

New in Version 4.7

Incorporation of all Previous Service

As well as the new facilities outlined in the paragraphs below, all service applied after the initial release of version 4.5 of EXIGENCE has been incorporated into this new version 4.7.

New 'Peek' Feature for Browsing Active IP Traces

This version of EXIGENCE permits browsing of active IP traces, with seamless progression from displaying data that has already been written to the Trace Data File (TDF) to data from the in-storage trace buffers yet to be written to the TDF. This new facility is generally referred to as 'Peek'. A message is shown at the bottom of the trace displays when using the 'Peek' function that both indicates the trace is active and also provides the rate at which packets are being captured.

This usability enhancement means that it is now possible to track the progress of a trace in flight, and stop it when you detect the condition you are seeking in the trace records (providing of course that packets are not being captured too quickly for you to analyze; appropriate filtering can be very helpful in this case). No special command is required to use this facility, the usual Browse command now works when the status of the trace is 'Active'. To help you track the progress of an active trace, the PF2 key positions the display to the latest trace entry captured. If you normally use the EXIGENCE Client, this new feature can be used on traces run in a single LPAR, but may also be used for group traces.

There are some minor restrictions: wrap mode traces (see "A Note on Wrap Mode Traces" on page 51 of the Reference manual) are not supported and functions which depend on EXIGENCE's trace pre-processing functions such as gathering together fragmented packets into a composite packet for display purposes, recognizing unacknowledged packets and flagging ICMP packets are not available (since these occur after the trace has been completely committed to disk). Filtering, however, is available.

Import and Export libpcap, Sniffer and OSAENTA Traces

In the previous version it was possible to export a trace in libpcap format using the EXIGENCE Java Client (only). EXIGENCE's capabilities in this area have been extended in version 4.7 so that it is now possible to *import* a trace originally captured in libpcap or Sniffer format and browse it in the same way as if it had been captured by EXIGENCE.

Similarly, you may now also import OSA traces captured using the OSA-Express Network Trace Analyzer (OSAENTA traces). libpcap, Sniffer and OSAENTA traces are imported in the usual way using the Import (IP trace) command and EXIGENCE determines the trace type from the data in the specified dataset.

The Export command has also been enhanced so that imported libpcap and OSAENTA traces can also be exported for shipping to IBM, or for import to other EXIGENCE systems.

Since the link-level header is available in both these trace types, the trace displays have been enhanced to cater for this. For example, the PF9 Flow display will recognize and display ARP requests and responses in libpcap traces, displaying the MAC addresses in place of the IP addresses. Also, the PF11 Expanded display now allows expansion (using the standard PF11 key) of the link header in all records and the ARP header and ARP data in ARP request and response records may also be expanded. For further details and example panels see the section “Libpcap, Sniffer and OSAENTA Trace Support” on page 188 of the Reference manual.

IPsec Support

This version of EXIGENCE now recognizes the presence of IPsec traffic in a captured trace and any secured trace records will be flagged as ‘IPsec ESP’ in the Flow display. The PF10 Detail display has been enhanced to show the first 4 bytes of the IPsec authentication header at the end of the IP address field and the IPsec header, while the PF11 Expanded display shows both the complete IPsec authentication header as well as the IPsec header. The full structure breakdown is available for both of the IPsec headers on the Expanded display.

Note that beyond the IPsec header lies the IPsec data which, while displayed by EXIGENCE on the PF11 Expanded display in the usual way, cannot be formatted or translated since it is securely encrypted and therefore unrecognizable by EXIGENCE. For further details and examples of IPsec support see “IPsec Support” on page 167 of the Reference manual.

Improvements to the Support for IPv6

EXIGENCE has had basic support for capturing, browsing, importing, exporting and printing IPv6 traces since version 4.1. This new version extends the support, providing text descriptions on the Flow display where it recognizes the packet’s contents. As much of the IPv6 address is displayed as possible on the Flow display given the restriction of the 3270 width, the full IPv6 addresses being displayed with the :: placeholder for repeated zero elements, on the PF10 Detailed and PF11 Expanded displays.

On the PF11 Detail display, the PF11 Expand key can be used on the IPv6 header and the secondary header to obtain structure breakdowns, and the Translate command (T) is available for the packet types that EXIGENCE normally recognizes (such as TN3270 or ICMP). For further details and examples see “IPv6 Support” on page 164 of the Reference manual.

You may also now key IPv6 format addresses in the Find window (see “Using the Search and Filter Function” on page 111 of the Reference manual) when using the ‘IPADDR’ search option, and EXIGENCE will convert the keyed IP address to hex and then scan the IP packets for the given address.

As part of this change, IP headers are now displayed on the PF10 and PF11 detailed panels as either ‘IPv6’ or ‘IPv4’ for clarity.

