

Alert Quality Management with Chaos Engineering



Prerequisites

1. Launch Instruqt when I say **START**.
2. **Personal** New Relic account.
3. Install Bernd's dashboard from:
https://github.com/berstr/agm_workshop

Prerequisites - QR Code

<https://bit.ly/2024-01-o11y-day-stuttgart-aqm>



Top Five Common Mistakes

- Don't know **what**, or the **right** thresholds
- Too many alerts, too many **false positives**
- No alerts maintenance or review process
- No business impact or end user in mind
- No proper description of alerts



Alert First, Talk Later

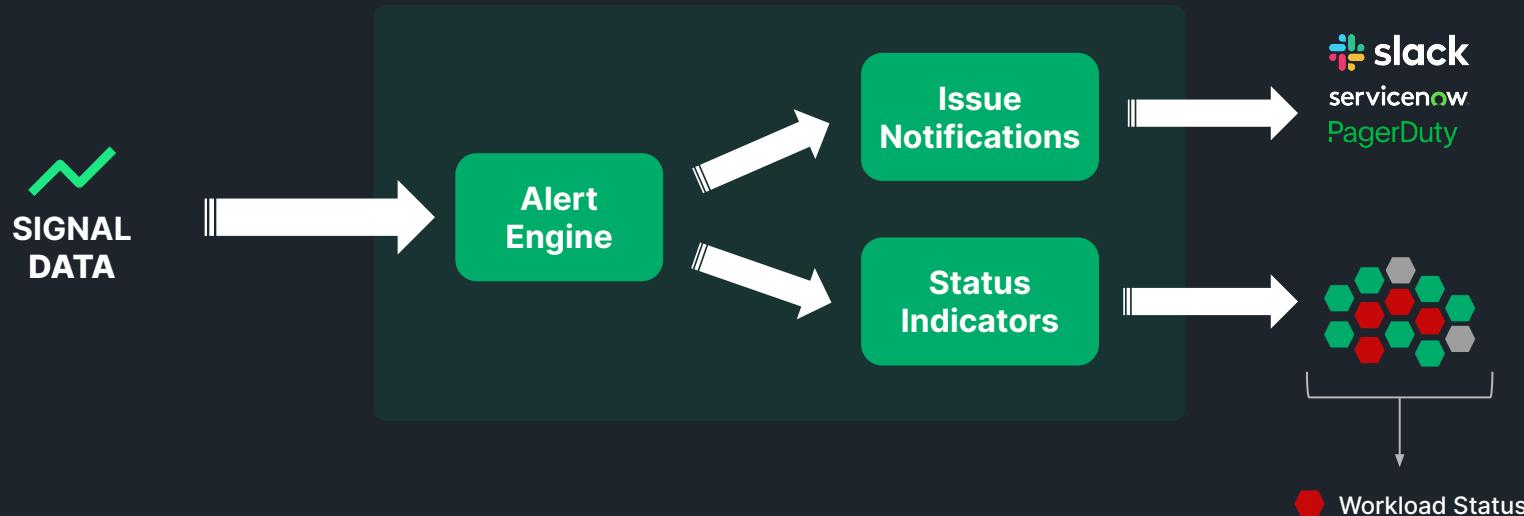
Alert quality management

Improving and optimizing the quality of your alerting

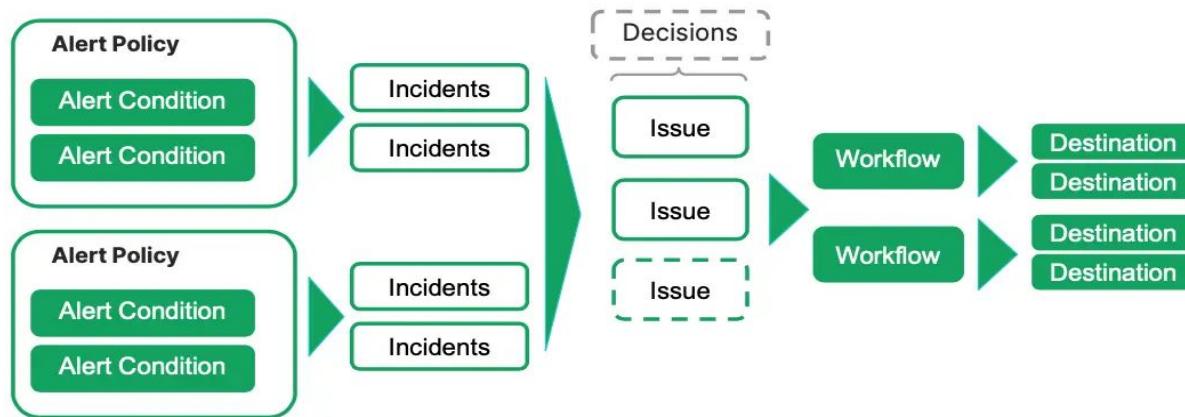
- Strategies to focus on **reducing the number of nuisance incidents** so that you focus only on alerts with **true business impact**
- Ensure that **fewer, more valuable** incidents are created
- Includes **strategies, best practice** and **tooling** for measuring and analysing **alert quality**



Getting Started with New Relic Alerts



Getting Started with New Relic Alerts



Policies - groupings of conditions where you define how you get notified when a incident occurs.

Conditions - configuration objects that you set up to open an incident.

Incidents - events where a condition threshold is breached.

Issues - a collection of one or more incidents that cause a notification to be sent.

Workflow - control where you want to **receive** notifications about issues.

Destination - control where you want to **send** notifications about issues.

16 Challenges to Learn about AQM



Alert Storm & Fatigue

- M.E.L.T
- NRQL - FACET

Bonus!
Post Mortem

Improve Alert Response

- Error Inbox
- Naming
- Tags
- Anomaly Detection
- Runbook URL

Improve Alert Quality

- Issue Preference
- Notification Method
- Enrichment
- Notification Integration
- Muting Alerts

Improve Alert Maintenance

- Alerts Overview UI
- AQM Dashboard
- Mean Time to Close
- O11y as Code

16 Challenges to Learn about AQM



Alert Storm & Fatigue

- M.E.L.T
- NRQL - FACET

Bonus!
Post Mortem

Improve Alert Response

- Error Inbox
- Naming
- Tags
- Anomaly Detection
- Runbook URL

Improve Alert Quality

- Issue Preference
- Notification Method
- Enrichment
- Notification Integration
- Muting Alerts

Improve Alert Maintenance

- Alerts Overview UI
- AQM Dashboard
- Mean Time to Close
- O11y as Code

What's causing the spike in CPU?



Challenge ONE

- Can you investigate what is causing the spike and where the script is running from?
- Without the use of **Events** and **Logs**, would it be difficult to identify the issue?
- What additional signals can we incorporate to improve **Mean Time to Recovery**?

What's causing the spike in CPU?



Challenge ONE

- Can you investigate what is causing the spike and where the script is running from?
- Without the use of **Events** and **Logs**, would it be difficult to identify the issue?
- What additional signals can we incorporate to improve **Mean Time to Recovery**?

Answer

Processes - stress-ng

Script - /root/alertqualitymanagementWithNR/chaos/script1.sh

What's causing the spike in CPU?



Challenge ONE

Processes running ⓘ Since 30 minutes ago			
Process Id	Process Display Name	CPU %	...
162677	stress-ng-cpu	11.207	Expand Get as image Get chart link
162698	stress-ng-udp-f	11.059	Export as CSV
162681	stress-ng-hdd	11.055	View query
162697	stress-ng-vm	11.009	Create alert condition Add to dashboard
162678	stress-ng-cpu	11.007	1
162682	stress-ng-hdd	10.805	1

Important!

By default, the agent doesn't send data about the operating system's processes.

To enable the sending of process data set enable_process_metrics to true.

To fine-tune which processes you want to monitor, configure include_matching_metrics.

View Query is great to help you fine-tune your alerts.

```
-workshopaqm-infra CRON[242494]: (root) CMD (sh /root/alertqualitymanagementWithNR/chaos/script1.sh)
-workshopaqm-infra stress-ng: invoked with 'stress-ng --cpu 4 --vm 2 --vm-bytes 2G --hdd 4 --fork 8 --matrix 0 -
t 180s --udp-flood 0 -t 3m --timeout 3m --metrics' by user 0 'root'
```

The location of the chaos script

Answer

Processes - **stress-ng**

Script - **/root/alertqualitymanagementWithNR/chaos/script1.sh**

Experiencing Alert Storm & Fatigue



Challenge TWO

- Can you identify which condition is using a special NRQL using **FACET**?
- **What will happen** when you turn on this special alert using FACET?

Experiencing Alert Storm & Fatigue



Challenge TWO

- Can you identify which condition is using a special NRQL using **FACET**?
- **What will happen** when you turn on this special alert using FACET?

