Foglight for Cassandra

Cartridge Guide

© 2018 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 Web site (https://www.quest.com) for regional and international office information.

Patents

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

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Table of Contents

Table of Contents 3

Introduction 6

Description 6

Business Challenge 6

Key Features 6

Foglight for Cassandra Requirements 7

Installing and Configuring Agents 8

Cassandra Agent User Permissions 8

Installing the Cassandra Cartridge 9

Creating the Cassandra Agent 10

Roles 13

Upgrading the Agent 14

Removing Monitored Databases 15

Administration 16

Opening the Databases Administration Dashboard 16

Reviewing the Administration Settings 16

Customizing Alarms for Foglight for Cassandra Rules 17

Introducing the Alarms View 17

Modifying Alarm Settings 17

Enabling or disabling alarms for selected agents 19

Modifying alarm threshold values 19

Editing the text of the alarm message 20

Reviewing Rule Definitions 21

Dashboards 22

Databases 22

Cassandra Clusters 22

Cluster Keyspaces 23

Cluster Tables 23

Traces Sample 24

Node Overview 25

Node Keyspaces 25
Node Tables 26
Node Table 26
Client Requests 27
Connections 27
JVM 27
Cache 28
Thread Pools 29
Slow Query Log 29
Rules 30
Cassandra Cache KeyCache HitRate 30
Cassandra ClientRequest SpikeRate 30
Cassandra CommitLog PendingTasks 30
Cassandra CommitLog WaitingOn 30
Cassandra Compaction PendingTasks 30
Cassandra Datacenter Availability 30
Cassandra DroppedMessage MutationDropped 30
Cassandra JVM Memory HeapMemoryRatio 30
Cassandra JVM OS SystemCPULoad 30
Cassandra JVM OS UsedPhysicalMemSizePct 30
Cassandra JVM OS UsedSwapSpaceSizePct 30
Cassandra Node Availability 30
Cassandra Node AvgReadLatency 31
Cassandra Node AvgWriteLatency 31
Cassandra Node LiveDiskSpaceUsedPercent 31
Cassandra Node PendingCompactions 31
Cassandra Node PendingFlushes 31
Cassandra Node RowCacheMissRate 31
Cassandra SchemaVersion 31
Cassandra Storage Exceptions 31
Cassandra Storage Load 31
Cassandra Storage TotalHints 31

Cassandra Storage TotalHintsInProgress 31
Cassandra Table AvgKeyCacheHitRate 31
Cassandra Table AvgReadLatency 32
Cassandra Table AvgRowCacheHitRate 32
Cassandra ThreadPools PendingTasks 32
Cassandra ThreadPools TotalBlockedTasks 32
Reports 33
Cassandra Cluster Summary 33
Cassandra Cluster Tables 33
Cassandra Node Executive Summary 33
Cassandra Node Health Check 33
Cassandra Storage Report 33

Introduction

Description

Complex applications that require storage of a massive amount of data and a flexible data structure require a new form of database. Cassandra database offers scalability and high availability without compromising performance on commodity hardware or cloud infrastructure. This makes it an ideal platform for mission-critical data and for replicating across multiple datacenters. Cassandra is a best-in-class solution, providing low latency for users and peace of mind, with an architectural rigidity designed to survive regional outages.

Business Challenge

Modern NoSQL databases like Cassandra are designed to support massive data processing and provide an equally large storage capability, but hosting Cassandra clusters with a large number of nodes can greatly increase the complexity of your data infrastructure. Understanding the performance of your Cassandra clusters is critical for diagnosing issues and planning capacity.

Foglight for Cassandra provides comprehensive performance monitoring and administration for all nodes in a cluster from a centralized console. You can collect statistical data from all JVMs in a cluster and key performance metrics like memory utilization statistics, task statistics of thread pools, storage statistics, CPU usage, operational performance, latency, and bottlenecking.

Key Features

Foglight for Cassandra provides a consolidated view of all monitored ***Cassandra Clusters,*** containing information on cluster structure, nodes, health status, and other key metrics. Derived calculations provide insight into the overall cluster workload taking into account activity on each node in the cluster.

View ***Cluster Health*** at a glance, displaying a topology of the cluster structure or a list of nodes with relevant performance and availability metrics. ***Tables*** can be viewed by cluster or namespace, aggregating associated metric information across nodes. ***Node*** Information is granular and includes Node Health and Alerts, Availability, Workload, Statements, Connections and Operations.

Understand every component of Cassandra performance. Granular ***performance metrics*** such as Reads/Writes, Caches, Bloom Filter, Buffer Pool, Memtables, and Commit Log are collected and stored for historical and trend analysis. JVM information is also collected and analyzed to help ensure optimal configuration and performance.

Understand response times with a breakdown of ***Client Requests*** to the node by type, showing metric histories for average latency, request counts, and request errors, broken down by error type. Understand the performance and availability between all nodes in your cluster. Foglight for Cassandra monitors all ***Connections*** including dropped messages, timeouts, and pending messages.

Alerts can be generated based on preset rules and thresholds as well as dynamically, based on situational anomalies. Alerting has been designed to help ensure the performance and availability of your Cassandra environment at all times and to keep it performing optimally.

Foglight for Cassandra Requirements

Foglight for Cassandra is compatible with **Apache Cassandra versions 2.1+ and DSE versions 4.8+**. However, some data may not be available in earlier versions. The following list itemizes which features become available at which versions.

v3.0:

Traces include client and command.

Buffer pool JMX metrics available.

Storage service JMX metrics available.

Various changes in JMX table metrics.

Foglight for Cassandra can be installed on **FMS 5.9.2+** and agents require **FglAM 5.8.5.2+**.

Installing and Configuring Agents

Cassandra Agent User Permissions

Using a superuser role or a role with user creation permissions, connect via cqlsh to a node on the cluster and create a new user for the Foglight Agent as follows:

For versions of Cassandra >= 2.2 or DSE >= 5.0:

```
CREATE ROLE IF NOT EXISTS foglightagent WITH PASSWORD = '<your-password>' AND LOGIN = true AND SUPERUSER = false;

GRANT SELECT ON ALL KEYSPACES to foglightagent;
```

For versions of Cassandra <= 2.1 or DSE <= 4.8:

```
CREATE USER IF NOT EXISTS foglightagent WITH PASSWORD '<your-password>' NOSUPERUSER;

GRANT SELECT ON ALL KEYSPACES TO foglightagent;
```

Enable remote JMX authentication as per the instructions here:

For Linux:

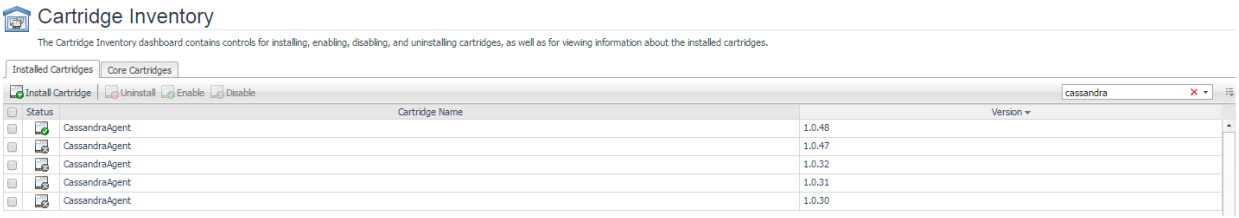
http://docs.datastax.com/en/cassandra/3.x/cassandra/configuration/secureJmxAuthentication.html

For Windows:

http://docs.datastax.com/en/cassandra_win/3.x/cassandra/configuration/secureJmxAuthentication.html

Installing the Cassandra Cartridge

1. Open Foglight Management Console.
2. From the navigation pane, select: **Dashboards** > **Administration** > **Cartridges** > **Cartridge Inventory**. The Cartridge Inventory screen appears. For more information on agents, see the *Foglight User Guide.*
3. Load the ***CassandraAgent-xxxx.car*** file by browsing to the location where the .car file exists and then clicking on "Install Cartridge". Leave the "Enable on Install" check box checked.
4. Once the installation is completed on the Foglight Management Server, the Cassandra Cartridge will appear in this list below as an installed cartridge.



Creating the Cassandra Agent

When an agent connects to the Foglight Management Server, it is provided a set of properties that is then used to configure its correct running state.

Values for Agent properties are provided by default with the Foglight Cartridge for Cassandra. However, the user will typically edit these properties for their environment. Agent properties may apply only to a specific agent instance, or may be applicable across multiple agents.

For more information about working with agent properties, see the *Foglight Administration and Configuration Guide.*

To create a new agent instance:

1. Open the Foglight web console.
2. From the navigation pane, select: **Dashboards** > **Administration** > **Agents** > **Agent Status**. The Agent Status screen appears.
3. Deploy the Cassandra agent package to the preferred agent managers.
4. When the deployment is finished, create a Cassandra agent instance with a name that you will be able to identify as related to the Cassandra Node you intend to monitor.
5. Select the checkbox next to the Cassandra agent row. The selected row is highlighted with a yellow background.
6. Click **Edit**, then **Edit Properties**.
7. Select **Modify the default properties for this agent**.
8. Edit the agent properties for the Cassandra agent instance:

DB Connection

The agent requires a connection to the cluster in order to gather information about the cluster and data structure. The agent may be referred to other nodes than the one specified.

- **IP or Hostname** – Host where Cassandra node is running. Default is “localhost”. (e.g.<hostname> or <IP address>)
- **Port** – The CQL native transport port for the Cassandra node. Default is 9042.
- **Username** – User that can connect to the Cassandra node.
- **Password** – Password of the user that can connect to the Cassandra node.
- **Use TLS/SSL?** – Whether the database connection should be made over SSL.

JMX Connections

The agent requires JMX access to individual nodes in the cluster to gather most operational metrics.

- **Node Connections** – IP/Hostname for each node in the cluster to be monitored must be added to this list. Values for the columns Port, Username, and Password can be specified for each node if they differ. If no value is provided for these, values will be taken from the default fields under JMX Connections (see below). Check "Use as Host Alias?" to indicate that the value provided for "IP or Hostname" should be used as an alias for the discovered hostname for the respective node. Secondary Property Lists are global and can be shared between agents. To create a new property list for a different cluster, clone an existing list and then edit and save it as the selected list for that agent.
- **Default Port** – JMX listening port for the Cassandra node. This value will be used as the default value in the Node Connections list if no other value is provided. Default is 7199.

- **Default Username** – JMX User that can connect to the Cassandra node. This value will be used as the default value in the Node Connections list if no other value is provided.
- **Default Password** – Password of the JMX User that can connect to the Cassandra node. This value will be used as the default value in the Node Connections list if no other value is provided.

Collection Periods

The Collection Interval fields in the agent properties are used to set the sample frequencies. You can turn off a collection by setting the interval to 0. The defaults are set based on the type of data being collected for relevancy.

- **Database and JMX** – Controls the query interval for the main data collection through both the database connection and the JMX connection.
- **Keyspace and table collections** – Controls the query interval for collection of data on individual keyspaces and tables both through the database connection and JMX connection. Note that these collections are more data and time-intensive and therefore a longer value should be used here than for the Database and JMX period.
- **Slow Query** – Controls the query interval for collection of the DSE Slow Query log.
- **Trace** – Controls the query interval for collection of the trace log. Note that tracing must be enabled on the Cassandra instance(s) separately for data to be collected.

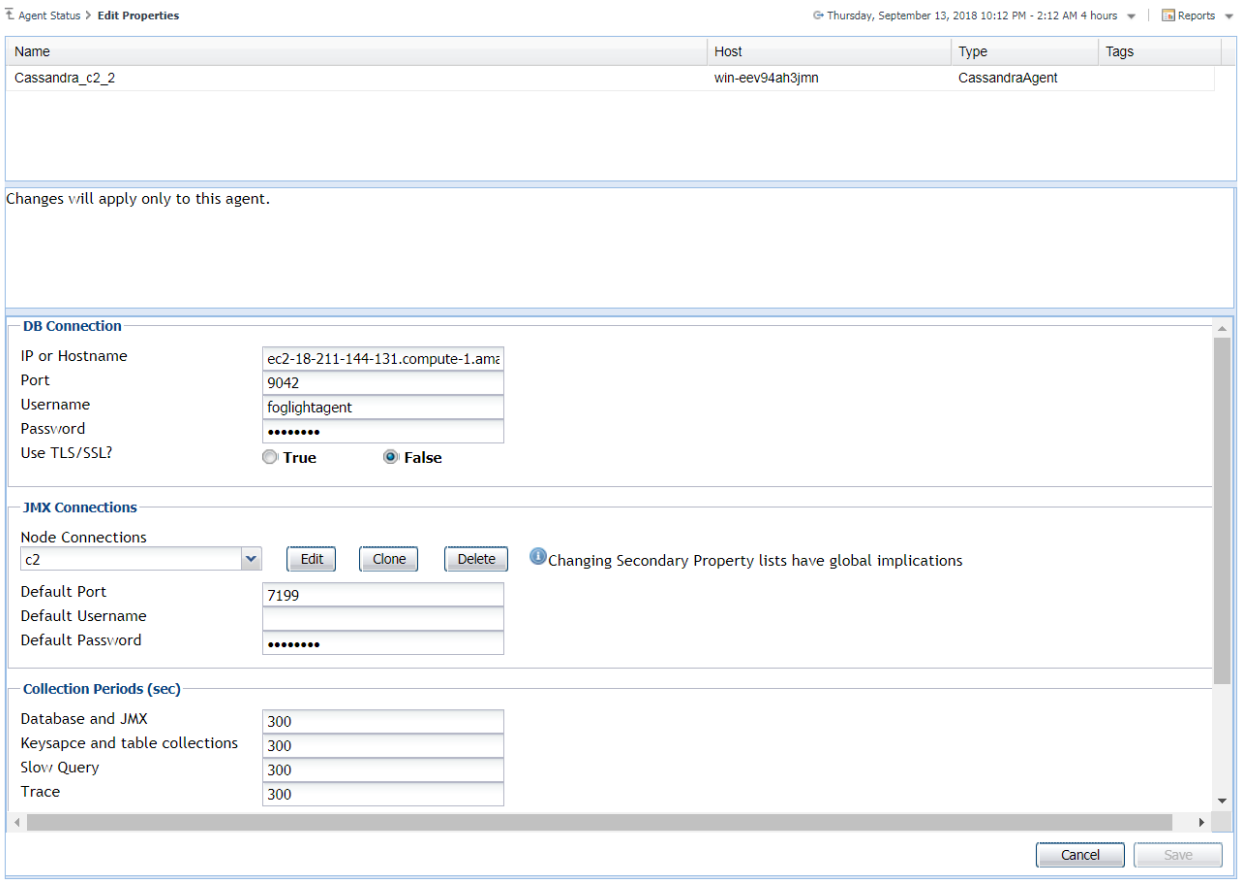
Options

Host Aliases

Aliases can optionally be added for Cassandra nodes in case hostnames as discovered by the agent differ from those used for the Hosts monitor. This Secondary Property List is a pairing of the uniquely identifying Host ID (a UUID string) and the desired hostname alias. There are two ways to determine a node's Host ID for use in the Aliases list. For a node that has already been monitored for some time, the Host ID can be found on the Nodes Table of the Cassandra Clusters dashboard (the Host ID column is hidden by default, so it will need to be made visible via the table's "Show columns" dialog). Host IDs can also be queried directly from a specific Cassandra instance with the following CQL:

```
SELECT host_id FROM system.local WHERE key='local';
```

Max traces/queries per period - The maximum number of traces or slow query entries to collect per their respective collection periods. Limiting the number here prevents the FMS from being overwhelmed by data (particularly from traces) on very active instances.


