NRU 304 「アラート設計の 基本と活用」

Nov 20, 2024



New

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。





Safe Harbor

This presentation and the information herein (including any information that may be incorporated by reference) is provided for informational purposes only and should not be construed as an offer, commitment, promise or obligation on behalf of New Relic, Inc. ("New Relic") to sell securities or deliver any product, material, code, functionality, or other feature. Any information provided hereby is proprietary to New Relic and may not be replicated or disclosed without New Relic's express written permission.

Such information may contain forward-looking statements within the meaning of federal securities laws. Any statement that is not a historical fact or refers to expectations, projections, future plans, objectives, estimates, goals, or other characterizations of future events is a forward-looking statement. These forward-looking statements can often be identified as such because the context of the statement will include words such as "believes," "anticipates," "expects" or words of similar import.

Actual results may differ materially from those expressed in these forward-looking statements, which speak only as of the date hereof, and are subject to change at any time without notice. Existing and prospective investors, customers and other third parties transacting business with New Relic are cautioned not to place undue reliance on this forward-looking information. The achievement or success of the matters covered by such forward-looking statements are based on New Relic's current assumptions, expectations, and beliefs and are subject to substantial risks, uncertainties, assumptions, and changes in circumstances that may cause the actual results, performance, or achievements to differ materially from those expressed or implied in any forward-looking statement. Further information on factors that could affect such forward-looking statements is included in the filings New Relic makes with the SEC from time to time. Copies of these documents may be obtained by visiting New Relic's Investor Relations website at ir.newrelic.com or the SEC's website at www.sec.gov.

New Relic assumes no obligation and does not intend to update these forward-looking statements, except as required by law. New Relic makes no warranties, expressed or implied, in this presentation or otherwise, with respect to the information provided.



本セッションのゴール

- New Relicの収集データを活用したアラート設定手順を理解
 ユーザー体験に近い指標に基づいたアラート設定を体験
- New Relicのアラート対応を効率化する方法を理解する



本セッションの想定対象者と前提条件

[対象者]

- 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、あるいは、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

[前提条件]

- 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)

- <u>New Relicの基礎</u>
- <u>ダッシュボードワークショップ</u>(NRQL入門編に相当)
- <u>NRQL reference</u>(公式ドキュメント)



タイムテーブル

時間(目安)	内容	
15:00-15:15	座学(1)	ユーザー視点のアラート
15:15-15:30	座学(2)	New Relicのアラート機能
15:30-15:40	ハンズオン (0)	環境を確認する
15:40-16:00	ハンズオン (1)	アラートポリシー・ワークフローを作成する
16:00-16:20	座学(3)	アラートコンディションの作成
16:20-16:35	ハンズオン (2)	アラートコンディションを作る
16:35-16:45	ハンズオン (3)	発生したアラートの確認
16:45-16:55	座学(4)	New Relicのアラート分析支援機能を使った異常検知
16:55-17:00		まとめ、アンケートご記入



座学**(1)** ユーザー視点のアラート

15:00 - 15:15 (15min)



new relic

© 2024 New Relic, Inc. All rights reserved.

突然ですが、、、 どんなアラート設定していますか?





アラートを設定する目的

対象システムが、何らかの対応が必要な状態であることの通知を受け取るため

1. システムの停止、またはパフォーマンスの悪化が発生

→ ユーザーへのサービス提供に支障が出ている

2. 1のような事象が近いうちに発生する兆候が出ている

<u>"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ト "</u>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



New relic. ¹³



© 2024 New Relic, Inc. All rights reserved.

New relic. 14

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



目的別のアラート設定例(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	応答時間	チェックエラー		
フロントエンド	CWV	JSエラー		
サーバーサイド	応答時間	4xx, 5xxエラー	スループット バッチ遅延	
インフラ				各種インフラ リソース



座学(2) New Relicのアラート機能

15:15 - 15:30 (15min)

© 2024 New Relic, Inc. All rights reserved.

New Relicのアラート機能

New Relicがリアルタイムに**収集しているデー タ**を使って、アラートを設定可能

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、通知を受信可能

*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ます

Critical Issue activated on Aug 13, 2023 1:49pm	Duration: 21h 53m Last updated Aug 14, 2023 10:47ar
C-site query result is > 1.0 for 5 minut	tes on 'Alert Condition ' Close Issue Acknowledge
ource: 🕥 🔄 Issue payload	
Incidents (16)	
Newest to oldest - Show open only	Critical Incident closed on Aug 14, 2023 10:47am See NRQL overview
	PageView query deviated from the baseline for at least 5 minutes on 'Condition1'
Critical Closed PageView query deviated from the	Alert Policy: ダッシュポ View/edit Condition: Condition View/edit Condition type: NRQL
Created: Today 9:12am	3.5
Critical Closed	
PageView query deviated from the baseline for at least 5 minutes on	2
Created: Today 8:11am 🕒 54m	1.5
Critical Open	0.5
EC-site query result is > 1.0 for 5 minutes on 'Alart Condition'	:00am 9:10am 9:20am 9:30am 9:40am 9:50am 10:00am 10:10am 10:20am 10:30am 10:40am 10:50am
Created: Aug 13, 2023 1:50pm (1) 21h 52m	Tags (11) Show all



New Relicのアラート構造全体像







New Relic アラート基本用語の整理

用語	概要
Alert Policy	 Alert Conditionをまとめて管理するためのグループ
Alert Condition	 アラート対象や閾値、集計方法の定義
Incident	 Alert Conditionで検出した個々の違反
Issue	 1つ以上のIncidentが示す、発生中の問題 実際の通知はIssueに対して行われる
Workflow	 発生したIssueを元にどこに通知するかを定義 実際の送付先はDestinations
Destinations	● メールやSlackなどの通知先





© 2024 New Relic, Inc. All rights reserved.



構成要素1: Alert Policy

New Relic のアラートは、Alert Policyという器にAlert Conditionを内包した構造となっている Alert Policyごとにアラートをグループ化したり、通知先の制御ができる ***通常、送信先やアラートの目的別にポリシーを分けることが多い**

Alert Policy	
Alert Condition (例: フロントエンド)	
Alert Condition (例: DBレスポンス)	
Alert Condition (例:サーバーサイドエラ ー)	
Alert Condition (例:JSエラー)	

NRU-Sample-Policy	✓ ☆ ① Metadata	Workloads V>R	epositories				
Get notified when issues s	tart. To get notifications abo	ut your issues, create a	workflow for this pol	icy. <u>See our docs</u> 🗗		Create wor	rkflow
ID: 4406018							
Alert conditions Notifications	s Settings					- New alert co	ondition
Q Search by condition name	or id	Condition Name = A	+				
Showing 6 conditions							
Alert condition	Query	Thresholds	Туре	Open issues	Last modified	Ena	
EC-site - Ajax throughput	SELECT rate(count(*	Critical: deviated fro Create a warning the	NRQL Baseline	0	Dec 27, 2023, 2:48pm		
EC-site - Throughput (ppm)	SELECT rate(count(*	Critical: deviated fro Create a warning the	NRQL Baseline	0	Dec 27, 2023, 2:48pm		
NRU304-Sample-End Use	SELECT apdex(apm	Critical: below 0.7 at Create a warning the	APM Metric	0	Jun 6, 2023, 4:10pm		
NRU304-Sample-NRQL-Er	SELECT percentage(Critical: above or eq Create a warning the	NRQL Query	0	Jun 6, 2023, 4:39pm		



構成要素1: Alert Policy

Issue Creation Preference

IncidentをIssueにグループ化して、通知をまとめる設定

例)1つのAlert Policyに2つのAlert Conditionを設定し、 その全てがCriticalになった場合

Condition1:フロントエンドのJSエラー率(<u>対象サイトは1つ</u>) Condition2:バックエンドのエラー率(<u>ホスト別に集計</u>、<u>対象ホストは3台</u>)

Incident Grouping

Group incidents within this policy

Tell us how you want to group incidents from this policy into issues. You get notified based on issues, not incidents.

• One issue per policy

One issue per condition

One issue per condition & signal This may create a large number of notifications.

This may create a large number of notifications.

Group with other incidents from other sources

Suppress noise with machine learning correlation (optional)

We'll analyze incidents from all policies and sources and group related incidents into issues. See our docs $\hfill\square$

設定名	Incident発生時の挙動	起票されるIssue
One issue per policy	同じAlert Policy から発生したIncidentを 一つのIssueにまとめる	1件
One issue per condition	同じAlert Conditionから発生した Incidentを 一つの Issueにまとめる	2件(フロントエンドは1件、 バックエンド全体で1件)
One issue per condition and signal	同じConditionであっても、 アラート対象ごとに個別に Issue を作成する	4件 (フロントエンドは 1件、 バックエンドは ホスト毎で3件)





*Issue Opened、Acknowledge、Issue Closedのどこで通知をするかはNotify Whenでカスタム可能



構成要素2: Alert Condition

New Relicが収集しているリアルタイムなデータを、集計・評価する仕組み

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

機能(例. APM, Browser等)ごとに用意されたプリセットから簡単にアラートを作れるほか、 自分でNRQLクエリを記述して、独自の Alert Conditionを作成することも可能

How would you like to do this?	Tell us where to look ①	
Use guided mode Recommended Choose from options and we'll build your query	AWS (4 types)	Browser applications
	C On host integrations (2 types)	🖽 Service Levels
Use NRQL to define your alert	兽 Synthetic monitors	□ VPC Networks

構成要素3: Workflow

発生したIssueと、通知先・通知内容の関連付け

Filter data

どのようなIssueで、このWorkflowを起動するか

Enrich (Additional settings内)

通知に、Issueに関する付加情報を付与する

Mute issues (Additional settings内)

Muting Rulesが設定されていた場合の挙動の設定

Notify (Destinations:後述)

通知先の定義と、通知内容のカスタマイズ

Test workflow

過去の該当データを元に、Workflowの通知テストを実行

Give it a unique, descript	ognize ive name you'll recognize later		
Filter data			
Select the kinds of issue Use the basic filter for th	s you want to send. e most common attributes or the a	dvanced filter for all attributes.	Basic Advance
Tag 🕕	Policy (i)	Priority 🕕	
	v v	v	
Additional settings			
Additional settings Notify Choose one or more des	tinations and add an optional mess	sage.	
Additional settings Notify Choose one or more des Add channel now ServiceNow incidents	tinations and add an optional mess	iage.	Slack
Additional settings Notify Choose one or more des Add channel now ServiceNow incidents Email Email	tinations and add an optional mess Webhook Webhook	sage. Jira	Slack PagerDuty



構成要素4: Destinations

Issueのライフサイクル変化(オープン/クローズ等)の通知を受け取ることができる

シンプルな通知



連携サービスへの通知





構成要素4: Destinations

- <u>Workflows変数や通知メッセージテンプレート</u>を用いて、柔軟に標題や内容をカスタム可能 ※補足: <u>custom incident description</u>とは別の情報付加機能
- "{{ "と入力することで、Workflows変数の補完機能を活用できます

Email	Slack	
Select users and emails you want to send notifications to. See our docs \Box^r Q Search by name or email	Slack destination New Relic ~	Select where you want to receive notifications Pick an existing destination or create a new one. See our docs [2]
Email subject {{ issueTitle }}	Channel Select Channel > Your user is not authenticated	Custom Details (optional)
Custom Details (optional) This payload uses Handlebars syntaxType "{{" to select from a list of variables.	This payload uses Handlebars syntax. Type "{{" to select from a list of variables.	Add a custom message at the bottom of every Slack notification. You can also select from an array of custom variables. Just type "{{" or double-press the Shift key, then select from the menu. You can also customize these variables with a Handlebars library.
Send test notification		Send test notification

Workflows変数: <u>https://docs.newrelic.com/docs/alerts-applied-intelligence/applied-intelligence/incident-workflows/custom-variables-incident-workflows/</u>通知メッセージテンプレート: <u>https://docs.newrelic.com/docs/alerts-applied-intelligence/notifications/message-templates/</u>





ハンズオン(0) 環境を確認する

15:30 - 15:40 (10min)



今回監視対象のサイト

[NRUジェラートショップ](ECサイト)

PHPおよびMySQLにより構築されたジェラート屋さんの ECサイトをモニタリングしています

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





今回の環境の監視構成

New Relicでモニタリング

- Synthetics(外形監視)
- Browser(フロントエンド)
- APM(バックエンド)
- Infrastructure(インフラ)





ハンズオン環境について

New Relic にログインして、 ユーザー名が "New Relic University Japan" であることを確認



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

▼ご注意下さい 普段 New Relic をお使いの方はセッションが残っている場合があります。 下記のいずれかのブラウザのプライベートブラウジングをご利用ください。

- Chrome:シークレットウィンドウ
- Firefox:プライベートウィンドウ
- Edge:InPrivate ウィンドウ



			_	14		
		New Relic University Japan japan-handson+nru@newrelic.com	Ful	l platfor	m user	
		User Preferences				
		Manage Your Plan				
		Administration				
		Theme		Dark		
		NRQL Console			-	
		NR-only admin functionality				
		Impersonate				
		Debug Mode			•	
iscussions		Manage Your Data				
elp	70	Other Lisers				
dd User	_					
ew Relic University J	a	Log Out				
						-

P



ハンズオン(0) UIの確認

- New Relicポータルの左ペインの "APM & Services"を選択し、EC-site アプリを選択します。
- Summaryが選択されていることを 確認します。
- ●表示するデータの表示幅を7 daysに変更します。

同様に、BrowserやInfrastructureを参照してください。







ハンズオン(1) アラートポリシー・ワ クフローを作成する

15:40 - 16:00 (20min)



ハンズオン(1)アラートを作成する

作業内容










ハンズオン(1-1) Alert policyを作成する 1/2

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





ハンズオン(1-1) Alert policyを作成する 2/2

- 右側から設定画面がスライドされてくるので、
 Policy nameには、ご自身が作成したとわかる名前をつけてください
- 5. <u>こちらのスライド</u>を参考に、好みの「Incident Grouping」を選択してください
- 6. [Suppress noise...]をチェック
- 7. [Create & close] をクリックします

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

	Create an alert policy Policies help you organize your alert conditions.						
	Policy name *						
4	Enter a short, descriptive name						
	Incident Grouping						
	Group incidents within this policy						
	Tell us how you want to group incidents from this policy into issues. You get notified based on issues, not incidents.						
5	• One issue per policy						
	One issue per condition						
	One issue per condition & signal						
	This may create a large number of notifications.						
	Group with other incidents from other sources						
6	Suppress noise with machine learning correlation						
	We'll analyze incidents from all policies and sources and group related incidents into issues. See our docs 🖸						
	Create & close Set up notifications						

1 new relic

ハンズオン(1-2) Workflowを作成する 1/6

- AlertsメニューのWorkflowsをクリックし、 [+ Add a workflow]をクリックします
- 2. ご自身のworkflowであることがわかる名前を入力 します
- 3. Filter dataで"Advanced"を選択し、 次のフィルタを設定します
 - a. Select or enter attribute: policyName
 - b. Select operator: exactly matches
 - c. Select or enter value: 作成したポリシーを選択
- 補足:上記3番の設定はBasicでも可能ですが、より柔軟な設定を行う場合には Advancedを活用します。

rze	Alerts				0	🛠 Ask Al 🖉
ssues & Activity	Workflows					
verview						
т	Workflows Issu	ue Notifications Log			11-	
lert Conditions	Set up and customi and how much info	ize your alert notifica rmation they receive	ations. Decide who	gets notified, in wha	t tool, + Add	a workflow
lert Policies	Q Search by wor	rkflow name or email	address +			
ert Coverage G Beta	Showing 1 workflow	vs				
LATE	Name		Destin	Last run	Enabled	
ources	Policy: 4975272	- NRU環境整備				
ecisions	,					
& NOTIFY						
uting Rules						
Vorkflows						
estinations						
100						
NGS						
onfigure your wo RUS04-Workflow e it a unique, descriptive name yo	orkflow will recognize later					
NGS congrad onfigure your wo RUS04-Workflow le it a unique, descriptive name yo iter data	orkflow w11 recognize later			3	Need h	elp?
nos anarat Rusad-Workflow Let a unique, descriptive name yc ter data ect the kinds of issues you want	orkflow will recognize later		0	3 Basic & Advanc	Need h	elp? docs [2]
In Sanaral Configure your we RU304-Workflow It a unique, descriptive name you ter data ter data besic filter for the most com	or send.	ed filter for all attributes	. 0	3 Basic & Advance	Need h Workflow	elp? docs 🖸
anaral onfigure your we RU304-Workflow e it a unique, descriptive name yo ter data tet ha kinds of issues you want the basic filter for the most com comulations policyName ~ (or send. cosend. sector watches watchy matches NRUS044	ed filter for all attributes	. 0	3 Basic & Advance	Need h Workflow	elp? docs 더
ANDS Annoral Configure your wo RU304-Workflow Iter data ect the kinds of issues you want the basis filter for the most com comutations.policyName ~ (- AND)	or send. o send. xxectly matches NRU304-	ed filter for all attributes Policy x	. 0	3 Basic Advance	Need h Workflow	elp? docs ⊠ੈ
NOS tenaral ORDJOA-Workflow le it a unique, descriptive name ye let a data et the kinds of issues you want the basis (file for the most com the basis (file for the most com the basis (file for the most com et basis (file f	orkflow will recognize later on send. mon attributes or the advance watchy matches NRU304-	ed filter for all attributes	. 0	3 Baic Advanc	Need h Workflow	eip? docs [s]
anaral anaral anaral Buildo-Wookflow e it a unique, descriptive name ye ter data ect the kinds of issues you want the basic filter for the most com the basic filter for the most com comutations policyName ~ (- AND) diditional settings	orkflow will recognize later oo send. mon attributes or the advance watchy matches NRU304-	ed filter for all attributes	. 0	3 Basic 🛃 Advanc × Clear filt	Need h Workflow	elp?
INDS anarcal anonfigure your wor UU304-Workflow ter data ter data ter data the basic file role the most cent the basic file role the most cent ter cancel the most c	or send. wattroaction and second watchy matches INRU304-	ed filter for all attributes	. 0	3 Baic 💩 Advanc	ed Workflow ers Destination	elp? docs [c ² m Docs [c ²
ANDS configure your work Buildow-Wookflow Iter data et the kinds of issues you want. the basic fifter for the most com the basic fifter for the basic	orichflow with recognize later original original original with advance with advance with advance with advance with advance with advance with advance with advance with advance with advance distribution with advance distribution with advance distribution with advance distribution with advance distribution distribut	ed filter for all attributes	. 0	3 Baic & Advanc × Clear filt	ed Workflow err. Destinati Manage o	eip? docs [s] m Docs [s] essimations [s]
ADD annaral annaral annaral annaral annaral annigue, your work ter data ter data ter data at the kinds of issues you want the basic file of the most com the basic file of the most com the basic file of the most com comulations policyName ~ (* - AND) dittional settings tify additional settings tify bigger of the most com to annel to	orkflow util recognize later oo send. on attributes or the advance mon attributes or the advance watchy matches NRU304- d add an optional message.	ed filter for all attributes Policy × Ø	Siack	3 Baic Advanc	ed Workflow ers Destination Manage of Workflow	elp? does C ² n Does C ³ estimators C ³ wigges C ³

ハンズオン(1-2) Workflowを作成する 2/6

- 4. Notify: Emailを選択します
- メール送信内容を設定します ご自身のメールアドレスを入力して下さい。
 (補足)新規で登録する場合、プルダウンメニューの <u>"Create new destination"</u>をクリックし、 メールアドレスの新規登録作業を行います。
- Send test notificationボタンをクリックし、テストメールを送信します。受信トレイを確認してみましょう。(次スライドで補足)
- 7. Saveボタンをクリックします

す		5	{{ issueTitle }}	
	Email		Custom Details (optional) This payload uses Handlebars syntaxType "{{" to select from a list of variables.	
	Email destination	6	Send test notification	
	Q Search by name or email			Cancel Ore
	Create new destination			🕥 new relic
	// iccusTitle W			

Notify

message

Test this work!

We'll use exis

configured and

Choose one or more destinations and add an optional

data from your account to test what

または

(5)

end a sample notification.

4

Email

O Search by name or email

Kaizawa@newrelic.com

now ServiceNow inciden

Slack

PagerDuty

Test workflow

elect users and emails you want to send notifications to. See our docs 🗹

S Webhook

Email

We found a possible problem above

0 X

o Jira

AWS EventBridge

Cancel

Activate workflow

ハンズオン(1-2) Workflowを作成する 3/6

受信したテストメールを確認します。

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

余裕があれば、Email subjectやCustom Detailsを変更し、 再度テストを行ってみてください。

 例えばIssueが起票された時刻をCustom Detailsに 含めるには、以下のように追記します。

Issue activated at : {{ issueActivatedAtUtc }}

"{{"と入力すると、利用可能な環境変数の一覧が表示されます。

🕥 new relic.		
Critical priority is Memory L minutes o Issue duration: S Go to issue	ssue is closed Jsed % is more than 90 for at least 2 n 'Some-Entity' 5 minutes	
1 incidents		
2 impacted en • ip-172-31-26-	tities 144.ap-northeast-1.compute.internal	-
Alert Policy	NRU-Sample-Policy	
Condition	NRU-Sample-Web transaction time (Baseline)	
Runbook	https://docs.newrelic.com/docs/alerts-applied- intelligence/newrelic-alerts/advanced- alerts/understand-technical-concepts/provide-runbook- instructions-alert-activity/	
NRQL	SELECT count(*) from Metric	
Custom Violation Description	condition-1-a desc	
Tags		

account. Account 3940716 assignmentGroup: Team1 assignmentGroup; Team2 Instrumentation.name: apm Ianguage php type. PM Baseline enablect true agentVersion: 10.10.0.1 Id: 32666626 accountid: 3940716 affectedService: service1 affectedService: service2 (acuesService) causeService: Service2 Instrumentation.provider: newRelic (nr.tracing: standard) policyid: 4406018 trustedAccountid: 3940716



ハンズオン(1-2) Workflowを作成する 4/6

8. 実際のルールでテストする際は、Test workflowボ タンを押します

※Alert Conditionをまだ設定していないためTest workflow ボ タンを押しても今回メール送信はされません (Warningが出ますが異常ではありません)

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

Notify Choose of message	one or more destinations and add an optional	kaizawa@newrelic.com			<u>ℓ</u> ×
		NOW: ServiceNow incidents	& Webhook	Jira	
		Slack	Email	AWS EventBridge	
	(PagerDuty			
	(3			
Test this We'll use	workflow existing data from your account to test what you've	Test workflow	ossible problem above.	9	
configure	and send a sample notification.				
				Cance Activate	workflow
				Cance Activate	workflow
				Cance Activate	workflow
	Email			Cance	workflow
	Email Select users and emails you want to send notifications Q. Search by name or email	to. See our docs [2]		Cance Activate	workflow
	Email Select users and emails you want to send notifications Q. Search by name or email	to. See our docs 12 ⁴		Cance Activate	workflow
	Email Select users and emails you want to send notifications Q. Search by name or email Email subject	to. See our docs 🖸		Cance	workflow
6	Email Sou want to send notifications Select users and emails you want to send notifications Search by name or email Email subject ((IssuefTrile))	to. See our docs 전		Cance	workflow
5	Email Sou want to send notifications Select users and emails you want to send notifications Search by name or email Email subject ((IssueTitle))	to. See our docs 전		Cance	workflow
5	Email Email Select users and emails you want to send notifications Center Select by name or email Email subject ((savefTile)) Custom Details (optional) This payload uses Handhebars syntaxType "(" to select	to. See our docs 년 [°] :t from a list of variables.		Cance	workflow
5	Email Control of the second se	to, See our docs 년 [~]		Cance	workflow
5	Email Email Sou want to send notifications Select users and emails you want to send notifications Q Search by name or email Email subject (tissueTitle 3) Custom Details (optional) This payload uses Handlebars syntaxType "(* to select	to, See our docs [2" t from a list of variables.		Cance	workflow
5	Email Select users and emails you want to send notifications Q Search by name or email Email subject ((IssueTrile)) Custom Details (optional) This payload uses Handiebars syntaxType "(* to select	to, See our docs [2" 		Cance	workflow
5	Email Email Select users and emails you want to send notifications Search by name or email Email subject ((IssueTrile)) Custom Details (optional) This payload uses Handiebars syntaxType "(* to select	to, See our docs [2" ct from a list of variables.		Cance	workflow

ハンズオン(1-2) Workflowを作成する 5/6

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

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





ハンズオン(1-2) Workflowを作成する 6/6

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

Alerts & Al Destinations	⑦ ć
Add a destination Add destinations where we send notifications.	
Vira Dira ServiceNow ReviceNow ServiceNow Se	obile push 有効 無効
Notifications Log Destinations (1)	
Manage destinations where we send notifications.	
Ty 🗘 Name 🗘 Two URL/Details Last updated 🗘 Updated by 🗘 Enabled 🗘	
✓ NRU304 メール通知サンプル smitsui+nru304@newrelic.com Jun 5, 2023 6:4 1004932171 €	
Ty 🗘 Name 🗘 Two URL/Details L	ast updated 🗘 Updated by 🗘 Enabled 🗘
NRU304 メール通知サンプル smitsui+nru304@newrelic.com J	un 5, 2023 6:4 1004932171 💽 …



座学(3) アラートコンディションの作成

16:00 - 16:20 (20min)



Alert Condition

New Relicが収集しているリアルタイムなデータを、集計・評価する仕組み 以下の4ステップで設定

- 1. シグナルを定義(何を監視対象とするか)
- 2. シグナルを集計(シグナルをどう集計するか)
- 3. 閾値を設定(集計結果をどう評価してインシデントを生成)
- 4. インシデントに情報追加



1. シグナルを定義

ガイドを使うか、直接NRQLでシグナルを指定することでシグナルを設定 (平均値・最大値・データ件数カウントなど)

> How would you like to do this? Use guided mode Recommended Choose from options and we'll build your query

Write your own query Use NRQL to define your alert

機能(例. APM, Browser等)ごとに用意されたプリセットから簡単にアラートを作れるほか、 自分でNRQLクエリを記述して、独自の Alert Conditionを作成することも可能



1. シグナルを定義 - Use guided mode

Golden Signalをベースにそれぞれの機能に合わせて、ガイド付きで対象となるシグナルを設定

🛆 AWS (4 types)		Browser applications		Hosts		
Cn host integrations (2 types)		□ Service Levels		③ Services - APM	0	
莺 Synthetic monitors		VPC Networks				
	 Select a met Golden metric: 	ric to monitor			機能毎に重要な監	視項目を簡単に選択可能
	Response tim	e (ms)	Throughp	ut	Error rate	
	Showing 1/1 1 11 k 1 k 900 800 900 600 500 400 300 200 100 200 1100am	ine series ()	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		個々のデータがシグ WithWathWater 200m 800m 900m	
2024 New Relic, Inc. All rights reserved	Query resul	Average query result Critical incident	3-00pm 4:	a-uupm 8:00pm	личин өлирт алирт	s new relic

1. シグナルを定義 - Write your own query

NRQLを使用してベースとなるシグナルを設定



© 2024 New Relic, Inc. All rights reserved.



2.シグナルを集計

データの性質に合わせてシグナルをどう集計するか設定

✓ Data aggre	egation	Window du	ation	生計期間
Window durati	on (i)			
1	minutes ~			
🔵 Use slidir	ng window aggregation (i)		J	
Streaming met	hod (i)			
 Event flow Best for steady See our docs [✓ ○ Event timer ○ Caden y or frequently reporting data (at 2	Least one Streaming n	nethod	:集計方法
Delay (i)				
2	minutes ~			
✓ Gap filling	strategy			
Fill data gaps v	with (i)			
	2711) - Galerado — 230-			



2. シグナルを集計 - Window Duration

アラート条件ごとに <u>集計ウインドウの期</u> <u>間を Window Duration</u> として設定しま す。 プレビューにおいて、チャート上にプロット される個々の点がシグナル、 点と点の間隔が集計ウインドウにあたり ます。



2. シグナルを集計 - Window Duration (Sliding window)

通常、集計ウィンドウの期間は互いに 重なりません。

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

適しているデータ

データの山谷が激しく、かつ短期間の集約では適切 に評価することができないデータ

- CPU%、スループット
- 不安定、頻繁でない、または一貫性のないシグ ナル







2. シグナルを集計 - Streaming method (Event Flow)

指定した遅延(Delay)の時間経過 し、後続のウィンドウのデータが到着 したタイミングで評価対象期間の データを集約 する。それを超えて到着 したデータは評価対象外。 後続データが到着しないと集計が閉

じないので注意が必要。





2. シグナルを集計 - Streaming method (Event Timer)

到着順序や発生間隔に一貫性のない データを評価するのに最適な方式で す。

集計ウィンドウ内のデータが最後に到着 してからの時間経過によって、集計ウィ ンドウが閉じられます 。



LogやSyntheticの監視のベストプラクティス

© 2024 New Relic, Inc. All rights reserved.



