

Foglight[®] for Container Management 2.0.0 User and Administration Guide



© 2019 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc. Attn: LEGAL Dept. 4 Polaris Way Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linux Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESX, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. VMware, ESX, ESXI, VSphere, VCenter, VMotion, and VCloud Director are registered trademarks of trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Vortes are trademarks of eclipser of Symantec Corporation or tis affiliates in the U.S. and other countries. and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademarks of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Quest is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Vormetric is a registered trademark of Vormetric, Inc. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. Amazon Web Services, the "Powered by Amazon Web Services" logo, and "Amazon RDS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Infobright, Infobright Community Edition and Infobright Enterprise Edition are trademarks of Infobright Inc. POLYCOM®, RealPresence® Collaboration Server, and RMX® are registered trademarks of Polycom, Inc. All other trademarks and registered trademarks are property of their respective

owners.

Legend

- **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
- **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
- i IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Foglight for Container Management User and Administration Guide Updated - August 2019 Foglight Version - 5.9.5 Software Version - 2.0.0

Contents

Understanding Foglight for Container Management
About Foglight for Container Management6
Architecture
Sizing Your Monitored Environment
Foglight Management Server Requirements8
Kubernetes Agent Requirements
Docker Swarm Agent Requirements
Getting Started
Prerequisite
Creating and Activating Agent
Configuring data collection interval24
Using Foglight for Container Management
Kubernetes
Monitoring Kubernetes Pods
Monitoring Kubernetes Nodes
Monitoring Kubernetes Clusters
Monitoring Kubernetes Other Components
Alarms
Capacity Management
Optimizer
Administration
Docker Swarm
Monitoring Docker Containers
Monitoring Docker Hosts
Monitoring Docker Swarm Clusters
Monitoring Docker Swarm Services
Alarms
Analytics
Kubernetes analytics
Docker Swarm analytics
Domains and Object Groups
Domains
Object Groups
Metrics
Kubernetes metrics
Docker Swarm metrics61
Rules
Kubernetes
Docker Swarm
Customization
About Us
We are more than just a name

Foglight for Container Management 1.2.0 User and Administration Guide Contents

Our brand, our vision. Together.	. 78
Contacting Quest	. 78
Technical support resources	. 78

5

Understanding Foglight for Container Management

- About Foglight for Container Management
- Architecture
- Sizing Your Monitored Environment
 - Foglight Management Server Requirements
 - Kubernetes Agent Requirements
 - Docker Swarm Agent Requirements
- Getting Started

clusters.

- Prerequisite
- Creating and Activating Agent
- Configuring data collection interval

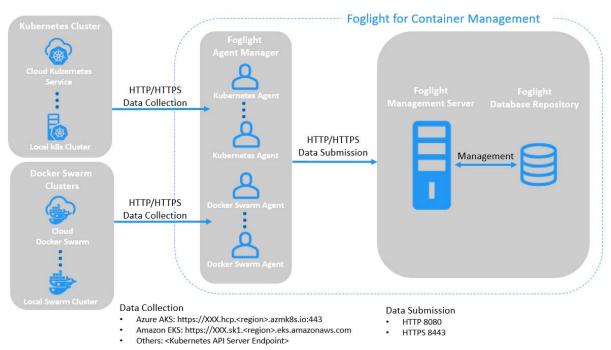
About Foglight for Container Management

Containers are a method of operating system virtualization that allow you to run an application and its dependencies in resource-isolated processes. Foglight[®] for Container Management simplifies this process by tracking each container, the resources it consumes, and the remaining compute of the container host, as well as providing you with the cluster information and pre-configured rules with notifications identifying the problem of your

6

Architecture





Foglight for Container Management consists of three main components:

- Foglight Management Server and Foglight Database Repository Responsible for managing, alerting, and viewing the collected data. Both components can be set to run on the same machine or reside on separate machines.
- Agent Manager Hosts the monitoring Kubernetes agents.
- Docker Swarm clusters Manages containerized applications in a clustered environment.
- Kubernetes clusters Manages containerized applications in a clustered environment.

Sizing Your Monitored Environment

Consider the possibility of a great amount of objects being collected, analyzed, and maintained by the application, several aspects of the underlying server must be taken into account. The sizing of the supporting clusters and containers depends on the complexity of the underlying environment. Sufficient processing power and CPU memory are required to support effective collection, server data handling, and analytics.

NOTE: Currently Quest validates the environment with up to 10000 containers. If your environment beyonds this scale, contact Quest Support.

Foglight Management Server Requirements

The minimum system requirements of the Foglight Management Server vary from the scale of clusters. The scale of clusters is determined by running containers.

Operating System	Maximum Containers	Foglight		Agent Manager	Agent Manager	
		JVM Settings	# of CPUs	JVM Settings	# of CPUs	
Windows 64-bit	1000	Xms Xmx=4G	2	Xms Xmx=4G	2	
	5000	Xms Xmx=8G	4	Xms Xmx=8G	4	
	10000	Xms Xmx=12G	6	Xms Xmx=12G	6	
Linux 64-bit	1000	Xms Xmx=4G	2	Xms Xmx=4G	2	
	5000	Xms Xmx=8G	4	Xms Xmx=8G	4	
	10000	Xms Xmx=12G	6	Xms Xmx=12G	6	

Table 1. Foglight Management Server requirements

If you are using an embedded Agent Manager, make sure to use the sum resources of both Foglight and Agent Manager.

Kubernetes Agent Requirements

Kubernetes Agent collects inventory and metrics every 5 minutes by default. Refer to Configuring data collection interval for details about how to change the collection interval.

Table 2. Kubernetes Agent requirements

Maximum Containers	Kubernetes Agent Col	Kubernetes Agent Collection Interval (minutes)		
	Inventory	Metrics		
500	5	5		
1000	10	10		
5000	30	30		
10000	60	60		

Table 2 is the recommendations for local Kubernetes clusters. If you deploy Kubernetes clusters on the Cloud Provider Kubernetes Service, consider your network rate and change your configurations based on different Cloud Provider and different region/zone of your cluster.

Docker Swarm Agent Requirements

Docker Swarm Agent collects inventory and metrics every 5 minutes by default. Refer to Configuring data collection interval for details about how to change the collection interval.

Table 3. Docker Swarm Agent requirements

Maximum Containers	Docker Swarm Agent Collection Interval (minutes)		
	Inventory	Metrics	
500	5	5	
1000	10	10	
5000	30	30	

Table 3 is the recommendations for local Docker Swarm clusters. For cloud environment, consider network rate and change configurations based on different Cloud Provider and different region/zone.

Getting Started

- Prerequisite
 - Kubernetes Agent
 - Preparing the Kubernetes credential
 - Enabling Heapster service in monitored environment
 - Docker Swarm Agent
 - Preparing Docker Swarm Agent credentials
 - Enabling Docker Remote API for monitored docker host
 - Uploading Docker Swarm Agent credentials
- Creating and Activating Agent
 - Creating and Activating a Kubernetes Agent
 - Creating and Activating a Docker Swarm Agent
- Configuring data collection interval

Prerequisite

Kubernetes Agent

Each Kubernetes Agent monitors the assets inside the selected Kubernetes Service Providers. To enable the data collection, complete the following prerequisites before create agent.

- Preparing the Kubernetes credential
- · Enabling Heapster service in monitored environment

Preparing the Kubernetes credential

The Kubernetes configuration file named *KubeConfig* is a standard configuration of Kubernetes and is required for Kubernetes agents to access the cluster. Foglight for Container Management verifies and supports the local Kubernetes and the following Cloud Kubernetes Service Providers. Based upon your environment, select either of approaches to get your *KubeConfig* file:

- **NOTE:** Data from different Kubernetes Agents with the same cluster name will be merged into one cluster.
 - Local Kubernetes
 - Azure Kubernetes Service (AKS)
 - Amazon Elastic Container Service for Kubernetes (EKS)
 - Google Cloud Platform Container Engine (GKE)
 - IBM Cloud Kubernetes Service
 - Openshift Origin

Local Kubernetes

If you build a Kubernetes cluster locally, find this *KubeConfig* file under the /etc/kubernetes/admin.kubeconfig on your master node.

Azure Kubernetes Service (AKS)

Before generating the Kubernetes credentials, record the following information:

- Azure Username
- Azure Password
- Azure Subscription Number
- The name of your AKS Cluster Resource Group
- The name of your AKS cluster

Download the Azure Command Line Interface and install it in your local platform, and then follow steps below to generate your Kubernetes credential:

1 Run the command *az* login.

Then a browser shows up, directing you to the Azure Portal where you should enter your Azure Username and Password to complete the authentication.

- 2 Run the command: az account set --subscription <azure subscription number>
- 3 Run the command: az aks get-credentials --resource-group <azure resource group name> --name <azure cluster name>
- 4 Find the Kubernetes configuration file under <USER_HOME>/.kube/config on your local platform.

NOTE: The token in this Kubernetes configuration file will get expired after two years. If you don't want the credential gets expired, refer to Foglight Container Tools for detail.

Amazon Elastic Container Service for Kubernetes (EKS)

Follow the Amazon EKS offical guide Getting Started with Amazon EKS. Follow the guide and complete Create a kubeconfig for Amazon EKS. in the end of the guide.

NOTE: If you don't want the credential gets expired, refer to Foglight Container Tools for detail.

Google Cloud Platform Container Engine (GKE)

Download the Google Cloud Client tool and install it in your local platform, and then follow steps below to generate your Kubernetes credential:

- 1 Generate the intermediate Kubernetes credential for your cluster.
 - a Log into your Kubernetes cluster, click **Connect** next to your cluster name.

Kubernetes cluste	rs	+ CREATE CLUS	TER 🕂 D	EPLOY C R	EFRESH	DELETE		
A Kubernetes cluster is a m Filter by label or name	nanaged group of	uniform VM <mark>in</mark> star	nces for running	Kubernetes. Learn r	nore			
Name A	Location	Cluster size	Total cores	Total memory	Notifications	Labels		
🗌 🥝 –gke-demo	us-central1-a	2	2 vCPUs	4.00 GB			Connect	/ :

b Click to copy the command below, and then run this command.



- c Find the intermediate Kubernetes configuration file under *<USER_HOME>/.kube/config* on your local platform. The following is the example of this intermediate Kubernetes configuration file.
 - **NOTE:** This Kubernetes configuration file cannot be used as the agent credential because the token in this file will get expired soon and "*cmd-path*" of the token directs to your local platform.

rind: Config
preferences: {}
19679
- name: gke_dulcet-bucksaw-208510_us-central1-a_jane-gke-demo
user:
auth-provider:
config:
access-token: ya29.GlzuBVkzkoVc1VUV 7yXM50DpQ7z7ahGzFA f2008FhxZjDICXRFdAw5ytBc9dHBT90yYK
cmd-args: config config-helperformat=json
cmd-path: C:\Users\jwang7\AppData\Local\Google\Cloud SDK\google-cloud-sdk\bin\gcloud.cmd
expiry: 2018-07-04T06:44:592
expiry-key: '{.credential.token_expiry}'
<pre>token-key: '{.credential.access_token)'</pre>
name: gcp

- d Open Google Cloud Client tool and run the following commands to create a Kubernetes service account that grants with the *cluster-admin* role and the access to your Google Kubernetes Engine (GKE) cluster.
 - a kubectl create serviceaccount <service account name>
 - b kubectl create clusterrolebinding <cluster role binding name> --clusterrole=cluster-admin serviceaccount=default:<service account name>

"default" in the above command is the namespace name of this service account name. The name space name will be "default" if you do not change it. You can also change to other namespace names, as needed.

c kubectl describe serviceaccount <service account name>

You will get the response similar as below. Record the <secret name> for later use.

C:\>kubectl describe	serviceaccount jane-gke-sa
Name:	jane-gke-sa
Namespace:	default
Labels:	<none></none>
Annotations:	<none></none>
Image pull secrets: Mountable secrets:	jane-gke-sa-token-x2n6w
Tokens:	jane-gke-sa-token-x2n6w
Events:	<none></none>

d kubectl describe secret <secret name>

You will get response similar as below. Record the token value (exclude "token:") for later use.

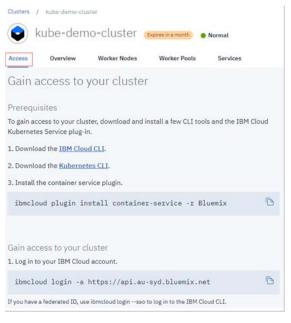
Name: Namespace: Labels: Annotations: 0032	jane-gke-sa-token-x2n6w default <none> kubernetes.io/service-account.name=jane-gke-sa kubernetes.io/service-account.uid=9f16c355-7f4f-11e8-9c03-42010ad</none>
	etes.io/service-account-token
Data ====	
ca.crt: 1 namespace: 7	
token: pY2VhY2NvdW50	yJĥbĠciOiJSUzIINiIsinR5cCl6IkpXUCJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3N1c Iiwia3UiZXJuZXR1cy5pby9zZXJ2aWN1YWNjh3UudC9uYUIlc3BW2UIOIJKZWZhd ZR1cy5pby9zZXJ2aWN1YWNjb3UudC9zWNvZXQubmFtZ5I6ImphoHtZ2t1LXNhL
va2VuLXgybjZ3 tZSI6ImuhbmUt	1 iwia3U iZXJuZXR1cy5pby9zZXJ2aWN1YWNjb3UudC9zZXJ2aWN1LWFjY291bnQub Z2t1LXNNI iwia3U iZXJuZXR1cy5pby9zZXJ2aWN1YWN ib3UudC9zZXJ2aWN1LWFjY
1bnQud₩lkIjoi tOnNlcnZpY2Vh	OVY×NmMzNTUtN2YØZiØ×MVU4LŤlĴMĎMtNDIwMTBhODAਔMDMyIiwic3UiIjoic3lžd Y2NvdV500mR1ZmF1bHQ6amFuZS1na2Utc2EifQ.VdRPVHLCqU3taVU5dyjZf4PPcQ
JumCzfilpO.jMF	tUPkgoyEURQ20K9ebPČf0m-4h3loIBSNuq8TokcZiUSK6nf6gToJliNAÕĚuNBwJ5z cTm6kP2BhhrvFkKnXNCaJRSmCIhHLBgtB4rqWKCdtJU8yfJTR253c8n2gTJ3WPL AKVDD_iPhLEvTRSMCGiixIUTfea8scwops9_cJx6LRY92FnucdwMrpnxU3alXW
	JreabM-VAxMksgrg3tIcwS1mU5U7ujSXcpk1j-Y0P2JYwFusytjP1ptZMrS0w

e Open the intermediate Kubernetes configuration file under <USER_HOME>/.kube/config, and then add the user and change the token to the new one.



IBM Cloud Kubernetes Service

If you have created your cluster on IBM Cloud Kubernetes Service, get the access from the console as described on the cluster's *Access* view. You will get a .pem file and a .yml file after you performing the steps.



By default IBM Cloud Kubernetes Service uses certificate authority file and token/refresh token. However, certificate authority data and service account token should be used in the Kubernetes Agent credential. After you successfully test your connection through "kubectl get nodes", follow the steps below to generate the Kubernetes Agent credential.

1 Run the command *kubectl config view -minify=true -flatten -o json*. You will get an output similar as below, then record the *<certificate authority data>* for later use.

C:\Users\jwang7\.kube>kubectl config viewminify=trueflatten -o json
(
"kind": "Config",
"apiVersion": "v1".
"preferences": <>.
"clusters": [
"name": "kube-demo-cluster",
"cluster": {
"server": "https://130.198.66.34:30244",
"certif icate=authority=data": "LSØtLS1CRUdJT iBDRUJUSUZJQØFURSØtL
SØtCk1JSUZSUENDQXkyZØF3SUJBZØ1KQU×5SPdFQUA2NmkrUUEwRØNTCUATSWIZRFFFQkN3UUFNRGt4T
npBMUJnTlYKQkFNTUxtUxpNall4WUZeESHRXpPVFExTUGAU1xUTJabU16TXpjd09UaGhZUEF6TFd0M
Ultun libuyuwihnda pZMkU3SGhjTkiUZ3doekEyTURUd05UUTNXaGNOTKRUeEIUSXhNRFU3TIRM1dqQ
UIVUT LIDUTWIINAAA DZANG SAAJIKIUZAAO EKEYTUNAAAGNOIKAA EKEYTUNAAAGNOIKA OKEISAANAA ON SIANAAANAA U
IVNVGRSI I IZZNZAUU REZZVECKI SI UNVZZI IVNSALI GAZDOUSZOWW PGDESCWI PERKZI U UNIKI I ANAUNE I FyZFdK bGNENY kRIZG I FdOast J SUMKSW BT L Jna 3 Foaz I HOX cvQk FRUZBQU 9 DQWc 4QU 1 J SUMDZØL DQ
IFyZranduntnwxkniz6IFaueljjsunkswpbikunasfoazinvxcwykrkkuzby0yDywe4y0IJsun226Dy WdFQXIIdk4xLipwe69CckJHTHITF0wvenBpRwo5M3RtYUUveGtYMnIve;HzeIZUTU5a4YIR6a2IxQ;UMU
zVØRkFkTUFQNEÜYRGJmZmpHckx3M20zZkxDL2huMnhvCjNRQTQ0U254ZIRRU1EKK0R2MUK3VkQzcD1pT
zZzY2JUanErckFUL3g1NXFtanRRcnprUGoxN1UzTjZ2SzEvdUsKY1pwSUdQ0U5WSEMxOHFaZXNkQ3Jja
FNIdEvØK2N3NXqvNEŽyQ3dRb1N1TVŮnUXBYWFREMŘxTdØ5yeXpXOWxZRvpyM2FraHQ3OSs5Y211U1BGR
3BQb2FBZXd0SjBQYØx5eDJDcnFeNG1DTHJxREZ6M3UMWVM3TFhtNEFhMys2OEUxCkM3UzkØNUhBTW26U
GpySXZUZT1vOŬE3UFBDc0pKYT1PM09IQ110b25mQn1EK1BZcExkBzdTZØN3WTFJaXc1ZzQKaU10dU04S
zŘícktPSnluK2ltRld6QUpPci94cjk2dy94Tml4UkllUkNPc2RzTUg1N3hPS3pqNlJvb2E3bGpPZAoyL
3Znb1Z0QkpxT1VPWU9QUEhybitjS09ZZ1Q5cnh2cWxXentQT1Jz0Fp1RD1qMmk4WURNeEd2L2ZybThRT
npUCkduYkxuckdWZUZCRØc3cG1tbXRZSUBw0CtGYnFxbntGUTZ5d2NX0TFqSnZ6ST1vZEp6ZnQ4Zk9IZ
kRNcjBteFgKR05aN1pHSU1FU1ZZU3JNTUt2RCtHT011SzBqRH1hRVpaY=80dU14R3YrU3NLMWZrc0JUW
UJvbWdBaDIvRC9UcApwNUU3SXI1NkcvL2Y3UGFHc3NDMTZBK2JØZ1ŽONk9oOUUsTXpHQUhTWWR6ZndRR
3dxcjB4NHRMU1V2c3A2U1dFC1BZSEVnRØJMbEY4Mn5XcEMzeFVDQXdFQVFhT1FNRTR3SFFZRFZSME9CQ
11FRKcxcUEyazQxZ21TcndIdX1tRkMKdzdsbWt1cE5NQjhHQTFUZE13UU1NQmFBRkcxcUEyazQxZ21Tc
ndIdX1tRkN3N2xta2UwTk1Bd0dBMVVkRXdRRgpNQU1CQWY4d0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dJQ
kFGc29JbWFydjJRckc4TTNKajQ5andUb2N0d21UU1JTC1NFd1RwanRvbWcGdEdÖdW9EW1UHbUHwSjRWa
3g5Wm9nRkUxZ8Yzb3ZPb1NFWFI4T316VGsxT24vZy9kbWUsQWwKajBHUVFoUEhCdG1HWVdtSy91ck1Ta
21Z0VJjQ3RvYU1oeUpvZTdnOXhIV3p2MzRQeTEx0ŨtnazE5YWZSYkRrQwo1UmpuQ011cWpCTŴdZOHZtV
VlieTMwMDA1Ni9pNjlZR1RXdT1FU10ZOS9WTGZnajNq0XA2Q21zHzIre1IwTVQ5CjZPcjd1bU0yL0YyM
8V1dmRSRGNtbjZQN1dnaDE4dWRDd2tnWno0T0ppbzJ60DBM0VdESnRTLytuNzF0VVVHNGcKMUU5TTEzT
F1I0W1KdTUwSĬIHb3p0S08zc0UCNmg4cTVZY2ĴóMXhhZmEvR1Byc1N2SmNBNEgwVFd2Rk8yVmhNcQp5V
0ZIMjBRbzlaK3hHQ2ULUk1OYjFkY2x6aktxOFQwK3JXK25wTi9FU0ZIZ1BIWmdiWW9UR3djYit6SjZha
HR1CmJWTVRzaUZSK0pCQUdmVj1XTE0vcFZnTG1YSDdrZkM4QjFaQ1N0cEZ2d0Z0eXNyQTk2RD1Td2tmS
GpvZ1J2eVAKaVxSRFZ4eHB60GovWTRkc2hDancwZmFyeW1EL3VMTVNZRjFTU2NZT1BaTUvvUGN2cUNFe
Fd1Z293REZqcjJIMQp2YnhpL31xcnpIZUJNMjgrZ1VWRERIazJXWVczU1ZqQnU3b3Y4QVNVbFhxY2NQU
ØZoNU10R1djeŨdWdjħFZUN4CkR0dEŨHTk1hR1ŻMSnY1eUhUb25TM0J3Z25ŔUTh2RWYzNGw3a29TZk1ĹR
1kxZWMØSDhvaWZaT3pyMEtØVEIxakMKOVBoNFZTS1Ixa2ZrCiØtLSØtRU5EIENFU1RJRk1DQVRFLSØtL
S9K''

- 2 Run the command kubectl create serviceaccount < service account>.
- 3 Run the command *kubectl describe serviceaccount <service account>*. You will get a response similar as below, then record <service account secret> (in this sample, it is jane-sa-token-xkqrk) for later use.

C:\Users\jwang7\.kube>kubectl describe serviceaccount jane-sa Name: jane-sa Namespace: default Labels: <none> Annotations: <none> Image pull secrets: <none> Mountable secrets: jane-sa-token-xkgrk</none></none></none>
Labels: <none> Annotations: <none> Image pull secrets: <none></none></none></none>
Annotations: Image pull secrets: Inone>
Image pull secrets: <none></none>
Mountable secrets: jane-sa-token-xkgrk
Tokens: jane-sa-token-xkqrk
Events: <none></none>

4 Run the command *kubectl describe secret <service account secret>*. You will get a response similar as below, then record <service account token> for later use.



5 Open the .yml file generated previously, which looks like below.

apiVersion: v1	
clusters:	
- name: kube-demo-cluster	
cluster:	
certificate-authority: ca-mel01-kube-demo-cluster.pem	
server: https://130.198.66.34:30244	
contexts:	
- name: kube-demo-cluster	
context:	
cluster: kube-demo-cluster	
user: Jane.Wang@quest.com	
namespace: default	
current-context: kube-demo-cluster	
kind: Config	
users:	
- name: Jane.Wang&quest.com	
user:	
auth-provider:	
name: oidc	
config:	
client-id: bx	
client-secret: bx	
id-token: eyJraWQiOiIyMDE3MTAzMC0wMDowMDowMCIsImFs2yI6IIJTMj	023
idp-issuer-url: https://iam.ng.bluemix.net/kubernetes	
 refresh-token: J1B9J8mzGdOecQbYvbmh7csxFZ5j1C9QEJxgWP7E157db 	_ws

6 Change the certificate authority to the data <certificate authority data> of this authority and change the users section to use <service account token>. Save your changes, and then you will get a credential file like below. This file will be used as the Kubernetes Agent credential to connect to your IBM cloud Kubernetes service cluster.



