

Foglight[®] for Container Management 7.1.0 User and Administration Guide



© 2023 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 Where next meets now 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 Times Linux are registered 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, JBoos, the JBoos logo, and 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, SoL Server, Visual Basic, Windows, Windows, Vista and Windows Server are either registered trademarks or 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. SPARC Is a registered trademark of SPARC International, Inc. in the United States and other countries. Toolucts bearing the SPARC trademarks of the United States, other countries, or both. MySQL is a registered trademark of MySQL as a registered trademark of Linus Torvalds in the United States, other countries, orben, System and UNIX are registered trademarks of Trademarks of VMware, Inc. in the United States and/or the riprisdictions. Sybase is a registered trademarks of the Mozilla Foundation. "Eclipse Foundation Member", Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Foundation Member", Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Foundation Member", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Foundat 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 Foglight Version- 7.1.0 Software Version- 7.1.0

Contents

Understanding Foglight for Container Management
About Foglight for Container Management
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 interval25
Using Foglight for Container Management
Kubernetes
Monitoring Kubernetes Clusters
Monitoring Kubernetes Nodes
Monitoring Kubernetes Workloads
Monitoring Kubernetes Pods
Monitoring Kubernetes Other Components
Alarms
Capacity Management
Cost
Optimizer
Administration
Docker Swarm
Monitoring Docker Containers
Monitoring Docker Hosts62
Monitoring Docker Swarm Clusters
Monitoring Docker Swarm Services66
Alarms
Analytics
Kubernetes analytics
Docker Swarm analytics
Domains and Object Groups
Domains
Object Groups
Reference
Metrics
Kubernetes metrics
Docker Swarm metrics
Rules
Kubernetes
Docker Swarm

Foglight for Container Management 7.1.0 User and Administration Guide Contents

Modifying alarms and threshold values	 95
Customization	 95
About Us	 100
Technical support resources	 100

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

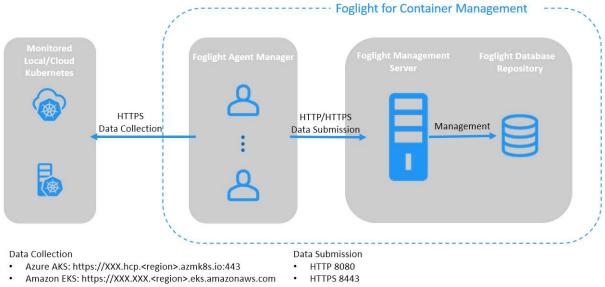
About Foglight for Container Management

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 clusters.

6

Architecture

Figure 1. Components of Foglight for Container Management



Others: <Kubernetes API Server Endpoint>

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.

i 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 Maximum		Foglight		Agent Manager		
System	Containers	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)		
Maximum Containers	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.

Foglight for Container Management 7.1.0 User and Administration Guide Understanding Foglight for Container Management

8

Getting Started

- Prerequisite
 - Kubernetes Agent
 - Preparing the Kubernetes credential
 - Enabling Heapster service in monitored environment
 - Enabling Prometheus 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:

- i 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.

9

Azure Kubernetes Service (AKS)

Before generating the Kubernetes credentials, record the following information:

- Azure Username
- Azure Password

i

- 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.

i 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.

To generate the intermediate Kubernetes credential for your cluster:

1 Log in to your Kubernetes cluster, click Connect next to your cluster name.

Kubernetes clust	iers	+ CREATE CLUS	TER 🕂 (DEPLOY CI	REFRESH	DELETE		
A Kubernetes cluster is a Filter by label or name	managed group of	uniform VM instar	nces for running	Kubernetes. Learn	more			
Name A	Location	Cluster size	Total cores	Total memory	Notifications	Labels		
🗆 🥝 -gke-demo	us-central1-a	2	2 vCPUs	4.00 GB			Connect	1

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

		and a start the second		
I can connect to y	ir cluster via command-line or i	ising a dashboard.		
Command-line	access			
onfigure <mark>kubectl</mark> o	mmand line access by running	the following comman	d:	
<pre>\$ gcloud contain</pre>	clusters get-credentials	ane-gke-demozone	us-central1-aproject	dulcet-bucksaw-20851
				L

- 3 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.

cind: Config	
preferences: {}	
users:	
 name: gke_dulcet-bucksaw-2 user: auth-provider: config: 	08510_us-centrall-a_jane-gke-demo
access-token: ya29.G	lzuBVkzkoVc1VUV 7yXM50DpQ7z7ahGzFA f2c08FhxZjDICXRFdAw5ytBc9dHBT90yYk
cmd-args: config con	fig-helperformat=json
<pre>cmd-path: C:\Users\j expiry: 2018-07-04T0 expiry-key: '{.creden token-key: '{.creden</pre>	ntial.token_expiry}'
name: don	

- 4 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. 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>
	<u> <none></none></u>
	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.

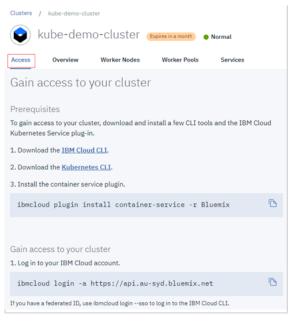
<pre>::\>kubectl describe secret jane-gke-sa-token-x2n6w tame: jane-gke-sa-token-x2n6w tamespace: default tabels: </pre> <pre>(none>) (nontations: kubernetes.io/service-account.name=jane-gke-sa kubernetes.io/service-account.uid=9f16c355-?f4f-11e8-9c03-42010a80) (ype: kubernetes.io/service-account-token) ata === == == ==: =::: 1115 bytes ===: =::: 2 bytes =:: 2 bytes =::: 2 bytes =::: 2 bytes =::: 2 bytes</pre>
<pre>lamespace: default _abels: cnone> innotations: kubernetes.io/service-account.name=jane-gke-sa kubernetes.io/service-account.uid=9f16c355-?f4f-11e8-9c03-42010a80 jgge: kubernetes.io/service-account-token lata ==== ==== ===== ======== ======= ======</pre>
abels:
.abels:
innotations: kubernetes.io/service-account.name=jane-gke-sa kubernetes.io/service-account.uid=9f16c355-7f4f-11e8-9c03-42010a80 /gge: kubernetes.io/service-account-token)ata ==== a.crt: 1115 bytes joken: eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXUCJ9.eyJpc3Mi0iJrdWJ1cm51dGUzL3N1cnZ joken: eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXUCJ9.eyJpc3Mi0iJrdWJ1cm51dGUzL3N1cnZ
kubernetes.io/service-account.uid=9f16c355-7f4f-11e8-9c03-42010a80 1032 (ype: kubernetes.io/service-account-token Data ==== a.ert: 1115 bytes Jomespace: 2 hytes Jomespace: 2 hytes Jomespace: 2 hytes Jomespace: 30 Jug211NiIsInR5cCI6IkpXUCJ9.eyJpc3Mi0iJrdWJ1cm51dGUzL3N1cnZ Jowespace: 2 hytes Jowespace: 30 Jug2121NiIsInR5cCI6IkpXUCJ9.eyJpc3Mi0iJrdWJ1cm51dGUzL3N1cnZ
1032 Sype: kubernetes.io/service-account-token Data ==== sa.crt: 1115 bytes samespace: 2 bytes soken: eyJhbGci0iJSUzIINiIsInR5cCI6IkpXUCJ9.eyJpc3Mi0iJrdWJ1cm51dGUzL3N1cmZ soken: eyJhbGci0iJSUzINiIsInR5cCI6IkpXUCJ9.eyJpc3Mi0iJrdWJ1cm51dGUzL3N1cmZ
[ype: kubernetes.io/service-account-token Data ==== a.crt: 1115 bytes Jomespace: 2 bytes Jomesiace: 2 bytes Jomesiace: 2 bytes Jowesiace: 2 bytes
Jata
Jata
 ca.crt: 1115 bytes comespace: 2 bytes comes: eyJhbGciOiJSUzIINiIsInR5cCI6IkpXUCJ9.eyJpc3MiOiJrdWJ1cm51dGUzL3N1cnZ y2UhY2WadU50[iyia3UjZXJuZXR1cv5pby9zZXJZaWN1YUNjb3UudC9uYW11c3BhY2UiOJJkZWZhdWx
 ;a.crt: 1115 bytes ;amespace: 2 bytes ;oken: eyJh6Gci0iJSUZIINiIsInR5cCI6IkpXUCJ9.eyJpc3Mi0iJrdWJ1cm51dGUzL3N1cnZ ;0V2UN2NW4U50Iiyia3UjZXJuZXR1cv5pbv9zZXJZaWN1YUNib3UudC9uYW11c3BhY2Ui0JJkZWZhdWx
a.crt: 1115 bytes namespace: 2 bytes :oken: eyJbbGciOiJSUzIINiIsInR5cCI6IkpXUCJ9.eyJpc3MiOiJrdWJ1cm5ldGUzL3N1cnZ Y2UhY2WudU50Iiwia3UiZXJuZXR1cv5pby9zZXJ2aWhIYUNib3UudC9uYW11c3BhY2UiOiJkZWZhdWx
namespace: 2 bytes soken: eydhoGciOiJSUzIINiIsInR5cCl6IkpXUCJ9.eydpc3MiOiJrdWJ1cm5ldGUzL3N1cnZ Y2UhY2WndU5ØIiwia3UiZXJuZXR1cv5pby9zZXJ2aWhIYUNjb3UudC9uYW11c3BhY2UiOJJkZWZhdWx
;oken:
;oken:
y2UhY2NvdW50Ĩ iwia3UiZXJuZXR1cv5pbv9zZXJ2aŴN1YWNjb3UudC9uYW11c3BhY2UiOiJkZWZhdWx
)I iwia3ViZXJuZXR1cy5pby9zZXJ2aWN1YWNjb3VudC9zZWNyZXQubmFtZSI6ImphbmUtZ2t1LXNhLXR
a2UuLXgybjZ3Iiwia3UiZXJuZXR1cy5pby9zZXJ2aWN1YWNjb3UudC9zZXJ2aWN1LWFjY291bnQubmF
22361mphpUtZ2t1LXNh1iwia3UiZXJuZXR1c55pby9zZXJ2aWN1YWNjb3UudC9zZXJ2aW11LWFjY29
bnQudWhIkIjoilQWyxNmHzNTUtNY2YQZiQXMWU4LJJJMPHtNDIwMTHODAwHDMUIwic3Uiloic3lzdGU
OnNicnZpYZUhY2NydW500nRlZmF1bHQ6amFuZS1na2Utc2EifQ.UdRPWHLCgU3taWV5dyjZf4PPcQmx
%XxXZDf1LT2t3tUPkgoyEWRQZOK9ebPCf0m-4h31oIBSNuq8TokcZiU5K6nf6gToJ1iNAQĚuNBwJ5zjp JumCzfiIp0jMPcTm6kF2BhhrvFkKnXNCaJRSmCIhHLBqtB4rqVKCdtJU8yfJTR253c8n2-gtT3XwPLxD
umCzfilpOjMPcTm6kF2BhhrvFkKnXNCaJRSmClhHLBqtB4rqWKCdtJU8yfJTR253c8n2-gtT3XwPLxD
PELLUzEXFr−vjaK?wDD_jFbLEyTRSmKQGiixIW1Tfea§scwops9_cJx6LŔY92FnucdwMrpnxU3aIXWUR
₁ 9B07EU5vdFXKJreabM-VAxMksgrq3tIcvS1mV5V7ujSXcpk1j-Y0P2JYwFusytjP1ptZMrSOw

5 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",
"certificate-authority-data": "LSØtLS1CRUdJTiBDRUJUSUZJQØFURSØtL
SØtCk1JSUZSUENDQXkyZØF3SUJBZØ1KQUx5SmdF0UA2NmkrTUEwRØNTcUdTSWIzRFFFQkN3VUFNRGt4T
npBMUJnT1YKQkFNTUxtUXpNall4WUdZeE5HRXpPUFExTTJGaU1XVTJabU16TXpjd09UaGhZVEF6TFd0M
UltUnlibUYwWlhNdApZMkU3SGhjTk1UZ3dOekEyTURUd05UUTNXaGNOTkRUeElÜSXhNRFU3T1RRM1dqQ
TUNUGN3T1FZRFZRUUREQzUrCk16STJNU0ZtTURSaE16azBOUE5oWWpGbE5tWmpNek0zTURrNF1XRXdNe
TFyZFdKbGNtNVxkR1Z6TFdOaE1JSUMKSWpBTkJna3Foa21H0XcyQkFRRUZBQU9DQWc4QU1JSUNDZØtDQ
WdFQX11dk4xL1pwc09CckJHTH1PT0wvenBpRwo5M3RtYUUyeGtYMnIvcjMzc1ZUTU5aY1R6a21xQjUMU
zVØŘkFkTUFQNEŮYRGJmZmpHckx3M20zZkxDL2huMnhvCjNŘQTQ0V254ZIRRU1ErK0R2MUk3VkQzcD1pT
zZzY2JUanErckFUL3q1NXFtanRRcmprUGoxN1UzTjZ2SzEvdUsKY1pwSUdQOU5WSEMxOHFaZXNkQ3Jja
FNIdEv@K2N3NXQvNEZvQ3dRb1N1TW0nUXBVWFREMkxTd05veXpX0WxZRvpvM2FraHQ30Ss5Y211U1BgR
3B0b2FBZXdOS 1B0Y055cDJDcmFsNG1DTHJXBZCM3UMVM3TFhtNEFhMvs2OEUxCkM3Uzk0NUhBTW96U
Grus XZUZT Luo UE 30 FBDc ØrkYT 1 PM09 I Q1 100 ArE 2010 NIK 15 FKRzdTZØN3VTFJAXc1 Z2 QKaU100 UØ4S
Gpys/20211000E30FB0C90FF11FH9714110Dc3m441EA1B2CEXcT0420F3M1F04AC1224A019009F3 2RJckF2SnluK21tR1d6QUpc194cjk2dy94Tm14lk11UkNpc2RzT041N3hP535pqN1Jub2E356pPZAoyL
2Rob 12/09/htt 110PU99/01/htt i S09/22/19/htt 20/11/20/htt 2/11/20/htt 2/12/09/htt
npUCkduYk×uckdWZUZCR0c3cG1tbXRZSUBw0CtGYnFxbntGUTZ5d2NXUTFqSnZ6ST1vZEp6ZnQ4Zk91Z
kRncjBteFgKR05aN1pHSU1FU1ZZU3JNTUt2RCtMT011SzBqRH1hRWpaYn80dU14R3YrU3NLMWZrc0JUW
UJvbWdBaDIvRC9UcApwNUU3SXIINkcvL2Y3UGFHc3NDMTZBK2J0Z1ZONk9o0UUsTXpHQUhTWR6ZndRR
3dxcjB4NHBMU1V2c3A2U1dFC1BZSEVmR0JMbEY4Mm5XcEHzeFVDQXdFQUFhT1FNBTR3SFFZRFZSHE9CQ
11FRKcxcUEyazQxZ21TcndIdX1tRkMKdzdsbWt1cE5NQjhHQTFVZE13UV1NQmFBRkcxcUEyazQxZ21Tc
ndIdX1tRkN3N2xta2UwTk1Bd0dBMUUkRXdRRgpNQU1CQWY4d0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dJQ
kFGc29JbWFydjJRckc4TTNKajQ5andVb2N0d21UU1JTC1NFd1RwanRvbWtGdEdÖdW9EW1VMbVMwSjRWa
3g5Wm9nRkUxZØYzb3ZPb1NFWFI4T316VGsxT24wZy9kbWUsQWwKajBHUVFoUEhCdG1HWVdtSy91ck1Ta
2IZOUJjQ3RvYU1oeUpvZTdnOXhIU3p2MzRQeTExOŨtnazE5YWZSYKRrQwo1UmpuQ011cWpCTWdZOHZtU
UlieTMwMDA1Ni9pNjlZR1RXdT1FU1ÙZOS9WTGZnajNqOXA2Q21zMzIrelIwTUQ5CjZPcjd1bU0yL0YyM
0V1dmRSRGNtbjZQN1dnaDE4dWRDd2tnWno0T0ppbzJ00DBM0VdESnRTLytuNzF0VVVHNGcKMUV5TTEzT
F1T0W1KdTUwSIIHb3p0S08zc0UCNmg4cTVZY2joMXhhZmEvR1Byc1N2SmNBNEgwVFd2Rk8yUmhNcQp5U
0ZIMjBRbzlaK3hHQ2ULUk10YjFkY2x6aktx0FQvK3JXK25vTi9FU0ZIZ1BIWmdiWW9UR3djYit6SjZha
HR1CmJWIVRzaUZSKØvCQUdmUjlXIEØvcFZnIG1YSDdrZkM4QjFaQ1N0cEZ2d0Z0eXNvQIk2BD1Id2tmS
GpvZ1J2eUAKaVxSRFŽ4eHB60ĞowWTRkc2hDancwZnFyeW1EL3UMTVNZRjFTU2NZT1BaTUwvUGN2cUNFe
Få1Z293REZgcjJIMqp2YnhpL31xcnpIZUJNMjgrZ1UWRERIazJXWWczU1ZgQnU3b3Y4QWNWbFhxY2NQU
ØZoNU 10R1d.jeŬdVd.jhFZUN4CkROdEŬHT k1 hRĬŽMSnY1eUhUb25TMØJ3Z25ŘUT h2RVYzNGv3a29TZk1LR
1kxZWM0SDhyaWZaT3pyMEt0UEIxakMKOUBoNFZTS1Ixa2ZrCi0tLS0tRU5EIENFU1RJRk1DQURFLS0tL
TRADALOS DIVANZALI JPJILEDVELI AANIKOVDONEZI SI LAZZFOIDEDSENOSELENTOINOKTP4VELDSEL SOK"

- 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-xkgrk) for later use.

C:\Users\jwang7\.kuba	e>kubectl describe servi	ceaccount jane-sa
Name:	jane-sa	
Namespace:	default	
Labels:	<none></none>	
Annotations:	<none></none>	
Image pull secrets:	<none></none>	
Mountable secrets:	jane-sa-token-xkqrk	
Tokens:	jane-sa-token-xkqrk	
Events:	<pre></pre>	

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.



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 file /etc/origin/master/admin.kubeconfig on the master node, download it and use it as the Kubernetes Agent credential.

If you could not access the file /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:

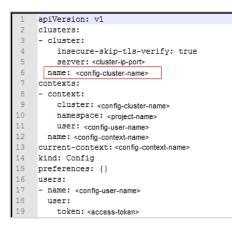
- OpenShift Username
- OpenShift Password

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 in to OpenShift and generate an intermediate Kubernetes configuration file.
 - a After logging in to OpenShift, click Command Line Tools on the upper right.
 - b 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 <*USER HOME*>/.*kube/config* on your local platform.

C Not secure https://10.4.120.18/8443/console/command-line	\$ O
NSHIFT ORIGIN	🕲 🖌 💄 hhu
Command Line Tools	
With the OpenShift command line interface (CU), you can create applications and manage OpenShift projects from a terminal. You can download the oc c using the links below. For more information about downloading and installing it, please refer to the Get Started with the CU documentation.	lient tool
Download oc :	
Latest Release of	
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 th session token:	ne same
oc login https://10.4.120.18:8443token* <hidden></hidden>	10
A taken 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 clipbe contents. After you login to your account you will get a list of projects that you can switch between:	pard
oc project «project-name»	ю.
If you do not have any existing projects, you can create one:	
oc new-project <project-name></project-name>	10
To show a high level overview of the current project:	
	IC.

c 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.
 - a Run the command oc project <project-name>.
 - b 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*

c 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 FjY29lbnQubmFtZSI6Im9zLWFkbWluIiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9 zZXJ2aWNlLWFjY29lbnQudWlkIjoiODMzNGU0NTQtNzQlYy0xMWU4LWFmNmEtMDA1MDU2YjY3 NDFhIiwic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW500mRlZmF1bHQ6b3MtYWRtaW4ifQ.RW H_AoXy2U1elkHN_Bs9IR1xo0zNCJlwcY0h3zuQnrkOFi8gVpX1177uhAPp7oIjPqDSWkUAN9F 6mP_tNdGwJsqRmHYEMOtCLnnIM61BYxIcABvwr66a0Z3Gn0D7EM5M_7XgKDC160N3W5NaH0D8 DpVTYqxkQ49u3qt4gqrcjVCaSsDNWlgGxY4KOIDrUbKkdgaRKzeD9o4Bv9VbYICqyxwoUebku JAcHiXGIcSe-ozS_zroPiltT5HW-RY0Pn3Fp3zBnydiokna0-mXot5lqoYc-R6E1U9YSrAOhWm9Q8ipiut60czXbmLPM4DYve6dmHi j5FquCqhod-QlA7aPw"

- d 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.
 - a Open and edit the intermediate configuration file.
 - b 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=<service-
account-token>
kubectl config set-context <new-context-name> --cluster=<config-cluster-
name> --user=<credential-name> --namespace=<project-name>
kubectl config use-context <new-context-name>
```

c 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.

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*

Enabling Prometheus service in monitored environment

There are various approaches to enable Prometheus on your Kubernetes cluster. Visit Prometheus Official Website to determine the approach that you are going to deploy your Prometheus service. Or you can refer to configuration management systems, such as helm (https://github.com/helm/charts/tree/master/stable/prometheus) or ansible (https://github.com/cloudalchemy/ansible-prometheus) to simplify your installation process.

In the Foglight Container **Administration** dashboard, a simple template is provided for you to deploy Prometheus service onto your cluster. For more information, see the Deploy/Migrate section in Metrics Collector on page 56.

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 <u>official guide</u>)

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
```

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

TLS secured

If TLS enabled, complete Preparing Docker Swarm Agent credentials on page 17 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 17, 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 <	$\overline{\tau}$ Credentials > Manage Credentials
IIII Expert View ↓	A credential is the information that gains access to system resou
Bookmarks There are no bookmarks Homes	patterning criteria that best suit your needs. For example, map a
Pointes V Pashboards 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 Challerine Response Challerine Response Docker CA Public Key Docker Client Private Key Docker Client Private Key Docker Client Public Key Docker Client Public Key Docker Client Public Key Dost Key Kube Config RSA Key Storage SNMP SUDO with Oustom Password SU SU with Password V

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.

