



PagerDuty Integration Setup

ScienceLogic Version 7.2.2.10

© 2003 - 2013, 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™
- Dynamic Component Mapping™

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

Table of Contents

Introduction	5
Overview	5
Who Should Read This Manual?	5
Prerequisites	5
Integration Steps	5
Create PagerDuty Service	8
Overview	8
Add Service	8
Importing the PagerDuty Power-Pack.....	12
Overview	12
Installation	12
Configure Credential.....	13
Configure Run Book Automation Policies	15
Overview	15
Run Book Actions	15
Automation Policies.....	16
Using PagerDuty Integration.....	22
Event Synchronization.....	Error! Bookmark not defined.
Workability.....	Error! Bookmark not defined.

Chapter

1

Introduction

Overview

This document is designed to help administrators integrate ScienceLogic EM7 management system with the PagerDuty Incident Management SaaS service. This chapter will help prepare you for the integration tasks.

Who Should Read This Manual?

Any EM7 administrator who wants to integrate with PagerDuty should read this manual. This manual might also be helpful for EM7 users who want to understand how PagerDuty integration works.

Prerequisites

- Requires PagerDuty service account
- Requires ScienceLogic EM7 7.2.2.x or better
- Requires administrative accounts for both products

Integration Steps

To integrate PagerDuty with ScienceLogic the following steps will be required.

- Create PagerDuty API Service
- Import PagerDuty Power-Pack into ScienceLogic system
- Create credential for PagerDuty API
- Align ScienceLogic Run Book Automation policies
- Advanced Integration (optional)

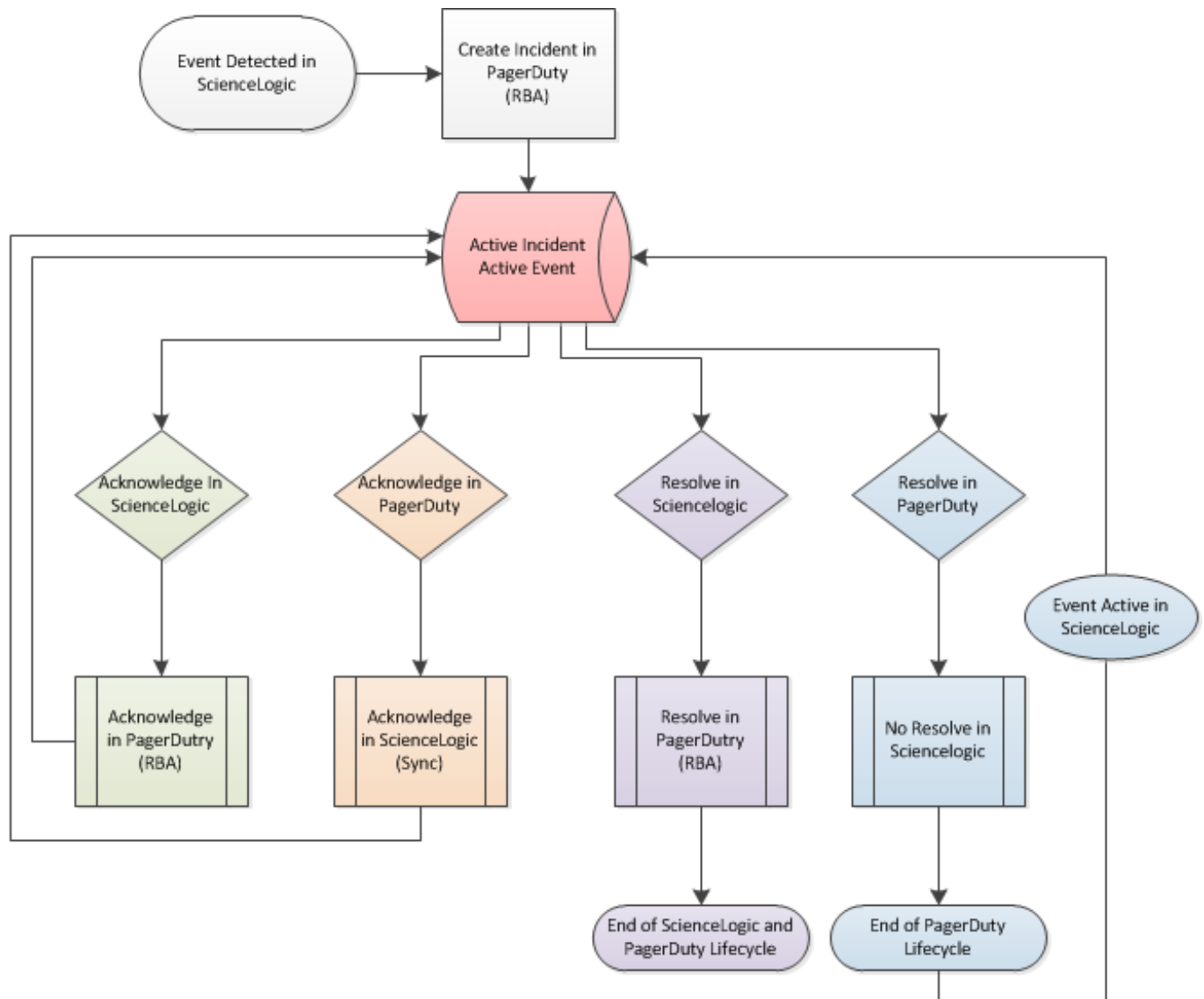
It is recommended that you familiarize yourself with the ScienceLogic Run Book Automation (RBA) functionality before activating the PagerDuty Power-Pack. The default PagerDuty RBA policies are very broad and will create new PagerDuty incidents for every event in ScienceLogic that is of severity minor, major, and critical.

Understanding the ScienceLogic PagerDuty Integration

The ScienceLogic PagerDuty integration Power-Pack offers several key functions areas:

1. Run Book Automation policies to trigger, resolve, and acknowledge events from ScienceLogic to PagerDuty
2. Dynamic Application to collect PagerDuty performance metrics, and synchronize incidents acknowledged from PagerDuty.
3. PagerDuty performance KPI dashboard with historical dynamic trending.
4. PagerDuty example credentials for both Run Book Actions and Dynamic Applications
5. PagerDuty device classes and icons for both Pingable and Virtual devices.

The PagerDuty integration relies on Run Book Automation policies to “push” both events and related event actions to PagerDuty. Activities emanating from PagerDuty, for instance acknowledging an incident, are synchronized through a Dynamic Application. The below diagram shows the dataflow for how ScienceLogic events and PagerDuty incidents are synchronized.



Incidents resolved in the PagerDuty will not automatically resolve events in ScienceLogic. This is because most events in ScienceLogic will automatically resolve themselves if they are no longer active or detected. For instance, if a monitored device is detected as being unavailable, ScienceLogic will create an event, and then create an incident in PagerDuty. If the incident in PagerDuty is resolved but the device is still detected as being unavailable, ScienceLogic will automatically create another event and PagerDuty incident. However if the incident is resolved in PagerDuty, but the event still remains in ScienceLogic, duplicate events will be suppressed. Once the event is no longer valid, ScienceLogic will automatically resolve the event and update the incident in PagerDuty.

Chapter

2

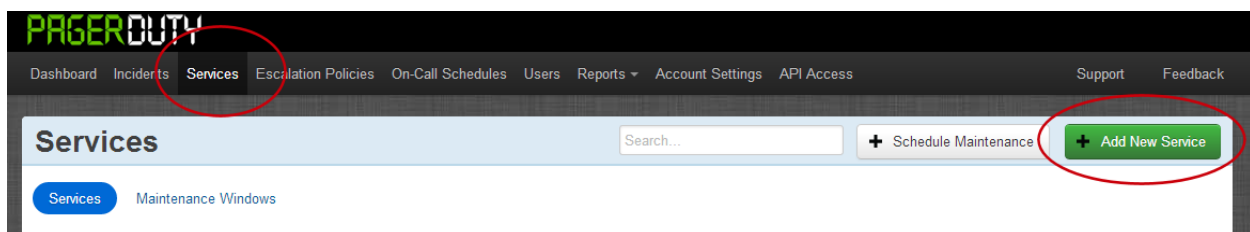
Configure PagerDuty

Overview

In this chapter we will create a PagerDuty “Generic API” service in the PagerDuty web portal for the ScienceLogic Run Book Automation integration. We will also add an API access key for ScienceLogic Dynamic Application performance and synchronization. Both steps will require you record the “key” to add to the respective ScienceLogic credential. You will need administrative access to your PagerDuty account.