Agent Status > Edit Properties
Thursday, September 13, 2018 10:12 PM - 2:12 AM 4 hours
Reports
Name
Host
Type
Tags
Cassandra_c2_2
win-eev94ah3jmn
CassandraAgent
Changes will apply only to this agent.
DB Connection
IP or Hostname
ec2-18-211-144-131.compute-1.ama
Port
9042
Username
foglightagent
Password
Use TLS/SSL?
True
False
JMX Connections
Node Connections
c2
Edit
Clone
Delete
Changing Secondary Property lists have global implications
Default Port
7199
Default Username
Default Password
Collection Periods (sec)
Database and JMX
300
Keysapce and table collections
300
Slow Query
300
Trace
300
Cancel
Save

Roles

Two roles, Cassandra User and Cassandra Administrator, are installed with the cartridge. Viewing Cassandra dashboards requires that a user be assigned one of these or have the core Administrator role. The Set Trace Probability function on the Traces Sample dashboard requires the Cassandra Administrator role.

Upgrading the Agent

1. Go to Dashboards > Administration > Cartridges > Cartridge Inventory and click the Install Cartridge button.
2. Locate the .car file on your system and install it with auto-enable selected. If you get a message that a bundled cartridge is of an older version than the one currently enabled on your FMS and will not be enabled, ignore it and continue.
3. Once the cartridge is installed and enabled, go to Dashboards > Administration > Agents > Agent Managers. Agent Managers that can be upgraded with newer agent packages will show “yes” in the Upgradable | Agents column. Select all Agent Managers you wish to upgrade and click the Upgrade button.

Note: If an Agent Manager is not upgradable, check that the Agent Manager version is compatible with the newer agent version. If it is not, the Agent Manager will need to be upgraded first.

Removing Monitored Databases

1. Go to the Databases dashboard.
2. Select the databases you wish to remove.
3. Click the Settings button, then click ok.

Note: Doing this will remove the monitoring agents as well as the historical data already collected. If you wish to delete only the agents, you can do that on the Administration > Agents > Agent Status page. Because the Databases dashboard only shows databases which are being actively monitored, you will only be able to view these databases by going through the MySQL > MySQL Global View dashboard.

Administration

Opening the Databases Administration Dashboard

You can edit agent settings for one or more Cassandra instances on the Databases > Administration dashboard.

> **NOTE:** If you attempt to select instances of more than one type of database, such as a Cassandra database and an Oracle database, an error message is displayed.

To open the Databases Administration dashboard:

1. In the navigation panel, under **Homes**, click **Databases > Cassandra**.
2. Select the check boxes beside one or more Cassandra instances.
3. Click **Settings** and then click **Administration**. The Administration dashboard opens, containing settings for all the selected agents. Settings are broken down into categories, which are organized under a Cassandra tree.

Reviewing the Administration Settings

The Databases Administration dashboard allows settings options for collecting, storing, and displaying data, which apply to all the currently selected agents. Click a category of settings on the left (for example: Connection Details) to open a view containing related settings on the right.

To view the full list of selected agents, click the **Selected Agents** button at the upper right corner of the screen. To change the list of agents to which the metrics will apply, exit the Databases Administration dashboard, select the requested agents and re-open the view.

Customizing Alarms for Foglight for Cassandra Rules

Many Foglight for Cassandra multiple-severity rules trigger alarms. To improve your monitoring experience, you can customize when alarms are triggered and whether they are reported. You can also set up email notifications.

Introducing the Alarms View

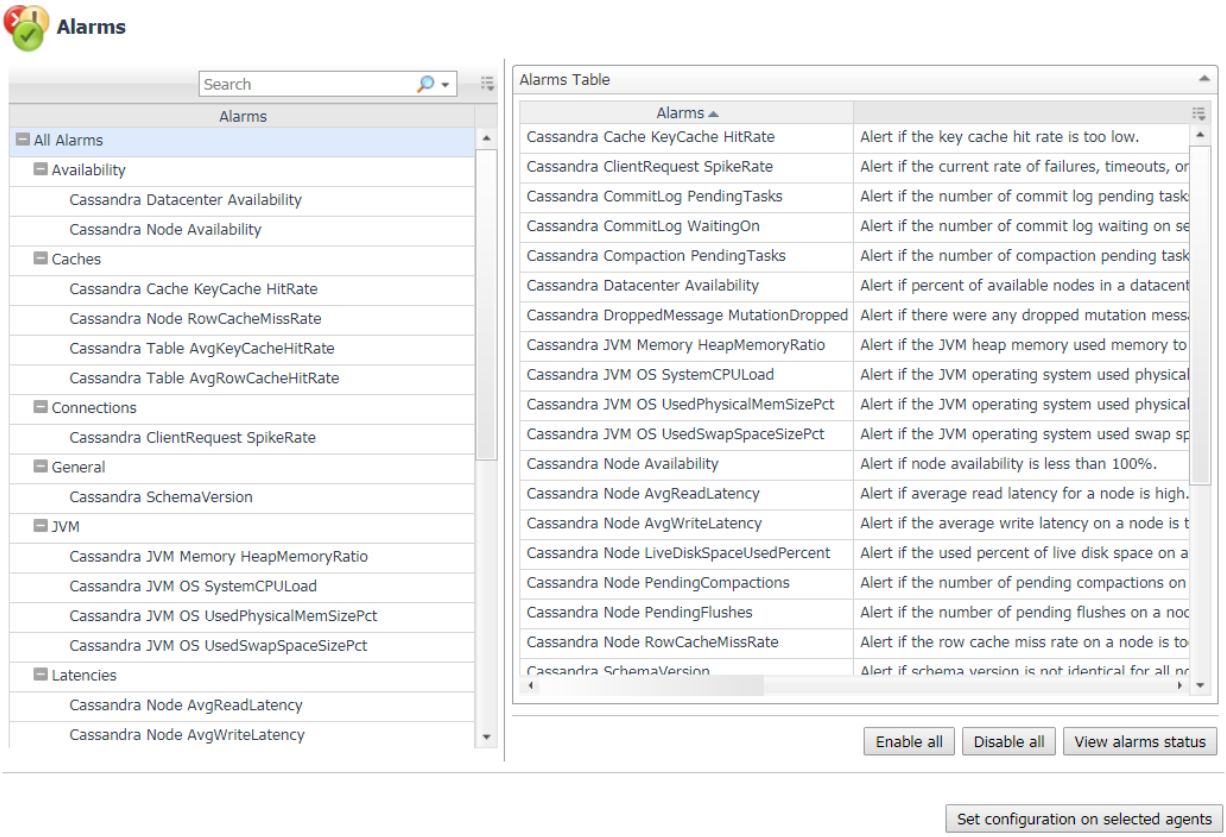
The Alarms view enables you to modify global settings and agent-specific settings for alarms.

To open the Alarms view:

1. Open the Administration dashboard as described in Opening the Databases Administration Dashboard.
2. Click **Alarms**. The list of agents that you selected on the Databases dashboard is shown in the upper right corner of the view.
3. From the Alarms view, you can complete the following tasks:
    a. Modifying Alarm Settings
    b. Reviewing Rule Definitions

Modifying Alarm Settings

You can customize how the alarms generated by the default Foglight for Cassandra rules are triggered and displayed in the Alarm view's Settings tab. All changes to alarm settings apply to the selected agents, with the exception of thresholds, which can be customized by agent.