Support for GRE

Previous versions of EXIGENCE supported translation of a GRE packet only when it was carrying a CASA payload (see “GRE/CASA Support” on page 183 of the Reference manual). This support has been enhanced so that standard GRE packets, irrespective of the underlying encapsulated payload, can be displayed.

The ‘Enc’ command is available on both the PF9 Flow display and the PF11 Expanded display for all GRE traces and enables you to see the datagram encapsulated within the GRE packet. If the encapsulated datagram is of a type that EXIGENCE recognizes (for example a TN3270 or ICMP packet) it can be further broken down on the PF11 Expanded display using the Translate (T) command. For further details and examples see “GRE Support” on page 180 of the Reference manual.

Enhancement to Filtering for GRE IPv4 Packets

There has been a change to the way in which filtering works for IPv4 packets that are encapsulated using GRE. This applies both to the filtering process during trace capture and also during trace import. If CASA is used in addition to GRE it will appear as UDP and port 1637. The filtering process does not consider anything encapsulated by the CASA structure.

The selection of a packet according to its IP version (IPv4 or IPv6) by the filtering process works as before on the encapsulating packet only, as does the filtering by link name.

Filter IP addresses are now checked against *both* the encapsulating *and* the encapsulated headers. If any one of the specified filter IP addresses are found in either the encapsulating or the encapsulated header the packet will be selected. Only if none of the specified IP addresses are found in either header level will the packet remain unselected.

The port and/or application filters are processed *for the encapsulated packet only*. Prior to this change any selection of values in these fields would have caused the packet to be ignored because the encapsulating GRE header does not contain port fields. This is a key change in behaviour since it enables you to filter packets which previously you would have been unable to do.

Similarly, the filter protocols selected will be checked for *in the encapsulated packet*. Note that this implies that using the ‘Num’ field to enter a value of 047 (GRE’s assigned number) will *not* select such packets.

New Operator Command

Previous versions of EXIGENCE provided commands that could be issued via a standard Modify (F) console command to define, redefine, start and stop traces. In this version a new command ‘IMPORT IPK’ has been added which enables you to import IP traces (only - SNA traces are not currently supported) using the same technique. All the usual trace formats are supported by the new command. For further details see “Importing an IP Trace” on page 221.

To enable you to run EXIGENCE operator commands from JCL, a new utility has also been provided called EXICMD which will in your *hlq*.LOADLIB after product installation. This utility accepts a command on the PARM parameter which the utility will pass to z/OS as if it had been issued from the console. This means that you could set up, for example, a second step in your CTRACE PROC to import a captured trace directly into EXIGENCE. The utility is not limited to EXIGENCE commands, you can issue any operating system command from JCL using this utility, provided the user under which the job runs has adequate RACF authority. See the section “The EXICMD Utility” on page 228 of the EXIGENCE Reference manual.

Support for Discarded Packets

The DISCARD parameter available for OSAENTA traces since z/OS version 1.9 has from version 1.10 of z/OS been introduced for the command that activates packet tracing. This parameter enables you to record in the trace IP packets that have a non-zero discard code. EXIGENCE has always recorded discarded packets but from version 4.7 provides enhanced support for them as follows:

- All trace displays by default indicate discarded packets using color and a discard message.
- The PF11 Expand function with the cursor positioned under a discard code/message provides the full description for the discard.
- The Trace Import function has been enhanced so that discarded packets in IP or OSAENTA traces are imported unchanged to the EXIGENCE trace dataset.
- New commands DSC, DSCON and DSCOFF have been added to cause discarded packets to be either displayed, or suppressed from the display. See page 196 in the Reference manual for a description of these new commands.

Improvement to the Trace List

The Trace Type field in the Trace List - Trace Data Management panel - has been enhanced so that the new trace types catered for in this version are more evident on the display:

- **TCP/IP SYSTCPOT** for imported OSAENTA traces
- **TCP/IP SYSTCPDA** for imported IP traces
- **TCP/IP libpcap** for imported libpcap format traces
- **TCP/IP Sniffer** for imported Sniffer format traces

The descriptions of VTAM and IP traces defined and captured by EXIGENCE remain unchanged.

Support for z/OS v1.12

This version of EXIGENCE supports all currently supported z/OS versions up to and including z/OS version 1.12.

New EXIGENCE PC Client v1.05

To provide all of the support related to the enhancements outlined in the sections above, a new version 1.05 of the EXIGENCE Client has been built. This will provide:

- Support for browsing libpcap and OSAENTA traces
- Recognition and annotation of IPsec traffic plus expansion of the IPsec ESP and IPsec Authentication headers
- Improved support for the display of IPv6 packets
- Support for non-CASA GRE traffic
- Support for packets with non-zero discard codes including discard code translation

The new Client is available from the WDS Customer Portal at https://portal.willdata.com/support_customerlogin.aspx.