**Relic Alert – Configuration**

Relic Alerts is a flexible and centralized notification system that unlocks the operational potential of New Relic. With a single tool to manage alert policies and alert conditions, you can focus on the metrics you care about most. This includes:

* Applications monitored by New Relic APM
* Client-side metrics monitored by New Relic Browser
* NRQL queries from New Relic Insights
* Hosts monitored by New Relic Infrastructure
* New Relic Mobile apps, including external services
* Monitors from New Relic Synthetics
* Plugins created via New Relic Plugins

**Use New Relic Alerts to monitor your entire infrastructure**

New Relic Alerts provides a single, coordinated alerting tool across all of your New Relic products. This allows you to manage alert policies and conditions that focus on the metrics for entities that you care about the most, such as Docker containers, JVMs, and more.

**Workflow**

Good alerts are about notifying individuals or teams about changes in the systems for which they are responsible. With New Relic Alerts, you can follow an alert from the initial warning to its final resolution, and examine patterns to help avoid alertable situations in the future.

New Relic Alerts allows you to decide what are the best alerting scenarios for any situation. To help you get started, see New Relic's best practices for alert policies (defining policies based on your architecture or your staffing requirements, deciding how many alert policies and conditions you may need, selecting effective channels for alert notifications).

**Customize your alerting scenarios**

To customize your alerting scenarios, refer to New Relic's recommended best practices. Take into consideration:

* Why you want to be alerted (policy)
* What criteria will trigger an alert (conditions)
* When do your selected metric levels escalate into alerting situations (thresholds)
* Who needs to be notified about the situation, and how are they notified (channels)

**Give the alerting scenario a name (policies)**

When designing alert policies, refer to New Relic's recommended best practices. You can make alert policies as simple or as complex as your organization requires to address alerting requirements for:

* The parts of your organization and resources that need personnel to be responsible for them
* The individuals who are responsible for one or more parts of your architecture

Use New Relic's user interface to create policies for New Relic Alerts as applicable for your New Relic subscription.

**Identify criteria to trigger an alert (condition)**

Each alert policy can contain as many conditions as you need. An alert condition includes three components:

* New Relic product (APM, Browser, etc.) and type of condition (metric, external service, etc.)
* Entities that the policy targets, such as apps monitored by New Relic APM or New Relic Browser, hosts monitored by New Relic Infrastructure, etc.
* Thresholds that escalate into alerting situations with increasing severity

Use New Relic's user interface to create policy conditions for New Relic Alerts as applicable for your New Relic subscription.

**Set severity levels (thresholds) to escalate alerts**

Your alert condition defines escalating severity levels (thresholds) to trigger an alert, including a required **Critical** (red) level and an optional **Caution** or **Warning** (yellow) level. Thresholds for every alert condition include:

* What metric to monitor (Apdex, response time, CPU usage, custom metrics, etc.)
* What value it tracks (count, average, etc.)
* What time frame elapses before triggering an alert notification

The color-coded health status indicator in the user interface changes as the alerting threshold escalates or returns to normal. This allows you to monitor a situation through New Relic's UI before a **Critical** threshold passes, without needing to receive specific notifications about it.

For example, you can define a **Critical** (red) alert that notifies you when the error percentage for your app is above 10 percent at least once in any five minute period. You can also define an optional **Caution** or **Warning** (yellow) alert with different criteria.

Use New Relic's user interface to create thresholds for your policy conditions for New Relic Alerts as applicable for your New Relic subscription. You can also link to your runbook URL or other operating procedures, so your team knows exactly what to do when the threshold triggers an alert notification.

**Decide who is notified and how (channels)**

New Relic offers a variety of notification channels that you can tailor to each alerting situation. For example, you may want product team members to view alert notifications through a company HipChat room, but you want your Network Operations Center to monitor **Critical** (red) alerts through webhooks. This gives you the flexibility to decide not only who but how to be notified about alerting situations.

Use New Relic's user interface to add notification channels and personnel to your policies for New Relic Alerts as applicable for your New Relic subscription.

**View alert incident or event details**

After you set up one or more alert policies that define alert conditions for your New Relic product entities, New Relic monitors the conditions you have defined. Depending on the threshold level and notification channel, you will receive alert notifications.

You can also view the alert incident or event details directly from the New Relic user interface. For example, you can see the color-coded health status indicator for an affected app from the **Applications** index, and select details from the **Recent events**.

**Infrastructure and Alerts: Add, edit, or view host alert information**

To add a New Relic Infrastructure alert condition to a New Relic Alerts policy:

1. From infrastructure.newrelic.com  , select any of these Infrastructure pages: **Hosts**, **Processes**, **Network**, or **Storage**. Mouse over the chart you want to alert on, select the ellipses  icon, and then select **Create alert**.

OR

From infrastructure.newrelic.com  , select **Settings > Alerts**, then select **Create alert condition**.

1. Type a meaningful condition name.
2. Select the **Alert type**, or refer to the examples for additional help with which type to select.
3. Apply filter sets to identify the set of hosts (and any additional options for interfaces, processes, etc. as applicable) that you want the alert condition to apply to.
4. Define the **Critical** (required) and **Warning** (optional, if available) thresholds for triggering the alert notification.
5. Optional: To create the condition criteria proactively but not receive alert notifications at this time, turn off the **Enabled** checkbox option.
6. Select an existing policy for the new condition.

OR

Select the option to create a new policy and identify the email for alert notifications.

1. Optional: Add a runbook url.
2. Select **Create**.

**Create alert conditions for Infrastructure integrations**

To create an alert condition for your New Relic Infrastructure integrations, use any one of these options:

* From New Relic Alerts: Select **Alert policies > New alert policy > Create new condition** and select Infrastructure as the product. You can also do this by clicking on a pre-existing policy and selecting **Add a condition**.
* From New Relic Infrastructure: Select the **Integrations** page, then select **Create alert** for any integration.
* From New Relic Insights: To create an alert condition while viewing your integration data on your dashboard, select **Create alert** beneath the integration description.

**View host alert events**

New Relic account can view New Relic Infrastructure alert incidents and individual violations through the user interface.

1. From infrastructure.newrelic.com  , select **Events**.
2. To change the hosts or time frame, use the search window, **Filter set**, or **Time** functions.
3. From the **Events** list, select the alert violation.
4. To view detailed information in New Relic Alerts about the selected violation, select the link.

**Update or delete host alert information**

To edit, disable (or re-enable), or delete host alert information:

1. From infrastructure.newrelic.com  , select **Settings > Alerts**.
2. Optional: Use the search window or **Select all** checkbox to locate one or more alert conditions.
3. Select any of the available functions to  edit, disable, enable, or  delete the selected conditions.

| **Alert features** | **Features in New Relic Infrastructure** |
| --- | --- |
| Alert policy conditions | * Create: Use the New Relic Infrastructure UI. * View, change, disable (or re-enable), or delete: Use the Infrastructure **Settings > Alerts** UI. |
| Information on alerts | * View summary information about events: Use the Infrastructure **Events** UI. * View detailed information about alert incidents or individual violations: Use the New Relic Alerts UI or the notification channelintegrated with the associated policy. |
| Alert policies | View, add, change, disable, or delete:   * For policies with a variety of notification channels: Use the New Relic Alerts UI. * For policies only needing email notifications: When adding a condition from the New Relic Infrastructure UI: From **Infrastructure > Settings > Alerts**, select **Create a new policy**, and add one or more email addresses as needed.   Add host conditions to an existing policy: Use the Infrastructure UI. |
| Notification channels | To view, add, change, or delete available notification options:   1. From infrastructure.newrelic.com  , select **Settings > Alerts**. 2. Optional: Search for the condition or policy name. 3. From the list of conditions, select the policy link to view notification channel information in the New Relic Alerts UI. |

**Alert conditions that generate too-long NRQL queries**

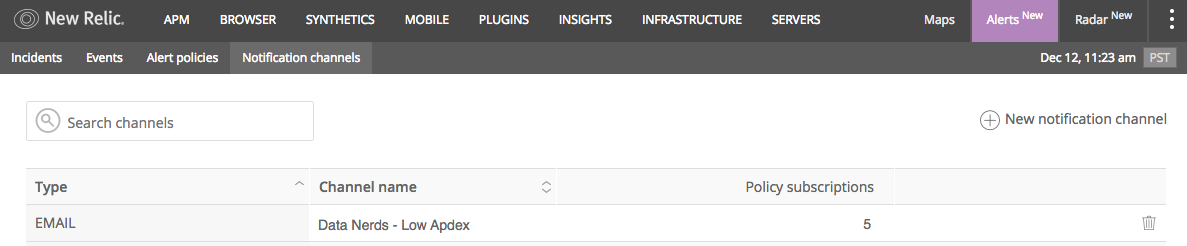
Alert conditions created in Infrastructure rely on behind-the-scenes NRQL queries, and NRQL queries have a 4096-character limit. This means that if your alert generates a very complex NRQL query that filters on many elements (for example, including many hosts, or many tags), it will exceed this limit and display an error message saying that the condition failed.

The solution to this problem is to reduce the number of elements you are using in your alert condition. For example, if you entered a large number of hosts that caused the condition to fail, you could reduce the number of hosts. Other solutions include:

* Reform your alert condition to target specific attributes that apply to the entities you're trying to target.
* Create custom attributes for the entities you want to target, and use those attributes in your alert condition.
* Use substrings to target hosts. For example: instead of targeting prod-host-01, prod-host-02 and prod-host-03, just target all hosts with prod-host-0 in the name.

**Create channels**

You can set up several different channel types and one or more channels for any alert policy from the New Relic Alerts user interface. You can also use custom payload webhooks to control how the alert is delivered.

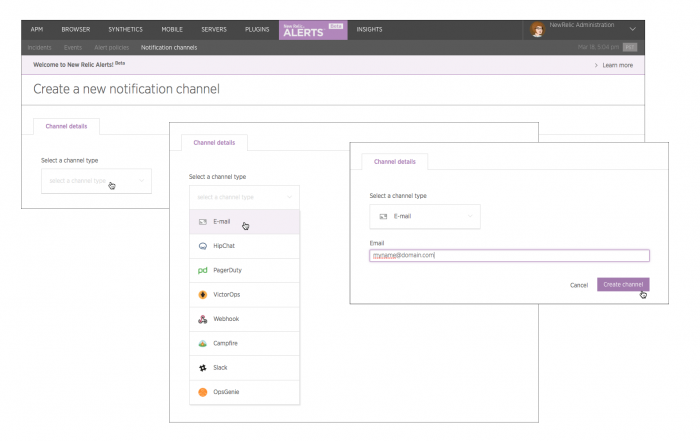


**alerts.newrelic.com  > Notification channels:** The **Notification channels** index lists existing notification channels. From here you can create and test new notification channels, search for and sort existing channels, update and add policies to them, or delete channels.

To create a notification channel in New Relic Alerts:

1. From **alerts.newrelic.com**  , select **Notification channels**.
2. Select  **New notification channel**.
3. From **Channel details**, select the type of channel.
4. Enter the required information for your selected channel type.
5. Select **Create channel**.
6. Optional: Select  **Send a test notification**.
7. Add the notification channel to one or more alert policies.

The **Alert policies** page includes the option to add notification channels directly to the selected policy.



Instructions for specific notification channels

New Relic Alerts supports these types of destinations as notification channels for alerts. New Relic's user interface also lists the available notification channel types.

**Show All**

**User**

**Email**

**HipChat Cloud**

**OpsGenie**

**PagerDuty**

**Slack**

**VictorOps**

**Webhook**

**xMatters**

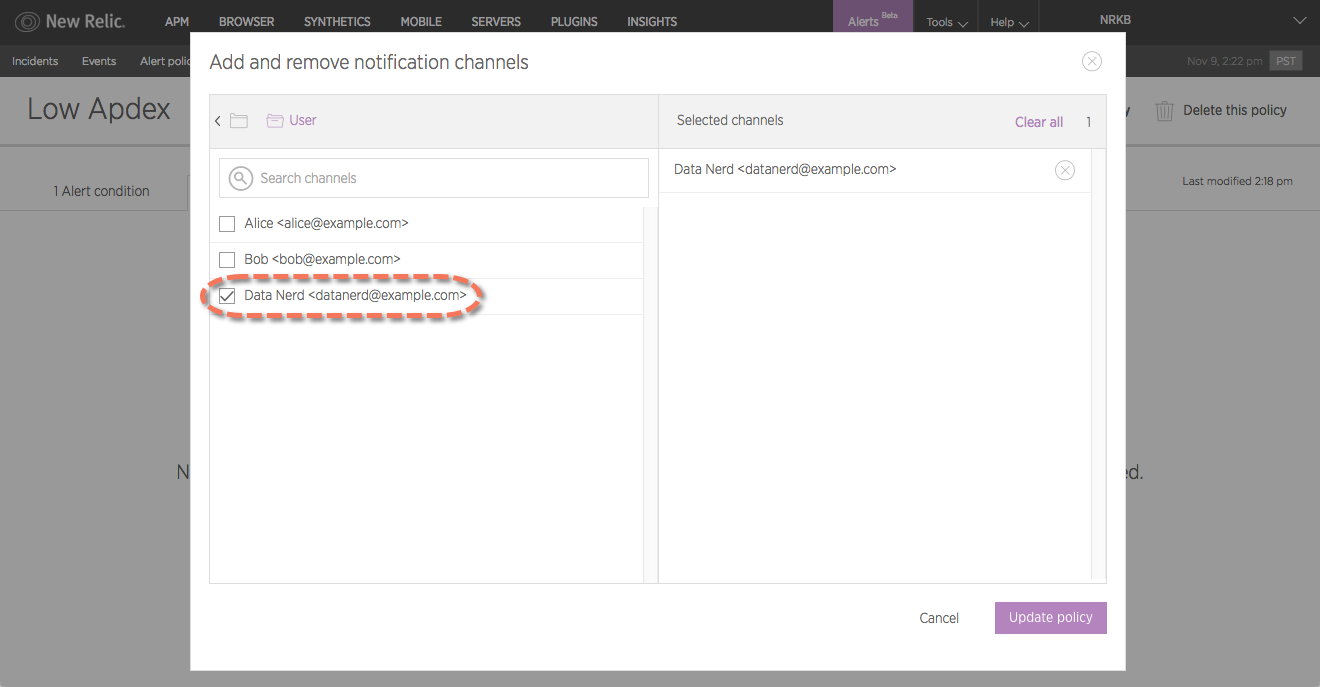
**Campfire**

Receive mobile push notifications

In order to receive mobile push notifications, your device must be registered and listed in **(account) > User preferences**. If the device is not listed in **User preferences**, log out of the app, log back in, and check again to see if it is listed.

To receive mobile push notifications:

1. Log in to your New Relic account via the mobile app at least once to ensure the device is registered.
2. Add the user channel to the alert policy.
3. Switch push notifications **On** for the device.



**alerts.newrelic.com  > Alert policies > (selected policy) > Notification channels > Add notification channels > User**: To receive push notifications on your mobile device, select your username from the list.

Acknowledge alert notifications

Anyone in your account can acknowledge alert notifications through the New Relic Alerts user interface or through their email notification. The ability to acknowledge alert notifications from other channels (ack back) is a planned enhancement for a future release.