



NRU 304 「AIOps とアラート設計の基本」

February 21, 2024

© 2023New Relic, Inc. All rights reserved

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。







Hiroko Umetsu

<u>Cloud Consultant</u>

for Gaming Industry

Infrastructure, Azure

New Relic Solutions Consultant

Safe Harbor

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

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

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

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



本セッションのゴール

 New Relicの収集データを活用した、ユーザー体験に近い 指標に基づいたアラート設定を体験する

 New RelicのAlOps機能を活用して、アラート対応の効率 化を実現する方法を知る



本セッションの想定対象者と前提条件

- これまでのインフラ監視から脱却し、ユーザー体験の悪化を迅速に知りたいと思っている
- 大量のアラートに悩んでいる、逆にアラートでは気づけない障害に悩んでいる
- アラートから素早く根本原因にたどり着きたい
- New Relicの基本的な知識をお持ちであること
- 簡単なNRQLを知っている

New Relicの知識に不安のある方はこちらを受講ください!(オンデマンド視聴可)

- <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)



Agenda

		M. WWXXWHOHITTE
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とAlOps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)

© 2024 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、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

- 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ド</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



© 2024 New Relic, Inc. All rights reserved.

S new relic. 1



© 2024 New Relic, Inc. All rights reserved.

new relic. 14

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	るサービス影響	将来のリス	くつの兆候
具体例	サイトが遅い	エラーを返す	キャパシティを 超える	リソースが 枯渇する
外形監視	チェック応答時間	チェックエラー		
フロントエンド	CWV	JSエラー		
アプリケーション	Apdex 応答時間	4xx, 5xxエラー	スループット バッチ遅延	
インフラ				各種インフラ リソース



座学(2) New Relicのアラート機能

15:15 - 15:30 (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

Critical Issue activated on Aug 13, 2023 1:49pm	Duration: 21h 53m	Last updated Aug 14, 2023 10:478
EC-site query result is > 1.0 for 5 minu Source: 🕥 🕞 Issue payload	tes on 'Alert Condition '	Close Issue Acknowledge
 Incidents (16) 		
Sort Newest to oldest ~ D Show open by	Critical Incident closed on Aug 14, 2023 10:47am Duration: 1h 35m	See NRQL overview
Critical Closed PageView query deviated from the baseline for at least 5 minutes on Created: Today 9:12am ③ 1h 35m	PageView query deviated from the baseline for at least 5 Alert Policy: ダッシュボ View/edit Condition: Condition1 View/edit C 4 3.5	i minutes on 'Condition1'
Critical Closed PageView query deviated from the baseline for at least 5 minutes on	3 25 2	MAUNA
Created: Today 8:11am () 54m	15	I.MMA M. M.
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



New Relicのアラート構造全体像











© 2024 New Relic, Inc. All rights reserved.

New Relic アラートの構成要素1: Alert Policy

ISSUE CREATION PREFERENCE

Alert Policy

Alert Conditionのグループ

Alert Condition

アラート対象や閾値、集計方法の定義

Incident

Alert Conditionで検出した個々の違反

Issue

ーつ以上の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 Specify how we create issues and group incidents into them. (You get notifications when an issue opens, is acknowledged, and closes.)



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



New Relic アラートの構成要素1: Alert Policy

New Relic のアラートは、Alert Policyという器にAlert Conditionを内包した構造となっている Alert Policyごとにアラートをグループ化したり、通知先の制御ができる

通常、送信先やアラートの目的別にポリシーを分けることが多い



NRU-Sample-Policy	・ ☆ ① Metadata	Ø Workloads ↔ R	epositories				
Get notified when issues s	start. To get notifications abo	out your issues, create a	workflow for this pol	icy. <u>See our docs</u> 🗹		Create wo	rkflow
ID: 4406018							
Alert conditions Notifications	s Settings						
O Search by condition name	orid	Condition Name = A	-			+ New alert co	ondition
Showing 6 conditions	90.000						
Alert condition	Query	Thresholds	Туре	Open issues	Last modified	Ena	
EC-site - Ajax throughput	SELECT rate(count(*	Critical: deviated frc Create a warning th	NRQL Baseline	0	Dec 27, 2023, 2:48pm		
EC-site - Throughput (ppm)	SELECT rate(count(*	Critical: deviated frc Create a warning th	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 th	NRQL Query	0	Jun 6, 2023, 4:39pm		



New Relic アラートの構成要素1: Alert Policy

Issue Creation Preference

IncidentをIssueにグループ化して、通知をまとめる設定

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

- Condition1: フロントエンドの JSエラー率 (対象サイトは1つ)
- Condition2: サーバーサイドのエラー率 (ホスト別に集計、対象ホストは3台)

設定名	Incident発生時の挙動	この例で起票されるIssue(通知件 数)
One issue per policy	同じAlert Policyから発生したIncidentを、一つの Issueにまとめる	1件
One issue per condition	同じAlert Conditionから発生したIncidentを、一つ のIssueにまとめる	2件(JSエラーで1件、サーバーサイ ドエラー全体で1件)
One issue per condition and signal	同じConditionであっても、アラート対象ごとに個別 にIssueを作成する	4件(JSエラーで1件, ホスト毎の サーバーサイドエラーで3件)



New Relic アラートの構成要素2: Alert Condition

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

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

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

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
Write your own query	Con host integrations (2 types)	I Service Levels
Use NRQL to define your alert ※詳細はこの後の章でご説明します	쵯 Synthetic monitors	VPC Networks



New Relic アラートの構成要素3: Workflow

発生したIssueと、通知先・通知内容の関連付け

Filter data

どのようなIssueで、このWorkflowを起動するか

Enrich (Additional settings内)

通知に、Issueに関する付加情報を付与する

Mute issues (Additional settings内)

Muting Rulesが設定されていた場合の挙動の設定

Notify (Destinations:後述)

