

Oracle Enterprise Operations Monitor

For enterprise IT managers who need to rapidly troubleshoot communications network outages and service degradations, the Oracle Enterprise Operations Monitor enables rapid problem detection, isolation and resolution using unique end-to-end session correlation and real-time analysis capabilities.

Overview

Oracle Enterprise Operations Monitor (EOM) is a service monitoring, troubleshooting and analysis offering that provides unprecedented, real-time insight into enterprise Voice over IP (VoIP) and Unified Communications (UC) network traffic. It enables enterprises to reduce operational costs, increase user satisfaction and accelerate the deployment of communications services.

Enterprise IT managers frequently face problems with communications services that are difficult to detect, isolate and resolve. The resulting lengthy mean-time-to-repair (MTTR) intervals can cause user dissatisfaction, lost productivity, and damage to brand image.

The EOM is specifically designed to help IT staff identify problems anywhere in their complex multivendor communications networks and rapidly resolve them. It is composed of passive probes that monitor and analyze network traffic, plus a Mediation Engine that correlates data and creates a comprehensive, end-to-end view of each session in real-time.

It also helps IT managers troubleshoot call quality issues in real-time with deep drill-down capabilities for both media and signaling – a true differentiator in the market.

Rapid problem detection and isolation

By their nature, problems in IP communications networks can be difficult to detect. They can occur intermittently anywhere along the call path and may affect signaling and/or media portions of a session. The user impact can range from unnoticeable, to a minor impairment, to even a complete service failure. Users may not always report the problem and, once they do, it may already be affecting a large population. Worst, most UC trouble issues are identified by the users before the IT department is even aware of them.

The Enterprise Operations Monitor detects problems in real-time across complex communication networks, including multivendor Unified Communications (UC) and/or Contact Center supporting networks, and issues alerts to IT staff so they can be pro-active. It uses passive probes to monitor and analyze both VoIP and UC communications protocols. Based on its collected data, EOM calculates over 250 key performance indications (KPIs)

Key features

- Real-time, passive VoIP and UC network monitoring
- End-to-end call correlation and analysis
- Fast and accurate problem localization
- Media quality analysis, including R-Factor and MOS scores
- Drill down to view messages per session, including live calls
- Vendor agnostic visibility into SIP, RTP, RTCP and other protocols
- Unparalleled insight into and analysis of signaling messages
- Embedded probes eliminate need for special monitoring equipment
- Cloud-ready with support for deployment on Oracle Cloud Infrastructure and Microsoft Azure

Key benefits

- Reduces MTTR and related operations costs
- Accelerates resolution of complex service provider and UC vendor problems
- Fast IT staff proficiency without training
- Provides full visibility into user activity in real time
- Monitors VoIP and UC networks produced by any vendor
- Rapid deployment without bulk provisioning

that enable the detection of a wide range of problems and provide early visibility into the network's degrading service levels.

EOM provides a granular leg-by-leg view of signaling and media for each session, including sessions in progress. Easy-to-read ladder diagrams enable IT staff to visualize and rapidly isolate problems to a network segment, network element or service provider interface, or to address the optimization of particular call flows where “brownout” situations (congestion induced performance issues) are hindering optimal performance.

Powerful and intuitive user interface

The Enterprise Operations Monitor's graphical user interface (GUI) is so intuitive that most IT staff can become productive in minutes, without any training. It displays data in a powerful hierarchy facilitating rapid drill down, problem isolation and resolution. Color-coded ladder diagrams and MOS graphs help to quickly identify problems, including those which have yet to cause user-noticeable issues.

