

NRU 304 New Relic ハンズオン Alerts & AlOps

Koji Aizawa June 08, 2022





Koji Aizawa

<u>Business</u> Building a Digital Platform and Services

Cloud Computing

AWS - EKS, ECS, Fargate, etc.

<u>Specialities</u>

kubernetes on AWS, containers



Twitter: <u>@kaojiri</u>

"Containers Power to Enterprise"

Safe Harbor

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

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

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

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



本日のゴール

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



本セッションの前提条件

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

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

- <u>New Relicの基礎</u>
- <u>ダッシュボードワークショップ(NRQL</u>入門編に相当)



Agenda

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





突然ですが

どんなアラートを設定していますか?





アラートを設定する目的

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

- 1. システムの停止、またはパフォーマンスの悪化が発生し、ユーザーへのサービス提 供に支障が出ている
- 2. 1のような事象が近いうちに発生する可能性がある兆候が出ている

<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



^{© 2022} New Relic, Inc. All rights reserved

new relic. ¹²

アラートのこれまでと、New Relicを使ったこれから



© 2022 New Relic, Inc. All rights reserved

13 new relic. 13

目的別、アラート設定例(Webアプリの一例)

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



New Relicのアラート機能

New Relicが収集しているありとあらゆるデー タを使って、アラートを設定することが可能

アラートを設定すると、アラート条件に従っ てインシデントが起票され、通知を受けるこ とができる

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



New Relicのアラート構造全体像 ALERTS i Notification CLASSIC Channel ß ********* DETECT 1 **IBIncident H**violation Incidents $(\mathbf{2})$ Issues Alert Policy Telemetry Data Incident Issue Alert Incident <u>=</u> □ Metric Condition Preference **(4)** Incident Issue 3 Issues Source ર્સ Event Issue Workflow now. Issue Anomalies Decision Log 0 Anomaly Anomaly Configuration CORRELATE ENRICH & Trace Anomaly (Option) NOTIFY i Notification Settings ß 設定 オブジェクト

New Relic のアラートは、Alert Policyという器にAlert Conditionを内包した構造となっている Alert Policyは複数のAlert Conditionを内包し、送信先を制御できる

通常、送信先やアラートの目的別にポリシーを分けることが多い

Alert Policy	アラートポリシー ③ Incident preference: By condition ③ Delete this policy id: 545592
Alert Condition (例: フロントエンドApdex)	2 Alert conditions 2 Notification channels Last modified Feb 7, 4:13 pm by Akihiro Ito
Alert Condition (例: DBレスポンス)	Search conditions
Alert Condition (例:サーバーサイドエラー)	All Entitles Sign diskUsedPercent > 90 for at least 2 mins Image: diskUsedPercent > 70 for at least 2 mins
Alert Condition (例:JSエラー)	APM APPLICATION METRIC BASELINE Web transaction throughput (Baseline) modified Nov 19, 338 pm by Akihiro Ito P Edit 🖄 Copy 🖀 Delete Office
: :	Image: Web transaction throughput deviates from baseline for at least 5 mins Image: Web transaction throughput deviates from baseline for at least 5 mins



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

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

ect a pro	duct				
IRQL	APM	Browser	Mobile	Synthetics	Infrastructure
~ L	7 11 101	DIOWSCI	mobile	Synthetics	mastractare



アラートのしきい値設定は2種類から選択可能

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



しきい値を超過した場合のアラート発報タイミング

• For at least xx minutes

しきい値をxx分継続して超過した場合のみIncidentが起票される

• at least once in xx minutes

しきい値を1回でも超過した場合にIncidentが起票される



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

その他条件の設定に関する詳細は以下参照:

https://newrelic.com/jp/blog/how-to-relic/alert-configuration-guidance



効果的な通知を送るためのプラクティス

Additional settingsのRunbook URLを設定することにより、
 アラート発報時に対応手順へのリンクにすぐにアクセスすることが可能

\sim	Additional settings				
	Close open violations after:	3	days ~	Why is this required?	
	Add custom violation des	scription			
	Runbook URL				
	http://				imes Remove



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

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

Incident Prederenceの設定によって、Issueを起票する(Incidentをまとめる)粒度を設定できる ※アラートポリシーを作成する際に設定(後で編集可)

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



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

lssueの起票粒度について

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

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

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

New Relic アラートの構成要素3: Workflows

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

Select Issues

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

100.6			
lanse			
Enter a name you'll recognize			
elect issues			
Build a query 🚫 Send all is	sues		
Select or enter attribute ()			
+ AND			
nrich (optional)			
nrich (optional)			
+ Build a query			
nrich (optional) + Build a query			
nrich (optional) + Build a query			
hrich (optional) Hulld a query Do not send notifications for <u>fully</u> a	nuted issues		
hrich (optional) H Build a query Do not send notifications for fully n Do not send notifications for fully c Always send notifications	nuted issues r <u>cartially muted</u> issues		
 hrich (optional) + Build a query Do not send notifications for <u>fully</u> of the provided send notifications for <u>fully</u> of Always send notifications 	nuted issues r <u>cartially muted</u> issues		
nrich (optional) + Build a query Do not send notifications for <u>fully</u> of Do not send notifications for <u>fully</u> of Always send notifications	nuted issues r <u>cartially muted</u> issues		
nrich (optional) + Build a query Do not send notifications for <u>fully</u> of Do not send notifications for <u>fully</u> of Always send notifications	nuted issues r <u>partially muted</u> issues	Jira	Slack
nrich (optional) + Build a query Do not send notifications for fully of Do not send notifications for fully of Always send notifications now. ServiceNow incidents	nuted issues r <u>partially muted</u> issues	Jira	Slack.
nrich (optional) Build a query Do not send notifications for <u>fully</u> o Do not send notifications for <u>fully</u> o Always send notifications New ServiceNow incidents Email	nuted issues r <u>partially muted</u> issues	Jira PagerDuty	Slack.

New Relic アラートの構成要素4: Destinations

Issueのライフサイクルに応じた通知を受けることができる

デフォルトで各New Relic ユーザーは利用できる通知先として登録されている Workflowsと関連づけると、以下の形式で通知される

- 登録メールアドレスに対する通知
- New Relicモバイルアプリ経由での通知
- その他、追加で利用可能な通知先一覧は以下のとおり



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



アラートを設定する前にやること

Apdex Tの値を適切に設定する

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

Apdex	score	0.88 [0.37] APP SERVER	0.81 [1.7] BROWSER	***
0.9		4	•	
0.85	\sim			\sim
0.8	Λ		~~\/	\wedge
0.75	/ \/			
	11.10 AM	11:20 AM	11:30 AM	

Application server

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

Apdex T 🔊

0.37

seconds

Please input a decimal or whole number only.

© 2022 New Relic, Inc. All rights reserved



Apdex T値について

それを満たせばユーザーが満足すると想定される、最大応答速度

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



ハンズオン**(1)** アラートを作成する

25min



© 2022 New Relic, Inc. All rights reserved

ハンズオン(1)アラートを作成する

[準備]

New Relicにログインしてください。<u>https://login.newrelic.com/login</u>

- ユーザー: japan-handson+2021@newrelic.com
- パスワード: oSz6nrupas
 (オー、エス、ゼット、ロク、エヌ、アール、ユー、ピー、エー、エス)

※本ハンズオンセミナーでは2つのNew Relicアカウントにログインします。 スムーズに切り替えを行うためにログイン時に[Remember my email]にチェックをつけてください ログイン切り替えは次項参照

※普段NewRelicをお使いの方はセッションが残っている場合がありますのでプライベートブラウジングをお使いください。

- Chrome : シークレットウィンドウ
- Firefox : プライベートウィンドウ
- Edge : InPrivate ウィンドウ
- IE: New Relicの一部機能はIEをサポートしていません。上記のいずれかのブラウザをご利用ください。



ログインするNew Relicアカウントを切り替える

ログイン時に[Remember my email]にチェックをつけておくと、 Log outした際に次にどこのアカウントにログインするか選択する画面が表示されるようになります。 詳細は<u>ブログ</u>を参照

⊋ new relic Log in to vour account	NRU-User Full platform user japan-handson+2021@newrelic.com	⑦ new relic
Multiple accounts found. Verify your email to view all your accounts.	User preferences API keys v	Log in to your account
Email japan-handson+2021@newrelic.com	Manage your plan	You have been signed out.
Password	View settings Theme New Light Dark Auto	japan-handson+2021@newrelic.com Original New Relic account
Remember my email 💿	NRQL console Show Hide Add more data Manage your data	japan-handson+2021@newrelic.com NewRelic.kk Default
Forgot your password? Trouble logging in? Create a free account	Support	Use a different account



今回監視対象のサイト

[NRUジェラートショップ](ECサイト)

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

全ての意品 ・ キーワードを入力 Q

💄 新規会員登録 🎔 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

• Zabbix:

○ インフラ



今回の環境の監視構成

[前提]

今回は赤字のアラートを設定してみます。

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



ハンズオン(1)アラートを作成する

作業内容

- 1. Alert Policyを作成する
- 2. Alert Condition (4つ) を作成する
- 3. Workflowsを作成する






使用アカウント: NewRelic.kk(ログイン先選択は<u>こちら</u>参照)



ハンズオン(1)-1 Alert policyを作成する 1/4

• Alert & Al メニューを開きます。

🔿 Nev	w Relic ONE"	All accounts	~									<u>[ilii</u> Query yo	ur data 🚦 A	pps Quick	start 🧲	83%	୦ ଡ	5	F 🔘
Home	Explorer	Browse data	C	Dashboards	Alerts & Al	АРМ	Browser	Infrastructure	Logs	s Mobile	Synthetics	More 🗸	Ø		🖞 Share	+ Create a workl	oad 🕕	+ Add	more data
Ŧ	entityType =	Service x	A	dd more fil	ters											i List	& Navigato	r 80	Lookout
YOU	IR SYSTEM			<u> </u>	Name 0			Accourt	nt C	End User ()	Page Vi) Respon	C Throug C	Error Ra (i.	Activity str	eam	Ŧ	Filters ~
000	All entities (31	18)		4	EC-site			NewRe	elic	312.818 ms	11 page	's 79.409 m	s …3 req/min	0 ;	s				
\oplus	APM/Services	s (5)		4	New Relie	c Pet Clini	c	New R	elic	488.935 ms	1.74 page	's 17.314 m	s 575 req/min	0 9	4	EC-site	viation closed	5	10:31 am
	Hosts (2)			\$	∎ FoodMe			New R	elic	1083.486 ms	94 page	/s 10.001 m	s 851 req/min	0 5	(HttpDispate deviated fro minutes on	her requests, im the baselii 'EC-site'	_per_mir ne for at	nute least 5
\heartsuit	Containers (3	9		4	≣ test-001			NewRe	elic	- 2		. 0	s O req/min	0 5	s				
۵	Mobile applic	ations (0)		4	≣ ap-001			NewRe	elic			25				 Warning vi 	plation opene	ed	10:29 am
0	Browser appli	ications (3)														HttpDispate deviated fro minutes on	her requests om the baseli 'EC-site'	_per_mir ne for at	nute Teast 5



ハンズオン(1)-1 Alert policyを作成する 2/4

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

● New Relic ONE [™] Account: 2511671 - New	RelicUniversity-Japan 🗸
Explorer Browse data Dashboards Alerts	s & Al Errors Inbox APM Browser Infrastructure Logs Mobile Syn
ANALYZE	😇 👻 Search for any attribute or value.
Overview	Opened violations by priority
Issues & activity	Since 3 days ago
DETECT	10 8
Alert conditions (Policies)	6 4
Anomaly detection	2
CORRELATE	Dec 13, Dec 13, Dec 13, Dec 13, Dec 14, 03:00 AM 09:00 AM 03:00 PM 09:00 PM 03:00 AM



ハンズオン(1)-1 Alert policyを作成する 3/4

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

Explorer Browse data Dashboards	Alerts & Al Errors Inbox APM Browser Infrastructure Logs	Mobile Synthetics More -			Сору р	ermalink 🛩
ANALYZE	(Search policies		+ Ne	w alert policy	Browse pre-bu	ilt alerts
Overview						
Issues & activity	Policy	Conditions ○	Channels 🗘 Open i	ncidents 🗘	Last ©	
DETECT	アラートポリシー	2	2	0	Apr 20, 2:01 am	197
Alert conditions (Policies)	インシデントインテリジェンス	1	0	0	5:52 am	面
Anomaly detection	ダッシュボードハンズオン用アラートポリシー	1	0	0	3:17 pm	Ŵ



ハンズオン(1)-1 Alert policyを作成する 4/4

ISSU

- 自分用とわかりやすい名前を付けてAlertPolicy Create alert policy
 を作成します
- New Relic アラートの構成要素② Incident
 Preference 1/2 を参考に、好みの「INCIDENT PREFERENCE」を選択してください
- 3. [Create policy without notifications]をクリック します
 - a. あえてすべてのコンポーネントを手動で作成したい ため、ここではAlert policyのみを作成します

Q	kalleq:test.policy
E CREATION PREFERENCE	Specify how we create issues and group incidents into them. (You get notifications when an issue opens, is acknowledged, and closes.) ① We streamlined our terminology, See what's changed 27
2	One issue per policy Group all incidents for this policy into one open issue at a time.
	One issue per condition Group incidents from each condition into a separate issue.
	One issue per incident No grouping. Create a separate issue for every incident.

(3)

Cancel

Create policy without notifications

ハンズオン(1)-2 Alert Conditionを作成する 1/18

[前提]

今回は赤字のアラートを設定してみます。

カテゴリ	カテゴリ 現在起こっている		将来のリス	スクの兆候
具体例	サイトが遅い	エラーを返す	キャパシティを 超える	リソースが 枯渇する
外形監視	チェック応答時間	チェックエラー		
フロントエンド	Apdex	JSエラー		
アプリケーション	Apdex 応答時間	4xx, 5xxエラー	スループット バッチ遅延	
インフラ				各種インフラ リソース



ハンズオン(1)-2 Alert Conditionを作成する 2/18

• 新規Alert Conditionの追加

4つのアラートを順番に設定していきます

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



ハンズオン(1)-2 Alert Conditionを作成する 3/18

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

© 2022 New Relic,

O New Relic ONE Account: 2511671 - 1	NewRelicUniversity-Japan 🛩	Litti Query your data 🔠 Apps 🛛 Quick	start.
Home Explorer Browse data Dash	boards Alerts & Al APM Browser Infrastructure	Logs Mobile Synthetics More -	
Overview	参加者名 アラートポリシー	Connect to Incident Intelligence	cident preference: By
ALERTS	id: 1314626		
Incidents			
Events	0 Alert conditions 0 Notification chan	inels () Add a notification channel to receive alerts	
Policies			
Notification channels			
Muting rules		202	
PROACTIVE DETECTION		5.5	
Settings	This	s policy doesn't have any condi	tions
INCIDENT INTELLIGENCE	Ale	ert conditions are the criteria for creating incide	ents.
Decisions	Ν	Jotifications are sent when incidents are create	ed.
Sources		Create a condition	D
Demission			

