



An AWS User's Guide to Getting Started with New Relic

Successfully migrate and optimize your applications in the cloud



Table of Contents

INTRO	03
ABOUT OUR PARTNERSHIP	03
GETTING STARTED	05
BASIC FEATURE OVERVIEW	07
BEST PRACTICES	22



Intro

Are you an AWS user looking to accelerate time to market? Lower costs? Or avoid painful mistakes as you migrate your applications to the cloud?

If you answered “yes” to one or all of the above, then this guide is for you. It offers everything you need to get started improving the performance of your AWS applications with end-to-end monitoring from New Relic.

From instructions for installing the agent to a basic feature overview to AWS best practices, this guide is full of useful information for New Relic newbies.

Although we recommend installing New Relic early on to monitor and ensure the success of your cloud migration, it's never too late to get better visibility into your application environment. So let's get started exploring everything that New Relic can do for you.

About Our Partnership

New Relic became an AWS partner in 2009 when we introduced on-demand application management for Java in the Amazon EC2 Cloud. Today, we are an AWS Advanced Technology Partner with tens of thousands of joint customers, including the Centers for Medicare and Medicaid (CMS), Condé Nast, Major League Baseball Advanced Media (MLBAM), and REA Group.

How the partnership benefits you

Whether you've already moved to the Cloud or are getting ready to migrate, New Relic helps AWS users improve the performance and end-user experience of their business-critical applications.

As a Software-as-a-Service (SaaS) company, New Relic understands both the challenges and opportunities of running in the cloud. This gives us deep cloud expertise and best practices we can offer to successfully migrate, operate, and optimize your cloud-hosted applications. With New Relic, AWS users are able to:

- **Accelerate time to market.** We make sure you do everything right the first time so you see revenue grow faster and bigger.
- **Avoid painful mistakes.** We help users find and fix problems before they throw your migration off track or impact end users.



- **Lower costs.** With visibility into both application and server-side performance, we make it easy to see where you're spending the most money so you can reallocate your resources appropriately.

New Relic helps AWS customers achieve the above benefits by giving them the ability to monitor, troubleshoot, and tune their applications in real time. Our software analytics suite of products can be used in conjunction with all of the following AWS tools:

- **Amazon CloudWatch:** Monitoring for AWS cloud resources and applications
- **AWS Elastic Beanstalk:** Quick deployment and management of app in the cloud
- **Amazon Elastic Compute Cloud (EC2):** Scalable virtual private servers
- **Amazon Relational Database Service (RDS):** Scalable database server with MySQL and Oracle support
- **Amazon Simple Storage Service (S3):** Web service-based storage
- **AWS OpsWorks:** Application management service

With seamless integration and end-to-end monitoring, there's really no reason why you shouldn't be using New Relic to monitor your AWS environment, especially since you can give it all a try for free.

Go to newrelic.com/aws to get a promo code for a free 30-day New Relic Pro trial.



Getting Started

To get started monitoring your AWS applications using New Relic, you'll first want to sign up for your free Standard account by going to newrelic.com/aws. You can also sign up by finding New Relic in the AWS Marketplace, an online store that helps customers find, buy, and immediately start using the software and services that run in the EC2 cloud.

Install the New Relic agent

Once you've signed up, you'll then need to install the New Relic agent. New Relic supports all types of AWS applications, whether they're built in Ruby, PHP, Python, Java, .NET or Node.js. You can find the appropriate installation instructions by clicking on the language of your choice below.

- [Installing New Relic for PHP](#)
- [Installing New Relic for Java](#)
- [Installing New Relic for .NET](#)
- [Installing New Relic for Python](#)
- [Installing New Relic for Ruby](#)
- [Installing New Relic for Node.js](#)

What are the requirements?

Before you install New Relic, make sure you have a supported Amazon Web Services account. Also keep in mind that you'll need your New Relic license key for installation. This will be a 40-character hexadecimal string that New Relic provides when you sign up for your account.

Tip: To view your license key, go to the New Relic title bar, select **(selected account) > Account settings**



Install the AWS Plugin

Now that you've got the agent set up, the next step is to install New Relic's AWS plugin. With this single plugin, you'll be able to monitor several AWS services through CloudWatch directly in your New Relic dashboard. This includes:

- **Amazon EC2**, which displays CloudWatch metrics for EC2, such as Disk Operations, CPU usage, and Network IO
- **Amazon Elastic Block Store (EBS)**, which displays CloudWatch metrics for EBS, such as Read/Write operations, queue length, and throughput
- **Elastic Load Balancing (ELB)**, which displays CloudWatch metrics for ELB, such as requests and latency
- **Amazon ElastiCache**, which displays CloudWatch metrics for ElastiCache using Memcached, such as commands executed, hits, misses, and free memory
- **Amazon RDS**, which displays CloudWatch metrics for RDS, such as CPU utilization, latency, and throughput
- **Amazon Simple Notification Service (SNS)**, which displays CloudWatch metrics for SNS, such as number of notifications delivered and number of messages published
- **Amazon Simple Queue Service (SQS)**, which displays CloudWatch metrics for SQS, such as messages and message visibility

To download the AWS plugin, go to the [New Relic Plugins](#) page or go to the [AWS Marketplace](#), where it is also available as an Amazon Machine Image (AMI).

All it takes to install:

1. Log into your New Relic account
2. Select and install the plugin
3. Start seeing your AWS data



Basic Feature Overview

Once you've got the New Relic agent and AWS plugin installed, you should be able to see all your AWS data in the Applications Overview dashboard. This dashboard gives you the basic information about the selected app, including Apdex score, throughput (requests per minute), transactions, error rate, recent events, and server information.

Applications Overview dashboard

To view your app's dashboard, go to the New Relic menu bar, select **APM > (selected app)**.

The **Monitoring > Overview** dashboard automatically appears.

From here, you can drill down into a number of different areas, including:

- **Response time:** By default, the Applications Overview shows response time and Apdex charts for (backend) web transactions. To view the corresponding charts for (frontend) browser monitoring transactions, select the Browser link above the chart. Or, to view any non-web transactions for your app, select the view option from the Response time drop-down.



- **Average:** New Relic captures all the requests that come in through your agent and displays the average response time to give you a general sense of your app's performance. You can quickly identify any spikes in response time, and what the source of those spikes are, whether it's in the code, the database, external calls, or elsewhere.
- **Histograms:** In addition to showing you the average response time of your app, you can also get a bigger-picture view of its performance with histograms. With this feature, all of your app's transactions are surfaced and plotted so that you can easily identify which ones are the most time consuming, and which ones are speeding past the rest.



- **Percentiles:** This feature allows you to view the response times of the 99th percentile and 95th percentile of your app's transactions, alongside the median and average. Percentiles prevents you from relying only on the average response time of your app, and potentially ignoring transactions that slow your app down.
- **Selected window of time:** In the top right-hand corner of New Relic you will see the selected time window (in this case the last 30 minutes). Expand the "time picker" menu to select the time period you wish to review.
- **Apdex score:** Your Apdex score is a measure of how much slow site performance contributed to poor customer experiences in your app.
- **Transactions:** This is where you'll see the top five most time-consuming (by default) web transactions, along with their average response time and throughput (requests per minute).
- **Error rate:** This shows you the percentage of errors your app has encountered for a selected time period.
- **Recent events:** Problems and other events (such as deployments) appear in this list. Depending on how the app/server is performing, you'll notice icons with hyperlinks to information about alerts, deployments, notes, and more. The color-coded bar at the top of the dashboard (showing your app's name) provides a "traffic light" changing between green, yellow, red, or gray to indicate your app's current health status.
- **Servers:** Here's where the status of your servers is located. This list will show you the Apdex score, response time, throughput, CPU usage, and memory of each of your monitored servers.

But that's only the beginning! Now that you're familiar with the Applications Overview screen, let's move on to the good stuff.

Transaction Traces

Sometimes you need the nitty-gritty transaction details to find out what exactly might be slowing your application down. The New Relic Transaction Traces feature does just that by arming you with pro-level diagnostics down to the SQL while replacing the time-consuming task of digging through log files. The result? Problems fixed fast.

In most instances, New Relic only collects streaming metric data. This data is aggregated, so that if the ORM Layer (such as ActiveRecord or Hibernate) were invoked 100 times during a 60-second time period, New Relic would collect one metric that was an aggregate of the 100 invocations.

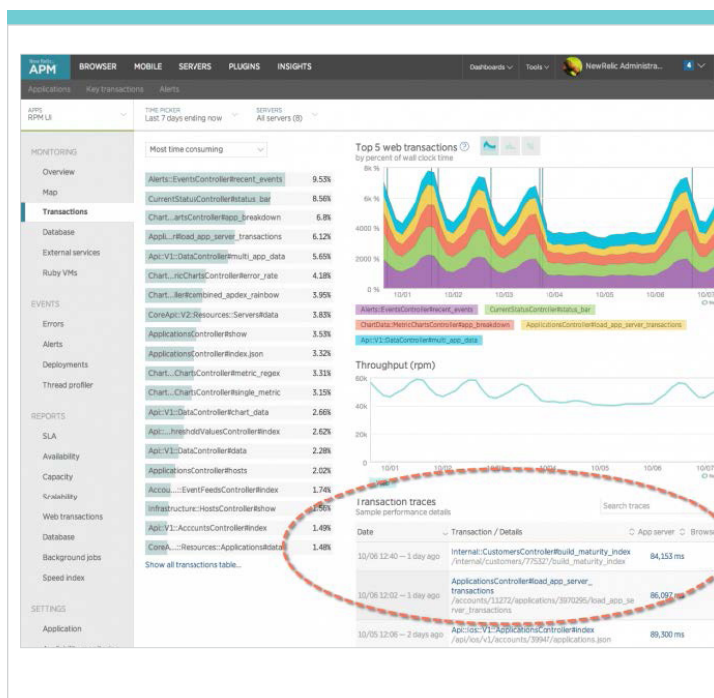


However, with the Transaction Traces feature, just the opposite happens. Each minute, transaction tracing collects data for your slowest individual HTTP requests, giving you visibility all the way down to the SQL. If a transaction is taking longer than a configurable time period, New Relic captures the exact invocation pattern and details related to the invocation, such as the particular SQL statement that was issued. You can then view each segment of the trace as colored bars in the Transaction Trace Summary tab.

What's particularly nice about New Relic's Transaction Traces feature is its user-friendly interface. Unlike other APM solutions you may have used, the New Relic interface is super easy to navigate and find what you're looking for.

If you have a New Relic Pro account and want to give the feature a try, from the New Relic menu bar, go to **Applications > (selected app) > Monitoring > Overview**.

Alternately, you can go to **Applications > (selected app) > Monitoring > Transactions**. Then, from the Transactions dashboard, select a link for any app server transaction trace. Once you're at the overview dashboard, you can then do a number of things, which are outlined below.