通知先の定義と、通知内容のカスタマイズ

Test workflow

過去の該当データを元に、Workflowの通知テストを実行

ilter data Neet the kinds of issues you want to be the basic filter for the most comm g () Policy	o send. mon attributes or the advanced	film familiantina 🗇 Ba	
elect the kinds of issues you want to lse the basic filter for the most comm ag () Policy	o send. mon attributes or the advanced	Ba	
Policy		niter for all attributes.	isic Advanced
~	Priorit	v 🛈	
	~	v	
Additional settings Jotify Choose one or more destinations and	f add an optional message.		
now ServiceNow incidents	Webhook	Jira 🏥	Slack
Email 👸	AWS EventBridge	Mobile push	PagerDuty





New Relic アラートの構成要素4: Destinations

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





New Relic アラートの構成要素4: Destinations

Send test notification Send test notification Cancel Save Stack destination New Relic New Relic New Relic Stack destination New Relic Your user is not Select Where you want to receive notifications Pick an existing destination or create a new one. See our docs C ³ Channel Select Channel Your user is not Select from a list of variables. Custom Details (optional) This payload uses Handlebars syntax. Type "(* to select from a list of variables. Yudocs, newrelic.com/docs/alerts-applied-intelligence/applied-intelli	Email Select users and emails you want to send notifications to. See our docs Ľ ⁴ Q Search by name or email Email subject {{ issueTitle }} Custom Details (optional) This payload uses Handlebars syntaxType "{" to select from a list of variables.	 Workflows変数を用いて、柔軟に標題や 内容のカスタムができます 補足: <u>custom incident</u> <u>description</u>とは別の情報付加機 能となります。 "{{"と入力することで、Workflows変数の 補完機能を活用できます。
Iows variables: Your user is not authenticated //docs.newrelic.com/docs/alerts-applied-intelligence/applied-inte Custom Details (optional) Custom Details (optional) Your user is not authenticated Custom Details (optional) Custom Details (optional) Add a custom message at the bottom of every Slack notification. You can alist of variables. type "{" or double-press the Shift key, then select from an array of custom variables-incident-workflows/ You can alist of variables. You can alist of variables.	Send test notification	Save Slack Slack Select where you want to receive notifications New Relic Slack Select where you want to receive notifications Save Select where you want to receive notifications Pick an existing destination or create a new one. See our docs [2]
	flows variables: ://docs.newrelic.com/docs/alerts-applied-intelligence/applied-inte ce/incident-workflows/custom-variables-incident-workflows/	Custom Details (optional) Custom Details (optional) This payload uses Handlebars syntax. Type "{f" to select from a list of variables. Custom Details (optional) Add a custom message at the bottom of every Slack notification. Add a custom message at the bottom of every Slack notification. You can also select from an array of custom variables. Just the menu. You can also customize these variables with a Handlebars library. Handlebars library.

補足: Issueのライフサイクルと通知タイミング

lssue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



© 2024 New Relic, Inc. All rights reserved.



補足:アラートを設定する前にやること

Apdex Tの値を適切に設定する

- Apdexはパフォーマンスに対するユーザーの満足度を示す指標
- 特にフロントエンドはエンドユーザー側のノイズに影響されやすいため、単純な応答時間の平 均よりも有用な場合が多い

Apde	ex score	0.88 [0.37] APP SERVER	0.81 [1.7] BROWSER
0.9			
0.85	\sim		
0.8			
0.75	, A		
M	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 _⑦

0.37 seconds

Please input a decimal or whole number only.

© 2024 New Relic, Inc. All rights reserved.



補足: Apdex T値について

それを満たせばユーザーが満足すると想定される、最大応答速度

APMおよびBrowserのアプリケーションごとに設定可能 (Application Settingsメニュー)



今回監視対象のサイト

[NRUジェラートショップ](ECサイト)

このハンズオンでは、PHPおよびMySQLにより構築されたジェラート屋さんの ECサイトを モニタリング対象にしています。

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



💄 新現会員登録 🎔 お気に入り 🔒 ログイン 🏋 🙆 🛛 ¥0

NRU

新入荷 ジェラート アイスサンド





今回の環境の監視構成

- New Relic:
 - 外形監視, フロントエンド(ブラウザ), アプリケーション、インフラ







ハンズオン(0) 環境を確認する

15:30 - 15:40 (10min)



ハンズオン環境について

New Relic にログインしてください。

New Relic : https://one.newrelic.com

- ・ 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)

ユーザー名が "New Relic University Japan" であることをご確認ください

[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。 プライベートブラウジングをお使いください。

また、ブラウザは下記のいずれかをご利用ください。

- 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



🗊 Dis

(?) Hel

	New Relic University Japar japan-handson+nru@newrelic.com	Eu	l platfo	rm user
	User Preferences			
	Manage Your Plan			
	Administration			
	Theme			
	NRQL Console			
	NR-only admin functionality			
	Impersonate			
	Debug Mode			•
ussions	Manage Your Data			
User	Other Users			
Relic University Ja				



ログイン後のアカウントの切り替え

"Japan NRU(Original NR Account)" の場合は 以下の操作にて、ユーザーの切り替えをお願いします ユーザー名 > Other Users > "Japan NRU" 再度パスワードを入力し、ユーザーの切り替えを実施ください。



"Japan NRU (Original NR Account)" ではなく

ユーザー "New Relic University Japan" を利用します



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(0) Apdex Tの設定箇所の確認

変更は行わない!!!

- New Relicポータルの左ペイン の"APM & Services"を選択し、 EC-siteアプリを選択します。
- Settings → Applicationを選択し ます。

EC-site	
Application settings	
Application alias Set a name for this application in New Relic. You can change the name here without modifying the agent configuration file. This may take 5-30 minutes to propagate through your reporting agent. Alias	Any saved change will restart all agents for this application
EC-site	
Apdex T is the response time threshold value for apdex. Set a response time your users would consider satisfactory. The default apdex T for an application server is 0.5 seconds. This applies to web transactions only.	
Apdex T ① e.5 Enter a decimal or whole number only.	




