FUJITSU

FUJITSU Software
Cloud Monitoring Manager V2.0.14

Release Notes

July 2021

Contents

About this Manual

This manual describes how system operators can install, operate, maintain, and monitor FUJITSU Software Cloud Monitoring Manager - hereafter referred to as Cloud Monitoring Manager (CMM).

The manual is structured as follows:

Chapter	Description
Introduction to CMM	Introduces CMM, its architecture and users.
Installation	Describes how to install and configure CMM.
Preparations for Application Operators	Describes how to prepare the monitoring environment for application operators.
Operation and Maintenance	Describes the main operation and maintenance tasks for CMM.
Monitoring	Describes the basic tasks involved in monitoring services and servers.
Log Management	Describes the basic tasks involved in managing the log data from the services and servers.
Glossary	Defines the central terms relevant for CMM.

Readers of this Manual

This manual is written for operators who install, operate, and maintain CMM. It also describes how the operators use CMM for monitoring and log management. The manual assumes that you have profound knowledge of OpenStack and CMM, especially the individual services CMM is composed of. For installing the CMM components, you must be familiar with the administration and operation of LINUX systems.

Notational Conventions

This manual uses the following notational conventions:

Notation	Description
`Add`	Names of graphical user interface elements.
`init`	System names, for example command names and text that is entered from the keyboard.
`<variable>`	Variables for which values must be entered.
`[option]`	Optional items, for example optional command parameters.
`one | two`	Alternative entries.
`{one | two}`	Mandatory entries with alternatives.

Abbreviations

This manual uses the following abbreviations:

Abbreviation	Description
CMM	Cloud Monitoring Manager
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
OS	Operating System
OSS	Open Source Software
PaaS	Platform as a Service
SaaS	Software as a Service

Available Documentation

The following documentation on CMM is available:

- *Overview:* A manual introducing CMM. It is written for everybody interested in CMM.
- *System Operator's Guide:* A manual for system operators describing how to install, operate, and maintain CMM. The manual also describes how to prepare the OpenStack platform for CMM and how to use the CMM monitoring functions.
- *Application Operator's Guide:* A manual for application operators describing how CMM supports them in monitoring their services and virtual machines in OpenStack.

Related Information

The following links provide information on open-source offerings integrated with CMM:

- *OpenStack* : Documentation on OpenStack, the underlying platform technology.
- *OpenStack Horizon* : Documentation on the OpenStack Horizon dashboard.
- *Monasca* : Information on Monasca, the core of CMM.
- *Grafana* : Documentation on Grafana, the open-source application used for visualizing metrics data.
- *Kibana* : Documentation on Kibana, the open-source application used for visualizing log data.

Links to more detailed information provided in this manual are subject to change without notice.

Trademarks

Red Hat is a trademark or a registered trademark of Red Hat Inc. in the United States and other countries.

Java is a registered trademark of Oracle and/or its affiliates.

Python and PyCon are trademarks or registered trademarks of the Python Software Foundation.

Other company names and product names are trademarks or registered trademarks of their respective owners.

High Risk Activity

The Customer acknowledges and agrees that the Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter “High Safety Required Use”), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. The Customer shall not use the Product without securing the sufficient safety required for the High Safety Required Use. In addition, FUJITSU (or other affiliate’s name) shall not be liable against the Customer and/or any third party for any claims or damages arising in connection with the High Safety Required Use of the Product.

Export Restrictions

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

1 Main Features

This chapter outlines the main features of this release.

1.1 Multi-Platform Support

CMM comes with a Docker-based installation. Production-ready Docker images are provided for a single-node installation. Docker accelerates deployment and rollback of the individual services CMM is composed of.

CMM follows a multi-platform approach. The Docker-based installation can be used for different OpenStack distributions. CMM supports and has been tested with Red Hat Enterprise Linux OpenStack Platform 16.1.