Add	Add A New "Docker CA Public Key" Credential					
~	Credential Properties	F	Resource Mapping			
~	Credential Name And Lo	New Resource Mapping Co	ondition			×
Þ			cannot access. The co		used to access. They can also be used to list the Is the system which Credentials can be used to	
	Policies	access different resource	:5,			
		Usage Access Resources Using	Docker Credential Target Host Name	-		
		Equal or Not Equal	💿 equals 🔵 do	Target Host Name	Access a resource using the name of the host wh	ere it resides.
		Matching Type	Domain Name 🗸	Target Host Address	Access a resource using the IP of the host where	it resides.
		Evaluate This Condition	3			
		Matching Values (Combined Using Logical	🕑 Add a New D			
		'OR' Operator)				
			Use the above Ad	the logical 'OR'	operator.	

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

New Resource Mapping Co	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	Add a New Domain Name	
'OR' Operator)	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	
	sed to relate this Credential to the resources it can be used to access. They can also be used to lis cannot access. The combination of these conditions tells the system which Credentials can be used s.	
Usage Access Resources Using Equal or Not Equal	Docker Credential → Target Host Address →	
Matching Type Evaluate This Condition (Exact Match (Case Sensitive) ↓ 9 ✔	
Matching Values (Combined Using Logical 'OR' Operator)	Add a New IP Address IP Address	

Foglight for Container Management 7.1.0 User and Administration Guide Understanding Foglight for Container Management Click Add to finish editing New Resource Mapping Condition and back to Resource Mapping. And then click Finish.

The **Docker CA Public Key** has been uploaded and mapped to the docker host. To monitor this docker host, upload **Docker Client Public Key** and **Docker Client Private Key** by 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.

Container Environment		G+ Nonday, November 23, 2020 4:15:36 PM + 5:15:36 PM 60 minutes 👻 🛛 🔂 Reports 🔸
Kubernetes Swarm (Preview)		Analytics 🔻
Kubernetes 👻		
Monitoring Configurations Storage Load B	lancer Alarms Administration	
Custers Nodes Workloads 2 0	Pods C A C 4 6 7 10	
Kubernetes Clusters Quick View		
Kubernetes Clusters	Kubernetes Clusters Summary	🖧 View Topology 🕑 Explore
Search Q	Events	
ContainereksInen/2	▲ 	Foret Sorros Name Count = tobelet 3
	Resource Utilizations	
	Top Cpu Utilization by Nede	Top Memory Ullization by Hode 1 4 % 1 4 % 1 102 10
	Top Network Transfer (Bytes) Rate by Hode	Top Disk I/O Lead by Hode 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
	Summary	aus da
	Name contaneeds Pods 21 Deployments 10 Jobs 0 Cron Jobs 0	Version 1.16 Nodes 2 Stateful Sets 0 Daemon Sets 3 Replacion Controllers 0
	▼ Status Normal	

3 In the Container dashboard, click Administration tab, and then click Create Agent. The Create Docker Agent wizard opens.

	Kubernetes Swarm (Preview)									An	alytics 🔻	
Kubernetes Monitoring Configurations Storage Load Balancer Administration Heapster metrics collector is marked as Deprecated. Support for Heapster metrics collector will be removed in the future releases. Users are encouraged to switch to the new Prometheus metrics collector.													
Agents													
9	5												
Agent		eactivate 🐌 Start Data Collection 📒	Stop Data	Collection 😑 Dele	ete 쉽 Upo	late Agent			Se	arch		<i>p</i> •	
Agent	🕏 Refresh 🛛 🕛 Activate 🕕 De					-	Agent Version		Metrics Collec	tor			
Agent		Foglight Agent Manager Host	Active	Data Collection	Alarms	Download Log	Agent Version	Туре	Metrics Collec Status		Deploy	₽ • Properties	
Agent Add	Sefresh 🕛 Activate 💿 Do Agent Name 🔺	Foglight Agent Manager Host	Active	Data Collection	Alarms	-		Prometheus	Metrics Collec Status Healthy	tor Migrate	Deploy		
Agent Add	🕏 Refresh 🛛 🕛 Activate 🕕 De	Foglight Agent Manager Host	Active	Data Collection	Alarms	Download Log	-		Metrics Collec Status	tor	Deploy	Properties	
Agent	Sefresh 🕛 Activate 💿 Do Agent Name 🔺	Foglight Agent Manager Host	Active	Data Collection	Alarms	Download Log		Prometheus	Metrics Collec Status Healthy	tor Migrate	Deploy	Properties	
Agent	Refresh U Activate Dr Agent Name A	Foglight Agent Manager Host	Active	Data Collection	Alarms	Download Log		Prometheus Heapster	Metrics Collec Status Healthy Healthy	tor Migrate	Deploy	Properties	
Agent Add Add Add Add Add Add Add	Refresh U Activate Dr Agent Name A	Foglight Agent Manager Host	Active & &	Data Collection	Alarms	Download Log		Prometheus Heapster Prometheus	Metrics Collect Status Healthy Healthy Healthy Healthy	tor Migrate	Deploy	Properties	

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

Crea	ate Docker Agent				×					
	Agent Manager	Agent Manager	gent Manager							
0	Agent Properties	Select the agent ma	Select the agent manager, enter the cluster name and agent name.							
0	Credential	Agent Manager	fms02 🔻		0					
0	Metrics Collector	Cluster Name	kubernetscluster		0					
0	Summary	Agent Name	Monitor@kubernetscluster		Θ					

- Agent Manager: The Kubernetes Agent will be create in the selected Agent Manager.
- Cluster Name: Customized cluster name which identifies a Kubernetes cluster.
- *Agent Name:* Auto-generated agent name. You can change the name according to your requirement. It should be a unique name.

5 Agent Properties

reate Docker Agent						
✓ Agent Manager	Agent Properties					
 Agent Properties 	Kubernetes API Service End Point	Https://www.hubec.com/colladuater-and/902-add/0266.0	0			
• Credential	Collected Event Level	ABNORMAL V	0			
Metrics Collector	Enable Proxy Proxy Type	HTTP T	0 0			
 Summary 	Proxy Server Address Proxy Server Port	10.0.0.1 M	0			
	Collector Configuration	defaultSchedule 🔻	View			

- *Kubernetes API Service End Point*: The format is: http(s)://<url:port>. If you have a Kubeconfig file, retrieve this endpoint from the file (path: clusters -> cluster -> server). If there are multiple clusters, find the current context related cluster server URL.
- 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.

Foglight for Container Management 7.1.0 User and Administration Guide Understanding Foglight for Container Management **20**

- Enable Proxy: To enable the proxy, select the checkbox. Enter the Proxy Server Address and Proxy Server Port information.
- Collector Configuration: Used to configure collection interval for inventory and metrics. You can
 change the collector intervals of defaultSchedule, however, this will affect all the Kubernetes
 Agents. Or you can create a new scheduler, configure the collector intervals, and then assign this
 scheduler to this agent.

Collector intervals to configure:

- inventory interval (inventory data collection interval).
- metrics interval (performance metrics data collection interval).

6 Credential

- If no credentials were found for the provided resource, configure credentials:
 - Credential Properties: Click Load from file to upload the credential and click Next.

Create Docker Agent	x
Agent Manager Agent Properties	Credential Properties Enter the properties for this credential.
▶ Credential	The user configured in this kubeconfig file should have cluster-admin role. Otherwise, collection will fail.
Credential Properties Credential Name and Lockbox	You can load the kube config from your file or copy and paste it to the text area.
Oregendal Name and Lockbox Metrics Collector	Kube Config 🧫 Load from file ap/Version: v1
• Summary	clusters: - cluster: certificate-authority-data: LSQL51CRUd71BDPX/USU22Q0FURS0tLSQtCk1JSUVSRENDQVD20F3SU3B20lSQUxa MnF0OFJ3TFp4Hn2V2nF6hmMiGL13RF253KwVKlodmWQQVFFTEIQQVcKRRFTE1Ba 0dBMv/PQVhGUkg1XgvXlaGsQTV7NexE1EXTVNR6VMF0Q0FFSXdEUVKS29aSVh2V05B UUVCQ1BF96dn5V9BBEHDQVdvdAdn5UBTGh5chCRustLstLV1y1Mitzms5cTQR31BE NX2220h10DYzTIdQU0HRTZUWEkzeFF4SWJqZF31K2c4Mis3zRX12L2WVJ3MB2c6ESS3dB1Y1 E2vRs2hvr1NNM1M1hVlg5BEE2nS2rfunpK2KC4Hai3zRX12L2WVJ3MB2c6ESS3dB1Y1 bnAz2GR0L2Q0HQ0HITICQU3FB6EWWFCmV13dB1d3dVdVC2pmmthQVFF1B eTBG0XIPR2NmalhiVHEwUK90EWVSR1BBRppvChH1Y0x2aTdvVF3UumRTVDDFgRH Nz82SThegVc5AF6ExQQ21ThpC4VMjbG6AFHEVTT2V13LEXFATUUMRSVVF HaXh1dkRpQ1kxVWEWG9pUEBIYk1vdF4WkN3kcdyRmR1WTZOMU9UMXh2Tmr5JUV1 *

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

Create Docker Agent								
✓ Agent Manager	Credential Name and Lockbox	Credential Name and Lockbox						
✓ Agent Properties	These properties identify the credential on the	These properties identify the credential on the Management Server.						
▶ Credential	Please provide a unique name to identify this o	redential.						
 Credential Properties 	kubeconfig							
Credential Name and Lockbox	A Lockbox contains a collection of encrypted cr	edentials and the keys used for their encryption and decryption.						
 Metrics Collector 	Lockbox 🔺	Password Required						
	 System 	No						
 Summary 								

If an existing credential is detected, go to Metrics Collector directly.

7 Metrics Collector

Currently both Prometheus metrics collector and Heapster metric collector are supported. However, users are encouraged to use the Prometheus metrics collector.

Create Docker Agent					
✓ Agent Manager	Metrics Collector				
✓ Agent Properties	(i) Heapster metrics collector is marked as Deprecated. Support for Heapster metrics collector will be removed in the future releases. Users are encouraged to switch to the new Prometheus metrics collector.				
✓ Credential					
Metrics Collector	Select Metrics Collector Prometheus				
• Summary	Heapster				

Prometheus metrics collector

Create Docker Agent		×
✓ Agent Manager	Prometheus Configuration Mode	
✓ Agent Properties	Your prometheus required to meet the following prerequisites:	
✓ Credential	1. Prometheus services type: Cluster IP.	
 Metrics Collector 	2. Exporter needed: 2.1 Node - exporter:0.16.0+	
Prometheus Configuration Mode	2.2 Kube - state - metrics	
 Prometheus Configuration 	Do you have prometheus in your cluster?	
• Summary	Yes, I have. No, I have not.	
	If you have no prometheus in your Cluster, we will provide a template for you to deploy one on the next step.	
	Prometheus Type	
	"Default" type allows Agent to use KubeConfig credentials to access the Prometheus service. "OpenShift Prometheus" type, you need to provide OpenShift Route Hostname, Username and Password for Agent to access the target OpenShift Prometheus.	
	Default OpenShift Prometheus	

Have existing Prometheus in your cluster.

NOTE: Ensure that you have Prometheus in your cluster before this step. We will check the service existence and health status after you click Next.

- Select Prometheus Type.
 - Default type: allows Agent to use KubeConfig credentials to access the Prometheus service. Enter the existing Prometheus service namespace and name to configure the metrics collector.

Create Docker Agent								
✓ Agent Manager	Prometheus Configuration							
✓ Agent Properties	Please enter prometheus service information.							
✓ Credential	Namespace kube-system							
 Metrics Collector 	Name	prometheus-server	0					
 Prometheus Configuration Mode 								
Prometheus Configuration								
• Summary								

- OpenShift Prometheus type: you need to provide OpenShift Route Hostname, Username, and Password for Agent to access the target OpenShift Prometheus.

 Agent Manager 	Prometheus Configura	ation	
Agent Properties		theus uses Route Hostname to access the OpenShift OAuth secu	
Credential	OpenSnift Koute	Hostname, Username and Password for Agent to access the targ	et OpenShift Prometheus.
Metrics Collector	Route Hostname	When // prometheuse its its existent multer default ave, disate	Θ
	OpenShift Username	openshift	0
 Prometheus Configuration Mode 	OpenShift Password	••••••	Θ
Prometheus Configuration			
Summary			
,			

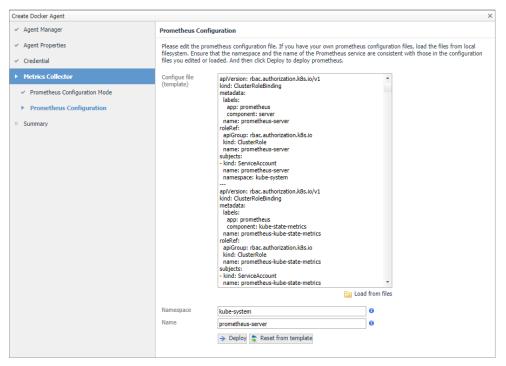
i NOTE: To find the Route Hostname, go to the **OPENSHIFT ORIGIN** dashboard, *Application* > *Routes*.

Your OpenShift Login User should have the privilege to access to the Prometheus.

Do not have existing Prometheus in your cluster.

A *Prometheus Configuration* wizard will appear. To configure the metrics collector, either use the default Prometheus template or upload your own Prometheus deployment .yml files through *Load from files*.

NOTE: Whenever you change the content in Configure file (template), ensure that the Namespace and Name fields are consistent with the Prometheus service configurations in your Configure file (template).
 If you are using the default template, there is no need to change anything.
 For a full version of the default template, see https://github.com/Foglight/Container/tree/master/prometheus



Reset from template: Helps you to reset the Configure file (template) content to the default template.

Deploy: Creates Prometheus components to your cluster with the Configure file. After clicking *Deploy*, a progress message will be displayed.

- If deployed successfully, a succeeded message will be displayed. Close the Validation Result page and then click Next to finish your agent creation process.
- If failed to deploy the Prometheus configuration, a Validation Result page will be displayed with possible solutions.

Heapster metric collector

Enter the existing Heapster service namespace and name to configure the metrics collector.

i IMPORTANT: Deploy the Heapster service to your cluster manually before creating an agent with Heapster as metric collector. Otherwise, connection test to your Heapster service will fail, and you cannot proceed to the next step.

Create Docker Agent	irreate Docker Agent X									
✓ Agent Manager	Heapster Configuration Card									
✓ Agent Properties	Please enter Heapster service information.									
 Credential 	Namespace	kube-system	0							
 Metrics Collector 	Name	heapster	0							
Heapster Configuration Card										
 Summary 										

8 Summary: click Finish.

Agent Manager	Summary		
Agent Properties	Agent Manager	23	
Credential	Cluster Agent Name	openshiftcluster Monitor@openshiftcluster	
Metrics Collector	Kubernetes API Service End Point	http://ouenaid.ini.ini.ini.ini.ini.ini.ini.ini.ini.i	
> Summary	Prometheus Type	OpenShift Prometheus	
Summery	Route Hostname	https://promotive.co.indication.co.	
	OpenShift Username	openshift	
	OpenShift Password	*****	
	Collected Event Level	ABNORMAL	
	Enable Proxy	false	
	Proxy Type	нттр	
	Proxy Server Address	38.6.6.1	
	Proxy Server Port	80	
	Collector Configuration	defaultSchedule	
	Credential	(1.6.6)	
	Lockbox	System	
	New or Existing Credential	New	
	Lockbox Password	The Lockbox is not a password secured Lockbox.	

9 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.

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.
- 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:

Name	Host	Туре	Tags
testagent	and the second statement of the	DockerSwarmAgent	
This agent is currently using prope	erties for DockerSwarmAgent agents.		
🖏 Modify properties for this age	it only.		
🖏 Modify the properties for all D	ockerSwarmAgent agents.		
Configuration			
Name	docker		
Host Name	localhost		
Docker Remote API End Point	THE LOCATION CONTRACTOR		
Swarm			
Swarm Name	default		
Data Collection Scheduler			

- 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.

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 Clusters
 - Monitoring Kubernetes Nodes
 - Monitoring Kubernetes Workloads
 - Monitoring Kubernetes Pods
 - Monitoring Kubernetes Other Components
 - Alarms
 - Capacity Management
 - Cost
 - 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

Kubernetes

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 2. Kubernetes Clusters Summary view

Container Environment								o honoup in		nutes 👻 📔 🔂 Repo
Kubernetes	Swarm (Prev	iew)								Analytics 🔻
Kubernetes		*								
	Configurations	Storage	Load Balan	cer Alarms	Administration					
Monitoring	Configurations	Storage	LUGU Dalali	Cer Alamis i	Administration					
2	7		199	80						
Clusters	Nodes		orkloads	Pods						-
Image: Second	O ▲ ▲ ● 1 1 1 1 1	7 :	 A 9 167 							•
			<u>791</u> 6 91	+ 0 2 02						
ibernetes Clusters Quic									(.	102.1
ubernetes Clusters				Kubernetes Clusters S	Summary				🚠 View Topology	Explore
	Search		् ।	Events						
containeraks1new2 containereks						T₃		Event Sources	Name kubelet	Count 3
Containerens						ļ l				
							containereks			
							Normal			
						+				
				16:15 16:20 16:25	16:30 16:35 16:40 16:45 16	50 16:55 17:00 17:05 17:10 17:15				
				Resource Utilizations						
					Top Cpu U	tilization by Node	т8	Top Memo	ry Utilization by Node	T 28
							4%			14 %
							t_			,,t_o
				16:20	18:25 16:30 16:35 16:40 1 Name		17:10 17:15 Usage •		18:45 18:50 18:55 17:00 17:05 17 me	10 17:15 Usage -
				 ip-082-088-20 	7 212 an ant-2.compute.intern		4.4 %	ip-112 and 12 ac-east-2.compute.intern		27.4 %
				 in 282-268-99 	12 an and 2.compute.internal		3.9 %	 ip-intensity intersection inter	mal	25.4 %
					Top Network Trans	sfer (Bytes) Rate by Node		O Top Dis	k I/O Load by Node	
							I 40			T
							1200			- 8
							1 "			
				16:20	16:25 16:30 16:35 16:40 1	3:46 16:50 16:55 17:00 17:05	t_	16:20 16:25 16:30 16:35 16:40	16:45 16:50 16:55 17:00 17:05 17	10 17:15
					Name	8:46 16:50 16:55 17:00 17:05	t_		18:45 18:50 18:55 17:00 17:05 17 ame	:10 17:16 Usage 🕶
				ip-020-068-00	Name 2020 un-east-2.compute.intern		17:10 17:16 Usage v 38.3 KB/s	N	ame al nvme2n1	Usage + 0.0 c/s
				ip-020-068-00	Name		17:10 17:15 Usage 🕶	N ip-102 \$60.00 02 we east-2.compute.intern ip-1 ast-2.compute.intern	ame al nvme2n1 al nvme1n1	Usage • 0.0 c/s 0.0 c/s
				ip-020-068-00	Name 2020 un-east-2.compute.intern		17:10 17:16 Usage v 38.3 KB/s	N	ame al nvme2n1 al nvme1n1 al nvme0n1	Usage * 0.0 c/s 0.0 c/s 0.0 c/s
				ip-110 100 00	Name 2020 un-east-2.compute.intern		17:10 17:16 Usage v 38.3 KB/s	N ip-100 160 00 00 we sast-2.compute.intern ip-1 sst-2.compute.intern ip-1 sst-2.compute.intern	ame al nvme2n1 al nvme1n1 al nvme0n1	Usage * 0.0 c/s 0.0 c/s 0.0 c/s
				ip-020-068-00	Name - 200east-2.compute.internal ast-2.compute.internal	al	17:10 17:16 Usage v 38.3 KB/s	N ip-103 566 05 vs east-2.compute.inter ip-1 ip-1 ip-1 sst-2.compute.inter ip-1 sst-2.compute.inter ip-1 ip-1	ame al Invme2n1 al Invme1n1 al Invme0n1 rnal Invme0n1	Usage v 0.0 c/s 0.0 c/s 0.0 c/s
				ip-110 100 00	Name	al containereks	17:10 17:16 Usage v 38.3 KB/s	0-10 160.00.00 est-2 compute inter 0-11 versit	ame al nvme2n1 al nvme1n1 al nvme0n1 mal nvme0n1 1.16	Usage v 0.0 c/s 0.0 c/s 0.0 c/s
				ip-110 100 00	Name - 200east-2.compute.internal ast-2.compute.internal	al	17:10 17:16 Usage v 38.3 KB/s	N ip-103 566 05 vs east-2.compute.inter ip-1 ip-1 ip-1 sst-2.compute.inter ip-1 sst-2.compute.inter ip-1 ip-1	ame al Invme2n1 al Invme1n1 al Invme0n1 rnal Invme0n1	Usage - 0.0 c/s 0.0 c/s 0.0 c/s
				ip-110 100 00	Name Name Name Pods	al containereks 21	17:10 17:16 Usage v 38.3 KB/s		ame al[mme2n1 al[mme1n1 al[mme0n1 1.16 2	Usage + 0.0 c/s 0.0 c/s
				ip-110 100 00	Name Pods Deployments	al containerels 21 10	17:10 17:16 Usage v 38.3 KB/s	N p-12: 560-96-02 un-saft-2 compute intern p-1 p-1 saft-2 compute intern p-1 e-p-1 e-saft-2 compute intern p-1 Version Nodes Stateful Sets	ame alivme2n1 alivme1n1 alivme0n1 1.16 2 0	Usage - 0.0 c/s 0.0 c/s 0.0 c/s

