New Relic APM Best Practices

10 Application Monitoring Tips You Need To Know

It's one thing to know how to use New Relic APM, but it's another thing to know how to use New Relic's application performance monitoring software well. Here are 10 best practices designed to help you become a New Relic APM master—and a key asset to your team!

1 Standardize application-naming conventions

Most New Relic agents provide a default application name, such as "My Application" or "PHP Application," if you don't specify one in your New Relic configuration file. You don't want to end up with 20 identically named applications, so always be sure to select a descriptive identifier for your apps as soon you deploy them. To keep things consistent and easy to navigate, New Relic recommends standardizing your application naming (e.g. all apps in Staging append [Staging] or the like at the end of their names.) Ideally, you want your new Java applications to be named automatically to reduce the chances of typographical errors and misnaming.

HOW TO DO IT:

1. For Java applications, automatic application naming can come from the following sources:
   - Request attribute
   - Servlet init parameter
   - Filter init parameter
   - Web app context parameter
   - Web app context name (display name)
   - Web app context path

   Choose the method that best fits your needs and follow these steps.

2. For non-Java applications, there are no automatic naming methods so refer to the documentation for your agent.

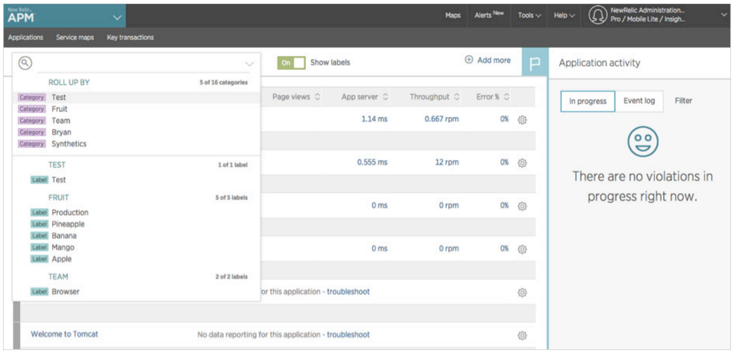
2 Add labels to your applications

When several different applications use the same account, and each application spans multiple environments (for example, development, test, pre-production, production), it can be hard to find a specific application in your overview dashboard. That's why we recommend adding labels to your apps so that you can segment them into logical groups. The two most common labels that mature APM customers use are application name and environment. So, for example, if you wanted to view the billing application in Test, you could simply filter by "billing app" (name label) and "test" (environment label).

New Relic APM is designed so that account owners and admins can label apps to "roll up" into an unlimited number of meaningful categories. You can also easily sort, filter, and page through all applications on your account's Applications list.

HOW TO DO IT:

1. From the New Relic APM menu bar, select **Applications**.
2. From the Applications index, select **Show Labels > On**.
3. To assign an app to a category, select the circled plus icon by its name.
4. Follow the guidelines to type the label; use the format Category:Value.
5. To save the new label, press **Enter** or **Return**.



No data reporting for this application - troubleshoot

There are no violations in progress right now.

3 Create and evaluate alert policies

When key performance indicators spike or drop, individuals and teams in your organization need to be notified. Alerting in New Relic provides a set of tools including dynamic baselines that allow you to detect problems before they impact your end users.

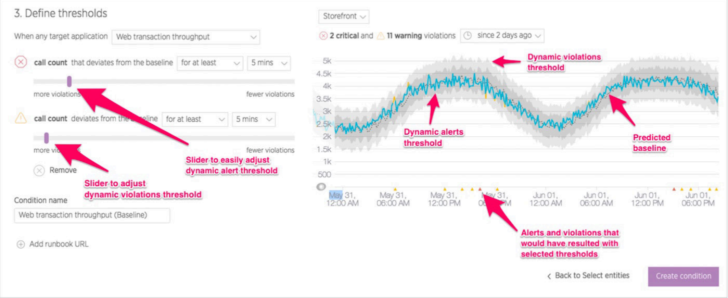
Alert policies can be set up in two primary ways:

- **Static threshold alerts** are great when you already know the nature of an application and its normal behaviors aren't likely to change anytime soon. Apdex score, response time, error rate, throughput are some of the static thresholds you can create alert policies on.
- **Dynamic baseline alerts** make it easy to determine and set dynamic alert thresholds for applications with varying seasonal patterns and growth trends (which make it difficult to set thresholds that define normal behavior). These alerts use baselines modeled from your application's historical metric data.