Add API Service (for Run Book Automation)

Login in to your PagerDuty portal using an administrator account. Click on the “Services” navigation menu at the top of the page, and then click on the “Add New Service” button.



Enter a “service name” (in our example we used ScienceLogic Notifications), and then select “Generic API system”. Once done, click the “Add Service” button.

PAGERDUTY

Dashboard Incidents **Services** Escalation Policies On-Call Schedules Users Reports Account Settings API Access

Add a Service

Service Details

Services are used to integrate your monitoring tools with the PagerDuty alerting system.

Service name
Enter a descriptive name for the service. Eg. "Nagios host checks" or "DB Servers".

Escalation policy
The policy specifies **who will be alerted** when faults are reported by your monitoring tool.

Service Type ?

- ☐ Generic email system
Any system that can be configured to send email.
- ☒ Generic API system
Any system that can be configured to make an HTTP API call.
- ☐ Cloudkick
The Cloudkick cloud server monitoring system.
- ☐ Keynote
The Keynote web and mobile performance monitoring system.
- ☐ Nagios
The Nagios network and infrastructure monitoring system.
- ☐ Pingdom
The Pingdom uptime monitoring system.
- ☐ Server Density
The Server Density server monitoring system.
- ☐ SQL Monitor
The Red Gate SQL Monitor database monitoring system.

Copy the "Service API Key", as this will be needed for the ScienceLogic Run Book Automation credential.

PAGERDUTY

Dashboard
Incidents
Services
Escalation Policies
On-Call Schedules
Users
Reports
Account Settings
API Access

Service: ScienceLogic Notifications

Edit this service
Delete this service
Manually open a new incident

Currently Active

In Progress

No maintenance windows currently in progress.

Upcoming

No maintenance windows scheduled in the future.

Schedule new maintenance

Disable this service

1-Click Immediate Maintenance

5 min15 min30 min60 min

API integration guide

Click here to access the documentation for the PagerDuty integration API.

0 Triggered

General Settings

Service name	ScienceLogic Notifications
Enabled	Yes
Escalation policy	Default

Integration Settings

Service type	Generic API view PagerDuty API documentation
Service API key	85ec93fdfe4e46cbbfc3c2d6d20699cd

Incident Settings

Incident ack timeout	Enabled: Acknowledged incidents time out after 30 minutes
Incident auto-resolution	Enabled: Open incidents will auto-resolve in 4 hours

Incidents

Resolve
Acknowledge
Reassign

	#	Opened On	Status
No open in			

First
Previous
Page 1 of 1
Next
Last

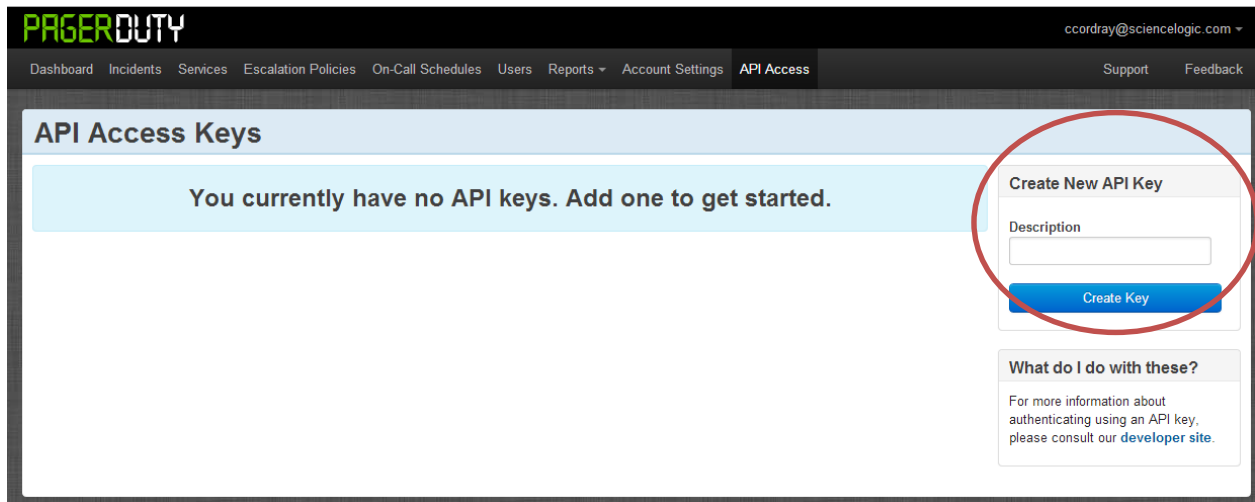
For your records, record the PagerDuty Service API key:

Service API Key: _____

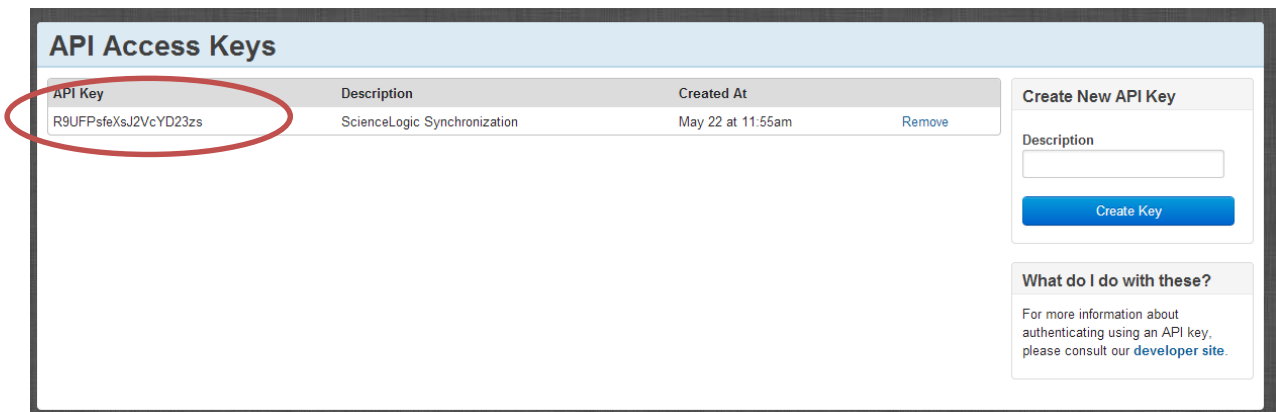
10

Add API Access Key (for Dynamic Application)

Login in to your PagerDuty portal using an administrator account. Click on the "API Access" on the navigation menu at the top of the page. If there is no API Access Keys defined, create a new key. Add a description for the key, for instance ScienceLogic Synchronization, and then select the "Create Key" button.



When complete, copy the API key for use with the ScienceLogic Dynamic Application Credential.