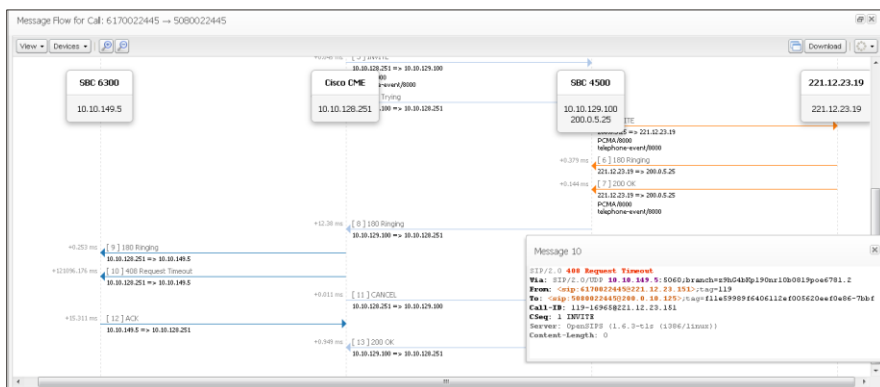


Figure 1. Ladder Diagrams Enable IT Staff to Quickly Visualize and Isolate Problems.

EOM automatically correlates all of the session-based data contain in the associated VoIP/UC messages received from multiple probes to provide a comprehensive view of each session, including sessions spanning multiple protocols. The data is cached by the Mediation Engine, enabling IT staff to look backwards in time to identify the cause and contributing factors of an alert.

Users can define alerts based on a wide range of signaling events, presence related traffic or media quality measurements and automatically create a trace for the traffic leading up to the alarm condition. Alert conditions can generate an SNMP trap or notify staff via email that includes the trace.

The EOM's dashboard features display panels that can be customized by each user to provide at-a-glance visibility to their most important metrics. EOM can monitor aggregate network activity, such as active calls and registered users, and performance data for specific network elements, trunk interfaces and endpoint devices.

True, real-time media analysis

Media quality problems can be introduced at any point along the call path, making them difficult to isolate and resolve. In addition, user complaints about call quality can be subjective and difficult to interpret. The Enterprise Operations Monitor's features real-time media monitoring and analysis tools

New features in latest releases

- Support for deployment on public cloud
- Monitoring support for non-call events:
 - Subscribe
 - Notify
 - Publish
- A more robust KPI definition framework
- Improved EOM performance
- An all new GUI allowing faster navigation and improving ease of use

“EOM allows us to go back in time and understand immediately what was happening in our network right before a problem occurred. That's invaluable and decreases our MTTR exponentially.”

José Pedro Corchón
Voice Systems,
Gneis Global Services
Bankinter

that enable IT staff to rapidly isolate and resolve a range of problems, such as one-way audio and codec mismatches.

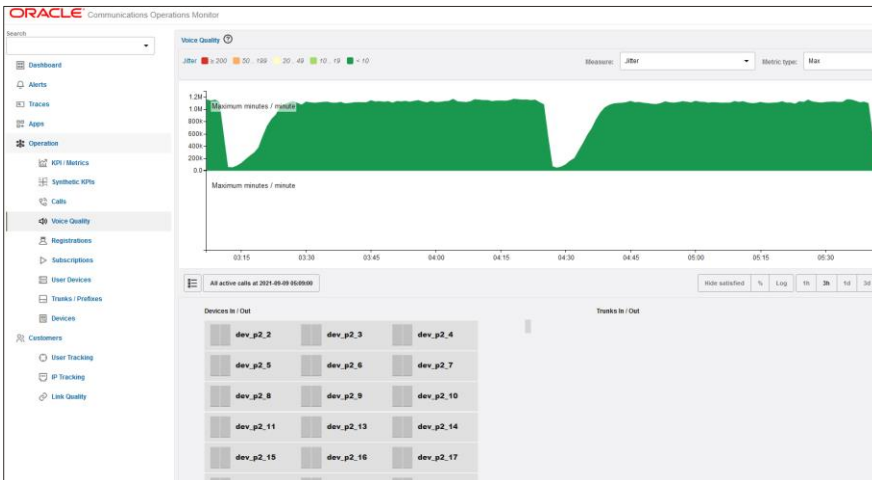


Figure 2. An Example of QoS Visualization.

EOM combines RTCP data provided by end-points with media quality measurements collected by its network probes to produce a detailed media analysis, including MOS scores. These probes enable problem localization by providing a QoS empirical analysis at both end-of-call reporting and at 10 second intervals for specific network segments. A color coded display enables staff to quickly identify poor media quality and drill-down from trunks to sessions. Packet loss rate, jitter and other detailed data can be analyzed per session.

