CleverView® for cTrace Analysis v8.2

Cloud Trace Analysis

CLEVER® Business Service Management

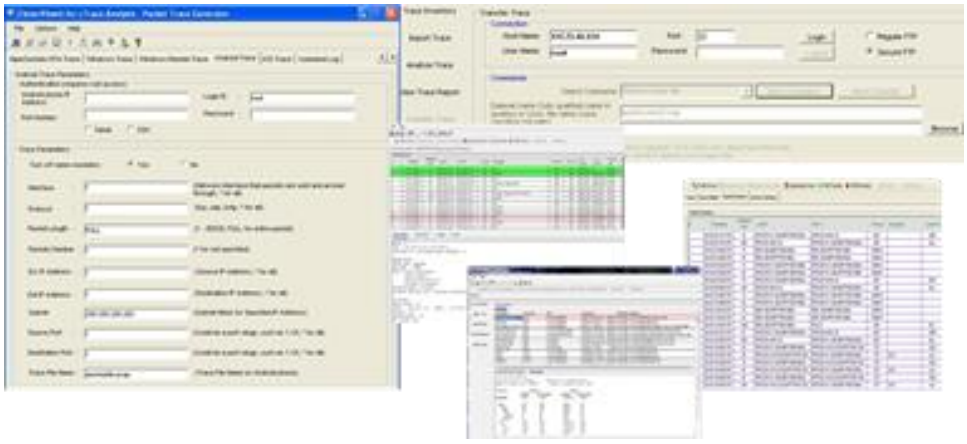
AES CLEVER® Solutions offer unsurpassed diagnostic and performance monitoring and reporting for enterprise environments, especially as cloud computing, blockchain, and data analytics are implemented.

CleverView® for cTrace Analysis allows users to generate and analyze IP packet traces across multiple systems. The expert functions enhance diagnostic efforts, accelerating virtualization, cloud, application, and IPv6 deployments. It supports IBM® z System, LinuxONE, Power Systems, open/distributed systems, and mobile devices resulting in user to server to mainframe deep dive analysis. Users now have expert analysis of network traffic for today's multi-architecture environments:

- ✓ z/OS®
- ✓ Linux®
- ✓ Linux on z System®
- ✓ Linux on LinuxONE
- ✓ z/VM®
- ✓ Android®
- ✓ iOS®
- ✓ z/VSE®
- ✓ AIX®
- ✓ OSA Express
- ✓ Windows®
- ✓ HiperSockets
- ✓ UNIX
- ✓ IBM i®

CleverView for cTrace Analysis allows users to simultaneously schedule (start and stop) traces from heterogeneous systems providing end-to-end viewing of IP packet flows. The in depth diagnostic capability and flow control details make this an essential trouble shooting tool for operations.

CleverView for cTrace Analysis can be scheduled to collect IP packet traces from Mobile devices, end user devices, open systems, IBM power and z systems. The intelligent **TRACE Diff** offers side-by-side comparison of traces. Other key features include packet details, session summary, query builder, and expert analysis.



Key Features

Cloud support

- **Multi-architecture trace generation** for z/OS®, OSAENTA, HiperSockets®, Windows®, Linux, Linux on System z, AIX®, UNIX, Android®, iOS®, IBM i, and more
- **Mobile to mainframe trace support**
- Cloud **import and analysis** for any trace generated with CleverView for cTrace Analysis, Sniffer, or any trace file with a .cap or .pcap extension
- **IPv4 and IPv6 protocol support** including IPv6 tunnel decoding
- **Protocol decoding** including Enterprise Extender, FTP, TN3270, IPv4, TCP, IPv6, TLS, OSAENTA, HTTP, IDS, and NetBIOS to name a few

Intelligent Analysis

- **Auto-scheduling** of packet capture
- Pinpoints performance issues by providing **host time/network time breakout**
- Simultaneous **interval based tracing**
- **Side-by-side trace comparison** with TraceDiff for faster problem resolution
- **QueryBuilder filters captured data** allowing focus on specific items under investigation
- **Critical session reports** with response times and transfer rates
- **Split screen display** provides both summary and detailed information on a single screen
- **Protocol summary** provides high level overview of captured detail

Security

- **Packet discard/port tracing** available
- **System level credentials** required
- Data trace reveals application level **inconsistencies** before encryption or after decryption

