Test Resources - Task #7064

Test certificates on mncheck are expired or expiring soon

2015-04-28 20:00 - Andrei Buium

Status:	Closed	**Start date:**	2015-04-28
Priority:	Normal	**Due date:**	
Assignee:	Mark Servilla	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			
Story Points:			

Description

I went through the certificates on mncheck.test.dataone.org
at /etc/dataone/client/ in testClientCerts

These certificates are expired:

cnDevUNM1.crt

urn:node:cnSandboxUNM1.crt
cnSandboxUNM1.crt
testPerson_Expired.crt
urn:node:cnDevUNM1.crt

These are expiring soon:

testEQPerson2.crt May 17
testPerson_NoSubjectInfo.crt May 17
testEQPerson3.crt May 17
urn:node:cnStageUNM1.crt May 15
cnStageUNM1.crt May 15
testGroupie.crt May 17
testRightsHolder.crt May 17
testPerson.crt May 17
testSubmitter.crt May 17
testEQPerson1.crt May 17

This one will be ok for a while:

testPerson_SelfSigned.crt May 3, 2112

History

#1 - 2015-04-28 20:04 - Andrei Buium

Note: The CN certs like cnDevUNM1.crt and similarly-named certs are just renamed versions of urn:node:cnDevUNM1.crt etc

#2 - 2015-04-28 22:22 - Andrei Buium

Note 2: I'm pretty sure testPerson_Expired.crt can be left as it is.

#3 - 2015-04-29 15:22 - Rob Nahf

yep. testPerson_expired was designed to be expired.

#4 - 2015-04-29 15:33 - Mark Servilla

Questions:

It appears that the previous set of certificates were signed by the DataONETestCA certificate authority; we are currently using the

DataONETestIntCA (test intermediate) certificate authority for signing all new MN test certificates - which CA should we use of this set of certificates?

You have in the list a number of certificates already in use by other entities (e.g., urn:node:cnSandboxUNM1.crt). Do you require these certificates? If so, should you use a copy of the existing certificate (as opposed to generating another "like" certificate)?

Thanks,
Mark

#5 - 2015-04-29 17:18 - Rob Nahf

we should probably use the IntCA - it's what's being used for CN client certs.

Regarding the CN certs, if they are set to expire in May (in two weeks), we will need to update those test CNs as well, so maybe it's a good idea to create them, and then we can work on installing them there.

Do you keep a record of each certificate you create? (along with the expriation) or do we need to check the CNs directly?

#6 - 2015-05-01 02:51 - Mark Servilla

The following x509 certificate bundles have been generated/signed by the DataONETestIntCA certificate authority and placed on the DataONE certificate exchange at https://project.dataone.org/~andreib:
* CN=testEQPerson1 (testEQPerson1.zip)
* CN=testEQPerson2 (testEQPerson2.zip)
* CN=testEQPerson3 (testEQPerson3.zip)
* CN=testGroupie (testGroupie.zip)
* CN=testPerson_NoSubjectInfo (testPerson_NoSubjectInfo.zip)
* CN=testPerson (testPerson.zip)
* CN=testRightsHolder (testRightsHolder.zip)
* CN=testSubmitter (testSubmitter.zip)
* CN=urn:node:cnStageUNM1 (urn_node_cnStageUNM1.zip)

The following x509 certificate bundles should be grabbed from the their respective servers since I do not have access to their keys:
* CN=urn:node:cnDevUNM1 (expiration Mar 18 19:44:48 2018 GMT)
* CN=urn:node:cnSandboxUNM1 (expiration Mar 19 18:16:54 2018 GMT)

#7 - 2015-05-05 20:54 - Rob Nahf

I forgot that the non-server test certificates need to have the serialized SubjectInfo embedded in them upon creation. Last time they were generated, Chris was the one who did it, and I see now that the automated "ca" script doesn't have the flexibility to add it.

Details on what's needed is at: https://repository.dataone.org/software/cicore/trunk/d1_integration/GeneratingITCertificates.txt

basically, openssl adds a custom extension that we predefined for CILogon certificates (name / oid)

"cilogon.oid.subjectinfo", "1.3.6.1.4.1.34998.2.1"

a shell script for setting extensions can be found here, but it looks like they are adding the extensions to the root CA, not the individual certificates themselves (which should be an option, because CILogon does has different extensions for each cert it issues)

http://vijairaj.blogspot.com/2009/01/creating-x509-certificates-with-custom.html

see also man pages:
man x509
man x509v3_config

Maybe we should get Chris's advice?

