Zenoss Insight Suite

SOLUTION BRIEF

Your IT systems
are producing massive
amounts of data.
How can you unleash that
data to empower your business?

zenoss
Own IT.

Zenoss Insight allows you to take advantage of all of the big data your systems are producing.

You can stream, push, or have Zenoss Insight **proactively collect any data format you want** – both structured and unstructured.

Letting you monitor, analyze, **and make full use of your data resources** across all of your systems to drive real business value.

Executive Summary

CHALLENGE

Lateral (or "east-west") monitoring has become an increasingly critical component of overall IT service assurance. As companies seek to understand the performance of an entire service transaction, from its point of origin all the way through to its conclusion, many systems of record are being exploited to gain insight. Among the most prevalent are log files and network traffic flow (NetFlow) data. These data sources provide detailed information about a wide range of applications typically running on an enterprise network, such as latency-sensitive voice and video traffic or mission-critical business services. However, legacy network monitoring tools only provide basic network fault and availability monitoring and fail to deliver the fundamental insights IT operations needs to understand application performance and actual network traffic patterns. Unfortunately, many modern log file analytics tools also prove frustrating because they force companies to make trade-offs due to their high cost per log volume, which limits the ability to look at all relevant data.

OPPORTUNITY

The Zenoss Insight suite of solutions is different. It allows you to take advantage of all of the data your IT systems are generating, adding greater contextual detail to the infrastructure quality and performance details you already receive from the Zenoss Service Dynamics platform. These tools can provide deep log file analytics, unified communications monitoring and management, and granular network performance details that can greatly improve overall service quality while simultaneously accelerating issue detection and remediation efforts.

BENEFIT

Real-time data analysis is a growing need for modern businesses as the rate at which they release new services continues to accelerate. Zenoss Insight incorporates real-time correlation at the point of collection with the ability to normalize and index all data sources (log, flow, RTCP, SNMP, etc.) under a single architecture. This greatly improves early detection of possible issues, provides immediate feedback on overall application and system performance, and allows you to instantly visualize complex information from automated or ad hoc data extractions.

Zenoss Insight

Modern IT infrastructures continue to grow in size, scale and complexity as technology stacks from multiple vendors are deployed across enterprise environments with the intention of seamlessly delivering services to end users. This demand for continuous service delivery and uptime also creates an unceasing production of log, flow and machine data. The opportunity to derive actionable intelligence from this data represents a tremendous advantage for organizations of every size. However, companies will require the ability to collect, analyze, visualize and respond to this data in real time in order to realize the full benefits. Otherwise, the information and trend intelligence captured by these processes is wasted – leading to extended outages, slower mean time to resolution, and excessive downtime.

CURRENT CUSTOMER IMPLEMENTATIONS:

+3 MILLION MANAGED ENDPOINTS

+10 MILLION CALLS PER HOUR

+100 MILLION LOGS ANALYZED PER DAY

+500TB OF DATA ANALYZED PER DAY

Zenoss Insight extends Zenoss Service Dynamics by allowing you to intelligently utilize all of your machine-generated log and flow data, providing even greater detail to your monitoring practice and ensuring your infrastructure is performing at optimum levels.