2. シグナルを集計 - Streaming method (Cadence)

Cadenceは、データのタイムスタンプではなく、 New Relic内部のシステムクロックに基づいて、一定の間隔で集計を行う方法 です。

多くのケースではEvent FlowまたはEvent Timerが適していますが、 モバイル端末やブラウザから送信されるイベントのように、 ユーザー端末の時刻設定に影響されて、タイムスタンプに一貫性がないデータを対象にする場合 に有効。



補足:データ転送の頻度を加味した設定例

データソース	説明	Streaming method	Delay/Timer
クラウド統合(GCP, Azure, AWS API Polling, AWS MetricStream)	ポーリングは離散的にデータが届く。ストリーミングはコンスタントに データが到着する。タイムラグを考慮しつつ、メトリクスの特性に合 わせて設定	Event Timer / Event Flow	ポーリング間隔以上 /10分前後
Infrastructureエージェント(OHI 含む)	エージェントが1分間隔でデータをコンスタントに送信	Event Flow	2分 (デフォルト)
APMエージェント	APMエージェントはデフォルトで5秒間隔でデータをコンスタントに送 信	Event Flow	2分 (デフォルト)
Browserエージェント	最長でも1分以内にコンスタントにデータを送信	Event Flow	2分 (デフォルト)
Mobileエージェント	Mobileエージェントはデフォルトで10分間隔でデータを送信。また、 アプリのオフライン、バックグラウンド実行によるデータ転送遅延を 考慮	Event Timer / Cadence	10分以上
Serverless(Lambdaレイヤ)	実行中/後にすぐにデータが送信される	Event Flow	2分 (デフォルト)
Log	ログ連携方法によるがAPIで直接転送を実装する以外は最長でも 分以内には送信されるAWS S3経由が最も遅延)	Event Timer (*) / Event Flow	2分 (デフォルト)
Synthetics	実行後すぐにデータが送信される	Event Timer (*) / Event Flow	2分 (デフォルト)
APIIによる転送	API(Trace/Metric/Event/Log)の利用方法に依存	Event Timer / Event Flow	API実行頻度による

*: NRQLアラートのWHERE句の絞り込み条件により0件になることが多い場合はデータロスと認識されて評価されないので Event Timerが適切



補足: Gap-filling strategy

概要

到着したデータに欠損が存在する場合に、欠損データをどう扱って評価 するか。以下の設定が可能

<u> 欠損のまま(None)</u>:

欠損データは閾値の違反に該当しないので、欠損がある場合に違反の アクションを起こしたくない場合に適しています。欠損データはそのまま 欠損データ(Null)として扱われます。

固定值(Custom static value):

妥当な固定値はケースによる。欠損した場合に違反の方に倒す、安全 サイドに倒す、もしくは対象メトリクスに応じた値。

<u>前出の値(Last known value)</u>:

値の変化が予測可能なもので、短時間で大きく変化しないもの。例えば ディスク使用率など。

出典:<u>データのギャップを埋める</u>



© 2024 New Relic, Inc. All rights reserved.

🕥 new relic.

3. 閾値を設定

アラートのしきい値設定は2種類から選択可能

種類	説明	アラートトリガー例
静的(Static)	ある特定の数値を上回った、または下回った場合にア ラートをトリガー	エラー発生割合が5%を超過した
動的(Anomaly)	いつもと異なる振る舞いをした場合にアラートをトリ ガー、どの程度の変動を許容するかを設定できる https://docs.newrelic.com/jp/docs/alerts-applied-intelligence/applied-intelligence/anom aly-detection/	エラー発生割合がいつもよりも増 加した



3. 閾値を設定

静的(Static) しきい値の超過を評価する方法

• For at least xx minutes

xx分間、しきい値を超過する状態が続いた場合に、Incidentが起票される

• at least once in xx minutes

xx分間で、しきい値を1回でも超過した場合に、Incidentが起票される

ーつのAlert Conditionには、CriticalとWarning(オプション)の閾値を設定可能

その他、アラート設定に関する詳細は以下もご参照ください

<u>ストリーミング・アラートの概念 | New Relic</u> (https://newrelic.com/jp/blog/how-to-relic/streaming-alert-concept) <u>アラート条件を正しく設定するための詳細ガイド | New Relic</u> (https://newrelic.com/jp/blog/how-to-relic/understand-nrql-alert-condition) アラート定義のガイダンス | New Relic (https://newrelic.com/jp/blog/how-to-relic/alert-configuration-guidance)

Severity level Critical ~						
When a query returns a value	above ~	1	for at least 🗸	5	~	minutes ~
			for at least			
Add threshold			at least once	in		



4. インシデントに情報追加

効果的な通知を送るためのプラクティス

- Send a custom incident description
 発報されるアラートに任意の情報を付加することが可能(参考情報)
- Runbook URL

アラート対応手順書や、情報を集約したダッシュボードにすぐにアクセスすることが可能

Send a custom incident description (optional) ()	
4,000 character limit	
Runbook URL (optional)	
https://	





ハンズオン(2) アラートコンディションを 作成

16:20 - 16:35 (15min)



ハンズオン(2-1) Alert Conditionを作成する 1/21

新規Alert Conditionの追加

4つのアラートを順番に設定していきます

- 1. フロントエンド:ページロード時間
- 2. アプリケーション: 4xx,5xxエラー(ホストごと発生数を設定する)
- 3. アプリケーション:応答時間(動的)
- 4. 外形監視:チェックエラー

Tips: Conditionの作成は、各自で作成したポリシーにアクセスし、 "New alert condition"ボタンから開始すると、後続のステップが理解しやすいかと思います。

具体的な手順は後続のスライドからご確認下さい。

ハンズオン(2-1) Alert Conditionを作成する 2/21

• 新規 Alert Conditionの追加

①フロントエンド:ページロード時間

- 1. Add alerts
 - a. Use guided mode
- 2. Tell us what where to look
 - a. Browser applications
- 3. Tell us what to watch
 - a. EC-site
- 4. Select a metric to monitor
 - a. Pageload time(s)

Condition名は適切なものを各自設定してください

(例:NRU304-yourname-NRQL-pageloadtime)



画面遷移(一部スキップありのヒント

Use guided mode Recommended

Write your own query

Choose from options and we'll build your query

Add alerts

具体的な手順は後続のスライドからご確認下さい。

🕥 new relic. 63

ハンズオン(2-1) Alert Conditionを作成する 3/21

- 1. Alerts メニューを開きます。
- 2. Alert Policies を開きます。
- 3. 前のハンズオンセクションで作成したポリシーを選択します。
- 4. 画面右側にある[+New alert condition] を選択して、新しい Alert Conditionを作成します。

🕥 new relic	ANALYZE	Alerts & Al				⑦ 🔆 Ask Al ⊘		
Q Quick Find	E Issues & Activity	Alert Policies		L Now elect condition	a probuilt alort conditions	- Now plast policy		
+ Add Data	DETECT			+ New alert condition + Brows	se prebuiit aiert conditions	+ New alert policy		
All Capabilities	Alert Conditions	Showing 5 policies	Policy Name = All					
Dashboards	Alert Policies	Name		Open issues	# of conditions			
Alerts & Al	Anomaly Detection	NRU-Sample-Policy		0	6			
Query Your Data	CORRELATE	NRU環境整備		0	2			
E Logs	a ^k Sources	Service Levels default policy for account 3940716		1			0	
III Traces	r Decisions	これがあなたのポリシーです。		•		(4)		lert condition
출 Synthetic Monitoring	ENRICH & NOTIFY	ダッシュボードハンズオン用アラートポリシー		•			Incid	Crecondition
Infrastructure	🔆 Muting Rules							
Kubernetes	ede Workflows							
🗒 Browser	🖂 Destinations							
Mobile	SETTINGS							
Errors Inbox	លើ General							



ハンズオン(2-1) Alert Conditionを作成する 4/21

• 「Use guided mode」を選択

١dd	a	ler	ts	
-----	---	-----	----	--

Use guided mode Recommended Choose from options and we'll build your query

Write your own query Use NRQL to define your alert

Build a classic alert Use our original alert builder form

「Browser applications」を選択して、「Next」を押下

Tell us where to look (i)							
△ AWS (4 types)	Browser applications	🚍 Hosts					
C On host integrations (2 types)	🖽 Service Levels						
兽 Synthetic monitors	UPC Networks						



ハンズオン(2-1) Alert Conditionを作成する 5/21

• 「EC-site」、「Pageload time(s)」を選択し「Next」をクリックします。

Tell us what to watch											
Select the entities to watch (max 20)											
Search entities by name or attributes. If you create new entities with these attributes, we'll watch those as well.											
All Selected 1											
Filter by name or tags											
Entities û											
EC-site											
nami-react-app											
• Golden metrics Other metrics											
Throughput (ppm)	Largest contentful paint (75 percentile) (s)	First input delay (75 percentile) (ms)									
Errors	Pageload time (s)	Ajax throughput (rpm)									
Preview chart for pageload time (s) (past 6 hours)											
		Cancel									