The Alarms list controls the contents displayed to the right and the tasks that are available.

- **All Alarms –** Displays all rules with configured alarms and indicates whether alarms are enabled. In this view, you can enable or disable alarms for all the rules at once. You can also set email notifications and define mail server settings.
- **Category of rules –** Displays a set of related rules with configured alarms. In this view, you can enable or disable alarms and also set email notifications for the category of rules.
- **Rule name –** Displays the alarm status for the selected rule. If the rule has multiple severity levels, displays the threshold configured for each severity level. In this view, you can enable or disable the alarm, edit the alarm text, and edit severity levels and their thresholds. You can also set email notifications for the alarm.

You can complete the following tasks:

- Enabling or disabling alarms for selected agents
- Modifying alarm threshold values
- Editing the text of the alarm message

Your changes are saved separately and applied over the default rules. This protects you from software upgrades that may change the underlying default rules.

Enabling or disabling alarms for selected agents

You can override the global alarm sensitivity level setting for the selected agents. You can enable or disable alarms for all rules, a category of rules, or an individual rule.

To see descriptions of the rules, follow the steps described in Reviewing Rule Definitions.

To enable or disable alarms:

1. In the Alarms view, click the **Settings** tab.
2. Decide on the scope for the change: all alarms, a category of rules, or a selected rule.
3. Complete the steps for the selected scope:

Scope	Procedure
All alarms	Click **All Alarms**. In the Alarms Settings tab, click either **Enable all** or **Disable all**.
Category of rules	Click a category. Click either **Enable all** or **Disable all**.
Selected rule	Click the rule. In the Alarms Settings tab, click the link that displays the alarm status. Select **Enabled** or **Disabled** from the list and click **Set**.

4. Click **Save changes**.

Modifying alarm threshold values

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. 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 severity levels and thresholds:

1. In the Alarms view, click the **Settings** tab.
2. Click the multiple-severity rule that you want to edit.
3. Click the **Alarms Settings tab.**
4. In the Threshold section, review the defined severity levels and existing threshold bounds for all target agents.
5. From this view, you can perform the following tasks:

Task	Procedure
Edit severity levels and set threshold (lower bound) values for all agents.	Click **Enhance alarm**. Select the check boxes for the severity levels you want enabled and set the threshold values. Click **Set**.
Change the threshold (lower bound) values for one agent.	Click **Edit** beside the agent name. Set the new threshold values and click **Set**.

Copy the changes made to one agent's threshold values to all other agents.	Click **Edit** beside the agent name that has the values you want to copy. Select **Set for all agents in table** and click **Set**.

6. Click **Save changes**.

Editing the text of the alarm message

For individual rules, you can change the message displayed when an alarm fires. You cannot add or remove the variables used in the message. This is a global setting that affects all agents.

To change the alarm message:

1. In the Alarms view, click the **Settings** tab.
2. Select a rule.
3. Click the **Alarm Settings** tab.
4. Click **Enhance alarm**. A Customize <rule> dialog box opens.
5. In the Message box, edit the message text. To restore the default message, click **Reset message**.
6. Click **Set**.
7. Click **Save changes**.

Reviewing Rule Definitions

If you want to review the conditions of a rule, open the rule in the Rule Management dashboard.

> **IMPORTANT:** Avoid editing rules in the Rule Management dashboard unless you are creating your own rules or copies. These rules may be modified during regular software updates and your edits will be lost.

You can create user-defined rules from the Rule Management dashboard. If you want to modify a rule, we recommend copying the rule and creating a user-defined rule. User-defined rules need to be managed from the Rule Management dashboard; these rules are not displayed in the Alarms view of the Databases Administration dashboard. For help creating rules, open the online help from the Rule Management dashboard.

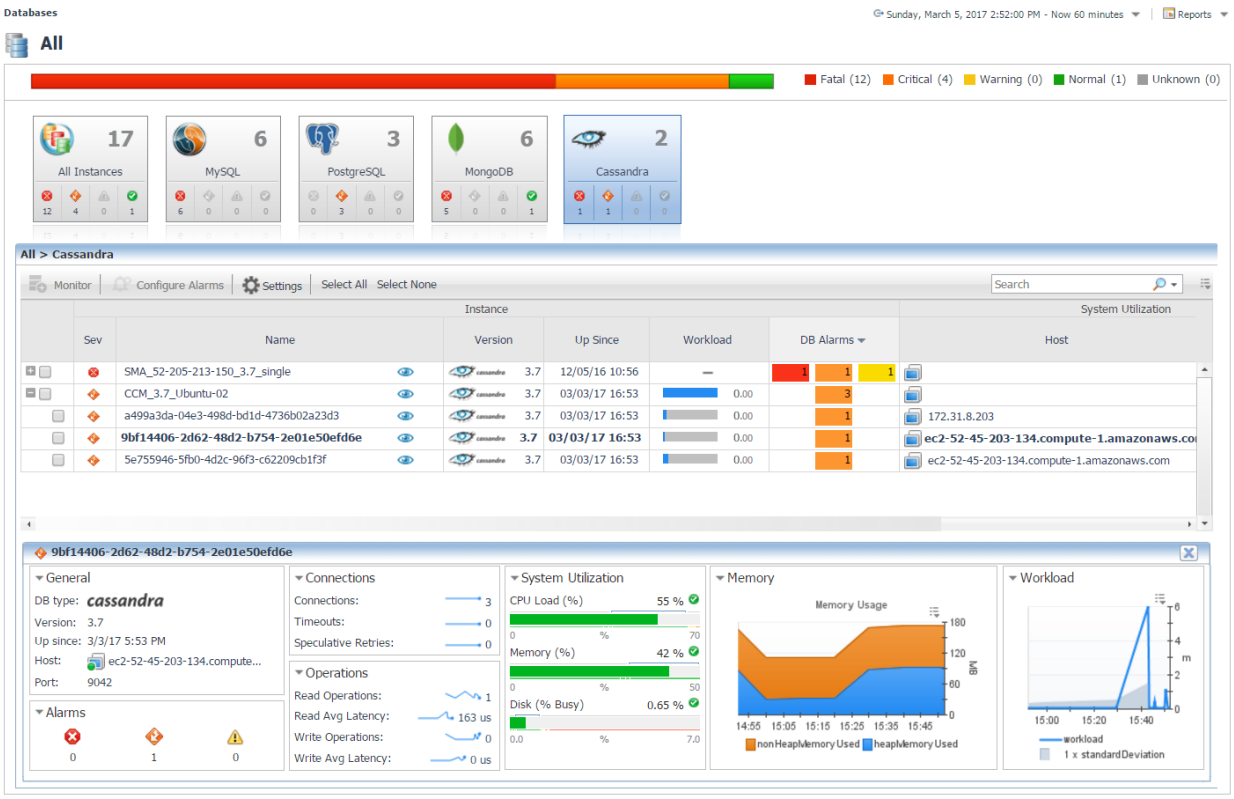
To open the Rule Management dashboard:

1. On the navigation panel, under **Homes**, click **Administration**.
2. In the Administration dashboard, click **Rules**.
3. Type **Cassandra** in the Search field to see the list of predefined rules for Cassandra databases. The Cassandra rules are displayed. From here, you can review threshold values, alarm counts, and descriptions.
4. To see the full rule definition, click a rule and then click **View and Edit**.
5. In the Rule Detail dialog box, click **Rule Editor**.
6. When you are done with your review, click Rule Management in the bread crumbs to return to the dialog box.
7. Click **Cancel** to avoid changing the rule unintentionally.