Openshift Origin

If you could access the /etc/origin/master/admin.kubeconfig on the master node, download this file which can be used as the Kubernetes Agent credential.

If you could not access the /etc/origin/master/admin.kubeconfig on the master node, follow instructions below to generate a permanent credential file.

Before generating the permanent Kubernetes credentials, record the following information and ensure you have granted the privilege for accessing the cluster-wide resources:

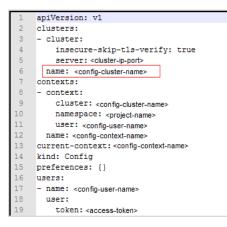
- Openshift Username
- Openshift Password

Download the Openshift Command Line Interface and install it in your local platform, and then follow steps below to generate your Kubernetes credential:

- 1 Log into Openshift and generate an intermediate Kubernetes configuration file.
 - 1 After logging into Openshift, click **Command Line Tools** on the upper right.
 - 2 Click the button next to the Session token field, copy the command, and then paste it in your local Command Line Tool. Make sure to find the intermediate Kubernetes configuration file under </br>USER_HOME>/.kube/config on your local platform.

enShift Web Console ×		
C A Not secure Https://10.4.120.18/8443/console/command-line	Ŷ	0 0
ENSHIFT ORIGIN C	D-	h huar
Command Line Tools		
With the OpenShift command line interface (CU), you can crease applications and manage OpenShift projects from a terminal. You can download the ac clien using the links below. For more information about downloading and installing it, please refer to the Get Started with the CU documentation.	tool	
Download or :		
Eveninging of t		
Latest Release if		
	ame	
Latest Release of After downloading and installing it, you can start by logging in. You are currently logged into this console as Nhuang. If you want to log into the CLI using the s	ame	5
Latest Release t? After downloading and installing it, you can start by logging in. You are currently logged into this console as hhuang : If you want to log into the CLI using the s session tolen:		5
Latest Release if After downloading and installing it, you can start by logging in. You are currendy logged into this console as Nhuang : If you want to log into the CLI using the s session taken: oc login https://10.4.120.18.8443 -token+chidden> A token is a form of a password. Do not share your API token. To reveal your token, press the copy to clipboard button and then pasts the clipboar		
Latest Release of After downloading and installing it, you can start by logging in. You are currently logged into this console as Nhuang. If you want to log into the CLI using the s session token: oc login https://10.4.320.18.8443-soken=Hrhidden> M A token is a form of a password. Do not share your API token. To reveal your token, press the copy to clipboard button and then paste the clipboard contents.		
Lates Release if. After downloading and installing it, you can start by logging in. You are currently logged into this console as Nhuang: If you want to log into the CLI using the s session token: or log: https://10.4.120.18.8443 -usiken-indidens After you login to your account you will get a list of projects that you can switch between;	8	
Latest Release if. After downloading and installing it, you can start by logging in. You are currently logged into this console as Nhuang. If you want to log into the CLI using the s session toben: in log hopp/170.4.120.18.843 -usken-indiden> After you login to your account you will get a list of projects that you can switch between: oc project -project-names	8	
Letest Release if After downloading and installing it, you can start by logging in. You are currently logged into this console as Nhuang . If you want to log into the CLI using the s session takes: set logn https://10.4.120.188.043—obten:ethidden> Ataken is a form of a password. Do not share your API token. To reveal your token, press the copy to clipboard button and then passe the clipboar Ataken is a form of a password. Do not share your API token. To reveal your token, press the copy to clipboard button and then passe the clipboar Ataken is a form of a password. Do not share your API token. To reveal your token, press the copy to clipboard button and then passe the clipboar Atter you login to your account you will get a list of projects that you can switch between: or project-orapicet-name> If you do not have any existing projects, you can create one:	•	

3 On your local platform, browse to open this configuration file. You may see the context similar to the following. Record *<config-cluster-name>* for later use.



- 2 The token generated in step 1 will be expired after 4 hours, however Foglight for Container Management needs a permanent Kubernetes credential. So you need to create a service account with "cluster-admin" role, and then get the authorization code (not expired) of this service account to generate our permanent Kubernetes credential.
 - 1 Run the command *oc* project <project-name>.
 - 2 Run the command oc create serviceaccount <service-account-name>.

You can check if your service account has been created successfully using the command: kubectl get serviceaccounts

3 Run the command *oc serviceaccounts get-token <service-account-name*. Then you will get a token *<service-account-token>* like below. Record this token for later use.

"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2V hY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZh dWx0Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6Im9zLWFkb WluLXRva2VuLWY0a2ZsIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLW FjY291bnQubmFtZSI6Im9zLWFkbWluIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9 zZXJ2aWNlLWFjY291bnQudWlkIjoiODMzNGU0NTQtNzQ1Yy0xMWU4LWFmNmEtMDA1MDU2YjY3 NDFhIiwic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW500mRlZmF1bHQ6b3MtYWRtaW4ifQ.RW H_AoXy2U1elkHN_Bs9IR1xo0zNCJlwcY0h3zuQnrkOFi8gVpX1177uhAPp7oIjPqDSWkUAN9F 6mP_tNdGwJsqRmHYEMOtCLnnIM61BYxIcABvwr66a0Z3Gn0D7EM5M_7XgKDC160N3W5NaH0D8 DpVTYqxkQ49u3qt4gqrcjVCaSsDNWlgGXY4K0IDrUbKkdgaRKzeD9o4Bv9VbYICqyxwoUebku JAcHiXGIcSe-ozS_zroPi1tT5HW-RY0Pn3Fp3zBnydiokna0-mXot5lqoYc-R6E1U9YSrAOhWm9Q8ipiut60czXbmLPM4DYve6dmHi_j5FquCqhod-QlA7aPw"

- 4 Run the following command to grant your service account with the "cluster-admin" privilege: kubectl create clusterrolebinding <cluster-role-binding-name> -clusterrole=cluster-admin --serviceaccount=default:<service-accountname>.
- 3 Generate a permanent Kubernetes configuration file and save it under <USER_HOME>/.kube/config file/credential.
 - 1 Open and edit the intermediate configuration file.
 - 2 Use kubectl to add user credentials, create new context, in the end change the existing contexts to the ones that you added in step 2. For example,

kubectl config set-credentials <credential-name> --token=<serviceaccount-token> kubectl config set-context <new-context-name> --cluster=<config-cluster-</pre>

kubectl config use-context <new-context-name>

3 Save the current Kubernetes configuration file.

Enabling Heapster service in monitored environment

There are various approaches to enable Heapster on your Kubernetes cluster. Visit Heapster official website to determine the approach that you are going to deploy your Heapster service, or you can follow instructions in https://github.com/foglight/container to deploy your service.

name> --user=<credential-name> --namespace=<project-name>

Some of the cloud platform Kubernetes service has enabled Heapster service for the cluster. If you have connected to the cluster, run the following command to check: *kubectl cluster-info*

Docker Swarm Agent

Each Docker Swarm Agent monitors the assets in one docker host. Docker Remote API needs to be enabled for the Docker Swarm Agent collecting data from the docker host. If TLS is enabled to secure the Docker Remote API, credential for Docker Swarm Agent needs to be prepared. Complete the following prerequisites before create agent.

- · Preparing Docker Swarm Agent credentials
- Enabling Docker Remote API for monitored docker host
- Uploading Docker Swarm Agent credentials

Preparing Docker Swarm Agent credentials

If TLS enabled to secure Docker Remote API, then complete the following guide to get the credentials for Docker Swarm Agent for the docker host. Otherwise, continue with Enabling Docker Remote API for monitored docker host on page 17

Refer to the <u>official guide</u> to generate the keys. Be aware that, during generating the keys, the Foglight Agent Manager host address should be in the allow access list.

Docker Swarm Agent needs following credentials, you can get them when you finish the official guide.

- CA Public Key (ca.pem in official guide)
- Client Public Key (cert.pem in official guide)
- Client Private Key (key.pem in official guide)

Enabling Docker Remote API for monitored docker host

Change *ExecStart* in docker service startup script as below.

Non-TLS secured

```
ExecStart=/usr/bin/dockerd -H tcp://0.0.0.0:2375 -H
unix:///var/run/docker.sock
```

NOTE: Access should be allowed to the TCP port 2375

TLS secured

If TLS enabled, complete Preparing Docker Swarm Agent credentials on page 16 first, then you will get the ca.pem, server-cert.pem and server-key.pem mentioned in the <u>official guide</u>.

```
ExecStart=/usr/bin/dockerd --tlsverify --tlscacert=ca.pem --tlscert=server-
cert.pem --tlskey=server-key.pem -H tcp://0.0.0.0:2375 -H
unix:///var/run/docker.sock
```

i NOTE: Access should be allowed to the TCP port 2375

Then restart docker service.

Uploading Docker Swarm Agent credentials

If TLS is enabled to secure Docker Remote API, go through this section to upload the credential for Docker Swarm Agent. Otherwise, skip this section.

When complete Preparing Docker Swarm Agent credentials on page 16, following credentials should be generated.

- CA Public Key
- Client Public Key
- Client Private Key

These are the credentials for Docker Swarm Agent, complete the following steps to upload the credentials.

On the **Administration > Credentials > Manage Credentials** dashboard, click **Add**, and then select Docker CA Public Key or Docker Client Public Key or Docker Client Private Key to upload related credentials. Take Docker CA Public Key as an example.

Navigation <	T Credentials > Manage Credentials
⊞ Expert View ▼	A credential is the information that gains access to system resou
Bookmarks There are no bookmarks Homes	a Credentialis dire information dial gains access to system resou patterning criteria that best suit your needs. For example, map a
Dashboards Active Directory Administration Agents Credentials Data Integration Management Server Rest API Rules & Notifications Schedules Setup Support Tooling Users & Security Alarms Apache BMK Remedy	E Select the Type of Credential to Add A Challense Response Challense Response Docker CA Public Key Docker Client Private Key Docker Client Public Key Docker Client Public Key Domain, User Name, and Password (Windows) DSA Key Kube Config RSA Key Storage SNMP SUDO with Custom Password SUD with Password -

In the Add a New "Docker CA Public Key" Credential dialog box, specify the following values:

- Credential Properties: Click Load from file to import Docker CA Public Key, and then click Next.
- Credential Name And Lockbox: Specify a unique name for this credential, and then click Next.
- Resource Mapping: Click Add. In the New Resource Mapping Condition dialog box, choose Target Host Name or Target Host Address for the monitored docker host.

 Credential Properties 		Resource Mapping		
Credential Name And Lo	New Resource Mapping O	ondition		
Resource Mapping Policies Mappin resourc usage	resources the Credential access different resource	l cannot access. The c es. Docker Credential	ombination of these conditio	an be used to access. They can also be used to list the ons tells the system which Credentials can be used to
	Equal or Not Equal		Target Host Name	Access a resource using the name of the host where it reside
	Matching Type	Domain Name 🗸	Target Host Address	Access a resource using the IP of the host where it resides.
	Evaluate This Condition	0		
	Matching Values (Combined Using Logica 'OR' Operator)	Add a New D		
		Use the above Ad		
			the logic	al 'OR' operator.

If choose Target Host Name, then enter the host name of the monitored docker host.

New Resource Mapping Cor	ndition	
	sed to relate this Credential to the resources it can be used to access. They can also be used to list t cannot access. The combination of these conditions tells the system which Credentials can be used t s.	
Usage Access Resources Using Equal or Not Equal	Docker Credential ↓ Target Host Name ↓	
Matching Type Evaluate This Condition 🧕	Domain Name → 9 🗹	
Matching Values (Combined Using Logical 'OR' Operator)	O Add a New Domain Name	_
	General distagent quest com	

If choose Target Host Address, then enter the IP address of the monitored docker host.

New Resource Mapping Co	ndition			
Mapping conditions are used to relate this Credential to the resources it can be used to access. They can also be used to list the resources the Credential cannot access. The combination of these conditions tells the system which Credentials can be used to access different resources.				
Usage Access Resources Using Equal or Not Equal Matching Type	Docker Credential ↓ Target Host Address ↓			
Evaluate This Condition				
Matching Values (Combined Using Logical	Add a New IP Address			
'OR' Operator)	IP Address 🔺			

Then click **Add** to finish editing **New Resource Mapping Condition** and back to **Resource Mapping**. Then click **Finish**.

Then **Docker CA Public Key** has been uploaded and mapped to the docker host. To monitor this docker host, **Docker Client Public Key** and **Docker Client Private Key** also need to be uploaded following the above steps.

Creating and Activating Agent

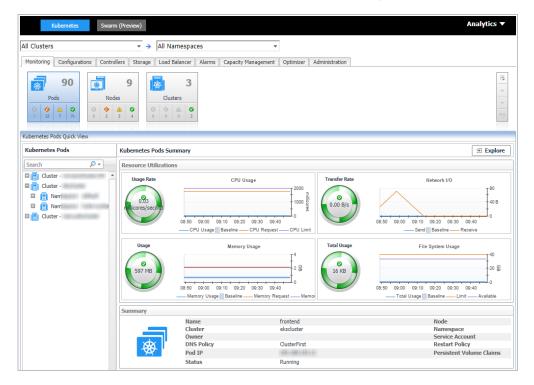
Foglight for Container Management supports Kubernetes Agent and Docker Swarm Agent.

- Creating and Activating a Kubernetes Agent
- Creating and Activating a Docker Swarm Agent

Creating and Activating a Kubernetes Agent

To create a Kubernetes agent on a monitored host:

- 1 Log in to the Foglight browser interface and make sure the left Navigation panel is open.
- 2 On the navigation panel, from **Standard View** click **Container Environment** or from **Expert View** click **Dashboards > Container**. Then the Container dashboard will display as below.



Foglight for Container Management 2.0.0 User and Administration Guide Understanding Foglight for Container Management 3 In the Container dashboard, click **Administration** tab, and then click **Create Docker Agent**. The **Create Docker Agent** wizard opens.

Kubernetes S	warm (Preview)				Analytics 🔻
All Clusters	✓ → All Namespaces	•			
Monitoring Configurations C	ontrollers Storage Load Balancer Alarms	Capacity Management Optimiz	er Administration		
Fasks:					
Agents					
5		- Data Gallastica 🦳 Darrena 🔶	the data of a cost	Gaussi	0-1
🕑 Add 🤹 Refresh 🛛 🕛 Activat	e Deactivate Start Data Collection Stor			Search Download Log	
O Add S Refresh ↓ ① Activat Agent Name ▲	e 🕜 Deactivate 🕨 Start Data Collection 📕 Stor Foglight Agent Manager Host	p Data Collection Remove Active Data Collection	Update Agent Alarms Edit Properties	Search Download Log	Agent Version
🕑 Add 🤹 Refresh 🛛 🕛 Activat		Active Data Collection	Alarms Edit Properties	Download Log	Agent Version

4 Agent Manager: specify the following values, and then click Next.

Create Docker Agent		×
 Agent Manager 	Agent Manager	
• Agent Properties	Enter the duster name and select the agent manager.	
 Credential Verification 	Cluster Name	
o Summary	The cluster name that you would like to create. nancyakscluster 0	
	Agent Manager	

- Cluster Name: unique name for the monitored cluster.
- Agent Manager. select an Agent Manager which manages the agent.
- 5 Agent Properties

Create Docker Agent			×
✓ Agent Manager	Agent Properties		
Agent Properties Credential Venfication Summary	Agent Name Kubernetes API Service End Point Kubernetes Version Heapster Service Namespace Heapster Service Name Collected Event Level Enable Proxy Proxy Type Proxy Server Address Proxy Server Port	Monitor@nancyakscluster 1.7 kube-system heapster ABNORMAL	0 0
	Collector Configuration	defaultSchedule v	View

- Kubernetes API Service End Point. Get this information from the KubeConfig file. For more
 information, see Enabling Heapster service in monitored environment on page 16.
- Kubernetes Version: 1.7 by default.
 - i | NOTE: Only need to change for OpenShift clusters.

- Heapster Service Namespace/Heapster Service Name: Get both values from the Heapster service configuration. For more information, see Enabling Heapster service in monitored environment on page 16.
- **NOTE:** If you monitor OpenShift Origin and enable the Hawkular metrics, then the Heapster Service Namespace should be openshift-infra, and the Heapster Service Name should be https:heapster:.
 - Collected Event Level: Set the collected event level, including ABNORMAL and ALL. ALL will collect both abnormal and normal events while Abnormal only collects abnormal events.
 - Enable Proxy: To enable the proxy, select the checkbox. Enter the Proxy Server Address and Proxy Server Port information.
- 6 Credential Verification
 - Do not configure a credential: click Next.
 - i NOTE: If an existing credential is detected, the screen will prompt, "An existing credential has been detected for this resource and the lockbox won't be released to the selected Agent manager. To continue the Agent creation steps, manually release the lockbox. Ignore this message if the lockbox has been released and click 'Next' to continue.".
 - Add cluster to a new credential.
 - Credential Type: Select the credential type from the list and click Next.

Create Docker Agent			
 ✓ Agent Manager ✓ Agent Properties 	Credent Select 1	i al Type he credential type from the list b	elow.
 Credential Verification 		Credential Type	Description
Credential Type Credential Properties Credential Name and Lockbox Resource Mapping Policies Summary	Ku	be Config	Note: The user configured in this kubeconfig file should have cluster-ad

• Credential Properties: Click Load from file to upload the credential and click Next.

Create Docker Agent		×
 Agent Manager Agent Properties 	Credential Properties Enter the properties for this credential.	
Credential Verification Credential Type	Note: The user configured in this kubeconfig file should have cluster-admin role. Otherwise, collection will fail.	
Credential Properties Credential Name and Lockbox Resource Mapping Policies Summary	Kube Config Cale Load from file apiVersion: V1 clusters: - cluster: - cluster	

 Credential Name and Lockbox: give a name for the credential, choose a lockbox, then click Next.

Create Docker Agent				>
 Agent Manager Agent Properties 		lential Name and Lockbox ese properties identify the credential on the Mana	gement Server.	
Credential Verification	Plea	se provide a unique name to identify this credenti	al	
 Credential Type 		econfig		
 Credential Properties 	A Lo	ockbox contains a collection of encrypted credentia	als and the keys used for their encryption and decryption.	
Credential Name and Lockbox		Lockbox 🔺	Password Required	
	0	-1000	No	*
 Resource Mapping 	۲	System	No	
Policies				
 Summary 				

• Resource Mapping: click Next.

Create Docker Agent	2		×
Agent Manager Agent Properties	Resource Mapping Select the appropriate resour	ce mapping option below.	
Credential Verification Credential Type Credential Properties Credential Name and Lockbox	This IP address only IP Range (IPv4 or IPv6) IP Block Using CIDR	IP Address: 7	
Resource Mapping Policies Summary			

 Policies: Add policies for this credential. This is an optional step. Click Next if you do not wish to add more policies at this time.

Create Docker Agent						×
 Agent Manager Agent Properties 	Policies Add policie	s for this credential. Thi	is is an optional step. Click 'Next' if you	do not wish to add more polic	ies at this time.	
Credential Verification	Qadd	Copy OPlete		Search	Ø -	15
 Credential Type 	Edit	Policy Type +		Details	p.]	
✓ Credential Properties		Failure Rate	Max Failure Count=3 and Time Pe			
 Credential Name and Lockbox 						
✓ Resource Mapping						
Policies						
 Summary 						

7 Summary: click Finish.

Create Docker Agent			
✓ Agent Manager	Summary		
 Agent Properties Credential Verification 	Cluster Agent Manager Orchestration Type	nancyakscluster fms02 Kubernetes	
Summary	Agent Name	Monitor@nancyakscluster	
	Kubernetes API Service End Point	Manual Control of the	
	Kubernetes Version	1.7	
	Heapster Service Namespace	kube-system	
	Heapster Service Name	heapster	
	Collected Event Level	ABNORMAL	
	Enable Proxy	false	
	Proxy Type	HTTP	
	Proxy Server Address	-849-0111	
	Proxy Server Port	00	
	Collector Configuration	defaultSchedule	
	Credential	kubeconfig	
	Lockbox	System	
	New or Existing Credential	New	
	Lockbox Password	The Lockbox is not a password secured Lockbox.	

8 Then, the agent will be created and activated automatically.

Creating and Activating a Docker Swarm Agent

Each Docker Swarm Agent monitored one docker host. If the docker host belongs to a Docker Swarm cluster, it will be considered as a manager/worker node. Otherwise, it will be considered to be a standalone docker host.

i NOTE: For a Docker Swarm cluster, you should create one Docker Swarm Agent for one host in the cluster, and if you want to monitor the whole cluster environment, you need to create all the Docker Swarm Agents for all the hosts in the cluster.

To create a Docker Swarm agent on a monitored host:

- 1 Login in to the Foglight browser interface and make sure the left navigation panel is open.
- 2 On the navigation panel, under **Dashboards**, click **Administration > Agents > Agent Status**.

The Agent Status dashboard opens.

3 In the Agent Status dashboard, click Create Agent.

The Create Agent wizard opens.

4 Host Selector. Select the monitored host that you want to monitor with the Docker Swarm agent instance that you are about to create, and then click **Next**.

NOTE: In order to select the host, the Foglight Agent Manager must be installed and running on the monitored host.

- 5 Agent Type and Instance Name: Specify the following values, and then click Next.
 - Agent Type: Select DockerSwarmAgent from the agent type list.
 - Agent Name: Specify the name of the agent instance that you are about to create using either of the following approaches:
 - Generic Name: This option is selected by default. A generic name is a combination of the host name and the agent type and uses the following syntax: agent_type@host_name.
 - Specify Name: Type that name in the Name field. For example, MyAgent.
- 6 On the Summary page, review the choices you have made, and then click Finish.

The Agents table refreshes automatically, showing the new Docker Swarm Agent.

- 7 On the *Agents* table, select the Docker Swarm Agent that you create, click **Edit Properties**, and then click **Modify the private properties for this agent**.
- 8 In the *Agents* properties view, check if the following values have been configured based upon your environment:

T. Agent Status > Edit Properties		G+ Tuesday, April 23, 2019 12:43 PM - 4:43 PM	4 hours 👻 📔 🖪 Reports
Name	Host	Туре	Tags
testagent	AND THE CONTRACTOR OF A DESCRIPTION OF A	DockerSwarmAgent	
This agent is currently using pr	operties for DockerSwarmAgent agents. Igent only.		
Modify the properties for a	ll DockerSwarmAgent agents.		
Configuration			
Name	docker		
Host Name	localhost		
Docker Remote API End Point	The second		
Swarm			
Swarm Name	default		
Data Collection Scheduler			
Collector Config	defaultSchedule	Edit Clone Delete	

- Name: give a name to the monitored docker host, it should be unique.
- Host Name: IP address or host name of the monitored docker host.

