RTI Secure WAN Transport

Release Notes

Version 5.2.0

Your systems. Working as one.

Printed in U.S.A. First printing.
June 2015.

Trademarks

Real-Time Innovations, RTI, NDDS, RTI Data Distribution Service, DataBus, Connext, Micro DDS, the RTI logo, 1RTI and the phrase, "Your Systems. Working as one," are registered trademarks, trademarks or service marks of Real-Time Innovations, Inc. All other trademarks belong to their respective owners.

Copy and Use Restrictions

Technical Support

Real-Time Innovations, Inc.
232 E. Java Drive
Sunnyvale, CA 94089
Phone: (408) 990-7444
Email: support@rti.com
Website: https://support.rti.com/

Release Notes

1 Supported Platforms

This release of *RTI® Secure WAN Transport* is supported on the architectures listed in Table 1.1.

Table 1.1 **Supported Platforms**

Operating System		CPU	Compiler	RTI Architecture Abbreviation
Linux	CentOS 6.0, 6.2, 6.3, 6.4	x86	gcc 4.4.5	i86Linux2.6gcc4.4.5
		x64	gcc 4.4.5	x64Linux2.6gcc4.4.5
	Raspbian "Wheezy" 7.0	ARMv6	gcc 4.7.2	armv6vfphLinux3.xgcc4.7.2
	Red Hat® Enterprise Linux® 5.0 (2.6 kernel)	x86	gcc 4.1.1	i86Linux2.6gcc4.1.1
		x64	gcc 4.1.1	x64Linux2.6gcc4.1.1
	Red Hat Enterprise Linux 6.0 - 6.5	x86	gcc 4.4.5	i86Linux2.6gcc4.4.5
		x64	gcc 4.4.5	x64Linux2.6gcc4.4.5
	Red Hat Enterprise Linux 7.0	x86	gcc 4.8.2	i86Linux2.6gcc4.8.2
		x64	gcc 4.8.2	x64Linux2.6gcc4.8.2
	Ubuntu® Server 12.04 LTS	x86	gcc 4.6.3	i86Linux3.xgcc4.6.3
		x64	gcc 4.6.3	x64Linux3.xgcc4.6.3
	Ubuntu 14	x86	gcc 4.8.2	i86Linux2.6gcc4.8.2
		x64	gcc 4.8.2	x64Linux2.6gcc4.8.2
	Wind River® Linux 4 (2.6 kernel)	x64	gcc 4.4.1	x64WRLinux2.6gcc4.4.1
Mac OS	OS X 10.8	x64	clang 4.1	x64Darwin12clang4.1
	OS X 10.10	x64	clang 6.0	x64Darwin14clang6.0
QNX	QNX® Neutrino® 6.5	x86	qcc 4.4.2 with GNU C++ libraries	i86QNX6.5qcc_gpp4.4.2
	QNX Neutrino 6.5.0 SP1	ARMv7a Cortex	qcc 4.4.2 with Dinkum libraries	armv7aQNX6.5.0SP1qcc_cpp4.4.2
Solaris	Solaris™ 2.10	Ultra SPARC®	gcc3.4.2	sparcSol2.10gcc3.4.2
Windows	All Windows® architectures listed in the *RTI Connext DDS Platform Notes* for the same version number			

Table 1.2 lists an additional target library for which RTI offers custom support. If you are interested in using this platform, please contact your local RTI representative or email **sales@rti.com**.

Table 1.2 **Custom Supported Platforms**

Operating System	CPU	Compiler	RTI Architecture Abbreviation
NI Linux Real-Time 3.2	ARM Cortex-A9	gcc 4.4.1	armv7AngstromLinux3.2gcc4.4.1.cortex-a9

2 Compatibility

RTI Secure WAN Transport is an optional product for use with *RTI Connext™ DDS* with the same version number.

This release uses OpenSSL 1.0.1L.

3 What's New in 5.2.0

- New platforms (see Table 1.1):
  - CentOS 6.0, 6.2, 6.3, 6.4
  - Red Hat Enterprise Linux 6.0 - 6.5, 7.0
  - Raspbian "Wheezy" 7.0
  - Mac OS X 10.8 and 10.10
  - Ubuntu 14
  - Additional Windows platforms (see *RTI Connext DDS Core Libraries What's New)*
- Windows platforms using Visual Studio 2005 are no longer supported.
- This release uses OpenSSL 1.0.1L.
- RTI's OpenSSL bundles include multiple builds in different directories. The release and debug builds are now in separate directories. For this reason, the path to the libraries will change with respect to earlier bundles.
- Starting with the OpenSSL 1.0.1h, RTI provides the OpenSSL static libraries with a "z" suffix. No suffix is used for dynamic libraries. This means that the name of the dynamic libraries is the same as in previous bundles, but the name of static libraries now has a 'z' suffix.

