



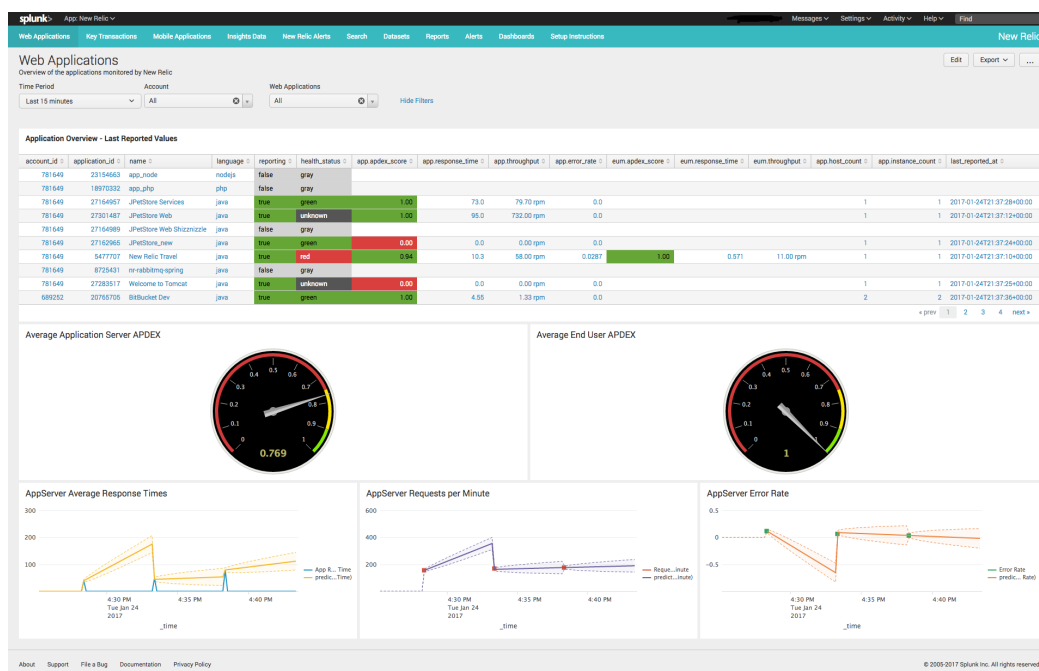
Splunk and New Relic: Better Together

With applications front-and-center of many enterprises' digital transformation, thousands of Splunk customers around the globe use Splunk to collect, index and analyze their machine data so they can prevent application failures and troubleshoot problems quickly when they occur. Many of those same Splunk customers are also using New Relic to provide in-depth code-level visibility into applications. Combined, the integration of Splunk and New Relic provides a COMPLETE view of how your applications are performing and enables you to [take a platform approach to application management](#).

Overview

The Splunk App and Add-on for New Relic use New Relic's REST APIs to gather data from the applications you are monitoring. This data can then be combined with all your other machine data in Splunk (wire data, log data, server data, and other infrastructure sources) to provide a complete picture of your applications' performance.

Install the Add-on, supply your New Relic account number and API Key and you will have access to metrics for your web applications, mobile applications, key transactions and policy violations right inside of Splunk. Install the App to access a comprehensive set of visualizations within Splunk. This application provides a set of dashboards and takes advantage of Splunk's built-in machine learning algorithms to predict future values of metrics providing the ability to forecast potential problems BEFORE they occur. APM is a great source of data for your IT Troubleshooting and Monitoring needs and this application will enable you to easily correlate your New Relic data with all other data sources ingested in Splunk.



What you will need

- Splunk Add-on for New Relic
- Splunk App for New Relic
- New Relic Account Number
- New Relic APM API Key
- (Optional) New Relic Insights API Key

Installation

The installation consists on 2 steps; installing the Splunk Add-on for New Relic and the Splunk App for New Relic. The Add-on is responsible for executing the rest calls, collecting the data from New Relic and indexing it into Splunk. The App provides the dashboards and saved searches.

To install navigate to Apps → Manage Apps and select the “Install app from File” button. Specify the location of the file you downloaded and install. Repeat this process for both the App as well as the Add-On.