Each alert policy can contain as many conditions as you need, and each alert condition includes three components:

- Type of condition (metric, external service, and so on)
- Entities that the policy targets (for example, apps monitored by New Relic APM or New Relic Browser, hosts monitored by New Relic Infrastructure, and so on)
- Thresholds that escalate into alerting situations with increasing severity

Once you have your alerting set up, you then want to make sure you're taking advantage of all viable notification channels. After all, what good are alerts if no one knows about them? You can manage alerts by creating specific user groups and by leveraging New Relic's integrated alert channels, including HipChat, JIRA, PagerDuty, Campfire, Webhook, and email. Be sure to evaluate alert policies on a regular basis to ensure that they are always valid.



3. Define thresholds

When any target application: Web transaction throughput

call count that deviates from the baseline for at least 5 mins

call count deviates from the baseline for at least 5 mins

Condition name: Web transaction throughput (Baseline)

HOW TO DO IT:

To set up dynamic baseline alerts:

1. To select the Dynamic Baseline Alerts capability and choose an application, go here. You will see a preview of the metric with the predicted baseline.
2. From the drop-down menu, you can select a metric for that application and see the corresponding baseline.
3. Using the threshold sliders, you can then set how closely you want your threshold to follow the baseline prediction.

To set up static threshold alerts:

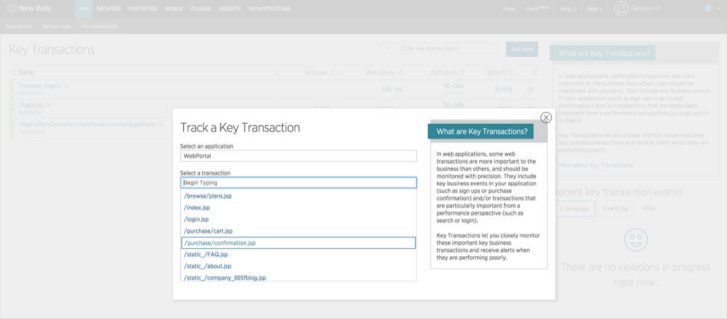
1. To change your Apdex settings, go here.
2. To set up your alert notification channels, go here.

4 Identify and set up key transactions

Depending on the nature of your application, some transactions may be more important to you than others. New Relic's key transactions feature is designed to help you closely monitor what you consider to be your app's most business-critical transactions—whether that's end-user or app response time, call counts, error rates, or something else. You can also set alert threshold levels for notifications when your key transactions are performing poorly.

HOW TO DO IT:

1. From the New Relic APM or New Relic Browser menu bar, select **Key transactions**, and select **Add more**. Then select the app and web transaction. OR from the selected transaction, select **Track as key transaction**.
2. Type a name for the key transaction, and select **Track key transaction**.
3. *Optional:* If the agent for the selected app supports custom alerting, use the default values that New Relic automatically fills, or select **Edit key alert transaction policy** to set the Apdex and alert threshold values.
4. To view the key transactions dashboard details, select **View new key transaction**.



Track a Key Transaction

Select an application: WebPortal

Select a transaction: Begin Typing

/browse/plans.jsp
/index.jsp
/login.jsp
/purchase/cart.jsp
/purchase/confirmation.jsp
/static_/FAQ.jsp
/static_/about.jsp
/static_/company_005fblog.jsp

What are Key Transactions?

In web applications, some web transactions are more important to the business than others, and should be monitored with precision. They include key business events in your application (such as sign ups or purchase confirmation) and/or transactions that are particularly important from a performance perspective (such as search or login).

Key Transactions let you closely monitor these important key business transactions and receive alerts when they are performing poorly.

5 Track deployment history

When development teams are pushing new code out as frequently as possible, it can be hard to measure the impact that each deployment is having on performance. One way to stay in tune with how these changes are affecting your application is via deployment reports. These reports list recent deployments and their impact on end-users and app servers' Apdex scores, along with response times, throughput, and errors. You can also view and drill down into the details to catch errors related to recent deployments, or file a ticket and share details with your team.

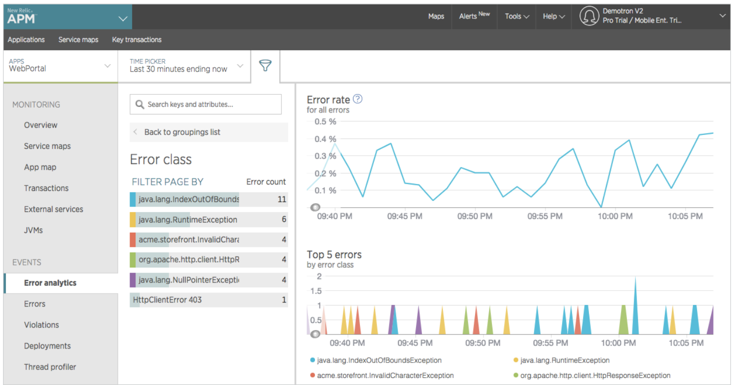
HOW TO DO IT:

1. To view the Deployments dashboard, from the New Relic menu bar, select **APM > (selected app) > Events > Deployments**.
2. To view performance after a deployment, go to the selected app's Overview dashboard in the **Recent events** section. Keep in mind that a blue vertical bar on a chart indicates a deployment. To view summary information about the deployment, point to the blue bar.

