ORACLE

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 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.

Oracle Enterprise Operations Monitor 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.

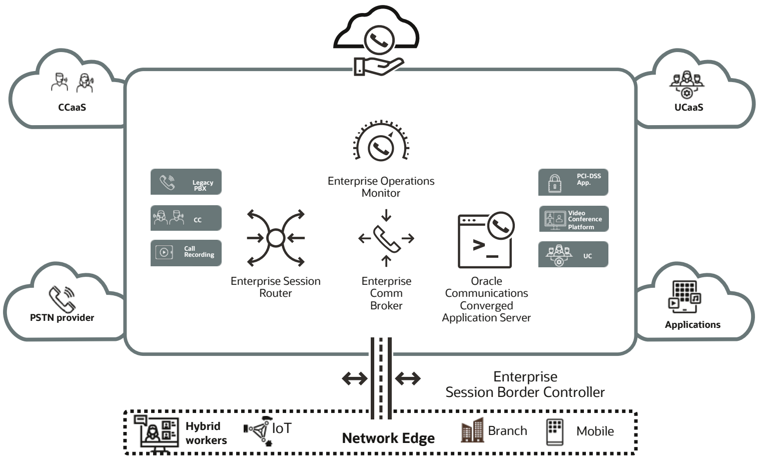

CCaaS
UCaaS
Enterprise Operations Monitor
Legacy PBX
CC
Call Recording
PCI-DSS App.
Video Conference Platform
UC
Enterprise Session Router
Enterprise Comm Broker
Oracle Communications Converged Application Server
PSTN provider
Applications
Enterprise Session Border Controller
Hybrid workers
IoT
Network Edge
Branch
Mobile

Figure 1. Enterprise Operations Monitor plays a key role in communication network monitoring.

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.

Enterprise Operations Monitor

Key features

- Real-time, passive VoIP and UC network monitoring
- Monitor MS Teams direct routing call
- 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, Amazon AWS, Google Cloud Platform and Microsoft Azure
- Optionally FIPS 140-2 compliant

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 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.

Oracle Enterprise Operations Monitor detects problems in real-time across complex communication networks, including multivendor Unified Communications (UC), Contact Center and UCaaS*1 supporting networks, and issues alerts to IT staff so they can be pro-active. It uses passive probes and UCaaS API access to monitor and analyze both VoIP and UC communications protocols. Based on its collected data, it calculates over 250 key performance indications (KPIs) that enable the detection of a wide range of problems and provide early visibility into the network's degrading service levels.

> "Enterprise Operations Monitor 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."

Global banking customer

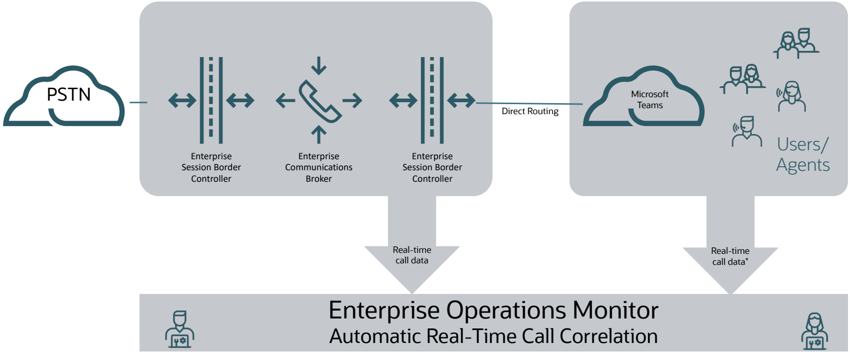

PSTN
Enterprise Session Border Controller
Enterprise Communications Broker
Enterprise Session Border Controller
Direct Routing
Microsoft Teams
Users/ Agents
Real-time call data
Real-time call data*
Enterprise Operations Monitor
Automatic Real-Time Call Correlation

Figure 2. Enterprise Operations Monitor collects call data for the complete communications flow.