ハンズオン(1)-2 Alert Conditionを作成する 4/18

- 外形監視:チェックエラー
- 監視設定は次のようにしてください。

1. Categories

a. Synthetics -> Single failure

2. Select a monitor

a. EC-CUBE-Checkout



ハンズオン(1)-2 Alert Conditionを作成する 5/18

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

New condition

74						
NRQL	APM	Browser	Mobile	Plugins	Synthetics	Infrastructure

Next, select entities

Cance

(X)



ハンズオン(1)-2 Alert Conditionを作成する 6/18

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

View:	All (4)	Selected (1)	Unselected (3
	View:	View: All (4)	View: All (4) Selected (1)

ハンズオン(1)-2 Alert Conditionを作成する 7/18

• コンディション名にわかりやすい名前を入力して「Create condition」をクリックします。

(X) Cancel

New condition

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

ハンズオン(1)-2 Alert Conditionを作成する 8/18

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

参加者名 アラ- id: 1314626	ートポリシー	Connect to Incident Intelligence	Incident preference: By policy Delete this policy
1 Alert condition	0 Notification channels	O Add a notification channel to receive alerts	Last modified 7:37 am by NRU-User
Search conditions SYNTHETICS MONITOR FAIL EC-CUBE-Checkout Monitor check failur	.URE わかりやすい通知名	Last modified 8	Add a condition

Add a condition



ハンズオン(1)-2 Alert Conditionを作成する 9/18

• 新規Alert Conditionの追加

②フロントエンド: Apdex(静的)

1. Categories:

a. Browser -> Metric

2. Select entities:

a. EC-site

3. Define thresholds

a. Critical: End User Apdexが5分間に1度でも(at least once)0.7を下回ったら(below)

Condition名は適切なものを各自設定してください



ハンズオン(1)-2 Alert Conditionを作成する 10/18

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

参加者名 アラー	トポリシー	Connect to Incident Intelligence	Incident preference: By policy	Delete this policy
id: 1314626				
1 Alert condition	0 Notification channels	(i) Add a notification channel to receive alerts	Last m	odified 7:37 am by NRU-User
Search conditions				① Add a condition
SYNTHETICS MONITOR FAILUF	№ わかりやすい通知名	Last modified 8	:05 am by NRU-User 🖉 Edit 🗍 Cop	y 🗓 Delete 🛛 🗖 📄
EC-CUBE-Checkout				
🛞 Monitor check failure				
				Add a condition



ハンズオン(1)-2 Alert Conditionを作成する 11/18

• Categories を設定します。

New condition

			¥			
L	APM	Browser	Mobile	Plugins	Synthetics	Infrastructure
	7 1147					
type	of conditi	on				

⊗ Cancel

Next, select entities



© 2022 New Relic, Inc. All rights reserved

ハンズオン(1)-2 Alert Conditionを作成する 12/18

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

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



ハンズオン(1)-2 Alert Conditionを作成する 13/18

Thresholds を設定しわかりやすい名前を設定します。

3. Define thresholds	EC-site \sim
When target browser application	
End User Apdex \sim has an apdex score below \sim	
0.7 at least once in V 5 minutes	0.8
	0.6
Add a warning threshold	0.4
Condition name	0.2
名前を追記 End User Apdex (Low)	
Add runbook URL	Apdex Critical threshold Critical violation
	K Back to Select entities Create condition



ハンズオン(1)-2 Alert Conditionを作成する 14/18

• 2つめのconditionが作成されました。

2 Alert conditions	0 Notification channels ① Add a notification chan	nel to receive alerts Last modified 7:37 a	m by NRU-User
Search conditions		⊕ Ado	l a condition
APM BROWSER APPLICATIO	M METRIC 名前を追記 End User Apdex (Low)	Last modified 8:28 am by NRU-User 🖉 Edit 🗇 Copy 📋 Dele	ete On
EC-site 🕀 Add entities			
End User Apdex < 0 \bigcirc \bigcirc Add a warning the	.7 at least once in 5 mins reshold		
SYNTHETICS MONITOR FAIL	URE わかりやすい通知名	Last modified 8:05 am by NRU-User 🖉 Edit 🔯 Copy 🏐 Dele	ete On
EC-CUBE-Checkout			
🛞 Monitor check failur	e		



ハンズオン(1)-2 Alert Conditionを作成する 15/18

- 新規Alert Conditionの追加
 ③アプリケーション:応答時間(動的)
- 1. Categories
 - a. APM -> Application metric baseline
- 2. Select entities
 - a. EC-site
- 3. Define thresholds
 - a. 次ページ参照

Condition名は適切なものを各自設定してください



ハンズオン(1)-2 Alert Conditionを作成する 16/18

• ベースラインアラートではスライドバーで感度が変化します。



Add runbook URL



Web transaction time
 Average web transaction time

To see values not visible in larger time windows, click and drag to zoom the chart

ハンズオン(1)-2 Alert Conditionを作成する 17/18

• 新規Alert Conditionの追加

④アプリケーション: 4xx,5xxエラー(ホストごとに評価)

1. Categories

a. NRQL

2. Enter a NRQL query and thresholds

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

1. Define thresholds

a. Critical: Staticで適宜好きな値(%)を設定してください

Condition名は適切なものを各自設定してください



ハンズオン(1)-2 Alert Conditionを作成する 18/18

- NRQLを入力すると自動的に参考となるChartが表示されます。
 - Define your signal

What's possible with NRQL	Alerting 🐱									
ignal loss violations and filler	d data gaps are cur	rently not refl	ected in the	chart. See ou	ir docs 🗗					
ihowing 1/1 time series ⑦										
.9										
4		1				- T	- i			
9										
4										
								1		
9					-					
4		1					- 1		. = =	w = - =
	^		_	~						

🕥 new relic. 59

ハンズオン(1)-3 Workflowsを作成する 1/2

- 1. Alerts & AIメニューのWorkflowsをクリックし
 - 、[+ Add a workflow]をクリックします
- 2. ご自身のworkflowsであることがわかる名前を 入力します
- 3. Select Issuesで以下を選択します
 - 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
- 4. Mute issues: デフォルトのまま
- 5. Notify: Emailを選択
 - a. ご自身のメールアドレスを入力してaddし、 [Update message]をクリック
- 6. [Activate workflow]をクリック

onlighte your worknow	Name		
ise this flexible system to filter, enrich and send your alert ata to the right destinations. ee our docs	kaizawa-test-workflows		
ilter your data	Select issues		
elect the kinds of issues you want to send.			
	 Build a query Send all 	issues	
	3 policyhame exactly matches	mu-test-policy *	
	+ AND		
	We don't see any issues matchin	a your filter. This doesn't mean it wo	n't work.
nrich your data	Enrich (optional)		
uild up to 5 NRQL queries to add more context to your sues.	1 Bullion surgery		
	~		
fute issues	(4)		
ou have rules in place that mute issues. Choose what to sute or ignore muting.	Do not send notifications for <u>full</u>	(muted issues	
ee our docs [5]	Always send notifications	Contraction of the second	
lotify	(5) _		
hoose one or more destinations and add an optional	2, Kalzawa@newrelic.c	Jam.	0 X
tessage.			
vessage.	FICTINE ServiceNow incidents	& Webhook	eit.
essage.	now ServiceNow incidents	Webhook	Jra AWS EventBridge
essage.	Now ServiceNow Incidents	🛞 Webhook	Jra
essage.	Now ServiceNow Incidents	🛞 Wethook	Jra
essage. est this workflow	Prove ServiceNow Incidents	Webhook	Jra