6 Start troubleshooting errors using error analytics

The New Relic APM error analytics feature gives you useful tools to analyze and resolve errors being reported by your applications, so you can immediately see where to focus your attention. DevOps teams can:

- Assess the health of applications with fine-grained data on error events over the past eight days.
- Select any parameter to group or filter errors shown; for example, error class, error message, host, transaction name, etc.
- Drill down into stack trace details to diagnose and resolve specific errors.
- Identify continuing trends in error rates for periods longer than eight days.
- Use links to share error data through New Relic Insights dashboards or through your organization's ticketing system to coordinate and resolve errors more quickly.



Error class

FILTER PAGE BY	Error count
java.lang.IndexOutOfBounds	11
java.lang.RuntimeException	6
acme.storefront.InvalidChara	4
org.apache.http.client.HttpR	4
java.lang.NullPointerExcepti	4
HttpClientError 403	1

HOW TO DO IT:

1. Start with the Error rate chart to see at a glance where there are unexpected spikes, dips or patterns in general.
2. Correlate general patterns on the Top 5 errors chart to alerts occurring during the same time period. Use groups and filters to examine the error events and attributes in more detail, and look for patterns with error messages or transaction names.
3. Explore and share Error trace table information, including specific stack trace details: associated host, user, framework code, customer attributes, etc.
4. Identify error patterns on the Error frequency heatmap for a selected grouping (host, error message, custom attributes, etc) within a time range.

7 Leverage New Relic's reporting capabilities

From SLA, deployment, and capacity to scalability, host usage reports, and more, New Relic APM offers a variety of downloadable reporting tools surfacing historical trends—all great ways to report to senior executive teams or customers. Take a look at the full list of reports and use them to your advantage.

HOW TO DO IT:

1. To view a report, from the New Relic APM menu bar, select **Applications > (selected app) > Reports**.
2. Select the report you'd like to see.
3. If you want to save or export a report to share, select **Download this report as .csv**, which will create a report with comma-separated values.

8 Look at your environment holistically

With service maps

Use New Relic service maps, a feature included in APM, to understand how apps and services in your architecture connect and talk to each other. Service maps are visual, customizable representations of your application architecture. Maps automatically show you your app's connections and dependencies, including databases and external services. Health indicators and performance metrics show you the current operational status for every part of your architecture.

HOW TO DO IT:

1. To access service maps, go to rpm.newrelic.com/apm > **Service maps.**
2. Name your map.
3. Rearrange, group, or add nodes on the map as needed.

With New Relic Insights

Offering a unified, end-to-end view, New Relic Insights lets you chart and query all your APM data, both the metric and event data the agent reports, alongside data any other New Relic agents report. It's all available in Insights out-of-the-box, from the time any of the agents, including APM, start reporting data to New Relic. You can extend your reported event data, with custom attributes and custom events for even more dimension to segment your data. You can also send third-party data to Insights.

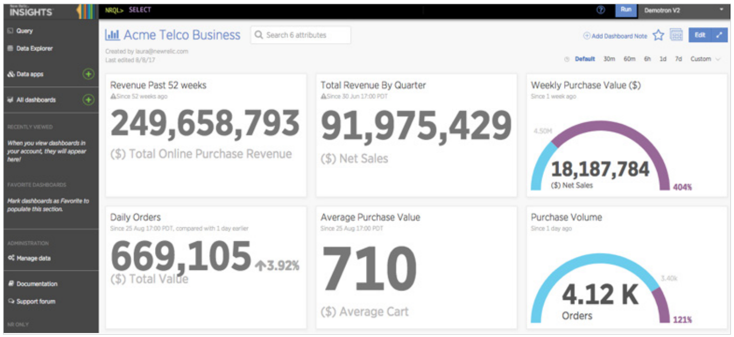
Use the data explorer to quickly browse your data taxonomy and add-to-insights to start adding charts from New Relic APM to a custom dashboard with a few clicks.

During an incident, open Insights and quickly ask a series of questions about your system with the New Relic Query Language (NRQL). For example, you can:

- Show web and mobile application information, server information, custom metric data, and plugin metric data all on a single dashboard interface.
- Create dashboards that present charts and tables with a uniform size and arrangement on a grid.
- Select existing New Relic charts for your dashboard, or create your own charts and tables.

