

Oracle® Key Manager 3

Oracle Enterprise Manager for Oracle Key Manager Installation
and Administration Guide

Release 12.1.0.1.0

E53401-02

July 2014

Oracle Key Manager 3 Oracle Enterprise Manager for Oracle Key Manager Installation and Administration Guide, Release 12.1.0.1.0

E53401-02

Copyright © 2007, 2014, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documents	vii
1 Description	
Overview	1-1
Supported Versions	1-2
Prerequisites	1-3
Configuring the OKM Appliance	1-3
Configuring Database-to-OKM / ZFS Storage Appliance-to-OKM Mappings.....	1-3
2 Plug-in Management	
Downloading the Plug-in	2-1
Deploying the Plug-in	2-1
Enabling Java Unlimited Cryptographic Strengths	2-1
Discovering Targets	2-2
Viewing Information About the OKM Cluster	2-3
Viewing Metrics and Reports	2-4
Viewing Metrics	2-5
Communicating Performance Issues	2-5
3 Metrics Collected by the Plug-in	
4 Default Threshold Values	
5 Upgrading the Plug-in	
6 Undeploying the Plug-in	
7 Troubleshooting Monitoring Deployments	
Metric Collection Errors	7-2
OKM KMA Audit Logs	7-2
Host Agent Logs	7-2

A Additional Resources

List of Figures

1-1	Large Enterprise Plug-in Deployment Example	1-2
2-1	OKM Cluster Summary	2-3
2-2	OKM Agent Performance	2-4
2-3	OKM KMA Performance	2-4

List of Tables

3-1	Metric and Collection Information.....	3-1
4-1	Metrics and Default Threshold Values	4-1
7-1	Appliance Problems and Solutions	7-1
7-2	Common Metric Collection Errors	7-2
7-3	Host Agent Logs.....	7-3

Preface

The Oracle Enterprise Manager (OEM) System Monitoring Plug-in extends Oracle Enterprise Manager Cloud Control to add support for monitoring Oracle Key Manager (OKM) storage appliances. This guide provides an overview of the plug-in and how to install and deploy it.

Audience

This guide is written for the Oracle Enterprise Manager Cloud Control administrator. As Cloud Control administrator, you will communicate closely with the OKM storage administrator to discuss performance and analysis of database deployments on the OKM appliance.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle® Key Manager 3 documentation set:

- *Oracle® Key Manager 3 Administration Guide*
- *Oracle® Key Manager 3 Systems Assurance Guide*
- *Oracle® Key Manager 3 Security Guide*
- *Oracle® Key Manager 3 Disaster Recovery Guide*
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle ZFS Storage Appliance, v1.4 Security Guide.*

Description

The Oracle Key Manager (OKM) appliance plug-in for Oracle Enterprise Manager (OEM) Cloud Control provides monitoring for OKM clusters. Each KMA belonging to a cluster is monitored by the plug-in. The plug-in provides the following primary features:

- Gathers and presents key management system, configuration, and performance information for OKM clusters
- Raises alerts for pre-selected configuration and monitoring data
- Ties together Oracle ZFS storage appliances and Oracle databases that use OKM for its encrypted data.
- Supports monitoring by remote agents in the Cloud Control environment.

Overview

The OKM Cluster plug-in for OEM Cloud Control can support a variety of OKM configurations. Before you deploy the plug-in, your planning process should consider the number of OKM clusters and each OKM cluster topology, along with the enterprise monitoring requirements.

Figure 1–1 presents a large hypothetical enterprise including OKM clusters on three continents: North America, Europe, and South America. By presenting a large enterprise example, the diagram demonstrates a variety of possibilities for deploying the plug-in.

