IBM WebSphere MQ SSLcheck
Version 1.0

26 November 2006

Dale Lane
IBM Hursley Park
Hursley
Winchester
SO21 2JN

Dale.Lane@uk.ibm.com

Take Note!

Before using this report be sure to read the general information under "Notices".

First Edition, November 2006

This edition applies to Version 1.0 of IBM WebSphere MQ SSLcheck and to all subsequent releases and modifications unless otherwise indicated in new editions.

Table of Contents

Notices

The following paragraph does not apply in any country where such provisions are inconsistent with local law.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates.

Any reference to an IBM licensed program or other IBM product in this publication is not intended to state or imply that only IBM's program or other product may be used. Any functionally equivalent program that does not infringe any of the intellectual property rights may be used instead of the IBM product.

Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, New York 10594, USA.

The information contained in this document has not be submitted to any formal IBM test and is distributed AS-IS. The use of the information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item has been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Trademarks and service marks

The following terms, used in this publication, are trademarks of the IBM Corporation in the United States or other countries or both:

- IBM
- WebSphere
- MQ
- GSKit

Summary of Amendments

Date	Changes
26 November 2006	Initial release

Preface

Abstract

This SupportPac provides a test tool to look for common configuration mistakes in WebSphere MQ SSL configurations and provides recommendations for resolving problems. It is intended to be run from the command-line on Windows and UNIX platforms where GSkit is used to provide WMQ SSL support.

Description

A test tool designed to look for common configuration mistakes in customer SSL configurations. Intended to be run from the command-line on Windows and UNIX platforms where GSkit is used to provide WebSphere MQ SSL support.

The tool can check an individual queue manager to confirm that SSL has been correctly configured. Alternatively, if also provided with a copy of SSL files used by an WebSphere MQ client, it simulates a connection between the queue manager and client which it can then examine and provide diagnostic feedback on.

Possible Uses

This SupportPac is designed for people who are trying to use SSL with their WebSphere MQ channels, and would like confirmation that channels have been correctly configured, or a more detailed explanation why their channels are failing.

Checks for

SSLcheck currently checks for

- Missing SSL files
- Incorrect SSLKEYR queue manager attribute
- Problems with key repository stash files (and recreate stash files if needed)
- Password settings
- SSL file permissions (UNIX systems only)
- Certificate labels
- Certificate expiry dates
- Valid chain of trust for certificates
- Common environment problems for GSkit
- JRE configuration
- Validate queue manager and client certificates against each other
- Verifies SSLCAUTH/SSLPEER settings with queue manager key repository
- Use of SSL CRLs

Intended future development:

- SSL file permissions (Windows systems)
- More detailed SSLPEER checking
- A version for WebSphere MQ v5.3 (i.e. a version using GSkit v6 rather than v7)

Chapter 1. Installation Instructions

Prerequisites

- ☐ SupportPac MH03 zip-file
- ☐ WebSphere MQ v6.0 or greater
- ☐ GSkit v7

Installation Procedure

1. Copy the executable for the intended platform from the bin directory of the MH03 zip file
2. (Windows only) Ensure that the location of the IBM GSkit DLL (by default C:\Program Files\IBM\gsk7\lib) is in the PATH where SSLcheck is to be run:
3. (AIX only) Ensure that the WebSphere MQ lib directory (/usr/mqm/lib64) is in the LIBPATH
4. Put the directory where SSLcheck is stored into the PATH

Chapter 2. Instructions

Running SSLcheck

Server-side only

This will check whether SSL has been correctly configured for the specified queue manager.

```
amqsslchk QMGRNAME
```

where:

- `QMGRNAME` is the name of the SSL-enabled queue manager to be tested

Server and client-side

This will check whether SSL has been correctly configured for both the specified queue manager, and a WebSphere MQ client.

```
amqsslchk QMNAME -clientkeyr clnt_key_repos_path -clientuser clnt_username
```

where:

- `clnt_key_repos_path` is the absolute path (omitting .kdb file extension) to an SSL key repository intended to be used by a client
- `clnt_username` is the username that will be running the client

Notes

- The environment variable MQSSLKEYR can be used instead of the -clientkeyr argument.
- This has not been tested in environments with remote user management / validation (e.g. use of LDAP)
- When running in server and client-side mode, SSLcheck attempts to emulate the connection made by WebSphere MQ using SSL. Firewall software configured to prevent software from opening connections can cause this to fail.
- If any problems are experienced with the tool, please collect output from running with `-debug` and send to dale.lane@uk.ibm.com