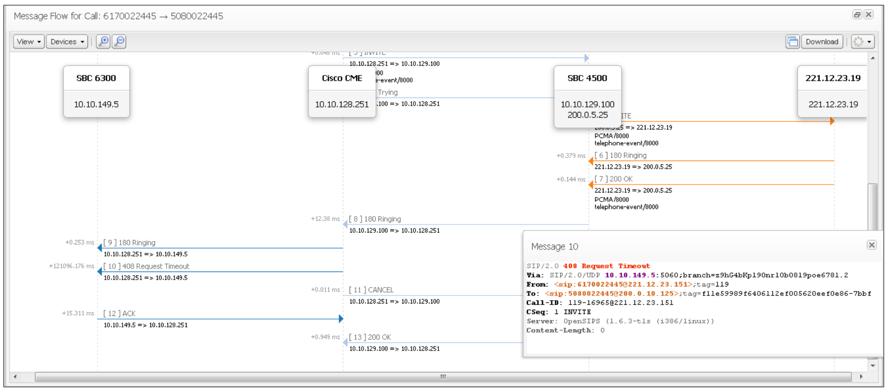
Oracle Enterprise Operations Monitor provides a granular leg-by-leg view of signaling and media for each session, including sessions in progress. Easy-to-read ladder diagrams enable IT staff to visualize and rapidly isolate problems to a network segment, network element or service provider interface, 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

Oracle 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.

Oracle Enterprise Operations Monitor 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.

*1 Microsoft Teams



```
SIP/2.0 408 Request Timeout
Via: SIP/2.0/UDP 10.10.149.5:5060;branch=z9hG4bKpl90nrl0b0819poe6781.2
From: <sip:6170022445@221.12.23.151>;tag=119
To: <sip:5080022445@200.0.10.125>;tag=f11e59989f6406112ef005620eef0e86-7bbf
Call-ID: 119-16965@221.12.23.151
CSeq: 1 INVITE
Server: OpenSIPS (1.6.3-tls (i386/linux))
Content-Length: 0
```

Figure 3. Ladder Diagrams Enable IT Staff to Quickly Visualize and Isolate Problems.

> "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."
>
> Global System Integrator

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.

Oracle Enterprise Operations Monitor's dashboard features display panels that can be customized by each user to provide at-a-glance visibility to their most important metrics. It 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 that enable IT staff to rapidly isolate and resolve a range of problems, such as one-way audio and codec mismatches.

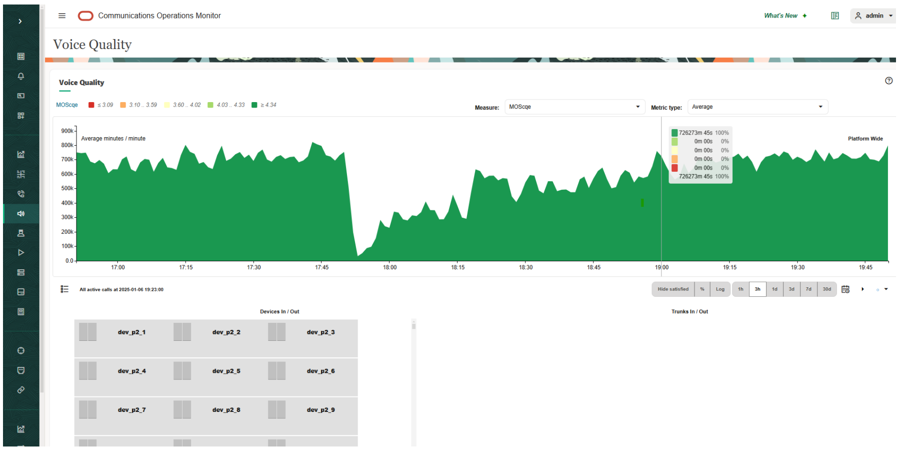


Figure 4. An Example of QoS Visualization.

