splunk>

GETTING STARTED GUIDE

GETTING STARTED WITH SPLUNK FOR CONTAINER MONITORING

Take an analytics-driven approach to container performance and troubleshooting

Introduction

Use of containers is on the rise, and with good reason. They enable you to develop, deploy and scale an app anywhere—helping you deliver better code and the best experience to your end users. However, this new technology also adds complexity to your infrastructure.

This guide outlines some of the insights you can gain by using Splunk software to monitor and troubleshoot your container ecosystem across the entire technology stack and the software development lifecycle (SDLC).

Containers—the New Wave of IT

Containers offer a portability that wasn't possible in traditional IT applications. Based on underlying Linux kernel technology, this portability abstracts the complexity of the compute layer, OS and application stack, ensuring that an app always runs the same, no matter what environment it's in. This enables developers to focus on what's most important—the application itself.

Containers also increase speed and flexibility, as they can be spun up in seconds. This helps you build, configure, test, deploy, update and migrate your apps faster and more easily.

All of these benefits are great for the business, but containers aren't without challenges. They can make it harder to monitor performance and logs. And if you can't find the source of errors and performance issues, it's difficult to maximize both agility and speed, while maintaining high service reliability. In addition, containers can have a short lifespan—sometimes only seconds. That makes the traditional log capture capabilities difficult and irrelevant to effectively perform container monitoring and troubleshooting.

To help you effectively run and develop applications using containers, your IT solutions must have the ability to index, search and correlate container-based data with other data sources for better service context, root-cause analysis, monitoring and reporting. Furthermore, container monitoring must be easy to implement and integrated with both your container deployments and your IT operations monitoring solution.

Getting Started

If you're already using Splunk software to monitor your IT environments, you're well on your way to effective container monitoring. Many of the data sources you're collecting and analyzing are the same ones you need for container monitoring and troubleshooting.

Using Splunk software, you can leverage a single solution to:

- Monitor and analyze container data and enable IT operations analytics
- Monitor container performance to ensure containers are available, and that issues are fixed quickly with minimal effort
- Help you gain insight on container resource usage, cluster capacity and the service impact of increasing cluster use for a specific service
- Gain better service context and accelerate root-cause analysis by indexing, searching and correlating container-based data with data from the entire technology stack

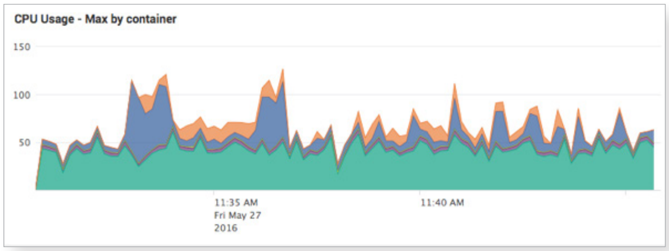
The first step is to configure the Splunk Log Driver for Docker. Using this log driver, you can pull Docker container information directly out of the containers themselves. This will help you reduce the effort required for monitoring logs seamlessly. Other helpful data sources are in the next section. And by correlating container data with other data sources in your architecture, you can gain a complete view of how your applications are performing.

Data Sources Table

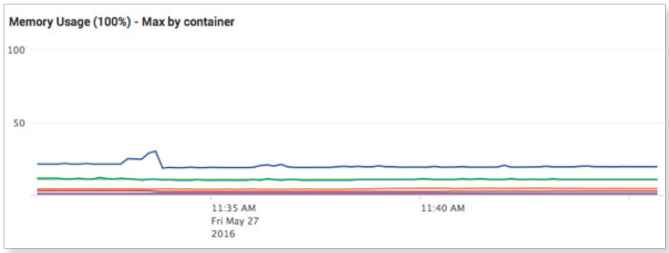
Data Type	Where to Find It	What It Can Tell You
Container and microservices logs	Logs can be ingested via any native Docker logging driver such as syslog, Splunk, JournalD and via Cloud integrations (e.g., Amazon CloudWatch, Google Cloud Platform Logging Export)	Container and application errors. Monitor any performance counters that can be calculated on top of logs (e.g., web and application server logs)
Container metrics and events	Docker APIs (e.g., Docker inspect, Docker top, Docker stats, Docker events), cloud APIs (e.g., AWS CloudWatch, Google Stackdriver)	Health, performance, availability and events generated by all monitored containers
Container clusters, nodes and applications	Docker UCP APIs and logs from containers	Application health, nodes, clusters and containers associated with an application, change history of containers and configuration
Application logs	Custom logs set by application developers	Application errors and other valuable machine data logged by developers
Wire data	Wire data probes (software based)	Communication between an app component, application response times and payload of applications as they traverse your network (even when you may not have direct visibility to some app components)

Using Splunk for Container Monitoring

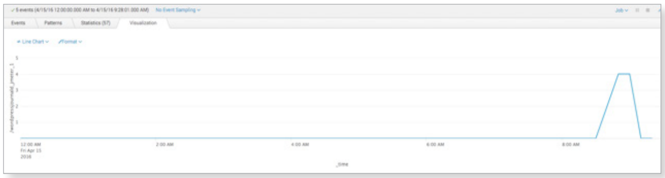
- **What to look for:** CPU utilization in order to manage required resources
- **Why?** To monitor impact on service reliability and container resource requirements
- **Example search:** source=docker_stats | eval cpu_percent | stats sum(cpu_percent) by time | timechart max(cpu_percent)