Answer

High Process Usage

Experiencing Alert Storm & Fatigue



Challenge TWO

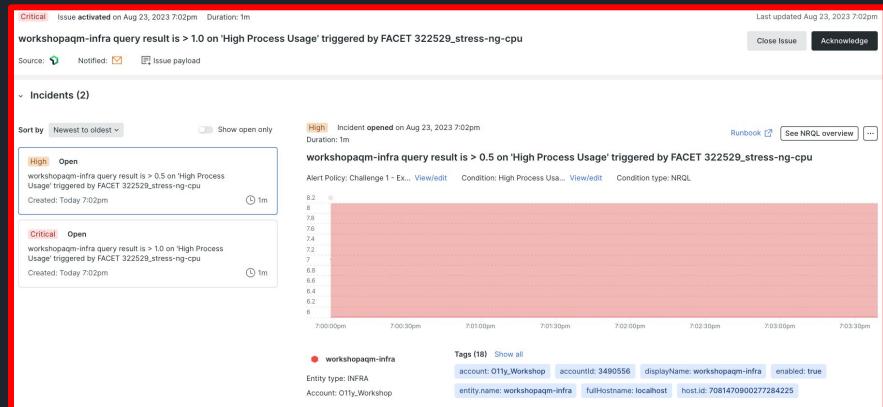
NRQL QUERY **High Process Usage**

```
NRQL> SELECT average(host.process.cpuPercent) FROM Metric FACET processId, processDisplayName WHERE entity.name = 'workshopaqm-infra'
```

Metric query result is > 1.0 at least once in 1 min
Metric query result is > 0.5 at least once in 1 min

Query the data you want to monitor ⓘ *

```
SELECT average(host.process.cpuPercent) FROM Metric FACET processId, processDisplayName WHERE entity.name = 'workshopaqm-infra'
```



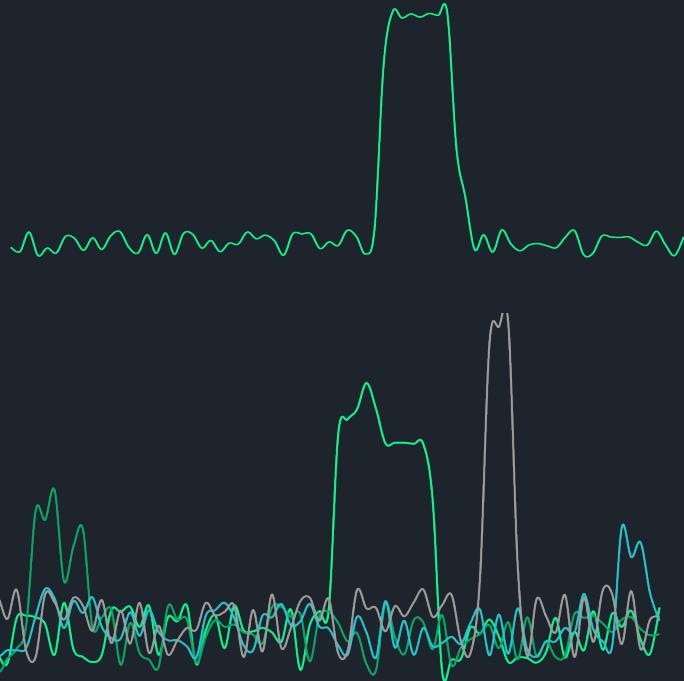
Answer

High Process Usage

Alert Storm & Fatigue

new relic

What is a Signal?



Signal

- Any data being sent to New Relic
- Result of an NRQL query against incoming data
- If you can query it you can alert on it!

Faceted signal

- Faceting the query results in multiple signals
- Each signal can trigger separate alerts
- Useful for large amounts of data points!

Faceted signal

Alert Issue

Based on NRQL without
FACET:

From Log Select count(*)
where message like
'%error=%'

Closed Issue

Critical Closed on Jan 16, 2024 10:52am Activated on Jan 16, 2024 10:48am Duration: 3m Last updated Jan 16, 2024 10:52am

Log query result is > 0.0 on 'Count of error logs > Zero'

Source: Issue payload Create postmortem

Incidents (1)

Critical Closed Log query result is > 0.0 on 'Count of error logs > Zero' Opened: Today 10:48am 3m

Critical Incident closed on Jan 16, 2024 10:52am Duration: 3m

Log query result is > 0.0 on 'Count of error logs > Zero'
Alert Policy: Initial policy Condition: Count of error logs > Zero

Incident period

5am 10:20am 10:25am 10:30am 10:35am 10:40am 10:45am 10:50am

Account: stransky-next-gen Tags (7)

account: stransky-next-gen accountid: 4207162 enabled: true id: 5514448 policyid: 1286597 trustedAccountid: 3434766 type: NRQL Query

Issue timeline & event log

Timeline Events Notifications

1 INCIDENT 1 Resolved

10:47am 10:48am 10:49am 10:50am 10:51am 10:52am

Critical High Medium Low

© 2023 New Relic, Inc. All rights reserved

Faceted signal

Alert Issue

Based on NRQL with
FACET:

From Log Select count(*)
where message like
'%error=%' FACET hostname

The screenshot shows the 'Active Issue' details for a critical alert. The alert was activated on Jan 16, 2024, at 11:06am, with a duration of 2m. The condition is 'vm030 query result is > 0.0 on "Count of error logs > Zero" triggered by FACET vm030'. The source is 'Issue payload'. A pink arrow points from the text above to the 'Incidents (1)' section.

Incidents (1)

Critical Open
vm030 query result is > 0.0 on "Count of error logs > Zero" triggered by FACET vm030
Opened: Today 11:06am 2m

Critical Incident opened on Jan 16, 2024 11:06am Duration: 2m
vm030 query result is > 0.0 on "Count of error logs > Zero" triggered by FACET vm030
Alert Policy: Initial policy Condition: Count of error logs > Zero

Query this data ...

Incident period

Impacted entities (1)

vm030 Entity type: INFRA Account: stransky-next-gen

Tags (14) Show all

- account: stransky-next-gen
- accountid: 4207162
- enabled: true
- fullHostname: vm030
- hostname: vm030
- hostStatus: running
- id: 5514448
- linuxDistribution: Ubuntu 22.04.2 LTS
- nr_deployed_by: newrelic-cli
- nr_logAccountId: 4207162
- nr_logEventId: Log
- policyId: 12866597

Search for a specific entity Health status Entity types Relationship depth: 1

Infrastructure (1 entity)

vm030 [Details] Host: stransky-next-gen Analyze performance in Lookout app

Activity Stream

Critical Issue Activated 11:06am
vm030 vm030 query result is > 0.0 on "Count of error logs > Zero"

Tags

Add a tag Use a key/value structure to create new tags

account: stransky-next-gen accountid: 4207162 agentName: infrastructure agentVersion: 1.47.2 coreCount: 2

Issue timeline & event log

Timeline Events Notifications

1 INCIDENT 1 Active

Critical High Medium Low

relic

Creating a Post Mortem



Challenge BONUS

- Postmortem is a retrospective process that teams use to analyze what worked and what didn't when responding to and resolving an incident.
- In the platform, the postmortem feature is a tool you can use to prepare a successful retrospective process for your team.
- Postmortems **automatically collect data** related to an incident, freeing up your team to focus on analysis and action items for improved responses to future incidents.

Creating a Post Mortem



Challenge BONUS

- Postmortem is a retrospective process that teams use to analyze what worked and what didn't when responding to and resolving an incident.
- In the platform, the postmortem feature is a tool you can use to prepare a successful retrospective process for your team.
- Postmortems **automatically collect data** related to an incident, freeing up your team to focus on analysis and action items for improved responses to future incidents.

Answer

From the issue feed, select an Open Issue for your postmortem.

Creating a Post Mortem



Challenge BONUS

The screenshot illustrates the workflow for creating a post-mortem. On the left, a modal window asks "Are you sure you want to close this issue?". It contains a note about closing related incidents and a checkbox for "Add postmortem beta". A red box highlights this checkbox, and a red arrow points to the right, indicating the transition to the next step. On the right, the "Create Postmortem" page is shown. It includes fields for "Impact Level" (set to Critical), "Name (required)", "What happened? (required)", "Root cause", "Recovery actions", and a "Timeline" section. The timeline shows an incident from Aug 23, 2023, at 7:02pm, detailing a policy violation for high process usage.

Answer

From the issue feed, select an Open Issue for your postmortem.

16 Challenges to Learn about AQM



Alert Storm & Fatigue

- M.E.L.T
- NRQL - FACET

Bonus!
Post Mortem

Improve Alert Response

- Error Inbox
- Naming
- Tags
- Anomaly Detection
- Runbook URL

Improve Alert Quality

- Issue Preference
- Notification Method
- Enrichment
- Notification Integration
- Muting Alerts

Improve Alert Maintenance

- Alerts Overview UI
- AQM Dashboard
- Mean Time to Close
- O11y as Code

Improve Alert Response

 new relic

What's causing additional issues?



Challenge THREE

- What went wrong in the game? **Can the game run successfully?**
- If we didn't add application-level insights, how would engineers resolve these issues?
- Why most engineers focus on the Infrastructure layer?
- Will players be able to enjoy the game without experiencing any major glitches or bugs?

[Improve Alert Response](#)

 new relic

What's causing additional issues?



Challenge THREE

- What went wrong in the game? **Can the game run successfully?**
- If we didn't add application-level insights, how would engineers resolve these issues?
- Why most engineers focus on the Infrastructure layer?
- Will players be able to enjoy the game without experiencing any major glitches or bugs?