ハンズオン(1)-3 Workflowsを作成する 2/2

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

いたったんマレファレナホシレナナ

Destinations

Alerts & AlメニューのDestinationsをクリックし、External addressとしてご自身のメールアドレス

אריד אריד new relic		Q Search across New Relic	± 0			Query you	ur data 🔟 🛔 Add data	🗄 Apps ⊘ Get started	1 0 6 5 100 0
Explorer Browse data Dashboards	Alerts & Al Errors inbox	APM Browser Infrastructure L	ogs Mobile Synthetics I	More 🗸 🦉					🖞 Share
ANALYZE	Add a destination Add destinations where w	re send notifications.							
Issues & activity	Jira	NOW ServiceNow	Stack	🔊 Webhook	pd PagerDuty	AWS Eve	ntBridge		
DETECT Alert conditions (Policies) Anomaly detection	Destinations (3) No Manage destinations whe	tifications Log rre we send notifications, including cred	entials.						
CORRELATE	〒 ← Search b Type : Name	y destination name	Two-way URL/Channel		Last updated	Updated by C	Enabled 😳	Status 🗘	
Decisions	NRU-User		japan-handson+ kaizawa@newre	2021@newrelic.com	Jun 6, 2022 7:46pm Jun 6, 2022 8:08pm	1001038720		DEFAULT	
ENRICH & NOTIFY Muting rules	Externa	al address	kaojiri@gmail.co	m	Jun 6, 2022 7:49pm	1001038720	120	DEFAULT	
Workflows New									

座学**(3)** AlOpsの意義



© 2022 New Relic, Inc. All rights reserved

ITサービスに発生しうる障害と監視の関連性

ITサービスに 理解できる 理解できない 発生しうる障害 8 \mathbf{C} \mathbf{C} Actionableな監視 とりあえずの監視 気づいたあとに正しく対処が 気づいても対処につなげられない (例.インフラのリソース使用率上昇) できる 気づける (例.ユーザーが特定の機能を使えない) ŝ Actionableな監視予備群 監視できていない未知の領域 障害発生して後手対応になったが 障害発生したが原因がわからず監 、原因がわかったので次回から監 視もできない 気づけない 視で気づける









ガートナーによる定義

https://www.gartner.com/en/information-technology/glossary/aiops-artificial-intelligence-operations

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

- 1. 異常検知
- 2. イベントの相関分析
- 3. 根本原因分析





AlOps が必要とされる 背景

1. モノリスからマイクロサービスへ

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



new relic. 66

AlOps が必要とされる 背景

2. 捕捉できるデータの増加と多様化

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



new relic. 67

© 2022 New Relic, Inc. All

監視にまつわる新たな課題

アラートを1つ1つ網羅的に 設定するのか問題



大量のアラートをどう解釈して トラシューするのか問題





new relic. 69



new relic. 70

AlOpsによってサービスの信頼性を高める

アラートを1つ1つ網羅的に 設定するのか問題

[解決するAlOpsの機能]

• 異常検知



手動でアラート設定せずとも自動で検知

大量のアラートをどう解釈して トラシューするのか問題

[解決するAlOpsの機能]

- ・ イベントの相関分析
- 根本原因分析



複数の事象を自動で関連付け、根本原因を推察





ハンズオン(2) AlOpsを使った異常検知 と原因分析(前編)

15min


今回の環境の監視構成(再掲)

• New Relic:

○ 外形監視, フロントエンド(ブラウザ), アプリケーション、インフラ

• Zabbix:

○ インフラ



ハンズオン(2)

1. 異常を自動検知する

[目的]

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

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

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



AIOps: 異常検知

ハンズオン(2)



2.1 様々なソースのアラートをまとめる: 通常のアラート

[目的]

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

- Alerts&Al -> Sourcesを選択
- Alertsカードを選択
- [+ Add a policy]をクリックして自分が作成したAlert Policyを追加する





ハンズオン(2)



2.2 様々なソースのアラートをまとめる: 異常検知情報の接続

[目的]

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

- Alerts & Al -> Anomaly Detectionを選択
- Add a configurationを押す
- 設定名は自分の名前、アカウントはNRU(2511671)、アプリはEC-site、No notification、 Correlate with other alerts をオンにして[Save configuration]





ハンズオン(2)



2.3 様々なソースのアラートをまとめる: Zabbixからのアラート

[目的]

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

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







使用アカウント: NewRelic.kk(ログイン先選択は<u>こちら</u>参照)



ハンズオン(2)異常を自動検知する

• 「Issues & activity」 をクリックします。

New Relic ONE" Acco	ount: 2511671 - NewRelicUniversity-Japan 🛩	🕞 Query your data 🕼 Instant Observability 🔡 Apps	⊘ Get started Q ⑦ 🖗 🛱 🚺 🤇
xplorer Browse data	Dashboards Alerts & Al Errors Inbox APM Browser Infrastrue	cture Logs Mobile Synthetics More -	togy permalink →
ANALYZE Overview	アラートポリシー ^{id: 545592}	Connect to Incident Intelligence 🔅 Incident prefere	ence: By condition Delete this policy
Issues & activity	2 Alert conditions 2 Notification	n channels	Last modified Feb 7, '20 7:13 am by Akihiro Ito
Alert conditions (Policies	Search conditions		① Add a condition
Anomaly detection	APM APPLICATION METRIC BASELINE Web	transaction throughput (Baseline)	🖉 Edit 🖄 Copy 💼 Delete 🛛 🗖 🔲
CORRELATE	EC-site ③ Add entities		
Sources Decisions	Web transaction throughput deviates	from baseline for at least 5 mins from baseline for at least 5 mins	
ENRICH & NOTIFY Muting rules	INFRASTRUCTURE METRIC Disk Used		Last modified Feb 5, '20 7:53 am Manage
Pathways	All Entities		
Destinations	⊗ diskUsedPercent > 90 for at least 2 mi ∧ diskl lsedPercent > 70 for at least 2 mi	ins	

ハンズオン(2)異常を自動検知する

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

	New Relic ONE* Account: 2511671 - New	wRelicUniversity-Jap	an 🐖		E	Query your da	ta 년날 Instan	nt Observability	BB Apps 🥝	Get started Q	 © © E E I 	0
	Explorer Browse data Dashboards	ts & Al Errors Inb	ox APM Browse	r Infrastructure	Logs Mobile Synthetic	s More 🗸	1		D Copy perm	nalink 👻 🤇 🔇	③ Since 3 days ago	~
	ANALYZE	Issues Inciden	Anomalies									
	Overview	₹ • Q	Searth or flick the dri	policies for justicies								
	Issues & activity											
	DETECT	8 6 4	- 0. X			10-01 		70 D.B.				ĩ
	Alert conditions (Policies)	2										
	Anomaly detection	Dec 12, 09:00 PM	Dec 13. Dec 13. 03:00 AM 09:00 AM	Dec 13, 03.00 PM	Dec 13, Dec 14, 09:00-PM 03:00 AM	Dec 14, 09:00 AM	Dec 14, 03:00 PM	Dec 14, 09:00 PM	Dec 15. D 03:00 AM 09	ec 15, Dec 15, 00 AM 03:00 PM	Dec 15, 0 09:00 PM 0	24c 3.0i
	CORRELATE	Netwock traff	fic 🔹 Cpu usage									
	Sources	STATE	NAME	ENTITY TYPE	SIGNAL				START	DURATION	CONFIGURATION	ŧ
	Decisions	Open	ip-172-31-26	Host	Cpu usage			11	27m ago	10	Host	
	ONRIGH & NOTIEX	Open	ip-172-31-26	Host	Cpu usage			Ar	27m ago	*	Host	
	Muting rules	Closed	ip-172-31-26	Host	Network traffic				27m ago	12m	Host	
© 2022 New Relic, Inc	Destinations	Closed	ip-172-31-26	Host	Cpu usage			1	27m ago	12m	Host	