Dashboards

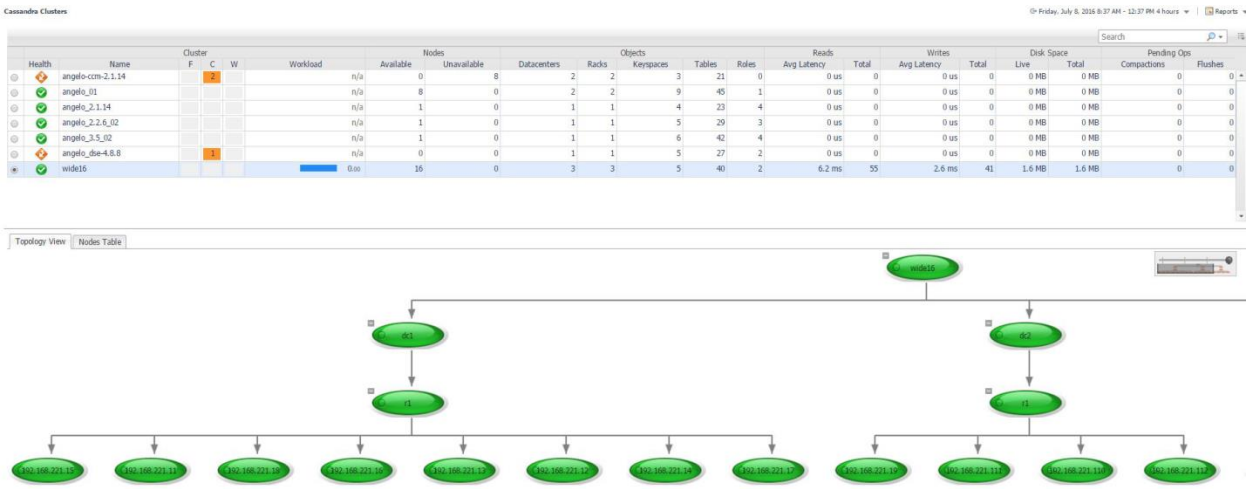
Databases

Foglight for Cassandra is now incorporated into the Databases dashboard along with any other monitored database types in your environment. Like other products, the list of databases can be filtered by type and severity level and includes basic information, alarms, and host utilization metrics. Clusters and Replica Sets can be expanded to show their individual nodes. Clicking on the eye icon in the Name column will bring up the Quick View with more key information. Clicking the name of an object will drill down to into the appropriate overview page.



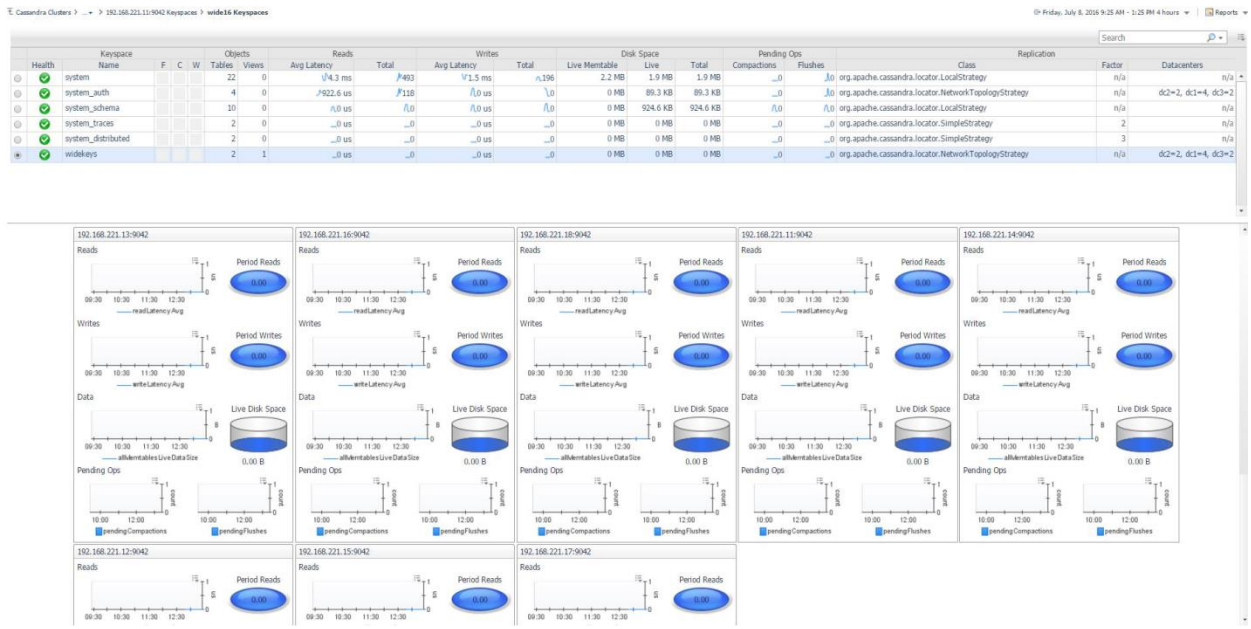
Cassandra Clusters

This dashboard lists all monitored Cassandra Clusters and contains high-level information on cluster structure, nodes, health status, and key metrics. The workload metric is used for comparing the amount of work a node is doing. Cluster workload averages the workloads of all nodes in that cluster. Selecting a cluster will update the bottom section of the page and display either a topology view of the cluster structure or a list of nodes with relevant information. In the Topology View tab, hovering over an object will show a health summary, while clicking on a node will drill down to the Node Overview page, as will clicking on a node location in the Nodes Table. In the cluster table, clicking the Keyspace or Table column values will drill down to the Cluster Keyspaces and Cluster Tables pages, respectively. Other column values for metrics will show a time plot when hovered or clicked on.



Cluster Keyspaces

This page lists all keyspaces in the selected cluster, aggregating metric information across nodes. Selecting a keyspace will update the section below, displaying a summary of that keyspace for each node in the cluster. Clicking the node location in the title of each summary will drill down to the Node Tables page for the selected node, filtering for only tables in that keyspace. In the Keyspace table, selecting the Tables column value will drill down to the Cluster Tables page, again filtering for only tables in that keyspace.



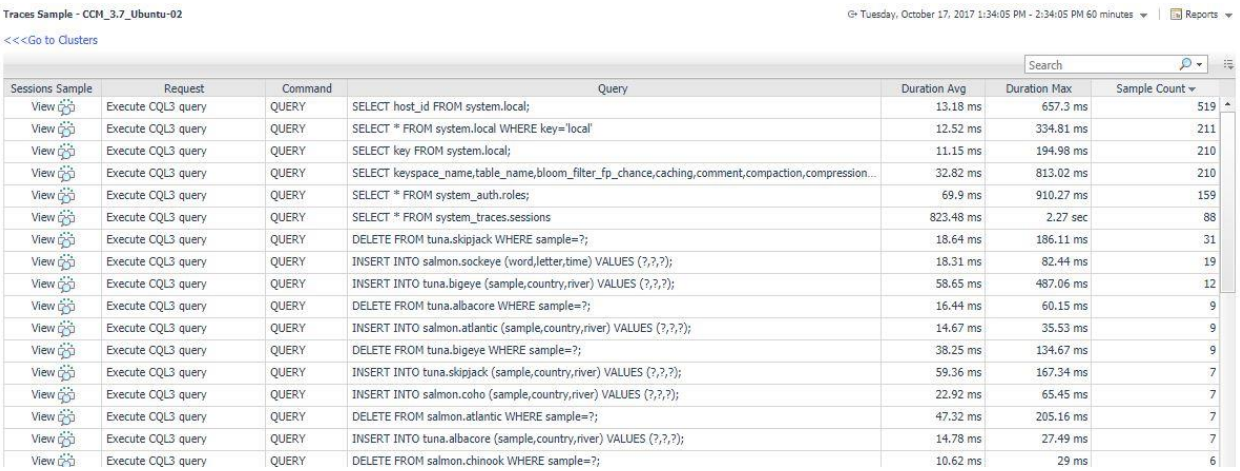
Cluster Tables

This page lists tables in the selected cluster, aggregating metric information across nodes. Selecting a table will update the section below, displaying a summary of that table for each node in the cluster. Clicking the node location in the title of each summary will drill down to the Node Table page for the

selected table. To filter the list of tables by keyspace, click the Select Keyspaces button at the top left of the table and select one or more keyspaces for which you wish to view tables.