For your records, record the PagerDuty API Access Key:

API Access Key: _____

Chapter 3

Importing the PagerDuty Power-Pack

Overview

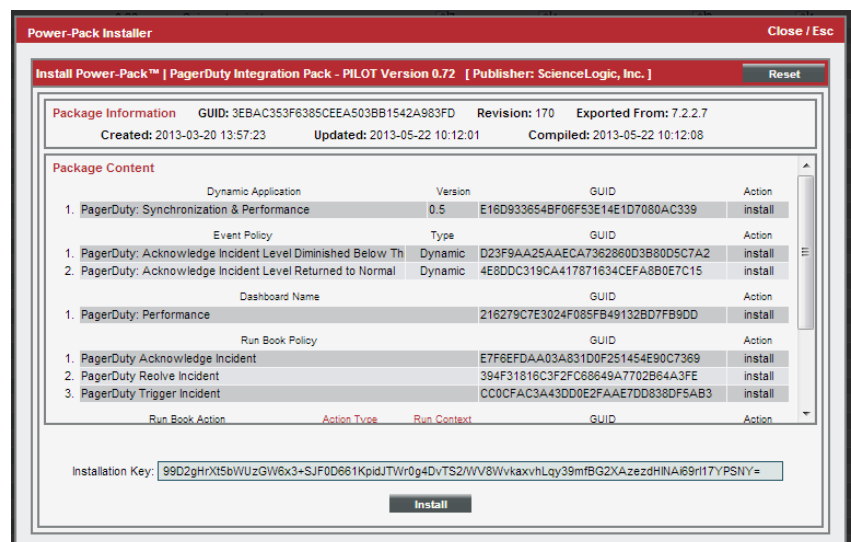
In this chapter we will install the PagerDuty Power-Pack and then configure both the Run Book Automation credential and the Dynamic Application credential.

Installation

Obtain the latest copy of the “PagerDuty Integration” Power-Pack. In this document we will be using version 0.7.x of the Power-Pack.

Using normal Power-Pack installation procedures, got the System tab, select Manage\Power-Packs, and then select the Action button, and select “Import Power-Pack” Locate the Power-Pack file, and then select the Import button.

Click install to begin the import process. Once the Power-Pack is installed, proceed to the next section to configure the credential.



Configure RBA Credential

With the Power-Pack installed, we can now configure our Run Book Automation credential. Navigate to the System tab, select Manage\Credentials. Locate the "PagerDuty RBA Credential" credential and then check on the wrench to edit it. In the "Username" field, enter the PagerDuty "Service API Key" you copied from the previous chapter. Click the Save button to update the credential, or use the Save As button to create a new credential.

The screenshot shows the 'Credential Editor [60]' window. The title bar is red with 'Close / Esc' on the right. Below the title bar is a red bar with 'Edit Basic/Snippet Credential #60' and 'New' and 'Reset' buttons. The main area is titled 'Basic Settings' and contains the following fields:

- Credential Name: PagerDuty RBA Credential
- Hostname/IP: events.pagerduty.com
- Port: 443
- Timeout(ms): 5000
- Username: 85ec93fdfe4e46cbbfc3c2d6d20699cd (circled in blue)
- Password: (empty field)

At the bottom of the window are 'Save' and 'Save As' buttons.

Configure Dynamic Application Credential

The Dynamic Application credential is needed if you wish to synchronize incident changes from PagerDuty to ScienceLogic. Navigate to the System tab and select Manage\Credentials. Locate the "PagerDuty DA Credential" credential and then check on the wrench to edit it.

In the "Username" field, enter the PagerDuty "API Access Key" you copied from the previous chapter. In the Hostname field, add the URL of our PagerDuty account, for instance: <http://mycompany.pagerduty.com>. This should be the same account that you use to access your PagerDuty administration interface. Click the Save button to update the credential, or use the Save As button to create a new credential.

Credential Editor [61] Close / Esc

Edit Basic/Snippet Credential #61 New Reset

Basic Settings

Credential Name		
PagerDuty DA Credential		
Hostname/IP	Port	Timeout(ms)
https://sciencellogic.pagerduty.com	443	5000
Username		Password
R9UFPsfeXsJ2VcYD23zs		

Save Save As

Chapter

4

Configure Run Book Automation Policies

Overview

In this chapter we will configure the PagerDuty Run Book Automation Policy, aligning the credential, and begin sending events to PagerDuty. The Run Book Automation policies provided by ScienceLogic will create outbound incidents in PagerDuty.

Run Book Actions

Navigate to the Run Book Actions page by clicking on Registry tab, then Run Book, and then Actions. You will notice three PagerDuty actions.

1. PagerDuty Trigger Incident
2. PagerDuty Acknowledge Incident
3. PagerDuty Resolve Incident

Each of these actions performs a different function and allows you to align different Automation policies based on your business needs. To configure these actions, we must manually edit each and align the proper PagerDuty credential that contains the PagerDuty API key.

Edit each Action by clicking on the yellow wrench, then select the PagerDuty Credential, then select Save.

Action Editor Close / Esc

Policy Editor | Editing Action [9] Reset

Action Name PagerDuty Acknowledge Incident (acknowledge existing)	Action State [Enabled]
Description Acknowledges a PagerDuty Incident	
Organization [System]	Action Type Run a Snippet
Snippet Credential PagerDuty RBA Credential	Action Run Context [Database]
Snippet Code <pre>import urllib2, urllib, json logger=em7_snippets.logger(filename='/data/tmp/pagerduty_trigger.log') app_name = 'PagerDuty Acknowledge Incident (Ack Existing)' def submit_json_request(json_request): target_url = 'https://events.pagerduty.com/generic/2010-04-15/create_event.json'</pre>	

Save

Note: PagerDuty Actions must run on the ScienceLogic Database, double check that the Action Run Context is set to Database.

Once complete, lets double check the PagerDuty Automation Policies.

Automation Policies

Like the PagerDuty Run Book Actions, there are three Automation Policies. Each Automation Policy performs a different task based on criteria established in the Policy. By default the PagerDuty Automation Policies are very broad, allowing every ScienceLogic event that has a severity higher than or equal to "minor" to trigger a PagerDuty incident. Although this may be good to begin testing your PagerDuty integration, it is advised to adjust each PagerDuty Automation policy to meet the needs of your business.

Navigate to the Run Book Automation page by clicking on Registry tab, then Run Book, and then Automation. You will notice three PagerDuty actions.

Click the yellow wrench for each policy to edit it. Note that the default policies work against all devices, in all organizations. Make sure the matching RBA Action is aligned. When complete making changes, click the Save button. With all Automation Policies validated, we can now proceed to the next chapter.

Science Logic - Management Platform - Google Chrome

192.168.2.22/em7/index.em7?exec=registry_policies_automation_editor&policy_id=2

Automation Policy Editor | Editing Automation Policy [2] Reset

Policy Name: PagerDuty Trigger Incident

Policy Type: [Active]

Policy State: [Enabled]

Organization: [System]

Criteria Logic: [Severity >=] [Minor,]

Match Logic: [Text search]

Match Syntax:

Repeat Time: [Only once]

Align With: [Devices]

☐ Include events for entities other than devices (organizations, assets, etc.)

Available Devices:

- System
- Cisco Systems: Unity Connection: CUC1.cisco.local
- D-Link: DGS-1224T: switch-001
- Generic: SNMP: HP94D6D1

Aligned Devices: (All devices)

Available Events:

- Critical: AKCP: AC Voltage sensor detects no current
- Critical: AKCP: DC Voltage sensor High Critical
- Critical: AKCP: DC Voltage sensor Low Critical
- Critical: AKCP: Dry Contact Sensor Low Critical

Aligned Events: (All events)

Available Actions:

- SNMP Trap: EM7 Event Trap
- Snippet: EM7 Ping Snippet
- Snippet: PagerDuty Acknowledge Incident (acknowledge ex
- Snippet: PagerDuty Resolve Incident (clear existing)

Aligned Actions:

- 1. Snippet: PagerDuty Trigger Incident (create new)

Save

Chapter

5

Configure PagerDuty Device and Dynamic Application

Overview

In this chapter we will create a PagerDuty device, and manually align the PagerDuty Synchronization and Performance Dynamic Application. The Synchronization and Performance Dynamic Application provided by ScienceLogic will provide near-real time performance data regarding your PagerDuty service, as well as synchronize changes emanating from PagerDuty.

Create PagerDuty Device

Although the PagerDuty Dynamic Application may be aligned to any ScienceLogic device, we this section will walkthrough creating a dedicated PagerDuty device. Navigate to the Discovery Console Panel by clicking on System > Manage > Discovery. Create a new discovery session to discover a pingable device, setting the IP address to the desired location. Next select "Discover Non-SNMP" devices, and when complete select Save.

