Oracle® Communications Session Monitor

Release Notes

Release 3.3.90

E60869-01

April 2015

ORACLE®

Oracle Communications Session Monitor Release Notes, Release 3.3.90

E60869-01

Contents

Preface

This document includes information about this release of the Oracle Communications Session Monitor product family.

The Session Monitor product family includes the following products:

- Operations Monitor
- Enterprise Operations Monitor
- Fraud Monitor
- Control Plane Monitor

Audience

This document is intended for all Session Monitor product family users.

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 that have purchased support 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.

Downloading Oracle Communications Documentation

Oracle Communications Session Monitor documentation and additional Oracle documentation is available from the Oracle Help Center Web site:

- http://docs.oracle.com

Related Documents

For more information, see the following documents in the Session Monitor documentation set:

- *Oracle Communications Operations Monitor User's Guide*: Describes how to use Operations Monitor and Enterprise Operations Monitor to monitor, detect, and

troubleshoot IP Multimedia Subsystem (IMS), Voice over Long-Term Evolution (VoLTE), and next-generation network (NGN) networks.

- *Oracle Communications Fraud Monitor User's Guide*: Describes how to install, configure, and use Fraud Monitor.
- *Oracle Communications Session Monitor Mediation Engine Connector User's Guide*: Describes how to configure and use Mediation Engine Connector.
- *Oracle Communications Session Monitor Developer's Guide*: Describes how to extend the Session Monitor product family by using the Oracle Communications Session Monitor SAU Extension.
- *Oracle Communications Session Monitor Security Guide*: Provides guidelines and recommendations for establishing a secure configuration and implementing security measures for the Session Monitor product family.

Document Revision History

The following table lists the revision history for this document:

Version	Date	Description
E60869-01	April 2015	Initial release.

1

Release Notes

This chapter lists the new and enhanced features, bug fixes, and resolved and known problems in release 3.3.90 of the Oracle Communications Session Monitor product family.

New Features

This section lists new and enhanced features in release 3.3.90 of the Session Monitor product family:

- Record Video Streams and Images with Media Recording
- Capture and Store Subscriber Call Details with Packet Inspector
- Message Flows Display ISDN User Part Binary Content

Record Video Streams and Images with Media Recording

Media recording in Operations Monitor now provides options to record video streams and images, in addition to audio streams and signaling messages.

See "Media Recording" in *Operations Monitor User's Guide*.

> **Note:** The Media Recording feature requires the Packet Inspector feature for recording video streams and images.

Capture and Store Subscriber Call Details with Packet Inspector

Packet Inspector now supports capturing and storing subscriber call details (call data) on the Probe machine.

Operations Monitor now provides the capability to download the call details from the Probe machine to a PCAP file.

See "Downloading Call Details to a PCAP File" in *Operations Monitor User's Guide*.

> **Note:** Packet Inspector requires the use of standalone probes only. Session Border Controller (SBC) probes are not supported for this feature.

Message Flows Display ISDN User Part Binary Content

When a SIP message contains ISDN User Part (ISUP) binary content, you can view the ISUP binary content as human-readable text. The ISUP binary content can be exported in PCAP, HTML, and PDF formats.

See "Viewing Call Event ISUP Protocol Messages" in *Operations Monitor User's Guide*.

Note: You cannot view the ISUP binary content when working with SVG-formatted message flows.

Policy Changes

Oracle no longer approves custom Python and third-party applications.

Caution: When creating your own applications, or using third-party applications, test your scripts in a test environment to ensure they are safe before uploading them to your production environment. Applications approved by Oracle are safe to use in your environments. However, non-approved applications could cause security and performance issues. Oracle is not responsible for any loss, costs, or damages incurred from using your own applications or third-party applications.

Summary of Customer-Reported Fixes

Table 1–1 lists the service request (SR) issues reported and provides a brief description of the resolution.

Table 1–1 Customer-Reported Fixes

Service Request (SR) Number	Bug Number	Description
3-10369760959	19919549	Searching for users within a **realm** took an extensive amount of time when selecting a past period of time. This has been fixed.
3-10365282921 3-10084899648	20720590	In some scenarios, the Voice Quality analysis subsystem was restarted. This has been fixed. The Voice Quality analysis subsystem no longer unexpectedly restarts.
3-10344153401	20617105	Unable to upload the **Global Blacklist** file in Fraud Monitor. This has been fixed.
3-10310687491	20584732	Disappearance of all platform devices in the **Platform Devices** page in General Settings after one or more devices are chosen and all possible realms are selected in the **Select in which realms the device is visible** dialog box. This has been fixed.