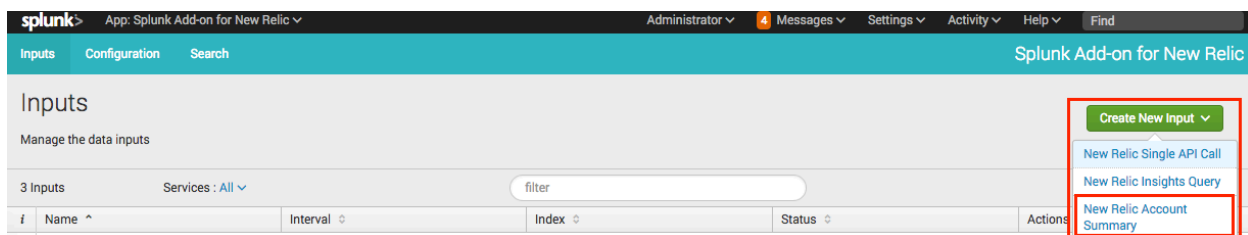
Configuration

The Splunk Add-on for New Relic contains three separate input types for New Relic data:

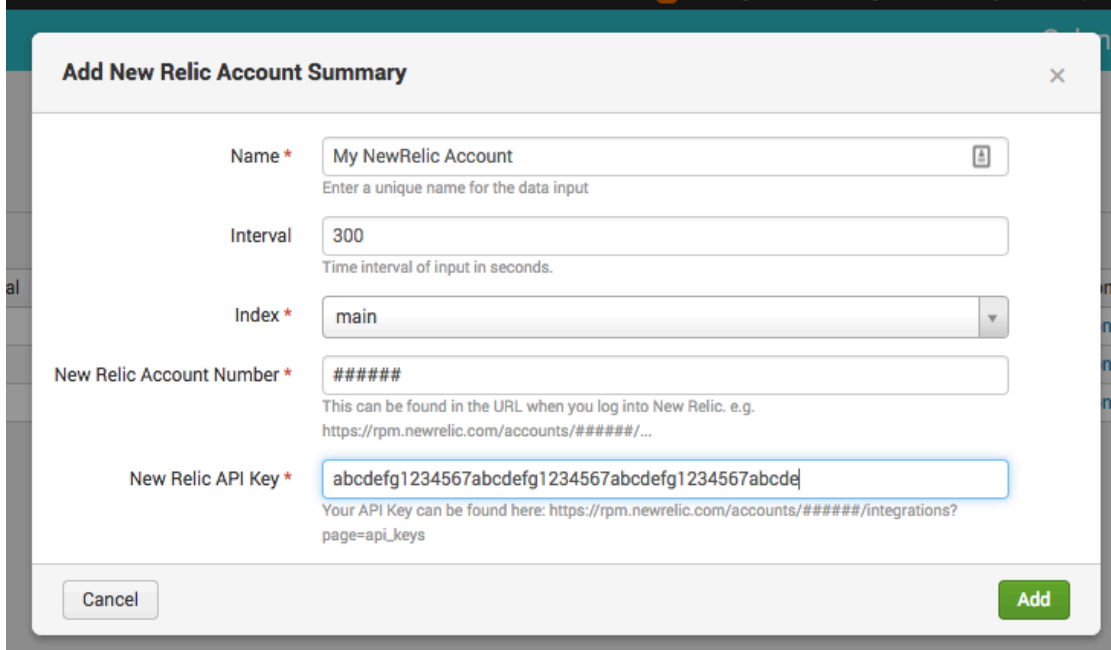
- Account Summary
- Single API Call
- Insights Query

In most cases you will only need to use the New Relic Account Summary input. For each New Relic account that you have, you will enter your New Relic Account Number and API Key and the Input will gather data for your applications, key transactions, mobile applications, alert policy violations.

To begin click the “Configure New Input” button and select “New Relic Account Summary”.



Enter your account details as follows:



Now visit the Splunk App for New Relic and see your New Relic data! Or you can now start searching using `sourcetype="newrelic_account"`

Note: Your API Key can be found in your New Relic account here:

https://rpm.newrelic.com/accounts/<account_number>/integrations?page=api_keys

Additional Inputs: New Relic Single API Call

In some cases, you may not want all of the Account Summary data for a given account. In these cases, or in cases where you may need to execute a different New Relic API call you can use the New Relic Single API Call input type.

Use the New Relic API Explorer (<https://rpm.newrelic.com/api/explore>) to identify the URL and any associated parameters required for your API call. Once you have identified the URL and parameters you'll need to enter those for your new input.