HOW TO DO IT:

1. From the New Relic menu bar, select **Dashboards > Create Insights dashboard**.
2. Type the dashboard's title, or keep the default name.
3. *Optional:* To create a dashboard with the selected application data only, select the **Legacy mode** checkbox.
4. Select the layout (Overview or Grid), and select **Create**.
5. Reuse this user flow to add additional charts, tables, and data to your dashboard.



9 Keep your agents current

With New Relic's SaaS platform, getting new features is as easy as updating your agent. Most likely your organization already has a set of scripts for deploying application upgrades into your environment. In a similar fashion, you can also automate your New Relic agent deployment to ensure that your systems are up to date. Both Puppet and Chef scripts are great examples of deployment frameworks that make life easier by allowing you to automate your entire deployment and management process.

HOW TO DO IT:

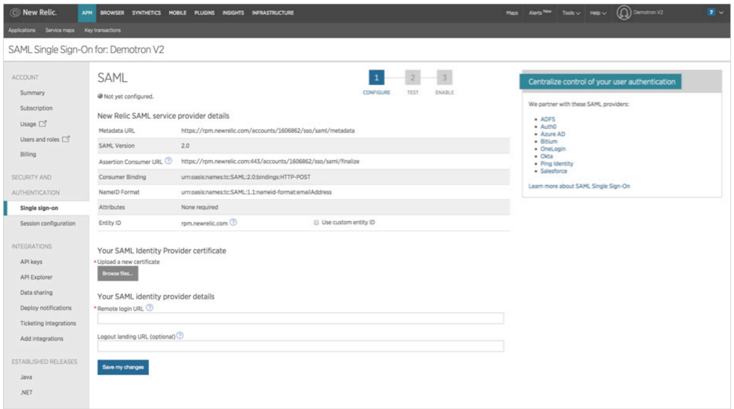
1. Regularly review which version of the agent you're using so that you know when an update is needed. If the latest agent release contains a needed fix or added functionality, download it.
2. To deploy the agent manually:
   - Back up the current agent directory.
   - Deploy the updated agent into the existing agent directory.
   - Modify configuration files by comparing new files with existing files. In particular, make sure things like license key and custom extensions are copied over to the new configuration.
   - Restart the application.
   - If problems arise, restore the old agent using the backup and restart.
3. To deploy the agent automatically **(preferred as a method to avoid errors)**, you can either:
   - Use existing deployment scripts, provided by they can be adapted to handle the deployment.
   - Create and maintain a script that specifically deploys and configures the New Relic agent. Ideally, the script would pull the agent files from a repository where the files are versioned (for rollback purposes). Once the script has been created:
     a. Shut down the application (unless script handles this).
     b. Run the deployment script.
     c. Start the application (unless script handles this).
     d. If problems arise, run the script to roll back to the previous version.

10 Enable role-based access (RBAC) and single sign-on (SSO)

Security is no doubt of utmost concern to your organization. To simplify password management for your employees and strengthen security, you may already be using SSO with your other systems. You should do the same with New Relic. Using New Relic's SSO integration feature, account administrators will be able to enforce strong passwords and restrict login via a corporate authentication mechanism. This way, New Relic users who have already authenticated using a corporate SSO system will be able to bypass the New Relic login prompt.

HOW TO DO IT:

1. Log in to New Relic as an admin and go to the SSO configuration page. From the New Relic title bar, select **(your account name) > Account Settings > Integrations > Single Sign On**.
2. From the SAML Single Sign On page, review your New Relic SAML Service Provider details.
3. To upload your SAML Identity Provider certificate, select **Choose File**, and then follow standard procedures to select and save the file.
4. Copy and paste in (or type) the Remove login URL that your users will use for Single Sign-On.
5. If your organization's SAML integration provides a redirect URL for logout, copy and paste in (or type) the **Logout landing URL**; otherwise leave blank.
6. Save, test, and enable.



SAML Single Sign-On for: Demotron V2

SAML

● Not yet configured.

New Relic SAML service provider details

Metadata URL	https://rpm.newrelic.com/accounts/1606862/sso/saml/metadata
SAML Version	2.0
Assertion Consumer URL	https://rpm.newrelic.com:443/accounts/1606862/sso/saml/finalize
Consumer Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Attributes	None required
Entity ID	rpm.newrelic.com □ Use custom entity ID

Your SAML Identity Provider certificate

*Upload a new certificate

Your SAML identity provider details

*Remote login URL

Logout landing URL (optional)

Centralize control of your user authentication

We partner with these SAML providers:

- ADFS
- Auth0
- Azure AD
- Bitium
- OneLogin
- Okta
- Ping Identity
- Salesforce

Learn more about SAML Single Sign-On

Want more user tips?

- View training videos at New Relic University.
- Read the documentation.
- Check out our Tutorials page.
- Ask a question in the New Relic Online Technical Community.