15, 9:00 PM 03:00 AM	Dec 15, 09:00 AM	Dec 15, 03:00 PM	Dec 15, 09:00 PM	Dec 16, 03:00 AN
Decisions	🛛 Low 😑 Mediu	m 😐 High 🖷 Cri	tical								
ENRICH & NOTIFY	STATE	PRIORITY	ISSUE NAME	CREATED	DURATI	DN ENTITIES	ANALYSIS S	UMMARY PATH		INC	IDENTS
Muting rules	Active	Critical	Web response time > 1 second	19m ago	19m	EC-site EC-CUBE-C	Signal: Late heck Componer	ency,	$ ightarrow \not\cong$	5	

• 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。

- E	ale = Active x	Search or click the d	ropdown for optio	ns		
No char	t data avail	able.				
STATE	PRIORITY	ISSUE NAME	CREATED	DURATION ENTITIES	ANALYSIS SUMMARY PATH	INCIDENTS



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。



• Issueをクリックすると詳細が表示されます。



Critical priority	y issue was close dex < 0.7 at lea	d st once in 5 minutes o	on 'EC-site'				Last updat	ted Mar 16, 3:42am
⑤ 4 Incidents	Source: 🔘	Notified: 📌 🔲 🗐	ue payload					
 Incidents (4) 	4)							
STATE 🗘	PRIORITY 🗘	INCIDENT NAME	CREATED 🗘	DU 🗘	ENTITIES 🗘	ANALYSIS SUM 🗘	SOURCE 🗘	EVENTS 🗘
Closed	Critical	Monitor failed for location Tokyo, JP on	Mar 16, 3:28am	6m	EC-CUBE-Checkout		ο	2
Closed	Critical	Web response time deviated from the	Mar 16, 3:26am	16m	EC-site	Components: Appl	0	2
Closed	Critical	Web response time > 1 seconds at least once	Mar 16, 3:26am	6m	EC-site	Components: Appl	0	2
		5 · · · · · · · · · · · · · · · · · · ·						
[,] Root cause	analysis							
Deployment	events (1)		Error logs			Attributes to inve	estigate	
1 Deployments		Last 12h						
Deployment 22m before issue created Application: EC-site			No logs detec	ted e're receiving	your logs, <mark>See our docs</mark>	No outstandin We don't see any chart different at	ig attributes y significant spikes or ttributes.	r dips when we

eserved 🔘 New Relic. 123

🕞 📑 Copy permalink 🗸 🛛 🗙

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