Mainframe packet trace exclusives:

- Capture and analyze both **OSA, and HiperSocket** IP packet diagnosis
- **Real-time packet** trace using z/OS API
- Capture multiple **LPAR** packet traces through the OSA interface from one z/OS system

AES
P.O. Box 50927
Palo Alto, CA 94303
(650) 617-2400
www.aesclever.com

AES - The Business Service Management Company

Highlights of CleverView for cTrace Analysis:

Trace Collection:

- Automated Trace Collection is available for z/OS Component, OSAENTA, HiperSockets, Windows local, Windows remote, z/OS Data, Linux, AIX. UNIX, Android, and iOS traces.
- Remote Windows Tracing allows auto-scheduled (start and stop) packet trace capturing on remote Windows machines, enhancing end-to-end problem diagnosis.

End-to-End Performance Analytics:

- Session and Packet Summary Reports reveals prevalent categories at a glance with customizable highlighting. Reports include **Sequence of Execution** (details of the packets exchanged during a given session) and **Response Time Summary (**summarizes all sessions between local and remote IP devices communicating through the same protocol).
- Server Time vs. Network Time Report provides host time and network time to enhance the performance diagnostic process.

Diagnostic Capabilities:

- Security Protocols Support enhances diagnostics for the Secure Socket Layer, supporting TLS and AT-TLS protocols
- OSA Real-Time tracing provides real-time OSAENTA trace capture and decoding on the z/OS.
- IPv6 protocol support allows both capture and decoding with decoding of ICMPv6 and IPv6 tunnel technologies.
- NetBIOS Packet decoding improves knowledge engineers ability to diagnose problems with the NetBIOS protocol.
- Trace Diff provides side-by-side trace analysis on one screen, including sequence number and application data comparison.
- Exception Reporting provides easy access to multiple error report types, grouped by defect category.

Supported Trace Samples:

- HiperSockets NTA Support enables the capture OSA LAN and HiperSockets LAN traffic.
- OSAENTA Trace Support offers a trace generator option to Start/Stop OSA-Express Network Traffic Analyzer (OSAENTA) traces and provides decoding and expert analysis. Decoding MAC addresses in OSAENTA is also available.
- z/OS Real-Time Packet Trace and OSAENTA trace use the documented z/OS API to provide real-time packet tracing and formatting on the host, offering real-time, on-demand network problem resolution and uniquely providing a view of TCP/IP network traffic as it occurs.
- DATA Trace Support decodes and displays the IP addresses, ports and application protocols from the data trace.
- Sniffer® Trace Support allows analysis of Network General™ Sniffer captured files. For example, a Sniffer trace provided from other teams can be compared side-by-side with CTRACE packets collected from the mainframe host side.
- z/VM Packet Trace Support imports and analyzes traces for fast network problem diagnosis at the packet level.
- Linux and UNIX IP Packet Traces imports and analyzes pcap traces, displays the pcap header, including Source/Remote Mac Address information.
- CTRACE Conversion Capability converts CTRACE to pcap format for decoding by Sniffer® and other similar products.

CleverView for cTrace Analysis v8.2 introduces the following new features:

- Enhanced Trace Type classification enhancing the understanding of how the trace was generated
- IDS Trace Analysis providing deep diagnostic capability into Intrusion Detection packets
- New capabilities in Query Builder supporting filtering by IDS Probe ID or IDS Correlator

System Requirements:

PC Workstation: 2 GHz or above, 4GB RAM, 500MB available disk space; Microsoft Windows Server 2016, Windows 10.
CleverView for cTrace Analysis z/OS Mainframe Requirements: IBM z/OS Architecture, 500-1000 3390-type device tracks, z/OS V2R2 or higher.
z/VM packet trace requires z/VM 4.4 or later.
Linux and UNIX IP packet trace supports traces generated by the tcpdump command.
Optional feature CLEVER Mobile for Trace: Operating Systems: Android: 4.0 and above and iOS: 5.0 and above

AES
aesclever.com

AES
P.O. Box 50927, Palo Alto, CA 94303 USA
Phone: (650) 617-2400 Fax: (650) 617-2420
Website: www.aesclever.com Email: info@aesclever.com

CLEVER

MM-6-1701-DS