ハンズオン(2-1) Alert Conditionを作成する 6/21

- 監視設定は次のようにしてください。
- 1. Window Duration
 - a. 1 minutes
- 2. Streaming method
 - a. Event flow
- 3. Delay
 - a. 2minutes

- 4. Set condition thresholdsa. Static
- 5. Severity level
 - a. Critical
- 6. When a query returns a value
 - a. above 1 for at least 5 minutes



ハンズオン(2-1) Alert Conditionを作成する 7/21

• それぞれ 設定を確認し「Next」をクリック。

C

	Fine-tune your signal		Set condition thresholds		
	✓ Data aggregation	4	• Static (i) 🔿 Anomaly (i)		
	Window duration (i)		Open incidents with a:		
1	1 minutes ~	5	Severity level Critical ~		
	O Use sliding window aggregation (i)		When a query returns a value		
	Streaming method ①	6	above ~ 1 for at least ~ 5 ~ minutes ~		
હા	Event flow Event timer Cadence Best for steady or frequently reporting data (at least one data point per aggregation				
	window).		+ Add threshold		
3	Delay (i)		(+) Add lost signal threshold		
ઁ	2 minutes ~				
	✓ Gap filling strategy				
	Fill data gaps with (i)				
	None ~				
	\sim Evaluation delay				
	Use evaluation delay (i)				
				Cancel Next	
2024	New Relic, Inc. All rights reserved.				s new relic

ハンズオン(2-1) Alert Conditionを作成する 8/21

コンディション名にわかりやすい名前を入力し、「Save condition」をクリックする。
 (例:NRU304-yourname-Performance)

	Add details	
$\left[\right]$	Name your alert condition * Use a clear name that indicates what's wrong	
	Close open incidents after ① 3 days ~	
	Send a custom incident description (optional) (i)	
	4,000 character limit	
	Runbook URL (optional)	
	https://	
	C Enable on save	
	Cancel View as code Save condition	
l rigł	nts reserved.	🗩 🕥 new relia

ハンズオン(2-1) Alert Conditionを作成する 9/21

• Summaryページが開き、Queryの内容やチャートが表示されます。「Close」をクリックします。





ハンズオン(2-1) Alert Conditionを作成する 10/21

• コンディションが作成されました。名前やcategoryをクリックすれば設定を編集できます。

Alerts & Al / Alert Policies これがあなたのポリ 『『Infrastructure Good	シーです。 - ☆ 🛛 Tags ① Metadat	a 🌀 Workloads				G	D C		
创 Summary MORE VIEWS	ID: 4932576								
 Add app Achange tracking 	O Search by condition name or id Condition Name - All +								
Logs	Showing 1 condition								
	Alert condition とってもわかりやすいコンディション名	Query SELECT average(duration) as 'P	Thresholds Critical: above 1 for 5 minutes Create a warning threshold	Type NRQL Query	Open issues				



ハンズオン(2-1) Alert Conditionを作成する 11/21

• 新規 Alert Conditionの追加

②アプリケーション: 4xx,5xxエラー(ホストごとに評価)

- 1. Categories
 - a. NRQL

2. Define your signal > Query the data you want to monitor

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

Condition名は適切なものを各自設定してください

(例:NRU304-yourname-NRQL-ErrorResponse)

具体的な手順は後続のスライドからご確認下さい。


ハンズオン(2-1) Alert Conditionを作成する 12/22

• 作成したポリシー内にて「+ New alert condition」をクリックする。

Alerts & Al / Alert Policies これがあなたのポリシーです	o 🗸 🙀 🕕 Metadata 🍥) Workloads				⑦ ≮ Ask	AI C
ID: 5106997							
Alert conditions Notifications Settings						+ New alert c	ondition
Q Search by condition name or id		Condition Name = All +					
Showing 1 condition							
Alert condition	Query	Thresholds	Туре	Open issues	Last modified	Enabled	
とってもわかりやすいコンディション名	SELECT average(duration) as '	Critical: above 1 for at least Create a warning threshold	NRQL Query		Feb 20, 2024, 10:23pm		()





ハンズオン(2-1) Alert Conditionを作成する 14/21

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



C Review your NRQL query									
Showing 1/1 time series (?)									
100%									
90.5									
90% 85%									
80%									
75%									
70%									
65%									
60%									
55%									
50%									
45%									
40%									
32%									
25%									
20%									
15%									
10%									
5%				 					
0%					/				
2:30pm 3:00pm Preview chart (past 6 hours)	3:30pm	4:00pm	4:30pm	/	6:00pm	6:30pm	7:00pm	7:30pm	
2:30pm 3:00pm Preview chart (past 6 hours) Review.your.NRQL.query.	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	7:00pm	7:aupm	
2:30pm 3:00pm Preview chart (past 6 hours) ① Review.your.NRQL.auery Showing 1/1 time series ②	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	7:00pm	7:supm	
2:30pm 3:00pm Preview chart (past 6 hours) ① Review your NRQL query Showing 1/1 time series ③ 0:006	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	7:00pm	7:supm	
2:30pm 3:00pm Preview chart (past 6 hours) () Review your NRQL query Showing 1/1 time series () 2:000	3:30pm	4:00pm	4:30pm		6:00pm	6-30pm	7:00pm	7:supm	
2:30pm 3:00pm Preview chart (past 6 hours) () Review your NRQL query Showing 1/1 time series () 0:005	3:30pm	4:00pm	430pm		6:00pm	6-30pm	7:00pm	7:supm	
2:30pm 3:00pm Preview chart (past 6 hours) ③ Review your NRQL avery Showing 1/1 time series ③ 0:00 0:00	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	7:00pm	7:supm	
230pm 300pm Preview chart (past 6 hours) () Review, your NRQL auery Showing 1/1 tim series () 0006 0005 0004	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	7:00pm	//supm	
230pm 300pm Preview chart (past 6 hours) Beview, your MRQL query Showing (11 time series 0 000 000 000 000 000 000 000 000	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	7:00pm	//supm	
2.30pm 3.00pm Preview chart (past 6 hours) Review your NROL suery Showing 1/1 time series ③ 2.006 2.006 2.004 2.002 2.002 2.004 2.002 2.002 2.005 2.004 2.002 2.005 2.005 2.	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	7.00pm	7-50pm	
2 30pm 3 00pm Preview chart (past 6 hours) Review soc.NRGL.even Showing 11 time series 00 00	3-30pm	4:00pm	4:30pm		6:00pm	6:30pm	700pm	7-50pm	
2 30pm 2 00pm Preview chart (past 6 hours) Review, sock MGL swery Showing 1/1 tims series Code Co	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	700pm	7250pm	
2 30pm 300pm Preview chart (past 6 hours) Review, you, NRQL aveny showing (11 time series 0 000 000 000 000 000 0 0 0	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	200pm	7-50pm	
2 30pm 3:00pm Preview chart (past 6 hours) Review your. MiGL.suer: Showing 11 time series 200	3:30pm	4:00pm	4:30pm		6:00pm	6:30pm	200pm	7:50pm	
200m 200m Preview chart (past 6 hours) Tearlier your MGL summ Schwing 1/1 time series Cons	3:30pm	4:00pm	4:30pm		6.00pm	6:30pm	200pm	7250pm	
2 30pm 3 00pm Preview chart (past 6 hours) Review your.NRGL.exer: Showing 11 time series Cool Coo	3:30pm	400pm	4:30pm		6.00pm	6:30pm	200pm	2:30pm	
2.30pm 2.00pm Preview chart (past 6 hours) Review, your, NRGL suery booking 1/1 time series 0	3:30pm	400pm	433pm		6.00pm	6:30pm	200pm	2:30pm	
2 30pm 3 00pm Preview chart (past 6 hours) Review your NRGL suer: Showing 11 time series Cool Coo	3:30pm	400pm	4:30pm		600pm	6-30pm	200pm	2:30pm	
2 30pm 2:00pm Preview chart (past 6 hours) Comments year, MRGL suler; Showing (1) time series Comments accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss accoss acco	3:30pm	400pm	433pm		6.00pm	6-30pm	200pm	Pogen	
2 30pm 3 00pm Preview chart (past 6 hours) Review souch RGL even Showing 11 time series Coose Coos Coo	3-30pm	400pm	4:30pm		6.00pm	6.30pm	700pm	2:30pm	
2 30pm 2 00pm Preview chart (past 6 hours) Brokey, soc. NRGL, suer: showing 1/t time series cos	3.30pm	400pm	433pm		6.00pm	6.30pm	200µm	2:50pm	



ハンズオン(2-1) Alert Conditionを作成する 15/21

- 任意のAlert Condition名を設定します。
 (例:NRU304-yourname-http-error)
- Send a custom incident descriptionと Runbook URLはオプションです。何か思 いついた内容を記載してみてください。
- Enable on saveが図の状態になっている ことを確認し、Save conditionをクリックし ます。
- 設定確認画面が表示されるので、Closeを クリックして閉じます。

とってもわかりやすいコンディション名			
Close open incidents after i 3	days ~		
Gend a custom incident description (op)	ional) 🕕	_	
ここに記述した情報が、Incidentの詳細	間情報としてアラート内に記載されます。		
1,000 character limit			
Runbook URL (optional)			
https://www.yahoo.co.jp			
D Enable on save			
D Enable on save			
D Enable on save			
D Enable on save		Cance	I <> View as code Save con



ハンズオン(2-1) Alert Conditionを作成する 16/21

• 新規 Alert Conditionの追加

③アプリケーション:応答時間(動的)

- 1. Categories
 - a. NRQL
- 2. Define your signal > Query the data you want to monitor