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:
 - Top CPU Utilization by Node: shows the nodes that CPU Utilization are top N highest.
 - Top Memory Utilization by Node: shows the nodes that Memory Utilization are top N highest.
 - Top Network Transfer (Bytes) Rate by Node: shows the nodes that Network Transfer (Bytes) Rate are top N highest.
 - Top Disk I/O Load by Node: shows the nodes that Disk I/O Load are top N highest.
 - Q: The icon indicates this metrics is collected by Prometheus metrics collector.
- 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 3. Kubernetes Clusters Explorer view Metrics tab

Container Environment ≻ Kubernetes Cluster: ekscluster		G+ Monday, November 25, 2019 9:42:40 AM - Now 60 minutes	s 👻 📔 Reports 👻
Kubernetes Cluster: ekscluster		Alarms Severity Fatal C Alarms Count	ritical Warning :Ę
Metrics Events			
→ Metric Selector			
Top Cpu Utilization by Node	Į ⁴ _2%	Top Memory Utilization by Node	===] ⁸⁰ 40%
	Metric Selector	×	
09:45 09:50 09:55 10:00 10:05 10:10 10:15 10:20 10:25 Name	Select All Select None Search	10:00 10:05 10:10 10:15 10:20 10:25 10:30 10:3 Name	15 10:40 Usage -
Name	Top Cpu Utilization by Node	2.compute.internal	61.4
ap 383-385-536-93, up and 3 computer internal	<u> </u>	2.compute.internal	52.4
a up 010 010 205 105 up and 3 compute internal	Top Disk I/O Load by Node	-2.compute.internal	32.9
	 Top Disk Read Latency by Node 		
	 Top Disk Write Latency by Node 		
Top Network Transfer (Bytes) Rate by Node	 Top Memory Utilization by Node 	op Network Transfer (Packets) Rate by Node	
TOP NETWORK TRANSFER (Bytes) Rate by Node	 Top Network Transfer (Bytes) Rate by Node 	op Network Transfer (Packets) Rate by Node	T 160
	Top Network Transfer (Dropped Packets) Rate by Noo	de	80 8
	Top Network Transfer (Errors) Rate by Node		For w
09:45 09:50 09:55 10:00 10:05 10:10 10:15 10:20 10:25 10	Top Network Transfer (Packets) Rate by Node	10:00 10:05 10:10 10:15 10:20 10:25 10:30 10:35	10:40
Name		Name	Usage 👻
 ip-232-258-255 as east 2 computerinternal 		-2.compute.internal	151.7 c
go 032-038-024-031 ao east-2 computerinternal		2.compute.internal	138.0 c
Ip 052 018 228 125 up each 2 compute internal		2.compute.internal	122.3 c
	•	•	

- *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.

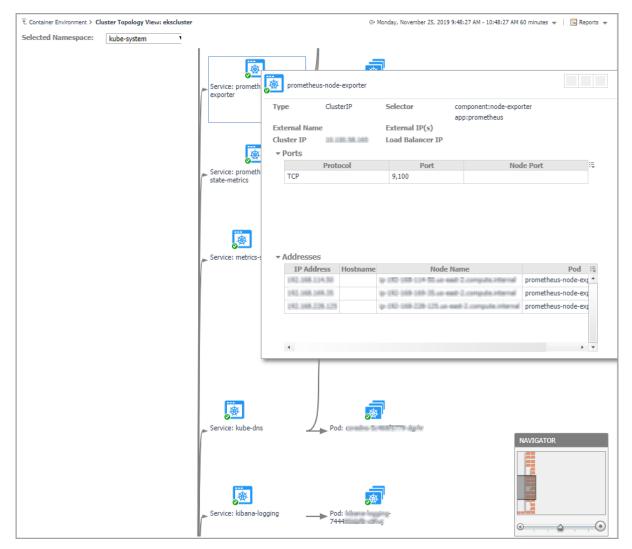
- *Type*: Indicates the severity of the event, including warning and normal.
- **NOTE:** The color in the heatmap indicates the severity of component alarms. Green: indicates normal. Yellow: indicates warning. Orange: indicates critical. Red: indicates fatal.

Figure 4. Kubernetes Clusters Explorer view Events tab

E Container Environment 3	Kubernetes Cluster: /	zurecluster							G+ Frida	y, August 2	, 2019 3:35:52 PM	- Now 60 min	utes 👻	Reports
											Alarms Severity	Fatal	Oritical	Warning ::
	ernetes C	luctor	··· ^ -··								Alarms Count	i atai	Citucal	warning : ;
Metrics Events Block size reflects th Topology Type Service	e count of events whil	e the color s	shows the al	arm sever	rity of the		y object.							
nginx-service	fve	pioneer	ring-s I	kube-dns		alternating-j	nginx	ingress-demo	hello-ngir	IX I	prometheu	promethe	u n	oendpoint
		metrics	s-server I	kilted-uni	сог	simple-depl	nginx-rs3-se	impressive-II	azure-vot	e	my-release	alertma	nager-o	kilte
postgresql	tiller-deploy													
		kubern	etes I	heapster		simple-depl	kubernetes	impressive-II	nslookup	se	cert-manage	kibana-l	og i	alternating.
	prom-prom											elasticse	ear i	azure-vote.
Events														
											Search			,₽ -
Na	me		Namespace		Invo	lved Object	Source	Reaso		6 N.	10			
ALCOHOLD STOLEN	a statute statute and		prometheus				azure-cloud-provider				d from similar e			
and the second	9		prometheus			d	service-controller	CleanupLoadBal		•	d from similar e		-	
and a contract of the second	7		prometheus			ık.	azure-cloud-provider			•	d from similar e			
The contraction of the second	and solution of the party of the		prometheus		-	ık	service-controller	CleanupLoadBal			d from similar e			
The second states			prometheus				azure-cloud-provider			-	d from similar e			
The states out the second			prometheus				service-controller	CleanupLoadBal			d from similar e			
The statement of the state	Contraction of the local distance		prometheus				azure-cloud-provider		-		d from similar e			
the statement statements	week place to be a state of the second	Warning p	prometheus	Service	h.,		service-controller	CleanupLoadBal	ancerFailed	(combine	d from similar e	vents): Erro	r cleaning) up load b

Cluster Topology view

Figure 5. 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 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.



Kubernetes Nodes Quick View				
Kubernetes Nodes	Kubernetes Nodes Summary			Texplore
Search 🔎 🗸	Resource Entitlement			*
	CPU Allocatable	CPU Request and Limit	Hemory Allocatable	Memory Request and Limit
▲ 👩 aks-kafka-18303267-vr	Resource Utilization			
	CPU Utilization	CPU Usage	Memory Utilization	Memory Usage
 ⊗ 		ond Usage Baseline — Request — Limit		2:00 12:10 12:20 12:30 Usage Baseline Request Limit
	11:40 11:45 11:50 11:55 12:00 12:05	rrk IIO (Bytes) Rate 12:0 12:15 12:20 12:25 12:20 12:35 Receive Bytes Rate — Network Transfer Bytes Rate		Filesystem INodes Usage 14 M 10 12:20 12:30 10 12:00 12:00 12:30 10 12:00 10
	O Total	Disk I/O Load	O Total	Disk I/O Latency
	11:40 11:45 11:50 11:55 12:00 12:05	12:10 12:15 12:20 12:25 12:30 12:35 Disk I/O Load	11:40 11:45 11:50 11:55 12:00 12:00 Disk Read	12:10 12:15 12:20 12:25 12:30 12:35 Latency Disk Write Latency
	Summary			
	Name OS Image Capacity	alto consendo a (EEEE)EEF reveal(H0000) Inco: Ubante DE 04.4 L73 attachalte optimised attachalter attachalter optimised attachalter hagenages DEreit hagenages DEreit hagenages DEreit hagenages DEreit hagenages DEreit hagenages DEreit	Closter Architecture Address Allocatable	deans-robbal and/or dei casandre (8302007-remail/8000) after/3000m after/3000m aphrenze di casage - 85°/30002705 happrage 50×0 happrage 50×0 memory = 20050800 memory = 20050800
4	Pod CIDR	13.246.33.0/24	Status	Normal

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 and Limit: Shows the trend of CPU request, limit, and capacity of this node.
 - Memory Request and Limit: 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 percentage of CPU usage divide CPU capacity.

CPU Usage: shows the usage, request, and limit of CPU.

- Memory Utilization: shows the percentage of Memory usage divide Memory capacity.
 - Memory Usage: shows the usage, request and limit of Memory.
- Total Network I/O: shows the sending, receiving, and transferring rate in byte/s, aggregated from all interfaces.

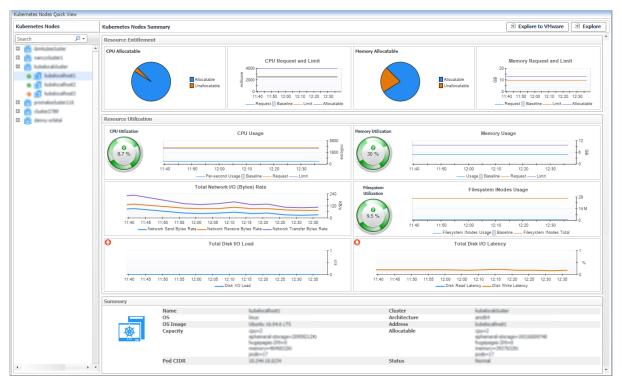
• Filesystem Utilization: shows the filesystem utilization.

Filesystem Inodes Usage: shows the inodes usage and total inodes.

- Total Disk I/O Load: shows the number of IOs in progress per second, aggregated from all disk devices.
- Total Disk I/O Latency: shows the read and write latency in percentage.
- Q: The icon indicates this metrics is collected by Prometheus metrics collector.
- 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.

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.

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 77.

	Kubernetes Node						G+ Saturday, March 14,				Reports
								larms Severity Jarms Count	Fatal	Critical	Warning :
		ue:	-cassandra-183	0.02807-0771					_		
General Metrics	Events										
Name		andra utotto	10.5 committee little	Kubelet Endpo	vint	10,250					
Architecture	andbi	Service Contractor	and an international states and a second states an	Operating Sys		linux					
Kernel Version		TTTT BULLET		Container Run		dischart // 5.6.8					
Kube Proxy Version	w8.01.5			Kubelet Versio		46.05.5					
Boot ID		0.0014-0405-0	1250-30404036a064	Machine ID			hitian2ati (36486/62	48			
Pod CIDR		030 dg/2240		External ID		a manufacture of					
Provider ID	Officialists Affic your	atotalF[2]/emonates Alany/geryweillarsy	Michice 6703-4882-48725- #Groups/mc_orbital-dav-id&_orbital-d Microsoft, Compute/ortualMichines5 # SEXXXXX7 orres/ortualMichines/D	Unschedulable	2	false					
Capacity	kulterri versetti reade or kulterri kalterri fallare fallare fallare fallare fallare fallare fallare fallare fallare fallare	0000 is Juberneties, i fies, iu/rolle- ag larneties, iu/rol profile- manag lomain, bets, iu fies, acure.com fies, iu/an(h- ar	ver-alis cassandra 18000000- ių jagent – mt denos type-Standard, Sris_us ali damotesiai/region-vestus (balandesiai/cane=0 braanditi jūdi damotesiai/cane=0 braanditi jūdi olinus (rinko-agent)	N-		node.alpha.kube	nes-azure-disk=6				
Lapacity	oppert aphana hugapa hugapa	ral storage=33 pm:353=0 pm:376=0 =354035566		Allocatable		cpu=3860m	ge=187150362315 :0 :0				
Status	worma										
Addresses											
Hostname	alo cas	andra usocco	L ² orresolation	InternalIP		38,248,8,34					
Pods											*
Search	P -										15
Alarm	Name	Status	CPU Usage Rate	Memory Usage 🔺	Filesystem Usage	Cluster	Namespao	e Contain	ers Ti	nit Contai	
	perator pronetheue nod		0.9 millicore(s)/s	26.0 MB	40.0 KB	Orbital_Denny	devops-monitorir		1	inc contai	0 *
V Kulhe group it		Running	2.1 millicore(s)/s	32.7 MB	36.0 KB	Orbital_Denny	kube-system	-	1		0
-			2.1 111110010(5//5	32.7 PD	30.0 ND						0
All the sector of the secto		Running				Orbital Denny	opendistro-log		1		

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

₹. Container Environment > Multisensus Multis India India India 2001.2110 annual101000	G• Monday, Novemb	er 25, 2019 9:30:02 AM - Now 60 minutes 👻 📔 Reports 👻
Kubernetes Node:	atalijijitah-orreasijalalala)	Alarms Severity Fatal Critical Warning := Alarms Count
General Metrics Events		
Utilization	CPU Ut	age
	Metric Selector ×	240
	Select All Select None Search	160 0
	CPU Resource	80
09:35 09:40 09:45 09:50 09:55 10:00 10:05 10:10 10:15		10:05 10:10 10:15 10:20 10:25 10:30
CPU Utilization Memory Utilization	Disk Read Latency by Device Disk Write Latency by Device Disk Write Latency by Device	U Limit —— CPU Usage
Memory Usage	Filesystem INodes Utilization by Device Total Network I/C) (Bytes) Rate
	Filesystem Utilization by Device Memory Detailed Usage	
	Memory Resource	
	Memory Usage	- 200 @
	Network Receive (Bytes) Rate by Interface Network Receive (Dropped Packets) Rate by Interface	ţ
09:35 09:40 09:45 09:50 09:55 10:00 10:05 10:10 10:13		10:05 10:10 10:15 10:20 10:25 10:30
Memory Usage Memory Request Memory Lin	n	ve Bytes Rate Network Transfer Bytes Rate

- Events tab: The Events 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

Container Environment > Kubernetes Node				G+ Tuesday, July 2, 20	19 12:51:54	PM - Now (50 minutes 👻 🛛	Reports
				Ala	rms Sever	ity Fa	tal Critical	Warning :
Kubernetes Node:	105-016	in Destatation	475	Ala	arms Coun	t		
Rubernetes Node.	100 110	to tot Hotel		and the second second second				
General Metrics Events								
Events								
					Sea	rch		<u>,</u>
Name	Type 🔺	Namespace	Kind	Involved Object	Source	Reason	Messa	ae
nginx-deployment-7b78fbdd7d-2p85p.15ab663c5c849bb1	Warning	-	Pod	and the same in the same	kubelet	Failed	Error: ImagePu	
nginx-deployment-7b78fbdd7d-k76hw.15ab663a473cbee5	Warning	default	Pod	and induced by Martha 1986	kubelet	Failed	Error: ImagePu	ullBackOff
invalidimage-bb487f87-55xhc.15ab663c5c7a65a3	Warning	test	Pod	training range and	kubelet	Failed	Error: ImagePu	ullBackOff
nginx-deployment-7b78fbdd7d-jwblz.15ab663c5c7e8ede	Warning	default	Pod	and deliverants by Manufilla poly-	kubelet	Failed	Error: ImagePu	ullBackOff
nginx-deployment-7b78fbdd7d-zknhx.15ab663e24cd2052	Warning	default	Pod	and induced in the second	kubelet	Failed	Error: ImagePu	ullBackOff
invalidimage-bb487f87-8dg6l.15ab663cab4506df	Warning	test	Pod	noutrining distance ranges	kubelet	Failed	Error: ImagePu	ullBackOff

Monitoring Kubernetes Workloads

Kubernetes workload is a group of Kubernetes resources. It includes the following Kubernetes resources types: deployment, daemon set, stateful set, replica set, replication controller, cron job, job, and pod. The *Kubernetes Workloads Quick View*, which appears after clicking **Monitoring > Workloads**, shows the data collected about the selected clusters and namespaces. This view consists of the following two panes:

- The Kubernetes Workloads tree view, which appears on the left of Kubernetes Workloads Quick View, lists the workloads existing in the monitored Kubernetes environment. The menu level differs from different workload types, following are some examples of the menu levels:
 - Cluster -> Namespace -> Deployment -> Replica Set -> Pod
 - Cluster -> Namespace -> Cron Job -> Job -> Pod
 - Cluster -> Namespace -> Daemon Set -> Job -> Pod
 - Cluster -> Namespace -> Stateful Set -> Pod
- The Kubernetes Pods Summary view, which appears on the right after you select an individual pod in the **Kubernetes Workloads** tree view.

Kubernetes Workloads Summary view

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

Figure 11. Kubernetes Workloads Summary view

Kubernetes Workloads Quick View											
Kubernetes Workloads Kubernetes Workloads Summary						🖲 Explore					
Search D -	Resource	Resource Utilizations									
Cluster - Ek_Cluster Mansspace - kube-system G coredns G coredns G coredns G coredns G corednsus-kube-state-metrics G corednsus-kube-state-metrics G corentheus-selver G corentheus-selver G corentheus-selver G ave-node G sour-node G corentheus-node-exporter Mansspace - wordress		zation	CPU Useg	16.25 16.35 Request Limit		Memory Usage 14-45 14-55 15:05 15:15 15:25 15:25 Usage Baseline Request Unit Filesystem Usage					
wordpress wordpress-mysql A wordpress-mysql		14:45 14:50 14:55 15:00 15:05 15:15 15:20 15:25 15:20 15:31 15:40 									
	Summary										
		Nam Clus		wordpress-mysql-5c659cd9c6		Namespace	wordpress Replica Set				
		Repl		Eks_Cluster 1		Type Label Selector	Match Labels: pod-template-hash=5c65 tier=mysql app=wordpress				
		Minimum Ready Seconds Status 1 running, 0 waiting			ed, 0 failed						
	Alarms	Alarms i									
	Seventy Time * Alarm Message 3/7/20 3:38 PM The Memory utilization 79.44% of container mysql of pod wordpress-mysql-5c659cd9c5-9mdw in namespace wordpress in cluster Eks_Cluster reaches warning the memory utilization of the m										
	4	8/31/20 11:49 AM	The Memory utilization 79.32%	of container mysql of pod wordpre	ss-mysql-5c659cd9c6-9mxd	hw in namespace wordpress in cluster Ek	cs_Cluster reaches warning thre				

The Kubernetes Workloads Summary view displays the following data:

- **NOTE:** If the selected workload type is a Pod, the metrics values are from the Pod. If the selected workload type is other than a Pod, then the metrics values are the aggregated values from all the related pods of the current workload (e.g. Deployment, Daemon Set, and so on).
 - *Resource Utilizations*: The resource utilization for the selected Kubernetes Workloads over a selected period of time, which includes the following:
 - CPU Utilization: The CPU utilization is calculated as the percentage of CPU usage rate and limit, and it will be unset or blank if the CPU limit is not configured.

CPU Usage: A comparison of per-second usage, request, and limit.

 Memory Utilization: The Memory utilization is calculated as the percentage of memory usage and limit, and it will be unset or blank if the memory limit is not configured.

Memory Usage: A comparison of usage, request, and limit.

- Total Network I/O (Bytes Rate): transferring, sending, and receiving rate in bytes.
- Filesystem Utilization: temporary filesystem utilization.

Filesystem Usage: temporary filesystem reading or writing rate in bytes.

- Summary: Displays the detailed information about the selected Kubernetes workload. The listed information might vary from different types of workload.
- Alarms: Displays the alarms aggregated from the pod and the current workload related to the pod.

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

Workloads Explorer view

The *Workloads Explorer* view opens when you click **Explore** in the Kubernetes Workloads 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 Utilization, CPU Usage and Quota, Memory Usage and Quota, Total Network I/O, Total Filesystem Usage, and Filesystem Utilization by Device are presented by default.
 - **i NOTE:** If the current workload is a Pod, then the metrics values are from the Pod. Otherwise, the metrics values come from aggregated values of the related pods of this workload (e.g. Deployment, Daemon Set).