Traces Sample

The Traces page shows sampled entries from Cassandra's tracing system. Entries with the same query are aggregated and presented by average and maximum sampled duration. Individual query executions, called "sessions", are retrieved along with each execution duration, timestamp, source, consistency level, etc. The internal events generated to process the query are retrievable per session on demand. Tracing is not enabled by default, but nodetool can be used to enable tracing on a portion of all queries with its subcommand "settraceprobability".



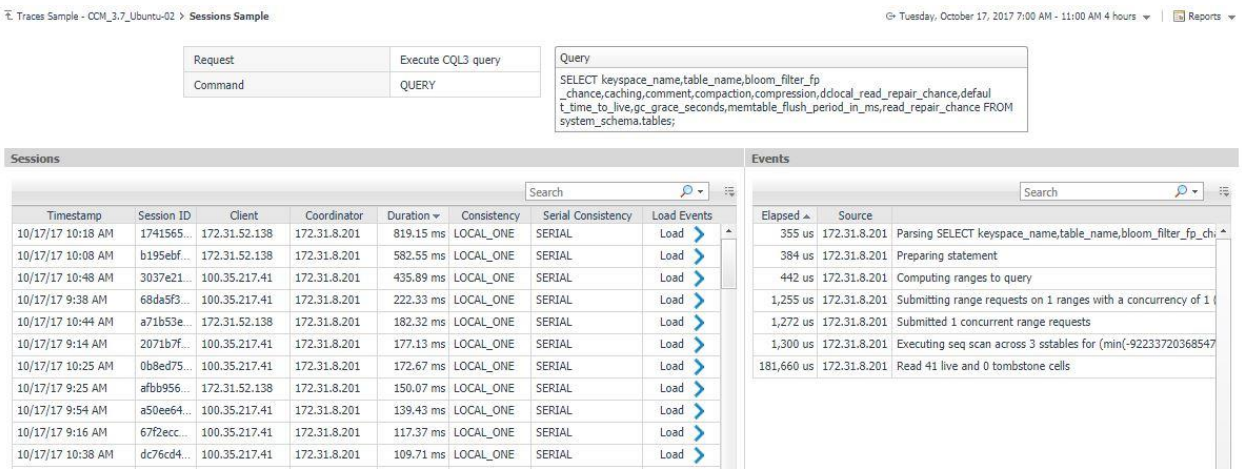
Traces Sample - CCM_3.7_Ubuntu-02

Tuesday, October 17, 2017 1:34:05 PM - 2:34:05 PM 60 minutes | Reports

<<<Go to Clusters

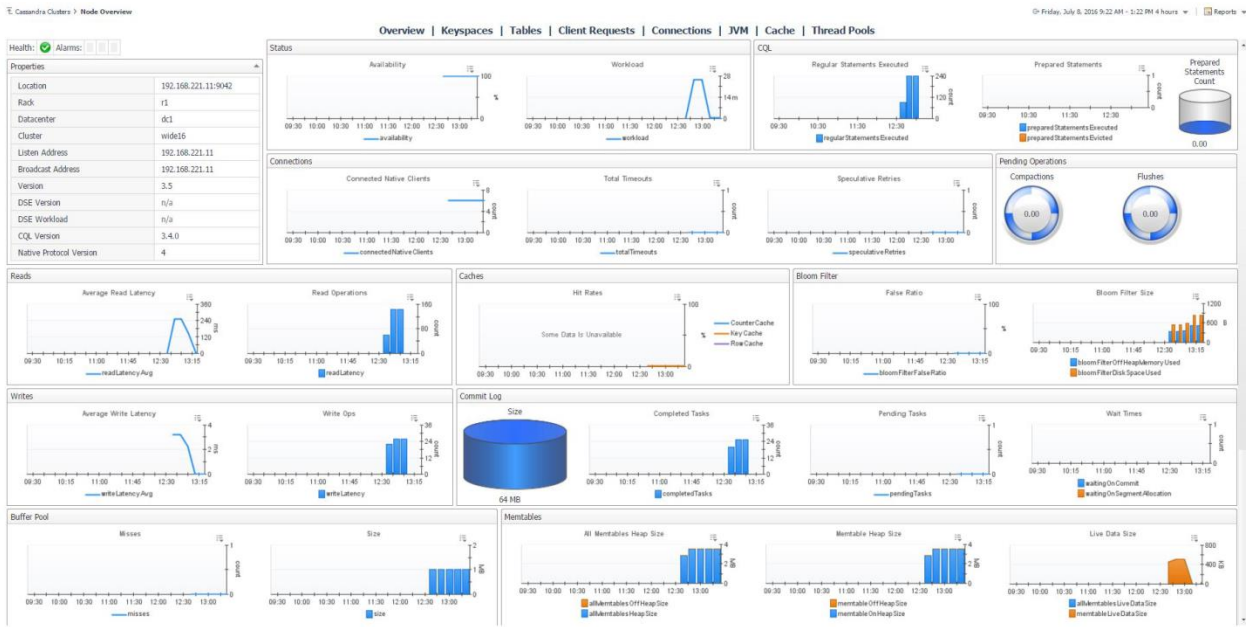
Search

Sessions Sample	Request	Command	Query	Duration Avg	Duration Max	Sample Count
View	Execute CQL3 query	QUERY	SELECT host_id FROM system.local;	13.18 ms	657.3 ms	519
View	Execute CQL3 query	QUERY	SELECT * FROM system.local WHERE key='local'	12.52 ms	334.81 ms	211
View	Execute CQL3 query	QUERY	SELECT key FROM system.local;	11.15 ms	194.98 ms	210
View	Execute CQL3 query	QUERY	SELECT keyspace_name,table_name,bloom_filter_fp_chance,caching,comment,compaction,compression...	32.82 ms	813.02 ms	210
View	Execute CQL3 query	QUERY	SELECT * FROM system_auth.roles;	69.9 ms	910.27 ms	159
View	Execute CQL3 query	QUERY	SELECT * FROM system_traces.sessions	823.48 ms	2.27 sec	88
View	Execute CQL3 query	QUERY	DELETE FROM tuna.skipjack WHERE sample=?;	18.64 ms	186.11 ms	31
View	Execute CQL3 query	QUERY	INSERT INTO salmon.sockeye (word,letter,time) VALUES (?,?,?);	18.31 ms	82.44 ms	19
View	Execute CQL3 query	QUERY	INSERT INTO tuna.bigeye (sample,country,river) VALUES (?,?,?);	58.65 ms	487.06 ms	12
View	Execute CQL3 query	QUERY	DELETE FROM tuna.albacore WHERE sample=?;	16.44 ms	60.15 ms	9
View	Execute CQL3 query	QUERY	INSERT INTO salmon.atlantic (sample,country,river) VALUES (?,?,?);	14.67 ms	35.53 ms	9
View	Execute CQL3 query	QUERY	DELETE FROM tuna.bigeye WHERE sample=?;	38.25 ms	134.67 ms	9
View	Execute CQL3 query	QUERY	INSERT INTO tuna.skipjack (sample,country,river) VALUES (?,?,?);	59.36 ms	167.34 ms	7
View	Execute CQL3 query	QUERY	INSERT INTO salmon.coho (sample,country,river) VALUES (?,?,?);	22.92 ms	65.45 ms	7
View	Execute CQL3 query	QUERY	DELETE FROM salmon.atlantic WHERE sample=?;	47.32 ms	205.16 ms	7
View	Execute CQL3 query	QUERY	INSERT INTO tuna.albacore (sample,country,river) VALUES (?,?,?);	14.78 ms	27.49 ms	7
View	Execute CQL3 query	QUERY	DELETE FROM salmon.chinook WHERE sample=?;	10.62 ms	29 ms	6



