Alerts

New Relic alerts are used to identify incidents or irregularities in your telemetry data and initiate workflows to resolve or notify staff about high-priority events

Alert Policies

Alert Policies are used to create alert conditions and define what combination of conditions constitute an issue. For example 95% CPU usage *and* high database latency together may constitute an issue, whereas either condition individually would not. A policy is made up of one or more Alert Conditions. You can also enable correlation as part of policy creation.

Creating Conditions

When creating a new condition, start by determining the source of the data that you will be looking at. You are able to select multiple monitoring sources for a condition. Once this has been done you will need to determine what metrics you are going to monitor. If using the guided mode, you can select either the **Golden Signals** or select from a set of prebuilt metrics.

Once the metric to monitor has been selected, then you will need to fine-tune the policy. This will adjust the data aggregation window, whether any gaps in data will be filled with calculated infill, and evaluation delays that might need to be configured, and whether the condition threshold is Static (predefined and fixed) or dynamic (adjusted based on data behaviour over time by New Relic). For streaming method, Event Flow is preferred for regularly reporting data, such as live reporting of data from a server. Event Timer is better suited for batched information such as data sent periodically by cloud providers.

Thresholds can be for either or both of Critical and Warning level, and a Lost Signal incident can also be configured to notify groups in the event that the monitoring signal is lost (such as a server going offline). Auto-closing of incidents can also be configured, which will automatically close an incident related to the triggered policy after a given period of time when the system has returned to baseline behaviour. Runbook URL's can also be added to provide direction to users on the steps to triage and possible remediate the issue in the event the alert is triggered.

If using New Relic Query Language (NRQL), instead of selecting the prebuilt metrics you are able to create a unique query for your dataset.

Incidents

An incident is a specific event where an alert policy's conditions have been crossed. They note the detail and state of the individual problems at the point the overall policy was triggered.

Issues

Issues are groups of one or more incidents. These determine when you are notified about incidents. Depending on the collection of incidents different actions can be initiated depending on the severity of the issue.

Decisions

Decisions are logical correlations of issues to reduce noise from multiple issues or incidents. If enabled, New Relic Incident Intelligence uses Decisions to evaluate whether existing issues can be correlated or grouped with newly created ones

Workflows

Workflows determine the notification process, including who is notified, which issues trigger a notification, and what information is included as part of the notification. Workflows allow both one-to-one and many-to-one relationships between issues and their destinations.

Configuring Workflows

When configuring a workflow using a Basic view, you are able to filter the workflow based on Tag, Policy or Priority. Using the Advanced view you can filter based on any criteria. Optionally you an also choose to add additional context data by including additional NRQL queries.

By default, notifications are sent when an issue is opened, acknowledged or closed. This can be adjusted in the workflow configuration settings

Destination

A destination is the end communication channel to people or services for issue notifications. Destinations are configured once and are then re-usable across Workflows on an individual account

---

Revision #1
Created 18 June 2025 21:24:22 by Sam
Updated 26 June 2025 05:23:26 by Sam