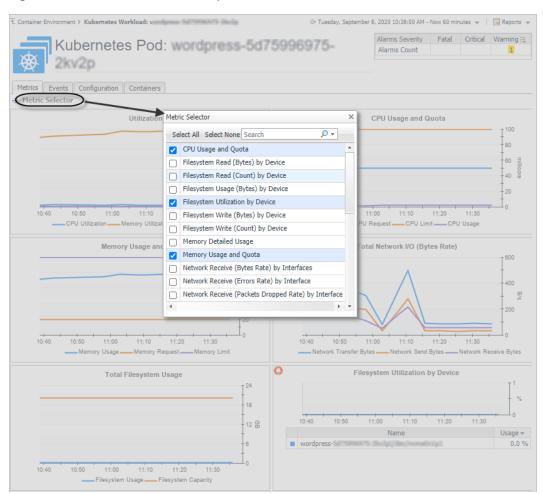


Figure 12. Kubernetes Workloads Explorer view Metrics Tab

- Events tab: The Event tab lists all the events occur on the workloads. It will not aggregate the alarms from
 other related workloads.
 - Name: name of the event.
 - Type: type of the event, Warning or Normal.
 - Namespace: namespace of where this event happens.
 - 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 13. Kubernetes Workloads Explorer view Events tab

Container Environment > Kubernetes Workload: fogli	ght-alarm-service	2					G+ Jul 2, 2020 - Now 1.8 mc	onths 👻 🗎	Reports
Kubernetes Dep	loymen	t: fogligl	ht-alarm-serv	vice			Alarms Severity Fatal Alarms Count	Critical	Warning :Ę <mark>1</mark>
Metrics Events Configuration Pods									
Events									
							Search		,
Name	Type 🔺	Namespace	Involved Object	Source	Reason		Message		
foglight-alarm-service.	Normal	default	foglight-alarm-service	linkerd-proxy-injector	Injected	Linkerd sidecar proxy injected			
foglight-alarm-service.	Normal	default	foglight-alarm-service	deployment-controller	ScalingReplicaSet	Scaled up replica set foglight-alar	m-service inflationity in 2		
foglight-alarm-service.	Normal	default	foglight-alarm-service	deployment-controller	ScalingReplicaSet	Scaled up replica set foglight-alar	m-service dubition to 3		
foglight-alarm-service. How the there the	Normal	default	foglight-alarm-service	deployment-controller	ScalingReplicaSet	Scaled up replica set foglight-alar	m-service dubations to a		_
foglight-alarm-service.	Normal	default	foolight-alarm-service	deployment-controller	ScalingReplicaSet	Scaled down replica set foglight-a	larm-service biliditished to 1		

Foglight for Container Management 7.1.0 User and Administration Guide Using Foglight for Container Management

37

- Configuration tab: The Configuration tab displays the overall information of the selected Kubernetes Workload over a selected period of time. It includes the following tables:
 - Summary: Summary information of this workload.
 - Pod Configuration: Pod related configuration. If the current workload is a pod, it displays the configuration of the pod. Otherwise, it displays the pod template information of the current workload to create related pods.
 - Container Configuration: Including containers configurations and Init-containers configurations. If the current workload is a pod, it displays the configuration of the pod containers. Otherwise, it displays the container template of the pod containers created by this workload.
 - Click ^I to see detailed information on this item.

Figure 14. Kubernetes Workloads Explorer view Configuration Tab

1. Container Environment > Kubernetes Workload: wor	rdpress-half/home.n/th. Beally					G- Thursday, Oct	iber 22, 2020 8:49:01 AM	Now 60 min	nutes 👻 🗎	💽 Reports 👻
Kubernetes Poo	d: wordpress-	73096375-2	1020				Alarms Severity Alarms Count	Fatal	Critical	Warning :Ę
Metrics Events Configuratio	on Containers									
Summary										
Name	ordpress-147100000175-284-28		Namespace	wordpress						
	intainereks		Туре	Pod						
Labels ap	p=wordpress pod-template-hash+it	tier=frontend	Annotations	kubernetes.io/psp=eks.privileged						
Status 1	running, 0 waiting, 0 succeeded, 0	ailed	Node	Ip (32) (68 99 92 up easil 2 com	nulla: Jritarroal					
Pod Configuration										*
Node Selector			Service Account	wordpress-5d75996975-2kv2p						
	efault-scheduler		Affinity	C'						
Restart Policy Ah	ways		Image Pull Secret							
	usterFirst		DNS Config	C ²						
Host Network			Host PID							
Host Aliases			Host IPC							
Hostname			Tolerations	Taint: node.kubernetes.io/not-re Taint: node.kubernetes.io/unrea						
Priority Class			Priority	0						
Preemption Policy			Restart Policy	Always						
Subdomain			Runtime Class Name							
Readiness Gates			Security Context	ď						
Volumes	<u>7</u>									
Container Configuration										-
Container Templates	 Summary 									
wordpress	Name	wordpress								
Init Container Templates	Image Command	wordpress:4.8-apache			Image Pull Policy Args	IfNotPresent				
Init Container Templates	Environment Variables	WORDPRESS_DB_HOST -	> sourchermon		Environment Froms					
		monal								
		WORDPRESS, DR. PROSM								
	Working Directory	Secol name-myndrigen,	Junio - Commission and		TTY					
	Stdin				Termination Message	policy=File				
					,,	path=/dm/harmination.log				
	Ports Lifecycle	wordpress -> TCP/80			Security Context Probes					
	Resources									
	Requests									
	cpu	50m			memory	20M				
		30111			inclusivy	2019				
	Limits									
	cpu	100m			memory	100Mi				
	Volume Devices and Mount	• C								

• *Pods* tab: The *Pods* tab displays the related Pods of the workload. This tab is not displayed if the workload type is a Pod.

Click the Pod name or the 🖻 button will navigate to the related Pod explorer view.

Figure 15. Kubernetes Workloads Explorer view Pods Tab

1. Contain	er Environment > Kubernetes Workload:	8/10/10/0					G+ Wednesday, Se	otember 9, 2020 1	:14:21 PM - No	ow 60 minut	tes 👻 🗌	🖪 Reports 👻
*	Kubernetes Dep	loyme	ent:	sa myaq				Alarms Alarms		Fatal	Critical	Warning :Ę <mark>1</mark>
Metrics	Events Configuration Pods											
Pods												*
Search	₽ •											÷Ę
Alarm	Name	Status	CPU Usage Rate	Memory Usage 🔺	Filesystem Usage		Node	Namespace	Containers	Init Con	tainers I	Explore
<u> </u>	winduren mynaf Saissandaus annahur	Running	0.4 millicore(s)/s	476.8 MB	24.0 KB	Eks_Cluster	ip USD 000 00 02 up each 2 compute internal	wordpress	1		٥(9

Containers tab: The Containers tab displays the related created by this pod. This tab is displayed only when the workload type is a Pod.

Click the Container name or the 🖻 button will navigate to the Container Dashboard.

Figure 16. Kubernetes Workloads Explorer view Containers Tab

1. Container	Environment > Kubernete	Workload:	Anna ang tantakan	81.00L	G+ Wednesday	/, September 9, 2020 2:02:13 PM	Now 60 minute	s 👻 📔 Reports 👻
	Kubernet	es Pod	: wordpress	- municipation	bookdaarda darraadra	Alarms Severity Alarms Count	Fatal C	ritical Warning:Ę 1
\mathfrak{B}				an general second and	Conditional and and a			
Metrics	Events Configuratio	n Containers						
Containe	rs							*
Alarm	Name Status	CPU	U Usage Rate	Memory Usage 🔺	Filesystem Usage	Image		Explore 🗮
A	(mysgl) running	0.4 n	nillicore(s)/s	476.8 MB	24.0 KB	mysql:5.6		

Container Dashboard

• Metrics tab on Container Dashboard

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

Figure 1	17.	Metrics	tab	on	Container	Dashboard
----------	-----	---------	-----	----	-----------	-----------

€ Container Environment ≻ Kubernetes Workload: wordpress	> Kubernetes Container: mysql	G+ Wedness	day, September	r 9, 2020 3:15:15 PM -	Now 60 min	utes 👻 🛛	🖪 Reports 👻
Kubernetes Container: r	nysql			Alarms Severity Alarms Count	Fatal	Critical	Warning :Ę 1
Metrics Configuration							
Utilization	I ^{so}		CPU U	Jsage and Quota			T ⁶⁰
	Metric Selector	×	1				40
	Select All Select None Search	•					- millicor
	CPU Usage and Quota	*	-				- 20
	Filesystem Read (Bytes) by Device						
15:20 15:25 15:30 15:35 15:40 15:45 15:50 15:55	Filesystem Read (Count) by Device		15:35 15:40	15:45 15:50 15:55	16:00 10	8:05 16:10	0 16:15
CPU Utilization — Memory Utilization — File			CPU Request	CPU Limit	CPU Usage		
	Filesystem Utilization by Device						
Memory Usage and Quota	Filesystem Write (Bytes) by Device						
	Filesystem Write (Count) by Device						
	Memory Detailed Usage						
	Memory Usage and Quota						
	Total Filesystem I/O (Bytes)						
	Total Filesystem I/O (Count) Total Filesystem Usage						
	Utilization						
15:20 15:25 15:30 15:35 15:40 15:45 15:50 15:55 1 Memory Usage Memory Request							
memory Usage memory Request me	Memory Limit						

- Configurations tab on Container Dashboard
 - Summary: summary information of this container.
 - Resources: resource request and limit configured for this container.
 - Volume Devices and Mounts: volumes mounted by this container.

Figuro	10	Configurations	tab	on	Containar	Dachboard
rigure	10.	Configurations	เสม	on	Container	Dastibuaru

T. Container Environment > Kuber	netes Workload: ca	> Kubern	etes Container: calico-typha	G+ Tuesday, Novemb	er 10, 2020 1:37:28 PM -	Now 60 min	nutes 👻 🗎	🖪 Reports 👻
Kuberr	netes Containe	r: calico-typh	а		Alarms Severity Alarms Count	Fatal	Critical	Warning :≒
Metrics Configu	ration							
Summary								· ·
Name	calico-typha		Container ID	docker: imanta ma entraita Ma				
Image Command	mcr.micros(# and and all a	NgRevsaa	Image Pull Policy Args	eac44e5u5u5u5u5u5u5u5u5u5u5u5u IfNotPresent				
Environment Variables	KUBERNETES_PORT_443_TC KUBERNETES_PORT_443_TC KUBERNETES_PORT_443_TC KUBERNETES_PORT_443_TC KUBERNETES_SERVICE_HOS TYPHA_HEALTHEMALED -> KUBERNETES_SERVICE_HOS YNPHA_CONNECTIONREEBAL > kubernetes TYPHA_LOGFILEPATH -> nor TYPHA_LOGFILEPATH -> nor	L- _ADDR -> azv true T-> kubernetes NCITNGMODE - none e	Environment Fron	15				
Working Directory Stdin			TTY Termination Mess					
Ports	calico-typha -> TCP/5473 hos	tPort=	Security Context	path=/dev/termination-log				
Lifecycle			Probes	[Liveness Probe] Threshold: Failure=3,Success= Time Seconds: InitialDelay=30 [Readiness Probe] Threshold: Failure=3,Success= Time Seconds: Period=10,Tim	,Period=30,Timeout 1 eout=1	=1		
Status	Is Ready: true Restart Count: 0 State: running Start Time: 2020-10-16 05:41	:52.0						
Resources								-
Volume Devices and Mour	nts							*
Vo Mount		Volume Name Volume Type	calico-multi hikan limitar Secret		un/monto/kubernet mulle tuken brit§r	es.iu/servit	an out	-

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 19. Kubernetes Pods Summary view

Kubernetes Pods Quick View					
Kubernetes Pods	Kubernetes Pods Summary				🖲 Explore
Search Q	Resource Utilizations				
	CPU Utilization C 0.51 %		Filesystem Utilization Filesystem Utilization 0.00 %	Memory Usage	1 14:35
 Image: and the first of two contents of without Image: an and the first of the firs	Summary			Read Bytes Rate Baseline Write	e Bytes Rate
figli dializaardi matte d A figli dializaardi matte 1 O figli dializaardi matte 2 O figli dializaardi matte 2	Name Cluster Node Selector Labels Alarms	elasticsearch-master-0 Jack_Test_Cluster	ne of the second second	Туре	elasticsearch Pod Aks-a on the and the set
	Severity Time Alarm Message 11/2/20 10:26 AM The Memory utilization	94.48% of container elasticsearch of pod el	asticsearch-master-0 in namesp	ace elasticsearch in cluster Jack_Test_Cluste	r reaches fatal thresh

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 Utilization: shows the percentage of CPU usage divides CPU limit, if the limit is configured for this Pod.
 - CPU Usage: shows CPU usage rate, request, and limit, the trend of usage rate, as well as request and limit configuration.
 - Memory Utilization: shows the percentage of Memory usage divides Memory limit, if the limit is configured for this Pod.
 - Memory Usage: shows Memory usage, request, and limit, the trend of usage rate, as well as request and limit configuration.
 - Total Network I/O: shows the sending, receiving, and transferring rate.
 - Filesystem Utilization: shows the Filesystem utilization.
 - Filesystem Usage: shows the read and write rate in byte/s.
- 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. For detailed information for each tabs in Pods Explorer view, see Workloads Explorer view on page 36.

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
- Storage
- Load Balancer

Configurations

Figure 20. Kubernetes Configuration Dashboard

Config Map Secret					
					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-clie
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-5fgt4dhcbf	nancyakscluster	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.

Storage

Figure 21. Kubernetes Storage Dashboard

						S	earch
Alarms	Status	Name	Cluster 🔺	Reclaim Policy	Claim	Storage Class	Source Type
0	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

Figure 22. Kubernetes Load Balancer Dashboard

								Sear	ch	, P +
Alarms	Name	Cluster 🔺	Namespace	Туре	Cluster IP	External IPs	Load Balancer Addresses	Ports	External Traffic Policy	Endpoint
0	fve	eksduster	default	ClusterIP	38.338.338.238	3.118.224,1.76		[TCP:8080, Target .		fve
0	guestbook	eksduster	default	LoadBalancer	13.135.241.74		###79027701547215#99027982588752500-0222572554# ##################################	[TCP:3000, Target .	. Cluster	guestbook
0	kubernetes	eksduster	default	ClusterIP	18.338.61			[TCP:443, Target P.		kubernetes
0	nginx-statefulset	eksduster	default	ClusterIP	None			[TCP:80, Target Po.		nginx-statefulset
0	nginx-stateless	eksduster	default	ClusterIP	None			[TCP:80, Target Po.		nginx-stateless
0	redis-master	eksduster	default	ClusterIP	13.335.44.358			[TCP:6379, Target .		redis-master
0	redis-slave	eksduster	default	ClusterIP	13.138.48.227			[TCP:6379, Target .		redis-slave
0	elasticsearch-logging	eksduster	kube-system	LoadBalancer	13.135.138.40			[TCP:9200, Target .	Cluster	elasticsearch-logging
0	heapster	eksduster	kube-system	ClusterIP	18.038.212.40			[TCP:80, Target Po.		heapster
0	kibana-logging	eksduster	kube-system	LoadBalancer	18.038.211.172			[TCP:5601, Target .	Cluster	kibana-logging
0	kube-dns	eksduster	kube-system	ClusterIP	10.030.0.00			[UDP:53, Target P		kube-dns
0	metrics-server	eksduster	kube-system	ClusterIP	18.138.172.201			[TCP:443, Target P.		metrics-server
0	prometheus-kube-state-metrics	eksduster	kube-system	ClusterIP	18.138.238.81			[TCP:80, Target Po.		prometheus-kube-sta
0	prometheus-node-exporter	eksduster	kube-system	ClusterIP	10.030.58.045			[TCP:9100, Target .		prometheus-node-ex
0	prometheus-pushgateway	eksduster	kube-system	ClusterIP	10.100.15.38			[TCP:9091, Target .		prometheus-pushgat
0	prometheus-server	eksduster	kube-system	ClusterIP	18.138.298.135			[TCP:80, Target Po.		prometheus-server
0	prometheus-server-lb	eksduster	kube-system	LoadBalancer	10.130.71.138		#405b6d0000000saub37e6e779(30000-s000775000c.us-eaut-3.els-amazonave.com	[TCP:80, Target Po.	Cluster	prometheus-server-lb
0	tiller-deploy	eksduster	kube-system	ClusterIP	18.038.024.53			[TCP:44134, Targe.		tiller-deploy
0	dashboard-metrics-scraper	eksduster	kubernetes-dashboard	ClusterIP	18 138 138 227			[TCP:8000, Target .		dashboard-metrics-so

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

Figure 23. Kubernetes Alarms Dashboard

					Age	ents	Clusters	Nodes	Pods	Controllers	Storages	Load Balancers	
									6 10 6	3 2	12		
Se	lect All L	Inselect A	ll Ackr	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 131.2ml	o of pod etcd-kube	eckamaster in namesp	ace kube-system	in cluster localckacluster of	ver threshold
0	5/15/19 1:11 AM	Â	false	6	postgresql- 6558cdf45c- 4s59k	KubePod	Kubernetes Pod Memory	The cpu usage 245.9ml	o of pod postgreso	ql-6558cdf45c-4s59k i	n namespace que	stfve in cluster nancyaksclu	ister over thr
	5/14/19 11:36 PM	8	false	•	fve-app- 76cccb864c- 968z6	KubePod	Kubernetes Pod Memory	The memory utilization	99.32% of pod fv	e-app-76cccb864c-96	8z6 in namespace	e default in cluster localckac	luster reach
	5/14/19 11:36 PM	8	false	8	kube-flannel-ds- amd64-j5n62	KubePod	Kubernetes Pod Memory	The memory utilization 90.00%.	94.75% of pod kı	ube-flannel-ds-amd64	j5n62 in namesp	ace kube-system in cluster l	localcluster1
	5/14/19 11:36 PM	8	false	8	kube-apiserver- kubeckamaster	KubePod	Kubernetes Pod Memory	The memory usage 549	.9mb of pod kube	e-apiserver-kubeckama	aster in namespa	ce kube-system in cluster lo	calckacluste
	5/14/19 11:36 PM	8	false	*	fglam-f7f795b8- 65k2c	KubePod	Kubernetes Pod Memory	The memory usage 868	.2mb of pod fglan	n-f7f795b8-65k2c in r	amespace defaul	t in cluster localckacluster o	ver threshol
	5/14/19 11:36 PM	8	false	*	fve-app- 76cccb864c- 968z6	KubePod	Kubernetes Pod Memory	The memory usage 3.9	gb of pod fve-app	-76cccb864c-968z6 in	namespace defa	ult in cluster localckacluster	over thresh
0	5/14/19 11:36 PM	8	false	•	tqa-loadtest- jmeter-slaves- 768d8c4dc9-sk	KubePod	Kubernetes Pod Memory	The memory usage 100 512.0mb.	3.4mb of pod tqa	-loadtest-jmeter-slave	s-768d8c4dc9-sk	hbk in namespace tqa in clu	ıster localclu
	5/14/19 11:36 PM	٩	false	•	jmeter-operator- 784bd76967- kfyrx	KubePod	Kubernetes Pod Memory	The memory usage 386 256.0mb.	.6mb of pod jmet	er-operator-784bd769	67-kfvrx in name	space kube-system in clust	er localcluste

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.

- **i 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.



🔅 Settings							
Resource Utilization			Recommendation				
Current Capacity	Current Performan	ce	Usage Baseline for Forecasting 30 days				
CPU 6.0 Core(s) Memory 20.4 GB	CPU Usage Rate Memory Usage CPU Request Memory Request	427.1 Millicore(s)/s 5.8 GB 1.7 Core(s) 2.0 GB	Resource Add the following within 30 days High CPU 0 Millicore(s) Memory 0.0 B				
Projected CPU Usage			Projected Memory Usage				
Utilization - المعالية الم معالية المعالية المعالي				Utilization C		¹⁰ ²⁰ ¹⁰ ¹⁰ ¹⁰ ¹⁰ ¹⁰ ¹⁰ ¹⁰	
Projected CPU Request			Projected Memory Request				
Request		i≅ 6 4 K 1 2 0 3 2 0 3 2 0 3 2 0 3 2 0 3 2 0 3 3 2 5 5 5 5 5 5 5 5 5 5 5 5 5	Request Capacity			20 10 B	
Growth Rate Per Week 213.2 Core(s)/s	Time To Ful	140 Days	Growth Rate Per Week 304.9 B Time To Full > 1 Year				

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.

Cost

Foglight for Container Management provide cost management feature for Kubernetes. The *Cost* view appears after clicking **Container > Kubernetes > Cost**. Currently, the Kubernetes costs for AKS and EKS environment are calculated.

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

Prerequisites

Container cost does not collect costs from cloud providers, but uses the cost data collected by cloud agents for parsing the Container environment cost. The cost start date is the first date of the current month.