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 Alert Policyを作成する 1. 2. Workflowを作成する ENRICH & CORRELATE DETECT (Option) NOTIFY Telemetry Issue Creation = □ Data Preference Metric Incidents -Issues 4 3 Alert Policy æ Incident Event Issue Workflow Alert Source now Condition Incident Issue \diamond Log ρd Decisions Trace









ハンズオン(1-1) Alert policyを作成する 1/2

- 1. Alerts&Al 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。

new relic Q Quick Find + Add Data	MALYZE : E Issues & Activity 네 Overview	Alerts & Al Alert Policies		$\left(+ \text{New alert condition} ight)$	+ Browse prebuilt elert conditions	+ ∜ Ask AJ @ + New Alert policy
All Capabilities All Entities	DETECT Alert Conditions Alert Policies	Q. Search by policy name or id Showing 4 policies	Policy Name = All	Onen issues	# of conditions	
Alerts & Al C Alerts & Al C Query Your Data APM & Services Logs Traces	د Anomaly Detection Alert Coverage G Beta connectate م ⁴ Sources م ⁴ Decisions	NRU-Sample-Policy NRU環境整備 Service Levels default policy for account 2940716 ダッシュボードハンズオン用アラートポリシー		0	6 2 1	
Synthetic Monitoring Infrastructure Kubernetes Browser Infrastructure Kubernetes Froms Inbox Apps Car Service Levels	EMBCH & NOTEV Muting Rules "" Workflows Destinations AETTHIOS G General					
we have a second	operved					

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
- 2. <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
- 3. [Suppress noise...]をチェック
- 4. [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

Er	nter a short, descriptive name
Inc	ident Grouping
Gro	oup incidents within this policy
Tell issu	us how you want to group incidents from this policy in ues. You get notified based on issues, not incidents.
0	One issue per policy
0	One issue per condition
0	One issue per condition & signal
Thi	s may create a large number of notifications.
Gro	oup with other incidents from other sources
	Suppress noise with machine learning correlation
We	II analyze incidents from all policies and sources and
	ted incidents into issues. See our docs 14

S new relic



ハンズオン(1-2) Workflowを作成する 1/6

- 1. Alerts & AIメニューの Workflowsをクリックし、[+ Add a workflow]をクリックします
- 2. ご自身のworkflowであることがわかる名前を入力し ます
- 3. Filter dataで"Advanced"を選択し、次のフィルタを 設定します
 - a. Select or enter attribute: policyName
 - b. Select operator: exactly matches
 - c. Select or enter value: 作成したポリシーを選択
- 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。

	-				
LYZE	Alerts & Al			0 4	Ask Al
Issues & Activity	Workflows				
Overview	Workflows Issue notifications log	1			۱. The second
ECT			1		
Alert Conditions	Set up and customize your alert notifi and how much information they recei	cations. Decide who ve.	gets notified, in what tool	+ Add a w	orkflow
Alert Policies	Q. Search by workflow name or em	ail address +			
Anomaly Detection	Showing 1 workflows				
Alert Coverage G Beta	100	100		1.22.05.13	
RELATE	Name	Destinations	Last run	Enabled	
Sources	Policy: 49/52/2 - NRU18965298	Email			
Decisions					
ICH & NOTIFY					
Muting Rules					
Workflows					
Destinations					

echane would be				
velit a unique, descriptive	i name you'll recognize later			
ilter data			3	Need help?
et the kinds of issues y the basic filter for the r	ou want to send. nost common attributes or th	e advanced filter for all attribu	tes.	dvanced Workflow docs 🖻
accumulations policyNam	exactly matches	NRU304-Policy × 🕗		
+ AND			(× C)	oar filters
Additional settings				
otify				Destination Docs 17
loose one or more destin Id channel	ations and add an optional m	essage.		Manage dectinations [2] Workflow triggers [2]
ServiceNow	S Webhook	art 🔕	Slack	

ハンズオン(1-2) Workflowを作成する 2/6

- 4. Notify: Emailを選択します
- 5. メール送信内容を設定します ご自身のメールアドレスを入力して下さい。
- 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

Choose of message	one or more destinations and add an optional	Akaizawa@newrelic.com		<u>@</u> ×
		NOW ServiceNow incidents	S Webhook	Jira
		Slack	Email	AWS EventBridge
	/	PagerDuty		-
2 999				
Fest this We'll use configure	a workflow existing data from your account to test what you've ed and send a sampli notification.	Test workflow We found a p	oossible problem above.	
				Cancel Activate workflow
	Email			
6	Email Select users and emails you want to send notification Q. Search by name or email	s to. See our docs \mathbb{M}^{n}		
5	Email Select users and emails you want to send notification Q. Search by name or email	ns to. See our doos. Si		
5	Email Select users and emails you want to send notification Q. Search by name or email Email subject (f issueTrite))	n to. See our door. S		
5	Email Fried users and emails you want to send notification Q. Search by name or email Email subject ((issue/Title)) Custom Details (optional)	as to. See our docs. G		
5	Email Final systematic send notification Government Email subject ((issueTite)) Custom Details (optional) This payroad uses Haindelears syntauType "()" to se	s to. See our docs 15" ect from a fat of variables.		
5	Email First V First	n to. See our doos C ^{ar}		
5	Email	is to: See our docs G [*]		
5	Email Field users and emails you want to send notification Q. Search by name or email Email subject (f issueThin)) Custom Details (optional) This payload uses Handlebars syntaxType "((" to se	n to. See our doos G [*]	Cancel (7)	