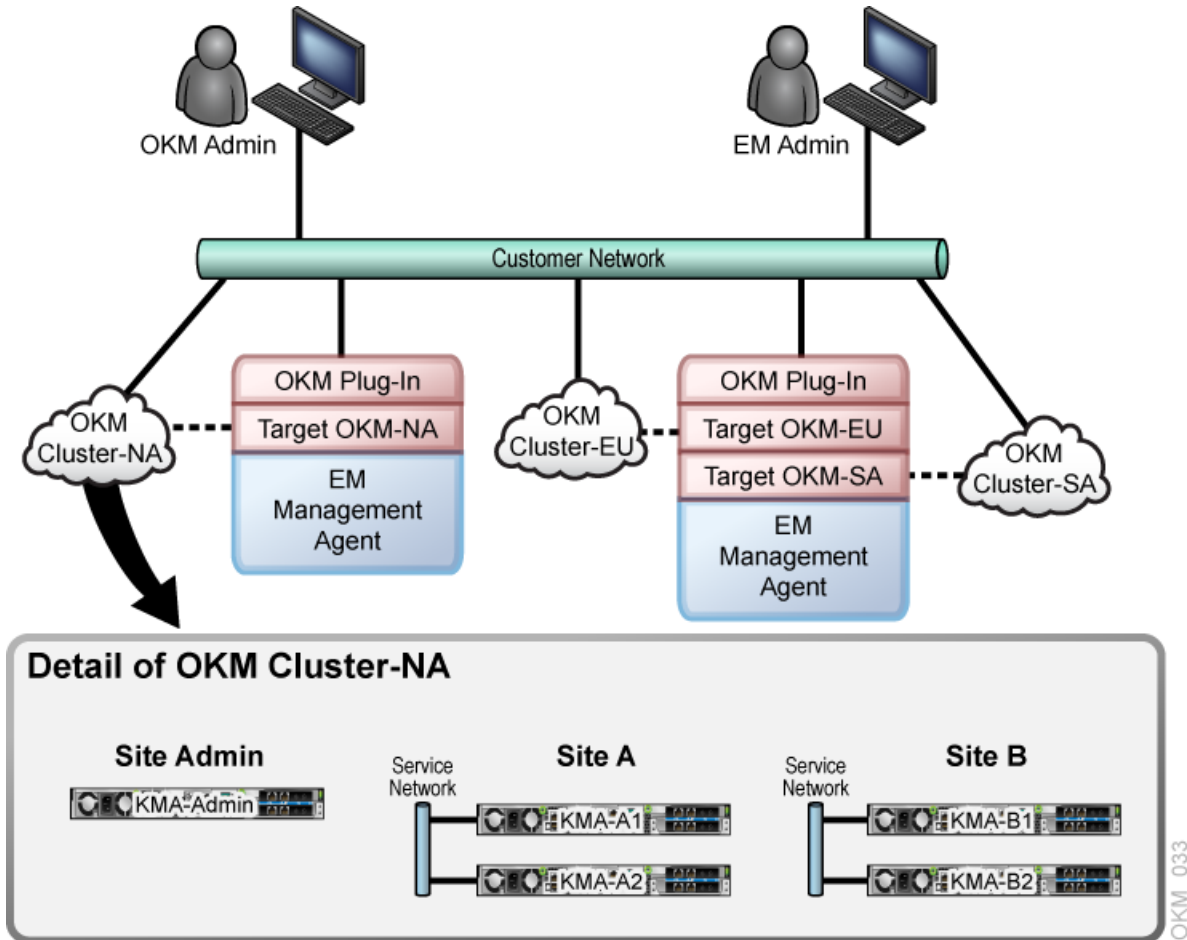
Figure 1–1 shows details for the North America cluster where there are three OKM sites configured:

- An Admin Site that is not servicing any OKM agents
- Sites A and B that service OKM agents with keys.

Sites A and B contain isolated service networks for their agents. Your planning process should consider which KMA within each cluster will be used for the monitoring target.

In this example, the North American cluster uses KMA-Admin as the KMA within the Admin site for the plug-in. This plug-in will be hosted in the Management Agent with the target labeled “OKM-NA.” You can configure other KMAs, but selecting this particular KMA minimizes traffic on KMAs that also service agents. You would need to perform a similar selection process for the other OKM clusters in Europe and South America.

Figure 1–1 Large Enterprise Plug-in Deployment Example



Supported Versions

Deployment of the Oracle Enterprise Manager System Monitoring Plug-in for OKM requires that the following software versions already be installed:

- Oracle Enterprise Manager Cloud Control 12c Release 4 (12.1.0.4.0) or higher (Oracle Management Server and Oracle Management Agent).
- The KMA used to monitor the OKM Cluster must be at Version 2.5.2 or later.

Note: Additional software requirements, such as the correct Java version in Cloud Control, are met through the required applications listed, provided the correct versions are installed. The plug-in can be installed on any operating system in which Enterprise Manager Cloud Control is running.

To enable the plug-in to communicate with the OKM AES-256 encryption key, you must first install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files on Management Agents that the plug-in is deployed to. See ["Enabling Java Unlimited Cryptographic Strengths"](#).

Prerequisites

Before you can deploy the plug-in and monitor OKM appliances, you must:

- Install the Oracle Enterprise Manager Cloud Control environment. Be sure to pay attention to security sections in the *Oracle Enterprise Manager Administrator's Guide*.
- Configure the OKM appliance by creating a new user or utilizing an existing user with an Operator role and exporting its certificates. See "[Configuring the OKM Appliance](#)".
- Review the *Oracle Enterprise Manager Plug-in for OKM Security Guide*.