4 What's Fixed in 5.2.0

4.1 Error When Enabling DomainParticipant

A *DomainParticipant* could not be enabled if it was configured to use *Secure WAN Transport*. When this issue occurred, the following message was displayed:

```
NDDS_Transport_WAN_plugin_property_from_DDS_property:Unexpected property:
dds.transport.wan_plugin.wan.parent.domain_participant_ptr. Closest valid
property: dds.transport.wan_plugin.wan.parent.parent.domain_participant_ptr
```

This problem has been resolved.

[RTI Issue ID COREPLG-315]

4.2 Errors Deserializing Messages when Using Secure WAN Transport

An issue in *Secure WAN Transport* may have caused deserialization errors upon receipt of STUN messages from a remote plugin. This problem has been resolved.

[RTI Issue ID COREPLG-327]

4.3 Unexpected Memory Growth when Sending and Receiving STUN Messages

An issue in *Secure WAN Transport* may have caused unexpected memory growth when sending and receiving STUN messages. Note that this was not a memory leak, since all the memory was returned upon WAN Transport plugin destruction. This problem has been resolved.

[RTI Issue ID COREPLG-328]

4.4 Unexpected Memory Growth when Accepting Connection from Remote Plugin

An issue in *Secure WAN Transport* may have caused unexpected memory growth upon accepting a new connection from a remote plugin. Note that this was not a memory leak, since all the memory was returned upon WAN Transport plugin destruction. This problem has been resolved.

[RTI Issue ID COREPLG-329]

4.5 Communication may not have Resumed after Killing and Restarting Secure WAN Participant

When using *Secure WAN Transport* over DTLS, ungracefully shutting down and restarting a participant may have resulted in unrecoverable communication failure. This issue has been resolved. The recovery time can be configured via a new WAN transport property: **dtls_connection_liveliness_interval**.

[RTI Issue ID COREPLG-347]

5 Compatibility

In *Connext DDS* 5.1.0, the default value for **message_size_max** for this transport changed. *Secure WAN Transport* also uses this value. Consequently, *Secure WAN Transport* 5.1.0 and higher is not off-the-shelf compatible with applications running older versions of this transport. See the *RTI Connext DDS Core Libraries Release Notes* for instructions on how to resolve the compatibility issue with older *Connext DDS* and *RTI Data Distribution Service* applications.

6 Known Issues

- When communicating over some networks, the Secure WAN Transport plug-ins may fail to send data larger than the MTU (maximum transmission unit) size available for the network. This is especially likely over wide-area networks. This scenario is also a suggested configuration of the DTLS protocol, according to the DTLS specification, which is IETF RFC 4347.

  If problems occur while sending large packets, set the maximum_message_size transport property to the MTU of your network *minus 28 bytes for the DTLS header* and set up your application according to the Large Data Use Cases "How To" provided in the online (HTML) documentation. For example, for an MTU size of 1500 bytes (for standard Ethernet), set **maximum_message_size** to 1500 - 28 = 1472.

  One instance of this problem for which there is no workaround is the case where the discovery packets are larger than your network's MTU. This could occur if user data, propagated properties, or type-codes are configured.

- An application using the WAN transport may appear to hang for several minutes if the WAN server is shut down and not restarted before the application tries to contact it, or if the application is unable to communicate with the WAN server.

  Two scenarios under which the application tries to contact the STUN server are during shut down and while establishing a connection with the initial peers.

  This issue is due to a sequence of synchronous STUN transactions with the STUN server. If you need to run WAN transport without a STUN server, here are some recommendations:

  - Decrease the blocking time by decreasing the number of STUN retransmissions. To do so, change the property, **stun_number_of_retransmissions**. For example, a change from the default of 7 retries to 5 retries will result in a total period of 3.1 seconds per synchronous operation. Note however, that this may impact the ability to reliably set up connections to peers over a WAN.
  - Decrease the blocking time by using a participant ID limit of zero when configuring the initial peer descriptors.

    For example, when the peer descriptor **wan://::1:10.10.1.150** is specified, DDS will try to contact five participants with the same WAN ID in different ports. Usually there is only one participant using the same WAN ID. Although the other four participants will never be reachable, the application still tries to establish communication with them by contacting the STUN server.

    You can reduce the number of participants to which the application will try to contact to one by using a participant ID limit of zero in the peer descriptor. For example, **0@wan://::1:10.10.1.150**.

    For information on peer descriptors, see the *Discovery* chapter in the *RTI Connext DDS Core Libraries User's Manual*.

7 Third-Party Licenses

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).