1 new relic. ⁸⁰

ハンズオン(2)異常を自動検知する

• 自動的に検知された値のいずれかをクリックします。





ハンズオン(2)異常を自動検知する

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



• 「Sources」をクリックします。

New Relic ONE"	Account: 2511671 - Ne	wRelicUniversity-Japan	*	
xplorer Browse d	ata Dashboards Ale	rts & Al Errors Inbox	APM Browse	er infrastructure L
ANALYZE		Issues Incidents	Anomalies	
Overview			earch or click the dr	opdown for options
Issues & activity				
DETECT Alert conditions (Po	licies)	8 6 4 2		
Anomaly detection		c 08, Dec 09, Ю РМ 09:00 AM	Dec 09, De 09:00 PM 09:0	c 10, Dec 10, 10 AM 09:00 PM
CORRELATE		Network traffic	• Cpu usage	
Sources		STATE	NAME	ENTITY TYPE
Decisions		Closed	ip-172-31-26	Host
ENRICH & NOTIFY		Closed	ip-172-31-26	Host
Muting rules				
Pathways		Closed	ip-172-31-26	Host
Destinations		Closed	ip-172-31-26	Host



© 2022 New Relic, Inc. All rights reserved

• 「Alerts」カードをクリックします。

xplorer Browse data Dashbo	ards Alerts & Al Errors inbox APM Browser Infra	structure Logs Mobile Synthetics More - 🏼 🦉
ANALYZE		
Overview		
Issues & activity	2 active sources	
DETECT	🕥 1 policy connected 🛛 🕥 1 configura	tion connected
Alert conditions (Policies)		
Anomaly detection	Available sources	
CORRELATE		
Sources	Alerts	REST API
Decisions	1 active policy	Use REST endpoint to easily ingest
ENRICH & NOTIFY	Ingest your existing alert policies for correlations to gain actionable insights and cross-source visibility of your stack.	other tool, including homegrown solutions.
Muting rules		
Workflows New		

New relic. 84

ハンズオン(2)様々なソースのアラートをまとめる(1)

• 「+ Add a policy」ボタンをクリックします。

Associated account: NewRelicUniversity-Japan (?)

New Relic Alerts source		
When connected policies generate activity, we'll automatically correlate it to filter out noise, add context, and identify issues. You'll get fewer notifications and have more information, so you can solve problems faster.	NEW RELIC IS CONNECTED	
OLICIES (1)		+ Add a policy
POLICY 0	ACCOUNT 0	
インシテントインテリシェンス 🗗	NewRelicUniversity-Japan	



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

crount	Δπ	O Saureb policier					
ccount.		C Sell of policies		View:	All (4)	Selected (2)	Unselected (
	POLICY ©		ACCOUNT NAME				
	インシテントインテリシェンス 🛃		NewRelicUniversity-Japan				
0	アラートポリシー ピ		NewRelicUniversity-Japan				
	ダッシュボードハンズオン用アラートポリシー ピ		NewRelicUniversity-Japan				
	参加著名アラートポリシーピー		NewRelicUniversity-Japan				



new relic. 86

• 自分のPolicyが追加された事を確認します。



New Relic Alerts source

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



• 「Anomaly detection」をクリックします。

V New Relic (DNE							
Explorer B	frowse data	Dashboards	Alerts & Al	Errors	Inbox	APM	Browser	Ir
ANALYZE			()	We'll ar	nalyze up entative fo	to 1,000 or more :	events per	mi n o
Overview								
Issues & ac	tivity							
DETECT				-		22 22 1		
Alert condi	tions (Policie	s)		0	New	Relic	Alerts s	οι
Anomaly de	etection			When co	nnected	policie	s generat	te a ide
CORRELATE				and have	e more ir	nforma	tion, so ye	DU
Sources								





• 「+ Add a Configuration」ボタンをクリックします。

Anomaly detection settings

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

Visibility

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

Anomaly visibility preferences

Notifications

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

+ Add a configuration

Q. Search configurations

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

lake this configuration	on easy to identify
Make this configurate	in cusy to ruentiny
分の名前	
What account do you	want to use?
count: 2511671 - NewRelicUn	iversity-Japan ~
What applications and	services do you want to include? (Select up to 1.000)
What applications and	I services do you want to include? (Select up to 1,000)
What applications and	Services do you want to include? (Select up to 1,000)
What applications and Service - APM	Search in this table All (2) Select (1/2) Unselected (1)
What applications and Service - APM APM Entities: 2	Search in this table All (2) Selected (1/2) Unselected (1)
What applications and Service - APM APM Entities: 2	Search in this table All (2) Selected (1/2) Unselected (1)
What applications and Service - APM APM Intíties: 2	Services do you want to include? (Select up to 1,000)
What applications and Service - APM APM Intíties: 2	Services do you want to include? (Select up to 1,000) Q Search in this table All (2) Selected (1/2) Name Image: Comparison of the second



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

 What signals 	should we monitor for	anomalies?			
Web throughput	Non-web thr	oughput 🕑 Error rate	Web resp	onse time 🛛	Non-web response time 🛛 🛃
 Where do you 	u want to receive notifie	cations?			
We'll write anomalies	we detect to NRDB, which mea	ns you can query them and view then	n in the anomalies tab.		
Slack	Webhook	No notifications 🤣			
 Do you want 	to correlate anomalies	from this configuration? ⑦			
Correlate with other a	alerts 💽				
Cancel	ave configuration				

設定が追加されたことを確認します。

Anomaly detection settings

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

Visibility

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

Anomaly visibility preferences

Notifications

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

Q. Search configurations

Configuration name 🔅	Applications 🔅	Account 🗘	Last updated 🗘	Destination 0	
自分名前	1	NewRelicUniversity-Japan	Apr 26, 2021 7:11pm		
sasaki-test	1	NewRelicUniversity-Japan	Apr 22, 2021 7:16pm		
nc. All rights reserved					🕥 new relig

+ Add a configuration

© 2022 New Relic, Inc. All rights reserved

参考 Zabbixの連携

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

xplorer Bro	owse data	Dashboards	Alerts & Al	Errors inbox	APM	Browser	Infrastructure	Logs	Mobile	Synthetics	More 🤟		0
ANALYZE													
Overview													
lssues & acti	vity		2	active so	ources								
DETECT			จ	1 policy conn	ected	1 cor	nfiguration con	nected					
Alert condition	ons (Policie	5)											
Anomaly det	ection		Availab	le sources									
CORRELATE								-					
Sources			r	Alerts					REST	API			
Decisions			1 act	ive policy	lert polic	ies for	U	se REST onitoring	endpoint t data for d	o easily inges correlations fr	it om any		
ENRICH & NO	DTIFY		correla cross-	ations to gain a source visibility	ctionable y of your	insights ar stack.	nd o	ther tool,	including	homegrown s	olutions.		
Auting rules													
Workflows	New											_	J

New relic. 93

参考 Zabbixの連携

• API URLとInsights Insert keyを作成し、それをコピーしてZabbix側に登録します。



Next to the Insert keys heading, select the + sign to create a new key.

For custom event formatting and payload examples, see our docs

About our REST API integration

We support a dedicated REST API interface so you can easily integrate with additional systems, including your own solutions, by using our REST API. This allows instrumentation of your code or other monitoring solutions to report any kind of event or metric.