Configuring the OKM Appliance

For the following procedure, use the Windows version of the OKM GUI if you are running the OKM Manager 3.0 GUI.

1. Create a user with an Operator role. Skip this step if you are using an existing user.
 - a. Log into the OKM Manager GUI as a Security Officer and click **User List**.
 - b. Click the **Create** button.
 - c. In the Create User dialog box, enter the User ID and select the **Operator** check box.
 - d. Under the Passphrase tab, enter the passphrase.
2. Export the Operator's certificates.
 - a. Log into the OKM Manager GUI as an Operator.
 - b. Click **System** and select **Save Certificates**.
 - c. Select **PKCS12** under the Format drop-down.
 - d. Enter a passphrase to use for the exported certificate. Make note of the password for the PKCS#12 file since it will be needed later. Click **OK**.

Note: Both the CA Certificate File Name and the Client Certificate File Name need to be accessible to the Enterprise Manager Agent with the plug-in deployed to it. These files can be saved directly to this location now or copied later before adding the target.

Configuring Database-to-OKM / ZFS Storage Appliance-to-OKM Mappings

In order for reports that include database-to-OKM and ZFS storage appliance-to-OKM mappings to work, the database, the host on which the database resides, and the ZFS appliance must be monitored by Oracle Enterprise Manager Cloud Control. For instructions on monitoring host storage and database instances, refer to the documentation provided with Oracle Enterprise Manager Cloud Control software (see [Appendix A, "Additional Resources"](#)).

Plug-in Management

This section describes how to download, deploy, and use the Oracle Enterprise Manager System Monitoring Plug-in in the Oracle Enterprise Manager Cloud Control 12c environment.

Downloading the Plug-in

You can download plug-ins in online or offline mode. *Online mode* refers to an environment where you have Internet connectivity, and can download the plug-in directly through Enterprise Manager from My Oracle Support. *Offline mode* refers to an environment where you do not have Internet connectivity, or where the plug-in is not available from My Oracle Support.

See the "Managing Plug-ins" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details on downloading the plug-in in either mode:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#CJGBEAHJ

Deploying the Plug-in

You can deploy the plug-in to an Oracle Management Service instance using the Enterprise Manager Cloud Control console, or using the EM Command Line Interface (EMCLI). While the console enables you to deploy one plug-in at a time, the command line interface mode enables you to deploy multiple plug-ins at a time, thus saving plug-in deployment time and downtime, if applicable.

See the "Managing Plug-ins" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for instructions on deploying the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#CJGCDHFG

Enabling Java Unlimited Cryptographic Strengths

To allow the Enterprise Management Agent to communicate with the OKM, you must enable its Java installation for stronger cryptography. First, locate the Java version, then download and install the files for the Java instance.

To find out the Java location and version being used for the Enterprise Management Agent:

1. Log in to the Enterprise Management Agent as the `oracle_user` and locate the file named `emd.properties` in the Enterprise Management Agent's installation directory.

2. Search the file for `JAVA_HOME` and make a note of this location. For example, in file `/export/home/Agent/agent_inst/sysman/config/emd.properties`, there is this entry:

```
JAVA_HOME=/export/home/oracle/Agent/core/12.1.0.3.0/jdk
```

3. Check the Java version. This is needed to know which files to download. To find out the Java version, run `java -version` in `$JAVA_HOME/bin`. For example, using the previous `JAVA_HOME` setting,

```
/export/home/oracle/Agent/core/12.1.0.3.0/jdk/bin/java -version
```

returns

```
java version 1.6.0_43
```

Only the first two numbers are significant (1.6).

4. Download the corresponding Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for that version of Java. Download from the Oracle Technology Network at:

<http://www.oracle.com/technetwork/java/javase/downloads>

For Java 1.6, download Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6; for Java 1.7, download Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7.

<http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html>

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

5. Unzip the download and follow the instructions.

You are instructed to place some files in the Java location specified previously by `JAVA_HOME` in step 2.

6. If the OKM Operator's certificates that were exported are not yet accessible to the Enterprise Management Agent with the OKM plug-in deployed, copy or move them now to a location that can be reached by the Enterprise Management Agent's user ID. These files must also be owned by the Enterprise Management Agent's user ID (who you are logged in as).