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。

Critical priority	ssue is closed	
Memory l minutes o	Jsed % is more than 90 for at least 2 on 'Some-Entity'	
Issue duration:	5 minutes	
Go to issue		
incidents		
impacted er	itities	
impacted er • ip-172-31-26	tities 144.ap-northeast-1.compute.internal	
e impacted er • ip-172-31-26 Nert Policy Policy Name	tities 144.ap-northeast-1.compute.internal NRU-Sample-Policy	
impacted er • ip-172-31-26 Vert Policy Policy Name Condition	tities 144.ap-northeast-1.compute.internal NRU-Sample-Policy NRU-Sample-Web transaction time (Baseline)	
e impacted er • ip-172-31-26 Nert Policy Policy Name Condition Runbook	NRU-Sample-Policy NRU-Sample-Policy NRU-Sample-Web transaction time (Baseline) https://docs.newrelic.com/docs/alerts-applied- intelligence/new-relic.alerts/advanced- alerts/understand-technical-concepts/provide-runbook- instructions-alert-activity/	
e impacted er • ip-172-31-26 Vert Policy Policy Name Condition Runbook NRQL	tities 1144.ap-northeast-1.compute.internal NRU-Sample-Policy NRU-Sample-Web transaction time (Baseline) https://docs.newrelic.com/docs/alerts-applied- intelligence/new-relic.alerts/advanced- alerts/understand-technical-concepts/arovide-runbook- instructions-alert-activity/ SELECT count(*) from Hetric	

nstrumentation name: apm language: php type: APM Baseline enabled: true arentVersion: 10.10.0.1 id: 32666626 accountid: 3940716 affectedService: service!

affectedService: service2 causeService: Service1 causeService: Service2 instrumentation.provider: newRelic nr.tracing: standard policvid: 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

Test this workflow We Gue a a sample motification. We fund a possible problem ab	nail AWS EventBridge
Test this workflow We fuse existing data from your account to test what you've Test workflow We fuse as asengli notification. We fuse the asengli notification. We fuse the asengli notification. We fuse the asengli notification.	nail AWS EventBridge
Test this workflow We Tuse existing data from your account to test what you've Test workflow We found a possible problem ab	
Email	Cance
Select users and emails you want to send notifications to. See our docs 12" Q. Search by name or email	
Email subject	
5	
Custom Details (optional)	1
This payload uses Handlebars syntaxType "((" to select from a fist of variables.	
6 Bend test hutflication	⊘)

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 & Al > 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。

ANALYZE	Alerts & Al						© 2
너 Overview	Destinations						
📃 Issues & Activity	Add a destination						
DETECT	Add destinations when	e we send notifications.					
Q Alert Conditions & Policies	s lira	DOW ServiceNow	Slack	S Webbook		AWS	
Anomaly Detection	• • • •			6	I regerberry	EventBridge	
🗞 Alert Coverage G Beta							
CORRELATE	Notifications Log	Destinations (1)					
^{뇌분} Sources	Manage destinations v	where we send notification	S.				
+ Decisions							
ENRICH & NOTIFY	₹ • Searci	1					
🗞 Muting Rules	Ty 🗘 Name 🗘	Tw	o URL/Details		Last updated 0 L	Jpdated by C Enabled	0
୍ୟୁ Workflows New	NRU304	メール通知サンプル	smitsui+nru30	4@newrelic.com	Jun 5, 2023 6:4 1	004932171	•
Destinations							



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						()		
Add a destination Add destinations wh	n here we send notifications.							
Jira	NOW ServiceNow	Slack	Kebhook	PagerDuty	AWS EventBridge	Mobile push	有効	無効
Notifications Log	Destinations (1)							0
Manage destinations	s where we send notification	15.						
Ty 🗘 Name	≎ Tw	o URL/Details		Last updated 🗘 Up	dated by 0 Enabled	10		
NRU3	04 メール通知サンプル	smitsui+nru30	4@newrelic.com	Jun 5, 2023 6:4 10	04932171			
Ту 🗘	Name 🗘		Two URL/	Details		Last updated	○ Updated by ○ Enabled ○	
	NRU304 メール通	通知サンプル	smits	ui+nru304@ne	wrelic.com	Jun 5, 2023 6:	4 1004932171	



座学(3) アラートコンディションの作成 <u></u>

16:00 - 16:20 (20min)



© 2024 New Relic, Inc. All rights reserved.

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? Use guided mode Recommended Choose from options and we'll build your query Write your own query Use NRQL to define your alert



New Relic アラートの構成要素2: Golden signal or Metric

Golden Signalをベースにそれぞれの機能に合わせて、ガイド付きで簡単にアラート条件を作成





New Relic アラートの構成要素2: Windows Duration

アラート条件ごとに、この集計ウインドウの期間を Window Duration 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。



1 new relic.

© 2024 New Relic, Inc. All rights reserved.

Sliding Window(オプション)

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、指定した時間分スライドさせ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。





New Relic アラートの構成要素2: Streaming method

Event Flow

頻繁かつ一定間隔で発生するデータに対するアラート設定に最適な方式です。 許容される遅延時間(Delay)よりも後に続くデータが到着すると、集計ウィンドウが閉じられ ます。





New Relic アラートの構成要素2: 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。





データ転送の頻度を加味した設定例

5	データソース	説明	Streaming method	Delay/Timer
クラウド統 合	GCP, Azure, AWS API Polling	ポーリングのため離散的にデータが届くこと、およびAWS Cloudwatchとポーリングのタイムラグを考慮	Event Timer	ポーリング間隔以上
	AWS MetricStream	ストリーミングでコンスタントにデータが到着する。AWS Cloudwatch側のタイムラグを考慮	Event Flow	10分前後
Infrastructu 含む)	ireエージェント(OHI	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	デェント	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⊥-	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⊥—	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	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)
APIによる東	云送	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vent Timerが適切

New Relic アラートの構成要素2: 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 合には、Cadenceが有効です。



補足: Gap-filling strategy

• Gap-filling strategy

集計結果が存在しない集計ウィンドウ(ギャップ)を検出した場合に0、任意の値、直前の集計結果のいずれかで、その期間の集計結果を埋めることができます。

ただし、集計結果が存在しないことを検出してギャップを埋めることができるのはNRQLクエリのWHERE句に該当する集計対象データが新た に到着したタイミングであり、集計対象データが存在しない状況をリアルタイムで検出して置換するものではない点に留意してください。