To use the cost data, ensure the following:

- For AKS cost, an Azure agent with the version 1.9.0 or above is required. The agent should be enabled to collect the inventory data of the AKS cluster resource group and that of the related infrastructure resource group, as well as the subscription cost related to the AKS cluster.
- For EKS cost, an AWS agent with the version 1.9.0 or above is required. The agent should be enabled to collect the regional inventory data related to the EKS cluster and the account cost related to the EKS cluster.
- **NOTE:** Cost metrics should be configured for cloud agents to collect cost data. Refer to the *Cost Tab* section in *Foglight Hybrid Cloud Manager User and Administration Guide* for detailed information.
 - The Kubernetes agent collects the inventory and metrics data. Otherwise, the cost data won't be displayed if there is no Kubernetes data on that day.
 - The clusters have been assigned to BUs. Otherwise, the clusters costs won't be displayed in Cost Dashboard.

Administration dashboard

Administration dashboard enables you to manage the relationships between your cluster and BU, configure budgets at cluster level, and view summarized information about cluster, BU, and cost.

You need to assign cluster to BU here in order to see cost metrics aggregated at different levels in Container Cost dashboards.

Business Units tab

Business Units tab enables you to manage your BU for your Organizations. You can create different BUs to manage your clusters.

Figure 25. Business Units tab

6) Ci	Cost data will not be effected by the selected cluster on above.							
k	Kubernetes Administration							
_	Clusters Business Units							
		Name 🔺	Location	Organization		Clusters		
	1.	Foglight	n/a	Quest Organization		1		
	Rainbow n/a Quest Organization 1							
	1.	Unallocated	n/a	Default Organization		0		

The Business Units tab displays the following information:

- Name: BU name.
- Location: Geographic location of the BU.
- Organization: Organization of this BU.
- Clusters: numbers of the Kubernetes clusters that have been assigned to this BU.
- Add: Add a new Business Unit and assign it to a specific organization.
- Delete: Delete a Business Unit.
- Click the button to edit the information of this Business Unit.
- Assign Organization: click the button to assign Business Unit to another Organization.

Clusters tab

Kubernetes clusters are collected by Kubernetes agents. By default, clusters will not be assigned to any BU and do not have a default monthly budget.

i NOTE: For EKS cluster, Container cost will automatically detect the EKS cluster collected by AWS agent for the cluster. However, if different AWS agent collects the same EKS cluster resources, then you need to assign the AWS account for this cluster.

Figure 26. Clusters tab

Cost data will not be effected by the selected cluster on above.										
Kubernetes Administration										
Clusters Business Units										
	Edit	Name	Business Unit	Platform	Spending	Monthly Budget	Last Month(Oct. 2020)	Month-to-Date(Nov. 2020)	Forecast(Dec. 2020)	Last Collected Date
	1	janh_ningle_vm	-	AKS	•		5 135.34	\$ 0.00	\$ 354.04	2020-10-26 🚯
	1	c ks	Foglight	EKS			\$ 79.94	\$ 35.05	\$ \$3.77	2020-11-06 🚯
	1	JanCluster	Rainbow	AKS	~	6 220.00	6 250 15	6 83.37	6 247.80	2020-11-07 🔞

The Clusters tab displays the following information:

- Name: The name of the Kubernetes cluster.
- Business Unit: The name of the BU.
- *Platform*: AKS, EKS, or On-Prem. If Container cost failed to detect the AKS or ESK cluster, it will display On-Prem by default.
- Spending: The trend of cost spending.
- *Monthly Budget*: Monthly budget, which can be configured through *Set Budget*.
- Last Month (Month. Year): The cost of last month.
- Month-to-Date (Month. Year): The cost of current month.

- Forecast (Month. Year): The cost prediction for next month.
- Last Collected Date: The latest date till when the cost data is collected. It depends on the Last collected time from different platforms.

When mousing over the time, the start date and the end date of container cost collection are displayed.

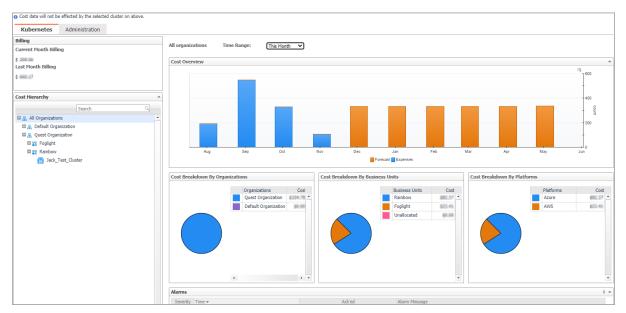
- Set Budget: Set monthly budget for the cluster
- Assign Business Unit: Assign the cluster to a specific BU.
- Remove from Business Unit: Remove the cluster from the selected BU.
- Assign AWS Account: This button will be enabled for editing only when an EKS cluster is selected.
- Click the button to change the monthly budge for the cluster.

Kubernetes dashboard

The *Kubernetes* dashboard displays a *Cost Overview* and several cost breakdown charts. The cost breakdown charts vary when choosing All Organizations, a single organization, a single BU, or a single cluster.

Kubernetes Overview

Figure 27. Kubernetes Overview



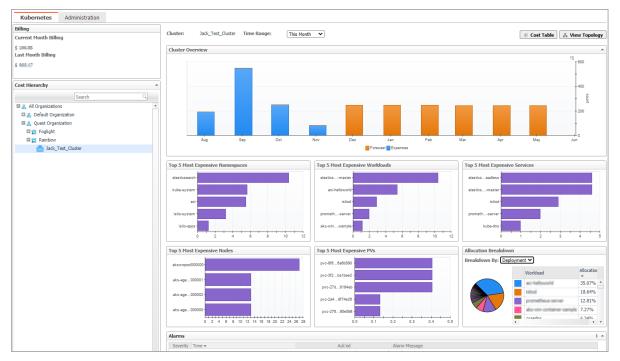
The Kubernetes overview shows the following information:

- *Time Range:* Enables you to change the time range for displaying the cost, including *This Month, Last Month,* or *Last N months.*
- Cost Overview: Monthly cost aggregated from all the clusters and the forecast aggregated cost for the continuing months.
- Cost Breakdown By Organizations: Cost categories by different organizations. Displayed when choosing All Organization.
- Cost Breakdown By Business Units: Cost categories by different BUs cross Organizations. Displayed when choosing All Organization or an organization.
- Cost Breakdown by Platforms: Cost categories by different platforms, such as AKS, EKS, and so on.
- *Most Expensive Clusters:* Displays the top N clusters that costs the most. Displayed when choosing an organization.

- Clusters Cost: Cost of the clusters of this BU. Displayed when choosing a BU.
- Alarms: all the cluster cost alarms. Currently we have over-budget alarm.

Cluster Overview dashboard

Figure 28. Cluster Overview



The Cluster overview dashboard shows the following information:

- *Time Range:* Enables you to change the time range for displaying the cost, including *This Month, Last Month*, or *Last N months*.
- *Cluster Overview*: The monthly cost aggregated from all the clusters of the organization and the forecast aggregated cost for the continuing months.
- Top 5 Most Expensive Namespaces: Displays the top 5 most expensive namespaces whose cost is aggregated from its workloads.
- Top 5 Most Expensive Workloads: Displays the top 5 most expensive workloads whose cost is aggregated from its related pods.
- *Top 5 Most Expensive Services*: Displays the top 5 most expensive services whose cost is aggregated from its related pods.
- Top 5 Most Expensive Nodes: Displays the top 5 most expensive nodes whose cost is collected from Azure or AWS.
- *Top 5 Most Expensive PVs*: Displays the top 5 most expensive persistent volumes whose cost is collected from Azure or AWS.
- Allocation Breakdown: Displays the Allocation Breakdown cost by Deployment or Stateful Set.
- Alarms: Displays all the cluster cost over-budget alarms.
- Cost Table button: Clicking the button will navigate to a Cost table grid layout dashboard.
- View Topology button: Clicking the button will navigate to a *Cluster Topology* View.

Cost Table

The Cost Table lists the detailed cost information calculated by different categories, including Infrastructure, Workload, and Service.

Figure 29. Cost Table

Cluster: Jack_Test_Cluster Time Range: This Month		frastructure ¥ frastructure	🔹 View Topology
Name	1/6-	orkload e Cost	
🍪 kuberne ise antitati teoreti teori e atta di atta zitati at	ContainerAzurePublicIpAddress S	ervice	/subscriptions/ esourceGroups/mc_container
🛞 6eab06 🖓 👘 a Horr a Horr and China and	ContainerAzurePublicIpAddressCo	st \$ (1/81)	/subscriptions/
🍪 kuberne se at the classification of the state of the	ContainerAzurePublicIpAddressCo	st \$ (1.01)	/subscriptions/
🛞 kubernellen alle tolattik och briefa at aafalle "httisefalle	ContainerAzurePublicIpAddressCo	st \$ (8.00)	/subscriptions/
🋞 kuberne instantistatista instantista instantista instanti	ContainerAzurePublicIpAddressCo	st \$ (6.00)	/subscriptions/
🛞 kuberne instant "haddat stadden mad dataan en beterk	ContainerAzurePublicIpAddressCo	st \$ (1.00)	/subscriptions/
le kuberne en ett anstanten i sterne sett met met i sett meter	ContainerAzurePublicIpAddressCo	st \$ (1.00)	/subscriptions/
🛞 kuberne insensionen 🐄 🖓 2001 bei ein ihren Stensenlichten	ContainerAzurePublicIpAddressCo	st \$ (1.00)	/subscriptions/
🛞 e916bcmlatia territti tia weekati akaanni e	ContainerAzureDNSZoneCost	\$ (1.00)	/subscriptions/
🍪 akswnp 💷	ContainerAzureScaleSetCost	\$ 27	/subscriptions/
🛞 akswin;	ContainerAzureScaleSetCost	\$ (1.00)	/subscriptions/
🛞 aks-agentused 200 titlite energy	ContainerAzureScaleSetCost	\$ 220	/subscriptions/
🛞 aks-age-Human 2010 Ministry arman, 1	ContainerAzureScaleSetCost	\$ (1.00)	/subscriptions/
🛞 aks-agentussel 200 titleten anna 2	ContainerAzureScaleSetCost	\$ (1.00)	/subscriptions/
🛞 akswnp 💷 🗄	ContainerAzureScaleSetCost	\$ (1.00)	/subscriptions/
🔕 aks-age-filosof 200 titlet anna 1	ContainerAzureScaleSetCost	\$ (1.00)	/subscriptions/
🔕 kubernetesi divramia gwa dikifizikia ikifa milifa aadib inita adadami	ContainerAzureDiskCost	\$ (2.40)	/subscriptions/
🔕 kuberneten Avramic over 30:42:500 Sathe High 12:5: 3:07/91a21aac2	ContainerAzureDiskCost	\$ (2.40)	/subscriptions/
🔕 kuberneties dynamic gwy mittlads i hyfu is tig arlads 525 mitiliatadia	ContainerAzureDiskCost	\$ (5.00)	/subscriptions/
🔕 kubernetissi divramisi gwa effedili "witi 523" 475" ana la 2002lia da 2003	ContainerAzureDiskCost	\$ (5.00)	/subscriptions/
🔕 kubernetten Avramin pvo 1504 (5075-5342) entiti da ab 1982-halizz haf	ContainerAzureDiskCost	\$ (1.04)	/subscriptions/
🔕 kuberneties denomic ges (1006,755,775) ett (b.a.(55)/213,585,251)	ContainerAzureDiskCost	\$ (5.04)	/subscriptions/ esourceGroups/MC_CONTAIL
🔕 kuberneties deramic ges 25/254525 is 25 4548 auto 7386208. brudy	ContainerAzureDiskCost	\$ (2.40)	/subscriptions/
6 f245efdmt 11 attacket 11	ContainerAzureStorageAccountCos	t \$ 0.00	/subscriptions/
(a) f245efd	ContainerAzureStorageAccountCos	+ < 8.13	/subscriptions/ esourceGroups/mc containe

- Infrastructure: Lists the Azure or AWS costs collected.
- Workload: The calculated workload cost is aggregated from its related pods. The workload types include deployment, statefulset, daemonset, and so on.
- Service: The service cost includes related workload and load balancer costs in AWS.

View Topology

Click View Topology button to open the Cluster Topology View.

Figure	30.	Cluster	Topology	View
--------	-----	---------	----------	------

€ Container Environment > Cluster Top	ology View			Nov 10, 2020 11:37:12 A	M CST 🔝 Reports 🧃
		Cluster		-	• •
EC2 Instance	EC2 Instance	Load Balancer	Load Balancer	Load Balancer	
ip \$ 5.6 Pods: 14	ip \$ 5.4 Pods: 13	\$ 3.0	arn:aws:elastic \$ 3.0	arn:aws:elastic \$ 2.7	

Clicking virtual machine, a popup view will be displayed to show the pods cost which run on this node and also the persistent volume that used by some pod.

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 31. Kubernetes Optimizer Dashboard

annes contenues	IEEnew2	·							
Monitoring (Configurations Sto	rage Load	Balancer Alarms	Capa	city Management	Optimizer C	Cost	Administration	
								📀 Settings	
VM Resizing U	Potentia	al Zombies							
Exclude earch	🔲 Show Exclud	led Items 0							
Name 🔺	Namespace	Type	CPU Usage	Memory	Network Transfer	File System Transfe		Recommendation	
) aks hellowoodd	aci	Deployment	0.2 Millicore(s)/s	45.5 MB	0.0 KB/s	40.0 KB	D	elete Deployment aks-helloworld in namespace aci.	
aks hellowedd on							D		
	aci ingress-basic	Deployment	0.2 Millicore(s)/s	45.5 MB	0.0 KB/s	40.0 KB	D	elete Deployment aks-helloworld in namespace aci.	
aks helioworld-one	aci ingress-basic	Deployment Deployment	0.2 Millicore(s)/s 0.2 Millicore(s)/s	45.5 MB 46.0 MB	0.0 KB/s 0.0 KB/s	40.0 KB 40.0 KB	D D D	velete Deployment aks-helloworld in namespace aci. Delete Deployment aks-helloworld-one in namespace ingress-basic.	
aks fail work for	aci ingress-basic ingress-basic	Deployment Deployment Deployment	0.2 Millicore(s)/s 0.2 Millicore(s)/s 0.2 Millicore(s)/s	45.5 MB 46.0 MB 37.3 MB	0.0 KB/s 0.0 KB/s 0.0 KB/s	40.0 KB 40.0 KB 40.0 KB	D D D D	velete Deployment aks-helloworld in namespace aci. velete Deployment aks-helloworld-one in namespace ingress-basic. velete Deployment aks-helloworld-two in namespace ingress-basic.	
aks aks det	aci ingress-basic ingress-basic istio-apps	Deployment Deployment Deployment Deployment	0.2 Millicore(s)/s 0.2 Millicore(s)/s 0.2 Millicore(s)/s 4.2 Millicore(s)/s	45.5 MB 46.0 MB 37.3 MB 82.2 MB	0.0 KB/s 0.0 KB/s 0.0 KB/s 2.7 KB/s	40.0 KB 40.0 KB 40.0 KB 40.0 KB	D D D D D	velete Deployment aks-helloworld in namespace aci. velete Deployment aks-helloworld-one in namespace ingress-basic. velete Deployment aks-helloworld-two in namespace ingress-basic. velete Deployment details-v1 in namespace istio-apps.	
) aks) aks) det) gra	aci ingress-basic ingress-basic istio-apps istio-system istio-system	Deployment Deployment Deployment Deployment Deployment	0.2 Millicore(s)/s 0.2 Millicore(s)/s 0.2 Millicore(s)/s 4.2 Millicore(s)/s 1.7 Millicore(s)/s	45.5 MB 46.0 MB 37.3 MB 82.2 MB 34.8 MB	0.0 KB/s 0.0 KB/s 0.0 KB/s 2.7 KB/s 130.9 B/s	40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB	D D D D D D D	velete Deployment als-helloworld in namespace aci. Delete Deployment als-helloworld-one in namespace ingress-basic. Velete Deployment als-helloworld-two in namespace ingress-basic. Delete Deployment delails-V in namespace istio-apps. Velete Deployment grafana in namespace istio-system.	
) aks aks) det) gra) isti	aci ingress-basic ingress-basic istio-apps istio-system istio-system	Deployment Deployment Deployment Deployment Deployment Deployment	0.2 Millicore(s)/s 0.2 Millicore(s)/s 0.2 Millicore(s)/s 4.2 Millicore(s)/s 1.7 Millicore(s)/s 7.0 Millicore(s)/s	45.5 MB 46.0 MB 37.3 MB 82.2 MB 34.8 MB 88.3 MB	0.0 KB/s 0.0 KB/s 0.0 KB/s 2.7 KB/s 130.9 B/s 5.2 KB/s	40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB		velete Deployment aks-helloworld in namespace aci. Velete Deployment aks-helloworld-two in namespace ingress-basic. Velete Deployment aks-helloworld-two in namespace ingress-basic. Velete Deployment details-v1 in namespace istio-apps. Velete Deployment istiod in namespace istio-system. Velete Deployment istiod in namespace istio-system.	
) aks) aks) det) gra) istic	aci ingress-basic ingress-basic istio-apps istio-system istio-system istio-system	Deployment Deployment Deployment Deployment Deployment Deployment Deployment	0.2 Millicore(s)/s 0.2 Millicore(s)/s 0.2 Millicore(s)/s 4.2 Millicore(s)/s 1.7 Millicore(s)/s 7.0 Millicore(s)/s 5.4 Millicore(s)/s	45.5 MB 46.0 MB 37.3 MB 82.2 MB 34.8 MB 88.3 MB 68.5 MB	0.0 KB/s 0.0 KB/s 2.7 KB/s 130.9 B/s 5.2 KB/s 5.4 KB/s	40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB	D D D D D D D D D D D	velete Deployment aks-helloworld in namespace aci. velete Deployment aks-helloworld-one in namespace ingress-basic. velete Deployment aks-helloworld-two in namespace ingress-basic. velete Deployment grafina in namespace istio-apps. velete Deployment istoo in namespace istio-system. velete Deployment istoo in namespace istio-system. velete Deployment istoo-ingressgateway in namespace istio-system.	
aks aks det isti isti ngin	aci ingress-basic istio-apps istio-system istio-system istio-system rwmpvc	Deployment Deployment Deployment Deployment Deployment Deployment Deployment Pod	0.2 Millicore(s)/s 0.2 Millicore(s)/s 0.2 Millicore(s)/s 4.2 Millicore(s)/s 1.7 Millicore(s)/s 7.0 Millicore(s)/s 5.4 Millicore(s)/s 0 Millicore(s)/s	45.5 MB 46.0 MB 37.3 MB 82.2 MB 34.8 MB 88.3 MB 68.5 MB 2.5 MB	0.0 KB/s 0.0 KB/s 0.0 KB/s 2.7 KB/s 130.9 B/s 5.2 KB/s 5.4 KB/s 0.0 KB/s	40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB		belete Deployment aks-helloworld in namespace aci. belete Deployment aks-helloworld-one in namespace ingress-basic. belete Deployment aks-helloworld-two in namespace ingress-basic. belete Deployment details-v1 in namespace istio-apps. belete Deployment grafiana in namespace istio-system. belete Deployment istio-ingressgatevay in namespace istio-system. belete Deployment istio-ingressgatevay in namespace istio-system. belete Pod nginx1 in namespace rympyc.	
) aks) aks) aks) det) gra) isti) isti) ngi) ngi	aci ingress-basic ingress-basic istio-apps istio-system istio-system rwmpvc nvmpvc	Deployment Deployment Deployment Deployment Deployment Deployment Pod Pod	0.2 Millicore(s)/s 0.2 Millicore(s)/s 0.2 Millicore(s)/s 1.7 Millicore(s)/s 1.7 Millicore(s)/s 5.4 Millicore(s)/s 0 Millicore(s)/s 0 Millicore(s)/s	45.5 MB 46.0 MB 37.3 MB 82.2 MB 34.8 MB 88.3 MB 68.5 MB 2.5 MB 2.5 MB	0.0 KB/s 0.0 KB/s 0.0 KB/s 2.7 KB/s 130.9 B/s 5.2 KB/s 5.4 KB/s 0.0 KB/s 0.0 KB/s	40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB 40.0 KB	D D D D D D D D D D D D D D D	elete Deployment als-helloworld in namespace aci. elete Deployment als-helloworld-one in namespace ingress-basic. elete Deployment als-helloworld-two in namespace ingress-basic. elete Deployment defails-vi In namespace istio-system. elete Deployment istod in namespace istio-system. elete Deployment isto-ingressgateway in namespace listo-system. elete Deployment isto-ingressgateway in namespace listo-system. elete Pod nginx2 in namespace rympyc.	

