for
Microsoft Lync™
Unified Communications is an ideal solution for many enterprises around the world, and Microsoft Lync™ is at the heart of facilitating the migration with their seamless desktop integration, feature rich communication and collaboration capabilities that combines voice, video and instance messaging with the power of presence.

Post deployment Microsoft Lync™ presents a unique challenge to administrators when it comes to management. The distributed architecture and application specific functions create a gap between the network, server and voice teams.

AnalytiX provides a holistic view into the Microsoft Lync™ ecosystem, taking into account all servers, services and network resources that impact the applications performance and user quality of experience. AnalytiX combines the LayerX real-time multi-vector correlation, Active Agents, Raptor Path Analyzer and vendor best practices to provide administrators with insight into areas needing remediation.

Monitoring Network Health and Key Performance Indicators

Network metrics can be measured by using stand-alone tools such as ping.exe, or by using advanced synthetic agent testing tools such as LayerX Raptor. The Lync Server itself takes advantage of the RTP/RTCP protocols, which samples network measurements on the voice and video call data. Combined with Quality of Experience (QoE), the Lync Server offers a robust source of network metrics spanning every network segment that carries Lync traffic. The Lync QoE network metrics are also the most accurate of their kind, and for this reason, LayerX uses a combination of network metrics produced by the Lync Call Server, our active agent and LayerX Raptor path analyzer to enable administrators to improve on the mean time for resolution.

Desktop Client Monitoring

Desktop Client health monitoring is feasible only for very limited scenarios because client configuration and runtime behavior are within the unmanaged space. The Quality of Experience (QoE) metrics provide post call telemetry on certain aspects of client runtime performance, such as CPU load and system resources after the call has completed. However, by implementing the LayerX active agent and Raptor, administrators are notified immediately to guide users towards making better choices that improve a users experience.

Another useful attribute of the LayerX active agent is simplified troubleshooting of client sign in issues. The active agent eliminates the need to RDP into the users machine to analyze log data; instead log data is streamed to a central repository where advanced correlation rules profile the sign in issues by category.

Lync Proactive testing

AnalytiX can be configured to run periodic system tests to determine the status of various AVM modules. For example: an administrator can be notified if a pair of users are having issues participating in an application sharing conference. Also a test is configured to verify that a user can connect to Exchange Unified Messaging and is able to leave a voice mail message for another user. AnalytiX incorporates a number of useful proactive elements to keep every administrator a step ahead.

AnalytiX Device Alarms

AnalytiX’s Knowledge Base (Policy Module) provides an instant look-up of recommended actions to resolve Lync specific alarms generated by each specific component. The Policy Module includes all the Microsoft Lync specific recommended actions and also provides administrators the ability to add, modify the priority of an alarm or even trigger an automated Incident Response Procedure (IRP). A simple but useful IRP could be restarting a stalled service or running a diagnostic trace. Other useful attributes of AnalytiX device alarms are:

- Alarm trending for recurring issues with a device.
- Centralized log collection with the ability to search through millions of events.
- Create custom dashboards with any of the collected log data.

AnalytiX with SDN API 2.0

The Lync SDN API is a software component developed by Microsoft. The API provides an interface to LayerX AnalytiX to access Lync network diagnostic information about Lync voice, video, desktop sharing and file transfers.
AnalytiX for Microsoft Lync delivers advanced CDR, Capacity reporting, Performance, Traffic Analysis

Microsoft Lync Server 2013 natively includes a Monitoring service, which provides the ability to collect and store Call Detail Records (CDR’s). Enabling this feature will configure Lync to record Lync usage across the entire media stack including peer-to-peer calls and all types of conferencing for all users. The bigger challenge is making sense of all CDR information captured in the database.

An extensive library of customizable reports puts this data into context and includes reports like:

- Worst Performing Endpoints
- Device reports
- QoS – Packet Loss, Jitter, MOS
- Server Performance
- Fault Summary
- Call Diagnostic
- Conference Diagnostic
- Media Quality
- Toll Fraud Alert report
- Call Detail Report

Some of the key elements monitored and alerted on:

- SIP error response rate
- Service state - Server Audio Test Service
- Service state - Server File Transfer Agent
- Service state - Server Front-End
- Service state - Server IM Conferencing
- Service state - Server Master Replicator Agent
- Service state - Server Replica Replicator Agent
- Active SIP Connections
- Active SIP TLS Connections
- Average Outgoing Queue Delay
- Average Flow-Control Delay
- Incoming SIP Requests/Sec
- Incoming Messages/Sec
- Events in Processing
- Active Conferences
- Connected Users by modality
- Throttled SIP Connections
- IM MCU Health and Performance
- User DataBase Queue Latency (msec)
- User DataBase Stored procedure Latency (msec)
- Number of failed connection attempts/Sec
- Round Trip custom threshold alerting
- Poor call custom threshold alerting
- Low memory, disk utilization and high CPU threshold alerting
- Support for SBC’s and Gateways – Sonus, ACME Packet, AudioCodes
- Multivendor support for Avaya, Cisco, NEC, ASPECT

AnalytiX provides administrators the ability to:

- Collect large volume of logs, correlate, alert and remediate when possible
- Puts your machine data into context
- Function specific dashboards for different stakeholders
- Leverage QoE data, event and error logs, SDN data, and LayerX active agent messages
- Use LayerX Raptor to determine call path and network statistics
- Real-time alerting on all Lync error codes with remediation steps