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

Condition名は適切なものを各自設定してください

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

具体的な手順は後続のスライドからご確認下さい。

New relic

ハンズオン(2-1) Alert Conditionを作成する 17/21 Add alerts 右側からスライドして表示される Add Use guided mode Recommended Choose from options and we'll build your query alerts画面から「Write your own Write your own query Jse NRQL to define your alert query」を選択する。 Build a classic alert Use our original alert builder form クエリ入力欄に次の NRQLクエリをコ From Transaction SELECT average(duration) WHERE appName = 'EC-site' ピー&ペーストして、Runをクリックしま す。 See our docs [2] for help with null values [2], loss of signal [2], or other query options Critical threshold *From Transaction SELECT average(duration)* 0.9 0.8 WHERE appName ='EC-site' 0.6 0.5 クエリ実行後、直近の状態を示す参考 0.2 チャートが表示されることを確認し、 10:30am 12:3000 2:30pm 3:0000 Ave Duration • Critical threshold • Critical inciden Nextをクリックする。 © 2024 New Relic. Inc. All rights reserved. **S** new relic

ハンズオン(2-1) Alert Conditionを作成する 18/21

- Set condition thresholdsの閾値のタイプを StaticからAnomalyに変更する。
- これまでの手順同様「Save condition」で保存 する。
 - もし時間の余裕がある場合、「XXX standard deviation(s)」のXXXの値を変 えることで、上部のチャートがどのように 表示を変えるかを確認してください。

	Set condition thresholds	
	🔿 Static 🕧 🧿 Anomaly 🛈	
	Threshold direction Upper and lower ~	
	Open incidents with a:	
	Severity level Critical ~	
+	When a query returns a value outside the threshold	
	by 3 standard deviation(s) for at least ~ 5 ~ minutes ~	Ş
	More incidents Fewer incidents	
	 Add threshold Add lost signal threshold 	
		Cancel
		new relic. ⁷⁹

ハンズオン(2-1) Alert Conditionを作成する 19/21

• 新規 Alert Conditionの追加

④外形監視:チェックエラー

- 1. Categories
 - a. NRQL
- 2. Define your signal > Query the data you want to monitor

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

Condition名は適切なものを各自設定してください

(例:NRU304-yourname-synthetics-check)

具体的な手順は後続のスライドからご確認下さい。



ハンズオン(2-1) Alert Conditionを作成する 20/21

- 右側からスライドして表示される Add alerts画面から「Write your own query」を選択する。
- クエリ入力欄に次のNRQLクエリをコ ピー&ペーストして、Runをクリックしま す。

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

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



ハンズオン(2-1) Alert Conditionを作成する 21/21

- Set condition thresholdsの閾値条 件を変更する。
 - 右側のサンプルを参考にして変 更する。
 - Above or equal toの適用
 - At least once inの適用
- これまでの手順同様「Save condition」で保存する。

Set condition	n thresholds					
O Static (i)	Anomaly (D				
Open incidents	s with a:					
Severity level	Critical ~					
When a query	eturns a value					
above or equ	al to ~ 1	at least once	in ~ 5	~ n	ninutes ~	
Add thr	eshold					
					Cancel	Next



参考:該当しない状態を「0」として扱いたい場合

アラート条件の評価が行われるのは、クエリのWhere句に該当する値が発生した場合です。

そのためWhere句で絞り込んだ結果が0件の場合はデータなし(NULL)扱いとなりアラート条件として評価されません。 例えば全てのresultが'SUCCESS'だった場合、以下のクエリでは「該当データなし」となります。アラートとして通知できま すが、復旧判定ができず状況によっては適切に通知できない場合があります。

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

その場合filter関数の中で絞り込むことで評価対象にすることができます

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

参考: Example: null value returned (有用なブログ情報: <u>こちらとこちら</u>)



ハンズオン(Optional#1) Enrichmentを試す 1/3

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Enrichmentの設定が通知内容にどう変更があるかを確認します。

<u>こちらのスライド</u>で簡単に紹介した Enrichの機能を試 してみましょう

Enrichmentとは:

- Workflow内で任意のNRQLを設定することで、 そのクエリ結果を補足情報として通知内容に含 めることができます(より詳細は、下部のドキュメ ント[1]をご確認ください)
- メール通知やSLACK通知では、NRQLのクエリ
 結果が画像としてが添付されます
 参者:

ドキュメント[1] <u>Enrichment機能の概要</u> ドキュメント[2] <u>アラート対象エンティティの絞り込み</u>



具体的な手順は後続のスライドからご確認下さい。

S new relic.

ハンズオン(Optional#1) Enrichmentを試す 2/3

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Enrichmentの設定が通知内容にどう変更があるかを確認します。

- Alerts > Workflowsにアクセスし、ハンズオンで利用している Workflow設定を開きます
- Workflow設定内のAdditional settingsボタンをクリックし、
 Enrich your dataトグルを有効化します
- 有効化すると右側から設定 UIがスライド表示されるので、
 Name your queryICEnrichment名を指定し、下部にNRQLを 設定します
 - a. サンプルNRQL: FROM Log SELECT message
 - b. Runボタンを押して、設定したNRQLの挙動をテストします



ハンズオン(Optional#1) Enrichmentを試す 3/3

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Enrichmentの設定が通知内容にどう変更があるかを確認します。

- 4. Save and exitボタンをクリックし、設定を保存します
- 5. Workflow設定のUI内にある**Test workflow**ボタンからテス ト通知を行います
 - a. 補足: テスト用の通知は過去に発生したアラートを基に して発報します。過去に発生したアラートがないような 新規の設定の場合、テスト用アラート発報を行わない ケースがあります
- 6. テスト後、**Update workflow**ボタンをクリックし、 Enrichmentの設定を保存します



ハンズオン(Optional#2) Notify Whenを試す

ハンズオン時間に余裕のある方は、全スライドで無効化した Workflowを再度有効化し、Notify Whenの設 定が通知内容にどう変更があるかを確認します。

- Alerts > Workflowsにアクセスし、ハンズオンで 利用しているWorkflow設定を開きます
- Workflow設定のNotifyセクション内で設定している通知項目の[...]をクリックし、ポップアップメニューからNotify when...を選択する
- 3. 任意の箇所にチェックを入れたり、外します
- 4. Workflowの設定UIに戻り**Update workflow**ボタ ンを押し、設定を更新する
- 5. 実際にアラートが発生した際に通知される内容に 変化があるかを確認する



補足: APIを活用してアラートテストを行う

New Relicが提供しているAPIを用いることで、仮想的にアラートを発報させるデータを生成することができます。(NRU302でもEvent APIの活用をオプションのハンズオンとして体験可能です)



© 2024 New Relic, Inc. All rights reserved.





ハンズオン(3) 発生したアラートの確認

16:35 - 16:45 (10min)









ハンズオン(3-1) 個々のアラートを確認する 1/3

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





ハンズオン(3-1) 個々のアラートを確認する 2/3

• Incidentをクリックします。





ハンズオン(3-1) 個々のアラートを確認する 3/3

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





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

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





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

 Issues ではユーザーが設定した AlertやAnomaly、API連携などの複数のアラートの中で関連しそう なものをまとめて取り扱います。





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

• Issueをクリックすると詳細が表示されます。

Alerts & Al													? ?
Issues &	Activity										< 🕒 si	ince 60 minutes ago (GMT+	-9) 🗸 >
Issues Inc	cidents Anoma	alies Postmort	tems										st issues
Q Filter by Show 1 0.8 0.6 0.4 0.2	ID or names	+										Are you seeing all the problems? We use machine learning recommend alerts for service that need them	to vices
0 4:24	4:29pm	4:34pm	4:39pm	4:44pm 4:49p	om 4:54pm	4:59pm	5:04pm	5:09pm	5:14pm	5:19pm	5:24pn	See alert coverage gap)S
• Low • M	Medium 🗕 High 鱼	Critical											
State	Priority	Created ↓	Duration	Issue name			Entity name		1	Notified	Contains	Actions taken	
Active	Critical	32m ago	30m	Transaction qu	ery deviated from t	he b	EC-site	. +1	۵		2 incidents	s	

new relic. 96

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

• どのIncidentがまとめられているのか確認することができます

Critical Activated on Nov 17, 2023 4:53pm Duration: 36	m	Last updated Nov 17, 2023 5:17pm
Transaction query deviated from the baseline Source: 🕥 Notified: 🗹 🗐 Issue payload	for at least 5	minutes on '非常にわかりやすいコンディション名を設定する' Close Issue Acknowledge
Incidents (2) Sort by Newest to oldest ~ Sh	ow open only	Critical Incident opened on Nov 17, 2023 5:01pm See NRQL overview
<mark>Critical Open</mark> NRU304-Synthetic Check query result is >= 1.0 on '少し複雑 コンディション名'	単な	NRU304-Synthetic Check query result is >= 1.0 on ' 少し複雑なコンディション名' Alert Policy: これがあなたのポリシーです。 View/edit Condition: 少し複雑なコンディション名 View/edit
Opened: Today 5:01pm	🕒 28m	Signal over time Synthetic checks Failure screenshot
Critical Closed Transaction query deviated from the baseline for at least 5 minutes on '非常にわかりやすいコンディション名を設定する'		© Incident period ~
Opened: Today 4:53pm	🕒 24m	15
		0 25pm 4:30pm 4:35pm 4:40pm 4:45pm 4:50pm 4:55pm 5:00pm 5:05pm 5:10pm 5:15pm 5:20pm 5:25pm
		NRU304-Synthetic Check Tags (17) Show all
		Entity type: SYNTH account: New Relic University Ja accountid: 3940716 apdexTarget: 7.0 enabled: true Account: New Relic University Japan enableScreenshotOnFailureAndS id: 37871380 monitorStatus: Enabled monitorType: Simple Browser