- Docker Remote API End Point. Docker Remote API endpoint of the monitored docker host. For more information, see Enabling Docker Remote API for monitored docker host on page 17.
- Swarm Name: specify the swarm cluster name for display. If the swarm name is kept as "default", then the cluster name will be displayed as "default (cluster ID)" on the dashboard. If a customized name is input here, then the customized cluster name will be displayed on the dashboard.
- **NOTE:** Ensure that the docker host inside the same cluster has the same configuration for Swarm Name.
- 9 Return back to the *Agents* table, select the above property changed Docker Swarm Agent, and then click **Activate**.

The new Docker Swarm Agent is created and data will be shown on the **Monitoring** tab after a few minutes.

Configuring data collection interval

The default data collection interval of agents is set to 5 minutes by default. Foglight for Container Management enables you to change this collection interval as needed.

i NOTE: Changing the data collection interval will take effect for all Kubernetes agents and Docker Swarm agents.

To configure the data collection interval:

- 1 On the navigation panel, under Dashboards, select Administration > Agents > Agent Status.
- 2 On the *Agent Status* dashboard, select the Kubernetes agent that you use to monitoring the container environment, and then click **Edit Properties**.
- 3 In the Edit Properties dashboard, click Edit next to the Collector Config field.
- 4 In the KubernetesAgent or DockerSwarmAgent Collector Config dialog box, change the following values, as needed:
 - Inventory Collector: Specifies the interval for collecting components.
 - Metrics Collector. Specifies the interval for collecting metrics.
- 5 Click Save.

Using Foglight for Container Management

- Kubernetes
 - Monitoring Kubernetes Pods
 - Monitoring Kubernetes Nodes
 - Monitoring Kubernetes Clusters
 - Monitoring Kubernetes Other Components
 - Alarms
 - Capacity Management
 - Optimizer
 - Administration
- Docker Swarm
 - Monitoring Docker Containers
 - Monitoring Docker Hosts
 - Monitoring Docker Swarm Clusters
 - Monitoring Docker Swarm Services
 - Alarms
- Analytics
 - Kubernetes analytics
 - Heatmap analytics
 - Scatter Plot analytics
 - Docker Swarm analytics
 - Heatmap analytics
 - Scatter Plot analytics
- Domains and Object Groups
 - Domains
 - Object Groups
- Metrics
 - Kubernetes metrics
 - Docker Swarm metrics
- Rules
 - Kubernetes
 - Docker Swarm

Customization

Kubernetes

Monitoring Kubernetes Pods

A pod contains one or multiple containers, such as Docker containers, which contains storage/network and the specification about how to run the containers. The *Kubernetes Pods Quick View*, which appears after clicking **Monitoring > Pods**, shows the data collected about the selected clusters and namespaces. This view consists of the following two panes:

- The **Kubernetes Pods** tree view, which appears on the left of *Kubernetes Pods Quick View*, lists the pods existing in the monitored Kubernetes environment.
- The Kubernetes Pods Summary view, which appears on the right after you select an individual pod in the **Kubernetes Pods** tree view.

Kubernetes Pods Summary view

The **Kubernetes Pods Summary** view appears on the right when you select a cluster in the **Kubernetes Pods** tree view.



Figure 2. Kubernetes Pods Summary view

The Kubernetes Pods Summary view displays the following data:

- *Resource Utilizations*: The resource utilization for the selected Kubernetes Pod over a selected period of time, which includes the following:
 - CPU Usage: Shows the CPU utilization summary for the selected Kubernetes Pod based on its total capacity during a selected time period.
 - Transfer Rate: Shows the network utilization summary for the selected Kubernetes Pod, including the average rate of network throughput, and the amounts of data sent to and received from the network.
 - Memory Usage: Shows the physical memory utilization summary for the selected Kubernetes Pod, broken into the amounts of memory that is swapped to disk, actively used, and allocated, all during a selected time period.

- File System Usage: Shows the file system resource utilization summary for the selected Kubernetes Pod, including the available/total/limited file system resource.
- Summary: Displays the detailed information about the selected Kubernetes Pod, including Name, Node, Cluster, Namespace, Owner, Pod IP, Service Account, DNS Policy, Restart Policy, and Status.

Click **Explore** on the upper right of the **Kubernetes Pods Summary** view to open the Pods Explorer view, which shows more detailed information about this Kubernetes cluster.

Pods Explorer view

The *Pods Explorer* view opens when you click **Explore** in the Kubernetes Pods Summary view, which includes the following tabs:

• *General tab:* The *General* tab displays the overall information of the selected Kubernetes Pod over a selected period of time, including the *Summary and Resource Information* table, the *Containers* table, and the *Init Containers* table. For more information, see Pod metrics *on page 60*.

Figure 3. Kubernetes Pods Explorer view General Tab

T. Container En	vironment	Kubernetes Pod: kube-proxy-8rdkl				G• Monday, :	June 24, 2019 9:28:17 Al	1 - Now 60 mir	nutes 💌 🛛	🖪 Reports 👻
	Warning :Ę									
General	Metrics	Events								
Summary a	nd Reso	urce Information								*
Cluster		vmwarecluster159			Namespace	kube-system				
Name		kube-proxy-8rdkl			Node	kuberuleworker3				
Labels		k8s-app=kube-proxy pod-template-genera								
	licy	Always								
	dline Sec	onds								
Persistent \	Volume (laim			Status	Running				
Containers										
Name	Status	Image			Command	Arguments	Environ	nent Varial	bles	1
kube-proxy	running				/usr/local/bin/kube-proxyconfig=/var/		[From Field P	verity Fatal Critical Warnin sunt Critical Warnin ironment Variables eld Path spec.nodeName] [/var/lb//	[/var/lib/kı	
	Darr									,
Init Contail	ners									
Name Stat	tus					Arguments		Volum	e Mounts	÷
					There Is No Data To	Display				

Metrics tab: The Metrics tab displays a Metric Selector allowing you to choose the metrics to be plotted on this dashboard. Charts of CPU Usage, Memory Usage, and Network I/O are presented by default.

nent > Kubernetes Pod: kube-proxy-Srdkl G+ Thursday, June 27, 2019 2:45:51 PM - Now 60 minutes 👻 📗 Reports 🤿 Alarms Severity Fatal Critical Warning Alarms Count Kubernetes Pod: kube-proxy-8rdkl Metric Selector Select All Select None Sea CPU Usage CPU Usage Rate CPU Utilization Filesystem Inode Usage Filesystem Usage Memory Page Faults Memory Page Faults Rate Filesystem Usage Memory Rss Memory Usage Memory Utilization Memory Working Set Network I/O Network I/O Error

Figure 4. Kubernetes Pods Explorer view Metrics Tab

- Event tab: The Event tab lists all the events occur on the pods.
 - Name: name of the event.
 - Type: type of the event, Warning or Normal.
 - Namespace: namespace of where this event happens.
 - Kind: type of the Kubernetes component on which this event occurs.
 - Involved Object: name of the Kubernetes component on which this event occurs.
 - Source: where this event has been triggered from.
 - Reason: reason of this event.
 - Message: detailed message of this event.

Figure 5. Kubernetes Pods Explorer view Events tab

t Container Environment > Kubernetes Pod:		G	3+ Thursday, June 27, 201	.9 2:13:23 PM	- Now 60 minu	utes 👻 🛛	Reports 🛪
Kubernetes Pod:	degelasymenti 70	280x467.6 jwbiz		ms Severity ms Count	Fatal	Critical	Warning :Ę <mark>1</mark>
General Metrics Events							
Events							
				Search	1		
	Type Namespace	Involved Object	Source	Search		lessage	<u>م</u>

Monitoring Kubernetes Nodes

A node, previously known as a minion, is a worker machine in Kubernetes. A node may be a VM or physical machine, depending on the cluster. Each node has the services necessary to run pods and is managed by the master components. The *Kubernetes Nodes Quick View*, which appears after clicking **Monitoring > Nodes**, shows the data collected about the selected clusters and namespaces. This view consists of the following two panes:

- The **Kubernetes Nodes** tree view, which appears on the left of *Kubernetes Nodes Quick View*, lists the nodes existing in the monitored Kubernetes environment.
- The Kubernetes Nodes Summary view, which appears on the right after you select an individual node in the Kubernetes Nodes tree view.

Kubernetes Nodes Summary view

The **Kubernetes Nodes Summary** view appears on the right when you select a node in the **Kubernetes Nodes** tree view.

Figure 6. Kubernetes Nodes Summary view

Kubernetes Nodes Quick View				
Kubernetes Nodes	Kubernetes Nodes Summary			Explore
Search 🔎 🔹	Resource Entitlement			*
(1) 2777Cluster (2) 10 762522bubmt156.prod. (2) 2784bumt156.prod. (2) 2784bumt166.prod. (2) 2778bubmt16.6.prod. (2) 2778bubmt16.6.prod. (2) 2777bubmt16.6.prod. (2) 10 777bubmt16.prod. (2) 10 702625bubmt116.prod. (CPU Allocatable		Henory Allocatable	Memory Request and Limit
 fog2623ubuntu16.prod fog2678ubuntu16.prod 	Resource Utilization			
	Utilization	CPU Usage 00:15 00:25 00:35 00:45 Usage Baseline CPU Request	Transfer Rate	Network UO
1 · · ·	Utilization	Memory Usage 00-15 00-25 00-35 00-45 00-45	Total Usage 0.00 B 0.05 00.05 00.15	File System Usage

The Kubernetes Nodes Summary view displays the following data:

- Resource Entitlement: The resource allocation for the selected Kubernetes node over a selected period of time, which includes the following:
 - CPU Allocatable: Shows the current allocatable CPU resources of this node.
 - Memory Allocatable: Shows the current allocatable Memory resources of this node.
 - CPU Request: Shows the trend of CPU request, limit, and capacity of this node.
 - Memory Request. Shows the trend of Memory request, limit, and capacity of this node.
- Resource Utilizations: The resource utilization for the selected Kubernetes node over a selected period of time, which includes the following:
 - CPU Utilization: Shows the CPU utilization summary for the selected Kubernetes node based on its total capacity during a selected time period.
 - Transfer Rate: Shows the network utilization summary for the selected Kubernetes node, including the average rate of network throughput, and the amounts of data sent to and received from the network.
 - Memory Utilization: Shows the physical memory utilization summary for the selected Kubernetes node, broken into the amounts of memory that is swapped to disk, actively used, and allocated, all during a selected time period.
 - *File System Usage*: Shows the file system resource utilization summary for the selected Kubernetes Pod, including the available/total/limited file system resource.
- Summary: Displays the detailed information about the selected Kubernetes node, including Name, Pod CIDR, OS, Architecture, OS Image, Address, Capacity, Allocatable, and Status.

Click **Explore** on the upper right of the **Kubernetes Nodes Summary** view to open the Nodes Explorer view, which shows more detailed information about this Kubernetes node.

i NOTE: If the virtual machines belong to the Container cluster, and they are monitored by other cartridges at the same time, for example, VMware, Infrastructure, AWS, or Azure. Then, the collected data will come from that cartridge directly and the **Kubernetes Nodes Summary** view will be different from the screenshot above. See Figure 7 for detailed information.

Container Environment G+ Monday, May 20, 2019 12:15:43 AM - 1:15:43 AM 60 minutes 👻 📔 Reports 👻 Analytics V Kubernet Swarm (Preview) All Clusters ▼ → All Namespaces -Monitoring Configura ns Controllers Storage Load Balancer Capacity Management Alarms Administration 76 8 3 Clusters 0 ø etes Nodes Ouick Kube etes Node Kubernetes Nodes Su Explore to VMware VM Explore Iocalkubecluster CPU Load CPU Utilization Network I/O Network Utilization kubeckamaster kubeckaworker EKS-DEMO 🖉 🧾 ip-192-168-228-125.u 00:20 00:30 00:50 01:00 01:10 00:40 00:50 01:10 00:40 @ ip-192-168-133-240.us % Used 🔲 Ba 🛛 🧑 ip-192-168-114-50.us nancyakscluster aks-nodepool1-113703 Memory Utilization Datastore Utilizatio aks-nodepool1-113703 aks-nodepool1-113703 1 10 🗑 - Transfer Rate 🔲 Basel

Figure 7. Kubernetes Nodes Summary view for VMware

- *Explore to VMware VM*: Click the button to open the *VMware Explorer* view, which is the same view from VMware cartridge. The *Explore to xx* button varies from the cartridge that is monitoring the machines. Currently, the supported cartridges include: VMware, Infrastructure, AWS, and Azure.
- Resource Utilizations: The displayed metrics will be slight different among different monitoring cartridges.

Nodes Explorer view

The *Nodes Explorer* view opens when you click **Explore** in the Kubernetes Nodes Summary view, which includes the following tabs:

General tab: The General tab displays the overall information of the selected Kubernetes node over a
selected period of time, including the Summary and Resource Information table and the Pods table. For
more information, see Node metrics on page 61.

T. Container Environment > Kubernetes N	lode: kuberuleworker2			G+ Monday, June 24, 2019 9:54:53 /	AM - Now 60 minutes	🔻 🕴 🖪 Reports		
				Alarms Severit Alarms Count		ical Warning		
Kubernete	es Node: kub	eruleworker2		Alaritis Counc		-		
General Metrics Events								
Summary and Resource Informa	ition							
Name	kuberuleworker2		Kubelet Endpoint	10,250				
Architecture	amd64		Operating System	linux				
Kernel Version	1101030-021080-021		Container Runtime Version	docker://18.6.3				
Kube Proxy Version	2-122		Kubelet Version	v1.14.1				
Boot ID	an opposite state to be a	NUCLEAR AND A CONTRACTORS	Machine ID	and the second statement of the	State - March			
Pod CIDR			External ID					
Provider ID			Unschedulable	false				
Labels	kubernetes.io/hostnam kubernetes.io/os=linux beta.kubernetes.io/orc beta.kubernetes.io/orc node-role.kubernetes.i kubernetes.io/arch=an	n=amd64 ·linux p/master=	Annotations	flannel.alpha.coreos.com/ flannel.alpha.coreos.com/ flannel.alpha.coreos.com/ volumes.kubernetes.io/co flannel.alpha.coreos.com/ kubeadm.alpha.kubernete node.alpha.kubernetes.io/	backend-type=vxla public-ip=10.4.117 ntroller-managed-a kube-subnet-mana s.io/cri-socket=/va	n .159 ttach-detach=tr ger=true		
Capacity	cpu=4 ephemeral-storage=40 hugepages-2Mi=0 memory=8009824Ki pods=110	137576Кі	Allocatable	cpu=4 ephemeral-storage=36990789981 hugepages=2Mi=0 memory=7907424Ki pods=110				
Status Addresses	Normal			·				
InternalIP	10111-0-0-1-000		Hostname	kuberuleworker2				
Pods								
Search 🔎 🗸								
Name	Status	Cluster	Namespace	Containers	Init Contain	iers		
The Part of the International Content of the	Running	vmwarecluster159	kube-system	1	Contain	1		
	Running	vmwarecluster159	kube-system	1		0		
	Running	vitiwarecluster159	Kubersystem	1		0		

Figure 8. Kubernetes Nodes Explorer view General Tab

 Metrics tab: The Metrics tab displays a Metric Selector allowing you to choose the metrics to be plotted on this dashboard. Charts of CPU Usage, Utilization, Memory Usage, and Network I/O are presented by default.

Figure 9. Kubernetes Nodes Explorer view Metrics Tab

E Container Environment > Kubernetes Node: kuberuleworker2	lleworker2	G+ Monday, June 24, 2019 9:54:53 AM - Now 60 minutes 👻 🔲 Reports - Alarms Seventy Fatal Critical Warning 🛱
General Metrics Events		
Metric Selector Utilization	Metric Selector	X CPU Usage
	CPU Resource	800
	CPU Usage	
	CPU Usage Rate	1400 g
	Filesystem Inode Usage	
09:55 10:00 10:05 10:10 10:15 10:20 10:25 10:30 10:35 1	🕑 Filesystem Usage	10:15 10:20 10:25 10:30 10:35 10:40 10:45 10:50
CPU Utilization — Memory Utilization	Memory Page Faults	CPU Request CPU Limit CPU Usage
Memory Usage	Memory Page Faults Rate	Network I/O
monory oadge	Memory Resource	T1
	Memory Rss	
	Memory Usage	
	Memory Working Set	- B
	Network I/O	
	Network I/O Errors	•
09:55 10:00 10:05 10:10 10:15 10:20 10:25 10:30 10:35	10:40 10:45 10:50 09:55 10:00 10 mory Limit	205 10:10 10:15 10:20 10:25 10:30 10:35 10:40 10:45 10:50

- Event tab: The Event tab lists all the events occur on the nodes.
 - Name: name of the event.
 - Type: type of the event, Warning or Normal.
 - Namespace: namespace of where this event happens.
 - Kind: type of the Kubernetes component on which this event occurs.
 - Involved Object: name of the Kubernetes component on which this event occurs.
 - Source: where this event has been triggered from.
 - Reason: reason of this event.
 - Message: detailed message of this event.

Figure 10. Kubernetes Nodes Explorer view Events tab

				Ala	rms Severi	ty Fa	tal Critical	Warning :
Kubernetes Node:	Kubernetes Node:				arms Count	t I		
	100-111	folia Mola		and the second second				
General Metrics Events								
Events								
					Sea	rch		⊘ + ∃
								-
Name		Namespace		Involved Object		Reason	Messa	
nginx-deployment-7b78fbdd7d-2p85p.15ab663c5c849bb1	Warning	default	Pod	And a second sec	kubelet	Failed	Error: ImagePo	ullBackOff
nginx-deployment-7b78fbdd7d-k76hw.15ab663a473cbee5	Warning	default	Pod	AND CONTRACTORS OF STREET, AND STREET,	kubelet	Failed	Error: ImagePo	ullBackOff
invalidimage-bb487f87-55xhc.15ab663c5c7a65a3	Warning	test	Pod	CONTRACTOR CONTRACTOR	kubelet	Failed	Error: ImagePo	ullBackOff
	Warning	default	Pod	and intervention in the second	kubelet	Failed	Error: ImagePo	ullBackOff
nginx-deployment-7b78fbdd7d-jwblz.15ab663c5c7e8ede					kubelet	Failed	Error: ImagePu	ullBackOff
nginx-deployment-7b78fbdd7d-jwblz.15ab663c5c7e8ede nginx-deployment-7b78fbdd7d-zknhx.15ab663e24cd2052	Warning	default	Pod		Kubacc			
	Warning Warning		Pod	trubilitingg signation for the party	kubelet		Error: ImagePu	

Monitoring Kubernetes Clusters

Kubernetes cluster is a group of kubernetes resources. There are two kinds of nodes inside a cluster, Kubernetes master and Kubernetes nodes. Kubernetes master is responsible for maintaining the desired state of your cluster which Kubernetes node is responsible to run your application and cloud workflows. The *Kubernetes Cluster Quick View*, which appears after clicking **Monitoring > Clusters**, shows the data collected about the selected clusters and namespaces. This view consists of the following two panes:

- The Kubernetes Clusters tree view, which appears on the left of Kubernetes Clusters Quick View, lists the clusters existing in the monitored Kubernetes environment.
- The Kubernetes Clusters Summary view, which appears on the right after you select an individual cluster in the **Kubernetes Clusters** tree view.

Kubernetes Clusters Summary view

The Kubernetes Clusters Summary view appears on the right when you select a node in the Kubernetes Clusters tree view.

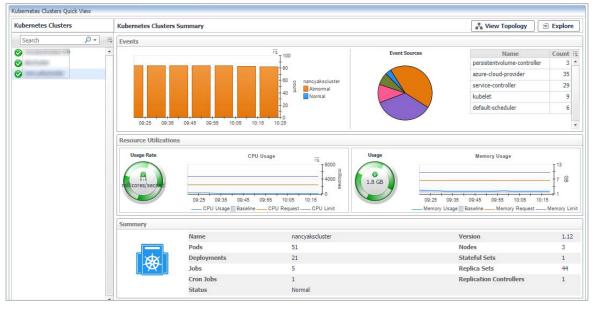


Figure 11. Kubernetes Clusters Summary view

The Kubernetes Clusters Summary view displays the following data:

- *Events*: The events occur on the selected Kubernetes cluster over a selected period of time, which includes:
 - The column chart on the left: Shows the timeline of the occurred events, which indicates at what time and how many events have occurred.
 - The pie chart on the right- Event Sources: Shows the events distribution for different event source.
- *Resource Utilizations*: The resource utilization for the selected Kubernetes cluster over a selected period of time, which includes the following:
 - Usage Rate: Shows the CPU usage summary for the selected Kubernetes cluster based on its total capacity during a selected time period.
 - Memory Usage: Shows the physical memory utilization summary for the selected Kubernetes node, broken into the amounts of memory that is swapped to disk, actively used, and allocated, all during a selected time period.
- Summary: Displays the detailed information about the selected Kubernetes cluster, including Name, Version, Pods, Nodes, Deployments, Stateful Sets, Jobs, and Replica Sets.

Click **Explore** on the upper right of the **Kubernetes Clusters Summary** view to open the Cluster Explorer view, which shows more detailed information about this Kubernetes cluster.

Click **View Topology** on the upper right of the **Kubernetes Clusters Summary** view to open the Cluster Topology view, which shows the topology graph from the application accessible aspect.

Cluster Explorer view

The *Cluster Explorer* view opens when you click **Explore** in the Kubernetes Clusters Summary view, which includes the following tabs:

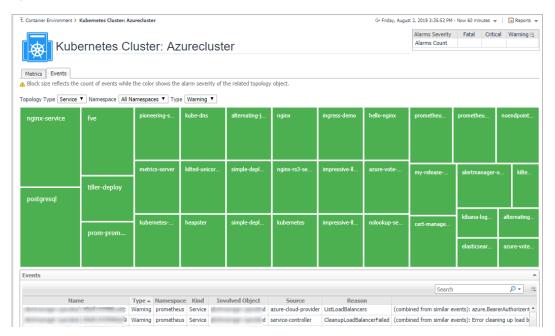
 Metrics tab: The Metrics tab displays a Metric Selector allowing you to choose the metrics to be plotted on this dashboard. Charts of CPU Usage and Memory Usage are presented by default.

Figure 12. Kubernetes Clusters Explorer view Metrics tab

Ξ Container Environment \succ Kubernetes Cluster: vmwarecluster:159		G+ Monday, June 2	4, 2019 9:17:12 AM -	Now 60 min	nutes 👻	🔝 Reports 👻
Kubernetes Cluster: vmwarec	uster159		Alarms Severity Alarms Count	Fatal	Critical	Warning 🗟
Metrics Events	Metric Selector × Select All Select None Search P +	Memory Lie	208			
	CPU Usage CPU Usage CPU Usage Rate Memory Usage	mentory us.	Memory Usage			
08-20 08-25 09-30 09-35 08-40 08-45 09-50 08-55 10:00 10 — CPU UsageCPU Request CPU Limit		19:40 09:45 09: Usage — Memory	50 09:55 10:00 Remest Memo		10:10	+2 B 10:15

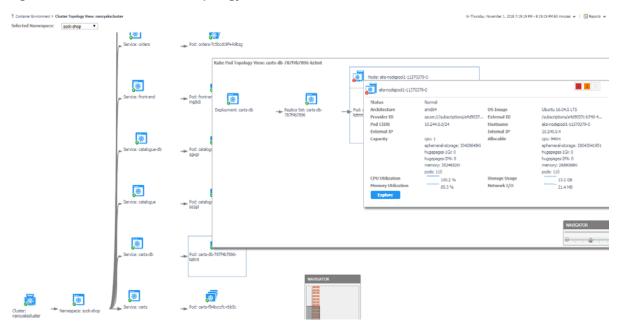
- Events tab: The Events tab shows a Heat Map of the events occur in this cluster. Heat maps will be refreshed automatically when you change either of the following fields:
 - Topology Type: Indicates the Kubernetes components on which the event occurs, including Pod, Node, and Service.
 - Namespace: Use the namespaces to filter the events.
 - Type: Indicates the severity of the event, including warning and normal.
 - **NOTE:** The color in the heatmap indicates the severity of component alarms. Green: indicates normal. Yellow: indicates warning. Orange: indicates critical. Red: indicates fatal.