Discovering Targets

To install the Oracle Enterprise Manager System Monitoring Plug-in on an Enterprise Management Agent, complete the following steps:

1. Log in to Enterprise Manager Cloud Control.
2. Select **Setup > Add Targets > Add Targets Manually**.
3. Select **Add Targets Declaratively by Specifying Target Monitoring Properties**.
4. In the Target Type drop-down list, select the **OKM Cluster** target type. Click **Add Manually**.
5. For the Monitoring Agent, click **Search**. In the window that is displayed, in the Target Type drop-down list, select **Agent** and from the table below, click and highlight the agent you want to use for monitoring your target. Click **Select**.
6. Click **Add Manually**.

7. Add the Target details and click **OK**. Wait until you see the confirmation and click **OK**.
8. To find the target, click **Targets > All Targets**.
9. Select **OKM Cluster** added above to go to the cluster summary page.

Viewing Information About the OKM Cluster

You access the OEM through a web browser. After you deploy the plug-in, the Oracle Enterprise Manager Cloud Control administrator can view information about the OKM cluster within OEM.

Figure 2–1 shows a summary of the OKM Cluster.

Figure 2–1 OKM Cluster Summary

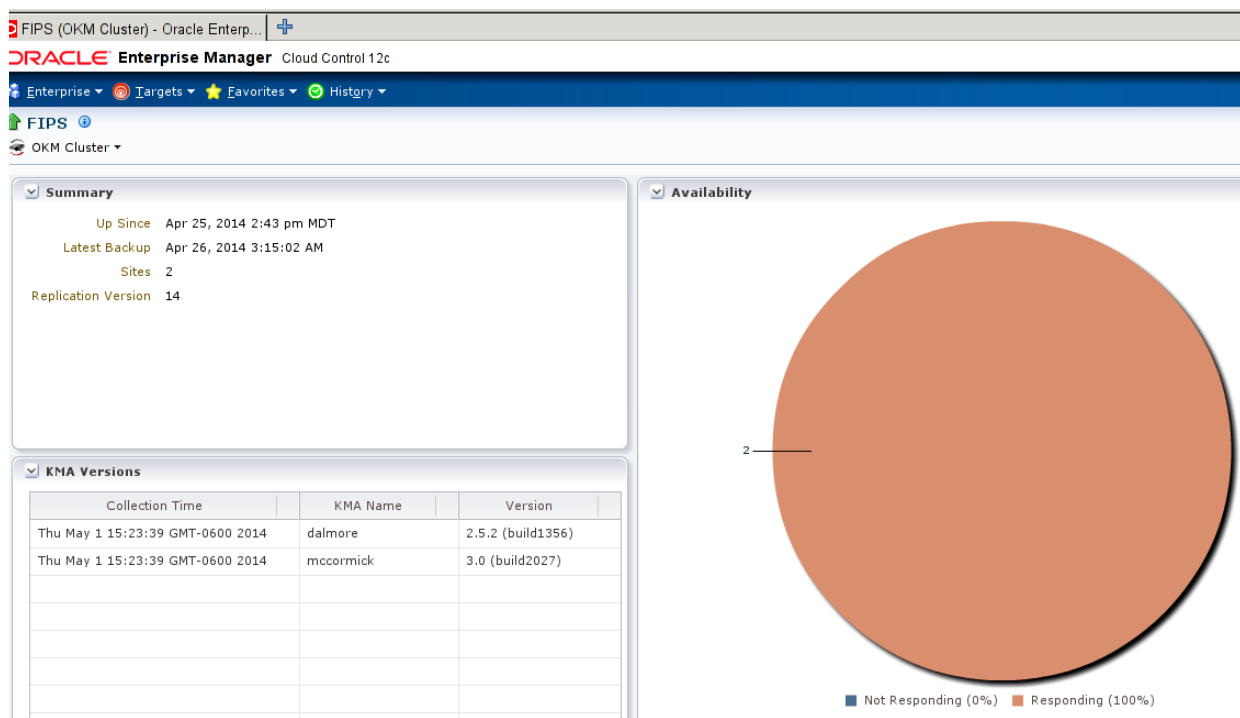


Figure 2–2 shows OKM Agent performance information.