Table 1–1 (Cont.) Customer-Reported Fixes

Service Request (SR) Number	Bug Number	Description
3-10307872151	20643394	Unable to display the probe metrics and KPI graphs in Operations Monitor. This has been fixed.
3-10246791661	20505952	Unable to alphabetically order the names of the devices in the **Platform Devices** page in Settings (the default order column is **Name**). This has been fixed.
3-10195332231	20646465	The maximum time to collect traces has been changed from 12 hours to 24 hours.
3-10124120351	20371203	Unable to display platform devices when adding a node panel device KPI to the Dashboard of Mediation Engine Connector. This has been fixed.
3-9885626481	20137566	Unable to export calls older than three days. This has been fixed.
3-9732426438	19815721	Unable to display user pages in user scenarios when a **realm** was not assigned. This has been fixed.
3-9705497956	20561821	Unable to ping a contact IP address, in the **Registrations** table on the **User Tracking** page in Operations Monitor. This has been fixed.

Fixed Known Problems

Table 1–2 lists known problems in previous releases that are now fixed.

Table 1–2 Known Problems Fixed

SR Number	Bug Number	Description
Not applicable	20735311	Diameter messages were ignored in Oracle Communications Control Plane Monitor if the **Terminal Information** AVP did not contain sub-AVPs. This has been fixed.
Not applicable	20520699	The device counter would show an incorrect count value when the **Number of registration attempts with a specific code per second** value was set. This has been fixed.
Not applicable	20352206	The Mediation Engine Connector search function did not retrieve all the saved calls from multiple Mediation Engines. This has been fixed.
Not applicable	20236577	When the deregistration of a contact was set on one segment of a call, all the other registration bindings of the other segments of a call were dropped. This has been fixed.

Table 1–2 (Cont.) Known Problems Fixed

SR Number	Bug Number	Description
Not applicable	20137584	Column widths reset to the original size after paging. Improved the GUI functionality that displays the application results in Operations Monitor.
Not applicable	20102192	The Operations Monitor **Rotate CDR files every N seconds** system setting was incorrectly setting the maximum amount of seconds. This has been fixed.
Not applicable	20093884	The browser time zone was displayed instead of the system time zone on the **Voice Quality** page. This has been fixed.
Not applicable	20093850	Improved the rounding values of the Packet Loss Rate (PLR) in Voice Quality reports. Changed the packet loss calculation to a floating point.
Not applicable	20006921	Improved the blue style and red style add-on color templates for IP tag style customization.
Not applicable	19974689	Improved the DTMF detection in rear call scenarios when call events are introduced in the INVITE messages.
Not applicable	19651916	Improved the Control Plane Monitor transaction handling with DIAMETER_UNABLE_TO_DELIVER (3002) in a call leg scenario.
Not applicable	19323924	Media would not record after the activation of a **Use user domains** setting. This has been fixed.
Not applicable	18973963	When a user entered the wrong password multiple times the deactivation of the user account was permanent. The user account deactivation behavior has been changed to temporary (15 minutes).
Not applicable	18718355	Due to a time zone issue, the System Diagnostics packages were not containing the full data of the requested time range. This has been fixed.
Not applicable	Not applicable	Issue when the Transaction KPI for INVITE contained a 480 reply. This has been fixed.
Not applicable	Not applicable	Alert definitions could be added with an incorrect device name. This has been fixed.
Not applicable	Not applicable	If VLAN was defined, conflicting IP addresses were not detected when adding new devices. This has been fixed.
Not applicable	Not applicable	Media was not recorded for call events when a domain name contained the character "-". This has been fixed to accept the character "-".
Not applicable	Not applicable	In Fraud Monitor, if the mail configuration was incorrect, SNMP traps for incidents were not sent. This has been fixed.