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

Issue timelineや関連するEntity情報、デプロイ履歴など、原因分析に役立つ情報が表示されます



ハンズオン(3-3) 届いたメール通知を確認する

• 通知されたEmailからIssue の詳細など、確認に役立つ情報が表示されます

Critic	al priority issue is active
NR	U304-Synthetic Check query result is >= 1.0
011	Synthetics
A	cknowledge Close issue Go to issue
corr	related issues
com	elateu issues
le've u	ised correlation to merge new issues into your active issue
• Ir	ised correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on
• Tr • Tr <u>'N</u>	used correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on RU304-baseline'
• Ir 'N	ised correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on RU304-baseline'
 Ir Incid 	ised correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on RU304-baseline' dents
• Ir ' <u>N</u> incid	ised correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on RU304-baseline' dents RU304-Synthetic Check query result is >= 1.0 on 'Synthetics'
/e've u • Ir <u>'N</u> • Incio	ised correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on RU304-baseline' dents RU304-Synthetic Check query result is >= 1.0 on 'Synthetics' Since 34 minutes ago until 4 minutes ago
• Incid	used correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on IRU304-baseline' dents RU304-Synthetic Check query result is >= 1.0 on 'Synthetics' Since 34 minutes ago until 4 minutes ago
Ve've u • Ir • Ni • Ni	used correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on iRU304-baseline' dents RU304-Synthetic Check query result is >= 1.0 on 'Synthetics' Since 34 minutes ago until 4 minutes ago
incid	used correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on IRU304-baseline' dents RU304-Synthetic Check query result is >= 1.0 on 'Synthetics' Since 34 minutes ago until 4 minutes ago
• Irr N	used correlation to merge new issues into your active issue ansaction query deviated from the baseline for at least 5 minutes on IRU304-baseline' dents RU304-Synthetic Check query result is >= 1.0 on 'Synthetics' Since 34 minutes ago until 4 minutes ago 1).5





座学(4) New Relicのアラート分析支援機能

16:45 - 16:55 (10min)

© 2024 New Relic, Inc. All rights reserved.



New Relic によるインシデント対応フロー



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)

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)



検知1: 重要な指標に対するアラートによる気づき







検知2: Lookoutによる傾向の可視化と探索







診断1: Correlationによるアラート統合とノイズの削減



							-	
9E1.05								
-		-		-				-
	trevisioned						· Cristal · High	· Madhare w Lo
-					-			
						-		
						-		
		_						
						-		
10-15 AW	10/20 AM 10/25 AM 10	1.30 AM		10-25 AM	10-69 AM 10-64 A	M - 10:44 AM	10.58	A00
+ Showmore	22							
ed activity	22							
ed activity	22 TULE		SOURCE	STATE	RELATED EVENTS	PAYLOAD	ANALYZE	NEW RELIC ORH
ed activity	22 THLE WellPartial is having latency problems feaching data from Plan Service	ಚೆ	source pr	STATE Closed	RELATED EVENTS	PAYLGAD	ANALYZE	NEW RELIC ORIG
ted activity runoared 2, 10:41am 2, 10:41am	22 The # Weldfurnel is hearing teacing problems freching, data from Plan Service Error rate	ೆ	sounce pr	STATE Closed Closed	RELATED EVENTS 2 2	PAYLOAD III) III)	ANALYZE	NEW RELIC ORIG
ed activity rupparte 2, 10:41am 2, 10:42am	22 70% # Welf-brid is hering latency problems feaching data from Plan Service Error rate Web requiring time > 300 milliassends for at least 5 minutes on Webfystal (p. 17)	c°	source pr O	STATE Closed Closed Closed	RELATED EVENTS 2 2 2	PAYLOAD 07 07 07	AMAA YZE O, Analyze	NEW RELIC ORIG
ted activity ruPDATED 2, 10:41am 2, 10:42am 2, 10:43am 2, 10:43am	TITLE TITLE Wolf-bind is having latency problems feeching data from Plan Service Briterine Work requestions time + 300 milliseconds for at least 5 minutes on Wolf-hirst (lp-17), CPU No 55 for at least 5 minutes on (hp-172-31-9-35)*	ଟ ଟ ଟ	source (x) O O	STATE Closed Closed Closed Closed	ABLATED EVENTS 2 2 2 2 2	PAYLOAD III) III) III) III)	AMALYZE Q. Analyze	NEW RELIC ORIG
ted activity tupoareo r2, 10:41am r2, 10:41am r2, 10:41am r2, 10:43am r2, 10:43am r2, 10:43am	Trice Trice WolfPrintel Is having Lettercy problems Recharg, data. from Plan. Service Drar Jole Wolf-requires time - 300 millioscends, for at least 5 minutes on YMShgraf (p. 17), CHU is + 55 millions 1 minutes on (p. 172-31-9-357) Error percentage > 455 he at least 5 minutes on Shgping Service	ය ප් ප් ප්	source pr O O O O	STATE Dosed Dosed Dosed Dosed Closed	ALATO IVINT 2 2 2 2 2 2 2 2 2	PAYLOAD (17) (17) (17) (17) (17) (17) (17)	ANALYZE : Q. Analyze Q. Analyze	NEW RELIC ORIG
ted activity turoareo r2,10:41am r2,10:41am r2,10:41am r2,10:43am r2,10:43am r2,10:43am r2,10:43am	22 The second se	ය ග් ග් හ් හ් හ්	50URCE pr 0 0 0 0 0 0 0	STATE Dosed Dosed Dosed Dosed Dosed Dosed	RELATIO POINTS 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PAYLOAD (22) (22) (22) (22) (22) (22) (22) (22	ANALVZE Q. Analyse Q. Analyse	NEW RELIC ORIG
ted activity 2, 10:41am 2, 10:41am 2, 10:41am 2, 10:41am 2, 10:43am 2, 10:43am 2, 10:43am 2, 10:43am 2, 10:44am	Twis Twis Twis Workbridt Is having latency problems fesching data from Plan Service Web required time > 300 milliassends for at least 5 minutes on "Web/Hybel (pp.17). CPU is > 55 for at least 5 minutes on "pr.172-31-9-357. Drue processings > 45% for at least 5 minutes on "Stopping Service Web/Hybel Is having latency problems festions, data from Plan Service Web/Hybel Is having latency problems festions, data from Plan Service Of Us is > 65 for at least 5 minutes on "pr.172-31-12.297	ස් ජේ ජේ ජේ ජේ ජේ ජේ ජී	50URCE pr 0 0 0 0 10 0 0	STATE Dosed Dosed Dosed Dosed Closed Closed Closed Dosed	REATO (VINTS 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PAYLOAD 00 00 00 00 00 00 00 00 00 00	ANALYZE Q. Analyze Q. Analyze	NEW RELIC ORIS
ted activity 2, 1041am 2, 1041am 2, 1041am 2, 1043am 2, 1043am 2, 1043am 2, 1043am 2, 1044am	22 VINL Workprint is having latency problems fetching data from Plan Service Processes Bree rade: Why requestions from Plan Service Why requestion from 2.30 milliseconds for at least 5 minutes on Systems fetching data from Plan Service Plan Service CPU is 2.55 for at least 5 minutes on Systems fetching data from Plan Service Service percentage × 45% for at least 5 minutes on Systems fetching data from Plan Service CPU is ~ 25 for at least 5 minutes on Systems fetching data from Plan Service CPU is ~ 26 for at least 5 minutes on Systems fetching data from Plan Service CPU is ~ 26 for at least 5 minutes on Systems fetching data from Plan Service CPU is ~ 26 for at least 5 minutes on Systems fetching data from Plan Service	ය ය ය ී ී ී ී ය ී ය ී ය ී	100/RCE (PT O O O O O O O	STATE Dosed Dosed Cosed Cosed Cosed Cosed Cosed Cosed Cosed	REATO DVINTS 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PAYLOAD 101 102 102 102 102 102 102 102	AMAAYZE Q. Analyze Q. Analyze	NEW RELIC ORIS
ted activity 2 2.1041am 2.1041am 2.1041am 2.1043am 2.1043am 2.1043am 2.1043am 2.1043am 2.1043am 2.1044am	Z2 X X X X X	ස් ස් ස් ස් ස් ස් ස් ස් ස් ස් ස්	50UNCT (07 00 00 00 00 00 00 00 00	STATE Oosed Oosed Oosed Coosed Coosed Coosed Coosed Coosed Coosed	RELATIO (VINTS) 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	PATLOAD 	ANALYZE C. Analyse C. Analyse	
ed activity 2,10-41am 2,10-41am 2,10-41am 2,10-41am 2,10-41am 2,10-41am 2,10-41am 2,10-44am 2,10-44am 2,10-44am 2,10-44am	With Problems Intercept problems (http://githugengians.com/ Problems) Problems Intercept problems (http://githugengians.	යි පී සී සී සී සී සී සී සී සී	300/00CF ρ1 Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο Ο	STATE Closed Closed Closed Closed Closed Closed Closed Closed Closed Closed Closed	RELATIO INVINTS 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PATLOAD (0) (0) (0) (0) (0) (0) (0) (0) (0) (0)	0, Analyse Q. Analyse Q. Analyse	