Figure 13. Kubernetes Clusters Explorer view Events tab



Cluster Topology view

Figure 14. Kubernetes Clusters Topology view



The *topology view* visualizes the relationships between the objects from the pods accessible aspect in your environment through an interactive dependency map. The map illustrates how different components relate to each other, and the levels of the available resources available to them. Click on Pod, another sub topology view will popup to show the relationship from pods controller to storage for the selected Pod. Click other components or click the Pod inside the sub topology view, an information view will popup to show alarms, basic information, some metrics. From the information popup view of Pod, Node and Cluster, click the Explore button will navigate to the explorer view of the selected Pod/Node/Cluster. The **NAVIGATOR** in the bottom-right corner allows you to easily set the zoom level by dragging the slider into the appropriate position.

Monitoring Kubernetes Other Components

Kubernetes other components here including pods controllers, services, ingresses, persistent volumes, secrets and so on. All these components are grouped and displayed in tabs.

- Configurations
- Controllers
- Storage
- Load Balancer

Configurations

Figure 15. Kubernetes Configuration Dashboard

					Search 🔎
Name	Cluster 🔺	Namespace	Labels	Annotations	Configured Data Keys
cluster-info	localckacluster	kube-public			kubeconfig
coredns	localckacluster	kube-system			Corefile
extension-apiserver-authentication	localckacluster	kube-system			client-ca-file, requestheader-extra-headers-prefix, requestheader-client-ca-file, requestheader-ca-file, requesthead
kube-flannel-cfg	localckacluster	kube-system	[app=flannel], [tier=node]		net-conf.json, cni-conf.json
kube-proxy	localckacluster	kube-system	[app=kube-proxy]		config.conf, kubeconfig.conf
kubeadm-config	localckacluster	kube-system			ClusterStatus, ClusterConfiguration
kubelet-config-1.13	localckacluster	kube-system			kubelet
metrics-server-config	localckacluster	kube-system	[addonmanager.kubernetes.io/m		NannyConfiguration
fair-lambkin-elasticsearch-curator-config	nancyakscluster	default	[heritage=Tiller], [app=fair-lamb		config.yml, action_file.yml
impressive-llama-mariadb-master	nancyakscluster	default	[heritage=Tiller], [app=mariadb		my.cnf
impressive-llama-mariadb-slave	nancyakscluster	default	[component=slave], [release=im		my.cnf
impressive-llama-mariadb-tests	nancyakscluster	default			run.sh
metricbeat-config	nancyakscluster	default	[k8s-app=metricbeat], [app=fair		metricbeat.yml
metricbeat-modules	nancyakscluster	default	[component=fair-lambkin-elastic		system.yml, kubernetes.yml
sysdig-agent	nancyakscluster	default		[kubectl.kubernetes.io/last-appli	dragent.yaml
understood-zebra-elasticsearch-curator-config	nancyakscluster	default	[release=understood-zebra], [he		action_file.yml, config.yml
aks-nodepool1-11370379-0-config-5fat4dhcbf	nancvakscluster	kube-system			kubelet

The Configurations dashboard includes Kubernetes Secret and Config Map.

- A Kubernetes Secret is an object that contains a small amount of sensitive data, such as a password, a token, or a key. Such information might otherwise be put in a Pod specification or in an image; putting it in a Secret object allows for more control over how it is used, and reduces the risk of accidental exposure.
- A Kubernetes Config Map binds configuration files, command-line arguments, environment variables, port numbers, and other configuration artifacts to your Pods' containers and system components at runtime. Config maps allow you to separate your configurations from your Pods and components, which helps keep your workloads portable, makes their configurations easier to change and manage, and prevents hardcoding configuration data to Pod specifications.

Controllers

Figure 16. Kubernetes Controllers Dashboard

(Deployment	Replica Set Replication Cor	itroller D	aemon Set	5	Statefu	ul Set		Job	G	on Job						
														Search	P	•	
Alarms	Status	Name	Cluster 🔺	Namespace	Replicas	Pods	Replica Sets	Is Paused	Min Ready Seconds	Progress Deadline Seconds	Revision History Limit	Rollback To Revision		Strategy			
8	Normal	fglam	localckacluster	default	1	1	1	False		2,147,483,647	2,147,483,647		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
8	Normal	fve-app	localckacluster	default	1	1	2	False	5	600	10		[RollingUpdate]	Max Surge:25%,Max Un	available:2	25%	
8	Normal	postgresql	localckacluster	default	1	1	1	False		2,147,483,647	2,147,483,647		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
<u>A</u>	Normal	coredns	localckacluster	kube-system	2	2	1	False		600	10		[RollingUpdate]	Max Surge:25%,Max Un	available:1	L.	
0	Normal	heapster	localckacluster	kube-system	1	1	1	False		2,147,483,647	2,147,483,647		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
\$	Abnormal	metrics-server-v0.3.1	localckacluster	kube-system	1	1	1	False		600	10		[RollingUpdate]	Max Surge:25%,Max Un	available:2	25%	
0	Normal	[Status Detail]									10		[RollingUpdate]	Max Surge:25%,Max Un	available:2	25%	
<u>î</u>	Normal		ssing:True, Reason:NewReplicaSetAvailable, Message:ReplicaSet "metrics-server-v0.3.1-8455948d4c" has successfully 10 [RollingUpdate]Max Surge:25%,Max Unavailable:25%														
2	INOLITION	progressed.								647	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Mormal	Available:False, Reason:MinimumReplicasUnavaila [Replicas Detail]	able, Message:Dep	ployment does	not have	minin	num ava	ilability.		647	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
8		Replicas:1								647	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Normal	Unavailable Replicas:1									10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Normal	alternating-jackal-nginx-ingress-default-backend	nancyakscluster	kube-system	1	1	1	False		600	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
Â	Normal	coredns	nancyakscluster	kube-system	2	2	2	False		2,147,483,647	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Normal	coredns-autoscaler	nancyakscluster	kube-system	1	1	1	False		600	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
<u>A</u>	Normal	heapster	nancyakscluster	kube-system	1	1	2	False		2,147,483,647	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Normal	kibana-logging	nancyakscluster	kube-system	1	1	1	False		600	10		[RollingUpdate]	Max Surge:25%,Max Un	available:2	25%	
0	Normal	kilted-unicorn-nginx-ingress-controller	nancyakscluster	kube-system	2	2	1	False		600	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Normal	kilted-unicorn-nginx-ingress-default-backend	nancyakscluster	kube-system	1	1	1	False		600	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
<u>A</u>	Normal	kubernetes-dashboard	nancyakscluster	kube-system	1	1	4	False		600	10		[RollingUpdate]	Max Surge:0,Max Unava	ilable:1		
0	Normal	metrics-server	nancyakscluster	kube-system	1	1	4	False		600	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Normal	tiller-deploy	nancyakscluster	kube-system	1	1	1	False		600	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
0	Normal	tunnelfront	nancyakscluster	kube-system	1	1	2	False		2,147,483,647	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
\$	Abnormal	invalidimage	nancyakscluster	test	2	2	1	False		2,147,483,647	10		[RollingUpdate]	Max Surge:1,Max Unava	ilable:1		
4	Normal	unabletoschedule	nancvakscluster	test	1	1	1	False		2.147.483.647	10		[RollingUpdate]	Max Surge: 1. Max Unava	ilable:1		

A controller manages a set of pods and ensures that the cluster is in the specified state. Instead of manually creating a pod, controllers can be used to create pods and to manage the pods. For example, the pods maintained by a replication controller are automatically replaced if they fail, get deleted, or are terminated. The *Controllers* dashboard presents the information related to the following controller types: *Deployment, Replica Set, Replication Controller, Daemon Set, Stateful Set, Job,* and *Cron Job.*

Storage

Figure 17. Kubernetes Storage Dashboard

							Search
Alarms	Status	Name	Cluster 🔺	Reclaim Policy	Claim	Storage Class	Source Type
o	Bound	pv-sc-no-sc-customize	localckacluster	Retain	pvc-sc-pv-customize-sc	no-sc-customize	HostPath
0	Available	pv-sc-default	localckacluster	Retain		default	HostPath
0	Available	pv-sc-invalid-provisioner	localckacluster	Retain		sc-invalid-provisio.	HostPath
0	Bound	pv-invalid-nfs	localckacluster	Recycle	pvc-invalid-sc-pv	slow	NFS
0	Available	pv-pvc-oversize	localckacluster	Retain		sc-oversize	HostPath
0	Available	pv-pvc-acm1	localckacluster	Retain		sc-pvc-acm1	HostPath
0	Bound	pvc-2b95e22d-dc28-11e8-b2ed-befa22179703	nancyakscluster	Delete	data-mehdb-1	default	AzureDis
0	Bound	pvc-45f1fe1e-5f54-11e9-b660-16063de8b09f	nancyakscluster	Delete	data-elasticsearch-2	default	AzureDis
0	Bound	pvc-59cb23a5-fd17-11e8-adf4-de8994810bc3	nancyakscluster	Delete	data-elasticsearch-0	default	AzureDis
0	Bound	pvc-7049bcb8-fd17-11e8-adf4-de8994810bc3	nancyakscluster	Delete	data-elasticsearch-1	default	AzureDis
0	Bound	pvc-90f76a94-2e94-11e9-810c-0a130f143c9f	nancyakscluster	Delete	alertmanager-prom-prometheus-operator-alertmanager-db-al	default	AzureDis
0	Bound	pvc-9727fba6-2e94-11e9-810c-0a130f143c9f	nancyakscluster	Delete	prometheus-prom-prometheus-operator-prometheus-db-prom	default	AzureDis

The Kubernetes storage contains volumes, storage class, persistent volume, and persistent volume claim. Volumes are on-disk files used by the containers for persistent their data as well as sharing with other containers. The *Storage* dashboard shows the information about the following storage classes:

- Storage Class provides a way for the administrator to describe the "class" of storage they offer.
- Persistent Volume subsystem provides an API for users and administrators that abstracts details of how storage is provided from how it is consumed.
- *Persistent Volume Claim* is used for dynamic volume provisioning which allow storage volumes to be created on-demand.

Load Balancer

S.	ervice Ingress	Endpoint						
5.	ingress	Endpoint						
Alarms	Name	Cluster 🔺	Namespace	Туре	Cluster IP	External IPs	External Name	IP Add
2	fve	localckacluster	default	NodePort	10.103.174.0			
2	fve-app	localckacluster	default	ClusterIP	10.111.36.15	1181781781		
2	kubernetes	localckacluster	default	ClusterIP	10.96.0.1			
2	postgresql	localckacluster	default	ClusterIP	10.98.70.60			
2	test	localckacluster	default	ClusterIP	10.99.240.162			
2	heapster	localckacluster	kube-system	ClusterIP	10.110.175.65			
2	kube-dns	localckacluster	kube-system	ClusterIP	10.96.0.10			
2	metrics-server	localckacluster	kube-system	ClusterIP	10.109.149.172			
2	kubernetes	localkubecluster159	default	ClusterIP	10.96.0.1			
2	kube-dns	localkubecluster159	kube-system	ClusterIP	10.96.0.10			
2	azure-vote-back	nancyakscluster	default	ClusterIP	10.0.71.228			
2	azure-vote-front	nancyakscluster	default	LoadBalancer	10.0.116.152			
3	hello-nginx	nancyakscluster	default	NodePort	10.0.28.128			

Figure 18. Kubernetes Load Balancer Dashboard

The *Load Balancer* dashboard includes information about Kubernetes service, endpoint, and ingress. A Kubernetes ingress can provide load balancing, SSL termination, and name-based virtual hosting. A Kubernetes service is an abstraction which defines a logical set of pods and a policy by which to access them - sometime called micro-services. Kubernetes will update the endpoint whenever the set of pods in a service changes.

Alarms

					-	ents	Clusters		Pods	Controllers	Storages	Load Balancers	
Se	elect All L	Inselect A	All Ackn	owle	dge Clear							Search	<i>p</i> -
	Time 🔻	Severity	Ack'ed		Impacting	Source	Rule Name	Alarm Message					
	5/15/19 1:22 AM	<u> </u>	false	*	etcd- kubeckamaster	KubePod	Kubernetes Pod Memory	The cpu usage 131.2r	nb of pod etcd-kube	eckamaster in namesp	ace kube-systen	n in cluster localckacluster o	ver threshold :
	5/15/19 1:11 AM	Δ	false	8	postgresql- 6558cdf45c- 4s59k	KubePod	Kubernetes Pod Memory	The cpu usage 245.9r	nb of pod postgreso	ql-6558cdf45c-4s59k i	n namespace que	estfve in cluster nancyaksclu	ister over thre
	5/14/19 11:36 PM	8	false	8	fve-app- 76cccb864c- 968z6	KubePod	Kubernetes Pod Memory	The memory utilizatio	n 99.32% of pod fv	e-app-76cccb864c-96	8z6 in namespac	e default in cluster localcka	cluster reache
	5/14/19 11:36 PM	۵	false	8	kube-flannel-ds- amd64-j5n62	KubePod	Kubernetes Pod Memory	The memory utilizatio 90.00%.	n 94.75% of pod ku	ube-flannel-ds-amd64	j5n62 in namesp	ace kube-system in cluster	localcluster15
	5/14/19 11:36 PM	8	false	8	kube-apiserver- kubeckamaster	KubePod	Kubernetes Pod Memory	The memory usage 54	9.9mb of pod kube	e-apiserver-kubeckami	aster in namespa	ce kube-system in cluster lo	ocalckacluster
	5/14/19 11:36 PM	8	false	8	fglam-f7f795b8- 65k2c	KubePod	Kubernetes Pod Memory	The memory usage 8	i8.2mb of pod fglan	n-f7f795b8-65k2c in n	amespace defau	lt in cluster localckacluster o	over threshold
	5/14/19 11:36 PM	0	false	•	fve-app- 76cccb864c- 968z6	KubePod	Kubernetes Pod Memory	The memory usage 3.	9gb of pod fve-app	-76cccb864c-968z6 in	namespace defa	ult in cluster localckacluster	over thresho
	5/14/19 11:36 PM	۲	false	•	tqa-loadtest- jmeter-slaves- 768d8c4dc9-sk	KubePod	Kubernetes Pod Memory	The memory usage 10 512.0mb.	103.4mb of pod tqa	-loadtest-jmeter-slave	s-768d8c4dc9-sł	chbk in namespace tqa in cli	uster localclus
	5/14/19 11:36 PM	٩	false	•	jmeter-operator- 784bd76967- kfyrx	KubePod	Kubernetes Pod Memory	The memory usage 38 256.0mb.	6.6mb of pod jmet	er-operator-784bd769	67-kfvrx in nam	espace kube-system in clust	er localcluste

Figure 19. Kubernetes Alarms Dashboard

The *Alarms* dashboard displays a list of alarms generated against the monitored Kubernetes environment. Use this view to quickly identify any potential problems related to a specific Kubernetes component.

Capacity Management

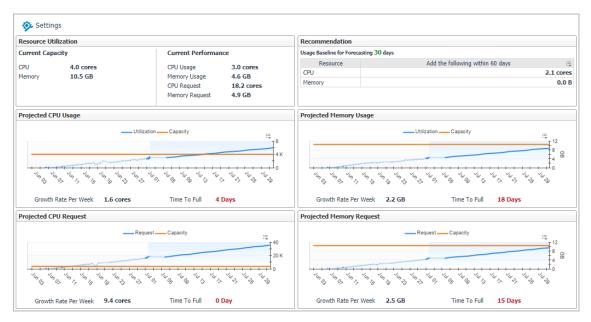
Foglight for Container Management provide capacity management feature for Kubernetes. This feature uses historical data to predict the trend and usage within a specific future period.

NOTE: If the Capacity Management tab is not displayed, ensure the following:

1. You have purchased a license for Capacity Management. If not, contact Quest Support to purchase a license.

2. You have the Container Administrator role.

Figure 20. Capacity Management for Kubernetes



The Capacity Management dashboard contains the following fields:

- Setting: Click to change the following values:
 - Baseline for Forecasting: Defines the historical period used for the calculations of metric views, current capacity, and recommended resources in the Resource Utilization view. The default value is 60 Days Trending.
 - Time Frame: Defines the predicted period for calculating metric views, current capacity, and recommended resources in the Resource Utilization view. The default value is Next 30 Days.
- Resource Utilization:
 - Current Capacity: current resource capacity.
 - Current Performance: current resource usage.
- Recommendation:

In this section, it shows how many resources are recommended to be added in the current trend, so as to meet the predicated usage.

- Projected CPU/Memory Usage: Shows the historical data and the predicted usage trend within the configured future period.
- *Projected CPU/Memory Request*: Shows the historical data and the predicted request trend within the configured future period.
 - Utilization: usage.
 - Capacity: upper bound which the usage might reach.
 - Growth Rate per Week: growth amount of the resource.
 - Time to Full: how many days the resource usage/request will reach the capacity.
 - **NOTE:** If a value *Never* is displayed at *Time to Full*, which means the usage/request trend is declining and the usage/request will never reach the capacity.

Optimizer

The Optimizer view appears after clicking Container > Kubernetes > Optimizer.

- **NOTE:** If the Optimizer tab is not displayed, ensure the following:
 - 1. You have purchased a license for Optimizer. If not, contact Quest Support to purchase a license.
 - 2. You have the Container Administrator role.

NOTE: The displayed views are varied if the cluster hosts are monitored by the agents of VMware, AWS, or Azure.

Figure 21. Kubernetes Optimizer Dashboard

Container Environment	Cluster select	or						G+ Thursday, June 27, 2019	3:49:58 PM - 4:49:58 PM 6	50 minutes 👻 📔 Reports 🦷
Kubernetes	Swarm (Prev	iew)								Analytics 🔻
		All Nam								
Monitoring Configurat	tions Controllers	Storage Load Bala	incer Alarms	Capac	ity Management	Optimizer Adminis	tration	Ŷ	🖌 Settings	Automate
VM Resources	CPU CPU	Memory	Storage	Unused	Resources Po	Detential Zombies				
ជា Reclaim								Reclaim Now	🖾 Reclaim La	ater
Exclude	Show Exclu	uded Items 0								
Name 4		space Type	CPU Usage	Memory	Network Trans	fer File System Transf	er	Recor	nmendation	
	defaul		-	0 MB	0	0 MB		ployment nfs-client-nfs-client		ace default.
 Istitution prime 	tqa	Deployment	0	0 MB	0	423.1 KB	Delete De	ployment tqa-loadtest-grafar	a in namespace tqa.	
	tqa	Deployment	0	0 MB	0	0 MB	Delete De	ployment tqa-loadtest-influx	lb in namespace tqa.	
	tqa	Deployment	0	0 MB	0	0 MB	Delete De	ployment tqa-loadtest-jmeter	r-master in namespace	e tga.
	tqa	Deployment	0	0 MB	0	223.6 KB	Delete De	ployment tqa-loadtest-jmeter	r-slaves in namespace	tqa.

The Optimizer view includes the following elements:

• **Cluster Selector**. The cluster selector is located at the top of the Optimizer view and allows you to select the environment that you want to optimize.

NOTE: The Namespace selector doesn't work for Optimizer dashboard.

- **Settings**. The Settings dialog box is used to change the time period and properties that are used for calculation. For more information, see Settings on page 40.
- Automate. Use the Automate menu to set the criteria for automatically sending recommendations for improvements. Currently, this button only functions for CPU and Memory when a VMware cluster is selected.
- **Reclaim Now** and **Reclaim Later** buttons. System administrator can select a VM from the list and review the Reclaiming Savings bar for information about how many resources can be reclaimed.
- **NOTE:** The **Reclaim Now** and **Reclaim Later** buttons are enabled only after selecting a checkbox from the table. Currently, the two buttons only function for **VM Resources**, **CPU**, and **Memory** when a VMware cluster is selected.

The **Automate**, **Reclaim Now**, and **Reclaim Later** buttons are displayed only when a VMware cluster is selected.

- **Exclude** button. Select an object you want to exclude from the table to enable the Exclude button, and click Exclude. Then, this object is added to the list of excluded objects under a specific category.
- Show Excluded Items button. Click the Show Excluded Items button to view the excluded objects. The Settings dialog box appears. For more information, see
- VM Resources/VM Resizing. Shows instance or virtual machine name, utilization, recommendations for both CPU and memory resources, and savings.
- **CPU**. Shows instance or virtual machine name, utilization, recommendations for CPU resource, and estimated savings.

- **Memory**. Shows instance or virtual machine name, utilization, recommendations for memory resource, and estimated savings.
- Storage. Shows virtual machine name, utilization, storage and modify recommendations, and savings.
- **NOTE: VM Resizing** will be displayed when a cloud cluster is selected. **VM Resources**, **CPU**, **Memory**, and **Storage** will be displayed when a VMware cluster is selected.
 - · Unused Resources table. Detects and shows those unused resources in container environment.

For example, persistent volume stays unused for more than 3 months. persistent volume stays in unbound status. This is due to the Unused Resources configuration in Settings.

 Potential Zombies table. Detects and shows the potential pod controllers in container environment, including Deployment, Daemon Set, Stateful Set, Replication Controller, as well as Pod that is not managed by any Pod Controller.

For example, if all pods managed by a pod controller are zombies, then we might suggest you to delete the whole pod controller.

Settings

Use the Settings menu to define the default optimization settings for your environment. The Settings Dialog box provides information about the following components:

- Configuration tab
- Waste tab
- Excluded tab
- Credentials tab
- Constraints tab

Configuration tab

Figure 22. Configuration tab

ttings Dialog								
*				+	-			
onfiguration W	/aste	Excluded	Credentials	Constr	aints			
	These sett	ings are for CPU.	Memory and Storage	Optimization				
		1201	hresholds					
CPU		4	lemory		Storage			
Warning: 75% Critical: 83%		Warning: 8	ming: 90% Crit	ical: 95%				
Resource C		טי	Memory		Storage			
Decourse			dation Calculation		Etas	200		
Reserve Margin	5	%	5 9	6	5	%		
	-	-		1,722	-			
Acceptable Variation	3 %	50 MHz	3 % 50	MB	3 %	1024 MB		
Recommended Basis	Maximum Pea	k Utilization 🔻	Maximum Peak Util	ization V	Maximum Pea	k Utilization		
Peak analysis period: 1	i minute(s)			Thr	eshold for mergin	g peaks: 5%		
Evaluate calculation ove	er this period of ti	me 30 Da	ay(s)	Hist	ory Period 30	Day(s)		
						Save Can		

The Configuration tab provides the recommended settings for CPU, memory, and storage optimization.

• **Thresholds**. Provides the values of a resource metric that define the Warning and Critical levels (for CPU, memory, and storage).

• **Recommendation Calculation** area. Allows you to define the following parameters for optimizing the CPU, memory resources in your environment, Storage resources not supported at current version:

To save any changes made to the **Configuration** settings, click **Save** at the bottom of the tab.