Answer

Errors (500, Boom, 401, 409) as seen in Error Inbox

[Improve Alert Response](#)

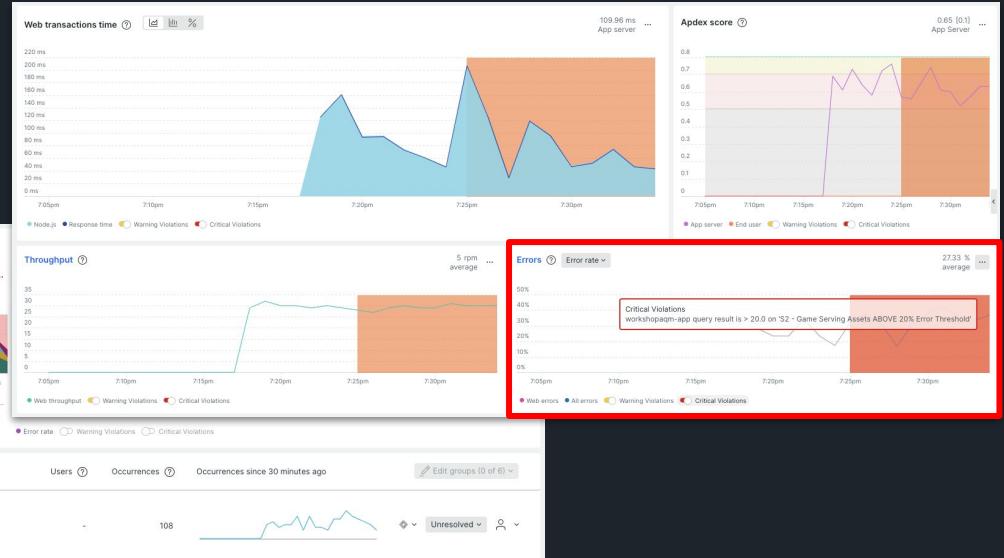
 new relic

What's causing additional issues?



Challenge THREE

The screenshot shows the New Relic interface with the 'Errors (errors in box)' link highlighted by a red arrow. The 'Errors overview' section displays a chart of error count over time, with several error types visible: Error, httpError 500, httpError 400, httpError 401, and httpError 409. A legend indicates the colors for each error type.



Answer

Errors (500, Boom, 401, 409) as seen in Error Inbox

Improve Alert Response

 new relic

Which alert contains S1?



Challenge FOUR

- The description and the tags must give you **self-descriptive** alerts to know which service is wrong, which environment is involved, which team owns it, and if it's impacting to end users. It helps you to answer faster and decide what to do.
- Service categorization helps with **prioritization** and allocation of resources.

Which alert contains S1?



Challenge FOUR

- The description and the tags must give you **self-descriptive** alerts to know which service is wrong, which environment is involved, which team owns it, and if it's impacting to end users. It helps you to answer faster and decide what to do.
- Service categorization helps with **prioritization** and allocation of resources.

Answer

S1 - Game Main API ABOVE 90 Percentile - including SIGNAL LOST

[Improve Alert Response](#)

 new relic

Which alert contains S1?



Challenge FOUR

NRQL QUERY S1 - Game Main API ABOVE 90% Percentile - including SIGNAL LOST

NRQL> SELECT percentile(duration, 90) FROM Transaction WHERE appName = 'workshopaqm-app' AND name = 'WebTransaction/Expressjs/GET//game'

✖ Transaction query result is > 4.0 at least once in 2 mins
⚠ Transaction query result is > 3.0 at least once in 2 mins

⌚ Consider the signal lost after minutes Minimum 1 minute

On signal loss:

Close all current open incidents

Open new "lost signal" incident
Notification sent based on issue creation preference

Answer

S1 - Game Main API ABOVE 90% Percentile - including SIGNAL LOST

Improve Alert Response

 new relic

Add tags to Terraform, or via the UI?



Challenge FIVE

- Your issues and incidents have these tags in their metadata.
- Use them to do flexible filters in workflows or add them to your notification payload.
- Tags are extremely important for review, reporting, and analysis.

[Improve Alert Response](#)

 new relic

Add tags to Terraform, or via the UI?



Challenge FIVE

- Your issues and incidents have these tags in their metadata.
- Use them to do flexible filters in workflows or add them to your notification payload.
- Tags are extremely important for review, reporting, and analysis.

Answer

`resource newrelic_entity_tags in TF, or via New Relic Tags UI`

[Improve Alert Response](#)

 new relic

Add tags to Terraform, or via the UI?



Challenge FIVE

```
# resource to create, update, and delete tags for a New Relic entity - App
resource "newrelic_entity_tags" "appname" {
  guid = data.newrelic_entity.appname.guid

  tag {
    key = "escalation"
    values = ["High"]
  }

  tag {
    key = "stack"
    values = ["Node.js", "Express", "Public"]
  }

  tag {
    key = "version"
    values = ["v2.1"]
  }

  tag {
    key = "team"
    values = ["Application"]
  }
}
```

via Terraform

The screenshot shows the New Relic APM interface for the 'workshopaqm-app'. The left sidebar lists various monitoring features: MONITOR, Recommendations, Distributed tracing, Service map, Dependencies, Transactions, Databases, External services, and Node VMs. The 'Transactions' section is currently selected. A red arrow points to the 'Tags' tab at the top of the main content area. A modal window titled 'Add a tag' is open, prompting the user to 'Use a key-value structure to create new tags'. It contains several tag entries: account: O1ly_Workshop, accountid: 3490556, agentVersion: 9.15.0; instrumentation.name: apm, instrumentation.provider: newRelic; language: nodejs, nr.tracing: standard, trustedAccountId: 1914858; escalation: High, stack: Express, Stack: Express; stack: Node.js, Stack: Node.js, stack: Public, Stack: Public; team: Application, Team: Application, version: v2.1.

via the UI

Answer

resource newrelic_entity_tags in TF, or via New Relic Tags UI

Improve Alert Response

 new relic

Configured with Anomaly Threshold?



Challenge SIX

- Explore anomaly based alerts.
- Anomaly thresholds use past data to dynamically predict the data's near-future behavior.
This will adjust over time as it learns the patterns of your data.
- Best for the environment when there is constantly available data.

[Improve Alert Response](#)

 new relic

Configured with Anomaly Threshold?



Challenge SIX

- Explore anomaly based alerts.
- Anomaly thresholds use past data to dynamically predict the data's near-future behavior.
This will adjust over time as it learns the patterns of your data.
- Best for the environment when there is constantly available data.

Answer

All Alerts with S3

[Improve Alert Response](#)

Configured with Anomaly Threshold?

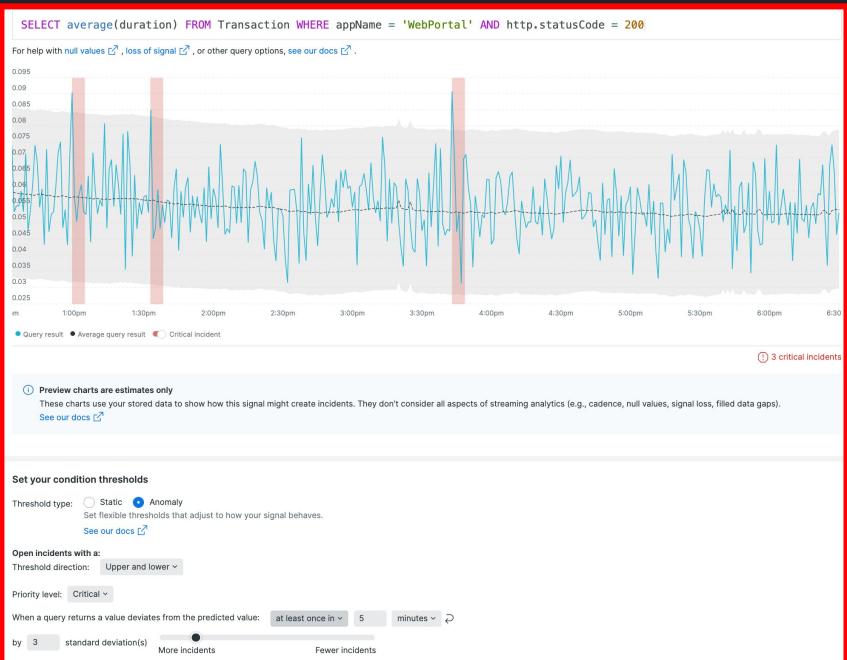


Challenge SIX

NRQL ANOMALY (BASELINE) QUERY S3 - Game Response Time DEVIATED from Dynamic Threshold

```
NRQL> SELECT average(newrelic.goldenmetrics.apm.application.responseTimeMs) FROM Metric WHERE entity.name = 'workshopaqm-app'
```

✖ Metric deviates from baseline at least once in 2 mins
⚠ Metric deviates from baseline at least once in 2 mins



Answer

All Alerts with S3

Improve Alert Response

 new relic

What is the current runbook URL?



Challenge SEVEN

- The runbook must describe remediation steps to follow and who to involve or escalate to.
- Includes identifying the individuals or teams responsible for implementing each step and the channels that should be used to escalate the issue if necessary.
- Outline any preventive measures that can be taken to avoid similar incidents in the future.

What is the current runbook URL?



Challenge SEVEN

- The runbook must describe remediation steps to follow and who to involve or escalate to.
- Includes identifying the individuals or teams responsible for implementing each step and the channels that should be used to escalate the issue if necessary.
- Outline any preventive measures that can be taken to avoid similar incidents in the future.

Answer

<https://www.atlassian.com/software/confluence/templates/devops-runbook>

What is the current runbook URL?