Oracle Enterprise Operations Monitor combines RTCP data provided by endpoints 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.

Related products

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

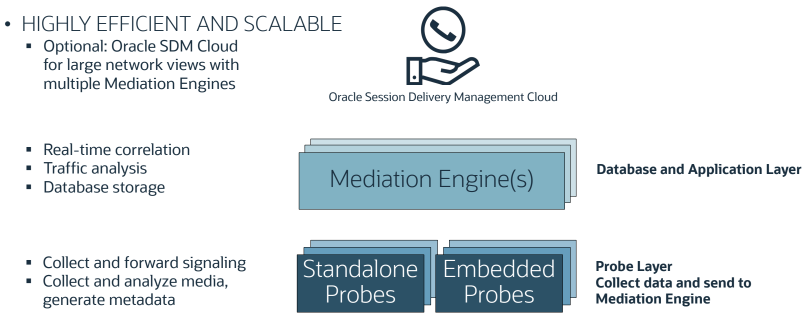
Highly scalable architecture

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 and the Enterprise Communications Broker for visibility into critical trunk connections. The Enterprise SBC probes also provide visibility into media quality on encrypted sessions. All Oracle Enterprise Operations Monitor 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.



• HIGHLY EFFICIENT AND SCALABLE
▪ Optional: Oracle SDM Cloud for large network views with multiple Mediation Engines
Oracle Session Delivery Management Cloud
▪ Real-time correlation
▪ Traffic analysis
▪ Database storage
Mediation Engine(s)
Database and Application Layer
▪ Collect and forward signaling
▪ Collect and analyze media, generate metadata
Standalone Probes
Embedded Probes
Probe Layer
Collect data and send to Mediation Engine

Figure 5. Mediation Engine Overview.

Security

When installed on FIPS 140-2 approved platforms, Enterprise Operations Monitor can be installed in FIPS 140-2 mode making the application FIPS compliant. Detailed information is available in documentation.

For enhanced privacy, exports can obfuscate sensitive data helping enterprises to be compliant.

Enterprise Operation Monitor also supports monitoring of Stir/Shaken traffic.

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

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. Enterprise Operations Monitor 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, it can generate call detail records (CDRs) in .CSV format for use with third party systems and via bulk exports in file archive format. Obfuscation of security sensitive fields is available.
High availability	1:1, Active/Active Mediation Engine configuration support with probe sharing.
FIPS 140-2 compliant	When installed on FIPS 140-2 certified platforms, Enterprise Operations Monitor can be installed within FIPS 140-2 compliancy

Specifications

FEATURE	DESCRIPTION
Protocols	SIP, RTP, SRTP, RTCP-XR, H.248/MEGACO, ENUM, MGCP, HTTPS (Stir-Shaken), and IPv4 transport is supported for all protocols and IPv6 is supported for SIP and RTP.
Probes	Passive probes are embedded in Oracle's Enterprise SBCs and Enterprise Communications Broker, 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	Oracle Enterprise operations Monitor 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.
UCaaS Monitoring	Allows monitoring MS Teams direct routing calls giving and end-to-end correlated view along with ability to filter UCaaS calls and monitor KPIs

Optional extensions

FEATURE	DESCRIPTION
UCaaS Monitoring extension	Enables to integrate with UCaaS APIs (Microsoft Teams) to gather call details for direct routing calls (MS Teams > SBC > PSTN or vice versa) and correlates with the SBC leg of the call. Thereby, provides end-to-end visibility into direct routing calls for faster and enhanced troubleshooting
Mediation engine connector	Enables the aggregation of data from across multiple Mediation Engines. When sessions span multiple monitored partitions, the Mediation Engine Connector correlates those sessions and presents an end-to-end view. It 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 monitoring database, 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 Enterprise Operations Monitor own development roadmap.
REST remote API extension	Both the Mediation Engine and Mediation Engine Connector 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 monitor'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.
Stir-Shalen traffic	Enables monitoring of Stir-Shaken traffic.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle