Monitoring New Relic

New Relic: APM PowerPack Beta version 100

Table of Contents

Introduction 3
What is New Relic? 3
What Does the New Relic: APM PowerPack Monitor? 4
Installing the New Relic: APM PowerPack 4
Configuring New Relic Monitoring 6
Prerequisites for Monitoring New Relic Services 6
Creating a SOAP/XML Credential for New Relic 7
Discovering New Relic Component Devices 8
Verifying Discovery and Dynamic Application Alignment 9
Relationships with Other Types of Component Devices 11
Viewing New Relic Component Devices 12
New Relic Dashboards 14
Device Dashboards 14
New Relic: APM Application 15
New Relic: APM Applications Group 16
New Relic: APM Server 17

Chapter 1

Introduction

Overview

This manual describes how to monitor New Relic web services in SL1 using the *New Relic: APM* PowerPack.

The following sections provide an overview of New Relic web services and the *New Relic: APM* PowerPack:

What is New Relic? 3
What Does the New Relic: APM PowerPack Monitor? 4
Installing the New Relic: APM PowerPack 4

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is New Relic?

New Relic is an Application Performance Tool (APM) that captures data and information about web-based applications. Users can measure the performance of their applications, which helps determine potential service delivery issues.

What Does the New Relic: APM PowerPack Monitor?

To monitor New Relic web services using SL1, you must install the *New Relic: APM* PowerPack. This PowerPack enables you to discover, model, and collect data about New Relic web services.

The *New Relic: APM* PowerPack includes:

- A sample credential you can use as a template to create SOAP/XML credentials to connect to the New Relic services you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics, and to collect configuration data for New Relic services
- Device Classes for each of the New Relic services SL1 monitors
- Event Policies and corresponding alerts that are triggered when New Relic services meet certain status criteria
- Device dashboards that display information about New Relic services

NOTE: The PowerPack does not model applications with "reporting: false" statuses.

Installing the New Relic: APM PowerPack

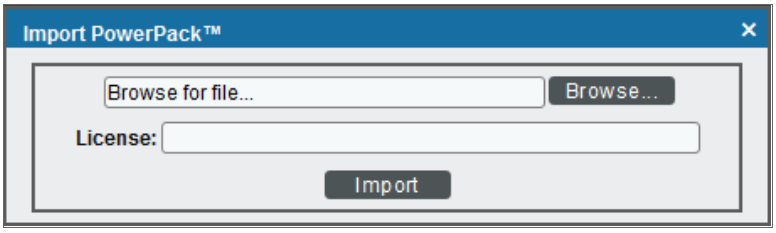
Before completing the steps in this manual, you must import and install the latest version of the *New Relic: APM*PowerPack.

NOTE: Ensure that you do not have the *New Relic: APM Pro* PowerPack installed before installing the *New Relic: APM* PowerPack. These PowerPacks are not compatible. If you have the *New Relic: APM Pro* PowerPack installed, it will need to be uninstalled prior to installing the *New Relic: APM* PowerPack. The historical data from the *New Relic: APM Pro* PowerPack will be deleted when it is uninstalled.

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Customer Portal.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.

4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

> **NOTE:** If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuring New Relic Monitoring

Overview

The following sections describe how to configure and discover New Relic services for monitoring by SL1 using the *New Relic: APM* PowerPack:

Prerequisites for Monitoring New Relic Services 6
Creating a SOAP/XML Credential for New Relic 7
Discovering New Relic Component Devices 8
Verifying Discovery and Dynamic Application Alignment 9
Relationships with Other Types of Component Devices 11
Viewing New Relic Component Devices 12

Prerequisites for Monitoring New Relic Services

To configure the SL1 system to monitor New Relic services using the *New Relic: APM* PowerPack, you must first have the following information about the New Relic services that you want to monitor:

- A New Relic REST API key. To generate the REST API key, go to the Account Settings page for your New Relic account.
- The username and password for your New Relic service.
- Insights Query Key. This is optional. Add this to the credential if you want to discover infrastructure groups used for server monitoring. You can generate this from your Insights account.

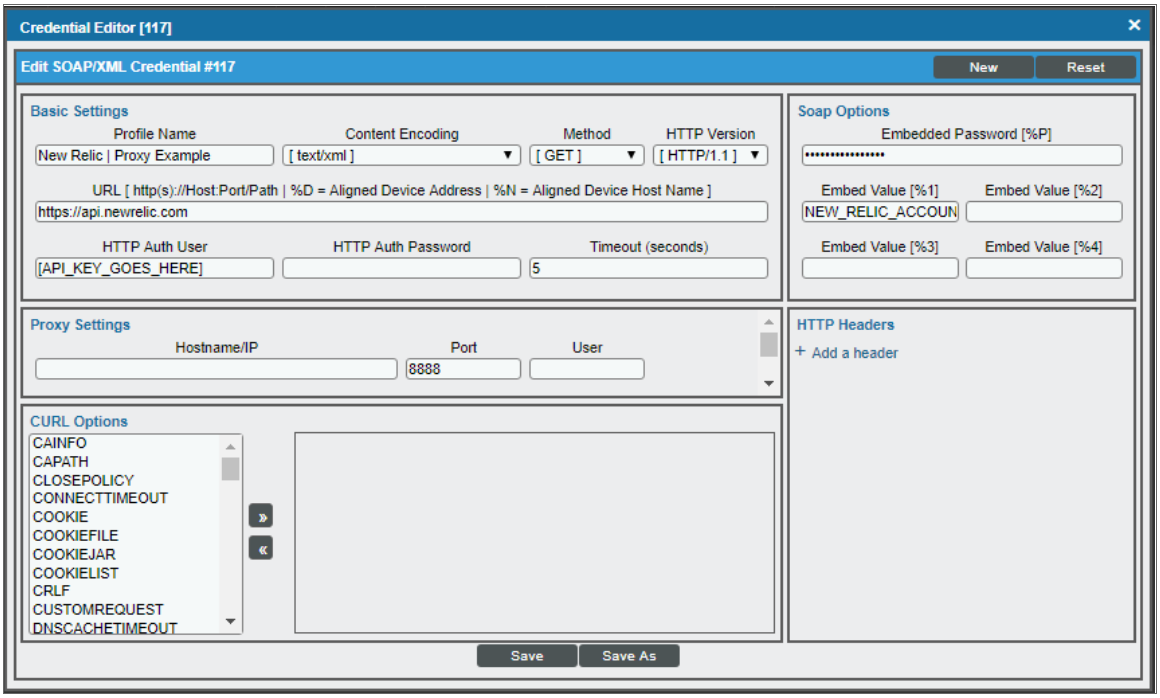
NOTE: Ensure that you do not have the *New Relic: APM Pro* PowerPack installed before installing the *New Relic: APM* PowerPack. These PowerPacks are not compatible. If you have the *New Relic: APM Pro* PowerPack installed, it will need to be uninstalled prior to installing the *New Relic: APM* PowerPack. The historical data from the *New Relic: APM Pro* PowerPack will be deleted when it is uninstalled.

Creating a SOAP/XML Credential for New Relic

To configure SL1 to monitor New Relic services, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *New Relic: APM* PowerPack to communicate with your New Relic service.

To configure a SOAP/XML credential to access New Relic:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **New Relic | Proxy Example** credential, and then click its wrench icon ( ). The **Edit SOAP/XML Credential** modal page appears.
3. Enter values in the following fields:



Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Leave this field as the default ("https://api.newrelic.com").
- ***HTTP Auth User***. Type your New Relic API key in this field.

- ***HTTP Auth Password***. Leave this field blank.

SOAP Options

- ***Embedded Password [%P]***. Type the Insights Query Key in this field if you want to discover infrastructure groups for server monitoring. If you do not have an Insights account, leave this field blank.
- ***Embed Value [%1]***. Type the ID number for your New Relic account.

4. For all other fields, use the default values.
5. Click the **[Save As]** button.

Discovering New Relic Component Devices

To model and monitor your New Relic devices, you must run a discovery session to discover your New Relic services.

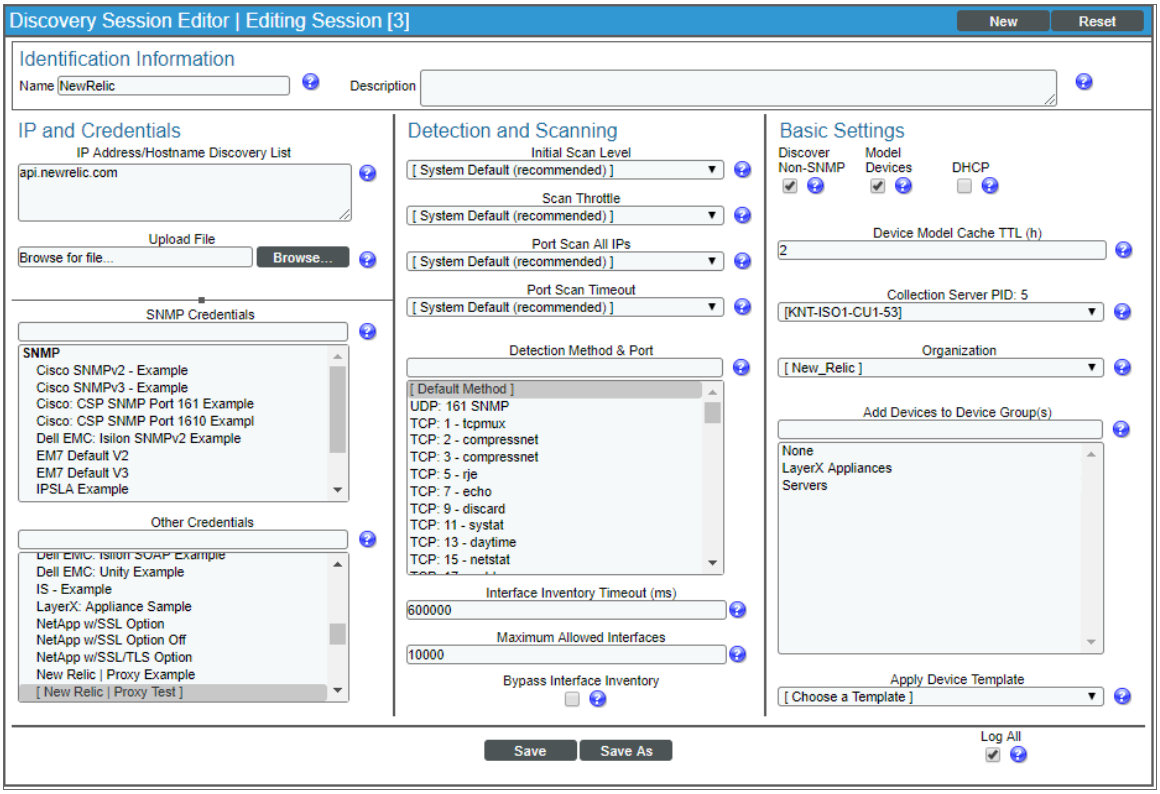
NOTE: The PowerPack does not model applications with "reporting: false" statuses.

Several minutes after the discovery session has completed, the Dynamic Applications in the *New Relic: APM*PowerPack should automatically align to the services and then discover, model, and monitor the remaining New Relic component devices.

To discover the New Relic service that you want to monitor, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button.

3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, define values in the following fields:



- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type "api.newrelic.com".
- ***Other Credentials***. Select the SOAP/XML credentials you created for the New Relic service.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

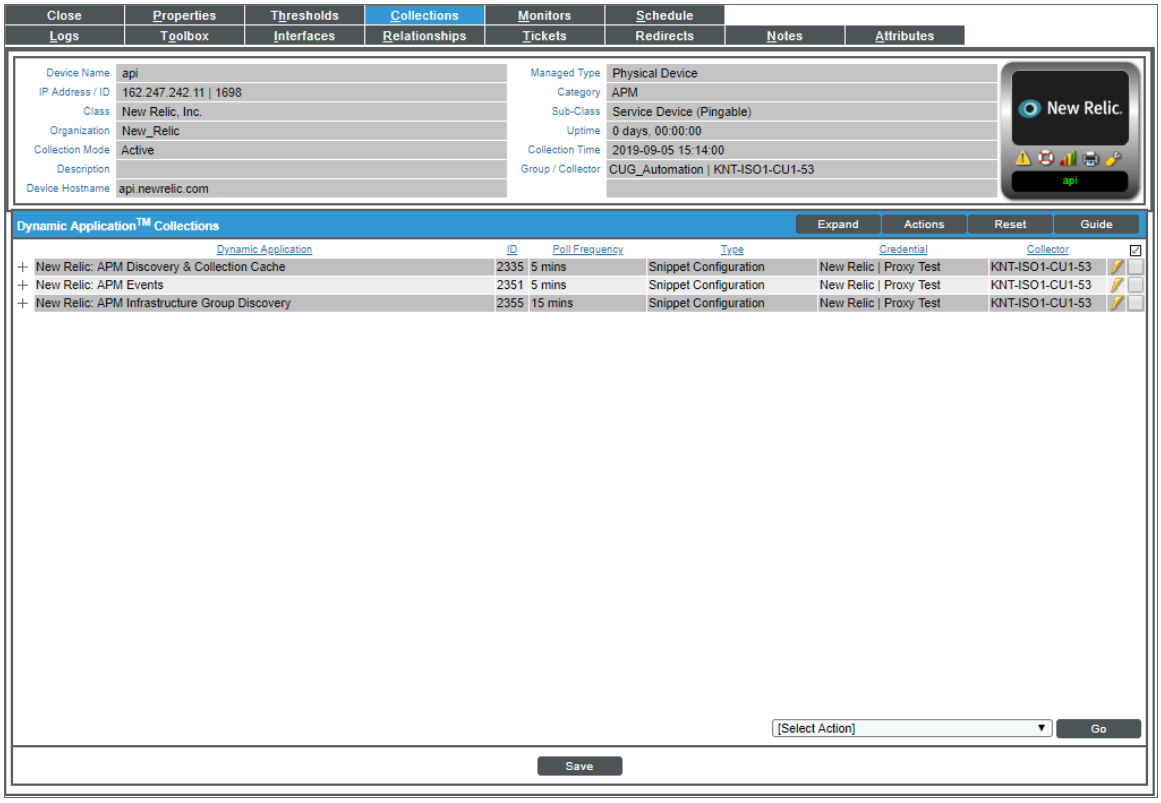
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning bolt icon ( ) to run the discovery session.
7. The **Discovery Session** window appears. When the device is discovered, click the device icon ( ) to view the **Device Properties** page for each device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the New Relic service ( ). From the **Device Properties** page for the New Relic service, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the service are automatically aligned during discovery.

> **NOTE:** It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

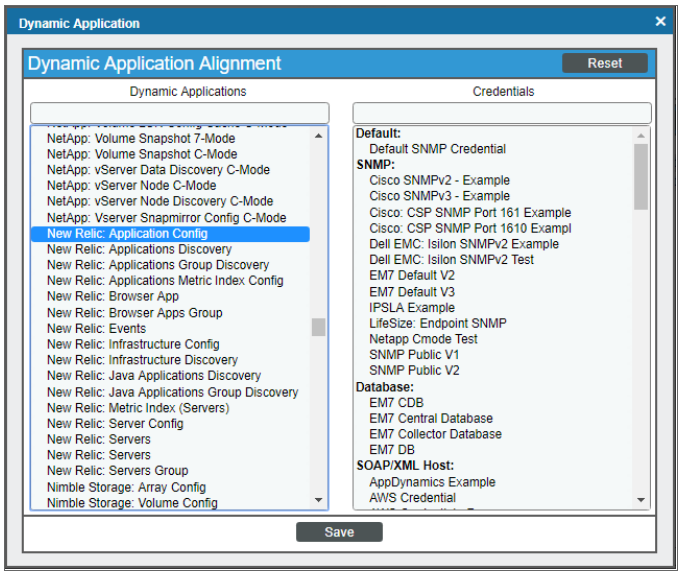


You should see the following Dynamic Applications aligned to the New Relic service:

- New Relic: APM Discovery & Collection Cache
- New Relic: APM Events
- New Relic: APM Infrastructure Group Discovery

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

1. Click the **[Action]** button, and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:



2. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
3. In the ***Credentials*** field, select the credential specified in the table.
4. Click the **[Save]** button.
5. Repeat steps 1-4 for any other unaligned Dynamic Applications.