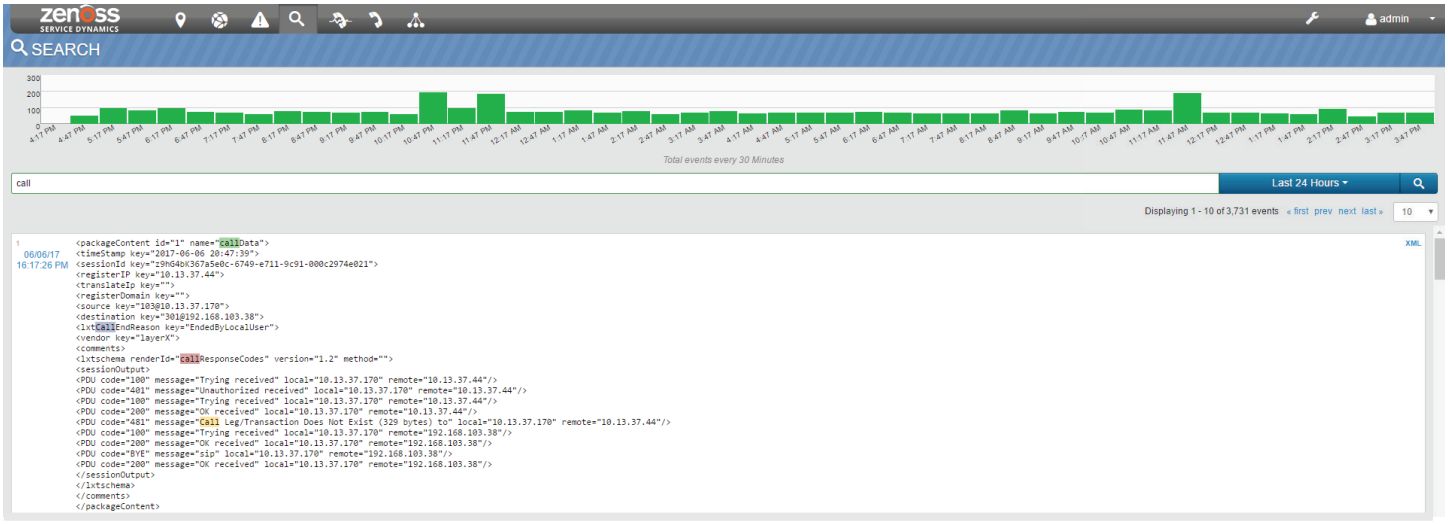
There are three distinct capabilities of the Zenoss Insight suite that highlight its key advantages:

Log Analytics - With no data collection caps or scale limitations

Unified Communications Monitoring – With out-of-the-box configurations for monitoring all major vendors and technologies

NetFlow Analysis – With a flexible deployment architecture that can scale to hundreds of thousands of flows per second and beyond

Within this document, we'll discuss how each of these capabilities works and the distinct value they can bring to your business.



Log Analytics:

At the heart of the Zenoss Insight suite you'll find a powerful log analytics engine built to digest large amounts of machine data and intelligently extract relevant information at scale. One of the primary advantages that sets Zenoss Insight apart from other log analytics tools is its ability to correlate disparate data types at the time of collection. Correlation of log data at the time of collection is critical to providing real-time feedback, events and alerts. Without correlation at collection, critical responsiveness can be significantly delayed – allowing problems to propagate to other systems and the business impact of downtime to grow exponentially.

ZENOSS INSIGHT'S LOG ANALYTICS CAPABILITIES CAN BE BROKEN INTO 4 KEY ACTIONS:

Collect, Analyze, Respond & Visualize

Collect

Zenoss Insight enables full utilization of the big data already being generated by your company's infrastructure and systems by allowing you to ingest information from any server, networked device, cloud resource, delivered service or application. With no data collection caps whatsoever and flexible scaling across your entire IT environment, there are no limits on the amount of data you can ingest. Any data format, whether structured or unstructured, can be streamed, pushed, pulled or harvested without restriction or cost penalty.

Analyze

By normalizing disparate data source files into a single uniform format, the patented Zenoss Insight correlation engine transforms enormous amounts of data into actionable information – allowing you to detect anomalies, identify faults, visualize trends, and keep your infrastructure performing at its peak.

Respond

Zenoss Insight deploys with thousands of proven, expertly developed correlation rules right out of the box, ensuring you gain immediate value and actionable intelligence from your data. By combining infrastructure statistics and software performance metrics with both log and flow data, Zenoss Insight provides a complete picture of overall application and system performance in a way not possible from single data point analysis. In addition, these intelligent polices minimize duplicate (or "false positive") events and facilitate faster resolution of any issues that arise.

Visualize

What good is data if you can't visualize it? Whether you're looking at real-time or historical data, with Zenoss Insight, all data extractions automatically create a report template that provides clear and customizable visualizations of the information. Zenoss Insight also provides predefined dashboards and policies for leading infrastructure manufacturers such as Cisco, Palo Alto Networks, Juniper, Dell, HP and Sonus. Or you can simply drag and drop the data extraction charts you want to create your own comprehensive, personalized dashboards. These individual report templates, dashboards and customized data charts can be combined into workbooks that provide holistic insight into any business service or practice area.