(The current ones expire on May 17th, 2015)

#8 - 2015-05-05 22:38 - Rob Nahf

I imported the newer certificates from the test CNs onto mncheck, and regenerated a self-signed cert that isn't expired (will expire in 2018). Repointed 'testClientCerts' to the 'testClientCerts-2015-05-05' directory. The existing test{Foo} certificates from the 2015-01-26 directory that expire on May 17th were copied here, too. Once the 'test{Foo}' certificates with subjectInfo are generated, we will update the /etc/dataone/client/ certs again.

#9 - 2015-05-12 21:05 - Mark Servilla

Revoking all previously generated test* certificates:

./ca -r Test testEQPerson1
Revoking certificate for testEQPerson1
Using configuration from openssl.cnf
Enter pass phrase for /Volumes/DataONE/DataONETestIntCA.key:
Revoking Certificate DA3263A2A12D00AA.
Data Base Updated

./ca -r Test testEQPerson2
Revoking certificate for testEQPerson2
Using configuration from openssl.cnf
Enter pass phrase for /Volumes/DataONE/DataONETestIntCA.key:
Revoking Certificate DA3263A2A12D00A3.
Data Base Updated

./ca -r Test testEQPerson3
Revoking certificate for testEQPerson3

Using configuration from openssl.cnf
Enter pass phrase for /Volumes/DataONE/DataONETestIntCA.key:
Revoking Certificate DA3263A2A12D00A5.
Data Base Updated

./ca -r Test testGroupie
Revoking certificate for testGroupie
Using configuration from openssl.cnf
Enter pass phrase for /Volumes/DataONE/DataONETestIntCA.key:
Revoking Certificate DA3263A2A12D00A6.
Data Base Updated

./ca -r Test testPerson_NoSubjectInfo
Revoking certificate for testPerson_NoSubjectInfo
Using configuration from openssl.cnf
Enter pass phrase for /Volumes/DataONE/DataONETestIntCA.key:
Revoking Certificate DA3263A2A12D00A4.
Data Base Updated

./ca -r Test testPerson
Revoking certificate for testPerson
Using configuration from openssl.cnf
Enter pass phrase for /Volumes/DataONE/DataONETestIntCA.key:
Revoking Certificate DA3263A2A12D00A8.
Data Base Updated

./ca -r Test testSubmitter
Revoking certificate for testSubmitter
Using configuration from openssl.cnf
Enter pass phrase for /Volumes/DataONE/DataONETestIntCA.key:
Revoking Certificate DA3263A2A12D00A9.
Data Base Updated

#10 - 2015-05-12 21:35 - Mark Servilla

The following x509 certificate bundles have been updated with the appropriate subject_info and placed on the certificate exchange:

- CN=testEQPerson1 (testEQPerson1-1.zip)
- CN=testEQPerson2 (testEQPerson2-1.zip)
- CN=testEQPerson3 (testEQPerson3-1.zip)
- CN=testGroupie (testGroupie-1.zip)
- CN=testPerson_NoSubjectInfo (testPerson_NoSubjectInfo-1.zip)
- CN=testPerson (testPerson-1.zip)
- CN=testRightsHolder (testRightsHolder-1.zip)

- CN=testSubmitter (testSubmitter-1.zip)

#11 - 2015-05-20 18:09 - Mark Servilla

All previous certificates contain an incorrect "alternate extension" - the XML snippet contains illegal content because attribute values are not quoted. I used a copy of the earliest version of each certificate in /ca/DataONETestCA/certs to obtain the XML snippet, which also contained the illegal content. Each certificate will need to be revoked and then regenerated.

The following x509 certificate bundles have been updated with the appropriate subject_info and placed on the certificate exchange:

- CN=testEQPerson1 (testEQPerson1-2.zip)
- CN=testEQPerson2 (testEQPerson2-2.zip)
- CN=testEQPerson3 (testEQPerson3-2.zip)
- CN=testGroupie (testGroupie-2.zip)
- CN=testPerson_NoSubjectInfo (testPerson_NoSubjectInfo-2.zip)
- CN=testPerson (testPerson-2.zip)
- CN=testRightsHolder (testRightsHolder-2.zip)
- CN=testSubmitter (testSubmitter-2.zip)

#12 - 2015-05-20 23:04 - Mark Servilla

- translation missing: en.field_remaining_hours set to 0.0

- % Done changed from 0 to 100

- Status changed from New to Closed

All certificates have been generated (multiple times) and all tests now pass - according to Andrei.