Waste tab

Figure 23. Waste tab

Waste Exclu	⊠ ude			
Th	ese settings are for Unused Resour	ces and Pot	ential Zombies	
Determine as waste if :	Resource has been created	30 🔻	Days	
	Persistent Volume Status	 Availa Relea Failed 	sed	
Detemine as a potential zomb	ie if :			
	d used for average calculation is source utilization	30 ▼	Days	
100.0	Millicore for CPU	100.0	KB for Network Transfer	
100.0	MB for Memory	100.0	MB for Disk Transfer	
Excluded N	amespace			
kube-syste	m,kube-public			
			(

The **Waste** tab allows you to configure the settings for determining resources wasted in your environment. These include unused resources and potential zombie Pod controllers.

- Determine as waste if: used to filter Unused Resources.
 - Resource has been created [time] days: Resources that has been created more than the set days will be considered here.
 - Persistent Volume Status: By default, select Available and Failed. For detailed information, go to https://kubernetes.io/docs/concepts/storage/persistent-volumes/#phase.
- Determine as a potential zombie if: used to filter Potential Zombies.

In container environment, Potential Zombie Pod Controller is considered here, including Deployment, Daemon Set, Stateful Set, Replication Controller, and Pod that is not managed by any Pod Controller. Settings work for single pod managed by Pod Controller. If all pods or partial pods of a Pod Controller are considered as zombies, different recommendations will be generated.

- *Time period used for average calculation is [time] days*: The average metrics for the pods are calculated, so a time range should be set to calculate the average value.
- Average resource utilization: only if a pod's metrics satisfy all the conditions, it will be considered to be a potential zombie pod.
- Excluded Namespace: pods in the namespace can be excluded in the Potential Zombies check.

To save any changes made to the Waste settings, click Save at the bottom of the tab.

Excluded tab

Figure 24. Excluded tab

	Remove	iş.
CPU	Name	Туре
		KubeDeployment
Memory		
Storage		
-		
Unused Resources		
Potential Zombies		
Potential Zombies		
Potential Zombies		

The **Excluded** tab allows you to remove a resource from the list of excluded objects. The **Excluded** tab includes the following information:

- On the left side, a navigation tree, that allows you to select the resource category.
- On the right side, the list of resources excluded from the selected category.

To remove resources from the list of **Excluded** objects, select the check boxes for these resources and click **Remove**. To save any changes made to the **Excluded** settings, click **Save** at the bottom of the tab.

The Excluded tab can also be accesses by clicking Show Excluded Items on the Optimizer tab.

Credentials tab

Figure 25. Credentials tab

Settings Dialog					
Configuration		Excluded		Constraints	
Add a New Cr	edential Group 🛛 🌜	Remove Credential (Groups	Search	<i>p</i> -
				Credentials	
🖾 🔲 🚡 Optimize	Storage-example		Administrator@	1000	
					Save Cancel

This tab is available in VMware environment. The **Credentials** tab allows you to add, edit, and remove credentials groups. This tab is only for the Storage rightsizer.

Constraints tab

Figure 26. Constraints tab

Settings Dialog								
1 p					[*		
onfiguration	Waste	Excluded	Crede	entials	Cor	nstraints		
Add a New Co	onstraint Group	Remove Constraint G	Groups		Sea	rch		<i>p</i> -
	Name 🔺		Min vCPU	Max vCPU	Min Memory	Max Memory	Min Storage	Max Storage
	Use the	above Add icon to add	d one or mo	ore Cred	ential Grou	ps.		

This tab is available in VMware environment. The **Constraints** tab allows you to set custom thresholds for select objects in the environment. These recommendations are displayed in the **Optimizer** tab > **VM Configuration**/ **CPU/ Memory/ Storage** views > **Modify Recommendation** column. Use this tab to add, edit, and remove constraints groups.

i IMPORTANT: A virtual machine may have several partitions. VM environment makes recommendations for each partition separately, but the custom constraints can be set only for the entire VM (not for individual partitions). Therefore, the custom constraint for storage are applied to all partitions on the selected VM.

Administration

Figure 27. Kubernetes Administration Dashboard

Container Environment					G+ Monday,	July 15, 2019 10:07:10 A	AM - 11:07:10 AM 60 minutes 👻 📔 🗈	Reports 🛪
Kubernetes	Swarm (Preview)						Analytics	•
159cluster	• •	All Namespaces		Ŧ				
Monitoring Configurations	Controllers Storage	Load Balancer Alarms	Capacity Management	Administratio	n			
Tasks:								
Create Do	cker Agent							
(
Agents								
📀 Add 🤣 Refresh 🛛 🕛 Act	Kubernetes Swarm (Preview) Analytics Sigcluster All Namespaces All Namespaces Storage Load Balancer Alarms Configurations Controllers Storage Storage Load Balancer Alarms Capacity Management Administration Administration Create Docker Agent Search Image: Controllers Add & Refresh Activate Deactivate Start Data Collection Stor Data Monitor Monitor Collection Alarms Edit Properties Download Log Agent Version Monitor Collection Alarms Edit Properties Download Log Agent Version							
🔲 Agent Name 🔺	Foglight Agent Manag	ger Host Ac	tive Data Collection	Alarms	Edit Properties	Download Log	Agent Version	
Monitor Monitor	All of the second second	1	g g		2	1	Version Up To Date	
Monitor _ or an or ac	10000	1	1		2		Version Up To Date	

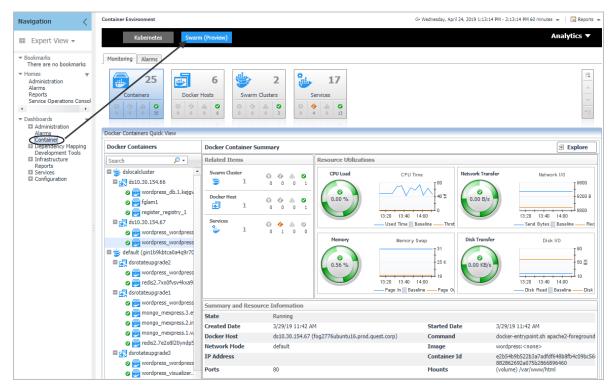
The Administration dashboard supports new agent creation and existing agents management. Use Create Docker Agent or Add to create a new agent. See Creating and Activating a Kubernetes Agent on page 19 for more information. Use Activate, Deactivate, Start Data Collection, Stop Data Collection, Remove, and Update Agent to manage the agent. Click Edit Properties to update the properties of the chosen agent.

i NOTE: The Administration dashboard can be accessed only when the users have both the Administrator role and the Container Administrator role. To grant the users with the Container Administrator role, go to Administration > Users & Security management under Administer Server > Manage Users, Groups, Roles > Roles tab.

Docker Swarm

The *Docker Container Quick View* appears after clicking **Monitoring > Containers**. Click **Swarm (Preview)** from the header on top to switch to Docker Swarm dashboard.





Monitoring Docker Containers

This view consists of the following two panes:

•

- The Docker Containers tree view, which appears on the left of Docker Containers Quick View, lists the
 containers existing in the monitored Docker environment. The containers in the tree view are grouped by
 cluster > docker host > container.
 - The Docker Container Summary view, which appears on the right after you select an individual container in the **Docker Containers** tree view.

Docker Container Summary view

The **Docker Container Summary** view appears on the right when you select a container in the **Docker Containers** tree view.

ntainer Environment		G	+ Wednesday, April 24, 2019 1:13:	14 PM - 2:13:14 PM 60 minutes 👻 📔 Repor
Kubernetes Swarm	n (Preview)			Analytics v
25 Containers O O A O		2 17 Services 4 0 13 3 0 0 13		
Docker Containers	Docker Container Summary			⊕ Explore
Search 🔎 🗸	Related Items	Resource Utilizations		
dslocalcluster dslocalc	Swarm Cluster Image: Constraint of the state of th		80 0 0 4:00 0 0 0 aseline Throt Disk Trans 0.00 KB/ 4:00 19 0 0	Peolo Pe
 mordpress_wordpress mongo_mexpress.3.e 	Summary and Resource Information State Running			
🛛 👼 mongo_mexpress.2.ir	Created Date 3/29/19 11:42 A	M	Started Date	3/29/19 11:42 AM
mongo_mexpress.1.w redis2.7e208l20yndp5	Docker Host ds10.30.154.67	(fog2776ubuntu16.prod.quest.corp)	Command	docker-entrypoint.sh apache2-foregrou
	Network Mode default		Image	wordpress: <none></none>
💷 🚮 dsrotateupgrade3	IP Address		Container Id	e2b54b9b522b3a7adfdf648b8fb4c09bc

Figure 29. Docker Container Summary view

The Docker Container Summary view displays the following data:

- Related Items: Shows the related Docker components grouped by type as well as the associated alarms.
- Resource Utilizations: The resource utilization for the selected Docker Container over a selected period of time, which includes the following:
 - CPU Load: Shows the CPU utilization of the selected container.
 - CPU Time: Shows the used time and throttled time of the selected container.
 - Network Transfer. Shows the transfer bytes rate of the selected container over a selected period of time.
 - Network I/O: Shows the total send/receive bytes of the selected container.
 - Memory: Shows the memory utilization of the selected container.
 - Memory Swap: Shows the mounts of memory pages that are swapped to disk.
 - Disk Transfer. Shows the disk transfer bytes rate of the selected container over a selected period of time.
 - Disk I/O: Shows the disk read/write bytes of the selected container.
- Summary and Resource Information: Displays the detailed information about the selected Container, including State, Command, Created Time, Started Time, Image, and so on.

Click **Explore** on the upper right of the **Docker Container Summary** view to open the Container Explorer view, which shows more detailed information about this container.

Container Explorer view

The *Container Explorer* view opens when you click **Explore** in the Docker Container Summary view, which includes the following tabs:

Monitoring tab: The *Monitoring* tab displays the overall information of the selected container over a selected period of time, including the *Summary and Resource Information* table, Resource Management table as well as the Metrics list. To set the Metrics list displayed, go to **Action > General > Metric Selector**. For more information, see Container metrics on page 61.

Figure 30. Docker Container Explorer view Monitoring Tab

Monitoring				
Summary and Resource Inf	ormation		A A	Properties
Summary and Resource Information State Running Created Date 4/3/19 3:47 AM Started Date 4/3/19 3:47 AM Started Date 4/3/19 3:47 Docker Host localdshot67 Container IId 2fad774837 Docker Host localdshot67 Command docker-entry Network Mode default IP Address Ports 80 Mounts (volume) /vz Environment Variables WORDPRESS, DB_PASSWORD-wordpress com.docker. WORDPRESS, DB_USER-wordpress com.docker. com.docker. PHPIZE, DEPS-apache2 dpress.2.vor dpress.2.vor APACHE_EINVARS-/etck/patcher/apache2 dpress.2.vor dpress.2.vor APACHE_EINVARS-/etck/patch				
Created Date	4/3/19 3:47 AM	Started Date	4/3/19 3:47	
Docker Host	localdshost67	Container Id	2fadf74a87d	Create dashboard
ímage	wordpress: <none></none>	Command	docker-entry	Reports
Network Mode	default	IP Address		✓ Metric Selector
Ports	80	Mounts	(volume) /va	Select All Select None Search 🔎 🗸
WORDPRESS DD_PASSWORD—wordpress WORDPRESS DD_EXER=wordpress PATH=fusr/local/sbin:/usr/local/bin:/usr /sbin:/wsr/local/sbin:/usr/local/bin:/usr pkp-config:rozc_ PHP_UIL_DIFS_/sct/apache2/envars APACHE_ENV/ASS_/sct/apache2/envars APACHE_ENV/ASS_/sct/apache2/envars APACHE_ENV/ASS_/sct/apache2/envars PHP_EXTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2disable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2-rdisable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2-rdisable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2-rdisable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2-rdisable-cgi PHP_CTRA_CONFIGURE_ARGS—with-apx2-rdisable-cgi PHP_CTRA_CONFIGURE_ARGS=with-apx2-rdisable-cgi PHP_CTRA			com.docker. com.docker. com.docker. com.docker. com.docker. com.docker.	
Swarm Information	ker Container: wordpress_wordpress_2.vqrefbjvasmbyuiporstzy67 Intering many zu Resource Information te Running te Running dated tate 47/19/3/7 dated tate 47/19/3/7 Gorenti (d) Zindfrägit Zindfrägit ter Nots oold doubte/ to 0 Hourits (volume) /vin vond Press: Conce> Command doker Hot Diddenset tronment Variables 00 WODDPESS: DB, HOST-db/306 Labels com.doker, com.do			
Swarm Cluster	inter: wordpress_wordpress_2.vqrefbjyasmbyuipors4zy67 sure: Information			
Swarm Node	fog2776ubuntu16 (avmi06px91fzcsv3uztyk3ici)	wordpress.2.vgrefbjvasmbyuipors4zy67 Wether and the second docker entry Container Id 22/df748747 DB pOST=dc3306 Labels com.docker. DB pOST=dc3306 Labels com.docker. Com.doc		
lesource Management	Container: wordpress. 2. vqreribjvasmbyuipors4zy67 ng and Resource Information and Code 4 47/19.347 AM Started Date 47/19.347 tost localdohot67 Container Id 27ad7487 tost localdohot67 contrant dode 4/3/19.347 tost localdohot67 tost l			
CPL		mory Utilization	- %	

Monitoring Docker Hosts

This view consists of the following two panes:

- The Docker Hosts tree view, which appears on the left of Docker Hosts Quick View, lists the docker hosts existing in the monitored Docker environment. The docker hosts in the tree view are grouped by cluster > docker host.
- The Docker Host Summary view appears on the right after you select an individual docker host in the **Docker Hosts** tree view.

Docker Host Summary view

The **Docker Host Summary** view appears on the right when you select a docker host in the **Docker Hosts** tree view.



tainer Environment		G+ Wednesday, April 24, 2019 1:23:16 Pl	M - 2:23:16 PM 60 minutes 👻 🛛 🖪 Repor
	n (Preview)		Analytics 🔻
Ionitoring Alarms		17 Services	
locker Hosts	Standalone Docker Host Summary		🖲 Explore
Search 🔎 🗸	Related Items	Resource Utilizations	
 default (gin1b9kbtca0a4q9r?) <lidefault (gin1b9kbtca0a4q9r?)<="" li=""> <lidefault (gin1b9kbtc<="" td=""><td>Swarm Cluster Image: Containers Image: Containers Image: Containers Image: Containers Image: Containers</td><td>This Host is Not Currently Being Monitored.</td><td>Network Transfer Rate</td></lidefault></lidefault>	Swarm Cluster Image: Containers Image: Containers Image: Containers Image: Containers Image: Containers	This Host is Not Currently Being Monitored.	Network Transfer Rate
	Summary and Resource Information Container Count by Status All (10), F Operation System CentOS Linux 7	Aused (0), Stopped (5), Running (5)	13:30 13:50 14:10 —— Transfer Rate Baseline

The Docker Host Summary view displays the following data:

- Related Items: Shows the related Docker components grouped by type as well as the associated alarms.
- Resource Utilizations: The resource utilization for the selected docker host over a selected period of time, which includes the following:
 - CPU Load: Shows the CPU utilization of the selected docker host.
 - CPU Used: Shows the used CPU resources aggregated from the containers running on the docker host.
 - Network I/O and Network Transfer Rate: Shows the transfer bytes rate of the selected docker host
 aggregated from the containers running on the docker host over a selected period of time.
 - Memory and Memory Consumed: Shows the memory consumed bytes aggregated from the containers running on the docker host.
 - Disk I/O and Disk Transfer: Shows the disk transfer bytes rate of the selected docker host
 aggregated from the containers running on the docker host over a selected period of time.
- Summary and Resource Information: Displays the detailed information about the selected docker host, including Container Count by Status, Operating System, Memory Total, and so on.

Click **Explore** on the upper right of the **Docker Host Summary** view to open the Docker Host Explorer view, which shows more detailed information about this container.

Docker Host Explorer view

The *Docker Host Explorer* view opens when you click **Explore** in the Docker Host Summary view, which includes the following tabs:

- Monitoring tab: The Monitoring tab displays the overall information of the selected docker host over a selected period of time, including the Summary and Resource Information table, Containers table, Images table, and Volumes table.
 - **NOTE:** All the docker host metrics are calculated from the aggregated metrics of the containing containers on the docker host.

	Environment > Docker Host: dsrotateupgrade3					G• Thursday	, April 25, 20	19 10:39:16	AM - Now 60	minutes 👻	🐻 Re	port
	Host: dsrotateupgrade3											
Ionitorii	-											
	and Resource Information											1
	er Count by Status All (22), Paused (0), Stopp	ed (9), Runnin	g (13)									
	n System CentOS Linux 7 (Core)			Host	dsrotateupgrade3 (10.4.1)	17.155)						
lemory	1.8 GB			Nano CPU	1							
ocker V				Cgroup Driver	cgroupfs							
	lost Swarm Information											
warm C				Swarm Role	Manager							
warm N	lode dsrotateupgrade3 (xypq2vtwrx4	ztdyo16cjg9v3)	Swarm Node Status	[ready]							
ontainer	S											
Alarms	Name			Id				Ima	ige		Netw Mod	1
0	voting_result.1.m1ab9gkqai8l1krg24oudykdt	aa25171d29a8076e9a0a076340a967927a237cccdc066b			37cccdc066b6e460c4e44d1a	d2979 do	ckersamples	/examplev	otingapp_re	sult: <none></none>	defa	i *
\odot	voting_vote.2.ua654o33tdvqp7fn3pvyqo0rb	133ae0269871fbe90b894be92719216e9beef2d46328c5d84				5dd4b4 dockersamples/examplevotingapp_vote: <none></none>					defa	i.
0	wordpress_wordpress.3.3d78lukeu8t9evlzq3mpt8					ec2 wo	rdpress: <n< td=""><td>one></td><td></td><td></td><td>defa</td><td>i.</td></n<>	one>			defa	i.
0	voting_redis.1.awis611hu72gyxl5hl5epjy6v		288e8a1dde3a	0e893913559c7e2202e96f5	2a88fadfe5b862d4b6988a735	5d896 redis: <none></none>					defa	i.
0	voting_vote.1.deivdnggt0nlrcb8qo0b8r1hd		f5eca4b5aec92	94745fe742a2eb9e12ee26b	13699edbc473cc6b334d9e78	78bc5d dockersamples/examplevotingapp_vote: <none></none>				te: <none></none>	defa	i.
õ	redis2.xypq2vtwrx4cztdyo16cjg9v3.vrubg5q34jlaq	8fih21mg6xex	149fa7578f49f332fed8ac292d61cd19dc8eafecdf45a1b3482201312fadf0e6				i redis: <none></none>				defa	i.
0	mongo_mongo.1.95ak9qe8gp158etdue4pwfu2w		78a7e75c36a9	ad2d mo	2d mongo: <none></none>				defa	i.		
Ö	mysql_phpmyadmin.1.0c2dfj4k6ghuo4n463mf8gj	'n	f89221041f8dd	bd7 ph	d7 phpmyadmin/phpmyadmin: <none></none>				defa	i.		
Ø	wordpress_db.1.7c7fttk36oijtcspb6zr1tjoh		1711d54e6f15255a20e37685ccf85ad6a3656beae84bf9ce44cb763d29d734a2			34a2 my	14a2 mysql: <none></none>				defa	i.
õ	wordpress visualizer.1.drlgdbtulabsbze5eriegdjg7		d1af858af9554	1af858af95546c4db25fc7218dc89bfe4c99b73980d746a2eea9dd74a489719			719 dockersamples/visualizer: <none></none>				defa	i.
õ	voting_visualizer.1.nwq4l4jm8bwpyvmh9wn30qdd	y	16b274edf0a97	b274edf0a972a313b61f785e3473571cfa6f380ef1a57991cc64fc53dddbb9			bb9 dockersamples/visualizer: <none></none>				defa	i.
0	mysql_mysql.1.mrroqco2fs7qm5pjk9y4bnjke		2c27187424e0	424e082060de9cbc9da6d2e9dac440cdbc50ffa626ed45157698cc72							defa	i.
õ	voting_db.1.8eol3l95f710l50jrvpq4j9hu		7a60a959fb3af	59fb3afa27006ed3383d69e966ae25270c1502f9f95127c6696ae226							defa	à
											Þ	*
nages												
State	Name					Size	Virtual Size	Comment	Containers	Not Upda Duratio		
~	dockersamples/examplevotingapp_result: <none></none>	sha256:e10df	791f13c3ac17e	a123dfce57e3297fcea05a34	b3bbf305749f22a9b3c83	216.0 ME	216.0 MB		1	2 minute(s)		-
~	phpmyadmin/phpmyadmin: <none></none>	sha256:c6ba3	na256:c6ba363e7c9bba3bc96aa490e31d		8c525fb8a36df2544c2aa54	158.2 ME	158.2 MB		1	2 minute(s)		1
~	mongo: <none></none>	sha256:0d183f48c313d863d26ae		6aed97c27a0fb73833674c8	7da2576b6282de2439a144c	389.5 ME	389.5 MB		1	2 minute(s)		1
亩	nate/dockviz:latest	sha256:93b52	259c1e18862e14	434e39678640cbdd555d1b8	e2742bc6f4da9c2b78acd8ab	6.3 MB	6.3 MB		0			1
~	mysql: <none></none>	sha256:7bb25	586065cd50457	e315a5dab0732a87c45c5fa	l619c017732f5a13e58b51dd	454.8 ME	454.8 MB		2	2 minute(s)		1
~	redis: <none></none>	sha256:d4dee	ec2c521cdae045	0218bd53c69611bacd2eb1	1838057a5de7dcb341c66cf5	144.2 MB	144.2 MB		1	2 minute(s)		1
~	postgres: <none></none>	sha256:d7cf9	8b297166b40ef	ca50ff11ef9c7e801d45a0f6	1ba316854984229667578	214.9 ME	214.9 MB		1	2 minute(s)		1
亩	alpine: <none></none>	sha256:5ch3a	a00f89934411f	ba5c063a9bc98ace875d8f9	2a77d0020542d0f2af4ad0	5.2 MB	5.2 MB		0			1

Figure 32. Docker Host Explorer view Monitoring Tab

- Containers table: Includes the containers on this docker host.
- Images table: Includes the images pulled onto this docker host.
 - □ Indicates this image is using by a container.
- Volumes table: Includes the volumes created on this docker host.
 - □ ■: Indicates this volume is using by a container.
 - $\overline{\mathbf{m}}$: Indicates no container is using this volume and the volume can be recycled.