Discovery Session Editor | Create New

IP and Credentials

IP Address Discovery List

50.112.113.204

Upload File

Browse for file... Browse...

SNMP Credentials

SNMP

- _COSMOS_V1
- _COSMOS_V2
- _EM7 Default V2
- _EM7 Default V3
- _LifeSize: Endpoint SNMP

Other Credentials

Basic/Snippet

- _AppCentrix PAN
- _Cisco CUC
- _Cisco Unified Communication - Ex
- _Cisco Unified Contact Center Exp
- _Cisco Unity Connection - Example

Detection and Scanning

Initial Scan Level

System Default (recommended)

Scan Throttle

System Default (recommended)

Port Scan All IPs

System Default (recommended)

Port Scan Timeout

System Default (recommended)

Detection Method & Port

[Default Method]

- UDP: 161 SNMP
- TCP: 1 - tcpmux
- TCP: 2 - compressnet
- TCP: 3 - compressnet
- TCP: 5 - rje
- TCP: 7 - echo
- TCP: 9 - discard
- TCP: 11 - systat
- TCP: 13 - daytime
- TCP: 17 - qotd
- TCP: 18 - msp

Basic Settings

Discover Non-SNMP

Model Devices

Duplication Protection

Collection Server PID:

_em7-serv

Organization

[System]

Add Devices to Device Group(s)

None

Puppet Nodes

Apply Device Template

[Choose a Template]

Save

Log All

Run the discover session by clicking on the lightning bolt icon. In the Discover Session modal, the device will be modeled as a standard Linux device.

Discovery Session | Discovery Session Complete

Refresh

Date Time	Discovery Log Message	Class Type
1. 2013-05-22 10:28:16	Auto-discovery session registered...	--
2. 2013-05-22 10:28:16	Collector is working...	--
3. 2013-05-22 10:28:16	Beginning auto-discovery session	--
4. 2013-05-22 10:28:24	50.112.113.204 (*IP) Discovered and modeled new device	Linux ICMP
5. 2013-05-22 10:28:26	Auto-discovery session completed	--

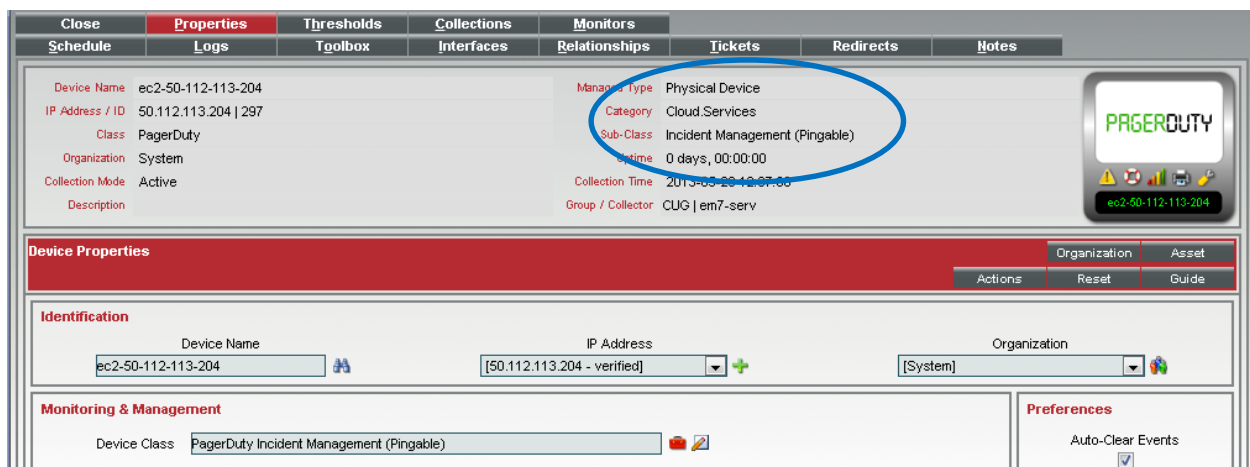
Click the device icon to edit the device properties. On the device properties page, click the red toolbox icon to change the device class. Select "PagerDuty | Incident Management (Pingable)" device class, then select Apply.

Select New Device Class

Close / Esc

- NetApp | LUN
- NetApp | Volume
- New Relic | Account
- New Relic | Application
- New Relic | Application Server
- New Relic | Ping Device
- New Relic | Virtual Device
- PagerDuty | Incident Management (Pingable)**
- PagerDuty | Incident Management (Virtual)
- PaloAlto Networks | Application
- PaloAlto Networks | Application Container
- PaloAlto Networks | Attack
- PaloAlto Networks | Attack Container
- Postgres | Postgres Server
- SolidFire | Account
- SolidFire | Accounts Container
- SolidFire | Cluster
- SolidFire | Drive
- SolidFire | Node
- SolidFire | Nodes Container

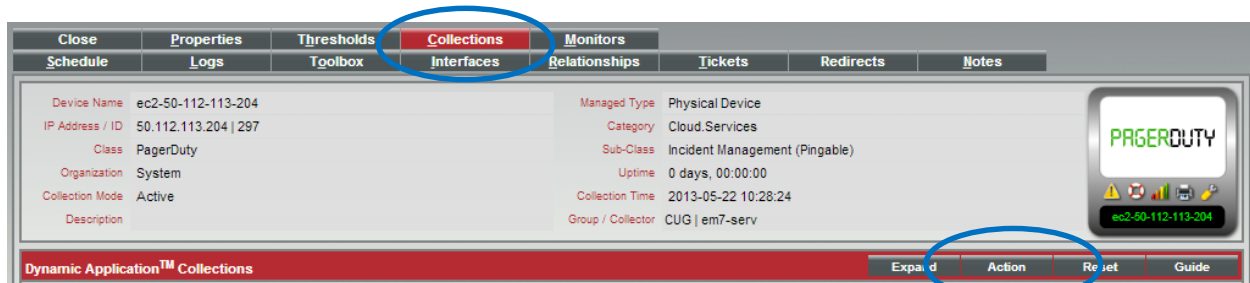
Apply



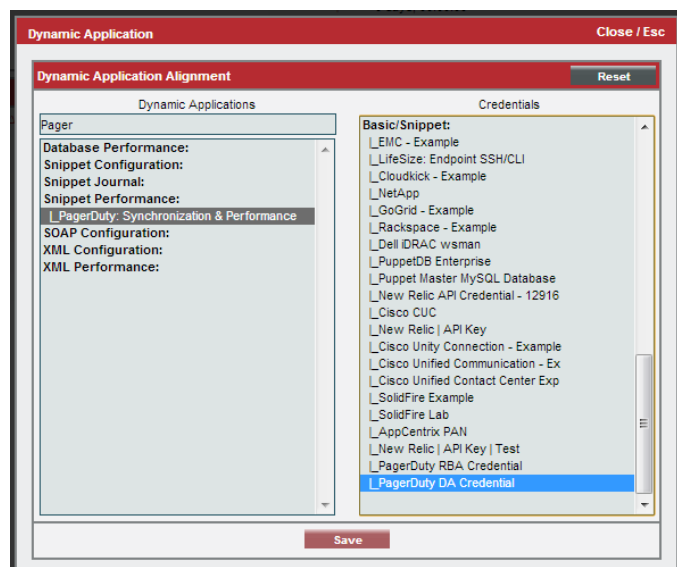
When complete the device icon and device class information will be aligned to PagerDuty.

Align Dynamic Application

To align the Pager Duty Synchronization and Performance Dynamic Application, click on the Collection tab while in the Device Properties panel.



