Infrastructure - Story #6545

Migrate DataONE off SHA-1 for certificates

2014-11-03 14:00 - Bruce Wilson

Status:	Closed	**Start date:**	2015-02-02
Priority:	Normal	**Due date:**	
Assignee:	Dave Vieglais	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	CCI-1.5.1		
Story Points:			

Description

SHA-1 is in the process of being deprecated, and DataONE should migrate away from this for signatures and message authentication, presumably to SHA-256. This includes the HTTPS certificates on web servers, the signatures in DataONE-issued certificates, and potentially other locations. However, this migration has the potential to make DataONE services inaccessible to some older operating systems. The prioritization of this work is that it is post-V2.0 deployment.

Subtasks:

Task # 6792: Update certificates being used by production CNs	**Closed**

History

#1 - 2014-11-05 13:40 - Dave Vieglais

A new certificate has been generated using SHA-2.

It is located at (but as of this writing not active for the server) cn-ucsb-1.dataone.org:

.dataone.org key: /etc/ssl/private/.dataone.org.20141104.key*
**.dataone.org crt: /etc/ssl/certs/*.dataone.org.20141104.crt
intermediate cert: /etc/ssl/certs/geotrust_intermediate.20141104.crt

Proceeding within installation on various operations and production servers.

#2 - 2014-11-05 13:47 - Dave Vieglais

Basic apache configuration on Ubuntu will be something like:

/etc/apache2/mods-available/ssl.conf:
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS"

/etc/apache2/sites-available/default-ssl:
SSLCertificateFile /etc/ssl/certs/*.dataone.org.20141104.crt*
SSLCertificateKeyFile /etc/ssl/private/.dataone.org.20141104.key
SSLCertificateChainFile /etc/ssl/certs/geotrust_intermediate.20141104.crt

#3 - 2014-11-05 17:45 - Dave Vieglais

Command line command to check the encryption being used by a server:

export TARGET="docs2.dataone.org"
openssl s_client -connect ${TARGET}:443 < /dev/null 2>/dev/null | openssl x509 -text -in /dev/stdin | grep "Signature Algorithm"

#4 - 2014-11-05 18:31 - Nick Outin

I updated the sites hosted at NCEAS (repository.dataone.org, docs.dataone.org, and the https://dataone.org redirect).

#5 - 2014-12-10 20:40 - Dave Vieglais

Wild card cert for *.test.dataone.org regenerated using SHA-2.

It is located at on cn-stage-ucsb-1.test.dataone.org:

.test.dataone.org key: /etc/ssl/private/*.test.dataone.org.20141210.key*
.test.dataone.org crt: /etc/ssl/certs/.test.dataone.org.20141210.crt
intermediate cert: /etc/ssl/certs/geotrust_intermediate.20141210.crt

Basic Apache configuration on Ubuntu (including disabling SSLv2 and v3 looks something like:

/etc/apache2/mods-available/ssl.conf:
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS"

/etc/apache2/sites-available/default-ssl:
SSLCertificateFile   /etc/ssl/certs/*.test.dataone.org.20141210.crt*
SSLCertificateKeyFile /etc/ssl/private/.test.dataone.org.20141210.key
SSLCertificateChainFile /etc/ssl/certs/geotrust_intermediate.20141210.crt

#6 - 2014-12-12 15:36 - Michael Campfield

The following hostnames have been updated with new keys and SSLv3 removal:
cn-dev-orc-1.test.dataone.org;443;sha256WithRSAEncryption;SSLv3Absent;
cn-sandbox-orc-1.test.dataone.org;443;sha256WithRSAEncryption;SSLv3Absent;
cn-stage-orc-1.test.dataone.org;443;sha256WithRSAEncryption;SSLv3Absent;
mn-sandbox-orc-1.test.dataone.org;443;sha256WithRSAEncryption;SSLv3Absent;
cn-stage-ucsb-1.test.dataone.org;443;sha256WithRSAEncryption;SSLv3Absent;

--Michael Campfield

#7 - 2015-01-19 23:11 - Dave Vieglais

- Target version set to CCI-1.5.1

#8 - 2015-02-02 14:38 - Dave Vieglais

- % Done changed from 0 to 30

- Category deleted (Authentication, Authorization)

- Assignee set to Dave Vieglais

- Status changed from New to In Progress

#9 - 2015-05-27 16:19 - Dave Vieglais

- % Done changed from 30 to 100

- Status changed from In Progress to Closed