🕥 new relic. 94

参考 Zabbixの連携

ZABB

○ 監視
 □ イン/
 □ レボ・
 へ 設定
 □ 営 管理

加速

メディ スグリ キュ-の サポ・ 王 Shar

🚢 🗅

© 2022 New Relic

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

X	40 M		alen_subject	(ALERI, SUBJECT)	相除
			event_id	(EVENTID)	刑
	Q		event nseverity	(EVENT.NSEVERITY)	用
=_A					除
			event_recovery_status	(EVENT.RECOVERY.STATUS)	刑除
거			event_recovery_value	(EVENT.RECOVERY.VALUE)	H
۴				[[*************************************	験
			event_source	(EVENT.SOURCE)	削時
	*		event_tags	(EVENT.TAGS)	削除
be.			event_time	(EVENT.TIME)	削除
			event_update_status	(EVENT.UPDATE.STATUS)	刑踪
ーグルーフ	e -		event_value	(EVENT.VALUE)	削除
ー		ר	host_name	(HOST.HOST)	刑餘
ħ			new_relic_bearer	Bearer eyJ0eXAiOiJKV1QiLCJhbGck	削除
	_		new_relic_proxy_url		削除
b: i			new_relic_url	https://collectors.signifal.io/v1/inciden	削除
			urgency_for_average	2	削除
一段定			urgency_for_disaster	1	朝餘
POF			urgency_for_high	2	前

) new relic. 95

参考 Zabbixの連携

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

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

D new relic. 96

座学(4) New RelicのAlOps機能



© 2022 New Relic, Inc. All rights reserved

New Relic AlOpsによるインシデント対応フロー





検知1:重要な指標に対する手動アラートによる気づき







検知2: Proactive Detectionによる異常の通知







検知3: Lookoutによる異常の可視化と探索







診断1: Correlationによるアラート統合とノイズの削減



14100								
-		-	-					-
ANCHENTS IN 1910	and the set						. Conut . rept	. Martine
						-		
		-						
						-		
						and the second second		
10.11.000	10.21 AM 10.21 AM 1	1.10.414		10.00 449	10.00 100	40 - 10 Mil 140		
+ Duerman	1122.000 1122.000 1			10.00 AM	1949 ANT 1944			
ted activity 2	1920.000			12.03 AW	1000 AM 1000			
turnation of the second	1923 ANI 1927 ANI 1		TOURCE	STATY STATY	ABLACKD EVENTS	PARLOAD	ANAL YZE	MEW RELIC ORD
ted activity 2	1922 ANN 1922 ANN 1922 2 THMA Wellow the finance justice of participants from the stars and the stars of the stars of	12	HOURCE IN	ERAN Deved	ABARD (1997)	PARLOAD (7)	ANALYTE	NEW RELIC ORI
transmitte total activity 2 turesates 2,1041am 2,1044am	1922 MM 1922 MM 1 MMA Methodal in fixing latency problems freming data from the Service price sole	12	increase in the second	STATY Doed Doed	ABLATED COUNTS	PARLOAD (7) (7) (7)	ANALYZE	NEW RELIC ORI
total activity 2 total activity 2 total activity 2 total activity 2	2 White Westerney problems freeholg data from the Sanote Disc case Westerney a 300 instituted with a street it instances on Westfarded (g. 17).	12	HOURCE H	STATY Chosed Chosed Chosed	ABLAND (1997) 3 3 3	PARIOAD (7) (7) (7)	Ania, X28 C. Acatus	NEW RELIC ORM
tech activity 2	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	12 ⁶ 12 ⁶	1048CI 60 00	STATY Dovid Dovid Dovid		PARIONE (7) (7) (7) (7) (7) (7)	ANALVEE	NEW RELIC OR
Internet 2	The second	12 ¹ 12 ¹ 12 ¹	100.8KG 0 0 0	STATE AND STATES Devel Devel Devel Closed Closed	ALLENS MUNITI 	PARIONE (7) (7) (7) (7) (7) (7) (7) (7) (7)	AMALYEE Q. Andyse Q. Andyse	NOW RELIC ONLY
Internet 2	2 2 2 Constants Model	22 22 23 21 21	Nounce M O O O O O O O	Staty Doed Doed Doed Doed Doed Doed	ARANG KONG 3 3 3 3 3 3 3 3 3 3	PARLOAD (7) (7) (7) (7) (7) (7) (7) (7)	AMALYEE C. Andyse C. Andyse	NUM RELICION
Internet	The second	ಜೆ ಬೆ ಬೆ ಬೆ ಬೆ	Housed M O O O O O O O	SPANY Chosel Oreed Chosel Chosel Chosel Chosel Chosel Chosel Chosel	ARANG OUNT 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	PARLOAD 02 02 02 02 02 02 02 02 02 02 02 02	Anderstee Q. Anderse Q. Anderse	нем жило око ос ос
IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	The second seco	20 20 20 20 20 20 20 20 20 20 20 20 20 2	HOUNCE M O O O O O O O O O O O	STATE Dised Dised Dised Dised Dised Dised Dised	2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	******** 67 67 67 67 67 67 67 67 67 67 67 67 67	. Anida veza Q., Anida veza Q., Anida vez	
utilization ed activity 2 upsatze 2 z, 10:41am 2 z, 10:40am 2	BOLK BOLK CONTRACT STATES AND ADDRESS A	22 23 23 23 24 24 24 24 24 24 24 24 24 24 24 24 24	100/000 101 00 00 00 00 00 00 00	EXXY EXXY Devel Oreed Closed C	2	PARTONE 02 02 03 03 03 03 03 03 03 03 03 03 03 03 03	AMARYSE Q., Analyse Q., Analyse	



診断2: Correlationによる根本原因の示唆



and the second se		③ 24m Mar 15, 11:
b response time > 700 milliseconds for at least 10 minu	tes on 'Plan Service'	
ssue summary		<i>0</i> 1
Analysis summary	Sugg	gested responders :
Golden signals: Latency 😳 📩 😒 Related components: Application	n©☆ 2∧	Alam Turing 😳 📩
mpacted entities (1) 💮 1 Application		
0. materia		
g hasano		* refolgening states of scenaria densities (D) much operation
toot cause analysis		
oot cause analysis eployment events (3)	Error logs (3)	Attributes to investigate (3)
eployment events (3) Deployments (3) C. Let 12h	Error logs (3) error logs Swee Mar 15, 11: Hans (red) Mar 15, 11: 41am	Attributes to investigate (3) Plan Service Divisions duration (millionist by Balastere room and Table ori Oberati
eployment events (3) Deployments ③ Lest 12h • Deployment Im after route croated	Error logs (b) error logs Score Mar 15, 11 Mars Unit Mar 15, 114(Jans 1	Attributes to investigate (3) Plan Service Distance durations (mg) factorial by Batastere type and Table and Operation 40 k
eployment events (3) Deployments (3) • Deployment In after some created Application: Plan Service	Error logs (3) error logs Score Mar 15, 11 Mars Unit Mar 15, 11 (Jans 1 53	Attributes to investigate (3) Plan Service Distance duration (mg) facewid by Galaxtere type and Table and Operation 40 k 50 k 50 k
eployment events (3) Deproyments (3) • Deployment (1) • Deployment (1) • Deployment (1) • Application: Ran Service Deployment (2) Deployment (2) • Deployment (2) • De	Error logs (3) error logs Some Mar TS, 11:Same Lines Mar TS, 11:4(Sam, 1) 58 58 58 56	Attributes to investigate (3) Plan Service Distance duration (mp) agressit by Balaxtore type and Table and Operation 40 k 10 k
epigyment events (3) oppigyments ① Last 12h • Deployment: Im after rouw created Apploator: Plan Service Deployment: Residence Periode approximation of Residence Heating bad query	Error logs (3) error logs Since Mar 15, 11 Iden (self Mar 15, 11 id)en. 1 0 3 5 5 5 5 7	Attributes to investigate (3) Plan Service Distances durative (mp3 agressist by Betastare type and Table and Operative 40 k
eployment events (3) opployments (3) opployments (3) opployment: In after source routed Application Plan Service Deployment guived(biolo.andemo.stem Revision : Heating baid guivery settible CALINE: Out to presenting to insure creation	Error logs (3) error logs Since Mar 13, 11: Iden Und Mar 15, 11: Glass 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	Attributes to investigate (3) Plan Service Distance duration (mp) foreind by Detasterer type and Table and Operation
eployment events (3) Deployments (3) Deployments (3) Application: Ran Service Deployment (3) Deployment (3) Dep	Error logs (3) error logs Since Mar 13, 11:15km Und(Mar 15, 11:45km 1 1 1 1 1 1 1 1 1 1 1 1 1	Attributes to investigate (3) Plan Service Distance durations (mm) Factorial by Batassere type and Table and Operation 40 k 40 k
loot cause analysis beployment events (3) Deployments	Error logs (3) Error logs Sona Mar 15, 111 Mare Undi Mar 15, 111 Alaen 1 1 1 1 1 1 1 1 1 1 1 1 1	Attributes to investigate (3) Plan Service Understand Automotive (mpl Factorist by Datastere type and Table and Operation 40% 10% 10% 10% 10% 10% 10% 10% 1
loot cause analysis beployment events (3) Deployments	Error logs (3) error logs Sons due (3, 11:18en Urd) Mar 15, 11:43en 1 1 1 1 1 1 1 1 1 1 1 1 1	Attributes to investigate (3) Plan Service Definitions durations (mp) foreind by Balaxiese type and Table and Operation 40 k 10