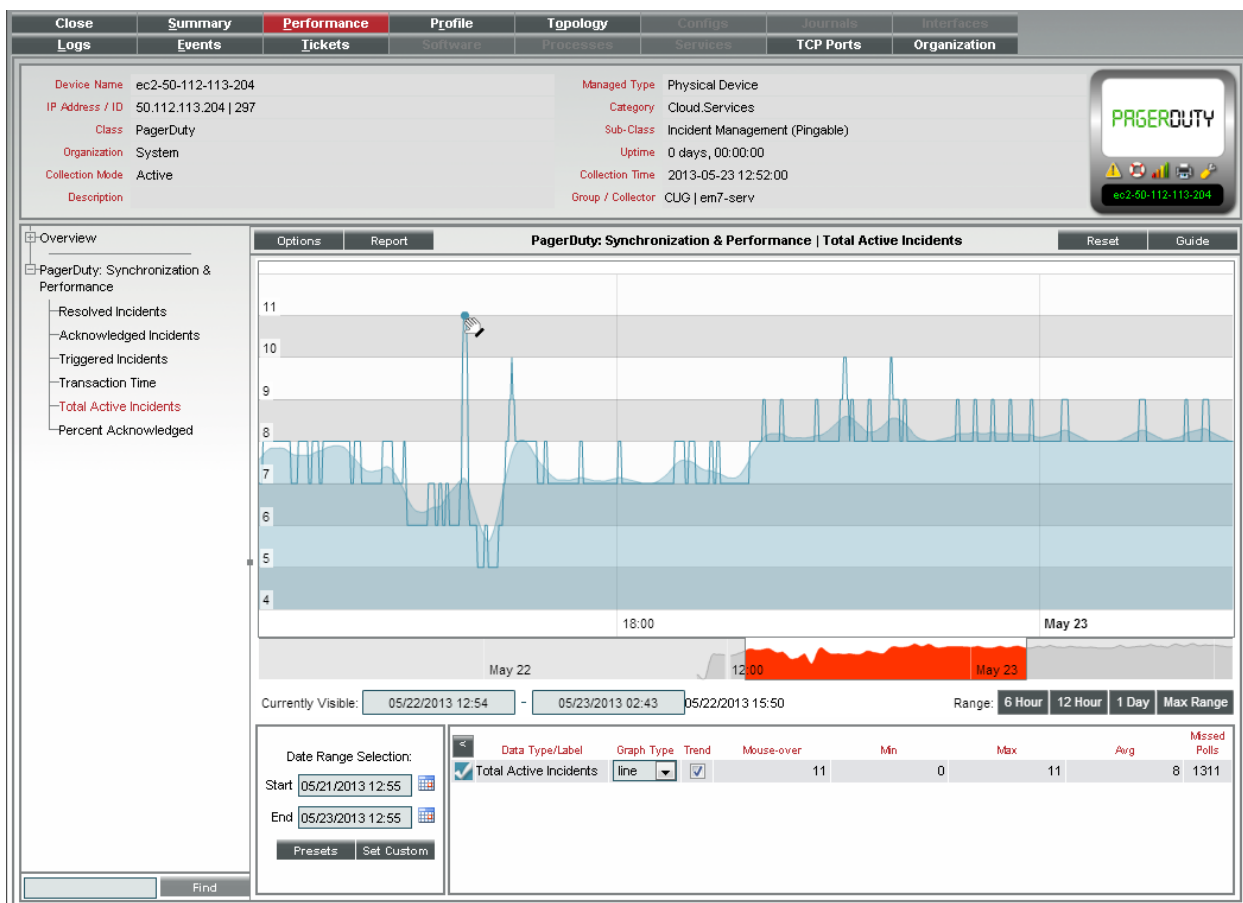
Next, select Action, then Add Dynamic Application. Type "Pager" in the search box, then Select the "PagerDuty" Synchronization & Performance" application. Select the "PagerDuty DA Credential" with the "API Access Key" you created in Chapter 3. Select the Save button to save changes.



Once aligned, the application will take about 60 seconds to populate. By default the application runs every 60 seconds looking for updates to existing ScienceLogic events and updating performance and status data.

The screenshot shows the 'Collections' tab in the ScienceLogic interface. At the top, there's a header with tabs: Close, Properties, Thresholds, Collections (selected), Monitors, Schedule, Logs, Toolbox, Interfaces, Relationships, Tickets, Redirects, and Notes. Below the header, the device information for 'ec2-50-112-113-204' is displayed, including its IP address, class (PagerDuty), organization (System), and collection mode (Active). The 'Dynamic Application™ Collections' section is expanded, showing a table of metrics. The table has columns for ID, Poll Frequency, Type, and Credential. The metrics listed are: Acknowledged Incidents, Percent Acknowledged, Resolved Incidents, Total Active Incidents, Transaction Time, and Triggered Incidents. Each metric has a 'Found' status and a 'Collecting' checkbox.

The application performance metrics will begin collecting every 60 seconds.



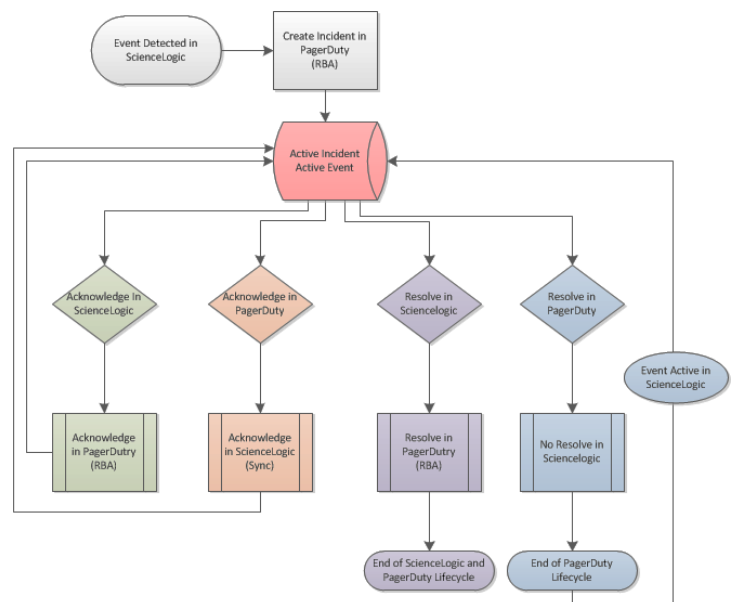
Chapter 6

Using PagerDuty Integration

Run Book (Forward Synchronization)

Every ScienceLogic event that matches the PagerDuty Run Book Automation policy will create a new PagerDuty incident. Once an incident is created, notification and escalation policies on the Pager Duty system will go into effect.

ScienceLogic's Run Book Automation integration is a forward synchronization process, meaning that events and activities emanate from the ScienceLogic system to the PagerDuty service system. Just as new ScienceLogic events will create new PagerDuty incidents, acknowledging or clearing events from within ScienceLogic's event monitor will perform the same function via the PagerDuty API.



Acknowledging incidents from the PagerDuty service portal will only update events in ScienceLogic if the PagerDuty Synchronization and Performance Dynamic Application is configured. If events are auto cleared by ScienceLogic, because either the event has timed-out or the system no-longer detects there's still a problem, events will also be automatically resolved in PagerDuty. The below example shows a ScienceLogic Event Console with several different active events:

Name	Type	Event Message	Severity	Acknowledged	Ticket	Age	Elapsed	Last Detected	EID	Source	Count	Notify
1. puppet-serv	Device	Device not responding to critical ping	Critical	☐	--	--	15 mins 35 secs	2013-03-21 15:02:51	12422	Internal	60	1
2. win2k8-64bit-89	Device	Device not responding to critical ping	Critical	☐	--	--	15 mins 35 secs	2013-03-21 15:02:51	12421	Internal	60	1
3. CUC1.cisco.local	Device	Device Failed Availability Check: UDP - SNMP	Major	☐	--	--	10 mins 51 secs	2013-03-21 15:02:22	12423	Internal	3	1
4. hp-printer	Device	Printer black ink C4906A toner low, current level: 5% full	Minor	☐	--	--	2 mins 52 secs	2013-03-21 15:00:21	12431	Dynamic	1	1
5. lin-serv	Device	Network latency exceeded threshold: 135.96 ms	Minor	☐	--	--	51 secs	2013-03-21 15:02:22	12433	Internal	1	1
6. WIN-SERV	Device	Network latency exceeded threshold: 125.63 ms	Minor	☐	--	--	51 secs	2013-03-21 15:02:22	12434	Internal	1	1
7. E3300	Device	Network Latency below threshold	Healthy	☐	--	--	10 mins 51 secs	2013-03-21 14:52:22	12430	Internal	1	--