Challenge SEVEN

Name your alert condition *

S3 - Game Response Time DEVIATED from Dynamic Threshold

Close open incidents after hours

This setting is related to the issue setting.
When the time periods in these two settings are different, our system uses the shorter time period. For example, if the close open incident setting is 3 days and the issue time setting is 2 days, our system would wait 2 days before closing the incident.
[View the issue setting](#)

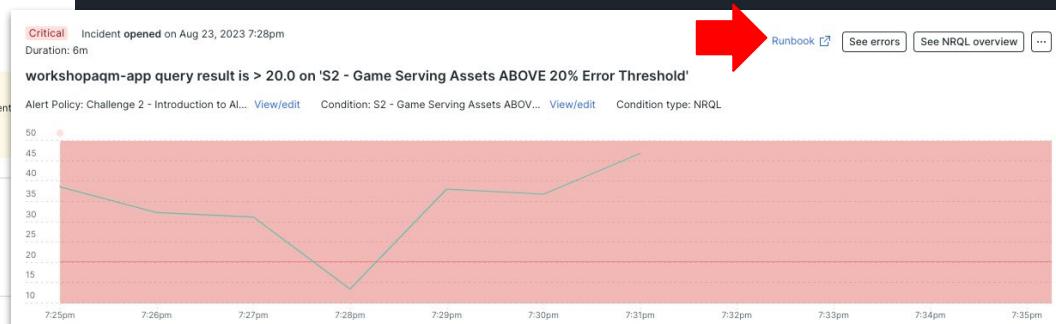
Send a custom incident description (optional)

The game response time deviated from the configured threshold, as seen with previous data points.

4,000 character limit

Runbook URL (optional)
<https://www.atlassian.com/software/confluence/templates/devops-runbook>

Enable on save



Answer

<https://www.atlassian.com/software/confluence/templates/devops-runbook>

Improve Alert Response

new relic

NRQL Condition tuning



Many more features for refining how signal data is processed and evaluated.



Fine tuning

Configure aggregation windows, delay and streaming methods to reliably process your signal



Gap filling

Reduce false alerts caused by sporadic data by specifying gap filling strategy



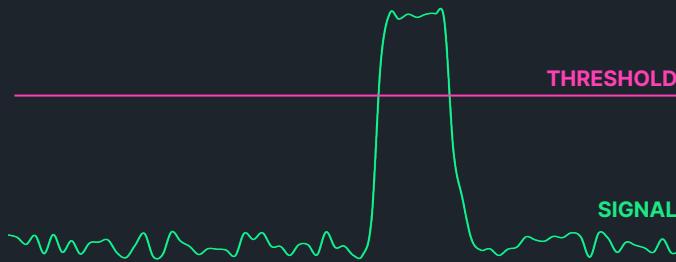
Signal loss

What to do if a signal is no longer being received

[Improve Alert Response](#)

 new relic

Conditions & Threshold



Signal Query

Defined by NRQL query including optional WHERE and FACET clauses.

Guided wizard available to help build.

*Additional non-NRQL conditions soon to be deprecated

Some examples

Signal	Threshold
% Error rate	% error > 5%
Average basket value	median(value) < \$20
Login attempts per user	uniqueCount(user) > 10

Threshold

Value, which if breached for a defined time period, will trigger an incident to be opened.

Can be set for both **warning** and **critical**

[Improve Alert Response](#)

 new relic

Conditions & Threshold



- Incidents **open** when a **signal breaches the threshold** defined in a condition.
- Incidents **close automatically** when the signal is no longer in breach.
- There will be some **latency** between signal breaching and incident opening based on condition settings.
- Incident will open for **each signal facet**
- Incidents can be **manually closed** by user

Improve Alert Response

 new relic

16 Challenges to Learn about AQM



Alert Storm & Fatigue

- M.E.L.T
- NRQL - FACET

Bonus!
Post Mortem

Improve Alert Response

- Error Inbox
- Naming
- Tags
- Anomaly Detection
- Runbook URL

Improve Alert Quality

- Issue Preference
- Notification Method
- Enrichment
- Notification Integration
- Muting Alerts

Improve Alert Maintenance

- Alerts Overview UI
- AQM Dashboard
- Mean Time to Close
- O11y as Code

What are the issue preference options?



Challenge EIGHT

- Creating a policy for each separate destination or audience needs to receive a notification.
- Consider grouping by entity, service, or technology to match the focus of your teams.
- Issues determine when you're notified about incidents disrupting your business. These incidents occur when they meet your alert conditions.

What are the issue preference options?



Challenge EIGHT

- Creating a policy for each separate destination or audience needs to receive a notification.
- Consider grouping by entity, service, or technology to match the focus of your teams.
- Issues determine when you're notified about incidents disrupting your business. These incidents occur when they meet your alert conditions.

Answer

One issue per condition

Improve Alert Quality

 new relic

What are the issue preference options?



Challenge EIGHT

Challenge 3 - Improvements to Alert Quality Management

id: 4730003

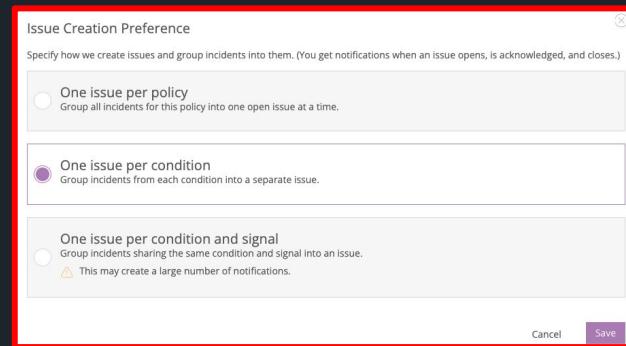
Correlate and suppress noise Issue Creation Preference: One issue per condition

Important!

Ask your team 2 important questions when deciding your issue preferences:

Q1 - Do we want to be notified every time something goes wrong?

Q2- Do we want to group all similar notifications together and be notified once?



Answer

One issue per condition

Improve Alert Quality

new relic

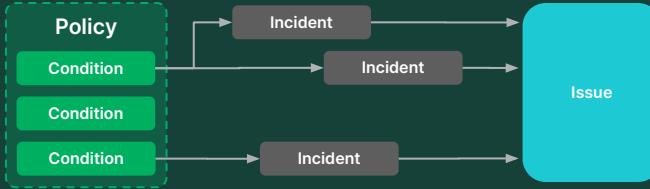
Incident Groupings



FEWER ISSUES

1

Per Policy

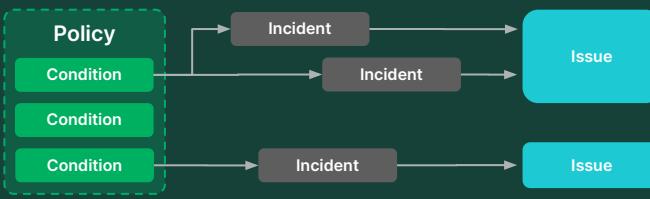


Only one issue will be open at a time for the **entire policy**.

- Requires immediate action and closing the issues to be effective

2

Per Condition

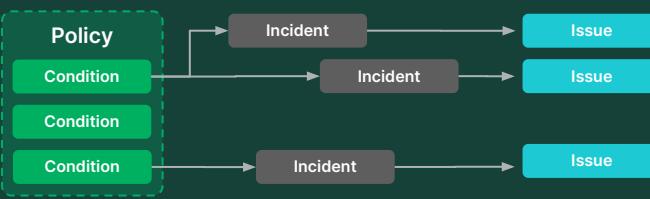


One issue will be open at a time for **each condition** in your policy.

- Useful for policies containing conditions that focus on entities that perform the same job

3

Per Incident



An issue will be created for **every incident** of **each condition** in your policy.

- Useful if you need to be notified of every violation or if you have an external system where you want to send alert notifications

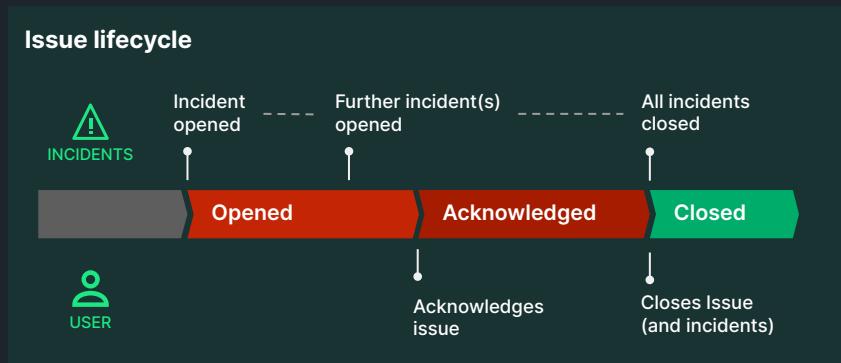
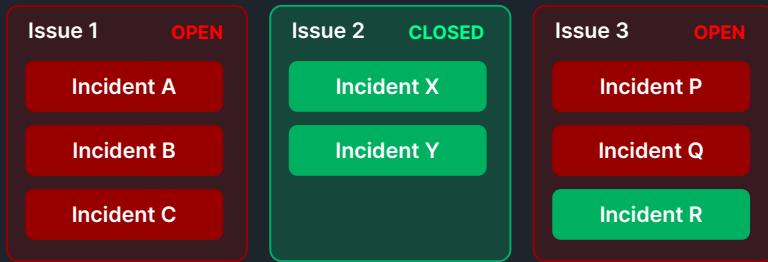
MORE ISSUES



Improve Alert Quality

new relic

Incident Groupings



"Incidents are the symptoms of a larger problem (the issue)"