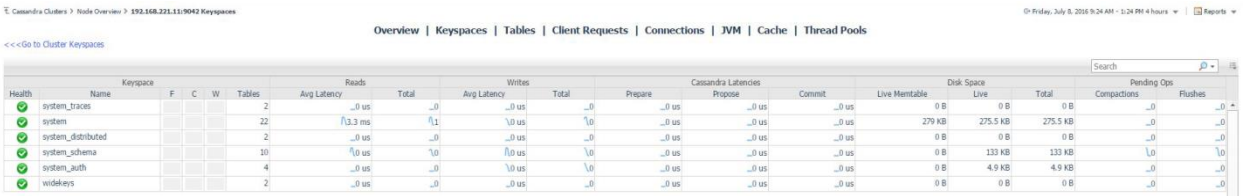
Node Overview

This page provides a comprehensive view of the Cassandra Node, with health and alarms and configuration information at the top left and metrics grouped into relevant categories on the rest of the page. Once in the node section of the dashboards, the navigation bar at the top of the page can be used to navigate between different pages containing more information on the selected node. The Node Selector in the action panel on the right can also be used to switch between nodes in the same cluster.



Node Keyspaces

This page lists all keyspaces on the selected node, with metric information on reads and writes, latency timing, disk space, and pending operations. Clicking the Keyspace Name or Tables column value will drill down to the Node Tables page, filtering for only tables in that keyspace. The “Go to Cluster Keyspaces” link above the table will link to that page for the same cluster, where you can compare keyspaces across different nodes by selecting a keyspace row.



Node Tables

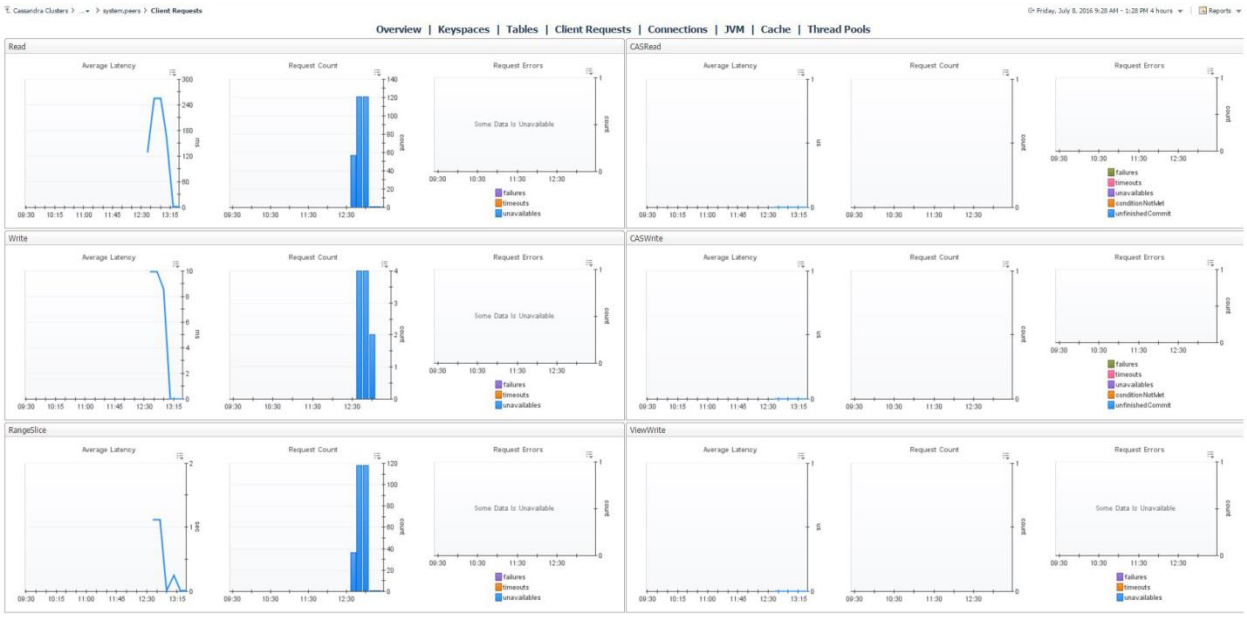
This page lists tables on the selected node, aggregating metric information across nodes, with metric information on reads and writes, latency timing, disk space, and pending operations. Clicking the Table Name column value will drill down to the Node Table page for more information on that table. The “Go to Cluster Tables” link above the table will link to that page for the same cluster, where you can compare tables across different nodes by selecting a table row. To filter the list of tables by keyspace, click the Select Keyspaces button at the top left of the table and select one or more keyspaces for which you wish to view tables.

Node Table

This page provides a comprehensive view of the table, with configuration information at the top left and metrics grouped into relevant categories on the rest of the page.

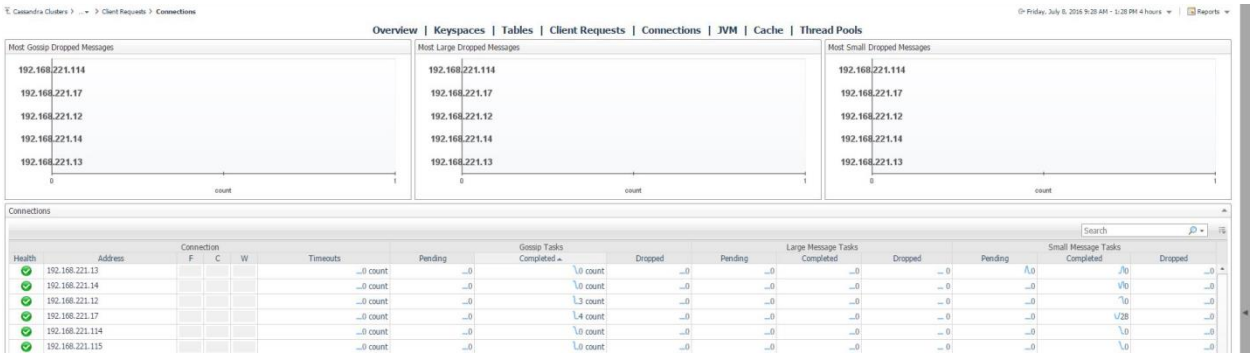
Client Requests

This page displays client requests to the node by type, showing metric histories for average latency, request counts, and request errors, broken down by error type.



Connections

The Connections page shows connections between the selected node and other nodes in the cluster. At the top of the page, three bar graphs show nodes with the most gossip, large, and dropped messages. The below table lists all connections, showing timeouts and result status of messages by task type.