Figure 33. Docker Host Explorer view Images table and Volumes table under Monitoring tab

State											
	Name			Id		Size		Comment Containers			n
~	dockersamples/visualizer: <none></none>			8dbf7c60cf8866bc03ac941f2462615ef		141.3 MB	141,3 MB	2	3 minute(s		
~	dockersamples/examplevotingapp_v	vote: <none< td=""><td></td><td>f6e8af4562c14ab06a2c9f3698e39efa6</td><td></td><td>79.7 MB</td><td>79.7 MB</td><td>2</td><td>3 minute(s</td><td>s)</td><td></td></none<>		f6e8af4562c14ab06a2c9f3698e39efa6		79.7 MB	79.7 MB	2	3 minute(s	s)	
Î	mongo-express: <none></none>		the second s		45eab173b8e039ff9cee40e672a99f882	91.5 MB	91.5 MB	0			
~	phpmyadmin/phpmyadmin: <none></none>	Docker Ho	ost Explore Cor	itainers				× 1	3 minute(s	s)	
Î	nate/dockviz:latest	Alarms		Name	Id			ii 0			
~	dockersamples/examplevotingapp_r	Additio		Warrie	10			1	3 minute(s	s)	
~	redis: <none></none>	0	wordpress_vi	sualizer.1.drlgdbtulabsbze5eriegdjq7	d1af858af95546c4db25fc7218dc89bfe4c	9b73980d74	5a2eea9dd7	^ 1	3 minute(s	s)	
~	redis: <none></none>	0	voting_visual	izer.1.nwq4l4jm8bwpyvmh9wn30qddy	16b274edf0a972a313b61f785e3473571c	a6f380ef1a5	991cc64fc5	1	3 minute(s	s)	
~	mongo: <none></none>							1	3 minute(s	s)	
~	wordpress: <none></none>							1	3 minute(s	s)	
面	alpine: <none></none>							0			
	postgres: <none></none>							1	3 minute(s	s)	
	mysql: <none></none>							2	3 minute(s	s)	
		-									
	Name							Labels		Containers	
State	Name							Labels	wordpress	Containers	100000000000000000000000000000000000000
State	wordpress_db-data	4					Þ	.stack.namespace	:wordpress		1
State	wordpress_db-data 95a60485f40181d593bf7cf987343		hfbfa89531	/uar/lib/dacker/volumes/5387a7aca0	7hffi 245nh77537#084.H755kfia1hfifa8053	412 N M		.stack.namespace	:wordpress		10000
State	wordpress_db-data 95a60485f40181d593bf7cf987343 5387a2aca97bffb3450b27537e984	4df35bf043			75ffb3456b27537e984df355f043bfbfa8953			.stack.namespace	:wordpress		and a second sec
State	wordpress_db-data 95a60485f40181d593bf7cf987343 5387a2aca97bffb3450b27537e98 c62c5e37af00a54d06ee6c6e04f9c	4df35bf043		/var/lib/docker/volumes/c62c5e37af0	0a54d06ee6c6e04f9c22cae1217b4806d9e	0.0 B	8	,stack.namespace ▼		1 1 1 1	
State	wordpress_db-data 95a60485f40181d593bf7cf987343 5387a2aca97bffb3450b27537e98- c62c5e37af00a54d06ee6c6e04f9c voting_db-data	4df35bf043 22cae1217	'b4806d9e40	/var/lib/docker/volumes/c62c5e37af0 /var/lib/docker/volumes/voting_db-da	0a54d06ee6c6e04f9c22cae1217b4806d9e ata/_data	0.0 B 35.4 MB	8	.stack.namespace			10
State	wordpress_db-data 95a6048540181d593bf7cf987343 5387a2aca97bffb3450b27537e98 c62c5e37af00a54d05ee6c6e04f9c voting_db-data 92c4ebb4a373d969d18e7140e88	4df35bf043 22cae1217 596cf82e28	7b4806d9e40	/var/lib/docker/volumes/c62c5e37af0 /var/lib/docker/volumes/voting_db-dc /var/lib/docker/volumes/92c4ebb4a3	0a54d06ee6c6e04f9c22cae1217b4806d9e ata/_data 73d969d18e7140e08596cf82e2806409412	0.0 B 35.4 MB	3 com.do	,stack.namespace ▼	ovting	1 1 1 1 1 1	
State	wordpress_db-data 95a60485401814593bf7cf987343 5387a2aca97bffb3450627537c898 c62c5e37af00a54d06ee6c6e04f9c voting_db-data 92c4ebb4a373d969d18e7140e885 8f9606b95a0b05416dcb6170d539	4df35bf043 22cae1217 596cf82e28 070cd2bab0	7b4806d9e40 8064094128 03ad9eaf824	/var/lib/docker/volumes/c62c5e37af0 /var/lib/docker/volumes/voting_db-di /var/lib/docker/volumes/92c4ebb4a3 /var/lib/docker/volumes/8f9606b95af	00a54d06ee6c6e04f9c22cae1217b4806d9e ata/_data 73d969d18e7140e08596cf82e2806409412 0b05416dcb6170d53970cd2bab03ad9eaf8;	0.0 B 35.4 MB 0.0 B 164.3 M	3 com.do	,stack.namespace ▼	ovting	1 1 1 1	5
State	wordpress_db-data 95a60485f40181d593bf7cf987343 5387a2aca97bffb3450b27537e84- c6225837af0a54d0bce6c6c8049c voting_db-data 92c4ebb4a373d959418e7140e088 8f9606959a0b05416dc6170d339 c053ac30f84dca062d0223cbc3408	4df35bf043 22cae1217 596cf82e28 070cd2bab0 837a559bd0	264806d9e40 2064094128 33ad9eaf824 ce7e8b92fc5	/var/lib/docker/volumes/c62c5e37af0 /var/lib/docker/volumes/voting_db-di /var/lib/docker/volumes/92c4ebb4a3 /var/lib/docker/volumes/9f9606b95at /var/lib/docker/volumes/c053ac30f84	0054d06ee6c6e04f9c22cae1217b4806d9e ata/_data 73d969d18e7140e08596cf82e2806409412 0005416dcb6170d53970cd2bab03ad9eaf82 kdca062d0223cbc340837a559bdce7e8b92f	0.0 B 35.4 MB 0.0 B 164.3 M 38.1 MB	3 com.do	,stack.namespace ▼	ovting	1 1 1 1 1 1 0 1	10
	wordpress_db-data 95a60485401814593bf7cf987343 5387a2aca97bffb3450627537c898 c62c5e37af00a54d06ee6c6e04f9c voting_db-data 92c4ebb4a373d969d18e7140e885 8f9606b95a0b05416dcb6170d539	4df35bf043 22cae1217 596cf82e28 170cd2bab0 837a559bd0 bdc89c6a30	b4806d9e40 064094128 03ad9eaf824 ce7e8b92fc5 c6b56a9703	/var/lib/docker/volumes/c52c5e37af0 /var/lib/docker/volumes/voting_db-di /var/lib/docker/volumes/92c4ebb4a3 /var/lib/docker/volumes/8f9606b95al /var/lib/docker/volumes/c053ac30f84 /var/lib/docker/volumes/c053ac30f84	00a54d06ee6c6e04f9c22cae1217b4806d9e ata/_data 73d969d18e7140e08596cf82e2806409412 0b05416dcb6170d53970cd2bab03ad9eaf8;	 0.0 B 35.4 MB 0.0 B 164.3 M 38.1 MB 92.0 B 	3 com.do	,stack.namespace ▼	ovting	1 1 1 1 1 1	

By clicking the number in the *Containers* column, a *Docker Host Explore Containers* view will open, which lists the containers using this image or this volume. Click the Name or ID of the container and an explore page of the container will appear.

 Metrics tab: The Metrics tab displays the Metrics list. To set the Metrics list displayed, go to Action > General > Metric Selector. For more information about the description of the metrics, see Container metrics on page 61.

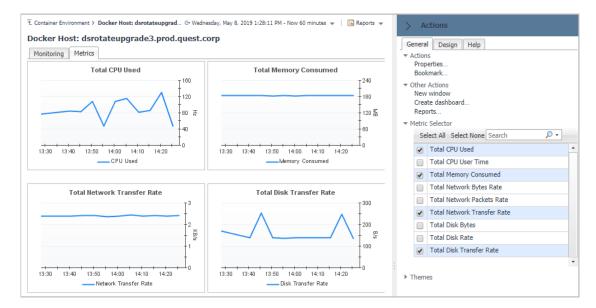


Figure 34. Docker Host Explorer view Metrics Tab

Monitoring Docker Swarm Clusters

This view consists of the following two panes:

- The **Swarm Clusters** tree view, which appears on the left of *Swarm Clusters Quick View*, lists the docker swarm clusters existing in the monitored *Docker* environment.
- The Docker Swarm Cluster Summary view, which appears on the right after you select an individual docker swarm cluster in the Swarm Clusters tree view.

Docker Swarm Cluster Summary view

The **Docker Swarm Cluster Summary** view appears on the right when you select a docker swarm cluster in the **Swarm Clusters** tree view.

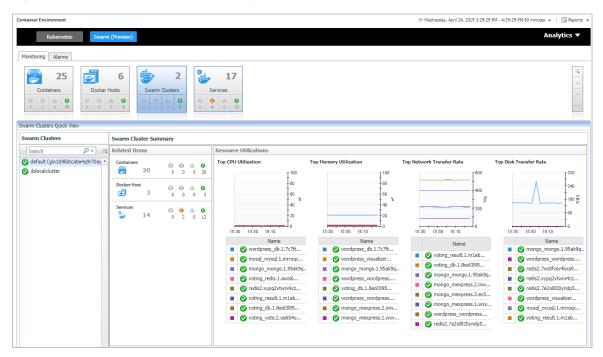


Figure 35. Docker Swarm Cluster Summary view

The Docker Swarm Cluster Summary view displays the following data:

- Related Items: Shows the related Docker components grouped by type as well as the associated alarms.
- *Resource Utilizations*: Shows CPU Utilization, Memory Utilization, Network Transfer Rate, Disk Transfer Rate metrics of the containers running in this docker swarm cluster in descending order.

Monitoring Docker Swarm Services

This view consists of the following two panes:

- The Swarm Services tree view, which appears on the left of Swarm Services Quick View, lists the docker swarm services existing in the monitored Docker environment.
- The Docker Swarm Service Summary view, which appears on the right after you select an individual docker swarm service in the Swarm Services tree view.

Docker Swarm Service Summary view

The **Docker Service Summary** view appears on the right when you select a docker swarm service in the **Docker Services** tree view.

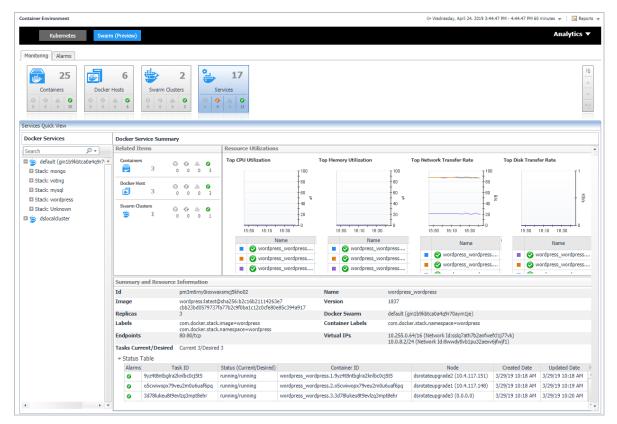


Figure 36. Docker Service Summary view

The Docker Service Summary view displays the following data:

- Related Items: Shows the related Docker components grouped by type as well as the associated alarms.
- *Resource Utilizations*: Shows CPU Utilization, Memory Utilization, Network Transfer Rate, Disk Transfer Rate metrics of the containers running in this docker swarm service in descending order.
- Summary and Resource Information: Shows the summary information of the docker swarm service, including Labels, Image, Mount Volumes, Ports, Container Status and so on.

Alarms

ontainer Environment							G+ Wednesday, May 15, 2019 1:17:24 AM - 2:17:24 AM 60 minute	is 👻 📄 Repor
Kubernetes Swarm (Preview) Analytics 🔻								
Monitoring Alarms								
C Alarms								
Containers Docker Hosts Swarm Services Swarm Tasks Clusters								
				Containers Do	cker Hosts Swarn	m Services S	iwarm Tasks Clusters	
				Containers Do	cker Hosts Swarn	m Services Si	warm Tasks Clusters	
Select All Unselect All	Acknowle	dge Cle						<i>p</i> +
Select All Unselect All	Acknowle Severity		ar					، م
			ar	Impacting		2 Rule Name	Search	

Figure 37. Docker Swarm Alarms Dashboard

Foglight for Container Management 2.0.0 User and Administration Guide Using Foglight for Container Management **51** The *Alarms* dashboard displays a list of alarms generated against the monitored Docker environment. Use this view to quickly identify any potential problems related to a specific Docker component.

Analytics

Foglight for Container Management provide analytics feature for Kubernetes and Docker Swarm.

Heat Map is a two-dimensional representation of data in which values are represented by colors. Showing collected metrics with elaborate heat maps allows you to understand complex data sets and the monitored cluster environment well.

Scatter Plot is used to display values in points using two variables for a set of data. The points is color-coded also, Color Metric can be used to display one additional variable.

- Kubernetes analytics
 - Heatmap analytics
 - Scatter Plot analytics
- Docker Swarm analytics
 - Heatmap analytics
 - Scatter Plot analytics

Kubernetes analytics

In the Container dashboard, choose **Kubernetes** from the header. Then click **Analytics** from the header, a drop down view will display with **Heatmap** and **Scatter** on it. Click **Heatmap** will navigate to the Kubernetes **Heatmap Analytics** dashboard, while click **Scatter** will navigate to the Kubernetes **Scatter Plot Analytics** dashboard.

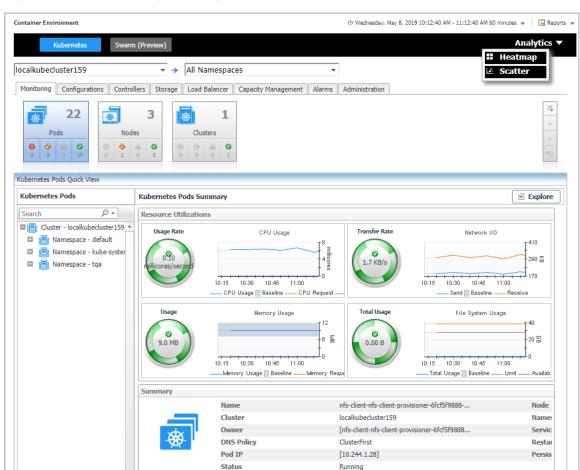


Figure 38. Kubernetes analytics Navigation

Heatmap analytics

Figure 39. Kubernetes Heatmap Analytics Dashboard

											6	e Friday, Nov	[High	- 4:10 AM 1	4 100/5 ¥	Repor	
pology Type Kube Pod 🔻 Cluster All Clu	usters V Namespa	ace All Namespa	ces 🔻 Selected I	Metric CPU Usag	e		Color M	etric Mem	nory Usage		T	Color Patte	m 🔍	High				
eatmap Chart																		
wordpress-db8f78568-72zff																	tunnelfron fluentd-ela heap	
be Pods Pod Name	CPU Usage Rate	CPU Usage	CPU Request	CPU Limit	Memory Usage	Memory Working	Memory R55	Memory Request	Memory Limit	Memory Page	Memory Page Faults	Memory Major Page	Page	Network	Receive	Network Transfer	, senu	E 1
	CPU Usage Rate	-		CPU Limit							Page	Major	Major	Network Send Bytes	Network Receive Bytes	Network Transfer	Network Send Rate	
	CPU Usage Rate 0.0 millicores/second	CPU Usage 0.0 millicores	CPU Request	CPU Limit 0.0 millicores		Working			Limit	Page	Page Faults Rate	Major Page	Major Page Faults	Selia	Bytes	Network Transfer 70.0 B	, senu	
Pod Name		0.0 millicores		0.0 millicores	Usage	Working Set	R55	Request	Limit	Page Faults	Page Faults Rate 0.0 c/s	Major Page Faults	Major Page Faults Rate	Bytes 0.0 B	Bytes 70.0 B	Transfer	Rate	
Pod Name inx-rzącz ure-vote-front-5df9b79c56-249nz	0.0 millicores/second	0.0 millicores 0.0 millicores	0.0 millicores	0.0 millicores	Usage 2.0 MB	Working Set 2.0 MB	R55	Request	Limit 0.0 B 256.0 MB	Page Faults	Page Faults Rate 0.0 c/s 0.0 c/s	Major Page Faults 0.0 count	Major Page Faults Rate 0.0 c/s 0.0 c/s	0.0 B 15.3 KB	70.0 B 28.1 KB	Transfer	0.0 B/s	
Pod Name Inv-rząz .re-vote-front-5df9b79c56-z49nz hdb-1	0.0 millicores/second 0.0 millicores/second 0.0 millicores/second	0.0 millicores 0.0 millicores 0.0 millicores	0.0 millicores 100.0 millicores	0.0 millicores 250.0 millicores	Usage 2.0 MB 53.3 MB 3.4 MB	2.0 MB 52.6 MB 3.2 MB	R55 1.4 MB	0.0 B 128.0 MB	Limit 0.0 B 256.0 MB 0.0 B	Page Faults 0.0 count 0.0 count	Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s	Major Page Faults 0.0 count 0.0 count	Major Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s	0.0 B 15.3 KB 45.3 KB	70.0 B 28.1 KB 69.3 KB	70.0 B 43.5 KB	0.0 B/s	
Pod Name ns-rzgz ire-vote-front-Sdf9b79c56-249nz hdb-1 rdpress-db8178568-722ff	0.0 millicores/second 0.0 millicores/second 0.0 millicores/second	0.0 millicores 0.0 millicores 0.0 millicores 841.6 millicores	0.0 millicores 100.0 millicores 0.0 millicores	0.0 millicores 250.0 millicores 0.0 millicores 0.0 millicores	Usage 2.0 MB 53.3 MB 3.4 MB	2.0 MB 52.6 MB 3.2 MB	R55 1.4 MB 44.8 MB 2.6 MB 77.8 MB	0.0 B 128.0 MB 0.0 B 0.0 B	Limit 0.0 B 256.0 MB 0.0 B	Page Faults 0.0 count 0.0 count 0.0 count 0.0 count	Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	Major Page Faults 0.0 count 0.0 count 0.0 count	Major Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	0.0 B 15.3 KB 45.3 KB 23.0 KB	70.0 B 28.1 KB 69.3 KB 35.0 KB	70.0 B 43.5 KB 114.6 KB	0.0 B/s 52.3 B/s 154.5 B/s	
Pod Name nv:rzqzz ire-vote-front-5df9b79c56-z49nz hdb-1 hdb-1 ne-vote-back-6659c5bf44-j9tz	0.0 millicores/second 0.0 millicores/second 0.0 millicores/second 14.0 millicores/second 0.0 millicores/second	0.0 millicores 0.0 millicores 0.0 millicores 841.6 millicores 0.2 millicores	0.0 millicores 100.0 millicores 0.0 millicores 0.0 millicores	0.0 millicores 250.0 millicores 0.0 millicores 0.0 millicores	Usage 2.0 MB 53.3 MB 3.4 MB 126.1 MB	Working Set 2.0 MB 52.6 MB 3.2 MB 123.4 MB	R55 1.4 MB 44.8 MB 2.6 MB 77.8 MB	0.0 B 128.0 MB 0.0 B 0.0 B	Limit 0.0 B 256.0 MB 0.0 B 0.0 B 256.0 MB	Page Faults 0.0 count 0.0 count 0.0 count 0.0 count	Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	Major Page Faults 0.0 count 0.0 count 0.0 count 0.0 count	Major Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	0.0 B 0.0 B 15.3 KB 45.3 KB 23.0 KB 366.0 B	70.0 B 28.1 KB 69.3 KB 35.0 KB 506.0 B	Transfer 70.0 B 43.5 KB 114.6 KB 58.0 KB	0.0 B/s 52.3 B/s 154.5 B/s 78.6 B/s	
Pod Name nv-rzącz rz-vote-front-5df9b79c56-z49nz hdb-1 dpress-db8f78568-72zff rz-vote-back-66595cb/14-j3tz -helloword-punk-worm-57b8bb98cf-9d4bd	0.0 millicores/second 0.0 millicores/second 0.0 millicores/second 14.0 millicores/second 0.0 millicores/second	0.0 millicores 0.0 millicores 0.0 millicores 841.6 millicores 0.2 millicores 0.0 millicores	0.0 millicores 100.0 millicores 0.0 millicores 0.0 millicores 100.0 millicores	0.0 millicores 250.0 millicores 0.0 millicores 0.0 millicores 250.0 millicores	Usage 2.0 MB 53.3 MB 3.4 MB 126.1 MB 9.0 MB 37.1 MB	Working Set 2.0 MB 52.6 MB 3.2 MB 123.4 MB 9.0 MB 37.0 MB	R55 1.4 MB 44.8 MB 2.6 MB 77.8 MB 8.4 MB	Request 0.0 B 128.0 MB 0.0 B 0.0 B 128.0 MB	Limit 0.0 B 256.0 MB 0.0 B 0.0 B 256.0 MB 0.0 B	Page Faults 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count	Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	Major Page Faults 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count	Major Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	0.0 B 0.0 B 15.3 KB 45.3 KB 23.0 KB 366.0 B	70.0 B 28.1 KB 69.3 KB 35.0 KB 506.0 B 140.0 B	Transfer 70.0 B 43.5 KB 114.6 KB 58.0 KB 872.0 B	0.0 B/s 52.3 B/s 154.5 B/s 78.6 B/s 1.0 B/s	
Pod Name nx-rzągz re-vote-front-5df9b79c56-z49nz hdb-1 rdpress-db8f78568-72zff re-vote-back-6659c8bf44-j8tz -helloworld-punk-worm-57b8b986f-944bb rdpress-mysql-7b4ffb6fb4-zabbm	0.0 millicores/second 0.0 millicores/second 0.0 millicores/second 14.0 millicores/second 0.0 millicores/second 0.0 millicores/second	0.0 millicores 0.0 millicores 0.0 millicores 841.6 millicores 0.2 millicores 0.0 millicores 0.0 millicores	0.0 millicores 100.0 millicores 0.0 millicores 100.0 millicores 0.0 millicores 0.0 millicores	0.0 millicores 250.0 millicores 0.0 millicores 250.0 millicores 0.0 millicores	Usage 2.0 MB 53.3 MB 3.4 MB 126.1 MB 9.0 MB 37.1 MB	Working Set 2.0 MB 52.6 MB 3.2 MB 123.4 MB 9.0 MB 37.0 MB	R55 1.4 MB 44.8 MB 2.6 MB 77.8 MB 8.4 MB 32.0 MB	Request 0.0 B 128.0 MB 0.0 B 0.0 B 128.0 MB 0.0 B	Limit 0.0 B 256.0 MB 0.0 B 256.0 MB 0.0 B 0.0 B	Page Faults 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count	Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	Major Page Faults 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count	Major Page Faults Rate 0.0 c/s	Send Bytes 0.0 B 15.3 KB 45.3 KB 23.0 KB 366.0 B 0.0 B 0.0 B 0.0 B	70.0 B 28.1 KB 69.3 KB 35.0 KB 506.0 B 140.0 B 70.0 B	Transfer 70.0 B 43.5 KB 114.6 KB 58.0 KB 872.0 B 140.0 B	0.0 B/s 52.3 B/s 154.5 B/s 78.6 B/s 1.0 B/s 0.0 B/s	
Pod Name	0.0 millicores/second 0.0 millicores/second 0.0 millicores/second 14.0 millicores/second 0.0 millicores/second 0.0 millicores/second 0.0 millicores/second	0.0 millicores 0.0 millicores 0.0 millicores 841.6 millicores 0.2 millicores 0.0 millicores 0.0 millicores 0.0 millicores	0.0 millicores 100.0 millicores 0.0 millicores 0.0 millicores 100.0 millicores 0.0 millicores 0.0 millicores	0.0 millicores 250.0 millicores 0.0 millicores 250.0 millicores 250.0 millicores 0.0 millicores 0.0 millicores	Usage 2.0 MB 53.3 MB 3.4 MB 126.1 MB 9.0 MB 37.1 MB 464.5 MB	Working Set 2.0 MB 52.6 MB 3.2 MB 123.4 MB 9.0 MB 37.0 MB 462.6 MB	R55 1.4 MB 44.8 MB 2.6 MB 77.8 MB 8.4 MB 32.0 MB 457.8 MB	Request 0.0 B 128.0 MB 0.0 B 128.0 MB 0.0 B 0.0 B	Limit 0.0 B 256.0 MB 0.0 B 256.0 MB 0.0 B 0.0 B 0.0 B	Page Faults 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count	Page Faults Rate 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s 0.0 c/s	Major Page Faults 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count 0.0 count	Major Page Faults Rate 0.0 c/s 0.0 c/s	Send Bytes 0.0 B 15.3 KB 45.3 KB 23.0 KB 366.0 B 0.0 B 0.0 B 15.8 KB	Receive Bytes 70.0 B 28.1 KB 69.3 KB 35.0 KB 506.0 B 140.0 B 70.0 KB	Transfer 70.0 B 43.5 KB 114.6 KB 58.0 KB 872.0 B 140.0 B 70.0 B	Send Rate 0.0 B/s 52.3 B/s 154.5 B/s 78.6 B/s 1.0 B/s 0.0 B/s 0.0 B/s	

Heat maps will be refreshed automatically when you change either of the following fields:

- *Topology Type:* Indicates the monitored topology object, including Kubernetes Pod, Kubernetes Node, and Kubernetes Cluster.
- Cluster: Lists all clusters available in the monitored Kubernetes environment.
- · Namespace: Lists all namespaces available in the monitored Kubernetes environment.
- Selected Metric: Populates a rectangle based upon the selected metrics. For example, if you select Memory Usage from the Selected Metric drop-down list, the rectangle area will be populated based on the used memory for the selected topology object. For more information about metrics, refer to Kubernetes metrics on page 60.
- Rendering related metrics: For example, if you select *CPU Usage Rate* and Red to Green, the rectangle of the topology object that has larger value of CPU Usage Rate will be rendered in red.
 - Color Metric: Renders the color of rectangle based upon the selected color metric.
 - Color Pattern: Offers two patterns, Red to Green (larger value shows in red) or Green to Red (larger value shows in green).