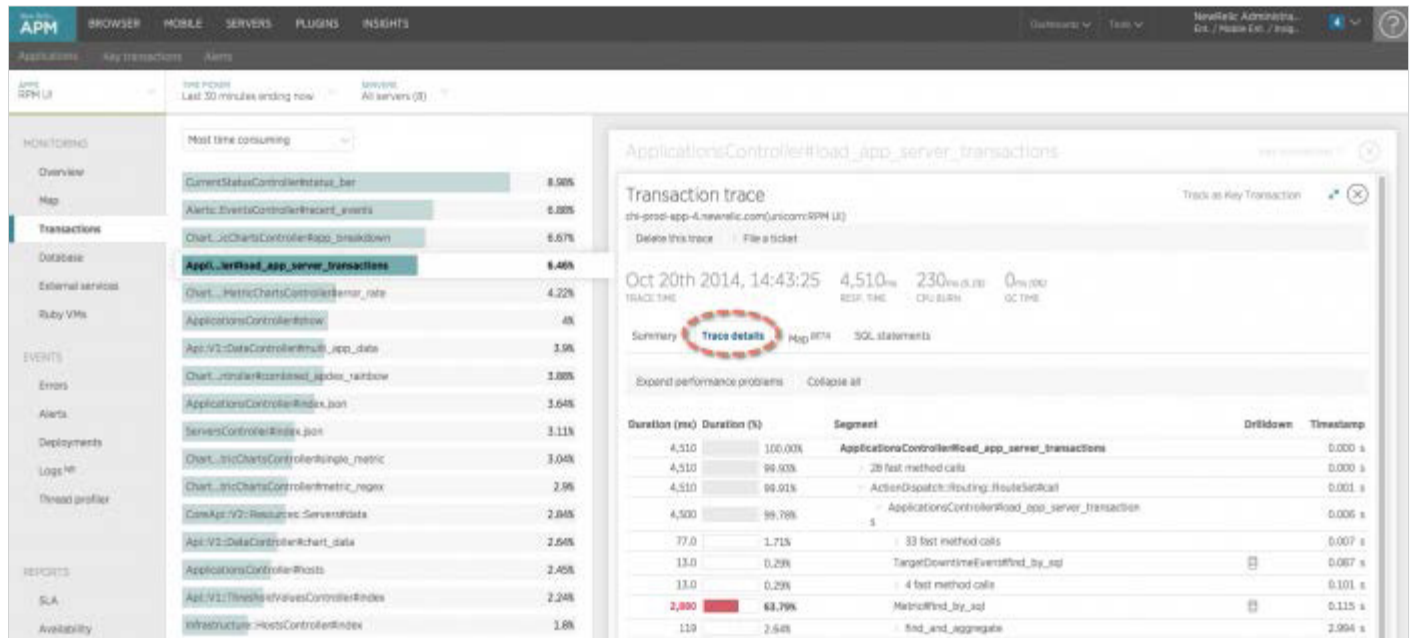
VIEWING THE TRANSACTION TRACE SUMMARY

New Relic sorts transaction traces by response time so that the slowest appears first. From New Relic APM's Transactions dashboard, you can view trace details for the transactions that take longer than your defined threshold.

Note: Depending on your selected app, the Type drop-down menu may not appear.

To view captured transaction traces for the selected time period:

- From the New Relic APM menu bar, select **Applications > (selected app) > Monitoring > Transactions**.
- If applicable, select the transaction **Type** (web, non-web, or all transactions).
- Optional: From the Transactions dashboard's **Transaction traces** table, change the sort order, use the search window, or select **Show more slow transactions** to locate a transaction trace.
- Select a link to view details about a transaction trace.



VIEWING TRANSACTION TRACE DETAILS

New Relic APM's transaction trace Details dashboard shows the total duration in milliseconds and as a percentage of the trace. This duration includes the time consumed by all nested calls within the segment.

The duration, bar chart, and percentage of each segment are color coded according to the amount of time consumed by the segment, minus time consumed in all nested calls. Also, the Timestamp column shows the relative offset in time that each segment started.

COLORS

Colors indicate percentages of total trace time spent within the segment.

- **Red:** More than 25% of the total trace time was spent within the segment.
- **Yellow:** More than 5% of the total trace time was spent within the segment (excluding the duration of any nested segments).
- **Gray:** All other segments.

"APPLICATION CODE" IN TRACES

If you see the phrase "Application code" in your transaction trace details, it generally means the agent did not have enough insight into that part of your code. You can use custom instrumentation to see more detail in that part of the code. "Application code" often appears in partial traces.

PARTIAL TRACES

Occasionally you may see a notice in the transaction trace details that "This is a partial trace." For performance reasons, New Relic APM only shows the first 2000 elements of a

transaction trace (900 for Node.js). If a transaction trace exceeds that number of segments (nodes), the agent truncates the transaction trace before sending it to the collector.

- Java, .NET, and Ruby agents truncate traces chronologically.
- Node.js: See Node.js agent configuration.
- PHP agent truncates traces based on priority: Database and memcache calls have highest priority. After those have all been captured, the PHP agent picks up the slowest functions or methods.

ROLLUP

A common problem when viewing transaction traces is deciding what is important and what is noise. New Relic makes smart guesses to make your job easier by automatically rolling up fast method calls and repeat calls.

- **Segments:** When New Relic detects four or more consecutive segments with a duration of 7.5 ms or less, the segments are collapsed into a rollup node. To view the details, expand the collapsed node.
- **Identical calls:** When New Relic detects four or more consecutive identical calls, this usually indicates an N+1 problem. The segments are collapsed into a rollup node. To view the first three calls in the sequence, expand the collapsed node.

DRILLDOWN OPTIONS

[Click here](#) to drill down into additional details of a trace.

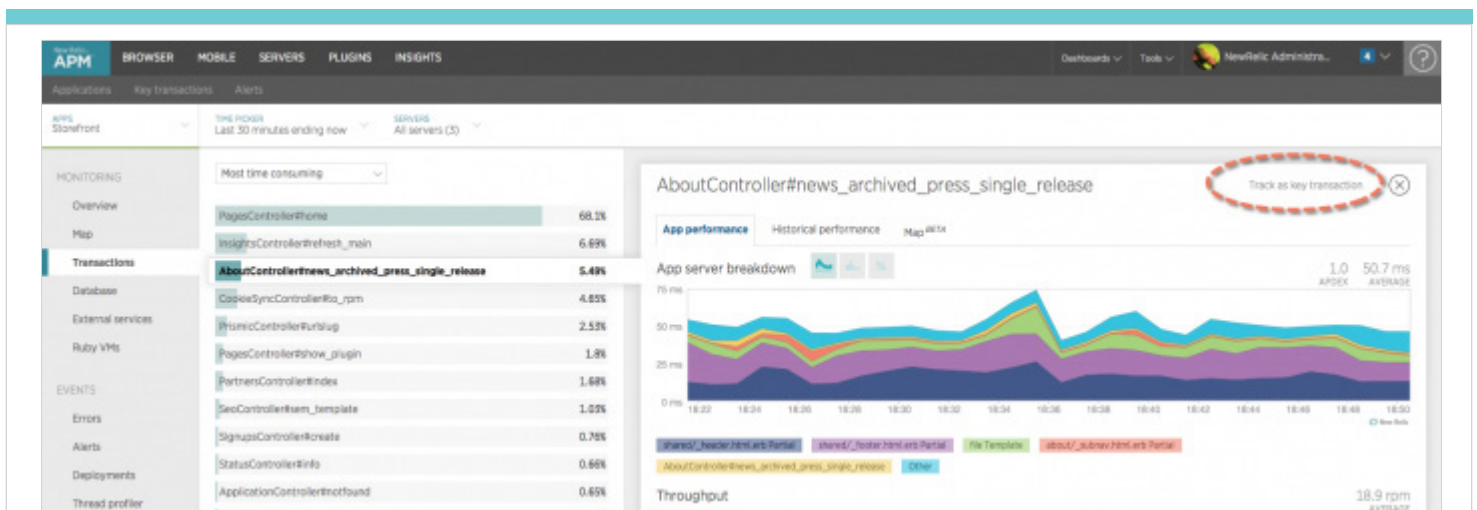


Key Transactions

Depending on the nature of your web application, some transactions may be more important to you than to others. If you're an e-commerce company, for example, you're likely interested in seeing transactions for sign-ups or purchase confirmations. Alternately, if your biggest concern is around performance, then transactions from searches or logins will probably be most important to you. These are what we would call your key transactions.

New Relic's Key Transactions feature lets you closely monitor and report on what you decide are your app's key transactions, such as end-user and app response time, call counts and error rates. You can also set alert threshold levels for notifications when your key transactions are performing poorly.

The first time you use the Key Transactions dashboard, a Welcome page appears. After you create one or more key transactions, the dashboard lists key transactions for all apps.



TO CREATE A KEY TRANSACTION

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. 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 transaction dashboard details, select **View new key transaction**.

The Key Transactions dashboard immediately refreshes and shows the Overview dashboard for your new transaction.



The first time you use the Key Transactions dashboard, a Welcome page will appear. After you create one or more key transactions, that dashboard will include a list of transactions for you to take a closer look.

Name	End user	App server	Call count	Error %
Incidents Index (Production) RPM UI	1.82 s	747 ms	194 calls 64.7 cpm	0.00%
Browser APM: Applications#show RPM UI	3.2 s	1,080 ms	102 calls 34 cpm	0.00%
Transactions Index RPM UI	3.44 s	1,190 ms	91 calls 30.3 cpm	0.00%
Platform::PluginPagesController#dashboard RPM UI	2.49 s	946 ms	87 calls 29 cpm	0.00%
APIv2: Components index RPM UI		1,350 ms	76 calls 25.3 cpm	0.00%
Server Show RPM UI	3 s	1,010 ms	537 calls 179 cpm	0.37%
Servers Index RPM UI	3.21 s	96.9 ms	2.13k calls	0.28%

VIEWING KEY TRANSACTIONS

Once you've created one or more key transactions, here's how you can view them:

Select **Key Transactions** from the top navigation bar. To drill down into details about a specific key transaction:

1. Select its name.
2. Select the type of view for app servers and browsers.

The Transactions menu lists each key transaction by its customized name, and the associated app's name appears below it. You can sort the list by any column heading and use any of the [standard user interface functions](#).

To view detailed information, select the key transaction's name on the Transactions list. The dashboard immediately refreshes with the selected key transaction's **Overview** information.

The key transaction's Overview dashboard presents summary information about your key transaction in charts and tables. From here you can drill down into specific details or select other tabs to view additional data.

ALERTS FOR KEY TRANSACTIONS

When you select a key transaction, you have the option to view its alert history and a link to the associated alert policy. To review key transaction alerts:

- From the New Relic APM or New Relic Browser menu bar, select **Key transactions > (selected key transaction) > Alerts**.
OR
- From the New Relic APM or New Relic Browser menu bar, select **Key transactions > (selected key transaction) > Overview**, and then select an alert link from the Recent events list.

For more information, see [View a key transaction's alert information](#).



New Relic
APM

BROWSERMOBILESERVERSPUGINSINSIGHTS

Dashboards Tools

ApplicationsKey transactionsAlerts

APP

Overview

Map

SLA report

Alerts

X-Ray

ALERTS

Daily SLA reportWeekly SLA report

Download this report as .csv

	08/24	08/31	09/07	09/14	09/21	09/28	10/05	10/12
End user tier								
Page views	1,360	1,440	2,020	1,700	1,300	1,810	1,740	1,680
Load time sec	3.74	3.74	3.66	3.76	3.9	3.76	3.86	4.28
Apdex	0.67	0.67	0.68	0.68	0.66	0.67	0.66	0.62
% Satisfied	40.2%	40.9%	41.2%	41.7%	39.7%	39.6%	40.4%	33.8%
% Tolerating	53.4%	52.5%	52.9%	51.7%	52.2%	54.0%	50.8%	56.4%
% Frustrated	6.5%	6.6%	6.0%	6.6%	8.1%	6.4%	8.8%	9.8%
Application server								
Requests thousands	1.49	1.57	2.09	1.76	1.74	1.68	1.89	2.14
Resp. time ms	202	220	224	237	225	210	226	208
Apdex	0.98	0.97	0.97	0.96	0.97	0.97	0.97	0.97
% Satisfied	95.0%	94.7%	93.9%	92.1%	94.5%	95.1%	93.9%	94.1%

SLA REPORTS FOR KEY TRANSACTIONS

Interested in getting daily or weekly Service Level Agreement (SLA) reports for your key transactions? No problem. You can view the information from the New Relic Transactions dashboard, or download it as a file with comma-separated values (CSV). The SLA reports include information about requests, response times, and end user satisfaction levels (a.k.a. Apdex values).

To view or download SLA reports for a key transaction:

1. From the New Relic APM or New Relic Browser menu bar, select **Transactions > (selected key transaction) > SLA report**.
2. Use any of New Relic's standard **user interface functions** and **dashboard features** to drill down into detailed information.
3. Select **Daily** or **Weekly** to view report data for that range.
4. Optional: To download the report as a CSV file, select **Download this report as .csv**.

Error Analytics

If you want to analyze the errors being reported by your applications, the New Relic APM Errors page is just the ticket. The Errors page will provide different data views depending on your account level, agent, and time window. The Errors page can be used to:

- Assess the health of your applications with fine-grained data on error events over the past 8 days.
- Identify long-term trends with error rates for periods longer than 8 days.
- Review recent error traces to diagnose and resolve specific errors.



To view the Errors page:

- From the New Relic menu bar, select **APM > Applications > (selected app) > Events > Error analytics**.
OR
- From the New Relic menu bar, select **APM > (selected app) > Monitoring > Overview**, and then select the **Error rate** table's title.

Use any of New Relic's standard user interface functions and page functions to drill down into detailed information.

[Click here](#) to learn more about using New Relic APM error analytics.

EVENT AND METRIC VIEW COMPATIBILITY

The Errors page provides two different data views. Error traces are available for both.

Error events: An **error event view** with two independently filterable charts and heat map is available to Pro and Enterprise customers with a supported agent for time periods within the past 8 days.

Error metrics: An **error metric view** is available for other account types, and for any time period that falls outside or extends beyond the past 8 days.

The following agents fully support both data views:

- Java 3.21.0 or higher
- Node.js 1.24.0 or higher
- PHP 5.1.130 or higher
- Python 2.58.0.43 or higher
- Ruby 3.134.0.305 or higher

If you are using the .NET agent, you need to be in version 3.1.65 or higher to access all the features of the metrics view on the **Errors page**.



Server Monitoring

In addition to a wide range of application performance monitoring tools, New Relic Servers also lets you see which servers have capacity issues and immediately take corrective action. After all, how can you know the application is healthy if you can't see the server it's running on? Specifically, New Relic Servers allows you to view and analyze critical system metrics, including CPU usage, physical memory, network activity, processes, and disk I/O utilization and capacity.

To start viewing details about your servers' health and recent server events, install the New Relic Servers agent for your server. [Click here](#) for details about installing **New Relic Servers for Linux**. [Click here](#) for details about installing **New Relic Servers for Windows**.

Once complete, go to the New Relic menu bar and select **Servers**. The Servers dashboard lists all of your servers reporting to New Relic's collector, including the server host names, current CPU, memory, and disk usage. You'll notice a color-coded "traffic light" indicating each server's current health.


The screenshot shows the New Relic Servers dashboard. The top navigation bar includes APM, BROWSER, MOBILE, **SERVERS**, PLUGINS, and INSIGHTS. Below the navigation bar, there's a search bar for filtering servers and a toggle for 'Show labels'. The main table lists servers with columns for Name, CPU, Disk IO, Memory, and Fullest disk. The servers are color-coded: green for healthy, yellow for warnings, and red for critical issues. The 'Recent events' panel on the right shows a list of events, including 'CHI-PROD-BGWORKER-4.NR-OPS.NET' with a 'Memory > 70%' warning and 'CHI-PROD-TIMESLICE-23.NR-OPS.NET' with a 'CPU > 66%' warning.

Name	CPU	Disk IO	Memory	Fullest disk
usw2-staging-pinger-01.newrelic.com Staging Pinger - Clients	0.32%	0%	31.2%	55%
usw2-prod-pinger-1.nr-ops.net	25.1%	0%	73.3%	81%
use1v-staging-www-3.awsdev.nr-ops.net Storefront (master), Storefront (release), 1 more ...	34.3%	29.3%	18.2%	32.8%
use1v-staging-www-2.awsdev.nr-ops.net Storefront (master), Storefront (release), 1 more ...	32.2%	25.8%	17.9%	32.8%
use1v-staging-www-1.awsdev.nr-ops.net Storefront (master), Storefront (release), 1 more ...	42.1%	22.5%	18.3%	32.7%
use1v-staging-whitelist-app-1.awsdev.nr-ops.net	1.41%	0%	13.4%	36.8%

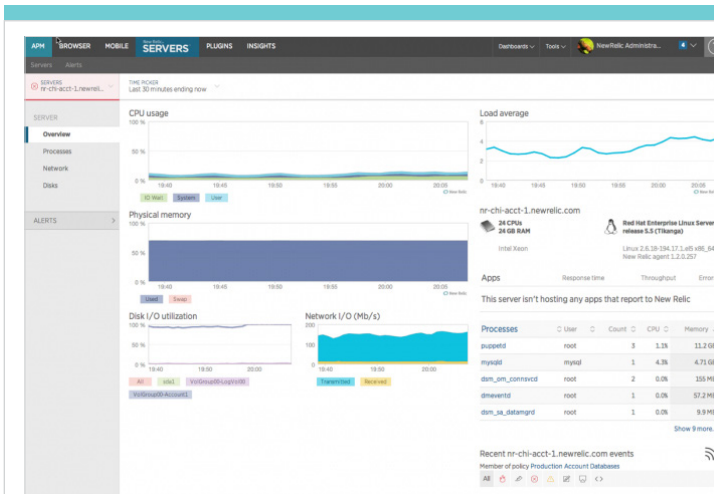
UNDERSTANDING SERVER "TRAFFIC LIGHTS"

- **Green:** The server is A-OK.
- **Yellow:** A warning that the server is experiencing some non-critical issues.
- **Red:** A critical alert that something is wrong with the server, or that the New Relic agent on this server is unable to communicate with the collector.
- **Gray:** No data is being reported for the server.



If you want to ...	Do this ...
Change the order that servers appear on the list	Click any column heading to sort in ascending or descending order.
Add a server to the dashboard	Click Add more and then follow the installation instructions for your specific platform.
Delete a server from the dashboard	To delete a server completely, make sure its “traffic light” is gray. Then click Delete . If you want to remove it from the list without deleting it completely, use the filter or search options.
Filter the list of servers	To filter or search by server name, app name, or tags, select the filter option. Or to search by host name, type the name in the search window.
Filter the list of recent events	Click the icon for specific types of events: notifications, critical alerts, warnings, deployments, or All . 
Set up an RSS feed for server events	On the Recent Server Events section of the dashboard, click the orange RSS icon.
View details about a server's health	Click the server's name to go to the Server Overview dashboard. Or, click the CPU , Disk IO , Memory , or Fullest Disk field for a specific server to see details about that specific metric for a server. For example, to view the list of processes running on a server, sorted by CPU usage, select the CPU field for the server.
View details about an event	Click the corresponding link for the event.
Define the alert thresholds for one or more servers	Click the gear icon, and use the Alerts and thresholds popup to type in the Caution (yellow) and Critical (red) values. For more information, see Server monitoring alerts .
Identify who receives alert notifications about one or more servers	Click the gear icon, and then select Configure server alerts .

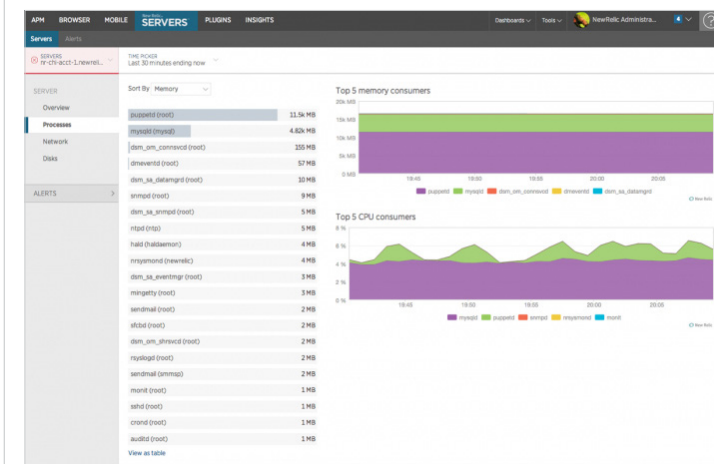
See a server that's not green and want to find out what's going on? To view summary and detail information about a specific server, select the server you want to check out from the **Servers** list. By default, the server's Overview page will appear.



SERVER OVERVIEW

The Server Overview dashboard shows summary information about a specific server for a selected time period, including:

- Charts with CPU usage information, load averages, physical memory, disk utilization, and network I/O.
- Information about the operating system and architecture, including the number of CPUs and the amount of RAM installed on the host.
- The list of applications being monitored by this server, including the response time, throughput, and errors. (**Tip:** For additional details, point the app’s “traffic light” or click on the app’s name.)
- A sortable list of running processes, including the name, user, count, and CPU and memory usage.



SERVER PROCESSES

If you want to check out all the processes running on a specific server, go to **Servers > (selected server) > Processes**. From the selected server's Processes dashboard, you can:

- View the list of processes as a graph (default) or table.
- Sort the list of processes by memory or **CPU usage***.
- View a chart of the top five memory consumers and a chart of the top five CPU consumers for the server.
- Point to or select any process for additional details, including memory and CPU statistics over time.

Use any of New Relic's standard **user interface functions** and **dashboard features** to drill down into detailed information.

** New Relic averages CPU usage for the time reported, not for the time window. This helps highlight processes that had high CPU usage but only reported briefly.*



Organize your servers and apps

In New Relic Servers, APM, and Synthetics, you can label and organize your servers and apps so they “roll up” into an unlimited number of meaningful categories. You can also easily sort, filter, and page through all your apps, servers, or monitors from their index pages.

By creating labels for categories and their values, and then rolling up apps and servers into specific categories, New Relic account owners and admins can identify useful groups. This makes it easier to find, view, and compare only the apps or servers that are meaningful to you. You can also see the health status for categories (and apps or servers within categories) at a glance.

To create, view, and select categories or labels for your list of apps or servers:

1. Select **Show labels > On**.
2. Select the app's or server's + icon, and create a new label or select an existing label.
3. To filter the list of apps or servers to view a specific category or label, use the search window.

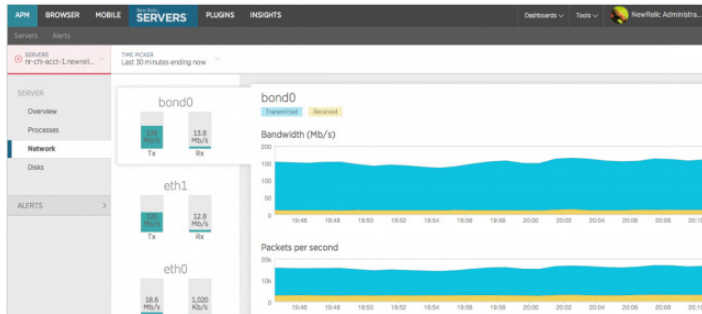
CREATE LABELS AND CATEGORIES

*Owners and Admins

To add a server or app to one or more categories, assign a meaningful label to the category first. You can create as many labels for an app or server as needed. You can also assign an unlimited number of apps or servers to a category.

- From the New Relic menu bar, select **APM**, **Servers**, or **Synthetics**.
- From the index, select **Show Labels > On**.
- To assign an app, server, or monitor to a category, select the plus + icon by its name.
- Follow the [guidelines](#) to type the label; use the format *Category:Value*.
- To save the new label, press **Enter** or **Return**.

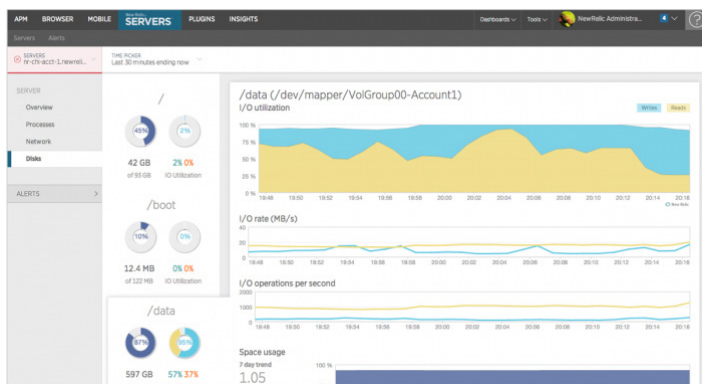
Once you've created your labels and categories, head on over to our Docs site to learn how to [view categories](#), [view apps and servers by label](#), or [remove a label from an entity](#).



NETWORK PERFORMANCE

Curious to see what's going on in a specific server's network? You can view a list of **network interfaces** and an indication of network transmit/receive throughput by going to **Servers > (selected server) > Network**.

From here, you can select a network interface from the list to view details about **Bandwidth (Kb/s)**, **Packets per Second**, or **Errors Per Second** over time. You can also point to, click, or drag anywhere on the charts for additional details.



DISK PERFORMANCE AND UTILIZATION

The Server UI also lets you view **information about I/O utilization**. To view these details, go to **Servers > (selected server) > Disks**.

The Disks dashboard shows a list of disks along with an indication of how much space is in use on the disk, and how much I/O utilization is taking place. Click any disk on the list to view a detailed breakdown of **I/O Utilization**, **I/O Rate (MB/s)**, **I/O Operations per Second**, and **Space Usage** over time. For example, the Space Usage indicates how much space might be in use seven days from now, and an estimate of when the disk might reach capacity.

As outlined above, there's a lot you can do with New Relic Servers. And getting a glimpse into your server health is just as important as viewing the application — because the greater visibility you have, the greater ability you have to stop any potential issues from escalating.



New Relic Alerts

New Relic offers a single tool to manage alert policies and alert conditions that focus on the metrics you care about most. This includes:

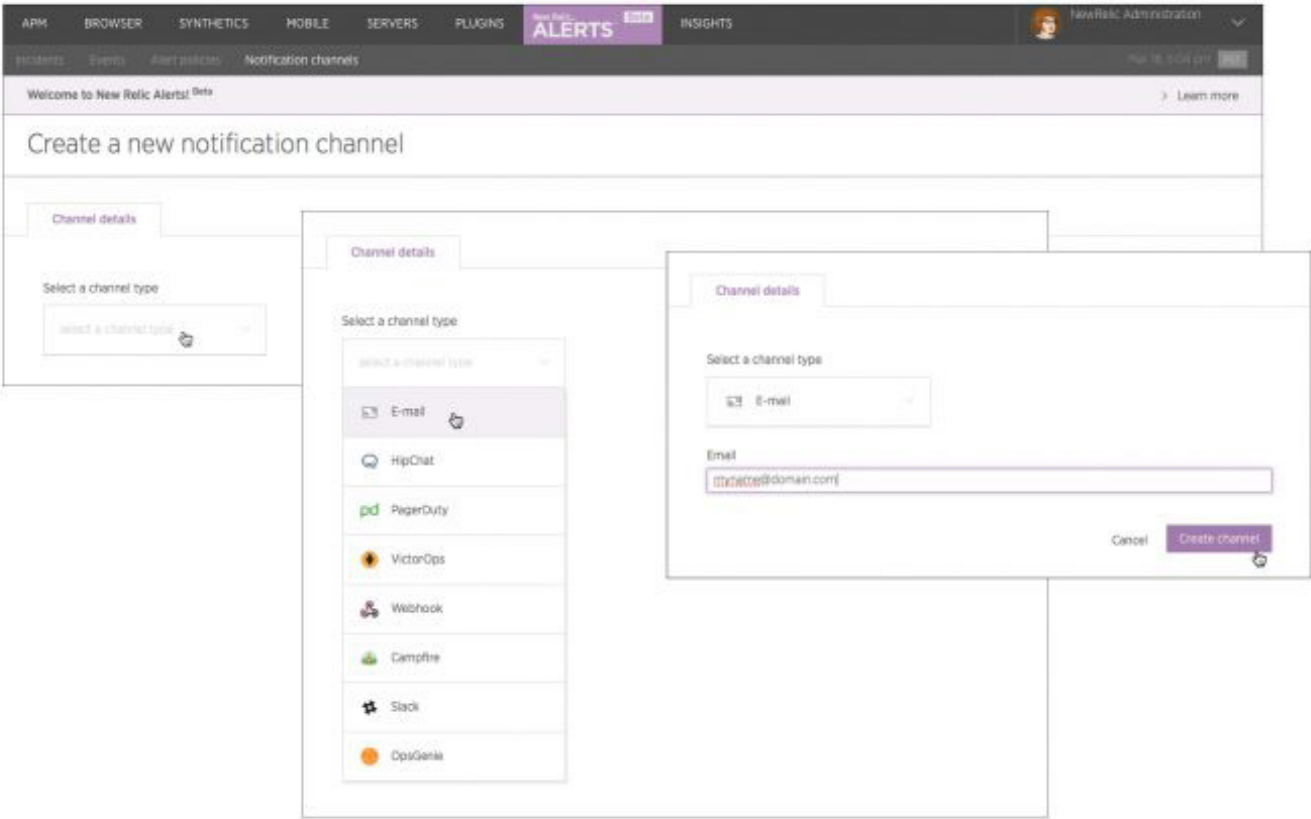
- Applications monitored by New Relic APM
- Client-side metrics monitored by New Relic Browser
- Servers monitored by New Relic Server
- Key transactions monitored by New Relic APM and New Relic Browser
- Plugins from New Relic Plugins
- Monitors from New Relic Synthetics
- New Relic Mobile, including external services