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/docs/alerts-applied-intelligence/new-relic-alerts/alert-condition ns/create-baseline-alert-conditions	エラー発生割合がいつもよりも増 加した



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) <u>アラート定義のガイダンス | New Relic</u> (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 ~
(+) Add threshold			for at least at least once	in		



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(<u>参考情報</u>)
- 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) (i)	
4,000 character limit	
Runbook URL (optional)	
https://	
Enable on save	





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



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



ハンズオン(2-1) Alert Conditionを作成する 3/21

- 1. Alerts&Al 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。

	ANALYZE Issues & Activity	Alerts & Al Alert Policies				⑦ ☆ Ask Al ∂	
+ Add Data	년 Overview			+ New alert condition + Br	owse prebuilt alert conditions	+ New alert policy	
BB All Capabilities	DETECT	Q. Search by policy name or id	Policy Name = All				
All Entities	Alert Conditions	Showing 5 policies					
Dashboards	Alert Policies	Name		Open issues	# of conditions		
① Alerts & Al	Anomaly Detection	NRU-Sample-Policy		//01	6	566	
Query Your Data APM & Services	CORRELATE	NRU環境整備		0	2	144	
2 Logs	" [#] Sources	Service Levels default policy for account 394071	6	1			
Traces	+\$+ Decisions	これがあなたのポリシーです。					A New alert condition
슬 Synthetic Monitoring	ENDICH & NOTIFY	ダッシュボードハンズオン用アラートポリシー		765			
1 Infrastructure	🛞 Muting Rules						
Kubernetes	⇒le ⁿ Workflows						
Browser	Destinations						
Mobile	SETTINGS						
Errors Inbox	General						

ハンズオン(2-1) Alert Conditionを作成する 4/21

• 「Browser applications」を選択し、設定画面を進みます。

Tell us where to look ①						
	Browser applications	🗏 Hosts				
C On host integrations (2 types)	□ Service Levels	③ Services - APM				
兽 Synthetic monitors	VPC 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。

Select the entities to watch (max 20)		
Search entities by name or attributes. If you create new	v entities with these attributes, we'll watch those as well.	
All Selected 1		
😇 Filter by name or tags		
Entities 🗘		
C-site		
nami-react-app)	
📄 🐞 nami-react-app		
 nami-react-app Select a metric to monitor 		
Select a metric to monitor Golden metrics Other metrics		
Select a metric to monitor Golden metrics Other metrics Throughput (ppm)	Largest contentful paint (75 percentile) (s)	First input delay (75 percentile) (ms)
Select a metric to monitor Golden metrics Other metrics Throughput (ppm) Errors	Largest contentful paint (75 percentile) (s) Pageload time (s)	First input delay (75 percentile) (ms)
nami-react-app Select a metric to monitor Golden metrics Other metrics Throughput (ppm) Errors review chart for pageload time (s) (past 6 ho	Largest contentful paint (75 percentile) (s) Pageload time (s) urs)	First input delay (75 percentile) (ms)
Select a metric to monitor Golden metrics Throughput (ppm) Errors review chart for pageload time (s) (past 6 ho	Largest contentful paint (75 percentile) (s) Pageload time (s) urs)	First input delay (75 percentile) (ms) Ajax throughput (rpm)



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. Severity level** a. Critical
- 5. 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。

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



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。

Add details				
Name your alert condition *				
Use a clear name that indicates what's wrong				
Close open incidents after () 3 days ~				
Send a custom incident description (optional)				
4,000 character limit				
Runbook URL (optional)				
https://				
C Enable on save				
	Cancel	View as code	Save condition	

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 印 Infrastructure Good	シーです。 🔹 🖒 Tags 🕕 Metada	ta 💿 Workloads				9	? ?
@: Summary	ID: 4932576						
MORE VIEWS	Alert conditions Notifications Settings						ondition
IIII Events explorer	Q Search by condition name or id	Condition N	ame = All +				
E Logs	Alert condition	Query	Thresholds	Туре	Open issues	Enabled (i)	
	とってもわかりやすいコンディション名	SELECT average(duration) as 'P	Critical: above 1 for 5 minutes Create a warning threshold	NRQL Query	0 0		



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)


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 v v (1) Metadata (Workloads Repositories				⑦ 💸 Ask	AI c ²
ID: 5106997							
Alert conditions Notifications Settings	i						
						+ New alert co	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 13/21

- 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。

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

 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 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。







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。
- 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。

Add details	
Name your alert condition *	
とってもわかりやすいコンディション名	
Close open incidents after () 3 days ~	
Send a custom incident description (actional)	
ここに記述した情報が、Incidentの詳細情報としてアラート内に記載されます。	
4,000 character limit	
Runbook URL (optional)	
https://www.yahoo.co.jp	
C Enable on save	Cancel (> View as code Save condition
Enable on save	



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)



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 Use 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。 **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。
 - Fine-tune your signalの値は初期値の ままにする。
- 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 (Ū			
Threshold direction Upper Open incidents with a: Severity level Critical ~ When a query returns a value.	r and lower ~			
by 3 standard deviation	on(s) for at least ~ Fewer inci	5 v	v minutes v	Ş
 ⊕ Add threshold ⊕ Add lost signal threshol 	old			
				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)



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。
 - Fine-tune your signalの値は 初期値のままにする。
 - 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 thresholds	
• Static (i) 🔿 Anomaly (i)	
Open incidents with a:	
Severity level Critical ~	
When a query returns a value above or equal to ~ 1 at least once in ~ 5 ~	
Add threshold	
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'





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



© 2024 New Relic, Inc. All rights reserved.