Figure 39 shows an example of heat map. This sample diagram represents the "wordpress-db8f78568-72zff" has the maximum amounts of CPU usage, while "fluentd-elastic-ef455uh68-72cfe" has a higher Memory Usage. If you switch the Color Pattern, then "wordpress-db8f78568-72zff" will turn to red. Clicking the object name on the heat map directs you to the relevant object *Explorer* dashboard. For more information, see:

- Pods Explorer view on page 27
- Pod metrics on page 60
- Nodes Explorer view on page 30
- Node metrics on page 61
- Cluster Explorer view on page 33

Cluster metrics on page 61

Scatter Plot analytics

Figure 40. Kubernetes Scatter Plot Analytics Dashboard

																				High
cology Type Kube Pod	▼ Cluster na	ncyaksclust	er 🔻 Namespac	e All Namespac	ts ▼ X Axis:	CPU Usage	2		 Y Axis: 	CPU Usag	e		▼ Color №	1etric Ne	twork Tran	nsfer	•	Color Patte	ern Ö	High
atter Chart																				
000 millicores																			_	
800 millicores																			•	
600 millicores																				
00 millicores																				
DD millicores																				
0 millicores	100 m	illicores	200 mil	licores	300 millicor	es	400 mi	illicores	50	0 millicore	s	600 mil	licores	7	00 millicor	es	800 m	illicores	9	900 millic
ibe Pods																				
Pod Name	CPU Usa	ge Rate	CPU Usage	CPU Request	CPU Limit	Memory Usage	Memory Working Set	Memory RSS	Memory Request	Memory Limit	Memory Page Faults	Memory Page Faults Rate	Memory Major Page Faults	Memory Major Page Faults Rate	Network Send Bytes	Network Receive Bytes	Network Transfer	Network Send Rate	Network Receive Rate	Netwo Transf Rate
ordpress-db8f78568-72z			841.6 millicores						0.0 B		0.0 count		0.0 count	0.0 c/s	23.0 KB		58.0 KB	78.6 B/s		
luentd-elasticsearch-6tf9r unnelfront-595448b4cc-k		res/second	10.8 millicores 24.2 millicores	100.0 millicores					200.0 MB 64.0 MB				0.0 count 0.0 count					522.8 B/s 32.3 KB/s		

The points on the chart will be refreshed automatically when you change either of the following fields:

- Topology Type: Indicates the monitored topology object, including Kubernetes Pod, Kubernetes Node, and Kubernetes Cluster.
- *Cluster:* Lists all clusters available in the monitored Kubernetes environment.
- Namespace: Lists all namespaces available in the monitored Kubernetes environment.
- X Axis: Indicates which metrics will be plotted on X axis.
- Y Axis: Indicates which metrics will be plotted on Y axis.
- Rendering related metrics:
 - Color Metric: Renders the color of circle based upon the selected metrics.
 - *Color Pattern*: Offers two patterns, Red to Green (larger value shows in red) or Green to Red (larger value shows in green).

Figure 40 shows an example of Scatter Plot analytics. The purple circle in the middle represents the following: "wordpress-db8f78568-72zff" CPU Usage is around 0.85 cores, its Memory Usage is around 121MB, and its value of Network Transfer Bytes is not high. For more information, see:

- Pods Explorer view on page 27
- Pod metrics on page 60
- Nodes Explorer view on page 30
- Node metrics on page 61
- Cluster Explorer view on page 33
- Cluster metrics on page 61

Docker Swarm analytics

In the Container dashboard, choose **Docker Swarm** from the header. Then click **Analytics** from the header, a drop down view will display with **Heatmap** and **Scatter** on it. Click **Heatmap** will navigate to the Docker Swarm **Heatmap Analytics** dashboard, while click **Scatter** will navigate to the Docker Swarm **Scatter Plot Analytics** dashboard.

ontainer Environment				G+ Wednesday, May 8, 2019	9:50:02 AM - 10:50:02	AM 60 minutes 👻 📔 🖬 Reports
Kubernetes Swarn	m (Preview)					Analytics ▼ Heatmap Scatter
25 <u>Containers</u> ○ ○ △ ○ ○ ○ ○ 4 21	6 Hosts 0 6 0 0 0		17 Services			
Docker Containers Quick View						(
Docker Containers	Docker Container Sum	mary	1			🕒 Explore
Search 🔎 🔻	Related Items		Resource Utilizatio	N5		
 localdscluster ds10.30.154.66 mortpress_db.1.kejgv 			CPU Load		Network Transfer	Network I/0
 ▲ → fglam1 ⊘ → register_registry_1 			0.33 %	8 ₹ 10:00 10:40	0.00 B/s	400 B 400 B 10:00 10:40
 ■ all ds10.30.154.67 Ø all wordpress_wordpress Ø all wordpress_wordpress 	Services		Memory	Used Time Baseline -	Disk Transfer	Send Bytes Baseline Disk I/O
 wygradedscluster ds10.4.117.154 mysql_phpmyadmin.1 voting_visualizer.1.bn voting_visualizer.1.szdmo3 			0.04 %	130800 130200 g 130200 g 129600 10:00 10:40 Page In Baseline	0.00 KB/s	120 60 5 10:00 10:40 Disk Read Baseline
wordpress_wordpress	Summary and Resource	Information][
🛛 🚍 wordpress_visualizer.	State	Running				
🗚 👼 mongo_mongo.1.lauh	Created Date	3/29/19 11:42 A	м	Sta	rted Date	3/29/19 11:42 AM
wordpress_wordpress	Docker Host		(fog2775ubuntu16.prod		nmand	docker-entrypoint.sh my
🛛 🕃 mongo_mexpress.1.u	Network Mode	default	. og 2. / oubunitu 20ipi oc	Ima		mysql: <none></none>
voting_redis.1.7u9zcr mysql_mysql.1.wwzcy	IP Address				itainer Id	0ac17ff0cef7c29bd78eb6 fbe2293c3639ee1db17b9
voting_vote.2.i77wq2	Ports	3306		Mo	unts	(volume) /var/lib/mysql

Figure 41. Docker Swarm Analytics Navigation

Heatmap analytics

Figure 42. Docker Swarm Heatmap Analytics Dashboard

					High		
logy Type Docker Container V Cluster All Clusters V Selected Metric CP	20 Utilization	▼ Color	Metric Memory Utilizatio	on 🔻 Color	Pattern		
					High		L
itmap Chart							
charc							
voting_worker.1.xygkjn8b2uuiipglelmvzpj2e						voting_db.1.xlele	
						voting_redis.1.nv	vfx2moecimr7v5sb3.
						voting_redis.1.nv	vfx2moecimr7v5sb3.
						voting_redis.1.nv	vfx2moecimr7v5sb3.
m Containers						voting_redis.1.nv	vfx2moecimr7v5sb3.
	CPU Utilization	CPU Time Used	Memory Utilization	Network Transfer Rate	Disk Transfer Rate	voting_redis.1.nv Memory Swap Page In	
tainer Name	CPU Utilization 2.9 %	CPU Time Used 57 ms	Memory Utilization 0.1 %	Network Transfer Rate 154.6 (RJ)s	Disk Transfer Rate 0.0 KB/s		
tainer Name 1g_redis.1.nwfx2moecimr7v5sb3gmqgtmk						Memory Swap Page In	Memory Swap Page Ot
name ng_redis.1.nwfr/2moecimr7V5sb3gmagtmk ng_vate.1.ia318mmgrxpbrdocs2wbvdd99	2.9 %	57 ms	0.1 %	154.6 KB/s	0.0 KB/s	Memory Swap Page In 485.0 count	Memory Swap Page Ou 422.0 count
ainner Name g_reds.1.nvh.2moecim/VSeb3gmagtmk g_vote.1.io318mmgavpbudcs2Avbvd99 g_vote.2.vh7xt16y4f6r402sdzysginrm	2.9 % 0.0 %	57 ms 0 ms	0.1 %	154.6 KB/s 0.0 B/s	0.0 KB/s 0.0 KB/s	Memory Swap Page In 485.0 count 22.5 K	Memory Swap Page Or 422.0 count 7.2 K
ng, geds. L. nvh/Zmoecim/7V58b3gmgptmk ng, vets. Li Jolt8mmg/vpbdocs2vbvdd99 gu vets. Li Jolt8mmg/vpbdocs2vbvdd99 gu vets. 2vh7VL Styriffer402sdzysginm ng_vorker. 1.vygkjn8b2uuipgleImvzpj2e	2.9 % 0.0 % 0.0 %	57 ms 0 ms 0 ms	0.1 % 0.5 % 0.5 %	154.6 KB/s 0.0 B/s 0.0 B/s	0.0 KB/s 0.0 KB/s 0.0 KB/s	Memory Swap Page In 485.0 count 22.5 K 20.4 K	Memory Swap Page Or 422.0 count 7.2 K 5.9 K
iainer Name jg_retai.1.mkfr.2moecimr?VSeb3gmagtmk g_rote1.io188mmgvxpbdocs2vMvdd99 g_rote2.rwh7rt16y4f6r402sdysginnm g_rote2.rwh7rt16y4f6r402sdysginnm g_rote1.ruhf23lgc52j4j2nzmvk5jeop	2.9 % 0.0 % 0.0 % 38.2 %	57 ms 0 ms 0 ms 737 ms	0.1 % 0.5 % 0.5 % 1.4 %	154.6 KB/s 0.0 B/s 0.0 B/s 403.0 KB/s	0.0 KB/s 0.0 KB/s 0.0 KB/s 0.0 KB/s	Memory Swap Page In 485.0 count 22.5 K 20.4 K 1.1 M	Memory Swap Page Or 422.0 count 7.2 K 5.9 K 1.1 M
iainer Name ig_redis_1.rwfn2moecimr?V5sb3gmagtmk g_vote_1.io3t8mmgvapbdacszwbvdd99 sg_vote_2.wh7x16y4f6r402sdysginnm g_worker.1.wyglopBbzuligpleImzpj2e g_voueller_1.dfj23lgr62/j4/2rumvk96pp catcluster_proxy.q2hagsrt56redmhdt4gcdea.sgxxxdfc/2wwl6i9giit38s1t	2.9 % 0.0 % 0.0 % 38.2 % 0.0 %	57 ms 0 ms 0 ms 737 ms 0 ms	0.1 % 0.5 % 0.5 % 1.4 % 0.3 %	154.6 KB/s 0.0 B/s 0.0 B/s 403.0 KB/s 40.7 B/s	0.0 KB/s 0.0 KB/s 0.0 KB/s 0.0 KB/s 0.0 KB/s	Memory Swap Page In 485.0 count 22.5 K 20.4 K 1.1 M 134.0 K	Memory Swap Page Or 422.0 count 7.2 K 5.9 K 1.1 M 125.2 K
rm Containers tainer Name g., eds. J., mk/k2/moed/mr/X-Sob3gmagtmk ngvote. J. io388mmg/wpbidocs2wbvdd99 g	2.9 % 0.0 % 0.0 % 38.2 % 0.0 % 0.0 %	57 ms 0 ms 0 ms 737 ms 0 ms 0 ms	0.1 % 0.5 % 0.5 % 1.4 % 0.3 % 0.2 %	154.6 KB/s 0.0 B/s 0.0 B/s 403.0 KB/s 40.7 B/s 0.0 B/s	0.0 KB/s 0.0 KB/s 0.0 KB/s 0.0 KB/s 0.0 KB/s 0.0 KB/s	Memory Swap Page In 485.0 count 22.5 K 20.4 K 1.1 M 134.0 K 13.9 K	Memory Swap Page Or 422.0 count 7.2 K 5.9 K 1.1 M 125.2 K 8.4 K

Heat maps will be refreshed automatically when you change either of the following fields:

- Topology Type: Indicates the monitored topology object, including Docker Container and Docker Host.
- · Cluster: Lists all clusters available in the monitored Docker Swarm environment.
- Selected Metric: Populates a rectangle based upon the selected metrics. For example, if you select Memory Time Used from the Selected Metric drop-down list, the rectangle area will be populated based on the used CPU time for the selected topology object. For more information about metrics, refer to Docker Swarm metrics on page 61.
- Rendering related metrics: For example, if you select *CPU Utilization* and Red to Green, the rectangle of the topology object that has larger value of CPU Utilization will be rendered in red.
 - Color Metric: Renders the color of rectangle based upon the selected color metric.
 - Color Pattern: Offers two patterns, Red to Green (larger value shows in red) or Green to Red (larger value shows in green).

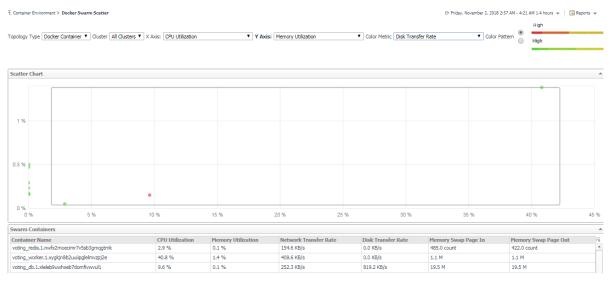
Figure 42 shows an example of heat map. This sample diagram represents the

"voting_redis.1.nwfx2moecimr7v5sb3gmqgtmk" has the maximum amounts of CPU Utilization which is the largest in size, and also it has the higher Memory Utilization since it is in Red. If you switch the Color Pattern, then "voting_redis.1.nwfx2moecimr7v5sb3gmqgtmk" will turn to green. Clicking the object name on the heat map directs you to the relevant object *Explorer* dashboard. For more information, see:

- Container Explorer view on page 46
- Docker Host Explorer view on page 47
- Container metrics on page 61

Scatter Plot analytics

Figure 43. Docker Swarm Scatter Plot Analytics Dashboard



The points on the chart will be refreshed automatically when you change either of the following fields:

- Topology Type: Indicates the monitored topology object, including Docker Container and Docker Host.
- Cluster: Lists all clusters available in the monitored Docker Swarm environment.
- X Axis: Indicates which metrics will be plotted on X axis.
- Y Axis: Indicates which metrics will be plotted on Y axis.
- · Rendering related metrics:
 - Color Metric: Renders the color of circle based upon the selected metrics.
 - Color Pattern: Offers two patterns, Red to Green (larger value shows in red) or Green to Red (larger value shows in green).

Figure 43 shows an example of Scatter Plot analytics. The purple circle in the middle represents the following: "voting_redis.1.nwfx2moecimr7v5sb3gmqgtmk" CPU Utilization is 2.9%, its Memory Usage is 0.1%, and its value of Network Transfer Bytes is not high. For more information, see:

- Container Explorer view on page 46
- Docker Host Explorer view on page 47
- Container metrics on page 61

Domains and Object Groups

Domains

A domain is a group of monitored components organized by monitoring technology. This dashboard shows a summarized view of your monitored enterprise organized by domain. Click on a sub-domain for detailed information about the contents and health of the domain.

To access the Domains dashboard, on the Navigation panel, click **Dashboards > Services > Domains**.

Click the + icon to display the components under Container.

Figure 44. Container Components in Domains dashboard

Domains				G+ Monday, June 24, 2019 10:16:44 AM	- Now 60 minutes 👻 📔 Re	eports
💻 Domains						
A domain is a group of m	onitored components organized by mo tents and health of the domain.	nitoring technology. This dashboard show	s a summarized view of your mo	nitored enterprise organized by domain	. Click on a sub-domain for	detail
	Name 🔺	State	History	Alarms	Agents	5
Container		•				
📥 Docker Swarm		S				
Kubernetes		🔶 💻		27 15	Solution	
Custom Applications		O				
Databases		S				
🗉 🤱 End User		0				
🛙 💼 Infrastructure		8				
Packaged Applications						

Click the State, History, Alarms, and Agents column, for detailed alarms and health information.

Object Groups

An object group is a mapping to a certain set of data types of the objects you are interested in.

To access the Object Groups dashboard, on the Navigation panel, click **Dashboards > Services > Object Groups**.

Figure	45.	Object	Groups	for	Container

0	Add	📝 Eo	lit 🤤 Remove					Search	,P -	
	Act Edit	ions Test	Name 🔺		Descr	iption		Is Disabled	Created by Foglight	
			Agents	All Agent objects.				false	true	
	1	-	All Models	All model objects.					true	
	1	-	Арр	The Application Tie	er includes all objects from .NET, Siebel, SA		false	true		
	2	-	Azure	All Azure Objects			false	true		
)	1	C	DB	The Database Tier	includes all objects from Oracle, SQLServe		false	true		
)	1	-	Docker Swarm	All Docker Swarm	Objects		false	true		
	1	-	Geo	All Geo Aware App	lications.			false	true	
	1	-	Global Services	All Global Services.				false	true	
	1		Hosts	All Host objects.				false	true	
)	1	C	Hyper-V	All Hyper-V Object	s			false	true	
	2	-	Java EE	The Java EE Tier in	cludes all objects from Weblogic, WebSph	ere, JBoss, OracleAS,		false	true	
	1	6	Kubernetes	All Kubernetes Obj	ects			false	true	
	1	-	OpenStack	All OpenStack Obje	ects			false	true	
)	2	6	User	The User Tier inclu	des all the objects for end user performan	ce.		false	true	
	2	-	VMware	All VMware Object	5			false	true	
	1	5	V/Mware Clusters	All VMware Cluster	e			false	true	
ıbe	rnete	s has :	19 subgroup(s)							
0	Add	Selec	t All Select None 🤤 R	emove				Search	,	•
	Action Edit		Nam	e 🔺	Description	Data Type	Query Conditi	ons Is Disabled	Created by Foglight	t
			Kubernetes Clusters		All Kubernetes Clusters	KubeCluster	n/a	false	true	
	1		Kubernetes Config Maps		All Kubernetes Config Maps	KubeConfigMap	n/a	false	true	
	1		Kubernetes Cron Jobs		All Kubernetes Cron Jobs	KubeCronJob	n/a	false	true	
	1	_	Kubernetes Daemon Set	s	All Kubernetes Daemon Sets	KubeDaemonSet	n/a	false	true	
			Kubernetes Deployment	s	All Kubernetes Deployments	KubeDeployment	n/a	false	true	
	1		Kubernetes Endpoints		All Kubernetes Endpoints	KubeEndpoint	n/a	false	true	
	1				All Kubernetes Ingresses	KubeIngress	n/a	false	true	
		Image: Water with the second						false		

Select Docker Swarm or Kubernetes to display the subgroups.

Metrics

Kubernetes metrics

Pod metrics

Table 4. Pod metrics

Metric name	Description
CPU Usage	CPU usage on all cores in millicores.
CPU Usage Rate	CPU usage rate on all cores in millicores/second.
CPU Request	CPU request (the guaranteed amount of resources) in millicores.
CPU Limit	CPU hard limit in millicores.
CPU Utilization	Percentage of CPU usage / CPU limit if user configured CPU limit for this pod.
Memory Usage	Total memory usage in bytes.
Memory Working Set	Total working set usage. Working set is the memory being used and not easily dropped by the kernel.
Memory Rss	RSS memory usage.
Memory Request	Memory request (the guaranteed amount of resources) in bytes.
Memory Limit	Memory hard limit in bytes.
Memory Page Faults	Number of page faults.
Memory Major Page Faults	Number of major page faults.
Memory Page Faults Rate	Number of page faults per second.
Memory Major Page Faults Rate	Number of major page faults per second.
Memory Utilization	Percentage of Memory usage / Memory limit if user configured Memory limit for this pod.
Network Send	Total send bytes.
Network Receive	Total receive bytes.
Network Send Rate	Total send bytes per second.
Network Receive Rate	Total receive bytes per second.
Network Send Errors	Total send errors count.
Network Receive Errors	Total receive errors count.
Network Send Errors Rate	Total send errors count per second.
Network Receive Errors Rate	Total receive errors count per second.
Network Transfer	Total send and receive bytes.
Network Transfer Rate	Total send and receive bytes per second.

Node metrics

Table 5. Node metrics

Metric name	Description
CPU Usage	CPU usage on all cores in millicores.
CPU Usage Rate	CPU usage rate on all cores in millicores/second.
CPU Request	CPU request (the guaranteed amount of resources) in millicores.
CPU Limit	CPU hard limit in millicores.
CPU Utilization	CPU utilization as a share of node allocatable.
Memory Usage	Total memory usage in bytes.
Memory Working Set	Total working set usage. Working set is the memory being used and not easily dropped by the kernel.
Memory RSS	RSS memory usage.
Memory Request	Memory request (the guaranteed amount of resources) in bytes.
Memory Limit	Memory hard limit in bytes.
Memory Page Faults	Number of page faults.
Memory Major Page Faults	Number of major page faults.
Memory Page Faults Rate	Number of page faults per second.
Memory Major Page Faults Rate	Number of major page faults per second.
Memory Utilization	Memory utilization as a share of memory allocatable.

Cluster metrics

Table 6. Cluster metrics

Metric name	Description
CPU Usage	CPU usage on all cores in millicores.
CPU Usage Rate	CPU usage rate on all cores in millicores/second.
CPU Request	CPU request (the guaranteed amount of resources) in millicores.
CPU Limit	CPU hard limit in millicores.
Memory Usage	Total memory usage in bytes.
Memory Request	Memory request (the guaranteed amount of resources) in bytes.
Memory Limit	Memory hard limit in bytes.

