OpenRTM-aist (Python) - 機能 #3409

⑩　セキュアな通信機能

2015/12/22 09:45 - n-ando

ステータス:	終了	**開始日:**	2015/12/22
優先度:	通常	**期日:**	2016/03/25
担当者:	miyamoto	**進捗率:**	100%
カテゴリ:		**予定工数:**	30.00時間
対象バージョン:	RELEASE_1_2_0		

説明

データポート、サービスポート間の通信をsslで保護する機能を実装すること。なお、この機能は、外部モジュールとして切り出せるように実装する必要がある。すなわち、セキュアな通信機能はモジュール化し、実行時に動的ロードすることで有効になるとともに、当該モジュールが存在しない場合は、他の個所を特に変更することなく動作すること。

関係しているリビジョン

リビジョン 642 - 2016/02/01 14:29 - miyamoto

[incompat,new_func,new_file,->RELENG_1_2] SSL encrypted connection has been implemente. refs #3409

リビジョン 653 - 2016/02/01 20:21 - miyamoto

[incompat,new_func,new_file,->RELENG_1_2] SSL encrypted connection has been implemented. refs #3409

リビジョン 688 - 2016/03/07 19:18 - miyamoto

[compat,bugfix,->RELENG_1_2] bug fix. refs #3409

履歴

#1 - 2016/01/14 16:20 - miyamoto

- 期日 を 2016/03/25 にセット

- 担当者 を miyamoto にセット

- 対象バージョン を RELEASE_1_2_0 にセット

- 進捗率 を 0 から 50 に変更

- 予定工数 を 30.00時間 にセット

#2 - 2016/01/14 21:37 - miyamoto

SSLによる通信を有効にするモジュールとしてSSLTransport.pyを実装した。
rtc.confに以下のような記述を追加することでSSLTransportInitが実行される。

manager.modules.preload: SSLTransport.py

さらに以下の記述を追加する事で、証明書、秘密鍵、パスワードの設定ができるようにした。
corba.ssl.certificate_authority_file: root.pem
corba.ssl.key_file: private-key.pem
corba.ssl.key_file_password: password

SSLTransportInit関数では、まずエンドポイントの設定を環境変数により行っている。

os.environ['ORBendPoint'] = 'giop:ssl::'

そしてSSLに関する設定を行う。
certificate_authority_file = manager._config.getProperty("corba.ssl.certificate_authority_file")
key_file = manager._config.getProperty("corba.ssl.key_file")
key_file_password = manager._config.getProperty("corba.ssl.key_file_password")
sslTP.certificate_authority_file(certificate_authority_file)
sslTP.key_file(key_file)
sslTP.key_file_password(key_file_password)

ただし、このORBの初期化前にこのモジュールのロードができないとSSLによる保護が有効にならないため、現在はまだ動作できていない。

#3 - 2016/01/15 23:52 - miyamoto

- ファイル test_SSLTrasport.zip を追加

- 進捗率 を 50 から 60 に変更

rtc.confのmanager.preload.modulesにモジュール名を記述する事でManagerのinitManager関数内でモジュールがロードされInit関数が呼び出される機能を追加した。

このためrtc.confへの記述方法を以下のように変更した。

manager.preload.modules: SSLTransport.py
corba.ssl.certificate_authority_file: root.crt
corba.ssl.key_file: server.pem
corba.ssl.key_file_password: password

ただしエンドポイントがsslのみの場合はRTシステムエディタなどからの操作ができなくなるため、他にエンドポインドがない場合はtcpを自動的に追加するようにしている。

if not OpenRTM_aist.toBool(prop.getProperty("manager.is_master"), "YES", "NO", True):
if len(prop.getProperty("corba.endpoints")) 0:
if len(prop.getProperty("corba.endpoint")) 0:
corba_args += " -ORBendPoint giop:tcp::"
prop.setProperty("corba.args",corba_args)

添付したテスト用コードでテストを行った。
テスト用コードを実行してomniORBのログを出した結果、sslが有効になっている事が確認できた。

omniORB: Perform SSL accept for new incoming connection giop:ssl:[::ffff:192.168
.0.2]:60389
omniORB: Server accepted connection from giop:ssl:[::ffff:192.168.0.2]:60389
omniORB: AsyncInvoker: thread id = 5 has started. Total threads = 4
omniORB: giopWorker task execute.
omniORB: Accepted connection from giop:ssl:[::ffff:192.168.0.2]:60389 because of
this rule: "* unix,ssl,tcp"
omniORB: inputMessage: from giop:ssl:[::ffff:192.168.0.2]:60389 38 bytes
omniORB: Handling a GIOP LOCATE_REQUEST.
omniORB: sendChunk: to giop:ssl:[::ffff:192.168.0.2]:60389 20 bytes
omniORB: inputMessage: from giop:ssl:[::ffff:192.168.0.2]:60389 96 bytes
omniORB: Receive codeset service context and set TCS to (ISO-8859-1,UTF-16)
omniORB: Creating new Python state for thread id 7744
omniORB: sendChunk: to giop:ssl:[::ffff:192.168.0.2]:60389 28 bytes

#4 - 2016/02/18 13:28 - n-ando

どのような条件で、endpoint が tcpかsslになるかの調査をお願いします。

#5 - 2016/02/20 00:36 - miyamoto

endpointをどのような条件でtcpかsslかを選択するかについて

指定方法①
クライアント側でORB_initのオプションORBclientTransportRuleを設定することでどのエンドポイントを優先するかを設定可能

例えば、

-ORBclientTransportRule "* ssl, tcp"

というオプションを追加するとsslが優先される。
sslとtcpを逆にするとtcpが優先される。

-ORBclientTransportRule "* tcp, ssl"

ここにssl、もしくはtcpを記述しなかった場合は、そのエンドポイントでの通信はできなくなる。

-ORBclientTransportRule "* ssl"

この場合はsslのエンドポイントでのみ通信ができる。

指定方法②
corbaloc形式でオブジェクトリファレンスを取得する場合は明示的に指定できる。

例えば、

corbaloc:ssliop:localhost:2810/ExampleEcho

とした場合はsslで通信する。

corbaloc:iiop:localhost:2810/ExampleEcho

の場合はtcpで通信する。

#6 - 2016/03/17 11:02 - miyamoto

- 進捗率 を 60 から 100 に変更

#7 - 2017/08/30 14:19 - n-ando

- ステータス を 新規 から 終了 に変更

ファイル

test_SSLTrasport.zip	4.55 KB	2016/01/15	miyamoto