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

🕥 new relic	ANALYZE	Alerts & Al
O ulick Find	i⊟ Issues & Activity	Issues & Activity
+ Add Data	overview	Issues Incidents Anoma
	DETECT	
🗐 All Entities	Q Alert Conditions	C Flitter by ID or names
Dashboards	Alert Policies	Snow timeline
() Alerts & Al	o Anomaly Detection	4
🕞 Query Your Data	ද්දී Alert Coverage G Beta	2
APM & Services	CORRELATE	0



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。

erts & Al													0
sues &	Activity											< 🕒 S	ince 60 minutes ago (GMT+9) 🐱
O Filter by	cidents Anoma	alies Postmort	tems										You're seeing the latest issue
Show	timeline												
1 0.8													Are you seeing all the problems?
0.4 0.2 0													We use machine learning to recommend alerts for services that need them.
4:24	4pm 4:29pm Medium • High •	4:34pm Critical	4:39pm	4:44pm	4:49pm	4:54pm	4:59pm	5:04pm	5:09pm	5:14pm	5:19pm	5:24pr	See alert coverage gaps
State	Priority	Created ↓	Duration	lssue na	me			Entity name			Notified	Contains	Actions taken
Active	Critical	32m ago	30m	Transact	ion query d	eviated from	the b	EC-site	+1	1		2 incident	···

New relic. 91

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

ransaction query deviated from the baseline fo purce: 🕥 Notified: 🗹 🖃 Issue payload	or at least 5 i	ninutes 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
icraterus (2) rrt by Newest to oldest ~ Shov Critical Open NRU304-Synthetic Check query result is >= 1.0 on 少し複雑な コンディション名	w open only	Critical Incident opened on Nov 17, 2023 5:01pm See NRQL overview) … Duration: 28m 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 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' Opened: Today 4:53pm	© 28m	Signal over time Synthetic checks Failure screenshot Incident period •
		1 05 0
		25pm 4:30pm 4:30pm 4:40pm 4:45pm 4:50pm 5:00pm 5:00pm



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 NR	U304-	Synt	s active hetic Che s'	eck query	result is >	= 1.0
	Acknowledge		Close issue	e Go	to issue	
l cor	related i	ssue	s			
Ve've i	used corre	lation t	to merge new i	ssues into your	active issue	tes on
Veve • D 2	used corre ransaction IRU304-ba	duery seline	to merge new i deviated from	ssues into your the baseline fo	active issue r at least 5 minu	tes on
Veve • D	used corre ransaction IRU304-ba	lation t query seline	o merge new i deviated from	ssues into your the baseline fo	active issue r at least 5 minu	tes on
We've i • D 12 3 inci	used corre ransaction IRU304-ba dents	query seline	o merge new i deviated from	ssues into your the baseline fo	r active issue r at least 5 minu	tes on
We've i D D D M S inci • N	used corre ransaction IRU304-ba dents RU304-Syr	ation t query seline	to merge new i deviated from Check query re	ssues into your the baseline fo esult is >= 1.0 o	r active issue r at least 5 minu n 'Synthetics'	tes on
We've i D D D D D D D D D D D D D	ansaction RU304-ba dents RU304-Syr Since 34 1	ation t query seline:	o merge new l deviated from Check query ri es ago until 4	ssues into your the baseline fo esult is >= 1.0 or minutes ago	r active issue r at least 5 minu n 'Synthetics'	tes on
We've i 1 1 1 3 inci • N	used corre ransaction IRU304-ba dents RU304-Syr Since 34 r	ation t query seline' athetic minute	o merge new l deviated from Check query re es ago until 4	ssues into your the baseline fo esult is >= 1.0 or minutes ago	: active issue r at least 5 minu n 'Synthetics'	tes.00
We've i 1 1 2 3 inci • N	used correl ransaction (RU304-ba dents RU304-Syr Since 34 r	ation t query seline:	o merge new i deviated from Check query rr es ago until 4	ssues into your the baseline fo esult is >= 1.0 or minutes ago	active issue r at least 5 minu n 'Synthetics'	tes.on
We've i 1 1 1 3 inci • N	used corre ransaction IRU304-ba dents RU304-Syr Since 34 1 1 0.5	lation t query seline' sthetic minute	o merge new i deviated from Check query re es ago until 4	ssues into your the baseline fo esult is >= 1.0 or minutes ago	active issue r at least 5 minu n 'Synthetics'	tes.on
We've • Li 2 3 inci • N	used corre ransaction IRU304-ba dents RU304-Syr Since 34 r 1 0.5 0	lation t query seline: athetic minute	io merge new l deviated from Check query ro	ssues into your the baseline fo esult is >= 1.0 or minutes ago	active issue r at least 5 minu n 'Synthetics'	tes.on

© 2024 New Relic, Inc. All rights reserved.





座学(4) New Relicのアラート分析支援機能と AlOpsを使った異常検知

16:45 - 16:55 (10min)



