

Socket Analyzer

TROUBLESHOOT NETWORK RELATED ISSUES AT THE SOCKET LEVEL

BrixBits Java Application Socket Analyzer is a comprehensive network socket monitoring solution that correlates network traffic to application threads and code segments. By intercepting socket activity regardless of who, what or where it was created, Socket Analyzer provides application stakeholders the critical information needed to troubleshoot network related Java application issues without dependence on the networking team.

Why Socket Analyzer?

Our attention spans have become so short that waiting even a nano-second for information to return from the server can mean the difference between a purchase and an abandoned shopping cart. Sockets have revolutionized the way Java applications interact with their application servers bringing information faster than ever to applications. But sockets have also introduced a new level of performance and security issues. Network performance, as well as security, is a vital part of the overall application service level management. More than ever, application server monitoring tools need real visibility into inbound and outbound socket transmission quality and performance, but this information is often unavailable even with today's best-in-class monitoring tools. Socket Analyzer is the only product on the market that runs inside the JVM and can tie the application code to the network at the socket level.

Product Highlights

- **Find and report on socket exceptions** - Identify all socket related events and exceptions such as connection resets or too many files open that can be hurting your application performance
- **Monitor TCP & UDP sockets and activity** - Discover which ports are in use by the application, what hosts are interacting with application servers, view port activity, socket exceptions and error counts for any TCP and UDP socket.
- **Capture networking metrics and response times** –Expose general network metrics as well as outbound connection times and inbound and outbound response times and notifies on related service issues.
- **Correlate networking events to application code** – Correlate network traffic to application server threads, code segments, etc. to get an application aware view of the network and trace networking issues back to the Java application code.
- **Capture raw TCP traffic** – Capture raw TCP traffic and HTTP requests, transactions and error status codes to quickly expose and be notified of application errors. The raw data can be sent to a common log format for easy integration with other applications.

Key Benefits

Immediate Notification of Network Events

Customizable notifications means getting notified of critical or severe network errors as they happen. No more digging through log files long after an event has taken place to find out what happened.

Visibility into Application Dependencies and Vulnerabilities

By identifying open ports or ports in use by other third party applications, Socket Analyzer makes it easy to identify potential vulnerabilities that may put application security at risk.

Identify Potential Service Issues

Exposing network quality issues, latency issues, exceptions and errors, makes it easy to quickly identify application service issues before they become a major problem for users.

Bridges Application Networking & Java Architecture

Bridges the application and the network by viewing at the socket level versus the network card level. Socket Analyzer connects the network traffic to the application code such as thread names, code trees and listener code segments. This provides application developers and stakeholders with on-demand tools for troubleshooting and monitoring without having to involve the networking team.



BrixBits | Socket Analyzer

Technical Features

MONITORS UDP AND TCP SOCKETS

Monitors both TCP and UDP client and server sockets and APIs such as RMI, JMS, Corba, JDBC, DNS, JNDI lookup, JMX and Web Services for usage, exceptions and errors.

IDENTIFIES OPEN PORTS & PEERS

Socket Analyzer identifies all peer hosts connected to the application server as well as all open ports and reports on port usage including activity levels, traffic levels, socket type, etc. to provide visibility into application server dependencies and vulnerabilities.

CAPTURES RAW NETWORK TRAFFIC INCLUDING SSL

Socket Analyzer captures raw traffic such as HTTP requests, transactions and status codes including data transmitted over SSL. SSL header data is reviewed after it is decrypted so there is no need to provide a private key to decrypt. The raw data is logged to a common format that can then be fed into other third party applications if more detailed decoding/packet analysis needs to be performed.

ISOLATES TRAFFIC TO THE SERVER

Unlike many networking applications that run in promiscuous mode monitoring all traffic across the entire network, Socket Analyzer only monitors traffic for the host it is running on.

REPORTS APPLICATION RESPONSE TIMES

Calculates and alerts on outbound connect time, inbound and outbound response times based on time to first byte, read and write rates and more to provide immediate notification of service related issues.

IDENTIFY SECURITY VULNERABILITIES

Socket Analyzer is a great security and auditing tool that looks for open sockets and back door network connections that can expose business critical applications to security vulnerabilities.

CONTINUOUS MONITORING OF NETWORK EXCEPTIONS

Socket Analyzer continuously monitors and alerts on all socket exceptions including timeouts, refused connections, peer resets, etc. providing visibility into the application server's network health.

CONFIGURABLE RULES BASED ALERTING

Quickly and easily configure which Socket Analyzer alerts to receive using our simple rules based system.

REAL-TIME CUSTOMIZABLE NOTIFICATIONS

Selectively convert events into operations based notifications such as SNMP traps, syslog messages, emails or text messages to be delivered in real-time.

DETAILED REPORTING

Detailed reports provide metrics and timing breakdowns for instrumented requests.

WORKS WITH ALL STANDARD J2EE LOGGING APIS

Socket Analyzer works with all standard J2EE logging APIs such as log4j, apache commons, jboss, tomcat juli, and more.

WORKS OUT OF THE BOX

Socket Analyzer is easy to install and requires zero configuration. You can be up and running within minutes.

CENTRALIZED EVENT MANAGEMENT CONSOLE

Our centralized event management console provides a single consolidated view of all Socket Analyzer agents, alerts, reports and configuration options.

EMBEDDED AGENT

Embedding our agent in the JVM means a lightweight solution with no additional process to manage. This method also gives us enhanced capabilities to capture data.

BrixBits, Inc.
802 Lovett Blvd
Houston, TX 77006
713.481.9595
Web: www.brixbits.com
Email: info@brixbits.com
LinkedIn: www.linkedin.com/company/brixbits-inc-