診断2: Correlationによる根本原因の示唆



		暖 合 Share :
eb response time > 700 milliseconds for at least 10 minu a s \circ pd $\rightarrow =$	ites on 'Plan Service'	③ 24m Mar 15, 11:57am
ssue summary		問 ^
Analysis summary : 🛞 Golden signals: Latency 🖓 📩 🛛 🛞 Related components: Application	Suggested responders 会 Alan Turing 促 会	
mpacted entities (1) ① 1 Application		
Plan Service		▲ Deployment events Q. Anomaly overview ⊕ Entity overview
loot cause analysis epioyment events (3)	Error logs (3)	Attributes to investigate (3)
Noot cause analysis Xeployment events (3) Deployments: ① Last 12h	Error logs (3) error logs Since Mar 15, 11:Ikans Until Mar 15, 11:Ikans	Attributes to investigate (3) Plan Service Database musicion (mp) factived by Datastere type and Table and Operation
beployment events (3) Deployments Deployment Deploy	Error logs (3) error logs Since Mar 15, 11:18am Unei Mar 15, 11:03am 1 0.6 0.6 0.4 0.2 0.2 0.2 0.2 0.2 0.2 0.2 0.2 0.2 0.2	Attributes to investigate (3) Plan Service Database duration (mg) faceted by Datastere type and Table and Operation
Root cause analysis Deployment events (3) Deployment Deployment Application: Flam Service Deploymer; guaraer@fiteica.mdemo.com Revision: Hottic: Floring bad query Rootbile cause; Due to provinely to issue creation Rootbile cause; Due to provinely to issue creation	Error logs (3) error logs Since Mue 15, 11:I.Barn Until Mar 15, 11:I.Barn 1 8.8 9.6 9.6 9.6 9.6 9.6 9.6 9.6 9.6	Attributes to investigate (3) Plan Service Database duration (mp) factored by Datastere type and Table and Operation 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 6 4 7 8 7 9 7



対処:様々なツールと連携しアクションを実行 検知 傾向分析 アラート通知 (可視化) æ 診断 Webhook now. ServiceNow Jira Slack AWS イベントの相関分析 根本原因分析 ig? Mobile push PagerDuty Email EventBridge 対処 (外部ITSMツール: Servicenow, Pagerduty等)



機能紹介: Correlate (Decisions)

Alerts \rightarrow Decisions

- Incidentの構造を分析して、関連性の高いものを一つの Issueにまとめる (対象エンティティ、Incidentデータ構造の一致度)
- 相関関係を持たせる基準はプリセットが用意されている ほか、独自に設定可

🕥 new relic	ANALYZE	Alerts & Al				0	<≉ Asl
Q Quick Find	Issues & Activity	Decisions				+ Create	e new c
All Capabilities All Entities	DETECT	These rules provide the logic we use to group inc	cidents and reduce yo	ur alert noise. See our docs	ß		
Dashboards	Alert Policies Anomaly Detection	Your decisions (14) Suggested decisions					
Query Your Data	Se Alert Coverage G Beta	Name and description	Correlations	Created by	Last edit	Enabled	
 APM & Services Logs 	CORRELATE	Application Anomalies and Violations wit Correlation activated because the anom	0	New Relic Al Global decision	Jan 6, 2023 1:45pm		
Traces	Decisions	Same New Relic Condition and Title Correlation activated because New Relic	0	New Relic Al Global decision	Nov 19, 2022 8:20am		
Infrastructure Kubarnatas	Muting Rules	Same New Relic Target Name (NRQL) Correlation activated because the New R	0	New Relic Al Global decision	Nov 19, 2022 6:41am		

Correlation activated because the anomalies and viola New Relic AI - Global decision 0 likes 0 dislikes	tions are generated from the same application
Decision logic Correlate by attributes	 Rule analysis No results found
entityld = entityld	Correlations
Filter by specific values	
When incident 1 has these values:	
origin = anomalies	
entityType contains Application	
And incident 2 has these values:	
origin = newrelic	
Advanced Setting	
Time window: 30 min	

© 2024 New Relic, Inc. All rights reserved.



まとめ


まとめ

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



• New Relicのアラート機能を活用して、アラート分析を効率化しましょう



アラート関連の情報

- アラート条件を正しく設定するための詳細ガイド
 - <u>https://newrelic.com/jp/blog/how-to-relic/understand-nrgl-alert-condition</u>
- アラート通知にログメッセージを記載する
 - <u>https://newrelic.com/jp/blog/best-practices/notification-with-log-message</u>
- New Relicアラートで0判定するにはfilter関数を使おう
 - <u>https://newrelic.com/jp/blog/best-practices/use-filer-fuction-if-you-want-to-detect-0-alert</u>





New Relicを活用するための様々な情報を確認できるドキュメントとなります

🅎 new relic.	Docs Developer Community Learn	@ •	ログイン	今すぐ開始				
New Relicのドキュメントへようこそ。								
	人気の検索キーワード: <u>NRQL, ログ, 集計, ベストブラクティス</u> , Kubernetes			$\overline{}$				
簡単な4ステップで開始								
 アカウント まだアカウントを せんか? こちら 	本存存成 ① New Relicの概要 ② New Relicのインストール ③ チュートリアノ New Relicの監視およびオブザーバビ リティツールの詳細をご覧ください UIC 移動し、New Relicのグンストール ③ チュートリアノ Shらウインアップ び ユタートガイド → インストール び ③ チュートリアノ	レ 記実的問題を が を読む →	祥決す					
人気のドキュメント								
すべて	Cのアプリとサービスを監視 ブラウザモニタリングをデプロイ する <u>詳細情報</u> → <u>詳細情報</u> → <u>詳細情報</u> → <u>詳細情報</u> →	<i>•</i>						



New Relic University <a>https://newrelic.com/jp/learn

New Relicについて基本から応用まで学べるコンテンツです





New Relic University (詳細)

New Relicの基礎から応用までを学べ、認定資格も取得できるセルフラーニングコンテンツです

Install	NRU 100	NRU 200	NRU 300/400	Exam
New Relic を使い始める	Observability/New Relic を知る	New Relic の主要機能を学ぶ	New Relic の使い方を体感する	資格を得る
New Relic One へのサインアッ プやエージェントインストールの 方法などのガイドを提供	New Relic One やオブザーバ ビリティに関する基礎知識を座学 にて学習	New Relic One に含まれるつ の主要機能に含まれる4の機 能群を動画で説明	New Relic One を実際に操作 し、主要機能を利用できる状態に するためのトレーニング	New Relicの知識を有しているこ とを証明するための試験、合格 すると資格バッジを授与
APM / Browser /Infrastructure/ Logs / Mobile (iOS/Android) / AWS 統合 / Azure統合 / GCP統合 インス トール手順	NRU Practitioner オブザーバビリティ入門 NRU 101 New Relic One 入門	NRU201 Telemetry Data Platform NRU202 Full Stack Closenability NRU203 Appled intelligence	NRU 301 アプリケーションとインフラ性能 観測の基本 NRU 302 ダッシュボード開発とNRQLの基 本	フルスタックオブザーバビリティ認定 試験
			NRU 303 SLI/SLO設計の基本	
			NRU 304 AlOps とアラート設計の基本	
			NRU 401 CodeStream による DevOps	
▶サインアップ方法 https://newrelic.com/jp/blog/how- to-relic/create-new-account			を想定したエラー分析対応の基本	
▶インストールガイド <u>https://newrelic.com/jp/blog/how-</u> to-relic/new-relic-faststen-guide				

Observabilityのスペシャリストを目指せ! Full Stack Observability Practitioner認定試験

【この認定試験を通じて身につくスキル】

- Observabilityの実現のためにNew Relicが取得するデータの理解と、目的に応じたデータ分析やアラート設定
- バックエンドおよびフロントエンドの問題発見とトラブルシューティング

【認定試験に向けた準備】

- New Relicの基本的な操作経験
- ラーニングパスに沿った学習

【合格者特典】

- デジタル認定証とバッジ











ロール別 New Relic ラーニングパス



New Relic サインアップのご案内

- 全機能が無料で使い放題 (1名)!
- 転送データが 100GB/月まで無料!
- 必要事項記入ですぐに利用開始!
- クレジットカード記入不要!
- 利用期限なし!

※ New Relic フリープランで始めるオブザーバビリティ!

サインアップされた方に抽選で New Relic Tシャップレゼント!! *②* 応募フォーム



🔗 <u>newrelic.com/jp/sign-up-japan</u>



New Relic実践入門 第2版 オブザーバビリティの基礎と実現





発売日:2023年12月11日 価格:3,410円(税込み)

翔泳社、Amazon等から販売中 https://www.shoeisha.co.jp/book/d etail/9784798184500



最新情報のキャッチアップにぜひ活用ください!

X(Twitter)

Qiita Organization

やってみた系の記事を公開

New Relicに関する情報発信





最新情報はこちら • <u>What's new</u> • <u>リリースノート</u> • <u>公式ブログ</u>

STATS A

https://twitter.com/NewRelicJapan

https://qiita.com/organizations/newrelic





New Relic 学習オンラインコンテンツのご案内

「New Relic を使ってアプリケーションを改善しよう」 がオンライン学習サービス Progate Path で公開されました!! エンジニアの実務に即した体験ができる実践的なコンテンツ になっており、無料で学習 することができます!!





NRUG ぬるぐで学ぶ

New Relic User Group

New Relic ユーザーが集い、実践事例 や最新機能紹介などを実施。初心者支 部や SRE 支部などが形成されており、 エンジニア同士でのネットワーキングや 信頼性の高い情報交換が可能。

ConnpassのNRUGページより ご登録ください。



© 2024 New Relic, Inc. All rights reserved.



アンケートご協力のお願い



Zoom画面を終了の際にアンケートの画面が表示されます。 是非、アンケートへのご協力をお願いいたします。

また、もっと詳しい話を聞きたい方は、 その旨を<u>アンケートにご記載</u>ください。

Thank you.