Zenoss Insight's ability to index any data format, search across all types of infrastructure, perform real-time data correlation, and archive data for historical analysis or auditing makes it a flexible tool for a wide array of use cases. One example is the ability to utilize log files for security information and event management (SIEM).

Log Analytics SIEM Example:

A major component of any robust security strategy is the ability to quickly and accurately detect and respond to threats. Zenoss Insight uses real-time collection, correlation and analysis to detect anomalies within your HR systems, personnel databases, identity management systems, firewall and proxy logs by providing a profile of all high privileged access users and setting a baseline for all company activity.

Using Zenoss Insight's advanced analysis and correlation capabilities, you can quickly identify malicious activity and then automatically isolate and remediate the problem. You not only minimize the time to detect and respond to issues but also automatically generate an audit report and dashboard view of all events. Having these available on a monthly or quarterly basis, without the need to manually set them up or run them, enables your security team to be more efficient and focus their efforts on resolving issues.

Unified Communications Monitoring:

Unified communications (UC) infrastructure allows organizations to communicate effectively across multiple channels and is a critical factor for companies trying to optimize business processes, manage information sharing, or increase productivity.

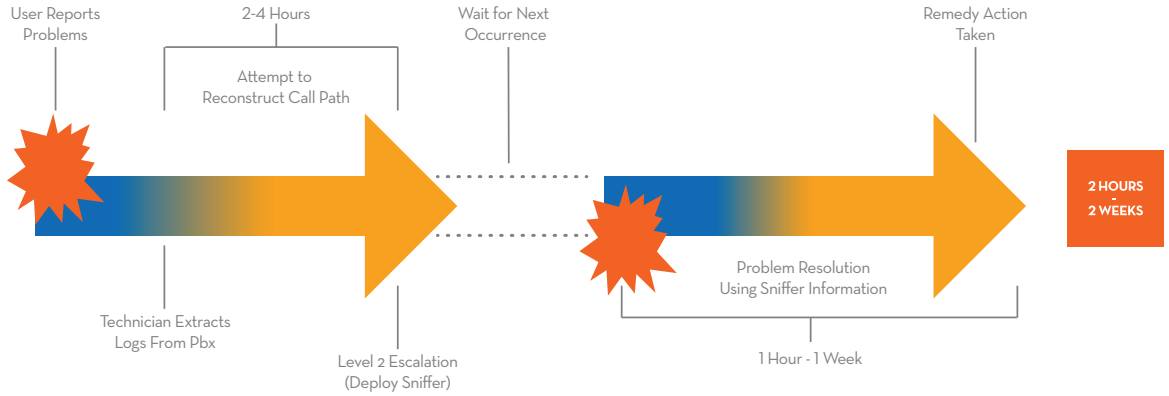
Effective UC monitoring focuses on quality of service, which extends far beyond simply knowing if a device is up or down, the current number of registered phones, or the number of calls attempted/active/completed. Just because a call was completed does not mean the user experience was of high quality. If a conversation is negatively affected by packet loss, incorrect codecs, flawed deployment configurations, or network latency across multiple network hops, the number of calls completed becomes irrelevant when weighed against the reality that information was not able to be successfully exchanged.

Pinpointing UC issues is complex and time consuming. A single UC call can travel through multiple servers, routers and gateways, across firewalls, and through multiple networks. These multiple hops can dynamically affect signal quality depending on the resources available at any given time. This makes accurately diagnosing call reliability and audio quality issues complex, and often costly, without the proper solution.

Utilizing machine data from UC infrastructure, coupled with expert policies for all major UC providers (such as Avaya, Cisco, Skype, BroadSoft, Oracle, Sonus, Aspect, Genesys, Pexip and many more), Zenoss Insight provides a holistic approach to UC monitoring and ensures UC environments consistently perform at their peak.