Relationships with Other Types of Component Devices

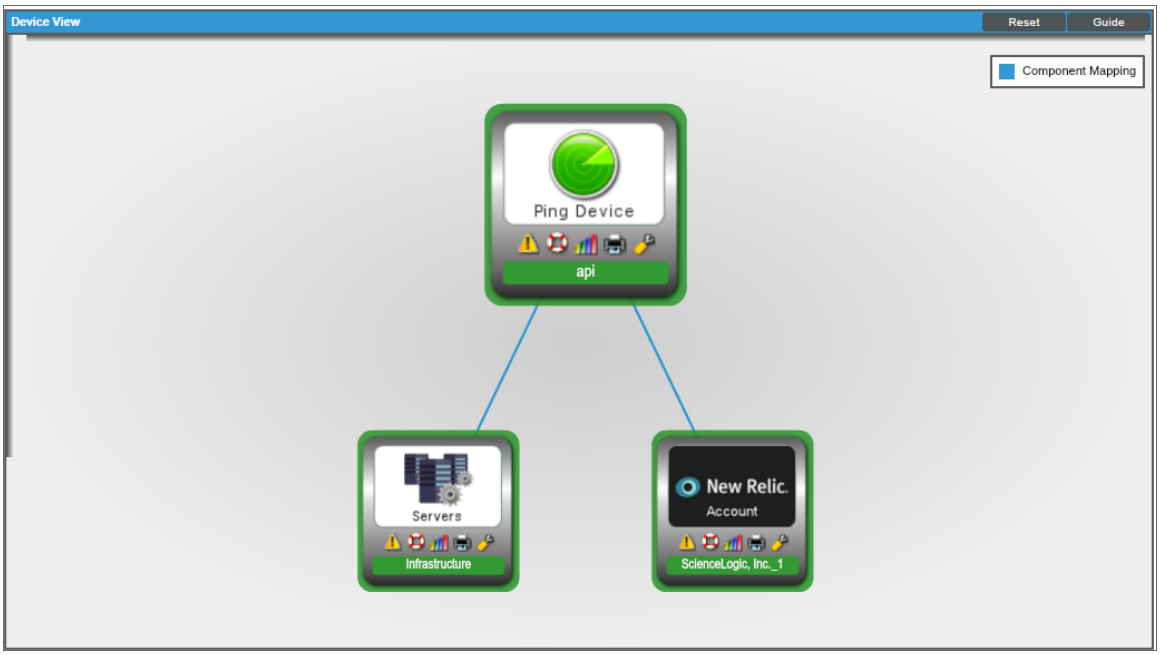
Additionally, the Dynamic Applications in the *New Relic: APM* PowerPack can automatically build relationships between New Relic devices and other associated devices:

- If you discover Linux devices using the Dynamic Applications in the *Linux Base Pack* PowerPack version 102 or later, SL1 will automatically create relationships between New Relic devices and Linux servers.
- If you discover Windows servers using the Dynamic Applications in the *Microsoft Base Pack* PowerPack version 107 or later, SL1 will automatically create relationships between New Relic devices and Windows servers.
- If you discover Windows servers using the Dynamic Applications in the *Microsoft: Windows Server* PowerPack version 108 or later, SL1 will automatically create relationships between New Relic devices and Windows servers.

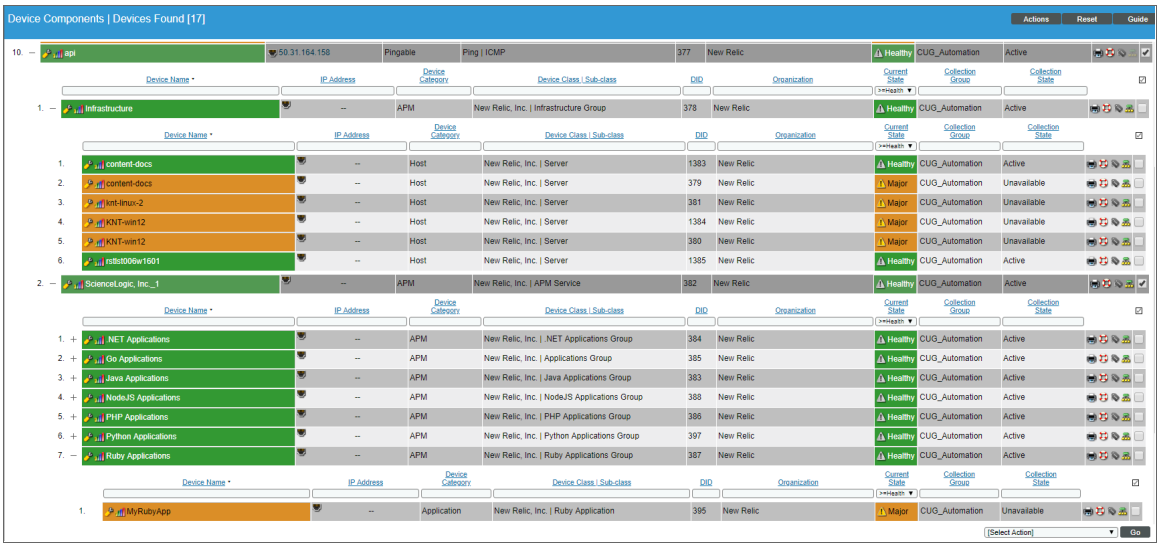
Viewing New Relic Component Devices

In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the New Relic service and all associated component devices in the following places in the user interface:

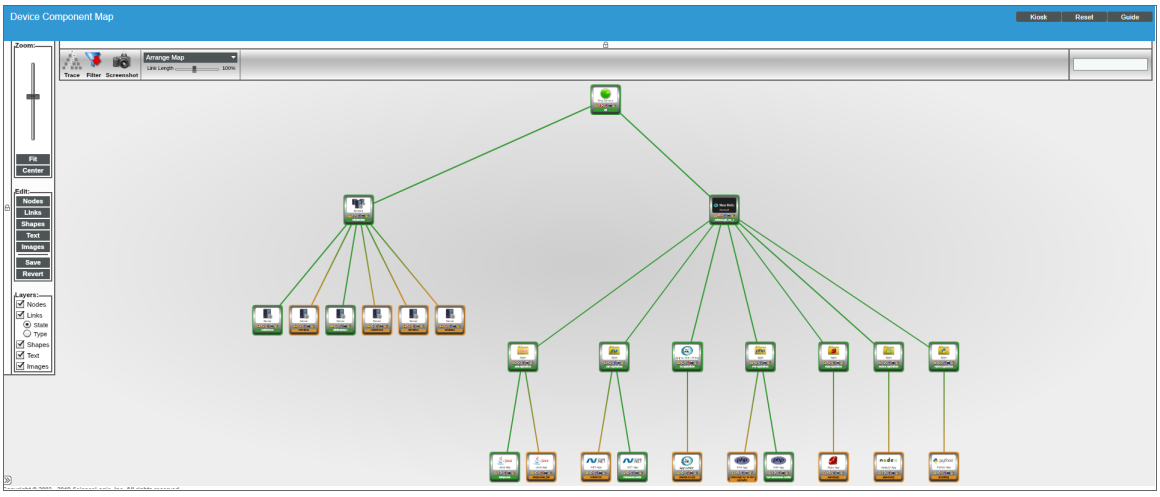
- The **Device View** modal page (click the bar-graph icon [ ] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-click to select any listed device. This reloads the page to make the selected device the primary device:



- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a New Relic service, find the service and click its plus icon (+):



- The **Component Map** page (Views > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a New Relic service, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Chapter 3

New Relic Dashboards

Overview

The following section describes the device dashboards that are included in the *New Relic: APM* PowerPack:

Device Dashboards ***14***

New Relic: APM Application *15*

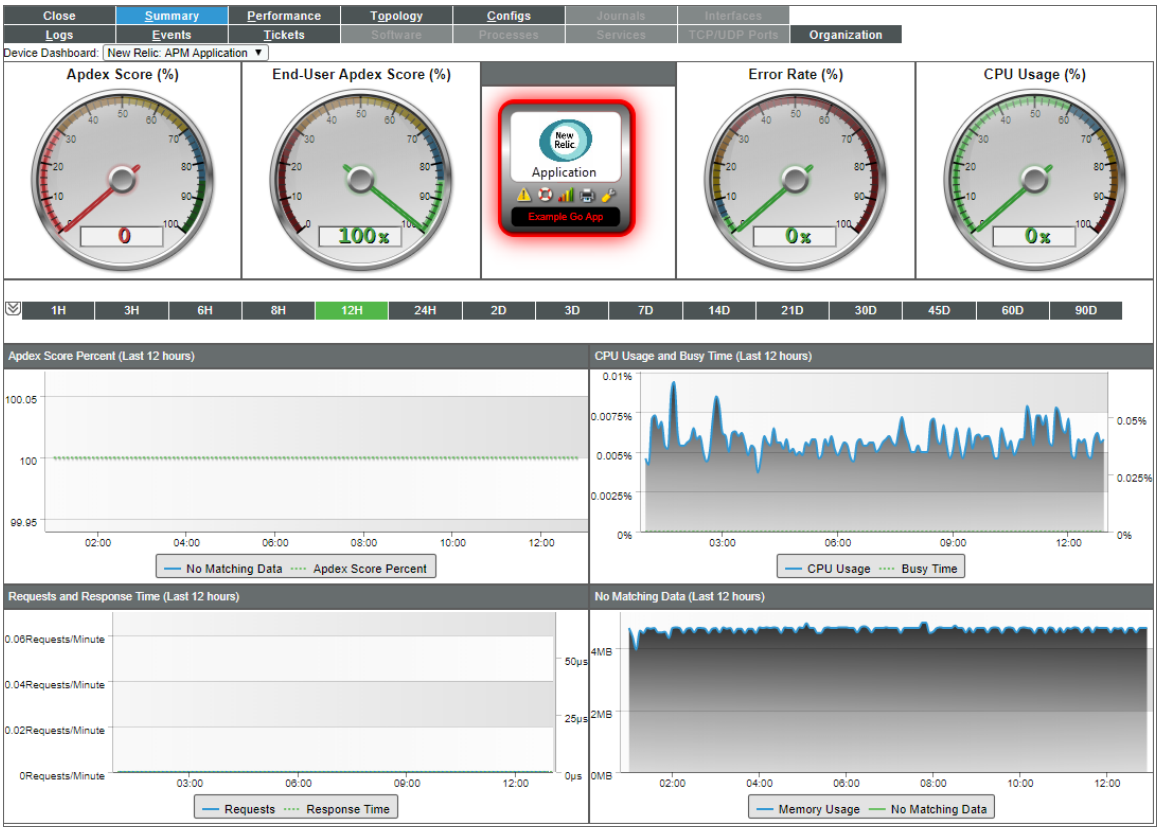
New Relic: APM Applications Group *16*

New Relic: APM Server *17*

Device Dashboards

The *New Relic: APM* PowerPack includes device dashboards that provide summary information for New Relic applications and applications groups.

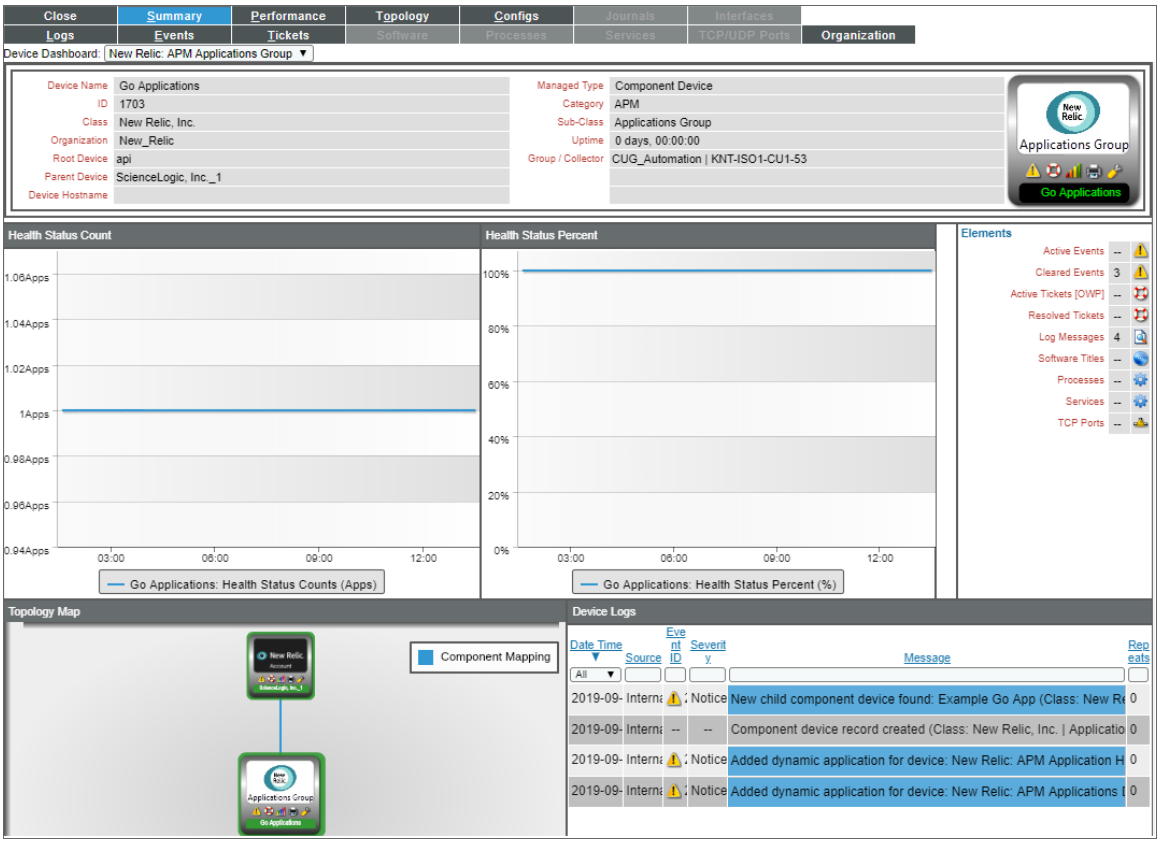
New Relic: APM Application



The New Relic: APM Application device dashboard displays the following information:

- Apdex Score
- End-User Apdex Score
- Error Rate
- CPU Usage
- Apdex Score Percent over a period of time
- CPU Usage and Busy Time over a period of time
- Requests and Response Time over a period of time
- Memory Usage over a period of time

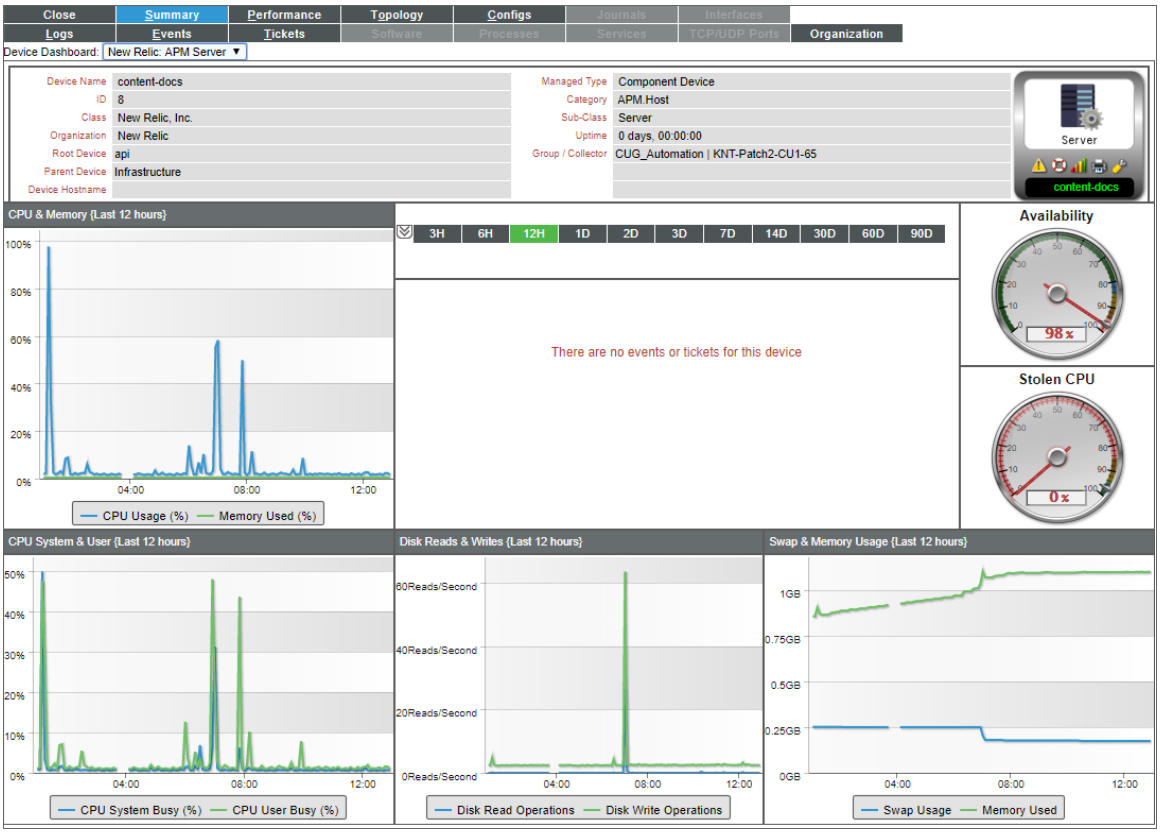
New Relic: APM Applications Group



The New Relic: APM Applications Group device dashboard displays the following information:

- Health Status Count over a period of time
- Health Status Percent over a period of time
- Topology Map
- Device Logs

New Relic: APM Server



The New Relic: APM Server device dashboard displays the following information:

- CPU and Memory over a period of time
- Events associated with the server
- Availability
- Stolen CPU
- CPU System & User over a period of time
- Disk Reads & Writes over a period of time
- Swap & Memory Usage over a period of time

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010