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.

You can set up [alert policies](#) and notification [channels](#) for all New Relic account types.

CREATE AN ALERT POLICY

1. Start by giving the new policy a meaningful name (maximum 64 characters); for example, the group or team's name, or the set of resources or services the alert policy is targeting.
 2. Create one or more conditions in the policy that target your resources monitored by New Relic products (maximum 100 conditions per policy).
 3. Define thresholds that trigger the alert incident.
 4. Make sure each alert condition has a concise and meaningful name, to be used in notification messages to quickly identify the condition.
 5. Optional: Include the runbook URL so that personnel responsible can follow standard procedures efficiently to manage the alert.
 6. Create one or more alert notification channels, and assign one or more channels to the policy.
 7. Specify how you want New Relic Alerts to roll up incident records when targets across your infrastructure violate one or more alert conditions.
- Repeat the steps to add more conditions or notification channels to an alert policy as needed.
- Learn more about alert policy workflow [here](#).



CREATE NOTIFICATION CHANNELS

Notification channels are where New Relic Alerts send alerts when incidents are opened, acknowledged, or closed. Here are the types of destinations you can set as notification channels for alerts:

- User
- Email
- HipChat
- OpsGenie
- PagerDuty
- Slack
- VictorOps
- Webhook
- Campfire

To create a notification channel:

1. From the New Relic menu bar, select **Alerts > 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.

To learn more about managing notification channels, [click here](#).



Best Practices

Now that you've got a basic understanding of New Relic's key features, you're ready to start getting serious with your AWS monitoring. Here are five best practices that can help you boost end-user experience, simplify performance management, and reduce the cost of your AWS environment.

1. Roll up your apps, instances, and servers

There's no need to roll up your sleeves when it comes to monitoring AWS in New Relic—just be sure to use labels and rollups if you're looking to make life easy. Using [New Relic APM](#), [New Relic Servers](#), and [New Relic Synthetics](#), you can cut through the noise of individual EC2 instances by labeling and organizing your apps, instances, and servers so they “roll up” into an unlimited number of meaningful categories. This makes it easier to find, view, and compare only the apps or servers that matter to you, or quickly see the comparative health status for categories (such as Instance Size, Region, or AMI) at a glance.

2. Consolidate your metrics into one view

If you're running on AWS, you're likely already looking at the metrics available in CloudWatch, but rather than toggle back and forth between Amazon's monitoring service and New Relic, you should install [New Relic's AWS plugin](#) to bring everything together into one view. By installing this single plugin, you can view data from key AWS tools such as AWS Elastic Beanstalk, Amazon EC2, Amazon RDS, and more via CloudWatch, alongside your New Relic application data. This way you can not only see how changes in your AWS environment are impacting performance, but also where you may be under- or oversizing your EC2 instances, which can help reduce cloud costs.

3. Automate your setup

When you're operating in a dynamic AWS environment, your underlying infrastructure is constantly shifting. And while AWS CloudFormation takes care of provisioning the resources, it raises the obvious question of how your application software is deployed, configured, and executed on your Amazon EC2 instances. That's why you should consider using an automation solution like [Chef](#) or [Puppet](#), which can automatically configure your systems and apps that sit on top of your infrastructure. Both tools make life easier by allowing you to automate your entire deployment and management process. And both can be easily integrated with New Relic.



4. Set up proper alerting

Sometimes it's hard to stay on top of every transaction and traced error. That's why New Relic makes it easy for you to stay in the know by allowing you to set thresholds for alerts on various metrics relating to your AWS applications, servers, and key transactions. You can manage alerts by creating specified user groups and by leveraging New Relic's integrated alert channels, including HipChat, OpsGenie, PagerDuty, Slack, VictorOps, and Campfire. If you're using a different alerting solution, use our Webhook feature to send a JSONObject anywhere you choose.

5. Keep an eye on the entire stack

The great thing about using New Relic to monitor your AWS applications is that it doesn't just give you visibility into a certain portion of your application stack, but lets you see the entire thing. If you spot a performance problem in New Relic APM, for example, you can easily trace that back to the hardware side using New Relic Servers or vice versa. You can test your app from outside the firewall using New Relic Synthetics, see what's going on at the interaction level using New Relic Browser, and also organize, query, and visualize all this data using New Relic Insights to answer key questions about application and customer experience—all in real time.

Want to learn more about optimizing your AWS applications using New Relic?

Visit the [Documentation site](#)

Check out [New Relic University](#)

Contact us at aws@newrelic.com