CN REST - Bug #7301

CN-stage allows connections to a MN that is operating a self-signed SSL server certificate

2015-08-18 18:12 - Mark Servilla

Status:	New	**Start date:**	2015-08-18
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Story Points:			

Description

CN-stage supports connections to a MN that is operating a self-signed SSL server certificate - this should not be allowed since the connection could occur with a rogue non-verified server.

This instance occurred with dataone-dev.ecoinformatics.org.au:443 on 18 August 2015:

Certificate chain
0 s:/CN=dataone-dev.ecoinformatics.org.au
i:/CN=dataone-dev.ecoinformatics.org.au

Issuer: CN=dataone-dev.ecoinformatics.org.au
Validity
Not Before: Aug 11 04:56:19 2015 GMT
Not After : Aug 8 04:56:19 2025 GMT
Subject: CN=dataone-dev.ecoinformatics.org.au

History

#1 - 2015-08-19 03:46 - Mark Servilla

After restarting d1-processing at approximate 03:30 19 August 2015 GMT, cn-stage began denying connections to dataone-dev.ecoinformatics.org.au:443 (see below). Apparently, the SSL information is either cached or ignored and operations presumably continue without exception. Note that, although a security exception was not thrown, no new content was harvested from dataone-dev.ecoinformatics.org.au:443.

[ERROR] 2015-08-19 03:30:01,090 (ObjectListHarvestTask:retrieve:251) urn:node:mnTestAEKOS- <?xml version="1.0" encoding="UTF-8"?>

class javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target