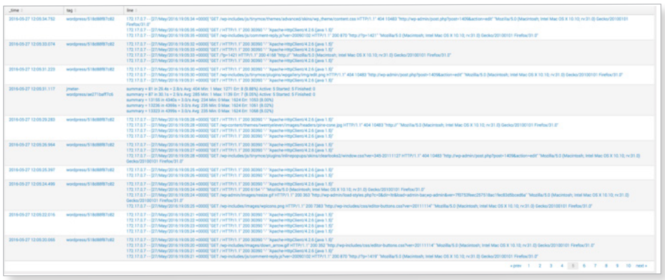
- **What to Look for?** Memory utilization across all containers over time
- **Why?** To gain insight into the availability and performance of containers in real time
- **Example Search:** source=docker_stats | eval container_name | table container_id container_name | timechart max(mem_percent)



- **What to Look For?** Errors that can cause downtime or service outage
- **Why?** To monitor and prevent errors related to memory utilization
- **Example Search:** Containers killed because memory limit was exceeed: source=docker_inspect State.Status="exited" | stats count by Name



- **What to Look For?** Errors in logs in a culpable container
- **Why?** To pinpoint and troubleshoot in real time to quickly isolate the specific container
- **Example Search:** Application logs from each container service: sourcetype=httpevent | spath output=tag path=tag | transaction tag maxevents=5 | table _time tag line



_time	tag	line
2016-05-27 12:05:34.752	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:34 +0000] "GET /wp-includes/js/tinymce/themes/advanced/skins/wp_theme/content.css HTTP/1.1" 404 10483 "http://wp-admin/post.php?post=1409&action=edit" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0" 172.17.0.7 - - [27/May/2016:19:05:35 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:35 +0000] "GET /wp-includes/js/comment-reply.js?ver=20090102 HTTP/1.1" 200 870 "http://?p=1421" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0"
2016-05-27 12:05:33.074	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:32 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:33 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:33 +0000] "GET /?p=1421 HTTP/1.1" 200 4168 "http://" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0" 172.17.0.7 - - [27/May/2016:19:05:34 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)"
2016-05-27 12:05:31.223	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:30 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:30 +0000] "GET /wp-includes/js/tinymce/plugins/wpgallery/img/edit.png HTTP/1.1" 404 10483 "http://wp-admin/post.php?post=1409&action=edit" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0" 172.17.0.7 - - [27/May/2016:19:05:31 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)"

2016-05-27 12:05:31.117	jmeter-wordpress/ae271baff7c6	summary + 81 in 29.4s = 2.8/s Avg: 404 Min: 1 Max: 1271 Err: 8 (9.88%) Active: 5 Started: 5 Finished: 0
		summary + 87 in 30.1s = 2.9/s Avg: 285 Min: 1 Max: 1139 Err: 7 (8.05%) Active: 5 Started: 5 Finished: 0
		summary = 13155 in 4340s = 3.0/s Avg: 234 Min: 0 Max: 1624 Err: 1053 (8.00%)
		summary = 13236 in 4369s = 3.0/s Avg: 235 Min: 0 Max: 1624 Err: 1061 (8.02%)
		summary = 13323 in 4399s = 3.0/s Avg: 235 Min: 0 Max: 1624 Err: 1068 (8.02%)

2016-05-27 12:05:29.283	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:28 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:28 +0000] "GET /wp-content/themes/twentyeleven/images/headers/pine-cone.jpg HTTP/1.1" 404 10483 "http://" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0" 172.17.0.7 - - [27/May/2016:19:05:29 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:30 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)"
2016-05-27 12:05:26.964	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:26 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:27 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:28 +0000] "GET /wp-includes/js/tinymce/plugins/inlinepopups/skins/clearlooks2/window.css?ver=345-20111127 HTTP/1.1" 404 10483 "http://wp-admin/post.php?post=1409&action=edit" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0"
2016-05-27 12:05:25.397	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:25 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:26 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)"
2016-05-27 12:05:24.499	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:24 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:24 +0000] "GET / HTTP/1.1" 200 6154 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0" 172.17.0.7 - - [27/May/2016:19:05:24 +0000] "GET /wp-admin/images/resize.gif HTTP/1.1" 200 363 "http://wp-admin/load-styles.php?c=0&dir=ltr&load=admin-bar,wp-admin&ver=7f0753feec257518ac1fec83d5bced6a" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0" 172.17.0.7 - - [27/May/2016:19:05:25 +0000] "GET /wp-includes/images/wpicons.png HTTP/1.1" 200 7383 "http://wp-includes/css/editor-buttons.css?ver=20111114" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0"
2016-05-27 12:05:22.016	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:21 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:22 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:23 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:24 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)"
2016-05-27 12:05:20.065	wordpress/518d88f87c82	172.17.0.7 - - [27/May/2016:19:05:20 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:20 +0000] "GET /wp-includes/images/down_arrow.gif HTTP/1.1" 200 352 "http://wp-includes/css/editor-buttons.css?ver=20111114" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0" 172.17.0.7 - - [27/May/2016:19:05:21 +0000] "GET / HTTP/1.1" 200 30390 "-" "Apache-HttpClient/4.2.6 (java 1.5)" 172.17.0.7 - - [27/May/2016:19:05:21 +0000] "GET /wp-includes/js/comment-reply.js?ver=20090102 HTTP/1.1" 200 870 "http://?p=1419" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:31.0) Gecko/20100101 Firefox/31.0"

Summary

Although containers can bring additional complexity to your infrastructure, they don't have to bring additional complexity to your job. In other words, it's critical to understand the availability, performance and usage of applications you've deployed with Docker. Using Splunk software, you can do this and additionally gain insight on containers that are deployed on-site, and also on services like Google Cloud Platform Container Engine. Since Splunk can monitor all your application and infrastructure components, you can gain insight across your entire application stack.

Try Splunk Cloud or Splunk Enterprise for free or learn more about **container monitoring**.
Already have Splunk? **Download Splunk Apps** on Splunkbase.

Learn more: www.splunk.com/asksales

www.splunk.com