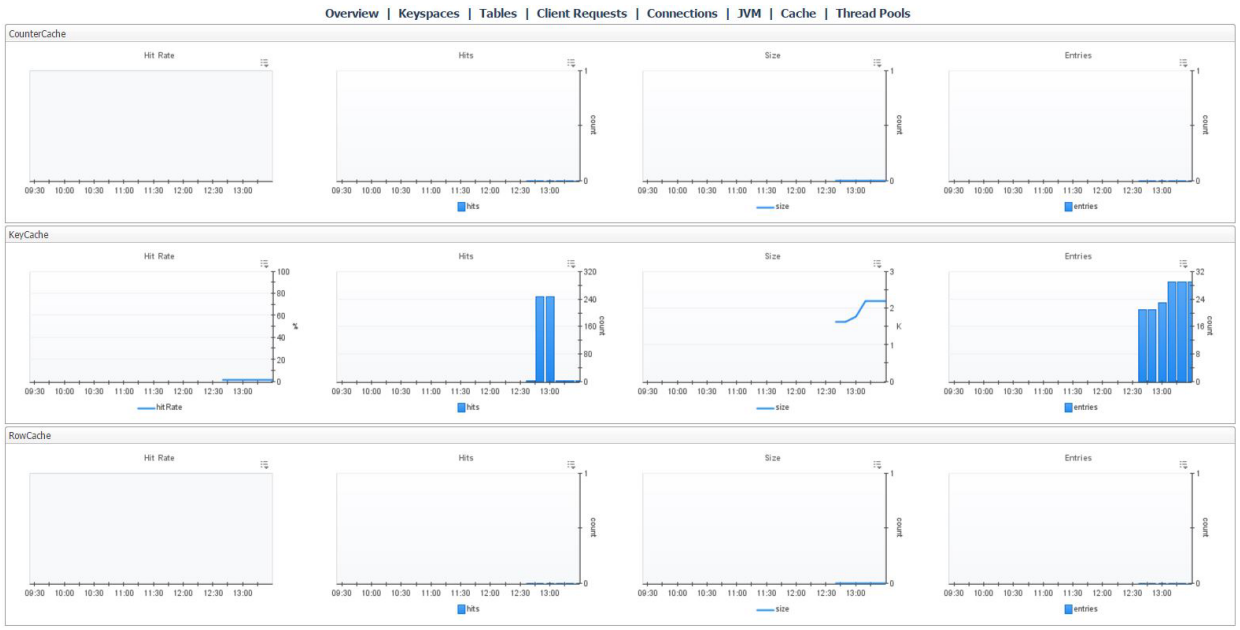


JVM

This page features information on the JVM that Cassandra runs on. The top row contains JVM properties, uptime, and information on memory and threading. The second row displays OS information and memory and CPU metrics. The final row features operational metrics for the various buffer pools, garbage collectors, and memory pools maintained by the JVM.

Cache

The Cache page features cache-related metrics including hit rate, hits, size and number of entries for the counter cache, key cache, and row cache.



Thread Pools

This page displays active and completed task statuses for every thread pool type in the Cassandra node, grouped into Request, Transport, and Internal categories. The page also features a table of dropped messages by stage and includes metrics for number of dropped messages and latencies for internal and cross node dropped messages.

Slow Query Log

The slow query log dashboard displays information on long running queries for DSE Cassandra servers. Slow query logging is enabled by default. The slow query threshold can be raised or lowered with the dsetool "perf cqlslowlog" subcommand.

Timestamp	Source IP	Username	Duration	Tables	Command(s)
10/17/17 9:17 AM	172.31.8.201	root	20 ms	slowspace.place	SELECT * FROM slowspace.place;
10/17/17 9:17 AM	172.31.8.201	root	2 ms	slowspace.place	SELECT * FROM slowspace.place;
10/17/17 9:17 AM	172.31.8.201	root	20 ms	slowspace.place	SELECT * FROM slowspace.place;
10/17/17 9:17 AM	172.31.8.201	root	2 ms	slowspace.place	INSERT INTO slowspace.place(id, ts, info, note) VALUES(uuid(), dateof(now()), 'some info', 'a note');
10/17/17 9:17 AM	172.31.8.201	root	31 ms	slowspace.place	INSERT INTO slowspace.place(id, ts, info, note) VALUES(uuid(), dateof(now()), 'some info', 'a note');
10/17/17 9:17 AM	172.31.8.201	root	86 ms	slowspace.place	INSERT INTO slowspace.place(id, ts, info, note) VALUES(uuid(), dateof(now()), 'some info', 'a note');

Rules

Cassandra Cache KeyCache HitRate
Alert if the key cache hit rate is too low.

Cassandra ClientRequest SpikeRate
Alert if the current rate of failures, timeouts, or unavailables for client request reads and writes is high relative to recent averages.

Cassandra CommitLog PendingTasks
Alert if the number of commit log pending tasks is too high.

Cassandra CommitLog WaitingOn
Alert if the number of commit log waiting on segment allocation and/or waiting on commit is too high.

Cassandra Compaction PendingTasks
Alert if the number of compaction pending tasks is too high.

Cassandra Datacenter Availability
Alert if the percent of available nodes in a datacenter is too low.

Cassandra DroppedMessage MutationDropped
Alert if there were any dropped mutation messages.

Cassandra JVM Memory HeapMemoryRatio
Alert if the JVM heap memory ratio of used memory to max memory is high.

Cassandra JVM OS SystemCPULoad
Alert if the JVM operating system used physical memory size percent is too high.

Cassandra JVM OS UsedPhysicalMemSizePct
Alert if the JVM operating system used physical memory size percent is too high.

Cassandra JVM OS UsedSwapSpaceSizePct
Alert if the JVM operating system used swap space size percent is too high.

Cassandra Node Availability
Alert if node availability is less than 100%.

Cassandra Node AvgReadLatency
Alert if average read latency for a node is high.

Cassandra Node AvgWriteLatency
Alert if the average write latency on a node is too high.

Cassandra Node LiveDiskSpaceUsedPercent
Alert if the used percent of live disk space on a node is too low.

Cassandra Node PendingCompactions
Alert if the number of pending compactions on a node is too high.

Cassandra Node PendingFlushes
Alert if the number of pending flushes on a node is too high.

Cassandra Node RowCacheMissRate
Alert if the row cache miss rate on a node is too high.

Cassandra SchemaVersion
Alert if schema version is not identical for all nodes.

Cassandra Storage Exceptions
Alert if there are storage exceptions on a node.

Cassandra Storage Load
Alert if the available disc space on a node is small relative to current storage load. This rule is only available in conjunction with the Infrastructure cartridge.

Cassandra Storage TotalHints
Alert if the number of storage total hints on a node is too high.

Cassandra Storage TotalHintsInProgress
Alert if the number of storage total hints in progress on a node is too high.

Cassandra Table AvgKeyCacheHitRate
Alert if the average key cache hit rate for a table across all nodes is low.

Cassandra Table AvgReadLatency

Alert if the average read latency on a table is too high.

Cassandra Table AvgRowCacheHitRate

Alert if the average row cache hit rate for a table across all nodes is low.

Cassandra ThreadPools PendingTasks

Alert if the number of thread pool pending tasks is high.

Cassandra ThreadPools TotalBlockedTasks

Alert if the number of thread pool total blocked tasks is high.

Reports

Cassandra Cluster Summary

Summary of a Cassandra Cluster with availability, disk space, operations, nodes, and largest keyspaces.

Cassandra Cluster Tables

Top Cassandra Cluster Tables by reads, writes, avg read/write latency, or disk space.

Cassandra Node Executive Summary

Executive summary of a Cassandra node with availability and connection info, workload and JVM resource usage, and top alarms.

Cassandra Node Health Check

Health check report for a Cassandra node with availability and connection info, workload and JVM resource usage, and top statements, alarms, and tables.

Cassandra Storage Report

Shows Cassandra server storage capacity, growth rate, etc. Note: Host monitoring must be enabled in order to retrieve space remaining and days remaining until full. Report on all servers that are projected to fill up before this many days. Report on servers with less than this percentage of remaining disk space.