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



#105				0.20				
NCIDENTS ## 101	Resolved						· Critical · High	· Madium # 14
_						1		
						-		
						1		
		_			-			
			-					
10-15 AM	10:20 AM 10:25 AM 10	CBO ANI		FOLTS ANY	10:49 AM 10:66 A	M - 10:44 AM	10.54	200 B
+ Show more	1020 AM 1023 AM 10	C30 ANA		HEES AN	10.45 AM 10.44 A	M - 10366 AM	12.54	A 00
to 15 AM	1620 AM 1625 AM 10	CIO AGO		FOLIES ANY	1049 AM 1844 A	M - 10.94 AM	10.04	888 200
10-15 AM - Show more ed activity UPDATED	1620 AM 1025 AM 10	C10 AM	SOURCE	STATE	ALATEO EVENTS	PAYLOAD	ANAL VZE	NEW RELIC ORM
ed activity 2, 10:41am	1020 AW 1025 AW 10 22 7014 Wetherball is having latency problems feaching data from Plan Service	10 AM	source pr	STATE Closed	1046AM 1046A ARLATED EVENTS 2	PAYLOAD	ANALYZE	NEW BELIC ORM
ed activity 2 2, 10:41am 2, 10:41am	1620 AM 1625 AM 10	10 AM	source pri	STATE Closed Closed	10.00 AM 10.00 A	PAYLGAD	ANALYZE	NEW RELIC ORM
10.15 AW - Show more ed activity 2, 10.41am 2, 10.41am 2, 10.42an	biblio Axe 16,05 AXE 10 22 TYRE Weithybrid is having intensy problems feathing data from Plan Service Exerce rate With requested time > 500 milliassends for at heart 5 minutes on Weithybrid ig 17 Exerce rate	යා සා ස් ස්	source pr O	STATE Dosed Oosed Oosed	IDARAM IDARA REATED EVENTS 2 2 2	PAYLOAD 02 02 02	ANALYZE Q, Analyze	NEW RELIC ORD
10.15.Aur Carlos Show more Carlos Show more C	biblio Axe tip 22 AXE TOTAL TOTAL	යා සං ස් ජේ ජේ	source (e) O O	STATE Dosed Dosed Dosed Dosed	10.01.04 MELATIO EVENTS 2 2 2 2 2	PAYLOAD 02 02 02	ANALYZE Q. Analyze	NEW RELIC ORD
10.15.444 + Show more ed activity 2, 10.41am 2, 10.41am 2, 10.43am 2, 10.43am 2, 10.43am	biblio Axe tic25 xxe tic2 v	ය ස් ස් ප් ප් ප්	source (e) O O O	STATE Dused Dosed Dosed Dosed Dosed Dosed	0.00.00 ARLATO DUDIT 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PAYLOAD III III III III III III III I	AMARVZE Q. Analyse Q. Analyse	NEW RELIC ORM
(0.15.447 - Show more ed activity 2 2, 10.41am 2, 10.41am 2, 10.41am 2, 10.41am 2, 10.43am 2, 10.43am	biblio Axee 1620 AXe 10 22 Trice WebPurchal In bueing leasency problems frechning data from Flam Service Environale WebPurchal In bueing leasency problems frechning data from Flam Service CPU Axe > 55 frect allowed from the 72:03 Poists CPU Axe > 55 frect allowed from the poist Services on Shipping for factors VebPorted in bueing leasency problems frechning data from Flam Service WebPorted in bueing leasency problems frechning data from Flam Service WebPorted in bueing leasency problems frechning data from Flam Service	යා ස් ස් ස් ස් ස් ස් ස්	source pri O O O O pri	STATE Dosed Obsed Obsed Obsed Obsed Obsed Obsed	60.00 M. 10 M A ABLARIO PAYMES 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PAYLOAD III III III III III III III I	AMALVZE Q. Analyze Q. Analyze	NEW RELIC ORM
(0.15.447 - Show more ed activity 2 2, 10.41am 2, 10.41am 2, 10.41am 2, 10.41am 2, 10.43am 2, 10.43am 2, 10.43am	biblio box Biblio	යාංශ ස් ස් ස් ස් ස් ස් ස්	5000ACE (AT (C) (C) (C) (A) (C) (C) (C) (C) (C) (C) (C) (C) (C) (C	STATE Closed Closed Closed Closed Closed Closed	0.00.04. 10.04.4 REATO PYINTS 2 2 2 2 2 2 2 2 2 2 2 2 2	PAYLOAD III III III III III III III I	ANAAYZE Q, Analyze Q, Analyze	NEW RELIC ORM
(135.44)	biblio boxe biblio boxe biblio boxe biblio boxe biblio boxe biblio boxe 22 Image: State of the state of	200000 201 201 201 201 201 201 201 201 2	500KCF (07 0 0 0 0 0 0 0 0 0 0	TTATE Oosed Oosed Oosed Cosed Cosed Cosed Cosed Cosed Cosed	0.00.04. 10.04.8 80.8470 PVMT 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PATLOND (1) (1) (1) (1) (1) (1) (1) (1)	AMAALYZE - Q, Analyze Q, Analyze	NEW RELIC ORM
(1335 AW - Show more ed activity 2, 1043am 2, 1043am 2, 1043am 2, 1043am 2, 1043am 2, 1043am 2, 1044am	biblio boot 1525 AW 10 22 Image: State S	200000 201 201 201 201 201 201 201 201 2	3004KCF 00 00 00 00 00 00 00 00	STATE Closed Closed Closed Closed Closed Closed Closed Closed Closed Closed	0.00.00 ARLATIC DODITS 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	PAYLOAD (1) (1) (1) (1) (1) (1) (1) (1)	ANALYZE Q. Analyze Q. Analyze	NEW RELIC ORN A 300 300 300 300 300 300 300 300 300 3



診断2: Correlationによる根本原因の示唆



		厦 合 Share
bind Cristal 2b response time > 700 milliseconds for at least 10 minu	tes on 'Plan Service'	③ 24m Mar 15, 11:57an
s O pd → ∰		
sue summary		e: ^
Analysis summary © Golden signals: Latency 🖓 📩 💿 Related components: Applicatio	Suggested respond	ers
pacted entities (1)		
Plan Service		Deployment events Q. Anomaly overview Entity overview
pot cause analysis	Error logs (3)	Attributes to investigate (3)
oot cause analysis eployment events (3) Jeployments. ① Last 12h	Error logs (3) error logs Since Mar 15, 111 (Earn Unit Mar 15, 111 (Earn	Attributes to investigate (3) Plan Service Outbase duvation (and larged by Datastore type and Table and Operation
eployment events (3) beployments ① Last 12h Deployment. 1m after issue created	Error logs (3) error logs Sonce Mar 15, 111 Earn Uniti Mar 15, 11 (Klaim 1	Attributes to investigate (3) Plan Service Gutabase invasion (ms) faceted by Datastere type and Table and Operation d3 k
bot cause analysis ployment events (3) peloyments Deployment Deployment Deployment Tm after issue created Application: Plan Service Deployer garker@telco.nedemo.com Revision: Hothic Filong bad query	Error logs (3) error logs 1 1 5.8 0.6 0.4 0.2	Attributes to investigate (3) Plan Service Contracted by Datastore type and Table and Operation
boot cause analysis polyment events (3) Peployment	Error logs (3) error logs Simile Mar 15, 111 Itani 8.8 0.6 0.6 0.4 0.2 0.4 0.4 0.4 0.4 0.4 0.4 0.4 0.4 0.4 0.4	Attributes to investigate (3) Plan Service Outbase function (mm) factried by Datastere type and Table and Operation 01 04 04 04 04 05 04 05 04 05 05 05 05 05 05 05 05 05 05
boot cause analysis beployment events (3) Deployments Deployment Deployment Deployment Deployment Deployment Deployment	Error logs (3) error logs Binon Mar 15, 111/Kam Until Mar 15, 114/Kam 1 58 56 56 56 56 56 56 56 56 56 56	Attributes to investigate (3) Plan Service Catabase duration (ms) Statistic by Datastere type and Table and Operation 04 05 05 05 05 05 05 05 05 05 05



