Infrastructure - Task #8034

Story # 7801 (Closed): Support for Let's Encrypt certificates

Verify support for lets encrypt certificates by DataONE java and python clients

2017-03-03 03:39 - Dave Vieglais

Status:	Closed	**Start date:**	2017-03-03
Priority:	Normal	**Due date:**	
Assignee:	Roger Dahl	**% Done:**	100%
Category:	d1_libclient_java	**Estimated time:**	0.00 hour
Target version:	CCI-2.4.0		
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

Test support for letsencrypt certificates by DataONE Java and Python tools, and what if anything needs to be done for support.

Associated revisions

Revision 18675 - 2017-03-08 20:10 - Rob Nahf

refs #8034: Adding two Let's Encrypt intermediate certificates to the d1-trusted-certs.crt file. (Starting with MIIE and MIIF). The first is cross signed with the IdenTrust root, and the other just by their own root.

Revision 18675 - 2017-03-08 20:10 - Rob Nahf

refs #8034: Adding two Let's Encrypt intermediate certificates to the d1-trusted-certs.crt file. (Starting with MIIE and MIIF). The first is cross signed with the IdenTrust root, and the other just by their own root.

Revision 18676 - 2017-03-08 22:13 - Rob Nahf

refs #8034: Replacing the LE intermediate certs with the LE root (starting with MIIFaz) and the IdenTrust root (starting with MIIDSj) certificates.

Revision 18676 - 2017-03-08 22:13 - Rob Nahf

refs #8034: Replacing the LE intermediate certs with the LE root (starting with MIIFaz) and the IdenTrust root (starting with MIIDSj) certificates.

Revision 18677 - 2017-03-08 22:21 - Rob Nahf

refs #8034: added the LE root (starting with MIIFaz) and the IdenTrust root (starting with MIIDSj) certificates to 2.3 branch; bumped pom version to 2.3.1.

Revision 18677 - 2017-03-08 22:21 - Rob Nahf

refs #8034: added the LE root (starting with MIIFaz) and the IdenTrust root (starting with MIIDSj) certificates to 2.3 branch; bumped pom version to 2.3.1.

History

#1 - 2017-03-03 20:08 - Rob Nahf

- Status changed from New to In Progress

- % Done changed from 0 to 30

libclient_java can support LetsEncrypt CA by including it in the src/main/resource/org/dataone/client/auth/d1-trusted-certs.crt file. SVN shows this file has not been changed since Oct 31, 2012, so the LetsEncrypt CA is definitely not yet supported.

#2 - 2017-03-03 20:55 - Matthew Jones

Java JDK 8u101 and beyond include the root certificate needed to validate Lets Encrypt certificates out of the box. So we've been upgrading Metacat and Morpho installs to recent Java versions (mostly 8u121) and that's been working great. Including the certificate in the libclient distribution will help with older clients, but we should also be careful to not override the default cert that now ships with Java 8.

#3 - 2017-03-08 17:28 - Rob Nahf

The CertificateManager checks for existence of a certificate before adding it from the trusted-certs file, so it should not clobber the existing one in Java8 environments.

#4 - 2017-03-08 22:13 - Rob Nahf

- Status changed from In Progress to Testing

- % Done changed from 30 to 50

https://letsencrypt.org/docs/certificate-compatibility/

The main determining factor for whether a platform can validate Let's Encrypt certificates is whether that platform includes IdenTrust's DST Root X3 certificate in its trust store. A secondary factor is whether the platform supports modern SHA-2 certificates, since all Let's Encrypt certificates use SHA-2.

Known Compatible (java)
Java 7 >= 7u111
Java 8 >= 8u101

wrt SHA-2, the minimum version is Java 1.4.2+, so we will not worry about that, since DatAONE requires minimum Java 1.6

Adding the LE and IdenTrust root CA certs to d1-tursted-certs.crt file. (previously I committed the intermediate certs mistakenly, so removed those)

#5 - 2017-03-09 17:22 - Rob Nahf

- Status changed from Testing to In Progress

- Assignee changed from Rob Nahf to Roger Dahl

- % Done changed from 50 to 30

created integration test to test ability of d1_libclient_java to trust the LE certificate. They have a test page to hit that uses their certificate: https://helloworld.letsencrypt.org/, and the test does a GET to that URL, and checks for handshake errors.

Handing the ticket over to Roger for the python side.

#6 - 2017-05-04 18:07 - Jing Tao

- Target version changed from CCI-2.3.4 to CCI-2.4.0

#7 - 2018-01-17 19:16 - Dave Vieglais

- % Done changed from 30 to 100

- Status changed from In Progress to Closed