10 Ways to Get the Most Out of New Relic Alerts

1

Define alert policies

Your alert policies define the conditions for when you or your team get notified of an event violating the thresholds you select. An alert policy can apply to one or more New Relic products. It can also contain one or more alert conditions and one or more notification channels. When designing your alert policies, consider:

- The parts of your infrastructure that need personnel to be responsible for them
- The individuals who are responsible for one or more parts of your infrastructure

2

Define alert conditions

Create one or more conditions to identify what triggers an alert for your selected policy. Each condition applies to a specific New Relic product. For example, you can create a single alert policy with a condition for error rate thresholds for all apps monitored by New Relic APM, a second condition with a custom metric for selected apps monitored by New Relic APM, and a third condition with a CPU percentage threshold for servers monitored by New Relic Servers.

3

Use meaningful names

Make sure each alert policy and alert condition has a concise and meaningful name. This provides useful information in notification messages that have limited characters, such as email subject lines, chat, etc. This also helps make it easier to skim the index in the New Relic alerting user interface.

Alert policy name recommendations:

- Your group or team's name
- The set of resources or services the alert policy is targeting

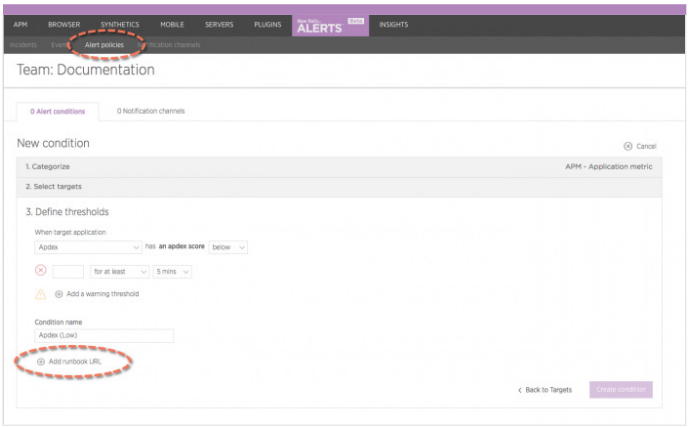
Alert condition recommendations:

- Use camel case or dotted decimal notation
- Describe the essence of what is being violated

4

Include a runbook URL

The alert policy's condition includes the option to include a Runbook URL. This is useful to provide information or standard procedures for handling an incident triggered when a situation violates the alert thresholds. The Runbook URL will appear in the **Incidents** dashboard details and in email notifications for the policy violation.



5

Define alert thresholds

Thresholds are the values and frequency that will trigger the alert when violated.

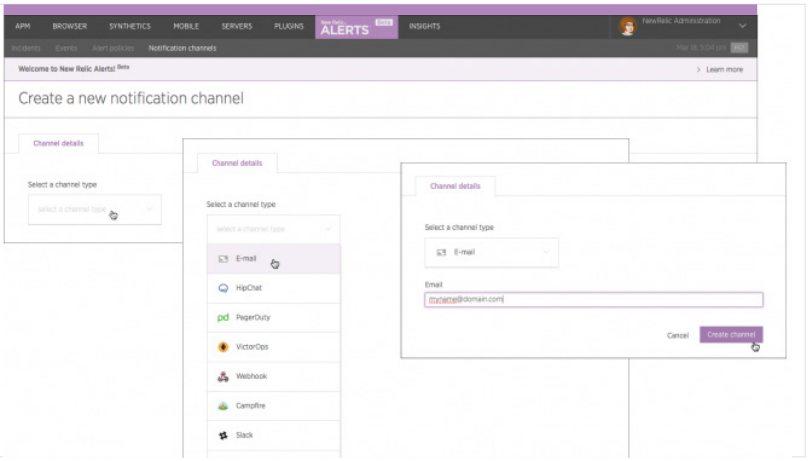
- For example, you can set an alert on web response time if any application has an average that is above the threshold of 5 seconds for at least the last 15 minutes.

Be sure to set your alerting thresholds when setting up policies and conditions.

6

Select notification channels

Notification channels are where alerts are sent when incidents are opened, acknowledged, or closed. Let the right people know when critical issues arise using channels your team already uses, such as Campfire, HipChat, OpsGenie, PagerDuty, Slack, VictorOps, as well as email and mobile push notifications to the New Relic iOS and Android app. You can set up several different channel types and one or more channels to any alert policy from the alerting interface. You can also control how the alert is delivered with custom payload webhooks.



7

Tailor notifications for different users

New Relic gives you the option to create notification channels and assign alert policies to them, and create alert policies and assign notification channels to them. This flexibility allows you to tailor who gets notified, using the method that is most useful to them. Avoid interrupting individuals who may ignore alerts that don't seem relevant to them. By tailoring notifications to the most useful channel and policy, you can help the right personnel receive and respond to incidents they care about in a systematic way.

8

Collect incident records

An incident is a window of time where one or more violations have occurred. It includes all of the open and close timestamps for each violation, as well as chart snapshots of the data being evaluated around the time of each violation. When an alert policy's condition violates a Critical (red) threshold, an incident record is created with detailed information to help you respond efficiently. To select when an incident is created and how violations are grouped, use the Incident preference setting inside your policy.

9

Specify how to roll up incident records

Choose one of three options for incident roll up, each with its own advantages.

- **By Policy (default):** A single incident is created for the selected policy and will accumulate all condition violations for every target into a single incident record.
- **By Condition:** A single incident is created for the selected condition. This is most useful when you want an individual incident record to focus on a specific condition. If the policy has multiple conditions, separate incident records for each condition will appear on your Incidents dashboards.
- **By Target and Condition:** This is the most granular level for creating incident records. This is useful, for example, when you want to monitor closely anything that is occurring anywhere across your infrastructure. An incident will appear on your Incidents dashboards for every violation that occurs within your policy.

10

Adjust your conditions over time

As you use New Relic products to help you optimize your entity's performance, tighten your alerts policy conditions to keep pace with your improved performance. If you're rolling out something that you know will negatively impact your performance for a period of time, loosen your threshold conditions to reduce alert noise.

Want more user tips?

Check out our Tutorials page.

Read the documentation.

Ask a question in the New Relic Community Forum.

New Relic.