EOM can record selected user sessions, enabling IT staff to listen to the same audio heard by the user and more rapidly debug probes. EOM also features DTMF and T.38 fax detection for visibility into IVR interactions and fax transmissions.

Highly scalable architecture

A flexible modular architecture makes the Enterprise Operation Monitor's highly efficient, cost-effective to deploy, and easily scalable from a mid-sized, single data center environment to a very large, geographically distributed enterprise.

Probes collect and forward signaling information to a central Mediation Engine for correlation and analysis, while media flows for each session are analyzed locally. Metadata is forward to the Mediation Engine to optimize bandwidth efficiency and scalability.

Probes are embedded in the Oracle Enterprise Session Border Controllers (E-SBC) and the Enterprise Communications Broker (ECB) for visibility into critical trunk connections. E-SBC probes also provide visibility into media quality on encrypted sessions. All EOM licenses include probe software that can be deployed on standalone x86 servers, providing flexibility to monitor additional network segments.

In geographically distributed networks, multiple Mediation Engines may be deployed to monitor the probes within each region. Optional Mediation Engines may be deployed to monitor the probes within each region. An optional Mediation Engine Connector provides a global dashboard through the same intuitive user interface.

“It’s really about being proactive. The alarming and end-to-end troubleshooting tools help us identify and resolve issues before they impact our customers.”

James Rubio
Manager,
EBS Technology
Infrastructure
INTUIT

Related products

- Oracle Enterprise Session Border Controller
- Oracle Enterprise Communications Broker
- Oracle Communications Session Delivery Manager
- Oracle Session Delivery Management Cloud

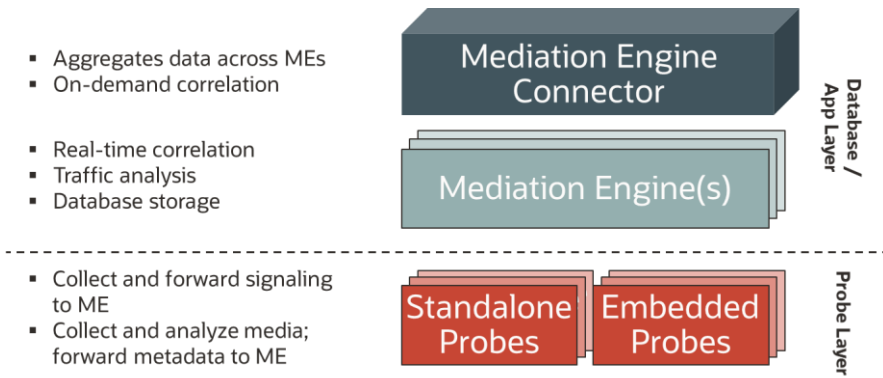


Figure 3. Mediation Engine Overview.