Table 1–2 (Cont.) Known Problems Fixed

SR Number	Bug Number	Description
Not applicable	Not applicable	Improved the functionality in the NEW REST API to retrieve the results of KPIs marked as favorites.
Not applicable	Not applicable	Added a new **Trusted IPs. Often internal IPs, used by Number Determination Sources** field, which is used to add the IP address of a trusted SGW/STP device.
Not applicable	Not applicable	Added the following warning note to the **Enforce stringent password rules** system setting: `Please note that this system setting should not be modified locally in a node that is part of a Mediation Engine Connector.`
Not applicable	Not applicable	Improved the numbering format of the Y axis in charts.
Not applicable	Not applicable	Improved the **Voice Quality** analysis calculation in setups that contain multiple probes.
Not applicable	Not applicable	In some scenarios, Megaco traffic would stop processing. This has been fixed.
Not applicable	Not applicable	Setting a marker bit in the RTP stream, resulted in a packet loss calculation (voice quality). This has been fixed.
Not applicable	Not applicable	During the installation of Control Plane Monitor, the message flow diagram was unable to load. This has been fixed.
Not applicable	Not applicable	In Control Plane Monitor, the transaction state in multi-home scenarios was incorrectly displayed. This has been fixed.
Not applicable	Not applicable	Control Plane Monitor would restart the core process. This has been fixed.

Known Problems

This section describes known problems and workarounds for release 3.3.90.

Upgrading

This section describes workarounds for problems you may encounter when upgrading to release 3.3.90:

- Upgrading from previous installations might take longer than expected.
- Some parts of data migration runs in the background after an upgrade is applied.

Upgrading from Release 3.3.80 to 3.3.90

- The procedure for setting a connection between Session Monitor probes and Mediation Engine has changed.

  To retain the connections between your Session Monitor probes and Mediation Engine after an upgrade, do one the following:

  – If you are using standalone Session Monitor probes:

a. After the upgrade, manually repeat the setup to connect your Session Monitor probes and Mediation Engine. For more information, see "Mediation Engine Connection List" in *Session Monitor Installation Guide*.

b. Download and add the trusted certificates to Mediation Engine. For more information, see "Configuring Encrypted Communication" in *Session Monitor Installation Guide*.

Note: By default, Mediation Engine rejects unencrypted connections.

– If you are using SBC probes, do one of the following:

* If you require secure connections between SBC probes and Mediation Engine, download and add the trusted certificates to Mediation Engine. For more information, see "Configuring Encrypted Communication" in *Session Monitor Installation Guide*.

* If you require unsecured connections between SBC probes and Mediation Engine, select the **Accept insecure connections from remote probes** check box in the **Trusted Certificate** page of Platform Setup Application.

- The IPv6 protocol is supported and the default capturing filters have been modified. If you experience any capturing issues after an upgrade, review the new default filters and settings in the **Media Protocols** and **Signaling Protocols** pages in Platform Setup Application and make changes where applicable.

Upgrading from Release 3.3.70 to 3.3.90

- The configuration to capture traffic has changed. Review the filters and settings in the **Media Protocols** page in Platform Setup Application and make changes where applicable.
- By default the IPFIX connection between SBC probes and Operations Monitor machines enforces secure communication. Check your configuration in the **Trusted Certificate** page in Platform Setup Application and on your SBC probes.

Upgrading from Release 3.3.60 to 3.3.90

- The **RTP recording data retention** system setting has been removed. The data retention of RTP recordings can be configured in the **Data Retention** page in Platform Setup Application.

Upgrading from Release 3.3.40 to 3.3.90

- You cannot directly upgrade from a release older than 3.3.50. If you are using a 3.3.40 version, upgrade to a 3.3.50 version and then upgrade to release 3.3.90.
- For security reasons, the user interface is available only over HTTPS. In some situations, after the upgrade is successfully completed the upgrade dialog will continue to show the running progress bar.

  If the upgrade progress bar does not disappear after 30 minutes of starting the upgrade, refresh the browser window.

Upgrading from Release 3.0 to 3.3.90

- You cannot directly upgrade from a release older than 3.3.50. If you are using a 3.0 version, upgrade to a 3.3.50 version and then upgrade to release 3.3.90.
- The storing of data changed. All call and registration history will be ignored when you upgrade from release 3.0 to a later version.

- When upgrading from a 3.1.X or 3.2.X version, it is possible that within a few hours after the upgrade the performance of the system will be lower and some calls may be lost.