The same events are synchronized in PagerDuty as triggered incidents:

#	Opened On	Status	Incident Details	Service	Assigned To	Details
136	Mar 21 at 3:02pm	triggered	Failure: MINOR: WIN-SERV: Network latency exceeded threshold: 125.63 ms. (View message)	ScienceLogic Notifications	Chris	Details
135	Mar 21 at 3:02pm	triggered	Failure: MINOR: lin-serv: Network latency exceeded threshold: 135.96 ms. (View message)	ScienceLogic Notifications	Chris	Details
134	Mar 21 at 3:00pm	triggered	Failure: MINOR: hp-printer: Printer black ink C4906A toner low, current level: 5% full (View message)	ScienceLogic Notifications	Chris	Details
133	Mar 21 at 2:52pm	triggered	Failure: MAJOR: CUC1.cisco.local: Device Failed Availability Check: UDP - SNMP (View message)	ScienceLogic Notifications	Chris	Details
132	Mar 21 at 2:47pm	triggered	Failure: CRITICAL: puppet-serv: Device not responding to critical ping (View message)	ScienceLogic Notifications	Chris	Details
131	Mar 21 at 2:47pm	triggered	Failure: CRITICAL: win2k8-64bit-89: Device not responding to critical ping (View message)	ScienceLogic Notifications	Chris	Details

Note: For this example all events are creating incidents in PagerDuty, which is a function of the ScienceLogic Run Book Automation policy and can be adjusted to meet the needs of your business.

Since PagerDuty requires a unique incident ID to de-duplicate events, ScienceLogic uses the device ID, called the DID, to help eliminate duplicate event storms for a single device. If a device has multiple events, the parent event (usually the highest severity event) will be used for the PagerDuty incident. If subsequent events appear after the initial event correlation process by ScienceLogic (usually time based), the new event will update the PagerDuty incident with the new description. In PagerDuty we can see the primary "critical" event for device "puppet-serv":

Incidents

Manually open a new incident

Your open incidents

4 triggered0 acknowledged

All open incidents

4 triggered0 acknowledged

Resolve

Acknowledge

Reassign

Go to Incident #

Show: All (137) | All open (4) | Triggered (4) | Acknowledged (0) | Resolved (133)

#	Opened On	Status	Incident Details	Service	Assigned To	
134	Mar 21 at 3:00pm	triggered	Failure: MINOR: hp-printer: Printer black ink C4906A toner low, current level: 5% full (View message)	ScienceLogic Notifications	Chris	Details
133	Mar 21 at 2:52pm	triggered	Failure: MAJOR: CUC1.cisco.local: Device Failed Availability Check: UDP - SNMP (View message)	ScienceLogic Notifications	Chris	Details
132	Mar 21 at 2:47pm	triggered	Failure: CRITICAL: puppet-srv: Device not responding to critical ping (View message)	ScienceLogic Notifications	Chris	Details
131	Mar 21 at 2:47pm	triggered	Failure: CRITICAL: win2k8-64bit-89: Device not responding to critical ping (View message)	ScienceLogic Notifications	Chris	Details

First

Previous

Page 1 of 1

Next

Last

Show 10 incidents per page

In ScienceLogic we can see several events for device “puppet-serv”:

Science Logic - Management Platform - Google Chrome

192.168.2.22/em7/index.em7?exec=device_summary&did=54

Close	Summary	Performance	Profile	Topology	Configs	Journals	Interfaces			
Logs	Events	Tickets	Software	Processes	Services	TCP Ports	Organization			
Device Name: puppet-serv IP Address / ID: 192.168.2.88 / 54 Class: Puppet Labs Organization: System Collection Mode: Unavailable Description: "Puppet Master"				Managed Type: Physical Device Category: Servers Sub-Class: PuppetDB Uptime: 8 days, 18:48:01 Collection Time: 2013-03-20 03:25:00 Group / Collector: CUG / em7-serv						
Vitals [Current] Device Rating: 1 Overall Health: Critical Availability: Critical Latency: 0.0000 ms. Vitals [Average] Avail. (24 Hr): 0% Latency (24 Hr): 0.00 ms.		Tickets and Events 1. Device not responding to critical ping 2. Device Failed Availability Check: UDP - SNMP 3. Network latency exceeded threshold: No Response			Elements Active Events: 3 Cleared Events: 215 Active Tickets [OWP]: -- Resolved Tickets: -- Log Messages: 2,358 Software Titles: 871 Processes: 125 Services: --					
Monitors / (Root): 8.000% /boot: 14.000% /home: 0.000%		System Component Utilization 								
Hourly Interface Usage In [Kbps] [eth0] 00:0C:29:FA:59:90 192.168.2.88 No interface data could be found for this interface.										

Copyright © 2003 - 2013 ScienceLogic, Inc. All rights reserved.

When events are acknowledged in ScienceLogic, the acknowledged status will be synchronized to PagerDuty. This process can take up to 60 seconds.

Organization		Contact Information		Severity			
System		Reston VA ScienceLogic Support (703)-354-1010		0 Healthy 1 Notice 3 Minor 1 Major 2 Critical			
Name	Type	Event Message	Severity	Acknowledged	Ticket	Age / Elapsed	
1. puppet-serv	Device	Device not responding to critical ping	Critical	☒	--	1 hr 8 mins	
2. win2k8-64bit-89	Device	Device not responding to critical ping	Critical	☒	--	1 hr 8 mins	
3. CUC1.cisco.local	Device	Device Failed Availability Check: UDP - SNMP	Major	☒ em7admin	--	1 hr 4 mins	
4. hp-printer	Device	Printer black ink C4906A toner low, current level: 5% full	Minor	☒	--	56 mins 7 secs	
5. HP94D6D1	Device	Network latency exceeded threshold: 100.97 ms.	Minor	☒	--	4 mins 7 secs	
6. ZYWALL-01	Device	Network latency exceeded threshold: 107.17 ms.	Minor	☒	--	4 mins 7 secs	
7. chris-work-pc	Device	Device reporting incomplete filesystem information	Notice	☒	--	2 hrs 11 mins	

Once synchronized the status of the PagerDuty incident is updated. Resolving an event in the ScienceLogic event monitor also updates the status of the Incident in PagerDuty.

139	Mar 21 at 3:52pm	triggered	Failure: MINOR: HP94D6D1: Network latency exceeded threshold: 100.97 ms. (View message 🔗)	ScienceLogic Notifications
138	Mar 21 at 3:52pm	triggered	Failure: MINOR: ZYWALL-01: Network latency exceeded threshold: 107.17 ms. (View message 🔗)	ScienceLogic Notifications
134	Mar 21 at 3:00pm	triggered	Failure: MINOR: hp-printer: Printer black ink C4906A toner low, current level: 5% full (View message 🔗)	ScienceLogic Notifications
133	Mar 21 at 2:52pm	acknowledged	Failure: MAJOR: CUC1.cisco.local: Device Failed Availability Check: UDP - SNMP (View message 🔗)	ScienceLogic Notifications
132	Mar 21 at 2:47pm	triggered	Failure: CRITICAL: puppet-serv: Device not responding to critical ping (View message 🔗)	ScienceLogic Notifications
131	Mar 21 at 2:47pm	triggered	Failure: CRITICAL: win2k8-64bit-89: Device not responding to critical ping (View message 🔗)	ScienceLogic Notifications

Note the below event which once resolved is also cleared in PagerDuty.