Click the "Configure New Input" button and select "New Relic Single API Call" and follow the prompts. Now start searching using `sourcetype="new_relic_single_api_call"`

Additional Inputs: New Relic Insights

New Relic Insights has a separate REST API and requires a separate Insights 'API Key'.

You can find and create Insights QUERY API Keys here:

https://insights.newrelic.com/accounts/<account_number>manage/api_keys

Once you have identified a New Relic Insights query that you would like run, you'll need to copy that query and paste it into your new input. Add a separate Input for each NRQL query you would like to execute.

Click the "Configure New Input" button and select "New Relic Insights Query".

Enter the following:

- Name your Query
- Enter your New Relic Insights Query API Key
- Enter your New Relic Account Number
- Enter the NRQL query you would like to execute

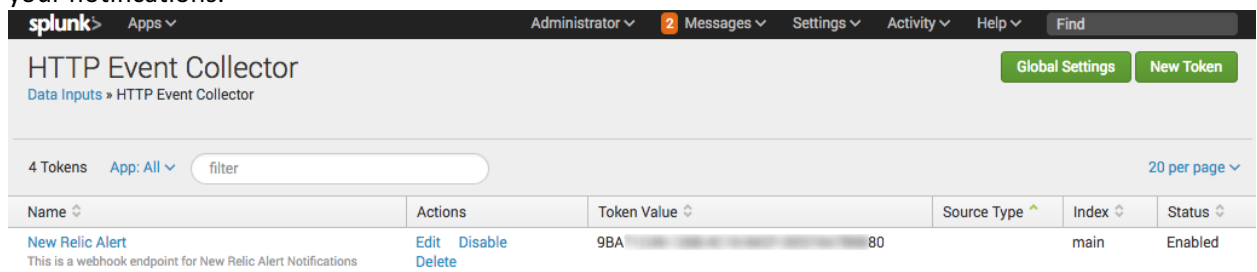
Now start searching using `sourcetype="newrelic_insights"`

Sending New Relic Alerts to Splunk

If you would like to go a step further and have New Relic send Splunk Notifications when Alerts are triggered, you will need to setup 2 components; a Splunk HTTP Event Collector (HEC) endpoint and a New Relic Webhook.

To setup the Splunk HEC endpoint follow these instructions:

1. Create a New HTTP Event Collector (HEC) Token to accept the Webhook from New Relic Settings --> HTTP Event Collector --> New Token
2. Be sure to provide a source value of `"newrelic_alert"` so that the dashboards will see your notifications.



Name	Actions	Token Value	Source Type	Index	Status
New Relic Alert <small>This is a webhook endpoint for New Relic Alert Notifications</small>	Edit Disable Delete	9BA...80	main	main	Enabled

Please make a note of the Token Value created here. You will need this to setup a WebHook in New Relic.

Next we'll need to configure a "Notification Channel" in the Alerts section of New Relic. Alerts can be found here: https://alerts.newrelic.com/accounts/<account_number>channels



When creating the Notification Channel keep the following in mind:

3. Use Splunk HEC Token Value (from step 1 above) as both the Channel ID and the Authorization parameter
4. The Base URL should be:
`https://<your Splunk Server>:8088/services/collector/raw?channel=<HEC Token>`
5. Create a new "Custom Parameter" Named Authorization with a value of Splunk <HEC Token>

Add this Notification Channel to your existing Alert Policies in New Relic and you're all set!

When New Relic triggers a policy violation, it will be automatically sent to Splunk.

Here's a completed example:

The screenshot shows the New Relic interface for configuring a Notification Channel. The top navigation bar includes links for APM, BROWSER, SYNTHETICS, MOBILE, PLUGINS, INSIGHTS, INFRASTRUCTURE, SERVERS, and Alerts (New). The left sidebar shows Incidents, Events, Alert policies, and Notification channels. The main content area is titled "Splunk HEC Endpoint". Below the title, there are two tabs: "Channel details" (active) and "Alert policies". The "Channel details" tab contains the following sections:

- Webhook**
 - Channel name:** Splunk HEC Endpoint
 - Base Url:** `http://t[redacted]:8088/services/collector/raw?channel=9B[redacted]9880`
- Basic Auth**
 - + Add basic auth
- Custom Headers**

Name	Value
Authorization	Splunk 9l[redacted]A7B9880

 - + Add custom headers