ハンズオン(3) AlOpsを使った異常検知 と原因分析(後編)

15min

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



今回の環境の監視構成(再掲)

• New Relic:

○ 外形監視, フロントエンド(ブラウザ), アプリケーション、インフラ

• Zabbix:

○ インフラ



ハンズオン(3)

1. 異常を可視化する

[目的]

AIOpsの異常検知の仕組みを使い、異常を可視化する機能を学びましょう

- Topメニューの"More"から"Lookout"を選択
 - 何が表示されているか確認しましょう
 - 目的に応じたカスタムのビューを作ってみましょう

注: Lookoutを見るときだけ、New Relic Original Accountにログインしてください (詳細は<u>こちら</u>)





ハンズオン(3)

2. 個々のアラートを確認する

[目的]

AIOpsに送られたアラートを把握します(後続の演習の事前確認)

- Alerts&Al -> Overview -> Incidentsで、Open中のアラートを確認する
 - それぞれ、Originがなにかを確認しましょう
 - メッセージから、どのようなアラートかを推測してみましょう




ハンズオン(3)

AIOps:イベントの相関分析

AIOps:根本原因分析

3. 複数のアラートを紐付け、トラブルシューティングに役立てる

[目的]

2で確認した個々のアラートがどのように紐付けられ、分析されているかを確認しましょう

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







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



ハンズオン(3)異常を可視化する

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

New Relic ONE** All accounts -	<u>later</u>	Query your data 🔡 Apps 🛛 Quick	start 🛑 👘 😸 – 83% O, 🕐 👰 🖓 –	
Home Explorer Browse data Dashiboards Allerts & Al APM Browser Infra	istructure Logs Mobile Synthetics	skout - 🥖	₫ Share	
Application golden signals by appName for 3 accounts 🖉 🛠 Comparing the lass 5 minutes to the preceding 60 minutes. Learn more 🛃 Last updated 4:49 am 💮 🛩	1. 55 A4 He Ke	WS Lambda Setup ealth Maps by Transactions ubernetes Cluster Explorer	Charge view Analyzing 3 appNames	
Oecreased . No comparison data available	Size shows relative amount	ookout	Q Deviating services	
Throughput Response t	lime Se Se Tr W	ew Relic Edge ervice Maps aces torkload views	We found no significant deviation in appNames from the prior time window.	
FoodMe New Helsc # EC-site	NevR	EC-site	丸の単位はアプリケー 丸の大きさは値の大き 丸の色は異常が発生 表現しています	ーション単位です きさを、 しているかどうかを



ハンズオン(3)異常を可視化する

© 2022 New Re

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

New Relic ONE* All account	3 *	🖮 Query your data 留 Apps Quick start 🛑 📾 📾 83% 🔍 ③ 😨 😴 🙆 ~
Home Explorer Browse data	a Dashboards Alerts & Al APM Browser Infrastructure Logs Mobi	le Synthetics Lookout → ✓ 見終わった。ちな一日ので見じます
Application golden Comparing the last 5 minutes Last updated 5:00 am	EC-site appName v Explore app 🗠	Performance Abnormal history Correlations Profile Traces
	Response time	Other performance indicators for EC-site各タブをクリックしてどのような
Decreased	Comparing the last 5 minutes to the preceding 60 minutes	Tentransartions 情報が見えるか見てみましょう
Throug	180% higher than the preceding 60 minutes Decreased Increased	2k
	Last 5 minutes average 227.192	11k
	Preceding 60 minutes minute average 81.026	500
	Preceding 60 minutes minute standard dev 14.834	0
	Apr 27, 3:59 - 4:59am compared to 1 hour earlier	WebTransaction/Action/Islock_search_product WebTransaction/Action/Shopping_Checkout WebTransaction/Action/Action/Product_add_tart WebTransaction/Action/Action/Action/Action/Action/Islock_cart Critical Violation
New Balls Pe	1.5.k 1.k 500 0	Top errors View errors 🖸 … by error class
	01:00 PM 01:10 PM 01:20 PM 01:30 PM 01:40 PM 01:50 PM 0;	3
	Avg Newrelic goldenmetrics.apm.application.response Time Ms	0.8
	Previous Avg Newrelic goldenmetrics apm application, response Time Ms.	9.6
i	Last 5 minutes compared to	

ハンズオン(3)異常を可視化する

• カスタムのビューを作成します

Manage Views -> Create a new queryを選択



ハンズオン(3)異常を可視化する

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

rowse data Dashboards Alerts & Al Errors inbox APM Browser	Infrastructure Logs Mobile Synth	teokout			
er weltenen einer die het en einer Kennen fen Die seren vereinen.			Create a new query		
in golden signals by applyame for 3 accounts			Select account		
unt View data from	Compare data to	Auto Refresh (All accessible accounts v		
ble accounts v Last 5 minutes v	Preceding 60 minutes	Last updated 3	Select data type 1 Eve	ntsを選択	
eased 🌒 🌒 🌒 🌒 🌒 Increased 🛛 🖶 Size shows relative amount		图] Add to	Metrics Events	S Or write a N	^{RQL query} ②Select your event -> Build a custom queryກ່າວ
Throughput	Res	ponse time	View a chart with Transaction : coun	t >	Transaction->countを選択
			Transaction : average + Add row	: duration	× 〒 6 ③Add rowL、 同じ要領でTransaction
			Facet by		->average->durationを選択
EC-site FoodMe			request.uri		④ reguest.uriを選択
		EC-site	View data from	Compare data to	
New Relic Pet C			Name your view (optional) csasaki (5)ご自身(の名前を入力	
			6 Create New View	wを押す 「 coo	te New View