Figure 2–2 OKM Agent Performance

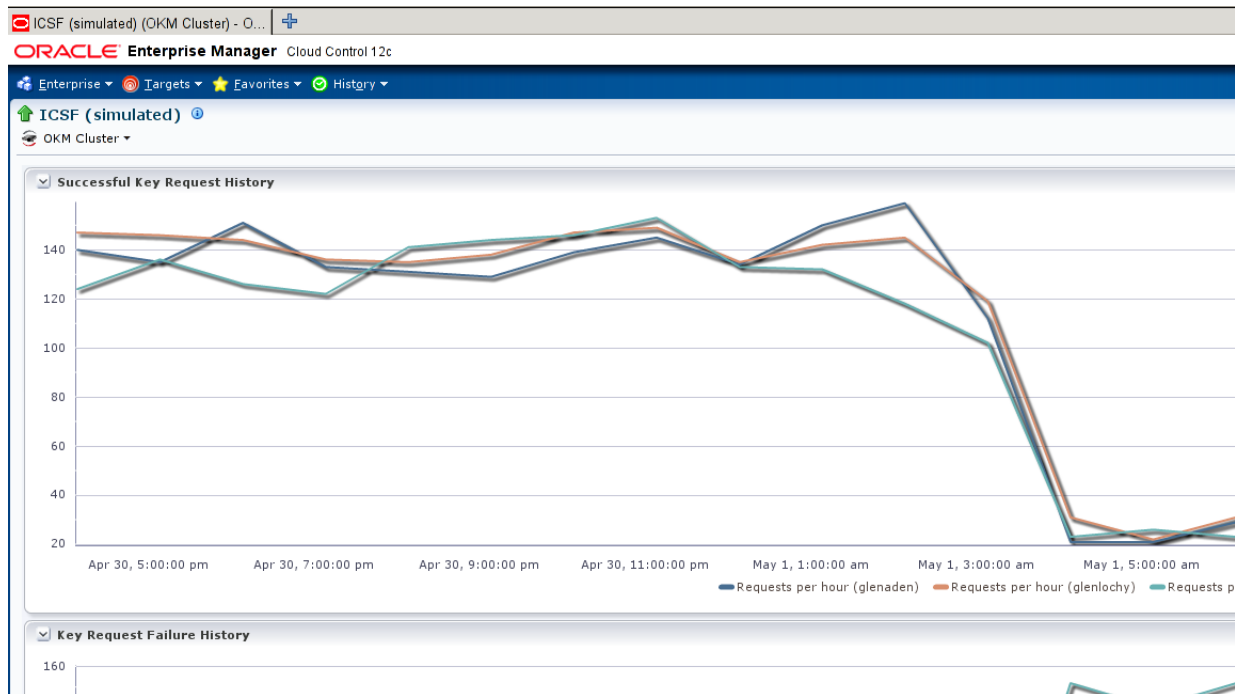
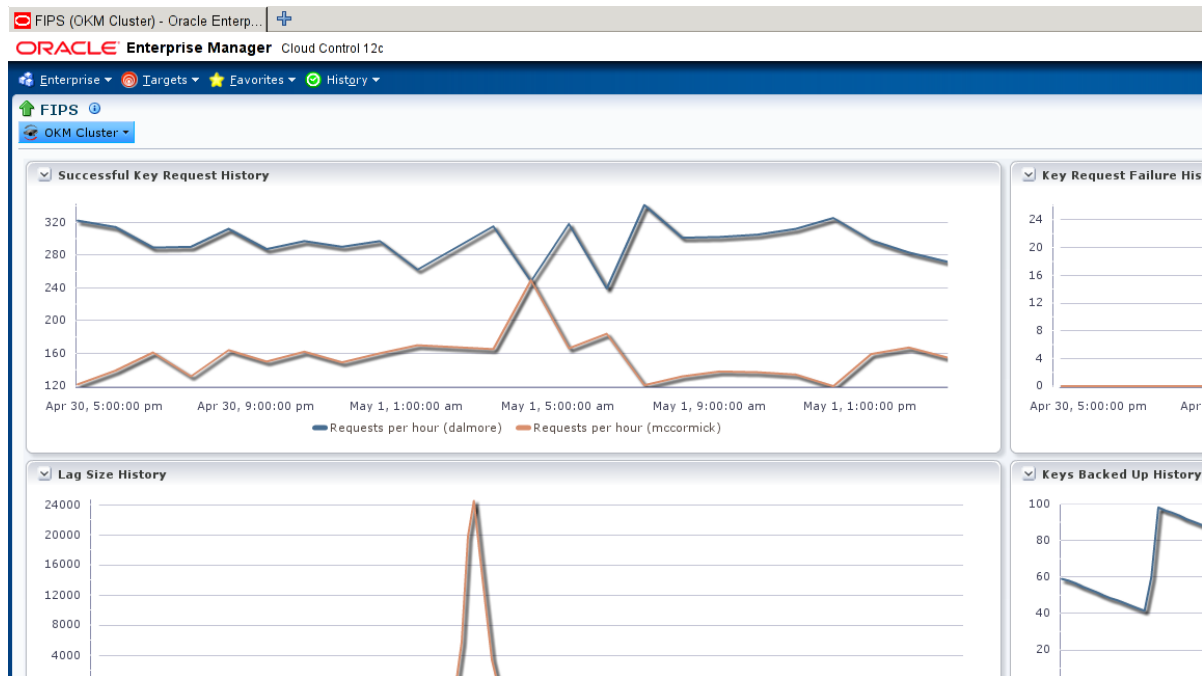


Figure 2–3 shows KMA performance information.