Features

FEATURE	DESCRIPTION
Multiple site and multiple protocol call correlation	Calls are correlated and analyzed across multiple network sites and protocols providing full, end-to-end visibility into the network. Users can filter and analyze data for a single call – identifying the caller and call recipient, their IP addresses, number of call segments, call flow diagram, call status, and all detailed call information – as it traverses the entire network.
Key performance indicator analysis	Over 250 KPIs monitor service accessibility, retention, and integrity. KPIs can be aggregated by service, site, and user. All KPIs can be accessed in real-time by a Simple Network Management Protocol (SNMP) manager and an optional REST API.
Session tracing	Real-time and historical call and transaction tracing facilities, with drill-down to ladder diagrams showing signaling transactions and media flows for each call across the entire network. Each leg of the call can be viewed and analyzed.
Network alerts	A highly flexible alert function can notify IT staff when specific KPI thresholds are crossed, including poor MOS quality or slow signaling responses. Arithmetic operators can generate alerts by comparing multiple metrics. Alerts can be exported to network management systems with SNMP traps.
Call logs	Active and completed calls transiting any part of the monitored network are logged and a filter capability can identify problematic calls for further analysis. The log enables IT staff to easily browse the network.
Packet decoding and filtering	Decodes the full protocol exchange between each network element in a session for a complete packet-by-packet view that enables better troubleshooting and problem isolation. EOM provides overall packet loss and the frequency of packet losses (Burst packet loss) so IT staff can better understand the impact on voice and video quality.
In-depth, root cause analysis	Enables users to drill down from the network level to the signaling level and localize problems to an element, customer, device type or end-user. Bidirectional data capture enables IT staff to quickly pinpoint the network segment where a message has not been sent and which party was affected.
Live user search	Live and historical user sessions can be searched using partial phone numbers or IP addresses. Search results present a list of all users associated with an IP address, their SIP URIs, and a list of sessions, including those in progress. IT staff can drill down on any displayed element to access signaling information and call detail records.
Reports and exports	A range of reports and file exports facilitate troubleshooting with third parties, such as service providers, UC vendors, and other enterprise departments. Flexible call reports can be created in PDF format that include the full details of protocol messages, ladder diagrams, media quality measurements and more. Selected traces can be exported in packet capture (PCAP) format. Optionally, EOM can generate call detail records (CDRs) in .CSV format for use with third party systems and via bulk exports in file archive format.
High availability	1:1, Active/Active Mediation Engine configuration support with probe sharing.

Specifications

FEATURE	DESCRIPTION
Protocols	SIP, RTP, SRTP, RTCP-XR, H.248/MEGACO, ENUM, MGCP, and IPv4 transport is supported for all protocols and IPv6 is supported for SIP and RTP.
Probes	Passive probes are embedded in Oracle's E-SBCs and Enterprise Communications Broker (ECB), and standalone passive probe software may be installed in any Intel 64-bit x86 compatible server using Oracle Linux or Red Hat Enterprise Linux operating system.
Probe-to-me communications	IETF IPFIX. All communications between probes and Mediation Engines can be encrypted.
External interfaces	SMTP email client, SNMP v3 client, and LDAP authentication client.
Deployment	Supports on-premises hardware, virtual machines (VM), and public cloud infrastructure VMs deployments.
Non-call events monitoring	EOM supports monitoring of non-call presence events such as subscribe, notify, and publish. Users can monitor these traffic parameters and define alerts and use a number of KPIs, specifically, to monitor non-call events.

Optional extensions

FEATURE	DESCRIPTION
Mediation engine connector (MEC)	Enables the aggregation of data from across multiple Mediation Engines (ME). When sessions span multiple monitored partitions, the MEC correlates those sessions and presents an end-to-end view. The MEC also aggregates metrics and KPIs, and enables further traffic analysis by providing both a global user-search and the RESTful API's GET capability.
Application support extension	Enables applications, both customized and in-built, to query information from the EOM, process it and store the results in an output table. It allows applications full access to all of the internal, real-time and historic data structures. The extension runs in a secure sandbox environment, and provides an application development environment independent of EOM's own development roadmap.
REST remote API extension	Both the ME and MEC make available via the RESTful API GET method historical call and session active user information, for further analysis by third-party systems. This data includes raw and aggregated data such as traces, calls, registrations, KPIs and user experience information.
CDR generation extension	Enables the generation of preliminary CDRs for successful and failed calls in .CVS format. These CDRs can be accessed remotely using an interface for FTP or SFTP-based GUIs, and can include all of the EOM's internal call related details.
Gateway Control Protocol	Enables support for H.248/MEGACO, and Media Gateway Control Protocol (MGCP).
ENUM protocol	Enables support for the ENUM protocol
Oracle Fraud Monitor (FM)	To identify fraudulent calls, FM uses ME's real-time data to build an end-to-end, correlated, network-wide session model. It then analyzes the model to determine user behavior, and compares it with individual learned behavioral patterns. Fraud incidents can be identified and alerts issued, allowing Enterprises to take evasive action including the disabling of users and trunks via their Enterprise Session Border Controllers. Other responses might include redirecting users to call analysts, to systems like voicemail, or in rate limiting their traffic.

Connect with us

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com). Outside North America, find your local office at: [oracle.com/contact](https://www.oracle.com/contact).

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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. 1121