対処: ITSM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) a 診断 Webhook now. ServiceNow Jira Slack AWS イベントの相関分析 根本原因分析 803 Mobile push PagerDuty Email EventBridge 対処 (外部ITSMツール: Servicenow, Pagerduty等)



機能紹介: Alert coverage gaps

Alert coverage gaps

Some of your services don't have alerts set up. Our machine learning engine recommends adding these alerts. See our docs 🗗 設定すべきアラートを通知します。 0% covered 1 entities Services - APM 現行ではAPMのみを対象としています。 Name 🗘 Error Rate Action Throughput EC-site 39.35 rea/min 0% Add alert Create an alert condition Account: 2511671 - NewBallet. Mueralty-Jacan Enter condition name Add an alert EC-site - Apdex EC-site Define your signal Add recommended conditions Enter NBQL Query (7 SELECT apdex(apm.service.apdex) FROM Metric WHERE entity.guid = 'NjUxMTYJNXxBUE180VB0TELD0VRJT058N001MDAwMDk3' FACET entity Our power users add these conditions to similar entities. .guid For help with rull values \$2, loss at signal \$2, or other query options, see our docs \$2 Highly recommended Critical EC-site - Error Percentage Y Threshold type: Baseline Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s). 1 Critical EC-site - Apdex ~ Threshold type: Baseline Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s). Critical EC-site - Response Time (Web) 0 · Threshold type: Baseline · Outry small · Average many small · Critical establi Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s). 2 critical violations for displayed time series Preview charts are estimates only. These charts use your stored data to show how this signal might create incidents. They don't consider all aspects of streaming analytics (in.g., cadence, mall values, signal loss. Red data page Next Set your condition thresholds Select policy to get notified Threshold Type: 🗍 Static 🗿 Anomaly Anomaly is useful when you want to define more flexible thresholds that adjust to how your data behaves. You'll get notified only when something behaves abno See our docs (3" Looking for more options? () Set up an alert from scratch. Threshold direction: Upper and lower -

 $^{\odot 2024 \text{ New Relic, Inc. All rights reserved.}}$ Alerts & AI \rightarrow Alert coverage gaps



機能紹介: Correlate (Decisions)

Alerts & Al \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

onew relic	ANALVZE	Alerts & Al				0	🔆 Ask
Q Quick Find + Add Data	三 Issues & Activity 团 Overview	Decisions				+ Creat	e new d
All Capabilities All Entities Dashboards	Alert Conditions Alert Policies	These rules provide the logic we use to group in	cidents and reduce yo	our alert noise. See our docs	đ		
① Alerts & Al	66 Anomaly Detection	Your decisions (14) Suggested decisions					
🗊 Query Your Data	Co Alert Coverage G Beta	Name and description	Correlations	Created by	Last edit	Enabled	
APM & Services Logs	correlate a ^K Sources	Application Anomalies and Violations wit Correlation activated because the anom	0	New Relic Al Global decision	Jan 6, 2023 1:45pm	•	
ITraces 魚 Synthetic Monitoring	Decisions	Same New Relic Condition and Title Correlation activated because New Relic	0	New Relic Al Global decision	Nov 19, 2022 8:20am	•	
10 Infrastructure	🔆 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	tions are generated from the same application
New Relic AI - Global decision 0 likes 0 dislikes	
Decision logic	 Rule analysis No results found
Correlate by attributes	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AIOps機能を活用して、アラート分析を効率化しましょう





お疲れ様でした!



New Relic サインアップ&応募 抽選で



プレゼント!



bit.ly/3CLGgZC



New Relicサインアップ登録で 抽選でNew Relic Tシャツが当たります! (毎月抽選)

応募ステップは下記①と②だけ!

① New Relic 無料サインアップ(Link)

② New Relic Tシャツ応募フォーム(<mark>Link</mark>)




New Relic (ずっと) 無料サインアップ Link

1名のフルユーザーアクセス、100GB/月のデータ保存容量



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



New Relic University 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	Observabili ty/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3つの主要機能に含まれ る54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 Observability NRU203 Applied 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 NRU 303 SLI/SLO設計の基本 NRU 304 AIOps とアラート設計の基本 NRU 401 CodeStream によるDevOps を想定したエラー分析対応の基本 	フルスタックオブザーバビ リティ認定試験
▶ <u>サインアップ方法</u> ▶ <u>インストールガイド</u>	▶オンデマンドセミナー (<u>practitioner</u>), (<u>nru101</u>)	▶ <u>主要機能解説動画</u>	▶ <u>開催スケジュール</u>	▶ <u>受験サイト</u>



ロール別 New Relic ラーニングパス



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。 (<u>https://nrug.connpass.com/</u>)





本当にお疲れさまでした。



最後となりますが、 是非、<u>アンケートへのご協力</u>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<u>アンケートにご記載</u>ください。

Thank you.

I))