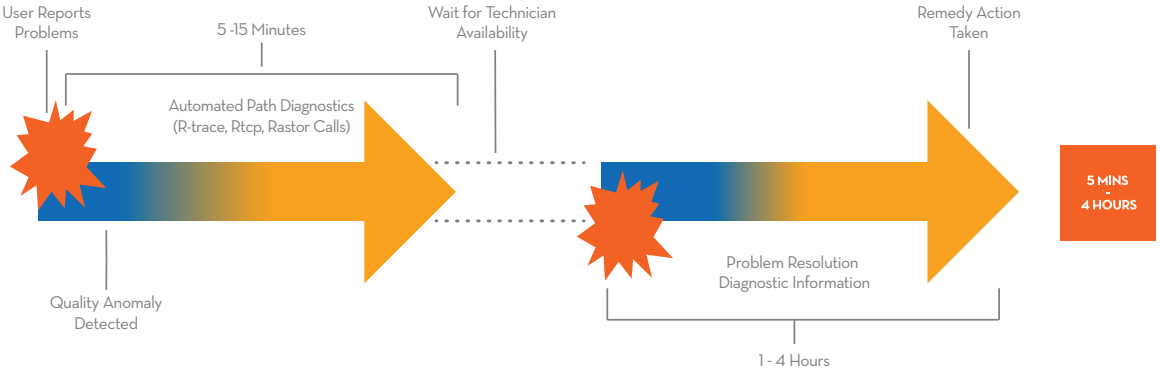
Let's compare a typical forensic UC monitoring approach against Zenoss Insight.

With many tools, issues are not proactively reported by the system. Instead, engineers must rely on users to report outages or poor call quality. The engineer must then manually recreate the event and utilize a packet sniffer to scan for possible call-quality issues.



In this case, the time and manual effort needed to recreate the incident, as well as retroactively isolate the root cause, is enormous. Additionally, if the network conditions are not exactly the same, the engineer may not immediately be able to pinpoint the source of the issue. Often, the result is a high resource cost for both time and people.

Conversely, Zenoss Insight automates the forensic analysis of call issues as they happen, in real time, through its correlation engine and policies. Zenoss Insight provides root-cause isolation within minutes and delivers detailed reporting on the incident's impact, duration and severity.



By utilizing proactive UC monitoring, problem isolation can be greatly simplified, and the time it takes to fix system issues can be shortened. Rather than relying on inefficient packet sniffers and simple alerting, network engineers are able to utilize actionable information for real-time troubleshooting and system optimization. By utilizing QoS, MoS, jitter and call-path monitoring alongside networkwide correlation, Zenoss Insight empowers companies to:

Capture critical events instantly via customizable policies

Pinpoint quality issues and expose bottlenecks via multihop call-path analysis

Visualize application and infrastructure health in real time

NetFlow:

NetFlow is a pivotal type of machine data that allows operators to understand the what, when and how of network traffic. NetFlow statistics can tell you which devices are connecting to each other, at what time those connections occurred, and how the connections were made (via source and destination IP addresses, port identifiers, time stamps, and TCP/UDP protocols).

While a single NetFlow log can contain a massive amount of useful information, it will not yield a complete view of how your entire network is truly performing. In order to make use of NetFlow information at scale, companies must be able to visualize traffic across tens, or even hundreds, of thousands of flows.

Zenoss Insight's native listener and distributed architecture can easily analyze hundreds of thousands of flows per second and transform network data into intelligence – providing proactive problem detection, efficient troubleshooting, and rapid problem resolution.

Identify top bandwidth consumers

Diagnose quality issues and system bottlenecks via multihop call-path analysis

Compare network utilization over time

Zenoss Insight's NetFlow analysis is vendor agnostic and can analyze NetFlow 5, NetFlow 9, jFlow, sFlow and IPFIX.

Conclusion

The Zenoss Insight suite extends Zenoss Service Dynamics beyond traditional application and system monitoring, allowing you to leverage your infrastructure's big data to perform log analytics, unified communications monitoring, and NetFlow analysis from a single unified, scalable platform.

Unified | Scalable | Intuitive | Powerful

Thousands of predefined alerts, events, auto-actions, dashboards and reports right out of the box.

About Zenoss

Zenoss works with the world's largest organizations to ensure their IT services and applications are always on. As the global leader in hybrid IT monitoring and analytics software, Zenoss provides complete visibility for cloud, virtual and physical IT environments. Zenoss customers gain IT performance and risk insights into their unique IT ecosystems through real-time analytics that adapt to the ever-evolving data center and cloud, enabling them to eliminate disruptions and accelerate business.

zenoss
Own IT.

To learn more, visit our website at

www.zenoss.com

ZENOSS IS THE GLOBAL LEADER IN HYBRID IT MONITORING AND ANALYTICS SOFTWARE