Figure 2–3 OKM KMA Performance



Viewing Metrics and Reports

The primary way to gather information about monitored instances of OKM appliances is viewing metrics. Metrics information is described in [Chapter 3, "Metrics Collected by the Plug-in"](#).

Viewing Metrics

As a rule, more “point in time” information is available in raw metric information than in reports.

To view the raw information collected from the OKM storage appliance:

1. Log in to Enterprise Manager Cloud Control.
2. Go to Targets > All Targets and select the **OKM Cluster** as the target.
3. From the target's home page, select Oracle Key Manager > Monitoring > All Metrics.
4. View the categories and information collected from the last collection interval.

The raw metric information that you have access to can be found in [Table 3–1, "Metric and Collection Information"](#).

Communicating Performance Issues

The most common use of the Oracle Enterprise Manager Cloud Control Plug-in (besides simple capacity monitoring and high-level information collection) is analysis of application performance degradation. Using Oracle Enterprise Manager Cloud Control, you can provide information to the OKM administrator related to performance degradation in the OKM cluster.

In the event of a resource contention issue, you can study levels of client access to determine how and when individual clients are accessing a KMA in the OKM cluster, along with the resources they are accessing.

The plug-in shows a history of security violations, which OKM agents (such as tape drives) are accessing which KMAs the most, and availability history (for example, if a KMA goes down frequently). If an Oracle database or a Solaris 11 server is an OKM client and starts getting failures, then this plug-in can report these failures.

Metrics Collected by the Plug-in

Oracle Enterprise Manager Cloud Control displays a direct mapping of information collected in the target OKM cluster. [Table 3–1](#) shows this mapping information.

Note: Information collected by the System Attributes from the Workflow data set indicates items that cannot be enabled/disabled by an administrator. This information is collected through scripts on each OKM storage appliance.

Table 3–1 Metric and Collection Information

Metric Name	Column	Polling Interval (Minutes)
Response	Status ¹	5
Agent Performance	AgentID ² Requests per hour ¹ Failures per hour Warnings per hour	60
Cluster Status	HSM Status ¹ KMA Name ² Lag Size ¹ Locked status Ready Keys Backed Up (%) Responding Service Responding ¹ Version	10
Configuration	Cluster Information FIPs Mode ¹ Latest Backup Replication Schema Version Sites Unenrolled Agents	1440 (1 Day)

Table 3-1 (Cont.) Metric and Collection Information

Metric Name	Column	Polling Interval (Minutes)
Entity Security Violations	Entity ID ² Violations per Hour	60
KMA Availability	KMAs Not Responding Responding	10
KMA Lock Status	KMAs Locked Unlocked	10
KMA Performance	Requests per Hour ¹ Warnings per Hour KMA Name ² Failures per Hour	60
KMA Security Violations	KMA Nam ² Violations per Hour	60

¹ Conditions Disabled.

² Key Field.

Default Threshold Values

You can set custom thresholds for some metrics within Oracle Enterprise Manager Cloud Control. The alerts received are contained within the product and are not set as Alerts and Thresholds on the OKM storage appliance itself.

Table 4–1 shows metrics that have thresholds set with their default values.

Table 4–1 Metrics and Default Threshold Values

Metric/Columns	Comparison Operator	Warning	Critical	Purpose
Agent Performance/Failures per Hour	>	5	NA	Issued when an OKM client (such as a tape drive or ZFS Storage Appliance) gets many request failures within the last hour.
Agent Performance/Requests per Hour	<	NA	NA	Issued when an OKM client is not sending any requests within the last hour (users can use this to indicate a client that is not encrypting).
Cluster Status/HSM Status	CONTAINS	NA	NA	Issued when the HSM status text matches a certain condition. CONTAINS can be set to "SOFTWARE" to indicate that a KMA is using software for encryption rather than an SCA6000 card (if installed). CONTAINS can be set to "ERROR" to indicate that an error has occurred with either software or hardware encryption.
Cluster Status/Lag Size	>	NA	NA	Issued if the lag size of a KMA gets large. A large lag size indicates a KMA is way behind on updates.
Cluster Status/Ready Keys Backed Up (%)	<	15	1	Issued if the no keys in the ready key pool have been backed up. If the keys have not been backed up and something happens to the cluster, the keys cannot be retrieved and encrypted data will not be able to be decrypted.
Cluster Status/Service Responding	<	NA	NA	Issued to indicate the service network of a KMA is not responding. 1 indicates the service network is responding, 0 indicates it is not responding, and a blank indicates it is not reachable or the response status is unknown.
Configuration/FIPs Mode	<	NA	NA	FIPs mode is 1 if enabled, 0 if disabled. Users can use this to indicate the cluster is not running in FIPs mode.

Table 4–1 (Cont.) Metrics and Default Threshold Values

Metric/Columns	Comparison Operator	Warning	Critical	Purpose
Configuration/Replication Schema Version	<	NA	14	Issued if the cluster replication schema version is downlevel. After an upgrade of the cluster, the replication schema version should set to the maximum.
Configuration/Unenrolled Agents	>	NA	NA	Issued to indicate potential incomplete configuration of a cluster if not all agents have yet enrolled.
Entity Security Violations/Violations per Hour	>	1	5	Issued for an OKM client that has multiple security violations within the last hour.
KMA Availability/Responding	<	2	1	Issued when KMAs in the cluster stop responding.
KMA Lock Status/Locked	>	0	NA	Issued when KMAs are locked. KMAs must be unlocked before they can provide encryption keys.
KMA Performance/Failures per Hour	>	5	NA	Issued when a KMA gets many key request failures within an hour.
KMA Performance/Requests per Hour	<	NA	NA	Issued when a KMA has not provided any keys within an hour. Could be used for performance monitoring.
KMA Security Violations/Violations per Hour	>	1	5	Issued for a KMA that has had multiple security violations within the last hour.

Upgrading the Plug-in

The Self Update feature allows you to expand Enterprise Manager's capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available through the Enterprise Manager Store, an external site that is periodically checked by Enterprise Manager Cloud Control to obtain information about updates ready for download. See the "Updating Cloud Control" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to update the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/self_update.htm

Undeploying the Plug-in

See the "Managing Plug-ins" chapter in the Oracle Enterprise Manager Cloud Control Administrator's Guide for steps to undeploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#CJGEFADI

Troubleshooting Monitoring Deployments

A variety of reasons could cause a monitored instance in the Oracle Enterprise Manager Cloud Control to return information improperly. These issues are typically associated with misconfiguration, incorrect permissions, or changing the configuration within one of the products.

Table 7-1 shows OKM Cluster problems and possible solutions.

Table 7-1 Appliance Problems and Solutions

Problem	Solution
OKM Cluster does not appear to be Up after being added as an instance to be monitored.	<p>An error could have been made when setting up the instance for monitoring, or a change in configuration on the KMA could be affecting communication. Check the following:</p> <ul style="list-style-type: none"> ■ Is the designated DNS name or IP address correct in the asset's Monitoring Configuration? ■ Is the named asset accessible from the Management Agent system? <p>This may be an indication that the timeout setting for the plugin could be increased, especially if the target goes down intermittently. To change the timeouts for the plugin, follow these steps:</p> <ol style="list-style-type: none"> 1. Log into the Management Agent system and navigate to the Management Agent installation directory. 2. Navigate to the <code>agent_inst</code> subdirectory. 3. Navigate to the subdirectory of the named asset. 4. Modify the values for <code>connectTimeout</code> and/or <code>transTimeout</code> in the <code>profile.cfg</code> file located in this directory. No restart of the Management Agent is necessary, the changes will take effect for the next polling cycle.
OKM Cluster is Up, but some items are missing from Summary and/or Performance pages.	<p>You must upload metrics before they can be displayed in the Summary or Performance pages. Metrics can take up to an entire collection cycle (up to 1 day for some metrics) to be uploaded. If the KMA is not responding consistently, this can affect metric collection. See the previous Solution for setting the timeouts for the plugin. Metrics and information about system values are collected in varying intervals. If you have a need for real-time information, refer to the Oracle Key Manager Management GUI.</p>
A Metric Detail is not showing a change made on the system.	<p>Metrics and information about system values are collected in varying intervals. In the worst case, a metric could be as much as 24 hours out of sync with a KMA. If you have a need for real-time information, refer to the Oracle Key Manager Management GUI.</p>
A certificate exported for the OKM Operator is not being accepted.	<p>If this certificate was exported using a 3.0.x Solaris Oracle Key Manager Management GUI, the size of the certificate file is 0. This certificate must be exported using an older GUI, or must be exported from a Windows Oracle Key Manager Management GUI.</p>

Metric Collection Errors

Some common configuration problems manifest as Metric Collection Errors. In some cases, these error messages contain an "Internal Error" followed by a longer Java Exception. The Support Center uses the Java Exception (if the problem is complex). Common Metric Collection problems are as follows in [Table 7-2](#).

Table 7-2 Common Metric Collection Errors

Metric Collection Error	Problem/Solution
No java security providers configured on Management Agent: TLS_RSA_WITH_AES_256_CBC_SHA	<p>Problem: The plugin cannot use AES256, which is required to communicate with OKM.</p> <p>Possible causes: The java used by the Enterprise Manager Management Agent has not been configured to use AES256.</p> <p>Solution: Follow the instructions in "Enabling Java Unlimited Cryptographic Strengths".</p>
1000 Access denied	<p>Problem: The credentials being used to monitor the system are being rejected by the KMA.</p> <p>Possible causes:</p> <ul style="list-style-type: none"> ■ The OKM User may not have an Operator role associated with it, or maybe be Disabled. ■ The certificate files associated with the Monitoring Credentials may be missing or inaccessible to the Management Agent system, or maybe be incorrect or corrupt. <p>Solution:</p> <ol style="list-style-type: none"> 1. Verify the User is configured correctly on the KMA. 2. Follow the instructions in "Configuring the OKM Appliance".

OKM KMA Audit Logs

For detailed debug information, use the audit log on the target OKM KMA.

Note: Debugging the reason that an OKM Agent is not properly collecting statistics from an OKM KMA can be more difficult and should only be done by service personnel. Contact the Oracle Support Center (see [Appendix A, "Additional Resources"](#)).

Host Agent Logs

Most problems (other than version mismatches) occur during the collection of metrics or response information. Look for the following logs on the Enterprise Management Agent host. The Enterprise Management Agent host may differ from the OEM Management Service location. In the following file locations, %AGENT_LOCATION % indicates the home directory of the Agent, typically similar to /export/home/oracle/OracleHomes/agent10g. An asterisk (*) indicates there are several files with additional extensions. [Table 7-3](#) lists host Agent log locations.

Table 7-3 Host Agent Logs

Agent Log Location	Description
%AGENT_HOME%/<targetName>/okmclient*.log	Contains errors that occurred below the Oracle Enterprise Manager Cloud Control framework during attempts to communicate with the OKM cluster. These files will typically contain fine-grained details on connection problems with an OKM KMA or failures that occur while retrieving information.
%AGENT_HOME%/sysman/log/emagent.trc*	These logs also contain connection exceptions and any information on using the data returned from the system to populate database tables.
%AGENT_HOME%/sysman/log/*	Remaining logs will contain finer-grained details on various elements in the Cloud Control Framework and 90% of the issues can be diagnosed with the above.

Note: When interacting with the Support Center or developers within your own help desk, include the emagent.trc* files for reference.

Additional Resources

Use the following links to access information that may be useful to you.

- Oracle Support Center
<http://www.oracle.com/support>
- Patches and updates downloads from My Oracle Support (MOS)
<https://support.oracle.com/CSP/ui/flash.html#tab=PatchHomePage%28page=PatchHomePage&id=g1ws8maj%28%29%29>
- Oracle Key Manager documentation
http://docs.oracle.com/cd/E50985_01/index.html
- Oracle Unified Storage Systems documentation
<http://www.oracle.com/technetwork/documentation/oracle-unified-ss-193371.html>
- *Oracle Enterprise Manager Concepts Guide*
http://docs.oracle.com/cd/B10501_01/em.920/a96674/toc.htm
- *Management of Heterogeneous Data Centers Using Oracle Enterprise Manager Plug-ins* (an Oracle White Paper)
http://www.oracle.com/technology/products/oem/pdf/dc_mgmt.pdf
- Oracle Enterprise Manager Cloud Control 12c documentation, including the *Oracle Enterprise Manager Concepts and Oracle Enterprise Manager Administration Guide*
http://docs.oracle.com/cd/E24628_01/index.htm
- *Oracle Enterprise Manager Cloud Control Upgrade Guide*
http://download.oracle.com/docs/cd/E24628_01/upgrade.121/e22625.pdf
- *Oracle Enterprise Manager, Cloud Control Extensibility Programmers Reference, 12c Release3 (12.1.0.3.0)*
http://docs.oracle.com/cd/E24628_01/doc.121/e25161/title.htm