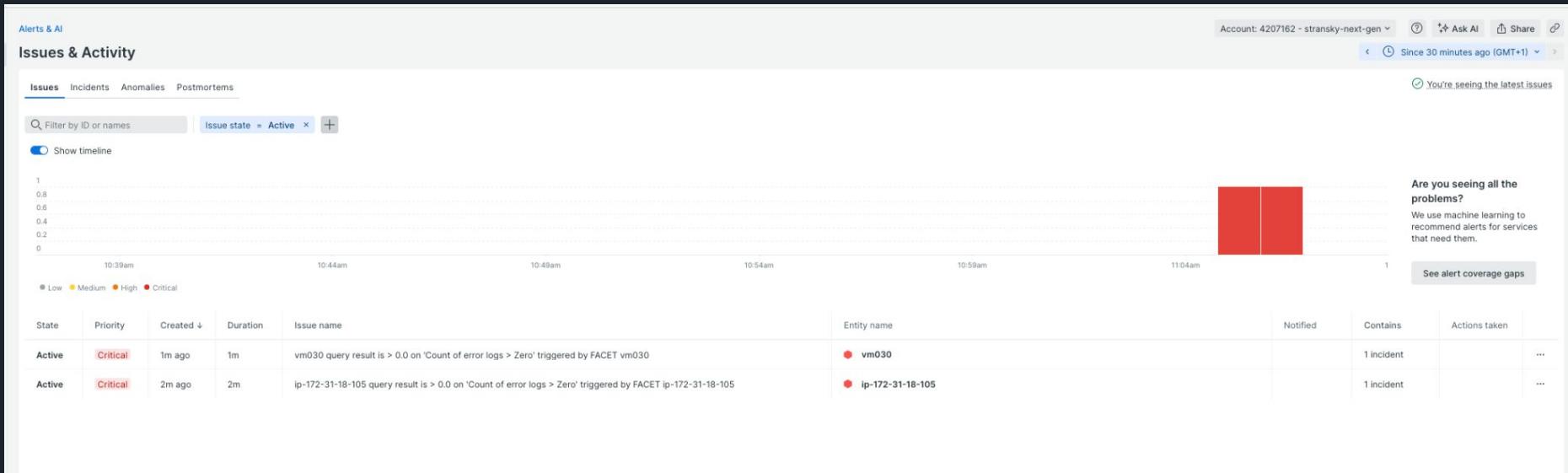
Issues **group incidents together**, reducing noise and driving notification workflows.

- Issues are **opened when incidents open**
- Issues can **contain multiple incidents**
based on policy preference or correlation decisions
- Issues **close automatically** when all contained incidents have closed or if inactive
- Issues can be **manually closed**, which close all contained incidents.

Improve Alert Quality

Quiz: Alert on log messages with “error=”

2 Hosts received such messages



Why are there 2 issues?

2 Hosts received log messages with “error=”

Why are there 2 Issues ?

NRQL Alert Condition with FACET:

From Log Select count(*)

where message like '%error=%'

FACET hostname

Alert Policy Issue Preference:

One Issue per Condition and Signal

The screenshot shows the 'Alert Policies' section of the New Relic interface. At the top, a yellow bar says 'Get notified when issues start. To get notifications about your issues, create a workflow for this policy. See our docs'. Below it, the 'ID: 1286597' is listed. There are tabs for 'Alert conditions', 'Notifications', and 'Settings', with 'Settings' being the active tab. Under 'Policy name', the text 'Initial policy' is shown. In the 'Correlation' section, the checkbox 'Correlate and suppress noise' is unchecked. In the 'Issue creation preference' section, the radio button 'One issue per condition and signal' is selected. A note below says 'Group incidents sharing the same condition and signal into an issue.' At the bottom right, there is a 'Save' button and a 'Delete policy' link.

2 Hosts received log messages with “error=”

A)

Condition NRQL: From Log Select count(*) where message like '%error=%'

Policy Preference: One Issue per Condition and Signal

How many incidents ?

How many issues ?



B)

Condition NRQL: From Log Select count(*) where message like '%error=%' FACET hostname

Policy Preference: One Issue per Condition

How many incidents ?

How many issues ?

2 Hosts received log messages with “error=”

A)

Condition NRQL: From Log Select count(*) where message like '%error=%'

Policy Preference: One Issue per Condition and Signal

How many incidents ? ⇒ 1

How many issues ? ⇒ 1



B)

Condition NRQL: From Log Select count(*) where message like '%error=%' FACET hostname

Policy Preference: One Issue per Condition

How many incidents ? ⇒ 2

How many issues ? ⇒ 1

The alerts send to, using which method?



Challenge NINE

- Define alert categories, expectations for handling their notifications, and a unique destination across your organization
- For example, proactive to Slack to notify before the incident occurs; reactive to PagerDuty to detect and notify of an ongoing incident; or informative to Jira.

The alerts send to, using which method?



Challenge NINE

- Define alert categories, expectations for handling their notifications, and a unique destination across your organization
- For example, proactive to Slack to notify before the incident occurs; reactive to PagerDuty to detect and notify of an ongoing incident; or informative to Jira.

Answer

Email

Improve Alert Quality

The alerts send to, using which method?



Challenge NINE

Challenge 3 - Improvements to Alert Quality Management
Id: 4730003

Correlate and suppress noise Issue Creation Preference: One issue per condition Delete this policy

11 Alert conditions Notification settings Last modified 7:51 pm by User 3838371

Add a destination
Add destinations where we send notifications.

Jira ServiceNow Slack Webhook PagerDuty AWS EventBridge Mobile push

Notifications Log Destinations (15)

Manage destinations where we send notifications.

Connection Type	Destinations
Policy Name	<input checked="" type="checkbox"/> Email

Answer

Email

Improve Alert Quality

 new relic

How do you enrich alerts in New Relic?



Challenge TEN

- Enrichments can give additional context on alert notifications by adding NRQL query results to them. The workflows enrich tool is similar to the query builder.
- Triage your alert notifications faster by providing additional metrics specific to the issue.

[Improve Alert Quality](#)

 new relic

How do you enrich alerts in New Relic?



Challenge TEN

- Enrichments can give additional context on alert notifications by adding NRQL query results to them. The workflows enrich tool is similar to the query builder.
- Triage your alert notifications faster by providing additional metrics specific to the issue.

Answer

Alert Workflow Enrichment

Improve Alert Quality

How do you enrich alerts in New Relic?



Challenge TEN

The screenshot shows the New Relic interface with a red arrow pointing to the 'Workflows' tab in the left sidebar. The main content area displays a configuration dialog for 'Additional settings' under 'Enrich your data'. The dialog contains two NRQL queries:

```
Linux Process Enrichment - Infrastructure
SELECT average(host.process.cpuPercent) as 'Processes' FROM Metric FACET processid, processDisplayName WHERE entity.name = 'workshopaqm-infra' SINCE 1 hour ago
```

```
Stress-ng Logs Enrichment - Logs
SELECT count(*) FROM Log WHERE allColumnSearch('CRON', insensitive: true) AND allColumnSearch('CMD', insensitive: true) since 1 hour ago FACET message
```

Below the queries is a 'Mute issues' section with three radio button options:

- Do not send notifications for fully muted issues
- Do not send notifications for fully or partially muted issues
- Always send notifications

At the bottom, there is a table listing existing workflows:

Name	Destinations	Last run	Enabled
Policy: 4462734 - Workshop AQM	Email	Jul 14, 2023 7:54pm	<input type="checkbox"/>
Challenge 3 - Improvements to Alert Quality Management	Email	Aug 23, 2023 7:55pm	<input checked="" type="checkbox"/>

Answer

Alert Workflow Enrichment

Improve Alert Quality

new relic

Where can I find notification integrations?

Challenge ELEVEN

- Add a responsible team as this team will be in charge of handling the first notification.
- Destinations are where we send notifications about your New Relic data. A destination is a unique identifier for a third-party system that you use.
- Destination settings contain the connection details to integrate with third-party systems and can be used across a variety of tools in New Relic.

Where can I find notification integrations?

Challenge ELEVEN

- Add a responsible team as this team will be in charge of handling the first notification.
- Destinations are where we send notifications about your New Relic data. A destination is a unique identifier for a third-party system that you use.
- Destination settings contain the connection details to integrate with third-party systems and can be used across a variety of tools in New Relic.

Answer

Alert Destination

[Improve Alert Quality](#)

Where can I find notification integrations?



Challenge ELEVEN

Add a destination

Add destinations where we send notifications.

Jira ServiceNow Slack Webhook PagerDuty AWS EventBridge Mobile push

Notifications Log Destinations (15)

Manage destinations where we send notifications.

Type Name Two-way URL/Details Last updated Updated by Enabled

Type	Name	Two-way	URL/Details	Last updated	Updated by	Enabled
Alerts	Alerts to Priority Team	Two-way	username@example.com	Aug 9, 2023 10:23pm	3838371	<input checked="" type="checkbox"/>



Answer

Alert Destination

Improve Alert Quality

 new relic

Notification Triage and Routing



- Control **when** you want to receive notifications about issues to the right channel
- **Notify correct teams** based on issue context
- Channels offer comprehensive **payload templating** options
- **Enrich notifications** with additional context from other data points

Workflow → Channel → Destination



Channels allow **multiple different message payloads** to be sent to **multiple destinations**

How do I mute alerts?



Challenge TWELVE

- Alerts sends out timely notifications when your system is having problems. You can use muting rules to stop being bombarded by messages that don't need your attention.
- Muted alerts will still gathers data on those incidents. Muting rules don't interfere with the alerts process and are applied at the point right before a notification is sent.

[Improve Alert Quality](#)

How do I mute alerts?



Challenge TWELVE

- Alerts sends out timely notifications when your system is having problems. You can use muting rules to stop being bombarded by messages that don't need your attention.
- Muted alerts will still gathers data on those incidents. Muting rules don't interfere with the alerts process and are applied at the point right before a notification is sent.

Answer

[Challenge 1 & Challenge 2](#)

[Improve Alert Quality](#)

How do I mute alerts?