1.2 Multi Tenancy for Log Management

CMM comes with multi-tenancy support for log management. The log data is securely isolated for each tenant. Access is provided only to the log data of the project to which the tenant is assigned. If a user is assigned to more than one project, the project to be monitored can be selected.

It is not required to configure an index pattern when accessing the log management dashboard in CMM for the first time. Based on a default index pattern, the user can instantly view and analyze his log data.

1.3 Log Metrics

CMM provides alerting features for monitoring the log data. The Log Metrics component consumes log data from the Message Queue, filters the data according to severity, and generates metrics for specific severities, for example, for errors or warnings. The generated metrics are published to the Message Queue and can be further processed by the Threshold Engine.

CMM users can use the log metrics like any other metrics available in CMM. Alarms can be defined as well as notifications that specify how CMM users are informed when a threshold value for the number of warnings or errors is reached or exceeded.

The automation of log handling includes the visualization of log metrics data on the monitoring dashboards. To make it easy to locate problems in huge amounts of log data, the monitoring overview in OpenStack Horizon displays any irregularities in the log data of the monitored system components.

1.4 Preconfigured Metrics Dashboards

CMM ships with preconfigured metrics dashboards that are specially geared to the needs of the system operators.

The dashboards are accessible instantly after installing CMM. The agent installation activates a set of standard metrics. The data collected by these metrics is automatically visualized in the dashboards without the need for manual interaction by the operator.

1.5 Compound Alarm Definitions

To handle a large variety of monitoring requirements, CMM supports compound alarm definitions. Compound alarm definitions combine multiple metrics, thus allowing the user to track and process more complex events.

To facilitate the process of defining alarms, CMM ships with a wizard that leads the user through the definition process step by step. The wizard splits the task of creating alarm definitions into a sequence of three chunks, each of which is presented on a separate page.

The page for defining an expression supports the user with comfortable features for building complex expressions. Subexpressions can be added and connected with AND or OR operators. Subexpressions can be removed, as required. They can also be reorganized within the expression.

Note: Restrictions apply to compound alarm definitions. Please refer to *Restrictions* on page 10 for details.

1.6 Deterministic Alarms

The `deterministic` property for alarm expressions avoids that an alarm status switches to `UNDETERMINED` when no metrics data has been received.

CMM distinguishes between two types of metrics:

- Periodic metrics send data on a regular basis without interruption. In case of an interruption, i.e. there is no more metrics data for the agent to collect, the alarm state changes to `Undetermined`. This ensures that the monitoring user instantly notices that he needs to check why no more data is collected and sent.
- Sporadic metrics are not send on a regular basis. The data is sent only in certain cases, for example, if an error or warning is found in the log data. Expressions related to sporadic metrics can now be marked as `deterministic`. This avoids that the alarm state changes to `UNDETERMINED`.

By default, the `deterministic` property is not set for an alarm expression.

1.7 Notification Engine Plugin System

Monasca Ussuri comes with a plugin system for the Notification Engine. It facilitates the development of plugins for additional notification methods, thus also allowing customers to implement and configure their own notification methods as required. CMM supports the following notification methods: `Email`, `PagerDuty` and `WebHook`.

1.8 Data Retention for the InfluxDB Database

The CMM Operator can configure data retention for the Metrics and Alarms Database. CMM uses the data retention features offered by InfluxDB.

By default, metrics and alarm history data is automatically deleted from the database if it is older than 31 days. This default is set with the installation of CMM. The CMM Operator can either

change the default when installing CMM, or update the data retention configuration at a later stage.

1.9 Data Retention for the Elasticsearch Database

The CMM Operator can configure data retention for the Log Database. CMM uses Elasticsearch Curator for managing data retention of Elasticsearch indices. Elasticsearch Curator jobs are automatically run by a Cron daemon, a time-based job scheduler that executes commands defined in a `crontab` configuration file. The file specifies shell commands for running jobs periodically according to a given schedule.

By default, an Elasticsearch index is automatically deleted if it is older than 31 days. This default is set with the installation of CMM. The CMM Operator can either change the default when installing CMM, or update the data retention configuration at a later stage.

1.10 Areas of Expertise

CMM comes with expertise and know-how in the following areas. This enables product customizations and solutions to meet specific customer requirements.

Log Metrics Component

The Log Metrics component provides metrics for log data to system operators. These metrics support CMM users in checking the severity of their log data.

Additional evaluations for log data can be prepared and configured by the system operator to provide further types of metrics. If you want to customize the Log Metrics component, contact your FUJITSU support organization for information.

Nagios Plugins

The CMM Metrics Agent can run Nagios plugins and send status codes returned by the plugins as metrics to the Monitoring API. Information on how to use Nagios checks in CMM can be obtained from the FUJITSU support organizations.

1.11 CMM Components

This release of CMM is based on the Ussuri version of Monasca.

It is based on the following middleware components:

CMM Component	CMM 2.0
Apache Kafka	V2.11-2.0.11
Apache Storm	V1.2.3
Apache Zookeeper	V3.4.14
Grafana	V7.4.3
Kibana	V7.3.0
Logstash	V7.3.0
Memcached	V1.5.22
logspout	V3.2.13
cadvisor	V0.33
elasticsearch-curator	V5.8.3
docker-ce	V19.03-15-2
docker-compose	V1.27.4

It is based on the following database components:

CMM Component	CMM 2.0
Elasticsearch	V7.3.0
InfluxDB	V1.8.5
MySQL	V5.7.34

1.12 System Environment

Operating Systems

CMM can be installed on a host machine with the following operating systems:

- Red Hat Enterprise Linux 7.7 (for Intel64)

Supported OpenStack Platforms

As underlying platform technology, the following OpenStack platforms are supported:

- Red Hat Enterprise Linux OpenStack Platform 16.1

Supported Web Browsers

CMM has been tested with the following Web browsers:

- Google Chrome 90.
- Microsoft Edge 91.
- Mozilla Firefox 58.

Notes:

- Mozilla Firefox 58:
  When accessing Grafana, a message is displayed: '`Your browser is not fully supported. A newer Browser version is recommended`'. This browser version has been extensively tested. There is no known restriction when using Firefox 58 to access CMM metric information via Grafana.
- All Browsers:
  When accessing Kibana, a message is displayed: '`Your browser doesn't meet the security requirements for Kibana`'. However, this message is not related to browser versions. Security in CMM is ensured: Only users with access to Horizon can successfully use Kibana to access CMM log information. Thus, this message can be safely ignored.

1.13 Documentation

The following documentation is available for this release:

- *Overview:* A manual introducing CMM. It is written for everybody interested in CMM.
- *System Operator's Guide:* A manual for system operators describing how to install, operate, and maintain CMM. The manual also describes how to prepare the OpenStack platform for CMM and how to use the CMM monitoring functions.
- *Application Operator's Guide:* A manual for application operators describing how CMM supports them in monitoring their services and virtual machines in OpenStack.

2 Restrictions

This chapter describes known restrictions of this release.

Update of Alarm Definitions

Update of alarm definitions does not work as expected when updating the following parameters:

- Function
- Time/Times
- Deterministic

If you want to change one of these parameters, pls. delete the existing alarm definition and create a new alarm definition.

Note: Time/Times cannot be specified in CMM UI when you create an alarm definition. If you want to specify values for time/times, please use monasca CLI.