The Optimizer view includes the following elements:

- 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 51.
- 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.
- **i** 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 Excluded tab on page 53.
- 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 32. Configuration tab

Settings Dialog Configuration Waste These settings are for CPU, Memory and	
These settings are for CPU, Memory and	Storage Optimization.
Thresholds	
CPU Memory	Storage
Warning: 75% Critical: 83% Warning: 85% Critical:	l: 90% Warning: 90% Critical: 95%
Recommendation Calcu	
Resource CPU I	Memory Storage
Reserve Margin 5 %	5 %
Acceptable Variation 3 % 50 MHz 3	% 50 MB 3 % 1024 MB
Recommended Basis Maximum Peak Utilization Maximum	n Peak Utilization 🔻 🛛 Maximum Peak Utilization
Peak analysis period: 15 minute(s)	Threshold for merging peaks: 5%
Evaluate calculation over this period of time $\boxed{30}$ Day(s)	History 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 33. Waste tab

Settings		×
Configuration	Waste Excluded These settings are for Unused Resources and Potential Zombies	
Determine as wa	iste if :	
	Resource has been created 1 T Days	
	Persistent Volume Status 🛛 🖌 Available	
	Released	
	Failed	
Determine as a p	potential zombie if :	
	Time period used for average calculation is 7 🔻 Days	
	Average resource utilization	
	100.0 Millicore/s for CPU 100.0 KB/s for Network	
	100.0 MB for Memory 100.0 MB for Filesystem	
	Excluded Namespace	
	Save	Cancel

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 34. Excluded tab

Settings Dialog			×
Configuration Waste	Excluded Credentials	s Constraints	
сри	Remove		Ę
	Name	Type KubeDeployment	
Memory		Kubebeployment	
Storage			
Unused Resources			
Potential Zombies			
		Save	Cancel

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 35. Credentials tab

Settings Dialog					×
Configuration	Waste	Excluded	Credentials	Constraints	
Configuration	waste	Excluded	Credentials	Constraints	
🗿 Add a New Cr	edential Group	Remove Credential Gr	roups	Search	<i>p</i> -
	Name 🔺			Credentials	
🗉 🔲 🙀 Optimizes	Storage-example		Administrator@	1.00.000	2
					Save Cancel
					Jave Calice

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 36. Constraints tab

Settings Dialog									×
÷,					-	*			
Configuration	Waste	Excluded	Credent	tials	Con	straints			
🚱 Add a New Co	onstraint Group	Remove Constraint G	Groups		Searc	:h		۶ - 🔍	
	Name 🔺			Max /CPU	Min Memory	Max Memory	Min Storage	Max Storage	
	Use the	above Add icon to add	d one or more	Crede	ntial Group	s.			
							S	ave Car	ncel

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 37. Kubernetes Administration Dashboard

Kubernetes	Swarm (Preview)									An	alytics 🔻
Kubernetes	~										
Monitoring Configurations 5	Storage Load Balancer Alarms Admin	istration									
	ector is marked as Deprecated. Support for He to the new Prometheus metrics collector.	eapster met	trics collector will be	removed ir	n the future release	s. Users are					
Tasks:											
Create Agent	etheus										
5											
Agents	te 🕡 Deactivate 🐌 Start Data Collection 🚪	Stop Data	a Collection 🍚 Del	ete 👚 Upd	late Agent				arch		<i>p</i> •
Agents	te ① Deactivate Deactivate Start Data Collection	Stop Data	a Collection 🤤 Del Data Collection	ete 👚 Upo Alarms	date Agent Download Log	Agent Version	Туре	Sez Metrics Collect Status	tor	Deploy	₽ • Properties
Agents Add SRefresh U Activa Agent Name A						Agent Version	Type Prometheus	Metrics Collect	tor	Deploy	
Agents Add SRefresh & Activa Agent Name A	Foglight Agent Manager Host	Active	Data Collection	Alarms	Download Log	-		Metrics Collect Status	tor	Deploy	Properties
Agents Add SRefresh & Activa Agent Name A	Foglight Agent Manager Host	Active	Data Collection	Alarms	Download Log	38.0	Prometheus	Metrics Collect Status	tor Migrate	Deploy	Properties
Agents Add Schefresh Charter Agent Name A Agent Name A Agent Name Agent Name Agent Name Agent Schutze	Foglight Agent Manager Host	Active &	Data Collection	Alarms	Download Log	 ☑ 3.8.8 ☑ 3.8.8 	Prometheus Heapster	Metrics Collect Status Healthy Healthy	tor Migrate	Deploy	Properties
Agents Add Schefresh C Activa Agent Name A Agent Name	Foglight Agent Manager Host	Active & & &	Data Collection	Alarms	Download Log	 3.8.8 3.8.8 3.8.8 	Prometheus Heapster Prometheus	Metrics Collect Status Healthy Healthy Healthy Healthy	tor Migrate	Deploy	Properties

- 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.
- **i IMPORTANT:** Heapster metrics collector is marked as Deprecated. Support for Heapster metrics collector will be removed in the future release. Users are encouraged to switch to the new Prometheus metrics collector.

The *Administration* dashboard supports new agent creation and existing agents management. It contains the following features:

- Create Agent task
- Remove Prometheus task
- Agents table

Create Agent task

Use *Create Agent* or the *Add* button to start a wizard to create a new agent. See Creating and Activating a Kubernetes Agent on page 19 for more information.

Remove Prometheus task

Remove Prometheus will start a wizard to remove the Prometheus successfully deployed through our platform.

i NOTE: Prometheus that are not deployed through our platform are not listed here.

You can remove Prometheus deployed from platform through this wizard. You can select Prometheus from multiple dusters in the following tables and dick remove button to remove them all. Agent Name * Metrics Collector Agent Name * Type Status Prometheus Prometheus Healthy	Remove Prometheus		X
Agent Name A Type Status	You can remove Prometheus deployed from platform t following tables and click remove button to remove the	hrough this wizard. You can select em all.	Prometheus from multiple dusters in the
Type Status	Agant Nama	M	etrics Collector
Prometheus Realthy			Status
	muniturEilenidu(Luter	Prometheus	Healthy
Remove			Remove

Select the Prometheus you want to remove and click Remove.

NOTE: All the related Kubernetes components will also be removed according to the template that you used to deploy the Prometheus through our platform.

If the Prometheus service is deleted successfully, a result message will be display. Otherwise, the *Remove Prometheus* wizard will appear again with error messages to guide you with further operations. Follow the messages and delete them again later.

Agents table

Use Activate, Deactivate, Start Data Collection, Stop Data Collection, Delete, and Update Agent to manage the agent.

Metrics Collector

- Type: the type of Metrics Collector, supports Heapster, Prometheus, or OpenShift Prometheus.
- Status:
 - Healthy: discovered the Kubernetes service of the Metrics Collector and the result for the health check of the service is successful.
 - Unhealthy: discovered the Kubernetes service of the Metrics Collector, however, the result for the health check of the service is failed.
 - Discover failed: failed to discover the Kubernetes service in your cluster. The Deploy 🖾 icon is enabled.
 - · Waiting for data update: waiting for status update after performing some operations for Metrics Collector.
 - Failed to update status: connection failed or other known issues. Contact the support.
- Migrate ↔: start a wizard to migrate Heapster to Prometheus Metrics Collector.

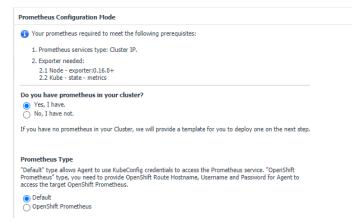
If the agent version is 3.0.0 and is using Heapster as the metric collector, you can Migrate from Heapster to Prometheus metrics collector.

Deploy I : start a wizard to configure or guide to deploy Prometheus to your cluster.

If our platform failed to discover Prometheus in your cluster and the Deploy 🖾 icon is enabled.

Migrate or Deploy process

Clicking Migrate D or Deploy Z will launch the Configure Prometheus Metrics Collector Wizard.



- Have existing Prometheus in your cluster.
- **NOTE:** Ensure that you have Prometheus in your cluster before this step. We will check the service existence and health status after you click Next.
 - Select the Prometheus Type.
 - Default type

Allows Agent to use KubeConfig credentials to access the Prometheus service. Enter the existing Prometheus service namespace and name to configure the metrics collector.

Prometheus Co	Prometheus Configuration						
Please enter pror	netheus service information.						
Namespace	kube-system	0					
Name	prometheus-server	0					

 OpenShift Prometheus type: you need to provide OpenShift Route Hostname, Username, and Password for Agent to access the target OpenShift Prometheus.

	theus uses Route Hostname to access the OpenShift OAuth secured Hostname, Username and Password for Agent to access the target C	
Route Hostname	When // prometheue-itable-existen, mater-definall, avr. diable	0
OpenShift Username	openshift	0
OpenShift Password		0

i NOTE: To find the Route Hostname, go to the OPENSHIFT ORIGIN dashboard, Application > Routes.

Your OpenShift Login User should have the privilege to access to the Prometheus.

Do not have existing Prometheus in your cluster.

A *Prometheus Configuration* wizard will appear. To configure the metrics collector, either use the default Prometheus template or upload your own Prometheus deployment .yml files through *Load from files*.

NOTE: Whenever you change the content in Configure file (template), ensure that the *Namespace* and *Name* fields are consistent with the Prometheus service configurations in your Configure file (template). If you are using the default template, there is need to change anything.

filesystem. Ensure	ometheus configuration file. If you have your own pro that the namespace and the name of the Prometheu loaded. And then click Deploy to deploy prometheus.	s service are consistent with those in th	
Configue file (template)	aplVersion: rbac.authorization.k8s.io/v1 kind: ClusterRoleBinding metadata: app: prometheus component: server name: prometheus-server roleRef: aplGroup: rbac.authorization.k8s.io kind: ClusterRole name: prometheus-server subjects: - kind: ServiceAccount name: prometheus-server namespace: kube-stare- metadata: labels: app: prometheus component: kube-state-metrics name: prometheus-kube-state-metrics name: prometheus-kube-state-metrics name: prometheus-kube-state-metrics subjects: - kind: ServiceAccount name: prometheus-kube-state-metrics subjects: - kind: ServiceAccount name: prometheus-kube-state-metrics - subjects: - kind: ServiceAccount name: prometheus-kube-state-metrics	► Load from files	
Namespace	kube-system	0	

Reset from template: Helps you to reset the Configure file (template) content to the default template.

Deploy: Creates Prometheus components to your cluster with the Configure file. After clicking *Deploy*, a progress message will be displayed.

• If deployed successfully, a succeeded message will be displayed. Close the *Validation Result* page and then click **Next** to finish your agent creation process.

• If failed to deploy the Prometheus configuration, a *Validation Result* page will be displayed with possible solutions.

Agent Edit properties

Click *in* Properties column of the Agents table to edit the property of the agent.

• For agent using Heapster as metric collector, a wizard similar as below will be displayed. Update the agent properties and save the changes. A new data collection process will be initiated.

Kubernetes Agent [Monitor]: Edit Properties Cluster Name *: 2789Cluster Kubernetes API Service End Point *:			
Kubernetes API Service End Point * : Imput: dimmage: and quest any time Imput: dimmage: and quest any time Collected Event Level *: Imput: dimmage: and quest any time Imput: dimmage: and quest any time Metrics Collector *: Heapster Service Name Imput: dimmage: and quest any time Proxy Enable Proxy	Kubernetes Agent [Monitor	r]: Edit Properties	×
Collected Event Level *: Alt ABNORMAL Ametrics Collector *: Heapster Service Name heapster Proxy Enable Proxy	Cluster Name * :	2789Cluster	0
Metrics Collector *: Heapster Service Name heapster • Proxy Enable Proxy •	Kubernetes API Service End Point * :	Https:///domps2.prod.gum8.com@	#© 0
Service Namespace kube-system • Service Name heapster •	Collected Event Level *:	ALL ABNORMAL	0
Proxy Enable Proxy 3	Metrics Collector *:	Heapster	
Proxy Enable Proxy		Service Namespace kube-system	0
		Service Name heapster	0
Save	Proxy	Enable Proxy	0
Save			
Save			
Save			
Save Canc			
			Save Cancel

 For agent using Prometheus as metric collector and the Prometheus is successfully deployed through our platform, a wizard similar as below will be displayed.

Kubernetes Agent [Monitor and the second	r]: Edit Properties					
Cluster Name * :	ibmk8scluster	ibmk8scluster				
Kubernetes API Service End Point $*$:	https://at.houtt2.com	teinen dauf. Um com 20057	0			
Collected Event Level *:	ALL ABNOR	ALL ABNORMAL				
Metrics Collector *:	Prometheus	Change to Heapster	0			
	Service Namespace	kube-system				
	Service Name	prometheus-server				
	Config File	Export				
Proxy	Enable Proxy		0			
			Save Cancel			

i NOTE: If the Prometheus is deployed through our platform, the Service Namespace and Service Name cannot be updated through *Kubernetes Agent Edit Properties wizard*. You can use *Remove Prometheus* to remove Prometheus and deploy a new one.

Export: export the deployed .yml file of the Prometheus. *Change to Heapster*: change from Prometheus Metrics Collector to Heapster. However, it is not recommended. • For agent using existing Prometheus as Metrics Collector, a wizard similar as below will be displayed.

👸 Kubernetes Agent [eks]: Edit Properties			×
Cluster Name * :	Ekscluster		0
Kubernetes API Service End Point * :	Https://withitematic	COLONESSES ADVOLTMAN AND ADVE	0
Collected Event Level *:	ALL O ABNORMA	AL	0
Metrics Collector *:	Prometheus	Change to Heapster	0
	Service Namespace *	kube-system	0
	Service Name *	prometheus-server	0
Proxy	Enable Proxy		0

- **NOTE:** If you are using your existing Prometheus as Metrics Collector, we will not help you to manage your Prometheus. Both the Service Namespace and Service Name can be updated in *Kubernetes Agent Edit Properties* wizard.
- For agent using OpenShift Prometheus as Metrics Collector, a wizard similar as below will be displayed.

Kubernetes Agent [Monitor@akscluster]: Edit Properties							
Cluster Name *:	aksduster	0					
Kubernetes API Service End Point *:	https://containeralia-	Die Chiel 201 Aus werte ward werte	0				
Collected Event Level *:		IAL	0				
Metrics Collector *:	Prometheus	Change to Heapster	0				
	Route Hostname	When // prometheus italian autient] 0				
	OpenShift Username	openshift	0				
	OpenShift Password	•••••] 🛛				
Proxy	Enable Proxy		0				
			Save Cancel				

59

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.

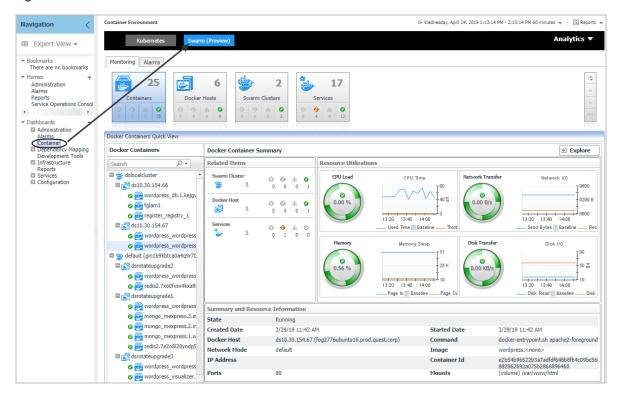


Figure 38. Docker Swarm Dashboard

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.

ontainer Environment		(+ Wednesday, April 24, 2019 1:13	:14 PM - 2:13:14 PM 60 minutes 👻 📔 Report
Kubernetes Swarm	ı (Preview)			Analytics v
Containers				
ocker Containers Quick View	Docker Container Summary			Explore
Search 🔎 🗸	Related Items	Resource Utilizations		
desocalcluster desocalc	Swarm Cluster ∅	Used Time 8 Memory Memory 5 0.56 %	80 40 5 14:00 asseline Throt	Vs Vs 13.20 13.40 14.00 Send Bytes Baseline Re Sfer Disk I/O
mongo_mexpress.3.e	Summary and Resource Information			
🖉 👼 mongo_mexpress.2.in	State Running Created Date 3/29/19 11:42 AM	4	Started Date	3/29/19 11:42 AM
📀 👼 mongo_mexpress.1.w		fog2776ubuntu16.prod.quest.corp)	Command	docker-entrypoint.sh apache2-foregrou
🛛 👼 redis2.7e2o8l20yndp5	Network Mode default	-	Image	wordpress: <none></none>
dsrotateupgrade3	IP Address		Container Id	e2b54b9b522b3a7adfdf648b8fb4c09bc
wordpress_wordpress wordpress_visualizer.	Ports 80		Mounts	882862692a075b2866896460 (volume) /var/www/html

Figure 39. 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 79.

Figure	40 .	Docker	Container	Explorer	view	Monitoring	Tab

Monitoring				General Design Help
Summary and Resource Inf	ormation		A A	Properties
State	Running			Bookmark
Created Date	4/3/19 3:47 AM	Started Date	4/3/19 3:47	✓ Other Actions New window
Docker Host	localdshost67	Container Id	2fadf74a87d	Create dashboard
Image	wordpress: <none></none>	Command	docker-entry	Reports
Network Mode	default	IP Address		▼ Metric Selector
Ports	80	Mounts	(volume) /va	Select All Select None Search 🔎 🗸
Environment Variables	WORDPRESS_DB_HOST=db:3306 WORDPRESS_DB_MSSVDR-wordpress WORDPRESS_DB_VSER-wordpress PATH=/usr/local/bini/usr/ /sbini/usr/bini/bin PHPIZE_DEPS=autocnf dpkg-dev file g++ gcc libc-dev make pkg-config ra2c PHP_IIII_DIR=/usr/local/etc/php APACHE_CONFIDR=/etc/apache2/ APACHE_ENVARS=/etc/apache2/envars PHP_ESTRA_BUILD_DEPS=apache2-dev PHP_ESTRA_BUILD_DEPS=apache2-dev PHP_CFLAGS=fstack-protector-strong -fpic -fpie-02 PHP_CFLAGS=fstack-protector-strong -fpic -fpie-02 PHP_CFLAGS=fstack-fstack-protector-strong -fpic -fpie-02 PHP_CFLAGS=fstack-fstack-fstack-fstack-fs	Labels	com.docker. com.docker. com.docker. com.docker. com.docker. com.docker. dortes.2.vgr	Throttled Time CPU Time Used CPU Utilization Memory Consumed Memory Swap Memory Utilization Network Bytes Network Bytes Network Packets Network Packets Disk Bytes Disk Bytes Disk Transfer Bytes Themes Application Monitoring
Swarm Information	88906804C012192			
Swarm Cluster	localdscluster (w120ohdn6fy27msxhonwmgf24)	Swarm Service	wordpress_v	
5warm Node	fog2776ubuntu16 (avmi06px91fzcsv3uztyk3ici)			
Resource Management			•	
CPL	Utilization Me	emory 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.

Figure 41. Docker Host Summary view

ntainer Environment		G+ Wednesday, April 24, 2019 1:23:16	PM - 2:23:16 PM 60 minutes 👻 📔 🖪 Repo
Kubernetes Swarr	m (Preview)		Analytics •
25 Containers O O O O 25 Occker O O O O O O O O		17 Services	
ocker Hosts	Standalone Docker Host Summary		Explore
Search 🔎 🗸	Related Items	Resource Utilizations	
 default (gin1b9kbtca0a4q9r?) ^ <	Svarm Guster ⇒ 1 0 0 0 1 Containers ⇒ 5 0 0 0 5 Services 3 0 1 0 2	This Host is Not Currently Being Monitored.	Configure Host Monitorin Network Transfer Rate 13:30 13:50 14:10 Transfer Rate Storage Transfer Rate 13:30 13:50 10:10 Tansfer Rate
	Summary and Resource Information Container Count by Status All (10), F Operation System CentOS Linux 7 Architecture x86_64 Memory Total 8,202,063,872	Attempty Consumed Baseline Attempt Consumed Consumed Consumed Consumed Consumer Cons	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.
 - **i NOTE:** All the docker host metrics are calculated from the aggregated metrics of the containing containers on the docker host.