Challenge TWELVE

Muting rules 

+ Add a rule

Use muting rules to mute notifications when you don't need them, like when you're performing maintenance. See our docs [↗](#)

Muting status	Name
ACTIVE	Muting All Alert Storm

Where a violation contains

Attribute policyName Operator contains Value Challenge 1

and a violation contains or a violation contains

Attribute policyName Operator contains Value Challenge 2

[+ Add another condition](#)

Answer

Challenge 1 & Challenge 2

Improve Alert Quality

 new relic

16 Challenges to Learn about AQM



Alert Storm & Fatigue

- M.E.L.T
- NRQL - FACET

Bonus!
Post Mortem

Improve Alert Response

- Error Inbox
- Naming
- Tags
- Anomaly Detection
- Runbook URL

Improve Alert Quality

- Issue Preference
- Notification Method
- Enrichment
- Notification Integration
- Muting Alerts

Improve Alert Maintenance

- Alerts Overview UI
- AQM Dashboard
- Mean Time to Close
- O11y as Code

Policy with the highest amount of alerts?



Challenge THIRTEEN

- Schedule a periodical review of alert conditions - use the Alerts overview page to check the incidents created and decide the action to do.
- We recommend you to tag the condition with the last review date, which will allow you to identify obsolete alerts.

Policy with the highest amount of alerts?



Challenge THIRTEEN

- Schedule a periodical review of alert conditions - use the Alerts overview page to check the incidents created and decide the action to do.
- We recommend you to tag the condition with the last review date, which will allow you to identify obsolete alerts.

Answer

Top policies creating incidents

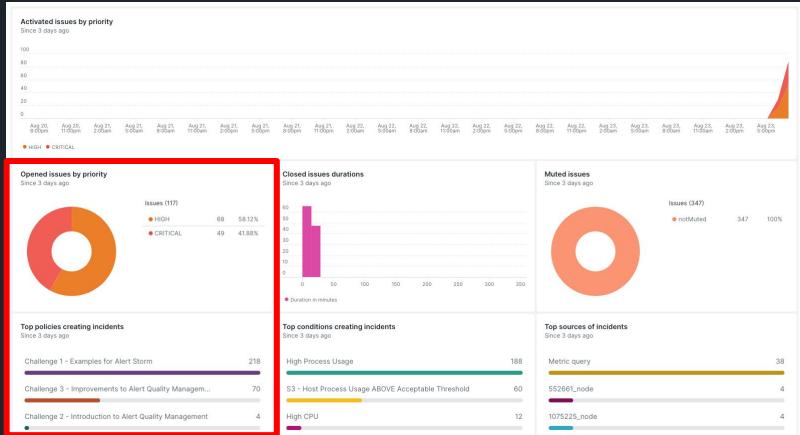
[Improve Alert Maintenance](#)

 new relic

Policy with the highest amount of alerts?



Challenge THIRTEEN



Answer

Top policies creating incidents

Important!

On the Alerts & AI Overview page, you'll find a consolidated view of your current alerts incidents. The Issues & activity page has views of your active issues, recent incidents, and anomalies.

Top policies creating incidents

A chart of the top five policies generating the most incidents. Click a policy name to filter the whole page by that policy's incidents.

Top conditions creating incidents

A chart of the top five conditions generating the most incidents. Click a condition name to filter the whole page by that condition's incidents.

Top sources of incidents

A chart of the entities generating the most incidents. If available, it uses the entity name. Otherwise, it will use the event type. Click an entity to filter the whole page by that entity's incidents.

Improve Alert Maintenance

 new relic

How do I install the AQM dashboard?



Challenge FOURTEEN

- Review the alert quality dashboard - focus on reducing the number of nuisance incidents so that you focus only on alerts with true business impact.
- This reduces alert fatigue and ensures that you and your team focus your attention on the right places at the right times.

How do I install the AQM dashboard?



Challenge FOURTEEN

- Review the alert quality dashboard - focus on reducing the number of nuisance incidents so that you focus only on alerts with true business impact.
- This reduces alert fatigue and ensures that you and your team focus your attention on the right places at the right times.

Answer

Add Data and search for Alerts Quality Management

Improve Alert Maintenance

 new relic

How do I install the AQM dashboard?



Challenge FOURTEEN

Add Data

All (1)

- Guided install (0)
- Application monitoring (0)
- Infrastructure & OS (0)
- Browser & mobile (0)
- Simulate traffic (0)
- Logging (0)
- Kubernetes & containers (0)
- Amazon Web Services (0)
- Azure (0)
- Google Cloud Platform (0)
- Security (0)
- Open source monitoring (0)
- ML models (0)
- Network (0)
- Partner (0)

Popular search terms: AWS Node Java PHP Kubernetes

Data sources (0) Dashboards (1) Alerts (0) Apps & visualizations (0)

Other (1)

Alert Quality Management
Created by Alec Isaacson (New Relic)
Last edit 6 months ago

Incident Count Since 1 week ago vs. 1 week ago
159 ▲ 21.4% Incident Count

Closed Incident Minutes (Accumulated) Since 1 week ago vs. 1 week ago
1.85 k ▾ 17% Incident Minutes

Incident MTTC (minutes) Since 1 week ago vs. 1 week ago
16.8 ▾ 1.2% Incident MTTC (minutes)

% Under 5min Since 1 week ago vs. 1 week ago
12.73% ▾ 64.5% % Under 5min

% Investigated Since 1 week ago vs. 1 week ago
2.04 ▾ 36.7% % Investigated

MTTI (minutes) Since 1 week ago vs. 1 week ago
1.9 ▾ 70.5% Incident MTI (minutes)

Alerting Count by Policy Since 1 week ago

Policy Name	Count	Minutes	% Investigated	MTTC	%<5min
Challenge 1 - Examples for Alert Storm	108	1.82 k	0	16.9	0
Challenge 3 - Improvements to Alert Quality Management	49	0	0	0	0
Challenge 2 - Introduction to Alert Quality Management	2	29	0	14.5	0

Incident Count Since 1 week ago vs. 1 week ago

Incident Duration Since 1 week ago vs. 1 week ago



Answer

Add Data and search for Alerts Quality Management

Improve Alert Maintenance

new relic

Exact NRQL needed to find out MTTC?



Challenge FIFTEEN

- Mean Time to Close (MTTC) - This is the average duration of incidents within the period of time measured. You want this number to be as low as possible.

Exact NRQL needed to find out MTTC?



Challenge FIFTEEN

- Mean Time to Close (MTTC) - This is the average duration of incidents within the period of time measured. You want this number to be as low as possible.

Answer

```
FROM NrAilncident SELECT average(durationSeconds/60) AS 'Incident MTTC (minutes)'  
WHERE event = 'close' AND priority = 'critical' SINCE 1 WEEK AGO COMPARE WITH 1 WEEK AGO
```

Exact NRQL needed to find out MTTC?



Challenge FIFTEEN

Mean time to close (MTTC) KPI

This is the average duration of incidents within the period of time measured. You want this number to be as low as possible.

Goal: Reduce MTTC

Best practices:

- Don't manually close incidents, as doing so can warp the accuracy of this KPI.
- Improve reliability engineering skills.
- Report AQM KPIs to all stakeholders.

```
FROM NrAiIncident SELECT average(durationSeconds/60) AS 'Incident MTTC (minutes)' WHERE event = 'close' AND priority = 'critical' SINCE 1 WEEK AGO COMPARE WITH 1 WEEK AGO
```

Copy

<https://docs.newrelic.com/docs/tutorial-create-alerts/manage-alert-quality/#volume>

Answer

```
FROM NrAiIncident SELECT average(durationSeconds/60) AS 'Incident MTTC (minutes)'  
WHERE event = 'close' AND priority = 'critical' SINCE 1 WEEK AGO COMPARE WITH 1 WEEK AGO
```

How do you use Terraform?



Challenge SIXTEEN

- Terraform is a popular infrastructure-as-code tool built by HashiCorp to provision all kinds of infrastructure and services, including New Relic dashboards and alerts.
- Automate your alert creation using Terraform where you can prevent undocumented changes and clear traceability by installing Terraform, read the getting started guide and visit the New Relic official guide.

[Improve Alert Maintenance](#)

 new relic

How do you use Terraform?



Challenge SIXTEEN

- Terraform is a popular infrastructure-as-code tool built by HashiCorp to provision all kinds of infrastructure and services, including New Relic dashboards and alerts.
- Automate your alert creation using Terraform where you can prevent undocumented changes and clear traceability by installing Terraform, read the getting started guide and visit the New Relic official guide.

Answer

Terraform cmd examples as seen in the workshop

Improve Alert Maintenance

 new relic

How do you use Terraform?



Challenge SIXTEEN

The screenshot shows two side-by-side interfaces. On the left is the 'New Relic Provider' documentation page, which includes sections for 'Getting started', 'Data sources', and 'Advanced'. On the right is a Terraform UI interface showing an alert configuration for 'S1 - Game Main API ABOVE 90% Percentile - including SIGNAL LOST'. A red arrow points to the 'View' button in the top right corner of the UI window.

S1 - Game Main API ABOVE 90% Percentile - including SIGNAL LOST

Alert conditions compare signal behavior to thresholds you set. When the signal goes outside those thresholds, we create an incident.

ID: 36024154 | Account: 3490556 - O1ty_Workshop | Policy: 4730003 - Challenge 3 - Improvements to Alert Quality Management

Define your signal

Define your signal

Select your signals

Build a query

Golden signal or metric

Query the data you want to monitor ⓘ

```
SELECT percentile(duration, 90) FROM Transaction WHERE appName = 'workshopaqm-app' AND name = 'WebTransaction/Expressjs/GET//game'
```

You can also view the TF code via the UI

Answer

Terraform cmd examples as seen in the workshop

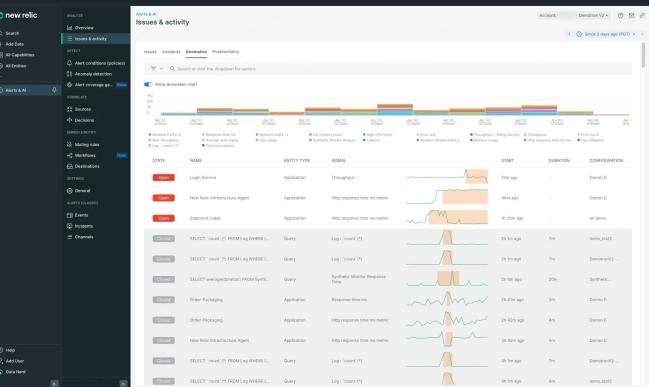
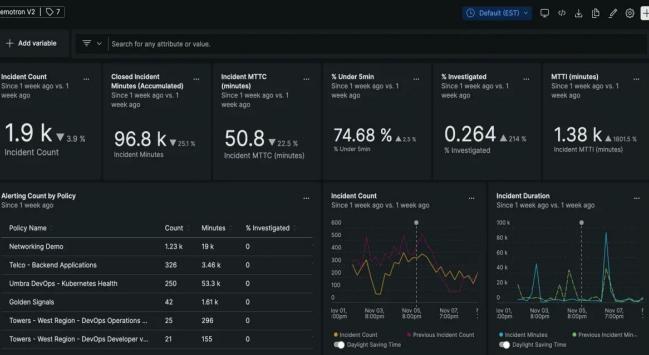
Improve Alert Maintenance

new relic

Alert Quality Management



- Strategies to focus on **reducing the number of nuisance incidents** so that you focus only on alerts with **true business impact**
- Ensure that **fewer, more valuable**, incidents are created for the right purpose
- Includes **strategies, best practice** and **tooling** for measuring and analysing **alert quality**



Improve Alert Maintenance

 new relic

Observability as Code



- Use graphQL (or Terraform) to **manage alerts programmatically**
- Allows for better **auditing** and **change control**
- Build workflows to **generate alerts automatically** from configuration



- Scale
- Stability
- Reusability
- Automation
- Compliance
- Security
- Innovation



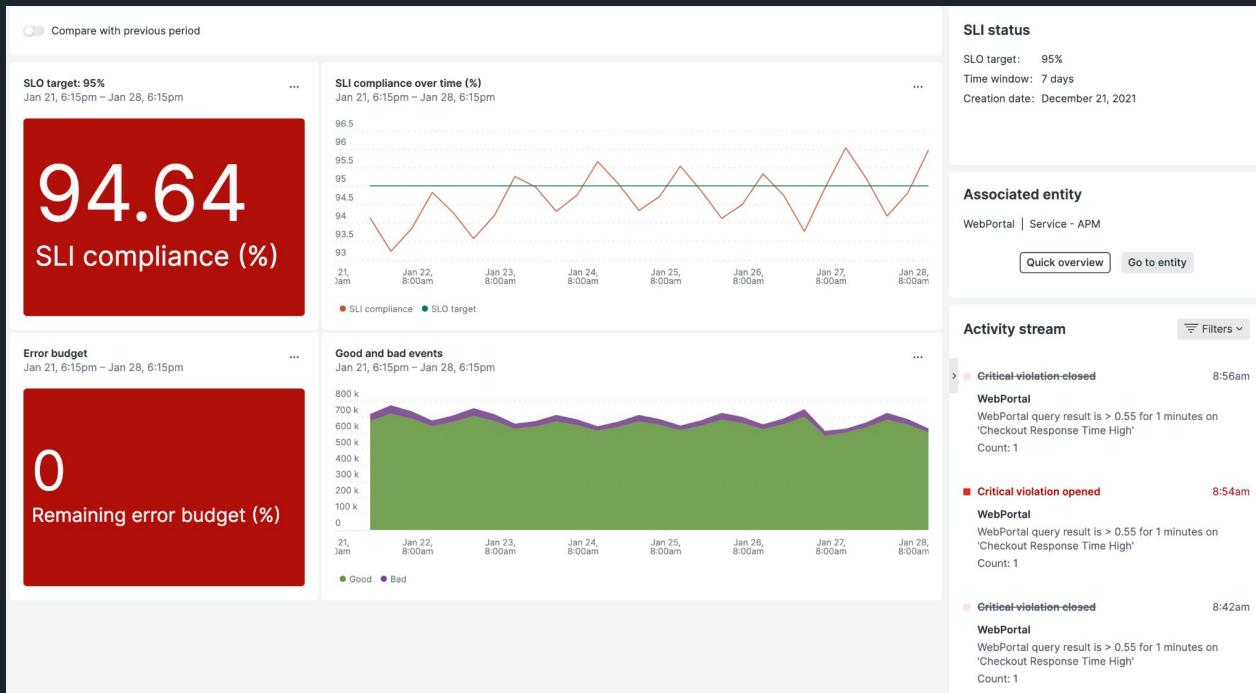
GraphQL

Improve Alert Maintenance

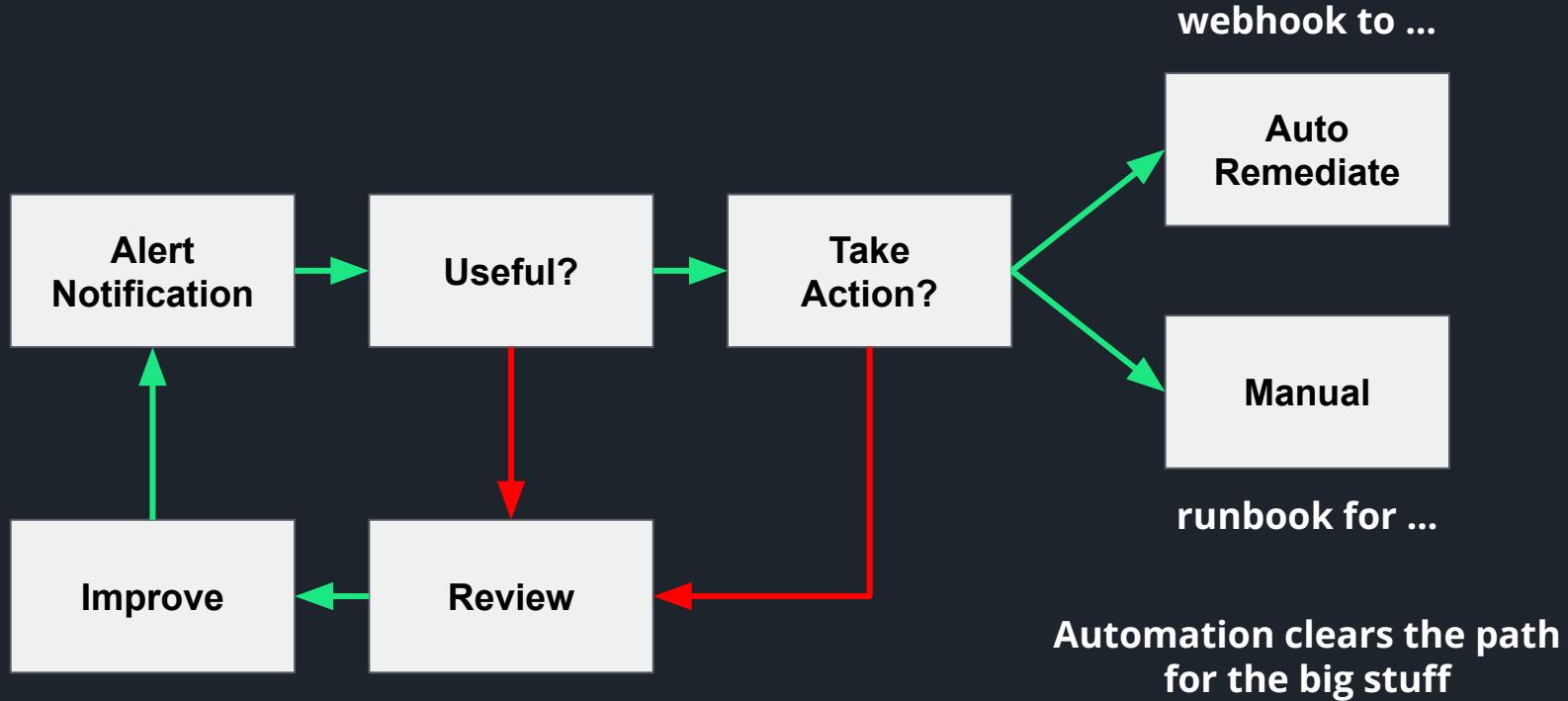
 new relic

Going Next Level

SRE based Alerts



End Goal - Alert Workflow



Insights - Standardization - Automation

```
Message
Secondary 1 error: serial comm error; (16) The directory cannot be removed.
Printer warning: printer not enabled
Reactor warning: reactor event loop (thread id=4294967295)...
NozzleInEvent error: hose 12 not valid
Application error: failed to get hose 0
Pump_ 1: state change from PriceChanging to SystemError: (7 -> 1)
Pump_ 5: Gilbarco Protocol: Data error received when sending preset limit
Pump_ 5: state change from SystemError to NotResponding: (1 -> 5)
Hose_ 7.0 warning: invalid state 3 for FuelNotFlowingEvent
Pump_ 2: error: failed to set current delivery
NozzleOutEvent error: hose 13.1 not valid
NozzleInEvent error: hose 13.1 not valid
Secondary 8 error: serial comm error; (1460) This operation returned because the timeout period ex
Timer_ -1, CPump warning: StartTimer failed to acquire mutex
ObjectBackup warning: failed to backup object 102, CDeliveryStack (retries: 9)
Deserialze error: bad buffer alignment
Pump_ 5: delivery 11 error: delivery totals lost - clear required
Timer_ 19, CDelivery warning: 30000 ms delay failed to signal; signalling now...
Pump_ 7: delivery 78 error: Preauth overrun, limit 80.00, total amount 80.23
Timer_ 5, CPump warning: 20000 ms delay timed out prematurely; rescheduling for 3601937 ms
Pump_ 5: error: unexpected PumpLocked event; state Authorizing aborted
ObjectStore error: invalid set at location 3088; deleted
ObjectStore error: failed to move file pointer, offset 1296, origin 0: file .../Journal/OBJBackup.obs not c
An error occurred processing -CompressedRegion
Pump_ 15: delivery 36 error: Preauth overrun, limit 80.00, total amount 85.43
```

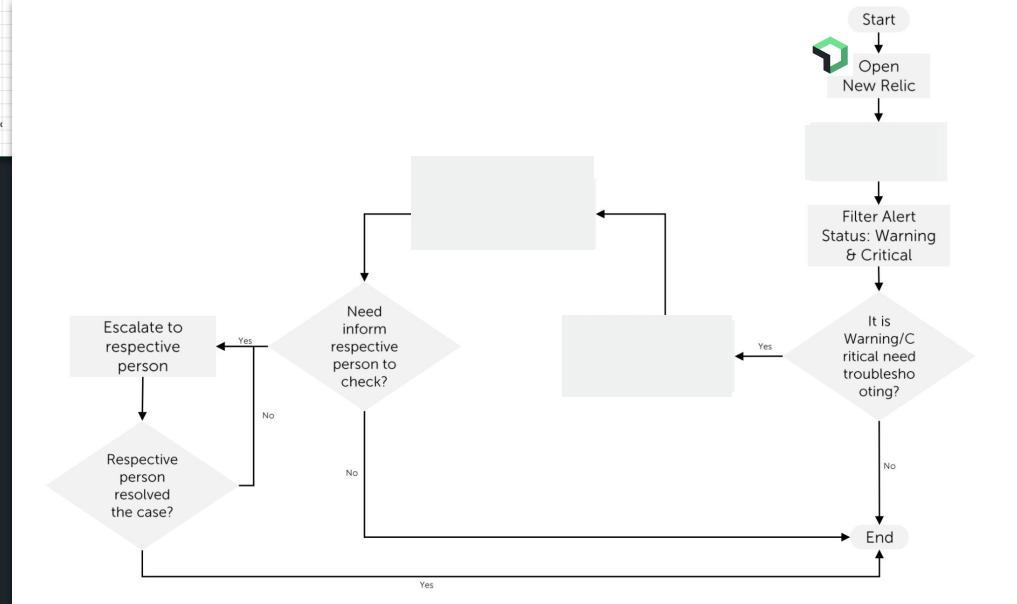
Logs

```
102: COM port removed
722: Printer is not enabled (expected)
538: Reactor watchdog timeout, many possible reasons.
179: Invalid nozzle ID event. May be caused by misconfiguration
127: Couldn't locate hose 0 object
58: Price change timed out
56: Dispenser did not accept the last multibyte command. If this is happening often it may indicate a dispenser communication issue and should be investigated further.
52: Dispenser is not responding
45: Requires additional context to identify the cause.
41: Requires additional context to identify the cause.
37: Couldn't locate hose 0 object
37: Couldn't locate hose 0 object
25: COM port removed
```

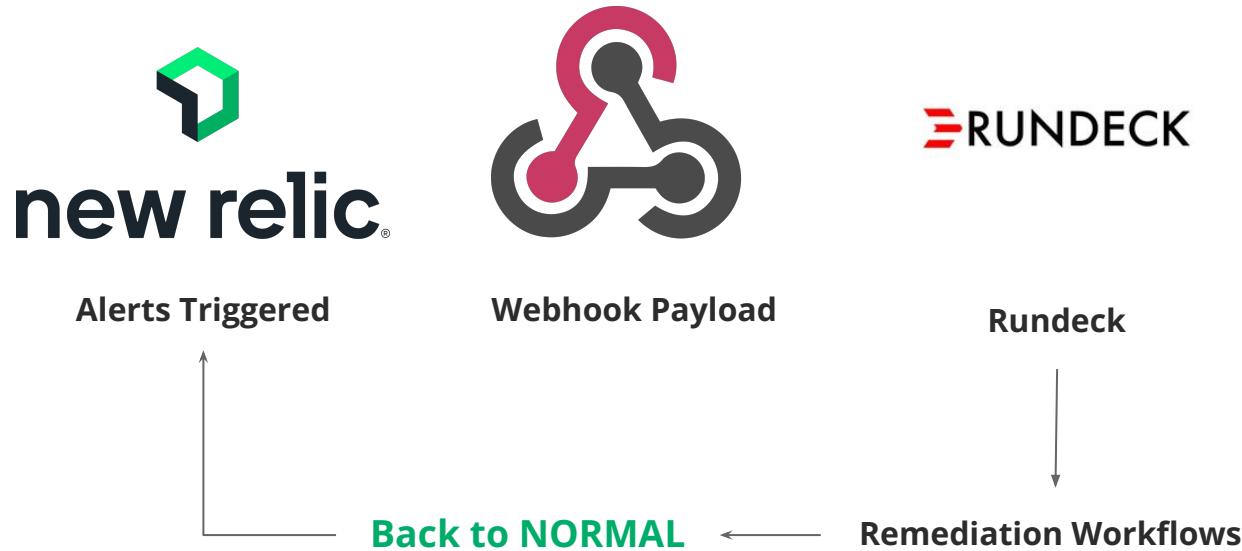


Match **PROBLEMS**,
with the right **WORKFLOW**

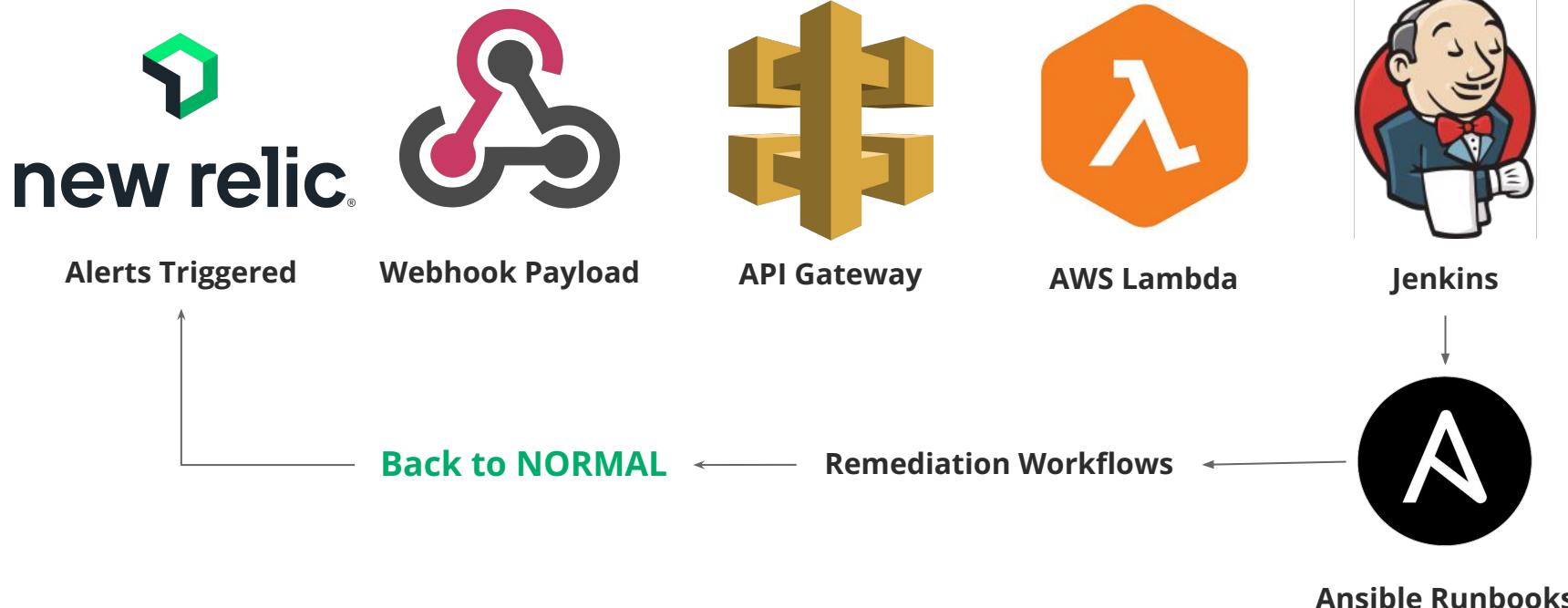
Once the right workflow is in
place, optimization is **EASY**



Examples - Self Remediation



Examples - Self Remediation



Alert Quality Management

Resources to help you get better

- [Alerts Best Practices](#)
- [Manage Your Alert Quality](#)
- [Alerting Concepts & Terms](#)
- [Issue Preference Options](#)
- [Anomaly Detection for Alerts](#)
- [Workflow Enrichment for Alerts](#)
- [Muting Rules](#)
- [Introduction to Terraform with New Relic](#)
- [New Relic Terraform Provider](#)
- [Hands On Lab with AQM](#)



You can fix Alert Storm & Fatigue!