ハンズオン(3)個々のアラートを確認する

- NewRelic.kkアカウントにログインし直します
- Alerts&Al、[Overview]をクリックします





ハンズオン(3)個々のアラートを確認する

• 「Incidents」タブをクリックします。

New Relic ONE™						D Que	ry your data 🔃	" Instant Obs	ervability 00	Apps ⊘ G	iet started O	0 👳	F) 10+ (
Explorer Browse data Dashboards	Alerts & Al Errors	Inbox APM	Browser Int	frastructure L	ogs Mobile	2 Synthetics M	More - 🦉		G	7 Copy permali	nk v k	Since 3	days ago 🐱
ANALYZE	We'll a represent	nalyze up to 1,00 entative for more	00 events per mo e subscription op	onth as part of y	our subscript	ion. We charge fo	or every event bey	ond that. Con	tact your New R	elic	Dismis	View u	sage data
Overview	-		14 3										
Issues & activity	Issue Inc	dents Anoma	lies							Associat	ed account: Ne	wRelicUniversi	ity-Japan ⑦
DETECT	₹ ×	Q. Search or c	lick the dropdow	n for options									
Alert conditions (Policies)													
Anomaly detection	6 4												
CORRELATE	2 0		1.								. En		·
Sources	Dec 13, 03:00 AM	Dec 13, 09:00 AM	Dec 13, 03:00 PM	Dec 13, 09:00 PM	Dec 14, 03:00 AM	Dec 14, 09:00 AM	Dec 14, 03:00 PM	Dec 14, 09:00 PM	Dec 15, 03:00 AM	Dec 15, 09:00 AM	Dec 15, 03:00 PM	Dec 15, 09:00 PM	Dec 16, 03:00 AM
Decisions	@Low 🔸 N	Aedium 🔸 High	Critical										
ENDER & NAMES		STATE	PRIORITY	INCIDE	NT NAME	CREATED	DURATION	ENTITIES	ANA	LYSIS SUMMARY	SOURCE	EV	ENTS
Muting rules		Closed	Critical	Monit for loc	or failed ation	12m ago	5m		Sign	al: Error	0	2	6
Pathways		Open	Critical	Web r	esponse	16m ago	16m		Sign	al: Latency	0	1	6
			<u> </u>	time o	eviated				Con	ponents:			1771

С.

ハンズオン(3)個々のアラートを確認する

• 個々のIncidentをクリックします。



ハンズオン(3)個々のアラートを確認する

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





ハンズオン(3)複数のアラートを紐付け トラブルシューティングに役立てる

• 「Issues」タブをクリックします。

O New Relic ONE**					S Query your	data 🔐 Instant	Observability	Apps 🥥 Get :	started Q	0 5	F) 10+ (0
Explorer Browse data Dashboards Alert	s & Al Errors Inbox	APM Browser	Infrastructure Lo	ogs Mobile	Synthetics More ~	1	r ED	Copy permalink	~ (Since 3 (days ago 🐱
ANALYZE	We'll analyze up representative	o to 1,000 events pe for more subscriptio	r month as part of yo on options.	ur subscription.	We charge for every	event beyond that. (Contact your New Reli	c	Dismiss	View us	age data
Overview											12
Issues & activity	Issues ncidents	Anomalies						Associated	account: Nev	vRelicUniversit	y-Japan ⑦
DETECT	\Xi 🚺 state = '	Active' × Search o	or click the dropdown	for options							
Alert conditions (Policies)											
Anomaly detection	1 0.8 0.6 0.4										
CORRELATE	0.2										
Sources	Dec 13, Dec 03:00 AM 09:00	13, Dec 13, 03:00 PN	Dec 13, 09:00 PM	Dec 14, 03:00 AM	Dec 14, De 09:00 AM 03:0	c 14, Dec 14, 00 PM 09:00 PM	Dec 15, 03:00 AM	Dec 15, 09:00 AM	Dec 15, 03:00 PM	Dec 15, 09:00 PM	Dec 16, 03:00 AN
Decisions	Low Medium	High Critical									
ENRICH & NOTIFY	STATE	PRIORITY	ISSUE NAME	CREATED	DURATION	ENTITIES	ANALYSIS SUMM/	ARY PATH		INC	IDENTS
Muting rules	Active	Critical	Web response time > 1 second	19m ago	19m	EC-site EC-CUBE-Check	Signal: Latency, Components: A.		> ≓	5	-

ハンズオン(3)複数のアラートを紐付け トラブルシューティングに役立てる

• オープン中のIssueが存在しない場合は「Active」フィルタを削除します。

₹0	itate = 'Active' ×	earch or click the d	ropdown for optic	85				
No cha	rt data availa	able.						
STATE	PRIORITY	ISSUE NAME	CREATED	DURATION	ENTITIES	ANALYSIS SUMMARY PA	тн	INCIDENTS
STATE	PRIORITY	ISSUE NAME	CREATED	DURATION	ENTITIES	ANALYSIS SUMMARY PA	тн	INCIE

120 new relic. 120

ハンズオン(3)複数のアラートを紐付け トラブルシューティングに役立てる

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



ハンズオン(3)複数のアラートを紐付け トラブルシューティングに役立てる

Issueをクリックすると詳細が表示されます。



ハンズオン(3)複数のアラートを紐付け トラブルシューティングに役立てる

• 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

© 2022 New Relic, Inc.

End user Apd	lex < 0,7 at lea:	st once in 5 minutes o	on 'EC-site'					
圖 4 Incidents	Source: Ο	Notified: 堂 💽 Iss	ue payload					
 Incidents (4)							
STATE 0	PRIORITY 💲	INCIDENT NAME	CREATED 🗘	DU 0	ENTITIES ©	ANALYSIS SUM	SOURCE 0	events 0
Closed	Critical	Monitor failed for location Tokyo, JP on	Mar 16, 3:28am	6m	EC-CUBE-Checkout		o	2
Closed	Critical	Web response time deviated from the	Mar 16, 3:26am	16m	EC-site	Components: Appl	o	2
Closed	Critical	Web response time > 1 seconds at least once	Mar 16, 3:26am	бm	EC-site	Components: Appl	o	2
 Root cause 	analysis							

E - Copy permalink ~ X

new relic. 123

ハンズオン(3) 複数のアラートを紐付け トラブルシューティングに役立てる

Issue 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



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



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



New Relic 実践入門

希望者に無償提供中

ついに発売された New Relic の全てを理解できる 330 ページにわたる技術書籍。オブザーバビリテ ィの基本から New Relic One の基本機能、さら には16のオブザーバビリティ実装パターンまで含め た、初心者から応用を理解したい上級者まで対象に した New Relic のパーフェクトガイドブック。

無償提供希望はこちらの Google Form から

https://forms.gle/jqiYmWRYt8Hf1nHk8

<u>紹介元情報: NRU304</u>



アプリケーション開発者 フロントエンド開発者 モバイルアプリ開発者 インフラ管理者 プロジェクトマネージャー プロダクトマネージャー **New Relic** 実践入門 監視からオブザーバビリティへの変革 松本 大樹、佐々木 千枝、田中 孝佳、伊藤 覚宏、清水 毅、 齊藤 恒太、瀬戸島 敏宏、小口 拓、東 卓弥、会澤 康二 (#) すべてを観測し、開発の高度化と 信頼性を高める運用を実現する Azure GCP モバイル Serverless Kubernetes ログ管理 高精度アラート AlOps SRE DevOps OSS 連携 SHOEISHA C Go Java NET Node.js PHP Python





kaizawa@newrelic.com @kaojiri

New Relic本はこちらから https://forms.gle/jqiYmWRYt8Hf1nHk8

i Fr

紹介元情報: NRU304



© 2022 New Relic, Inc. All rights reserved