New Relic

White Paper

Guide to Getting Started with New Relic APM

Tips and tricks for gaining comprehensive visibility with the most trusted application performance management solution

Whether it's outages, crashes, or lags, organizations with unreliable software won't have users for very long.

Manually troubleshooting complex software or relying on customer complaints during urgent incidents is not only incredibly stressful, it virtually guarantees your users will flee for a competitor before you even have time to resolve the issue.

New Relic APM gives your modern development team the visibility needed to address problems quickly and proactively before they impact your users. In turn, you're able do your job more effectively while improving the overall user experience.

For software engineers, SREs, and DevOps professionals, New Relic APM provides real-time data about your application performance and the level of satisfaction that your end users experience. Our automatic instrumentation gives you built-in dashboards to see how your app is performing, whether it's built in Java, Python, Go, or any of our supported languages. Combined with opinionated workflows, New Relic APM quickly detects anomalies, discovers deficiencies, and helps you identify ways to improve performance on key metrics for business-critical applications and distributed services.

For those just entering the world of APM, it can seem pretty daunting. We get it, and we're here to provide support on your journey from APM beginner to APM wizard. Once you've installed the New Relic APM agent, start by following these pointers to get the most out of this powerful tool.

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 the name in your New Relic configuration file. You don't want to end up with 20 applications that all have the same name, 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, we also recommend standardizing your application naming (for example, all apps in staging have [Staging] at the end of their name). Ideally, you want your new applications named automatically, rather than manually, to help cut down 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 fits best with 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. For non-Java apps, there's no automatic naming but you can set the app name via a script to ensure consistency. For info about which config methods to use, see the documentation for your specific agent.

2. Add labels to your applications

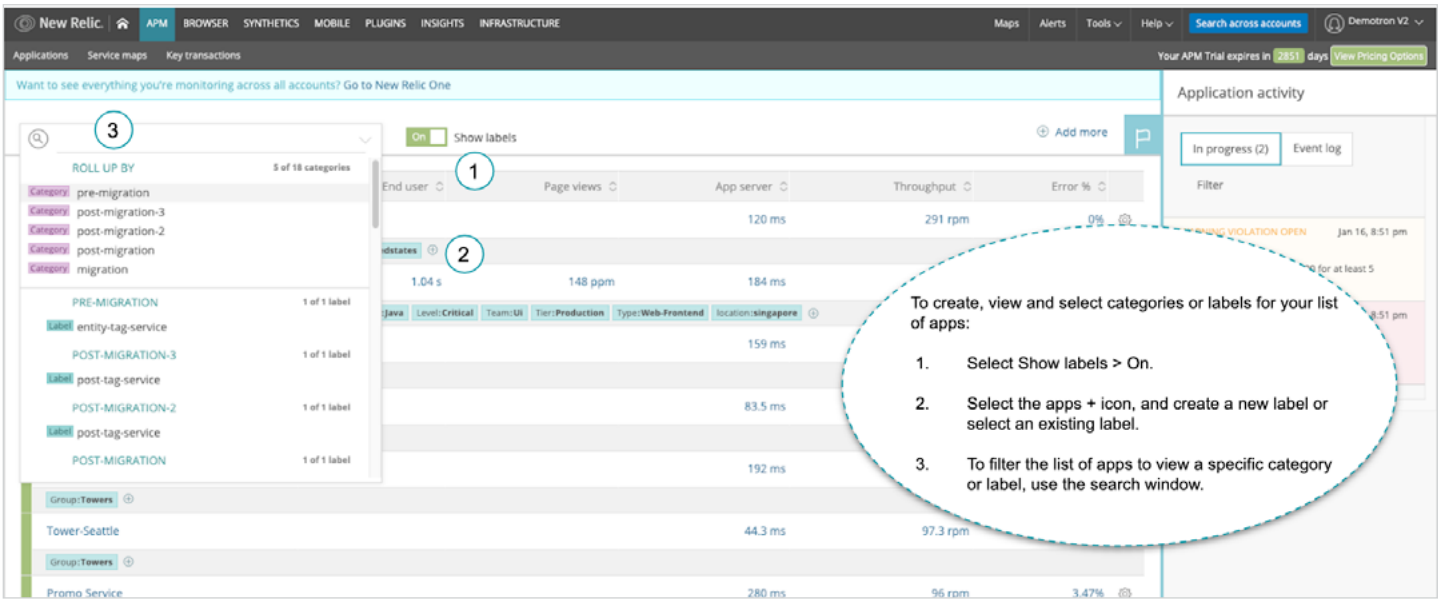
When you've got several different applications using the same account and each application spans multiple environments (e.g., development, test, pre-production, production), it can be hard to find a specific application in your overview dashboard.

That's why we recommend adding labels to your apps so you can organize them by segmenting 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 so they "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.**



Add labels to your applications

3. Create and evaluate alert policies

Most of your alerts are going to be based on your Apdex score, which measures users' satisfaction with the response time of your application. Apdex T is the central value for Apdex—you want to make sure you set it at a value that is meaningful to your specific app. We recommend setting your Apdex T value to 0.95 seconds to strive for true optimization.

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 leveraging New Relic's integrated alert channels. Just be sure to evaluate alert policies on a regular basis to ensure that they are always valid. And, if you're interested in helping your on-call teams detect, diagnose, and respond to incidents faster, check out New Relic Applied Intelligence (AI).

HOW TO DO IT:

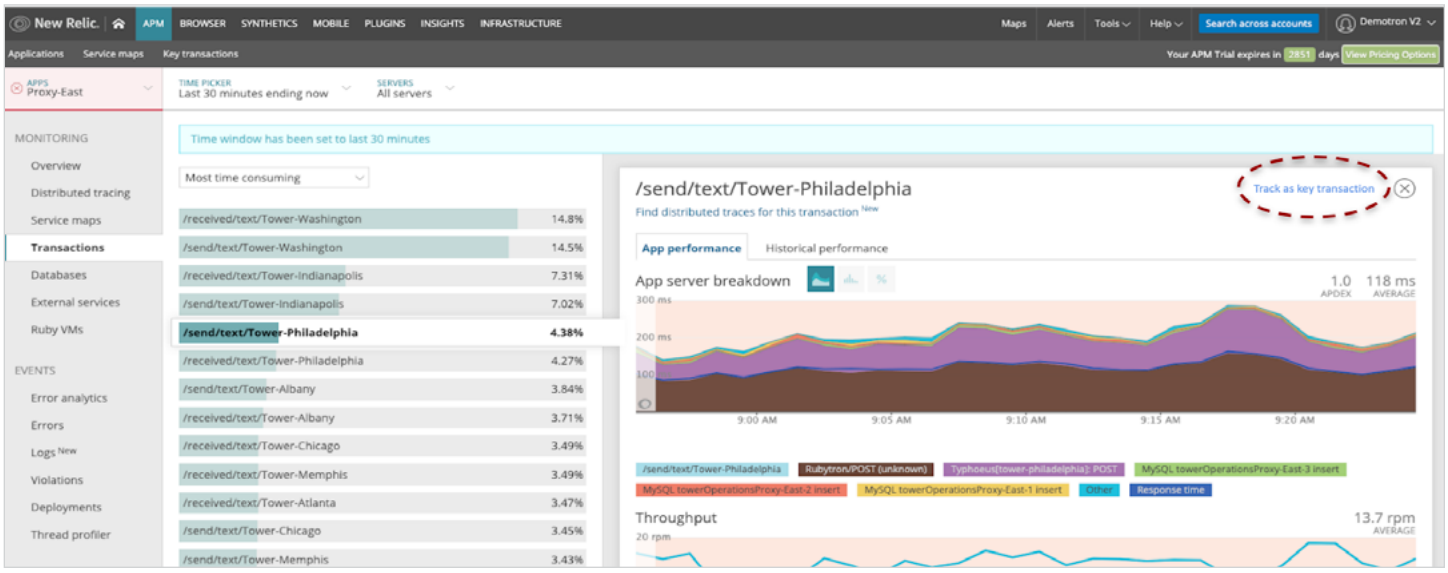
1. Change your Apdex settings.
2. Set up your alert notification channels.

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 let you closely monitor what you decide are your app's most business-critical transactions, whether that's end-user or app response time, call counts, error rates, and more. You can also create alerts to notify you when your key transactions are performing poorly.

HOW TO DO IT:

1. From the New Relic APM 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.



Identify and set up key transactions

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.**

5. 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 to surface historical trends—all great ways to report to senior executive teams or customers.

Take a look at the full list of reports available, 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.

6. Look at your environment holistically

The great thing about using New Relic to monitor your applications is that it doesn't just give you visibility into a certain portion of your application stack, but into the entirety of it. Say you're an Amazon Web Services (AWS) user. New Relic Integrations offer a number of useful ways to give you added visibility into your AWS applications. From mobile and browser monitoring to synthetics testing and more, the New Relic platform is designed to provide end-to-end visibility into the performance of your applications.

HOW TO DO IT:

1. If you aren't using any New Relic products beyond APM, sign up for other solutions that pique your interest. Many New Relic products offer a free demo and trial, which you can use to test out the solution before purchasing it.
2. Once all products are deployed, you can easily switch between different New Relic products using the menu bar on the top of your overview screen.

7. Keep your agents current

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.

Running the latest agents ensures that you have access to all our instrumentation, API methods, and bug fixes. (To see the latest improvements we've shipped to our agents, see our release notes.)

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 to know when an update is needed. If the latest agent release contains a needed fix or some additional functionality you want, download it.
2. To deploy the agent manually, see our instructions for full details.
3. To deploy the agent automatically (preferred as a method to avoid errors), you can either:
   - Use existing deployment scripts, provided 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). Check out our documentation for your agent to see what steps your script will need.
4. Once the script has been created, shut down the application (unless the script handles this).
5. Run the deployment script.
6. Start the application (unless the script handles this).

If problems arise, run the script to roll back the version to the previous version.

8. Automate user management and single sign-on

New Relic supports the SCIM 2.0 standard for automatically provisioning users and the SAML 2.0 standard to allow single sign-on (SSO). By configuring the New Relic SCIM/SSO application for your identity provider, you can automatically send New Relic any user permission changes you make within the identity provider.

New Relic users can then be created, updated, and deactivated from your identity provider, without the separate step of having to use a New Relic UI or API. In addition, users can log in to New Relic by just clicking on the SCIM/SSO application tile from their identity provider home page.

HOW TO DO IT:

1. To get started with SCIM and SSO, you'll need to work with your account representative on configuration by providing a list of the New Relic account IDs associated with your organization. For full details, check out Automated User Management.
2. To obtain a SAML certificate, start by viewing a list of the SAML service providers that New Relic currently supports for SSO integration by going to the New Relic title bar, selecting **(account dropdown) > Account settings > Security and authentication > Single sign-on.** To integrate with an SAML provider, you'll need to provide information about your New Relic account, which you can learn more about in Integrating with a SAML Provider for SSO.

Want more New Relic APM best practices and tips?

Register for our free New Relic University course, Get Started with APM, to learn more of the basics of managing your applications and services.