Organization		Contact Information		Severity			
System		Reston VA ScienceLogic Support (703)-354-1010		2 Healthy 1 Notice 3 Minor 1 Major			
Name	Type	Event Message	Severity	Acknowledged	Ticket	Age	
1. puppet-serv	Device	Device not responding to critical ping	Critical	☒	--	1 hr 1	
2. win2k8-64bit-89	Device	Device not responding to critical ping	Critical	☒	--	1 hr 1	
3. CUC1.cisco.local	Device	Device Failed Availability Check: UDP - SNMP	Major	☒ em7admin	--	1 hr 7	
4. E3000	Device	Network latency exceeded threshold: 115.77 ms.	Minor	☒	--	2 mins	
5. hp-printer	Device	Printer black ink C4906A toner low, current level: 5% full	Minor	☒	--	59 min	
6. lubu-serv	Device	Network latency exceeded threshold: 110.41 ms.	Minor	☒	--	2 mins	
7. chris-work-pc	Device	Device reporting incomplete filesystem information	Notice	☒	--	2 hrs	
8. HP94D6D1	Device	Network Latency below threshold	Healthy	☒	--	2 mins	
9. ZYWALL-01	Device	Network Latency below threshold	Healthy	☒	--	2 mins	

In PagerDuty, the incident is removed, but can be found by clicking the "Resolved" link.

Your open incidents				All open incidents			
4 triggered 1 acknowledged				4 triggered 1 acknowledged			
Resolve	Acknowledge	Reassign	Go to incident #	Show: All (141) All open (5) Triggered (4) Acknowledged (1) Resolved (136)			
#	Opened On	Status	Incident Details	Service	Assigned To		
139	Mar 21 at 3:52pm	resolved	Failure: MINOR: HP94D6D1: Network latency exceeded threshold: 100.97 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
138	Mar 21 at 3:52pm	resolved	Failure: MINOR: ZYWALL-01: Network latency exceeded threshold: 107.17 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
137	Mar 21 at 3:27pm	resolved	Failure: MINOR: ZYWALL-01: Network latency exceeded threshold: 109.1 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
136	Mar 21 at 3:02pm	resolved	Failure: MINOR: WIN-SERV: Network latency exceeded threshold: 125.63 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
135	Mar 21 at 3:02pm	resolved	Failure: MINOR: lin-serv: Network latency exceeded threshold: 135.96 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
134	Mar 21 at 3:00pm	resolved	Failure: MINOR: hp-printer: Printer black ink C4906A toner low, current level: 5% full (View message 🔗)	ScienceLogic Notifications	--		Details
130	Mar 21 at 2:47pm	resolved	Failure: MINOR: E3000: Network latency exceeded threshold: 106.63 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
129	Mar 21 at 2:42pm	resolved	Failure: MINOR: lin-serv: Network latency exceeded threshold: 102.48 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
128	Mar 21 at 2:37pm	resolved	Failure: MINOR: HP94D6D1: Network latency exceeded threshold: 102.33 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
127	Mar 21 at 2:22pm	resolved	Failure: MINOR: WIN-SERV: Network latency exceeded threshold: 105.95 ms. (View message 🔗)	ScienceLogic Notifications	--		Details
First Previous Page 1 of 14 Next Last				Show 10 incidents per page			

Acknowledging in PagerDuty (Reverse Synchronization)

Incidents that are acknowledged in the PagerDuty portal or Smart Phone applications will synchronize back to ScienceLogic if the PagerDuty Dynamic Application has been installed.

The screenshot shows the PagerDuty Incidents dashboard. At the top, there are tabs for Dashboard, Incidents, Services, Escalation Policies, On-Call Schedules, Users, Reports, Account Settings, and API Access. The Incidents tab is active, showing a summary of 6 triggered and 1 acknowledged incidents. Below this, there are filters for Open (7), Triggered (6), Acknowledged (1), and All (7). A table of incidents is displayed, with incident #762 circled in red. The incident details for #762 are: Created On: May 22 at 10:58, Details: Failure: CRITICAL: puppet-srv: Device not responding to critical ping, Service: ScienceLogic Notifications, Assigned To: ccdray, Status: Acknowledged.

By default, synchronization can take up to 60 seconds, however users can change the frequency by editing the Dynamic Application properties. In order to maintain continuity of user assignment, ScienceLogic matches the PagerDuty assigned username to the ScienceLogic username. If there is a match ScienceLogic events will be updated to matching PagerDuty incidents. If no username can be found, no updates will be made.

For instance, if the username in ScienceLogic is "jdoe", the same username must exist in PagerDuty for the reverse synchronization process to update events in ScienceLogic. The primary reason for this is because of ScienceLogic uses advanced auditing and change control process that must know which user account is acknowledging events.

The screenshot shows the PagerDuty mobile app interface. It displays a 'Triggered' incident assigned to 'Ian Enders' with a status of 'Acknowledged'. The incident log shows a notification sent to Ian Enders by push notification to iPhone.

The screenshot shows the ScienceLogic Event Console. The interface displays a list of events with columns for Item, Type, Event Details, Severity, and Last Detected. Event #762 is highlighted with a red circle and has a severity of 'Critical'.

PagerDuty Interface

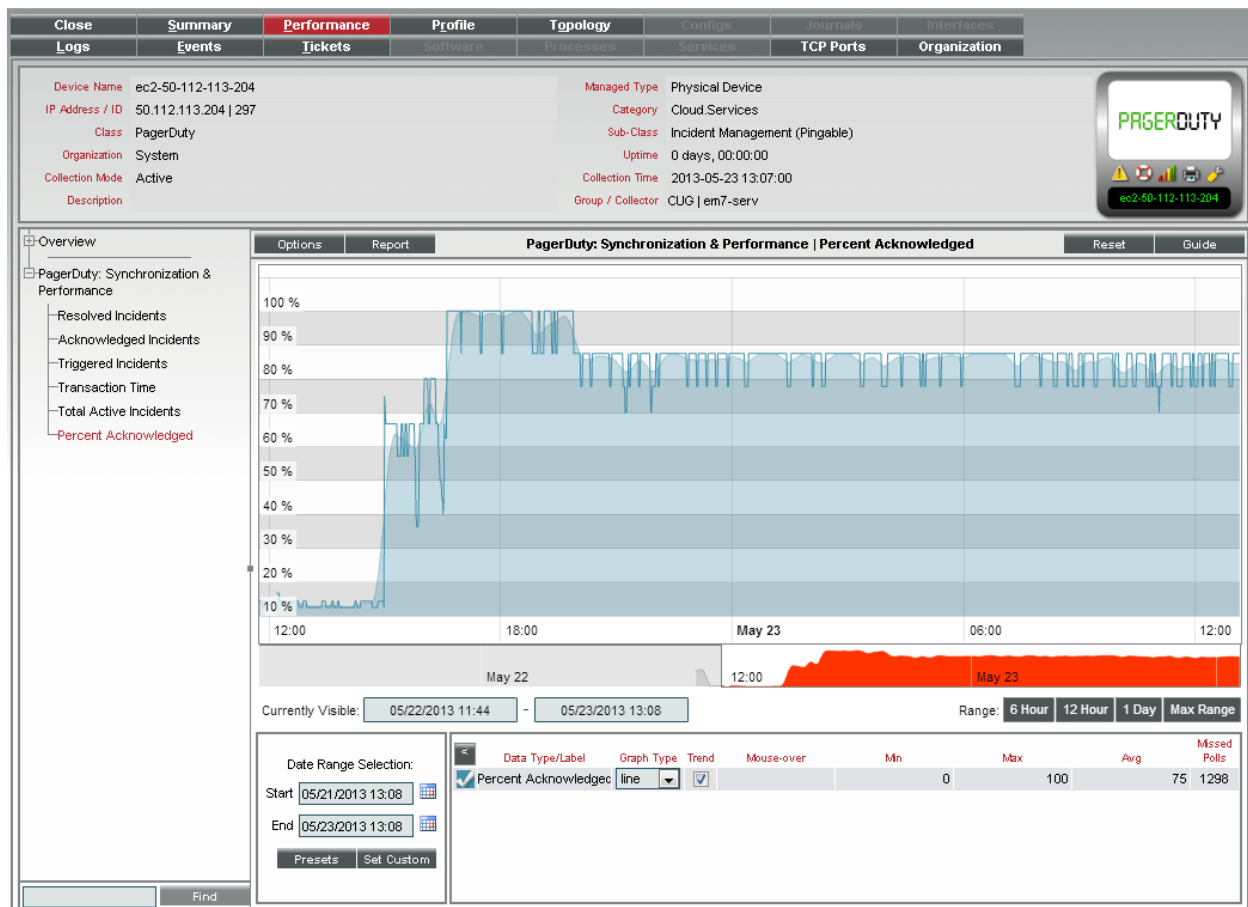
In PagerDuty, any ScienceLogic created incident will have additional notes and details about the event. The details include information about the device, including the last occurrence, severity, and IP address. Users can also navigate from PagerDuty to ScienceLogic by clicking the Client URL link.

	762	May 22 at 10:58	Failure: CRITICAL: puppet-serv: Device not responding to critical ping	ScienceLogic Notifications	ccordray	Acknowledged	Details -
Service Key							
85ec93fdfe4e46cbbfc3c2d6d20699cd							
Description							
CRITICAL: puppet-serv: Device not responding to critical ping							
Incident Key							
54							
Details							
Event Message		{ "Device": "puppet-serv", "IP Address": "192.168.2.88", "Severity": "CRITICAL", "Event": "Device not responding to critical ping", "Last Occurred": "2013-05-22 15:58:30", "First Occurred": "2013-05-22 15:58:30", "Occurrence Count": "1", "Source": "Internal" }					
Client							
ScienceLogic URL 							
View Message 							

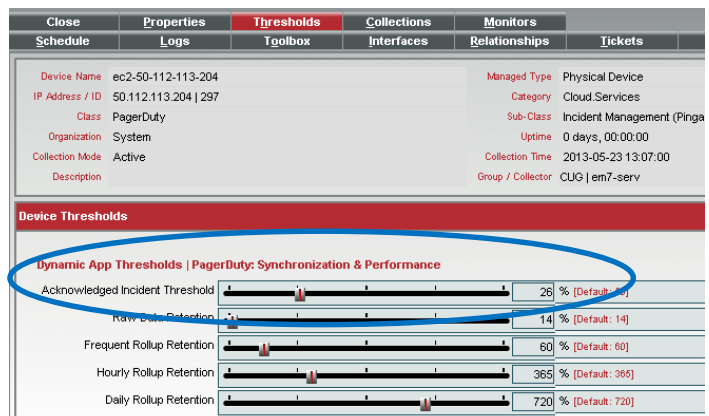
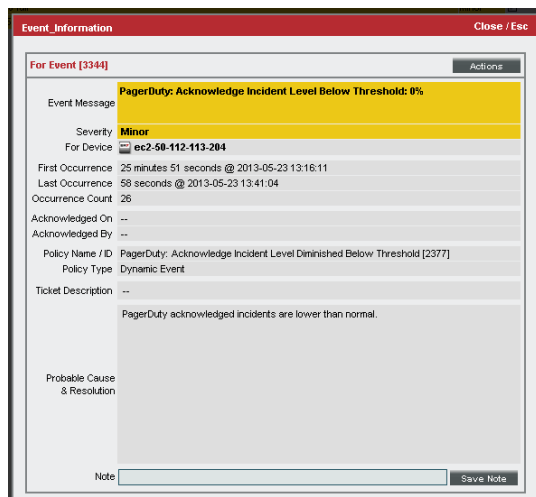
Performance Metrics and Dashboard

If the "PagerDuty Synchronization & Performance" Dynamic Application is installed, users can see several different performance metrics. Those include:

- Number of Resolved Incidents
- Number of Acknowledged Incidents
- Number of Triggered Incidents
- Transaction Time of PagerDuty API Requests
- Number of Active Incidents (Acknowledged + Triggered)
- Percentage of Acknowledged Incidents



In addition to the above performance metrics, the "Percentage of Acknowledged" metric also has an alarm threshold that can be adjusted to meet the needs of your environment. The threshold value can be set on the Device Properties > Thresholds tab.



In addition to performance metrics and alerts, the

The screenshot displays the PaperDuty dashboard, a comprehensive monitoring interface. At the top, a navigation bar includes links for Home, Dashboard, Views, Events, Tickets, Knowledge, Reports, Registry, System, and Preferences. The main dashboard area is organized into several key sections:

- PaperDuty Service Availability:** A large circular gauge on the top left indicates 100% service availability.
- PaperDuty Average Active Incidents (30 Mins):** A line chart on the top right shows a peak of 7.93 incidents.
- PaperDuty Active Incidents:** A line chart on the middle left shows a peak of 8.27 incidents.
- PaperDuty Triggered Incidents:** A line chart on the middle right shows a peak of 6.07 incidents.
- PaperDuty Percentage of Acknowledged Incidents:** A line chart on the bottom right shows 100.00% acknowledgment.
- PaperDuty Resolved Incidents:** A line chart on the bottom left shows a peak of 0.40 incidents.
- PaperDuty Transaction Time:** A line chart on the bottom middle left shows a peak of 4.70 seconds.
- PaperDuty Request Latency:** A line chart on the bottom middle right shows a peak of 91.49 ms.
- Active Events Table:** A table in the center-right lists recent events with columns for ID, Message, Operation, Status, Severity, Acknowledged, and Last Sensor Count. The table shows several events related to sensor checks and network latency.

Advanced Configuration and Troubleshooting

Audit Logging

When an event is acknowledged or resolved in ScienceLogic (event monitor or auto-clear), it runs the matching RBA policy and tells the PagerDuty API to acknowledge/resolve the matching incident. The PagerDuty API does not support any fields to indicate who acknowledged the incident; as a result API acknowledged incidents show up as "Through the API".

Although this is normal behavior, ScienceLogic also provides audit logging of who on the ScienceLogic system acknowledges or resolves an incident. This is available by navigating to the Incident Log of any incident.

PAGERDUTY

Dashboard
Incidents
Services
Escalation Policies
On-Call Schedules
Users
Reports
Account Settings
API Access

Details for: Incident #1809

Service	ScienceLogic Notifications
Current status	Resolved
Opened on	May 29 at 5:10pm
Resolved on	May 29 at 5:12pm
Opened for	2 min
Resolved by	(automatically)

Incident Log

Time	Activity
May 29, 2013 at 17:12 (less than a minute ago)	Resolved through the API. Description: Incident Cleared by user em7admin in ScienceLogic (View message)
May 29, 2013 at 17:10 (2 minutes ago)	Acknowledged through the API. Description: Incident Acknowledged by user em7admin in ScienceLogic (View message) View in ScienceLogic
May 29, 2013 at 17:10 (2 minutes ago)	Notified ccordray by email at ccordray@sciencelogic.com.
May 29, 2013 at 17:10 (2 minutes ago)	Notified ccordray by push notification to CCordray-iPhone.
May 29, 2013 at 17:10 (2 minutes ago)	Assigned to ccordray.
May 29, 2013 at 17:10 (2 minutes ago)	Triggered through the API. Description: CRITICAL: PB Legacy API - legacy::api: Application busy more than 90 percent of time (View message) View in ScienceLogic

Incident Suppression by Device

Incidents in PagerDuty are created (triggered) using a unique ID. This ID is set by ScienceLogic when the Run Book Automation policy creates a new PagerDuty Incident. To help eliminate spurious events, ScienceLogic uses the DID of the device as this ID. The result is that only one PagerDuty incident per ScienceLogic device is created. If there are multiple ScienceLogic events per device, the highest severity event will be used to trigger the RBA policy.

ScienceLogic Only Incidents

Only incidents created by ScienceLogic Run Book Automation policies will be acknowledged and resolved by ScienceLogic. Other incidents in PagerDuty will not be impacted.

The Synchronization & Performance Dynamic Application does report on the total number of incidents (triggered/acknowledged/resolved) across all types of incidents for a given account. In other words, if an incident was not created by ScienceLogic, it will still be represented in the performance metrics.



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

International: +1-703-354-1010