Syntax to create an alarm definition with monasca CLI:

```
monasca alarm-definition-create [-h] [--description <DESCRIPTION>]
[--severity <SEVERITY>]
[--match-by <MATCH_BY_DIMENSION_KEY1,MATCH_BY_DIMENSION_KEY2,...>]
[--alarm-actions <NOTIFICATION-ID>]
[--ok-actions <NOTIFICATION-ID>]
[--undetermined-actions <NOTIFICATION-ID>] [-j]
<ALARM_DEFINITION_NAME> <EXPRESSION>
```

Pls. write `<EXPRESSION>` in quotes.
Simple example:

```
monasca alarm-definition-create TEST-ALARM-DEF
"avg(cpu_perc{hostname=host1},120)>90 times 5"
```

Triggering Alarms for Compound Alarm Definitions

Due to a known issue in the Monasca Threshold Engine, an alarm is not triggered under the following circumstances:

- The alarm expression combines two metrics using OR as a logical operator.
- The threshold value at which an alarm is to be triggered has been exceeded for one metrics, but no metrics data has been received for the other metrics that is combined in the expression.

Accessing the Kibana Dashboard After Switching the OpenStack Project

Errors occur due to problems with browser caching. When you switch to another OpenStack project in OpenStack Horizon and then try to access Kibana, the Kibana dashboard may appear to be not loading properly.

- Workaround: For all browser versions supported: Please use the default options of your browser to reload the page.

Filtering More Than One Element in Kibana Using Firefox

Errors occur due to this known issue in Kibana 7.3.0 Kibana Issue 41567

- Workaround: For filterning more than two elements: Please use the Filter line. Example:

  ```
  hostname: "docker-host" and not (service: "kibana" or service: "logspout")
  ```

Appendix A: Open Source Software

The following Open Source Software (OSS) is included in and used by CMM. The list is restricted to the major OSS projects that are relevant for CMM 2.0:

Software	Description	License	Info
Apache Kafka V2.0.1	A distributed publish-subscribe messaging system. The CMM Message Queue is based on Kafka.	Apache 2.0	Info
Apache Storm V1.2.3	An open-source distributed real-time computation system for consuming streams of data and processing them in arbitrarily complex ways. The CMM Threshold Engine is based on Apache Storm.	Apache 2.0	Info
Apache Zookeeper V3.4.14	A open-source service for maintaining configuration information, naming, providing distributed synchronization, and providing group services. CMM uses Zookeeper for administrating the Message Queue.	Apache 2.0	Info
Elasticsearch V7.3.0	An open-source application that provides a highly scalable full-text search and analytics engine. CMM uses Elasticsearch as the underlying technology for storing, searching, and analyzing log data.	Apache 2.0	Info
Grafana V7.4.3	An open-source application for visualizing large-scale measurement data. CMM integrates with Grafana for visualizing the CMM monitoring data.	Apache 2.0	Info
InfluxDB V1.8.5	An open-source database specifically designed to handle time series data with high availability and high performance requirements. CMM uses an InfluxDB database for storing metrics and the alarm history.	MIT	Info
Kibana V7.3.0	An open-source analytics and visualization platform designed to work with Elasticsearch. CMM integrates with Kibana for visualizing the CMM log data.	Apache 2.0	Info
Logstash V7.3.0	An open-source application that provides a data collection engine with pipelining capabilities. CMM integrates with Logstash for collecting, processing and outputting logs.	Apache 2.0	Info
Memcached V1.5.22	An open-source distributed memory object caching system. CMM uses Memcached for dynamically alleviating the data load that is processed by the log management components.	BSD 3	Info
MySQL V5.7.34	Relational database system used by CMM for storing configuration information, alarm definitions, and notification methods.	GNU GPL V2 w. FOSS Exception	Info
logspout V3.2.13	Log routing for Docker container logs	MIT	Info

cadvisor V0.33	Analyzes resource usage and performance characteristics of running containers.	Apache 2.0	Info
elasticsearch-curator V5.8.3	Elasticsearch Curator helps you curate, or manage, your Elasticsearch indices and snapshots.	Apache V2.0	Info
docker-ce V19.03-15-3	Docker Engine is an open source containerization technology for building and containerizing your applications.	Apache 2.0	Info
docker-compose V1.27.4	Docker Compose is a tool for defining and running multi-container Docker applications.	Apache 2.0	Info