Eiguro 42	Dockor H	ost Explorer	N woive	onitoring '	Tab
Figure 42.	DOCKEI HU	υδι εχρισιεί	VIEW IVI	omitoring	Iab

	Environment > Docker Host: dsrotateupgrade3					G* marsua	y, April 25, 20	19 10:59:10	AM - NOW OUT	minutes 🕈 [[Repo
ocker	Host: dsrotateupgrade3										
Monitorii	ng Metrics										
ummary	and Resource Information										
ontaine	er Count by Status All (22), Paused (0), St	opped (9), Runnii	ng (13)								
peratio	n System CentOS Linux 7 (Core)			Host	dsrotateupgrade3 (10.4.1	17.155)					
lemory	1.8 GB			Nano CPU	1						
ocker V	/ersion 18.09.2			Cgroup Driver	cgroupfs						
	lost Swarm Information										
warm C				Swarm Role	Manager						
warm N	lode dsrotateupgrade3 (xypq2vtwr	4cztdyo16cjg9v3	3)	Swarm Node Status	[ready]						
ontainer	s										
Alarms	Name			Id				Ima	ge		letw([#] Mod
0	voting_result.1.m1ab9gkqai8l1krg24oudykdt		aa25171d29a8	076e9a0a076340a967927a	237cccdc066b6e460c4e44d1	ad2979 do	ckersamples	/examplev	otingapp_re	sult: <none> d</none>	lefau '
\odot	voting_vote.2.ua654o33tdvqp7fn3pvyqo0rb		133ae0269871	fbe90b894be92719216e9be	ef2d46328c5d849a5acec025	dd4b4 dd	ckersamples	/examplev	otingapp_vo	ote: <none> d</none>	lefau
\bigcirc	wordpress_wordpress.3.3d78lukeu8t9evlzq3mp	t8ehr	7b6b79b24d5d	7efa67e4ac707fc1efcc696d	af36c6205dae4fd1645123d3	dec2 w	ordpress: <n< td=""><td>one></td><td></td><td>d</td><td>lefau</td></n<>	one>		d	lefau
\odot	voting_redis.1.awis611hu72gyxl5hl5epjy6v		288e8a1dde3a	0e893913559c7e2202e96f5	2a88fadfe5b862d4b6988a73	5d896 re	6 redis: <none></none>				
\bigcirc	voting_vote.1.deivdnggt0nlrcb8qo0b8r1hd		f5eca4b5aec92	294745fe742a2eb9e12ee26b	13699edbc473cc6b334d9e7	8bc5d do	dockersamples/examplevotingapp_vote: <none></none>				
0	redis2.xypq2vtwrx4cztdyo16cjg9v3.vrubg5q34j	aq8fih21mg6xex	149fa7578f49f	332fed8ac292d61cd19dc8e	afecdf45a1b3482201312fadf	De6 re	redis: <none></none>				
\odot	mongo_mongo.1.95ak9qe8gp158etdue4pwfu2	v	78a7e75c36a9	056c9abc9eba4d636f2a155	8ff236873d67bd114f21df12a	ad2d m	mongo: <none></none>				
0	mysql_phpmyadmin.1.0c2dfj4k6ghuo4n463mf8	qj7m	f89221041f8d	dcdb2c594bf9a304af3924d8	b1f26700ecc794f7173b52e4	7bd7 pł	pmyadmin/p	ohpmyadmi	n: <none></none>	d	lefau
0	wordpress_db.1.7c7fttk36oijtcspb6zr1tjoh		1711d54e6f15	255a20e37685ccf85ad6a36	56beae84bf9ce44cb763d29d	734a2 m	/sql: <none></none>	,		d	lefau
\bigcirc	wordpress_visualizer.1.drlgdbtulabsbze5eriegdj	q7	d1af858af9554	+6c4db25fc7218dc89bfe4c9	9b73980d746a2eea9dd74a48	9719 do	ckersamples	/visualizer:	<none></none>	d	lefau
\bigcirc	voting_visualizer.1.nwq4l4jm8bwpyvmh9wn300	ddy	16b274edf0a9	72a313b61f785e3473571cfa	6f380ef1a57991cc64fc53dd	dbb9 do	ckersamples	/visualizer:	<none></none>	d	lefau
\odot	mysql_mysql.1.mrroqco2fs7qm5pjk9y4bnjke		2c27187424e0	82060de9cbc9da6d2e9dac4	40cdbc50ffa626ed45157698	cc722 m	/sql: <none></none>	•		d	lefau
\bigcirc	voting_db.1.8eol3l95f710l50jrvpq4j9hu		7a60a959fb3a	fa27006ed3383d69e966ae2	5270c1502f9f95127c6696ae	26db pc	stgres: <non< td=""><td>ne></td><td></td><td>d</td><td>lefau</td></non<>	ne>		d	lefau
(
nages											
State	Name			Id		Size	Virtual Size	Comment	Containers	Not Update Duration	d 🗄
~	$dockersamples/examplevotingapp_result:<\!non$	e> sha256:e10d	f791f13c3ac17e	fa123dfce57e3297fcea05a3	4b3bbf305749f22a9b3c83	216.0 M	8 216.0 MB		1	2 minute(s)	
~	phpmyadmin/phpmyadmin: <none></none>	sha256:c6ba	363e7c9bba3bc	96aa490e31da3e266e6f7e5	d8c525fb8a36df2544c2aa54	158.2 M	3 158.2 MB		1	2 minute(s)	
~	mongo: <none></none>	sha256:0d18	3f48c313d863d	26aed97c27a0fb73833674c8	37da2576b6282de2439a144d	389.5 M	389.5 MB		1	2 minute(s)	
Ē	nate/dockviz:latest	sha256:93b5	259c1e18862e1	434e39678640cbdd555d1b8	8e2742bc6f4da9c2b78acd8al	6.3 MB	6.3 MB		0		
~	mysql: <none></none>	sha256:7bb2	586065cd50457	e315a5dab0732a87c45c5fa	d619c017732f5a13e58b51dc	454.8 M	8 454.8 MB		2	2 minute(s)	
*	redis: <none></none>	sha256:d4de	ec2c521cdae04	50218bd53c69611bacd2eb1	0838057a5de7dcb341c66cf5	144.2 M	3 144.2 MB		1	2 minute(s)	
*	postgres: <none></none>	sha256:d7cf	98b297166b40e	fca50ff11ef9c7e801d45a0f6	c1ba316854984229667578	214.9 M	3 214.9 MB		1	2 minute(s)	
亩	alpine: <none></none>	sha256:5ch3	aa00f89934411	ffba5c063a9bc98ace875d8f9	2e77d0029543d9f2ef4ad0	5.2 MB	5.2 MB		0		

- 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.

State Name ~ sha256:8dbf7c60cf8866bc03ac941f2462615ef21ddb791304475ad3dbdca9fadc2557 141.3 MB 141.3 MB ~ dockersamples/examplevotingapp_vote:<none> sha256:f6e8af4562c14ab06a2c9f3698e39efa68a6c78a3074b88f539d124e674c8077 79.7 MB 79.7 MB 3 minute(s) sha256:376d1d9e09954917b9d53d7550728ca45eab173b8e039ff9cee40e672a99f882 91.5 MB 91.5 MB \square mongo-express:<none> phpmyadmin/phpmyadmin:<none> Docker Host Explore Containers ~ 3 minute(s) 15 \square nate/dockviz:latest Alarms Id dockersamples/exam ~ levotingapp_ 0 wordpress_visualizer.1.drlgdbtulabsbze5eriegdjq7 d1af858af95546c4db25fc7218dc89bfe4c99b73980d746a2ee ~ redis:<none> 3 minute(s) voting_visualizer.1.nwq4l4jm8bwpyvmh9wn30qddy 16b274edf0a972a313b61f785e3473571cfa6f380ef1a57991cc64fc5 redis:<none> 3 minute(s) ~ ~ mongo:<none ~ wordpress:<none> 3 minute(s) 亩 alpine:<none> ~ postgres:<none> ~ mysql:<none> 3 minute(s) State Labels ~ wordpress_db-data 95a60485f40181d593bf7cf987343 ~ 5387a2aca97bffb3450b27537e984df35bf043bfbfa89531... ~ ~ c62c5e37af00a54d06ee6c6e04f9c22cae1217b4806d9e40... /var/lib/docker/volumes/c62c5e37af00a54d06ee6c6e04f9c22cae1217b4806d9e4... 0.0 f /var/lib/docker/volumes/voting_db-data/_data 35.4 MB ~ voting_db-data ~ 92c4ebb4a373d969d18e7140e08596cf82e28064094128... /var/lib/docker/volumes/92c4ebb4a373d969d18e7140e08596cf82e28064094128... 亩 8f9606b95a0b05416dcb6170d53970cd2bab03ad9eaf824.../var/lib/docker/volumes/8f9606b95a0b05416dcb6170d53970cd2bab03ad9eaf82... 164.3 MB ~ c053ac30f84dca062d0223cbc340837a559bdce7e8b92fc5... /var/lib/docker/volumes/c053ac30f84dca062d0223cbc340837a559bdce7e8b92fc. 38.1 MB 亩 a061620cef2324ff8ea72ef20a956bdc89c6a3c6b56a9703... /var/lib/docker/volumes/a061620cef2324ff8ea72ef20a956bdc89c6a3c6b56a9703... 92.0 B 4a2115e21cc7c0cc7e600f3637f47e135a727c9e1ba3f24c... /var/lib/docker/volumes/4a2115e21cc7c0cc7e600f3637f47e135a727c9e1ba3f24c... ~

Figure 43. Docker Host Explorer view Images table and Volumes table under Monitoring tab

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 79.

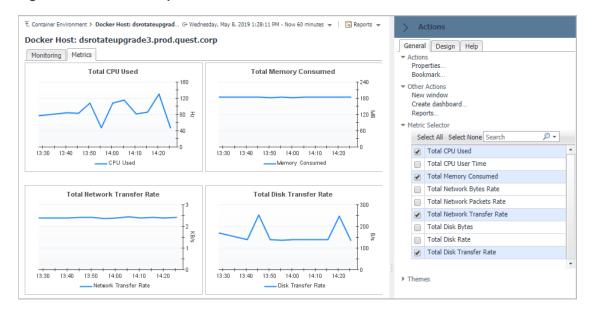


Figure 44. Docker Host Explorer view Metrics Tab

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.

G+ Wednesday, April 24, 2019 3:29:29 PM - 4:29:29 PM 60 m tes 👻 🛛 🖬 Rep Kut Monitoring Alarms : 25 6 2 17 -Services rm Clusters 0 ▲ ⊘ ٠ 0 Swarm Clusters Swarm Cluster Summary <u>,</u> Related It Resource Utilization default (gin1b9kbtca0a4g9r7 Top CPU Utilization Top Memory Utilization Top Network Transfer Rate Top Disk Transfer Rate 8 20 dslocalcluste 100 • 3 8/ 160 😽 40 - 40 14 15:30 16:10 16:10 15:30 15:50 15:50 15:30 15:50 16:10 15:50 16:10 Name Name Name Name wordpress_db.1.7c7ft.. wordpress_db.1.7c7ft... mongo_mongo.1.95ak9q. Ø 0 voting_result.1.m1ab... mysal mysal.1.mrroac... wordpress visualizer... wordpress wordpress voting_db.1.8eol3l95... mongo_mongo.1.95ak9q.. mongo_mongo.1.95ak9q. redis2.7xo0fvsv4kxa9... wordpress_wordpress... mongo_mongo.1.95ak9q redis2.xypq2vtwrx4cz.. voting_redis.1.awis6... mongo_mexpress.2.inw.. . redis2.xypg2vtwrx4cz... voting db.1.8eol3l95... redis2.7e2o8l20yndp5.. Smongo_mexpress.3.ev5... voting_result.1.m1ab... wordpress_wordpress.... wordpress_visualizer... mongo_mexpress.1.wxv.. voting db.1.8eol3195... mongo mexpress.2.inw... mysal mysal.1.mrroac... wordpress_wordpress... voting_vote.2.ua654o.. voting_result.1.m1ab.. mongo_mexpress.1.wxv.. redis2.7e2o8l20yndp5...

Figure 45. 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.

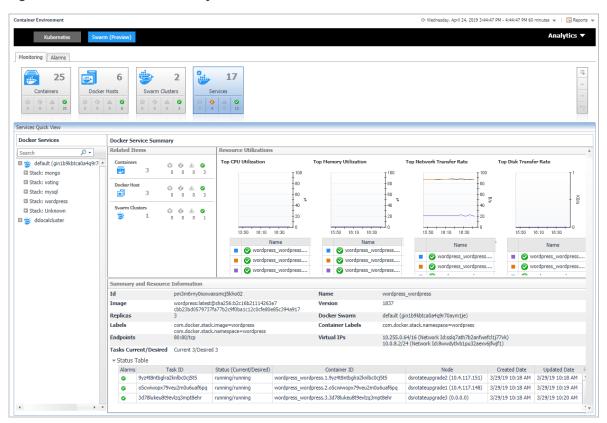


Figure 46. Docker Service Summary view

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

Figure 47. Docker Swarm Alarms Dashboard

Cont	tainer Environment							G+ Wednesday, May 15, 2019 1:17:24 AM - 2:17:24 AM 60 minutes 👻 📋 🖪 Reports
	Kubernetes		Swarm (Previ	ew)			Analytics 🔻
M	onitoring Alarms							
(1	Alarms							
~					Containers Do	cker Hosts Swarn	n Services S	warm Tasks Clusters
							2	
Se	elect All Unselect All	Acknowle	dge Cl	ear			2	Search P •
	elect All Unselect All	Acknowle	-		Impacting	Source	2 Rule Name	
			-			Source DockerSwarmService	Rule Name	Search D -

Foglight for Container Management 7.1.0 User and Administration Guide Using Foglight for Container Management 67

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.

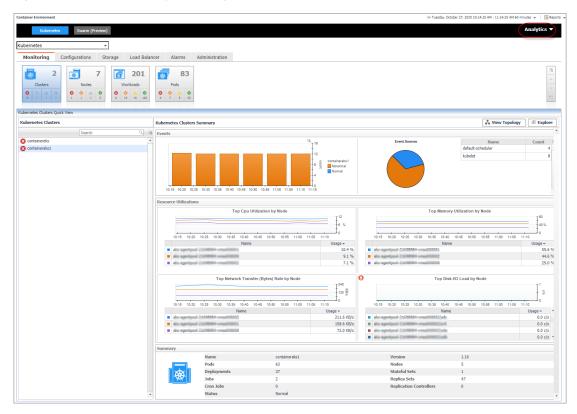
Scatter Plot is used to display values in points using two variables for a set of data. The points is color-coded also, Color Metric can be used to display one additional variable.

- 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 48. Kubernetes analytics Navigation



Foglight for Container Management 7.1.0 User and Administration Guide Using Foglight for Container Management

68

Heatmap analytics

Figure 49. Kubernetes Heatmap Analytics Dashboard

Container Environment > Kubernete:	: Heatmap													High	G+ Mond	ay, November 25, 201	9 10:21:00 AM - 11:21	:00 AM 60 r	ninutes 👻 Low	🖪 Rej	orts
pology Type Kube Pod 🔻 Clu	ster orbital	Namespace A	Namespaces	▼ Selec	ted Metric C	CPU Utilizati	on	•	Color Metric (Memory Util	lization	▼ Co	lor Pattern	High					Low		
eatmap Chart														_							
fedicht-acent-manao	n anan k	Chevel (Chevel)	i ot	ital-notific	ition-sen	ike 766	idd547-1	25twd		cassanc	dra-2				са	ssandra-1		fogl	ight-ala	orbit	al.
																		fogl	i fo	gli ^{fr}	g
																		foglig	jht-d	rbital	
										cassanc	ira-0										
															60	gight-rule-ma	mager-7785				ļ
																					ĺ
ibe Pods																					
Pod Information			CPU				Me	mory						Network					Filesyst	m	
Name	Namespace	Usage	Request	Limit	Utilization	Usage	Request	Limit	Utilization	Send Bytes	Receive Bytes	Send Packets	Receive Packets	Send Errors	Receive Errors	Send Dropped Packets	Receive Packets Dropped	Usage	Limit	Utilizati	0
be growy brand?	kube-system	2.0 millicore/second	100.0 millicore			121.4 MB				20.3 KB/s	56.3 KB/s	74.1 c/s	71.0 c/s	0.0 c/s	0.0 c/s	0.0 c/s	0.0 c/s	36.0 KB	62.0 GB	0.0 %	
ure-cri-retworkmonitur-dlift;	kube-system	1.0 millicore/second				56.1 MB				63.7 KB/s	83.2 KB/s	252.0 c/s	262.6 c/s	0.0 c/s	0.0 c/s	0.0 c/s	0.0 c/s	36.0 KB	62.0 GB	0.0 %	
nault-flevolume-6677c	kube-system	0.0 millicore/second	50.0 millicore	50.0 millicore	0.0 %	22.0 MB	100.0 MB	100.0 MB	22.0 %	0.0 B/s	85.5 B/s	0.0 c/s	2.0 c/s	0.0 c/s	0.0 c/s	0.0 c/s	0.0 c/s	40.0 KB	62.0 GB	0.0 %	
ure-ip-manp agent climit?	kube-system	0.2 millicore/second	50.0 millicore	50.0 millicore	0.3 %	15.3 MB	50.0 MB	250.0 MB	6.1 %	84.6 KB/s	93.0 KB/s	344.8 c/s	339.6 c/s	0.0 c/s	0.0 c/s	0.0 c/s	0.0 c/s	36.0 KB	62.0 GB	0.0 %	
				50.0 millicore		2.0 MB		100.0 MB		0.0 B/s	74.7 B/s	0.0 c/s	1.8 c/s	0.0 c/s		0.0 c/s	0.0 c/s	40.0 KB			

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

- *Topology Type:* Indicates the monitored topology object, including Kubernetes Pod and Kubernetes Node.
- 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 75.
- 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 49 shows an example of heat map. Clicking the object name on the heat map directs you to the relevant object *Explorer* dashboard. For more information, see:

- Workloads Explorer view on page 36
- Workloads metrics on page 75
- Nodes Explorer view on page 33
- Node metrics on page 77
- Cluster Explorer view on page 29
- Docker Swarm metrics on page 79

Scatter Plot analytics

Figure 50. Kubernetes Scatter Plot Analytics Dashboard

Container Environment > Kuberr	etes Scatter										G• Monday, N	ovember 25, 3	2019 10:30:4	IS AM - 11:3	10:45 AM 6	0 minutes		eports y
opology Type Kube Pod 🔻	Cluster orbital	 Namespace 	All Namespaces	▼ X Axis:	CPU Utilization	•	Y Axis:	Memory Uti	lization	▼ Co	olor Metric	CPU Utilizati	on	۲	Color Pa	ittern	High High	
																0	_	_
catter Chart																		
00																		
80																		
50 F					•													
~ •					••													
•		•																
40																		
20																		
0																		
0	10	20	30		40		50		60		70		80			80		
ibe Pods														Netwo				
	Information			CPU					mory		Send	Receive	Cond			Pacaina	Send	Rece
Name		Namespace	Usage	Request	Limit	Utilization	Usage	Request	Limit	Utilization	Bytes		Packets	Packets	Errors	Errors	Send Dropped Packets	Pack
ure ip maap agent diretz		kube-system	0.2 millicore/second	50.0 millicore	50.0 millicore	0.4 %	15.1 MB	50.0 MB	250.0 MB	6.0 %	117.2 KB/s	2.7 MB/s	473.4 c/s	1.4 K/s	0.0 c/s	0.0 c/s	0.0 c/s	0.0 c
gvault flervolume ikvi67		kube-system	0.0 millicore/second			0.0 %	22.0 MB		100.0 MB		0.0 B/s	79.7 B/s				0.0 c/s		0.0 c
hitfune flevvoi installer c76			0.0 millicore/second			0.0 %	1.9 MB		100.0 MB		0.0 B/s	133.8 B/s				0.0 c/s		0.0 c
ture ip maap agent Alph Witnee Aeroni-installer vCor		kube-system	0.3 millicore/second 0.0 millicore/second			0.6 %	18.1 MB 2.0 MB		250.0 MB 100.0 MB		20.3 KB/s 0.0 B/s	44.3 KB/s 55.7 B/s		64.4 c/s 1.3 c/s		0.0 c/s		0.0 c

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 and Kubernetes Node.
- 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.
- YAxis: 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 50 shows an example of Scatter Plot analytics. For more information, see:

- Workloads Explorer view on page 36
- Workloads metrics on page 75
- Nodes Explorer view on page 33
- Node metrics on page 77
- Cluster Explorer view on page 29
- Docker Swarm metrics on page 79

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.

Figure 51. Docker Swarm Analytics Navigation

ontainer Environment				G+ Wednesday, May 8, 201	9 9:50:02 AM - 10:50:02 A	AM 60 minutes 👻 📔 Repor
Kubernetes Swarr	n (Preview)					Analytics 🔻
Monitoring Alarms						Heatmap Scatter
25 <u>Containers</u> ⊘ ⊘ ▲ ② ○ ○ 4 ②	6 Hosts		17 Services			
ocker Containers Quick View	1					
Docker Containers	Docker Container Su	mmary				Explore 3
Search 🔎 🗸	Related Items		Resource Utilizatio	ns		
 icoldscluster icoldscl	Swarm Cluster 1 Docker Host Services 1 Services 1	Image: Constraint of the state of the s	CPU Load 0.33 % Memory 0.04 %	CPU Time 10 10 10 10 10 10 10 10 10 10	Network Transfer	Network I/O 800 400 B 10:00 10:40 Disk I/O 10:00 10:40 0 5 8 1/O 10:00 10:40 0 5 8 1/O 10:00 10:40 0 5 8 1/O 10:00 5 8 1/O
voting_vote.1.5zdmo3 Image: Contract of the second secon	Summary and Resou	rea Information		Tage III Dasenie		Disk ReadDasenie
🛛 💮 wordpress_visualizer.	State	Running				
🗚 📻 mongo_mongo.1.lauh	Created Date	3/29/19 11:42 A	м	St	arted Date	3/29/19 11:42 AM
ø sordpress_wordpress	Docker Host		fog2775ubuntu16.prod		mmand	docker-entrypoint.sh my
📀 👼 mongo_mexpress.1.u	Network Mode	default	. og 2. / odbanta zoiprot		lage	mysql: <none></none>
🖉 📻 voting_redis.1.7u9zcr. 🛕 📻 mysql_mysql.1.wwzcy	IP Address	o croore			ntainer Id	0ac17ff0cef7c29bd78eb fbe2293c3639ee1db17b
voting_vote.2.i77wq2	Ports	3306 33060		Mo	ounts	(volume) /var/lib/mysql

Heatmap analytics

Figure 52. Docker Swarm Heatmap Analytics Dashboard

Container Environment > Docker Swarm Heatmap						iday, November 2, 2018 2:56 AM - 4	20 AM 1.4 hours 👻 📔 Reports 🤘
opology Type Docker Container 🔻 Cluster All Clusters 🔻 Selected Metric CPU U	Itilization	▼ Color	Metric Memory Utilizatio	on 🔻 Color	Pattern		Low
leatmap Chart							
voting_worker.1.xygkjn8b2uuiipglelmvzpj2e						voting_db.1.xlele	b9uwhxeb7domfivwv
warm Containers						voting_redis.1.nv	vfx2moecimr7v5sb3
warm Containers Container Name	CPU Utilization	CPU Time Used	Memory Utilization	Network Transfer Rate	Disk Transfer Rate		vfx2moecimr7v5sb3 Memory Swap Page Out
	CPU Utilization 2.9 %	CPU Time Used 57 ms	Memory Utilization 0.1 %	Network Transfer Rate 1546 KB/s	Disk Transfer Rate 0.0 KB/s		
Container Name						Memory Swap Page In	Memory Swap Page Out
Container Name voting_redis.1.nwfx2moecimr7v5sb3gmqgtmk	2.9 %	57 ms	0.1 %	154.6 KB/s	0.0 KB/s	Memory Swap Page In 485.0 count	Memory Swap Page Out 422.0 count
Container Name voting_redis.1.nvfs/2moecimr7v5sb3gmqgtmk voting_vote.1.io3t8mmg/xptvdocs2wbvdd99	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 Out 422.0 count 7.2 K
Container Name voting_redis_inwit62moeclm/7v5ab3gmagtmk voting_vote_lu326mmgvapbudoc32vbvdd99 voting_vote_lu326mgvapbudoc32vbvdd99	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 Out 422.0 count 7.2 K 5.9 K
Container Name voting_redis_1.nwfs2moceim7V58b3gmagtmk voting_vote_1.lo3t8mmgvxpbxdccs2wbvdd99 voting_vote_2.wtfs4f64402sd2ysginnm voting_worker.1.sysgin8b2uuipgleImvzpj2e	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 Out 422.0 count 7.2 K 5.5 K 1.1 M
Container Name voting_redis_1.nwh2moacim/7V58b3gmggtmk voting_vote_1.lv03t8mmgvxptvdces2vlvvdd99 voting_vote_2.vh7kt[6y4f6r402sdysginnm voting_vote_1.svgh6nb2.auligpleImvzpj2e voting_visuelizer.1.offj23lgc62/j4j2nzmvK9jeop	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 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 Out 422.0 count 7.2 K 5.9 K 1.1 M 125.2 K
Container Name voting_redis_1.nwh2moacimr7Vs8b3gmagtmk voting_vote_1.lo388mmgxvpbudocs2vbvdd99 voting_vote_2.vh7x16y4f6r402sdysginnm voting_vorker_1.vygfon8b2.utipgleImzg12e voting_vsualizer_1.offj23lg6s21/f1zmnvkSjeop tomcatcluster_proxy-q2hagsrt156redmvhdHgcdea.sgxxfcl2wwl6i9giit38s1t	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 Out 422.0 count 7.2 K 5.9 K 1.1 M 125.2 K 8.4 K

Foglight for Container Management 7.1.0 User and Administration Guide Using Foglight for Container Management **71**

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 79.
- 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 52 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 62
- Docker Host Explorer view on page 63
- Container metrics on page 79

Scatter Plot analytics

Figure 53. 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.
- YAxis: Indicates which metrics will be plotted on Y axis.
- Rendering related metrics: .
 - Color Metric: Renders the color of circle based upon the selected metrics.

72

Color Pattern: Offers two patterns, Red to Green (larger value shows in red) or Green to Red (larger value shows in green).

Figure 53 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 62
- Docker Host Explorer view on page 63
- Container metrics on page 79

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 54.	Container	Components	in Domains	dashboard
------------	-----------	------------	------------	-----------

lomains			G+ Monday, June 24, 2019 10:16:44 AM -	Now 60 minutes 👻 📔 🖪 Re	eports
💂 Domains					
A domain is a group of monitored components organized by moni information about the contents and health of the domain.	toring technology. This dashboard show	rs a summarized view of your mor	nitored enterprise organized by domain.	Click on a sub-domain for	deta
Name 🔺	State	History	Alarms	Agents	
Container	\$				
👜 Docker Swarm	S				
Kubernetes	🎸 📕		27 15	S	
Custom Applications	O				
Databases	S				
🗉 🤱 End User	S				
Infrastructure	0				
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 55. Object Groups for Container

•	Add	📝 Ed	dit 🤤 Remove					Search	+ 🔍	
	Acti Edit	ions Test	Name 🔺		Descr	iption		Is Disabled	Created by Foglight	
)	1		Agents	All Agent objects.				false	true	
	2	6	All Models	All model objects.				false	true	
	1	-	Арр	The Application Tie	er includes all objects from .NET, Siebel, SA	P, PeopleSoft and		false	true	
	2	6	Azure	All Azure Objects				false	true	
	2	6	DB	The Database Tier	includes all objects from Oracle, SQLServe	r, Sybase and Db2 ca		false	true	
	2		Docker Swarm	All Docker Swarm	Objects			false	true	
	2	6	Geo	All Geo Aware App	lications.			false	true	
	1		Global Services	All Global Services				false	true	
	1		Hosts	All Host objects.	Host objects.			false	true	
	2		Hyper-V	All Hyper-V Object	-			false	true	
	1		Java EE	The Java EE Tier in	he Java EE Tier includes all objects from Weblogic, WebSphere, JBoss, OracleAS,			false	true	
	2		Kubernetes	All Kubernetes Obj	Il Kubernetes Objects			false	true	
	1		OpenStack	All OpenStack Obj	Il OpenStack Objects			false	true	
	2		User	The User Tier inclu	des all the objects for end user performan	ce.		false	true	
	1		VMware	All VMware Object	s			false	true	
		F 2	VMware Clusters	All VMware Cluster	All VMware Clusters			false	true	
			19 subgroup(s)						Ø +	1
"	Add		t All Select None 🤤 R	emove				Search	• •	
	Actio Edit		Nam	e 🔺	Description	Data Type	Query Condition	ns Is Disabled	Created by Foglight	
			Kubernetes Clusters		All Kubernetes Clusters	KubeCluster	n/a	false	true	
	1		Kubernetes Config Maps		All Kubernetes Config Maps	KubeConfigMap	n/a	false	true	
		_	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	
	1	_	Kubernetes Deployments	5	All Kubernetes Deployments	KubeDeployment	n/a	false	true	
	1		Kubernetes Endpoints		All Kubernetes Endpoints	KubeEndpoint	n/a	false	true	
	1	_	Kubernetes Ingresses		All Kubernetes Ingresses	KubeIngress	n/a	false	true	
	1	_	Kubernetes Jobs		All Kubernetes Jobs	KubeJob	n/a	false	true	

Select Docker Swarm or Kubernetes to display the subgroups.

Reference

- Metrics
 - Kubernetes metrics
 - Docker Swarm metrics
- Rules
 - Kubernetes
 - Docker Swarm
 - Customization

Metrics

Kubernetes metrics

Workloads metrics

Table 4. Workloads metrics

Metric name	Description
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 Cache	Number of bytes of page cache memory.
Memory Swap	Container swap usage in bytes.
Memory Request	Memory request (the guaranteed amount of resources) in bytes.
Memory Limit	Memory hard limit in bytes.
Memory Utilization	Percentage of Memory usage / Memory limit if user configured Memory limit for this pod.
Network Send Bytes Rate	Network send bytes per second.
Network Receive Bytes Rate	Network receive bytes per second.

Table 4. Workloads metrics

Metric name	Description
Network Transfer Bytes Rate	Network send and receive bytes per second.
Network Send Errors Rate	Network send errors count per second.
Network Receive Errors Rate	Network receive errors count per second.
Network Transfer Errors Rate	Network send and receive errors count per second.
Network Send Packets Rate	Network send packets count per second.
Network Receive Packets Rate	Network receive packets count per second.
Network Transfer Packets Rate	Network send and receive packets count per second.
Network Send Dropped Packets Rate	Network send dropped packets count per second.
Network Receive Dropped Packets Rate	Network receive dropped packets count per second.
Network Transfer Dropped Packets Rate	Network send and receive dropped packets count per second.
Filesystem Usage	Number of bytes that are consumed by the container on this filesystem.
Filesystem Capacity	Number of bytes that can be consumed by the container on this filesystem.
Filesystem Utilization	Percentage of Filesystem Usage / Filesystem Capacity.
Filesystem Read Bytes Rate	Filesystem read bytes per second.
Filesystem Write Bytes Rate	Filesystem write bytes per second.
Filesystem Read Rate	Filesystem read counts per second.
Filesystem Write Rate	Filesystem write counts per second.

i | NOTE:

- Workloads metrics are for the following workloads types, Deployment, Daemon Set, Stateful Set, Replica Set, Replication Controller, Cron Job, Job, and Pod.
- For workloads types except Pods, the metrics values come from the aggregated metrics values of the related Pods.

Container metrics

Table 5. Container metrics

Metric name	Description
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 Cache	Number of bytes of page cache memory.
Memory Swap	Container swap usage in bytes.
Memory Request	Memory request (the guaranteed amount of resources) in bytes.
Memory Limit	Memory hard limit in bytes.
Memory Utilization	Percentage of Memory usage / Memory limit if user configured Memory limit for this pod.
Filesystem Usage	Number of bytes that are consumed by the container on this filesystem.
Filesystem Capacity	Number of bytes that can be consumed by the container on this filesystem.
Filesystem Utilization	Percentage of Filesystem Usage / Filesystem Capacity.
Filesystem Read Bytes Rate	Filesystem read bytes per second.
Filesystem Write Bytes Rate	Filesystem write bytes per second.
Filesystem Read Rate	Filesystem read counts per second.
Filesystem Write Rate	Filesystem write counts per second.

Node metrics

Table 6. Node metrics

Metric name	Description
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.
CPU Allocatable	Available CPU to allocate to workloads.
CPU Capacity	Hard CPU capacity of node.
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 Cache	Number of bytes of page cache memory.
Memory Swap	Container swap usage in bytes.
Memory Request	Memory request (the guaranteed amount of resources) in bytes.
Memory Capacity	Hard memory capacity of node.
Memory Limit	Memory hard limit in bytes.

Table 6. Node metrics

Metric name	Description
Memory Allocatable	Available Memory to allocate to workloads.
Memory Utilization	Memory utilization as a share of memory allocatable.
Network Send Bytes Rate	Network send bytes per second.
Network Receive Bytes Rate	Network receive bytes per second.
Network Transfer Bytes Rate	Network send and receive bytes per second.
Network Send Errors Rate	Network send errors count per second.
Network Receive Errors Rate	Network receive errors count per second.
Network Transfer Errors Rate	Network send and receive errors count per second.
Network Send Packets Rate	Network send packets count per second.
Network Receive Packets Rate	Network receive packets count per second.
Network Transfer Packets Rate	Network send and receive packets count per second.
Network Send Dropped Packets Rate	Network send dropped packets count per second.
Network Receive Dropped Packets Rate	Network receive dropped packets count per second.
Network Transfer Dropped Packets Rate	Network send and receive dropped packets count per second.
Filesystem Usage	Number of bytes that are consumed by the container on this filesystem.
Filesystem Capacity	Number of bytes that can be consumed by the container on this filesystem.
Filesystem Utilization	Percentage of Filesystem Usage / Filesystem Capacity.
Filesystem Inodes Usage	Number of Inodes that are consumed by the container on this filesystem.
Filesystem Inodes Total	Number of Inodes that can be consumed by the container on this filesystem.
Filesystem Inodes Utilization	Percentage of Filesystem Inodes Usage / Filesystem Inodes Capacity.
Filesystem Read Bytes Rate	Filesystem read bytes per second.
Filesystem Write Bytes Rate	Filesystem write bytes per second.
Filesystem Read Rate	Filesystem read counts per second.
Filesystem Write Rate	Filesystem write counts per second.

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.
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

i NOTE: Foglight 7.1.0 uses Alarm Templates to gather alarm rules into a domain-specific template that is easily modified and applied to targets. Alarm rules can be modified using the Alarm Templates dashboard.

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.

For information on customizing alarms templates and rule, refera to Modifying alarms and threshold values and Customization.

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	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	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	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.		

Kubernetes Container Restart for Termination with Invalid State

Purpose

This rule checks for container that restarted and previously terminated in an invalid state within the last 12 hours.

Scope

KubeContainer

Conditions	Severity	Action
Container that restarted and previously terminated in an	Critical	Send email to Kubernetes
invalid state within the last 12 hours.		Administrator

Usage

NOTE: All the Pod usage related rules are disabled by default, these rules are used as default values or examples for the customers to customize their different kinds of workloads. For how to customize the rules, refer to Customization on page 95.

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 95. 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

KubePodCpu

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 95. 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

KubePodMemory

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 95. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePodCpu

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 millicores/second.

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 95. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePodMemory

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 bytes.

Kubernetes Pod Network Receive

Purpose

This rule detects abnormal Network Receive Rate in bytes/second 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 95. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePodNetwork

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 bytes/second.

Kubernetes Pod Network Send

Purpose

This rule detects abnormal Network Send Rate in bytes/second 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 95. You can also change value of the registry variables or use your own value to change the threshold of each severities.

Scope

KubePodNetwork

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 bytes/second.

Kubernetes Pod Filesystem Utilization

Purpose

This rule checks kubernetes pod filesystem utilization to see if it reaches the defined threshold. The filesystem utilization rule only works for pod that configures filesystem limit.

Scope

KubePodStorage

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.		Kubernetes: PodFilesystemUtilization Fatal	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: PodFilesystemUtilization Critical	None
Pods whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	Kubernetes: PodFilesystemUtilization Warning	None

*Note: the unit is percentage.

Kubernetes Node CPU Utilization

Purpose

This rule detects abnormal CPU Utilization 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

KubeNodeCpu

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 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

KubeNodeMemory

Conditions and Severities

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 Rate in bytes/second 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

KubeNodeNetwork

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 bytes/second.

Kubernetes Node Network Send

Purpose

This rule detects abnormal Network Send Rate in bytes/second 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

KubeNodeNetwork

Conditions and Severities

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 bytes/second.

Kubernetes Node Network Transfer

Purpose

Periodically check Kubernetes node Network Transfer Rate in bytes/second, if the value is too high and changes too much, then an alarm will be triggered.

Scope

KubeNodeNetwork

Conditions	Severity	Threshold (Registry Variable)*	Action
Nodes whose usage is about to reach the limit, the ration is above the value configured in fatal Threshold.		Kubernetes: NodeNetworkTransferFat al	Send email to Kubernetes Administrator
Nodes whose usage is about to reach the limit, the ration is above the value configured in critical Threshold.	Critical	Kubernetes: NodeNetworkTransferCriti cal	None
Nodes whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	Kubernetes: NodeNetworkTransferWar ning	None

*Note: the unit is bytes/second.

Kubernetes Node Filesystem Utilization

Purpose

Periodically check Kubernetes node Filesystem Utilization, if the value is too high and changes too much, then an alarm will be triggered.

Scope

KubeNodeFilesystem

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Nodes whose usage is about to reach the limit, the ration is above the value configured in fatal Threshold.		KubeNodeFilesystemUtili zationFatal	Send email to Kubernetes Administrator
Nodes whose usage is about to reach the limit, the ration is above the value configured in critical Threshold.	Critical	KubeNodeFilesystemUtili zationCritical	None
Nodes whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	KubeNodeFilesystemUtili zationWarning	None

*Note: the unit is percentage.

Kubernetes Container CPU Utilization

Purpose

This rule checks Kubernetes container CPU utilization to see if it reaches the defined threshold. The CPU utilization rule only works for container that configures CPU limit.

Scope

KubeContainerCpu

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

*Note: the unit is percentage.

Kubernetes Container Memory Utilization

Purpose

This rule checks Kubernetes container Memory utilization to see if it reaches the defined threshold. The Memory utilization rule only works for container that configures Memory limit.

Scope

KubeContainerMemory

Conditions and Severities

Conditions	Severity	Threshold (Registry Variable)*	Action
Containers whose usage is about to reach the limit, the ration is above the value configured in fatal Threshold.		Kubernetes: ContainerMemoryUtilizati onFatal	Send email to Kubernetes Administrator
Containers whose usage is about to reach the limit, the ration is above the value configured in critical Threshold.		Kubernetes: ContainerMemoryUtilizati onCritical	None
Containers whose usage is about to reach the limit, the ration is above the value configured in warning Threshold.		Kubernetes: ContainerMemoryUtilizati onWarning	None

*Note: the unit is percentage.

Container Cost Cluster Budget Over Spending

Purpose

Detecting container cluster whose budget is over spending.

Scope

AbstractKubernetesClusterCost

Conditions	Severity	Threshold (Registry Variable)*	Action
Cluster current month cost which is about to reach the limit, the ration is above the value configured in fatal Threshold.	Fatal	ContainerCost:OverBudg etFatal ContainerCostAdmin	Send email to Kubernetes Administrator
Cluster current month cost which is about to reach the limit, the ration is above the value configured in critical Threshold.	Critical	ContainerCost:OverBudg etCritical	None
Cluster current month cost which is about to reach the limit, the ration is above the value configured in warning Threshold.	Warning	ContainerCost:OverBudg etWarning	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	Critical	Send email to Docker
service.		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	Warning	None	
submission periods.			

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 95. 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 95. 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.

Modifying alarms and threshold values

i IMPORTANT: Avoid editing rules in the Administration > Rules & Notifications > Rule Management dashboard. Default rules may be modified during regular software updates and your edits will be lost. Always use the Alarm Templates dashboard.

You can and should modify the thresholds associated with alarms to better suit your environment. If you find that alarms are firing for conditions that you consider to be acceptable, you can change the threshold values that trigger the alarm. You can also enable or disable severity levels to better suit your environment.

When a rule has severity levels, a Threshold section appears in the Alarm Settings tab showing the severity levels and bounds by agent. Many rules, such as Baseline rules, do not have severity levels and thresholds.

When editing thresholds, ensure that the new values make sense in context with the other threshold values. For most metrics, threshold values are set so that Warning < Critical < Fatal. However, in metrics where normal performance has a higher value, the threshold values are reversed: Warning > Critical > Fatal.

To change alarm status and threshold values:

- **i IMPORTANT:** The procedure below is a summary. Refer to **Viewing, Creating, and Managing Alarm Templates** in the *Foglight 7.1.0 User Guide* for more information on editing alarm templates for more information on working with alarm templates.
 - 1 In the Navigation panel, click Alarm Templates.
 - 2 If you have previously configured an alarm template, select that template.

Otherwise, click the Factory Template to view the default rules. Duplicate the factory template to make an editable copy, selecting the appropriate domains.

- 3 Click the appropriate domain tab.
- 4 Scroll or search to find the alarm rule you want to edit. Click the rule to select it.

Edit the rules using the procedure described in **Viewing**, **Creating**, **and Managing Alarm Templates** in the *Foglight 7.1.0 User Guide*

Customization

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

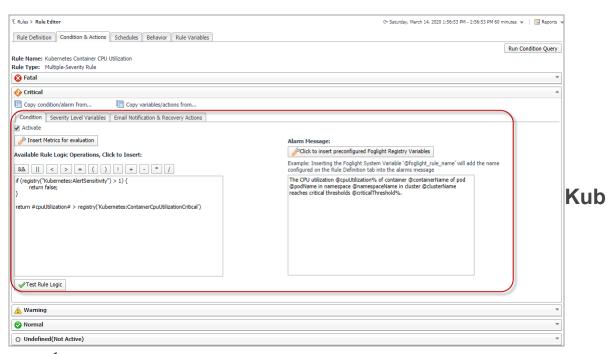
To access Rule Scope and Condition, do the following:

- 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.

Figure	56.	Rule	Scop	e
---------------	-----	------	------	---

T. Rules > Rule Editor	G+ Saturday, March 14, 2020 1:56:53 PM - 2:56:53 PM 60 minutes 💌 📋 💽 Reports 🤜
Rule Definition Condition & Actions Schedules Behavior Rule Variables	
Basic Information Rule Name: Kubernetes Container CPU Utilization Rule Type: Multiple-Severity Rule Cartridge Name(Cartridge Version): Kubernetes-Agent (3.0.0) Rule Triggering: Time Driven © Driven Driven © Schedule Driven	Description (Optional) Rule Description: This rule checks kubernetes container CPU utilization to see if it reaches the defined threshold. The CPU utilization rule only works for container that configures CPU limit. Alarm Description:
Rule Scope Cartridges: Kubernetes-Agent Topology Type: KubeContainerCpu Property: Property:	rties • • •

Figure 57. Condition



ernetes

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.

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit https://www.quest.com/.

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.