Docker Swarm metrics

Container metrics

Table 7. Container metrics

Metric name	Description
CPU Utilization	CPU utilization.
CPU Time Used	Total CPU time that a container used.
CPU Throttled Time	Total time that a container's CPU usage was throttled.
Memory Page Fault	Total page fault count of a container's Memory.
Memory Consumed	Total memory consumed of a container in bytes.

Foglight for Container Management 2.0.0 User and Administration Guide Using Foglight for Container Management 61

Table 7. Container metrics

Metric name	Description
Memory Utilization	Memory utilization.
Memory PageIn Rate	Total page in count of a container's Memory.
Memory PageOut Rate	Total page out count of a container's Memory.
Disk Read Bytes	Total disk read bytes.
Disk Write Bytes	Total disk write bytes.
Disk Transfer Rate	Sum of total disk read and write bytes.
Network Send Packets	Total network send packets count.
Network Receive Packets	Total network receive packets count.
Network Send Bytes	Total network send bytes.
Network Receive Bytes	Total network receive bytes.
Network Inbound Dropped Packets	Total dropped packet count of all the packets coming into the container.
Network Outbound Dropped Packets	Total dropped packet count of all the packets going out from the container.
Network Transfer Rate	Sum of network send bytes and receive bytes per seconds during a specific period.

Rules

Foglight for Container Management allows you to create flexible rules that can be applied to complex interrelated data from multiple sources within your clusters. You can associate several different actions with a rule, configure a rule so that it does not fire repeatedly, and associate a rule with schedules to define when it should be evaluated or not.

Different types of data can be used in rules, including registry variables, raw metrics, derived metrics, and topology object properties.

There are two types of rules: simple rules and multiple-severity rules. A simple rule has a single condition, and can be in one of three states: *Fire*, *Undefined*, or *Normal*. A multiple-severity rule can have up to five severity levels: *Undefined*, *Fatal*, *Critical*, *Warning*, and *Normal*.

Rule conditions are regularly evaluated against monitoring data (metrics and topology object properties collected from your monitored environment and transformed into a standard format). Therefore, the state of the rule can change if the data changes. For example, if a set of monitoring data matches a simple rule's condition, the rule enters the *Fire* state. If the next set does not match the condition, the rule exits the *Fire* state and enters the *Normal* state.

Rules can be configured to send emails, pager messages, or perform other actions you define. Performance data can be viewed and analyzed using Foglight for Container Management.

Foglight for Container Management includes a number of predefined rules used to monitor the health of your container clusters. You are allowed to modify these rules to satisfy your different requirements. Many of these rules listed and described in this section have thresholds defined within them. Those thresholds include standard deviations, utilization percentages, and so on, are default values predefined in the registry.

Kubernetes

All rules are controlled by registry variable Kubernetes:AlertSensitivity. If the value is 0, then no alarm can be fired. If the value is 1, warning level alarm can be fired. If the value is above 1, then all level alarm can be fired.

Kubernetes Administrator email address can be configured in Registry Variable KubernetesAdmin.

Health Check

Kubernetes Pod Health Check

Purpose

This rule detects abnormal Pod health status and fires alarm for different severity abnormal health status.

Scope

KubePod

Conditions and Severities

Conditions	Severity	Action
Pods that is in Failed or Unknown status. Or the node which is running the pod gets disconnected.	Critical	Send email to Kubernetes Administrator.
Pods that is in CrashLoopBackOff status.	Warning	None

Kubernetes Pod Health Check (Pending Phase)

Purpose

This rule detects Pods that stays in pending phase for an abnormal long time.

Scope

KubePod

Conditions and Severities

Conditions	Severity	Action
Pods that is pending for two continuous data submission periods because of Failed to schedule to Node.	Critical	Send email to Kubernetes Administrator.
Pods that is pending for two continuous data submission periods because container is not ready.	Warning	None

Kubernetes Container Health Check

Purpose

This rule detects abnormal Container health status and fires alarm for different severity abnormal health status.

Scope

KubeContainer

Conditions and Severities

Conditions	Severity	Action
Container that is terminated for abnormal reasons.	Critical	Send email to Kubernetes
		Administrator.

Kubernetes Node Health Check

Purpose

This rule detects abnormal Node health status and fires alarm for different severity abnormal health status.

Scope

KubeNode

Conditions and Severities

Conditions	Severity	Action
Nodes that is not Ready or out of disk or network unavailable.	Critical	Send email to Kubernetes Administrator.
Nodes whose memory or disk is under pressure.	Warning	None

Kubernetes Deployment Health Check

Purpose

This rule detects abnormal Deployment health status and fires alarm for different severity abnormal health status.

Scope

KubeDeployment

Conditions and Severities

Conditions	Severity	Action
Deployment is not available.	Critical	Send email to Kubernetes Administrator.
Deployment has failed to create some of the replicated pods.	Warning	None

Kubernetes Daemon Set Health Check

Purpose

This rule detects abnormal Daemon Set health status and fires alarm for different severity abnormal health status.

Scope

KubeDaemonSet

Conditions and Severities

Conditions	Severity	Action
Some of the pods created by the Daemon Set is not available or mis-scheduled.	Critical	Send email to Kubernetes Administrator.
The daemon set doesn't have enough replicated pods running that meets its desired replicated pods count.	Warning	None

Kubernetes Job Health Check

Purpose

This rule detects abnormal Job health status and fires alarm for different severity abnormal health status.

Scope

KubeJob

Conditions and Severities

Conditions	Severity	Action
Job that is failed.	Warning	None

Kubernetes Persistent Volume Health Check

Purpose

This rule detects abnormal Persistent Volume health status and fires alarm for different severity abnormal health status.

Scope

KubePersistentVolume

Conditions and Severities

Conditions	Severity	Action
Persistent Volume that is in failed status.	Warning	None

Kubernetes Persistent Volume Claim Health Check

Purpose

This rule detects abnormal Persistent Volume Claim health status and fires alarm for different severity abnormal health status.

Scope

KubePersistentVolumeClaim

Conditions and Severities

Conditions	Severity	Action
Persistent Volume Claim that is in failed status.	Warning	None

Kubernetes Persistent Volume Claim Health Check (Long Pending)

Purpose

This rule detects abnormal long pending Persistent Volume Claim and fires alarm for different severities.

Scope

KubePersistentVolumeClaim

Conditions and Severities

Conditions	Severity	Action
Persistent Volume Claim that is pending for two continuous	Critical	None
data submission periods.		

Usage

Kubernetes Pod CPU Utilization

Purpose

This rule detects abnormal CPU Utilization for Pods, and fires alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities. This rule only works for those Pods that configures CPU limit.

Scope

KubePod.metrics

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Pods whose usage is about to reach the limit, the ration is above the value configured in fatal Threshold.	Fatal	Kubernetes:PodCpu UtilizationFatal	Send email to Kubernetes Administrator
Pods whose usage is about to reach the limit, the ration is above the value configured in critical Threshold.	Critical	Kubernetes:PodCpu UtilizationCritical	None
Pods whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	Kubernetes:PodCpu UtilizationWarning	None

*Note: the unit is percentage.

Kubernetes Pod Memory Utilization

Purpose

This rule detects abnormal Memory Utilization for Pods, and fires alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities. This rule only works for those Pods that configures Memory limit.

Scope

KubePod.metrics

Conditions	Severity	Threshold (Registry Variable)*	Action
Pods whose usage is about to reach the limit, the ration is above the value configured in fatal Threshold.	Fatal	Kubernetes:PodMemory UtilizationFatal	Send email to Kubernetes Administrator
Pods whose usage is about to reach the limit, the ration is above the value configured in critical Threshold.	Critical	Kubernetes:PodMemory UtilizationCritical	None
Pods whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	Kubernetes:PodMemory UtilizationWarning	None

*Note: the unit is percentage.

Kubernetes Pod CPU Usage

Purpose

This rule detects abnormal CPU Usage for Pods, and fires alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePod.metrics

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Pods whose usage is above the value configured in fatal Threshold.	Fatal	Kubernetes:PodCpu UsageFatal	Send email to Kubernetes Administrator
Pods whose usage is above the value configured in critical Threshold.	Critical	Kubernetes:PodCpu UsageCritical	None
Pods whose usage is above the value configured in warning Threshold.	Warning	Kubernetes:PodCpu UsageWarning	None

*Note: the unit is percentage.

Kubernetes Pod Memory Usage

Purpose

This rule detects abnormal Memory Usage for Pods, and fires alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePod.metrics

Conditions	Severity	Threshold (Registry Variable)*	Action
Pods whose usage is above the value configured in fatal Threshold.	Fatal	Kubernetes:PodMemory UsageFatal	Send email to Kubernetes Administrator
Pods whose usage is above the value configured in critical Threshold.	Critical	Kubernetes:PodMemory UsageCritical	None
Pods whose usage is above the value configured in warning Threshold.	Warning	Kubernetes:PodMemory UsageWarning	None

*Note: the unit is percentage.

Kubernetes Pod Network Receive

Purpose

This rule detects abnormal Network Receive in bytes for Pods, and fire alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePod.metrics

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Pods whose usage is above the value configured in fatal Threshold.	Fatal	Kubernetes:PodNetwork ReceiveFatal	Send email to Kubernetes Administrator
Pods whose usage is above the value configured in critical Threshold.	Critical	Kubernetes:PodNetwork ReceiveCritical	None
Pods whose usage is above the value configured in warning Threshold.	Warning	Kubernetes:PodNetwork ReceiveWarning	None

*Note: the unit is percentage.

Kubernetes Pod Network Send

Purpose

This rule detects abnormal Network Send in bytes for Pods, and fire alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePod.metrics

Conditions	Severity	Threshold (Registry Variable)*	Action
Pods whose usage is above the value configured in fatal Threshold.	Fatal	Kubernetes:PodNetwork SendFatal	Send email to Kubernetes Administrator
Pods whose usage is above the value configured in critical Threshold.	Critical	Kubernetes:PodNetwork SendCritical	None
Pods whose usage is above the value configured in warning Threshold.	Warning	Kubernetes:PodNetwork SendWarning	None

*Note: the unit is percentage.

Kubernetes Node CPU Utilization

Purpose

This rule detects abnormal CPU Utilization in bytes for Nodes, and fire alarm on different severities. It is enabled by default. You can change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubeNode.metrics

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Nodes whose utilization is above the value configured in fatal Threshold.	Fatal	Kubernetes:NodeCpu UtilizationFatal	Send email to Kubernetes Administrator
Nodes whose utilization is above the value configured in critical Threshold.	Critical	Kubernetes:NodeCpu UtilizationCritical	None
Nodes whose utilization is above the value configured in warning Threshold.	Warning	Kubernetes:NodeCpu UtilizationWarning	None

*Note: the unit is percentage.

Kubernetes Node Memory Utilization

Purpose

This rule detects abnormal Memory Utilization in bytes for Nodes, and fire alarm on different severities. It is enabled by default. You can change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubeNode.metrics

Conditions	Severity	Threshold (Registry Variable)*	Action
Nodes whose utilization is above the value configured in fatal Threshold.	Fatal	Kubernetes:NodeMemory UtilizationFatal	Send email to Kubernetes Administrator
Nodes whose utilization is above the value configured in critical Threshold.	Critical	Kubernetes:NodeMemory UtilizationCritical	None
Nodes whose utilization is above the value configured in warning Threshold.	Warning	Kubernetes:NodeMemory UtilizationWarning	None

*Note: the unit is percentage.

Kubernetes Node Network Receive

Purpose

This rule detects abnormal Network Receive in bytes for Nodes, and fire alarm on different severities. It is enabled by default. You can change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubeNode.metrics

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Nodes whose utilization is above the value configured in fatal Threshold.	Fatal	Kubernetes:NodeNetwork ReceiveFatal	Send email to Kubernetes Administrator
Nodes whose utilization is above the value configured in critical Threshold.	Critical	Kubernetes:NodeNetwork ReceiveCritical	None
Nodes whose utilization is above the value configured in warning Threshold.	Warning	Kubernetes:NodeNetwork ReceiveWarning	None

*Note: the unit is percentage.

Kubernetes Node Network Send

Purpose

This rule detects abnormal Network Send in bytes for Nodes, and fire alarm on different severities. It is enabled by default. You can change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubeNode.metrics

Conditions	Severity	Threshold (Registry Variable)*	Action
Nodes whose utilization is above the value configured in fatal Threshold.	Fatal	Kubernetes:NodeNetwork SendFatal	Send email to Kubernetes Administrator
Nodes whose utilization is above the value configured in critical Threshold.	Critical	Kubernetes:NodeNetwork SendCritical	None
Nodes whose utilization is above the value configured in warning Threshold.	Warning	Kubernetes:NodeNetwork SendWarning	None

*Note: the unit is percentage.

Docker Swarm

All rules are controlled by registry variable Docker:AlertSensitivity. If the value is 0, then no alarm can be fired. If the value is 1, warning level alarm can be fired. If the value is above 1, then all level alarm can be fired.

Docker Swarm Administrator email address can be configured in Registry Variable Docker:DockerAdmin.

Health Check

Docker Container Status

Purpose

This rule detects abnormal Container health status and fires alarm for different severity abnormal health status.

Scope

DockerContainer

Conditions and Severities

Conditions	Severity	Action
Container that is already stopped for abnormal reason.	Critical	Send email to Docker
		Swarm Administrator

Docker Container Status - Paused

Purpose

This rule detects abnormal long-time paused Container and fires alarm for different severity abnormal health status.

Scope

DockerContainer

Conditions	Severity	Action	
Container paused for two continuous data submission periods.	Warning	None	

Docker Service Status

Purpose

This rule detects abnormal Docker Swarm Service health status and fires alarm for different severity abnormal health status.

Scope

DockerService

Conditions and Severities

Conditions	Severity	Action
Missing some of the replicated task running for this service.	Critical	Send email to Docker Swarm Administrator

Docker Task Status

Purpose

This rule detects abnormal Docker Swarm Task health status and fires alarm for different severity abnormal health status.

Scope

DockerTask

Conditions and Severities

Conditions	Severity	Action
Task that is in failed, orphaned or remove status.	Critical	Send email to Docker
		Swarm Administrator

Docker Task Status -- pending

Purpose

This rule detects abnormal long-time pending Docker Swarm Task and fires alarm for different severity abnormal health status.

Scope

DockerTask

Conditions	Severity	Action	
Task that is in pending status for two continuous data submission periods.	Warning	None	

Usage

Docker Swarm Container CPU Utilization

Purpose

This rule detects abnormal CPU Utilization for Docker Swarm Containers, and fire alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities. This rule only works for those Containers that configures CPU limit.

Scope

DockerContainerCPU

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Container whose usage is about to reach the limit, the ration is above the value configured in fatal Threshold.	Fatal	Docker:ContainerCpu UtilizationFatal	Send email to Kubernetes Administrator
Pods whose usage is about to reach the limit, the ration is above the value configured in critical Threshold.	Critical	Docker:ContainerCpu UtilizationCritical	None
Pods whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	Docker:ContainerCpu UtilizationWarning	None

*Note: the unit is percentage.

Docker Swarm Container Memory Utilization

Purpose

This rule detects abnormal Memory Utilization for Docker Swarm Containers, and fire alarm on different severities. It is disabled by default. You can customize it and enable it based on your different requirements. For more details about customization, refer to Customization on page 74. You can also change value of the registry variables or use your own value to change the threshold of each severities. This rule only works for those Containers that configures Memory limit.

Scope

DockerContainerMemory

Conditions	Severity	Threshold (Registry Variable)*	Action
Container whose usage is about to reach the limit, the ration is above the value configured in fatal Threshold.	Fatal	Docker:ContainerMemory UtilizationFatal	Send email to Kubernetes Administrator
Pods whose usage is about to reach the limit, the ration is above the value configured in critical Threshold.	Critical	Docker:ContainerMemory UtilizationCritical	None
Pods whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	Docker:ContainerMemory UtilizationWarning	None

*Note: the unit is percentage.

Customization

To customize a rule, Rule Scope and Condition will be used frequently.

To access Rule Scope and Condition, do the following:

- 1 Under **Dashboards**, click **Administration** > **Rules & Notifications** > **Rules**, then click on the rule and select *View and Edit*.
- 2 Click **Rule Editor** on the *Rule Detail* popup dialog box. Then click **Continue** on the *Confirm Edit Rule* popup dialog box.
- 3 On the **Rule Editor** dashboard, *Rule Scope* can be located on the **Rule Definition** tab and Condition can be located on the **Condition & Actions** tab.

₹ Rules > Rule Editor G•	Monday, July 29, 2019 2:16:31 PM - 3:16:31 PM 60 minutes 💌 📋 🖪 Reports 👻	
Rule Definition Condition & Actions Schedules Behavior Rule Variables		
Basic Information Rule Name: Kubernetes Node Network Receive Rule Type: Multiple-Sevenity Rule Cartridge Name(Cartridge Version): Kubernetes-Agent (20.0) Rule Tragering: Time Driven © Time Driven © Event Driven © Schedule Driven	Description (Optional) Rule Description: Periodically check kubernetes node network receive bytes, if the value is too high and changes too much, then an alarm will be triggered. Alarm Description:	
Schedule Driven Rule Scope Cartridges: Kuberleapster/Metrics KubeNode.metrics		

Figure 46. Rule Scope

Figure 47. Condition

T Rules ≻ Rule Editor	G+ Monday, July 29, 2019 2:51:36 PM - 3:51:36 PM 60 minutes 💌 📋 🖪 Reports 💌
Rule Definition Condition & Actions Schedules Behavior Rule Variables	
	Run Condition Query
Rule Name: Kubernetes Node Network Receive	Run Condition Query
Rule Type: Multiple-Severity Rule	
S Fatal	ره ا
🚱 Critical	*
Copy condition/alarm from 🔚 Copy variables/actions from	
Condition Severity Level Variables Email Notification & Recovery Actions	
Activate	
Jusert Metrics for evaluation	Alarm Message:
	Click to insert preconfigured Foglight Registry Variables
Available Rule Logic Operations, Click to Insert:	
8& < > = () ! + - * /	Example: Inserting the Foglight System Variable `@foglight_rule_name' will add the name configured on the Rule Definition tab into the alarms message
if (registry("Kubernetes:AlertSensitivity") > 1) {	The network receive @networkRxValue of kubernetes node @nodeName in cluster @clusterName reach critical threshold
return false;	©registryNetworkReceiveCritical.
return #networkRx# >= registry("Kubernetes:NodeNetworkReceiveCritical")	
return #networkkx# >= registry(kubernetes:nodenetworkketervechickar)	
Test Rule Logic)
A Warning	v
📀 Normal	▼
O Undefined(Not Active)	*

Kubernetes

Filter Pods by Cluster

Finding Pods inside cluster "kubecluster", enter following statement in the Scope of a rule, and choose KubePod as the Topology Type in the Rule Scope.

KubePod where namespace.cluster.name='kubecluster'

Filter Pods by Namespace

Finding Pods inside namespace "default" of Cluster "kubecluster", enter following statement in the Scope of a rule, and choose KubePod as the Topology Type in the Rule Scope.

KubePod where namespace.cluster.name='kubecluster' and namespace.name='test'

Filter Nodes by Cluster

Finding Nodes inside cluster "kubecluster", enter following statement in the Scope of a rule, and choose KubeNode as the Topology Type in the Rule Scope.

KubeNode where cluster.name='nancyakscluster'

Filter Pod by Labels

Find Pods with labels "run=nginx" and "env=prod" among all clusters, enter following statement in the Scope of a rule, and choose KubePod as the Topology Type in the Rule Scope.

KubePod where labels.key='run' and labels.value='nginx-rollingupdate' and labels.key='env' and labels.value='prod'

If you want to find Pods by labels in namespace "test" of cluster "kubecluster", you can append and namespace.cluster.name='kubecluster' and namespace.name='test' to the end of above statement.

Filter Node by Labels

Find Nodes with labels "env=prod" among all clusters, enter following statement in the Scope of a rule, and choose KubeNode as the Topology Type in the Rule Scope.

KubeNode where labels.key='env' and labels.value='prod'

If you want to find Nodes by labels in cluster "kubecluster", you can append *and cluster.name='kubecluster'* to the end of above statement.

Filter Pod Metrics by Pod Labels

Find Pods Metrics with labels "run=nginx" and "env=prod" among all clusters, enter following statement in the Scope of a rule, and choose KubeHeapsterMetrics as the Topology Type in the Rule Scope.

KubePod.metrics where object.labels.key='run' and object.labels.value='nginx' and object.labels.key='env' and object.labels.value='prod'

If you want to find Pods by labels in namespace "test" of cluster "kubecluster", you can append and namespace.cluster.name='kubecluster' and namespace.name='test' to the end of above statement.

Filter Nodes Metrics by Node Labels

Find Node Metrics with labels "env=prod" among all clusters, enter following statement in the Scope of a rule, and choose KubeHeapsterMetrics as the Topology Type in the Rule Scope.

KubeNode.metrics where object.labels.key='env' and object.labels.value='prod'

If you want to find Nodes by labels in cluster "kubecluster", you can append *and cluster.name='kubecluster'* to the end of above statement.

Docker Swarm

Filter Container by Swarm Cluster

Find Containers in cluster "dockercluster", enter following statement in the Scope of a rule, and choose DockerContainer as the Topology Type in the Rule Scope.

DockerContainer where dockerSwarm.service.cluster.name='kicakdscluster'

Filter Container by Labels

Find Containers with labels "com.docker.stack.namespace=nginx" and "env=prod" among all clusters, enter following statement in the Scope of a rule, and choose DockerContainer as the Topology Type in the Rule Scope.

DockerContainer where labels.key='com.docker.stack.namespace' and labels.value='nginx' and labels.key='env' and labels.value='prod'

If you want to find Containers by labels in cluster "swarmcluster", you can append *and dockerSwarm.service.cluster.name='kicakdscluster'* to the end of above statement.

Filter Docker Host by Swarm Cluster

Find Docker Hosts in cluster "dockercluster", enter following statement in the Scope of a rule, and choose DockerHost as the Topology Type in the Rule Scope.

DockerHost where dockerSwarmNodeInfo.node.cluster.name='kicakdscluster'

Filter Container CPU Usage by Container Labels

Find Container CPU Usage by container labels "com.docker.stack.namespace=nginx" and "env=prod" among all clusters, enter following statement in the Scope of a rule, and choose DockerContainerCPU as the Topology Type in the Rule Scope.

DockerContainerCPU where container.labels.key='com.docker.stack.namespace' and container.labels.value='nginx' and container.labels.key='env' and container.labels.value='prod'

If you want to find Containers by labels in cluster "swarmcluster", you can append and container.dockerSwarm.service.cluster.name='kicakdscluster' to the end of above statement.

Filter Container Memory Usage by Container Labels

Find Container CPU Usage by container labels "com.docker.stack.namespace=nginx" and "env=prod" among all clusters, enter following statement in the Scope of a rule, and choose DockerContainerMemory as the Topology Type in the Rule Scope.

DockerContainerMemory where container.labels.key='com.docker.stack.namespace' and container.labels.value='nginx' and container.labels.key='env' and container.labels.value='prod'

If you want to find Containers by labels in cluster "swarmcluster", you can append and container.dockerSwarm.service.cluster.name='kicakdscluster' to the end of above statement.

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build communitydriven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation[™].

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx/.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.