Infrastructure - Task #6787

Story # 6625 (Closed): Requirement of Java 1.8 for Dataone V2

Ensure Java 7 Client code can communicate over SSL

2015-01-30 20:42 - Chris Jones

Status:	Closed	**Start date:**	2015-01-30
Priority:	Normal	**Due date:**	
Assignee:	Jing Tao	**% Done:**	100%
Category:	Environment.Production	**Estimated time:**	0.00 hour
Target version:	CCI-2.3.0		
Milestone:	CCI-2.0	**Story Points:**	
Product Version:	*		

Description

After testing clients in the Sandbox2 environment, we've found some issues with SSL connections from Java 7 clients. The issue looks to be related to Java 7's support for SNI, which is discussed here:
https://stackoverflow.com/questions/7615645/ssl-handshake-alert-unrecognized-name-error-since-upgrade-to-java-1-7-0

CN's making calls as clinets to MNs may get this same error. By adding the -Djsse.enableSNIExtension=false parameter for the JVM, the issue looks to be fixed, but this may not be the best solution. Determine how to configure Apache web servers to support SNI, or use this solution as a fallback.

Related issues:

Related to Infrastructure - Story #7586: LogAggregation fails for MN in produ...	**Closed**	**2016-01-15**
Blocks Infrastructure - Bug #6785: Change format type of NetCDF from METADATA...	**Closed**	**2015-01-30**

History

#1 - 2015-01-30 21:19 - Jing Tao

I did see this issue before. But the solution is to modify the apache configuration -- adding a new properties ServerName and ServerAlias on both CNs and MNs. It works perfectly on sandbox-1 and stage-1 env. Here is an example:

ServerName cn-sandbox.test.dataone.org
ServerAlias cn-sandbox-ucsb-1.test.dataone.org

Those cns are running Ubuntu 12 and open jdk 7. Mainly MNs are running Ubuntu 14 and open jdk 7.

I am a little bit confused why sandbox-2 doesn't work on this way.

#2 - 2015-01-30 21:32 - Chris Jones

- Blocks Bug #6785: Change format type of NetCDF from METADATA to DATA added

#3 - 2015-02-02 16:29 - Chris Jones

Thanks Jing - it's good to know that this is an easy fix. Have you updated the dataone-cn-os-core buildout to add this configuration into the CN installation or upgrade? I can make the change manually in the Sandbox2 environment, but we need it to be permanent.

#4 - 2015-04-15 19:51 - Jing Tao

- % Done changed from 0 to 100

- translation missing: en.field_remaining_hours set to 0.0

- Status changed from New to Closed

I double checked code (postinst in dataone-cn-os-core) and found the setting:

replace the token SERVER_NAME in the site file

```
    if [ -n ${DEB_QUESTION_VALUES[dataone-cn-os-core/cn.router.hostname]} ]; then
        if ! (sed -i.bak  's/SERVER_NAME/'${DEB_QUESTION_VALUES[dataone-cn-os-core/cn.router.hostname]}'/' ${A
PACHE_CONF_DIR}/sites-available/${SITE} >> ${D1_LOG_DIR}/${D1_LOG_FILE} 2>&1); then
            log "Unable to modify SERVER_NAME in ${SITE} Apache"
        fi
    else
            log "dataone-cn-os-core/cn.router.hostname can not be set in ${APACHE_CONF_DIR}/sites-available/${
SITE}"
    fi

    ## replace the token SERVER_ALIAS in the site file

    if [ -n ${DEB_QUESTION_VALUES[dataone-cn-os-core/cn.hostname]} ]; then
        if ! (sed -i.bak  's/SERVER_ALIAS/'${DEB_QUESTION_VALUES[dataone-cn-os-core/cn.hostname]}'/' ${APACHE_
CONF_DIR}/sites-available/${SITE} >> ${D1_LOG_DIR}/${D1_LOG_FILE} 2>&1); then
            log "Unable to modify SERVER_ALIAS in ${SITE} Apache"
        fi
    else
            log "dataone-cn-os-core/cn.hostname can not be set in ${APACHE_CONF_DIR}/sites-available/${SITE}"
    fi
```

#5 - 2015-10-05 14:47 - Chris Jones

- % Done changed from 100 to 30

- Status changed from Closed to In Progress

- Estimated time set to 0.00

I'm reopening this issue because the above fix only works in one direction (MNs calling the CN). We need to disable SNI support programmatically. For some context, here's my response to Mark Flynn re: SSL failures with this same error:

Hi Mark,

To follow up on this sync issue, I had remembered that we had a similar error with the CNs (see #6787).

This is an issue with Java 7 (on the CNs) enabling SNI support (see this Stack Overflow discussion).

Jing added a fix where the Apache 'ServerName' and 'ServerAlias' directives where specifically set in the CN's configuration, and that allowed Java-7-based MNs calling the CNs to connect correctly.

The error we're seeing with your GMN is effectively the opposite direction. The CN is enforcing the SNI rules for SSL to succeed with MNs. So, for flynn-gmn-1.test.dataone.org, I added the 'ServerName' and 'ServerAlias' directives to the gmn-ssl.conf file. I then restarted Apache on flynn-gmn-1.

I rolled back the ‘last harvest date’ attribute for flynn-gmn-1 in the CN’s LDAP entry for your node, and sync tried again with:

[DEBUG] 2015-10-05 07:18:25,259 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-test
[DEBUG] 2015-10-05 07:18:25,259 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-test_0723
[DEBUG] 2015-10-05 07:18:25,260 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-test2
[DEBUG] 2015-10-05 07:18:25,260 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue-
Task-urn:node:mnTestFLYNN-43c7c7bbc83c1f4ad9b7d81bc3728333
[DEBUG] 2015-10-05 07:18:25,260 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-dave.test.0001
[DEBUG] 2015-10-05 07:18:25,260 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-dv.test.002
[DEBUG] 2015-10-05 07:18:25,261 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-dv.test.003
[DEBUG] 2015-10-05 07:18:25,261 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue-
Task-urn:node:mnTestFLYNN-5a9f126793a1c21a33f9db1c08e07208
[DEBUG] 2015-10-05 07:18:25,261 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-d1.test.004
[DEBUG] 2015-10-05 07:18:25,261 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue-
Task-urn:node:mnTestFLYNN-c2a8ed7ddbf759a67b2d5ea256f05fb8
[DEBUG] 2015-10-05 07:18:25,261 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-cell
[DEBUG] 2015-10-05 07:18:25,262 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-dv.test.005
[DEBUG] 2015-10-05 07:18:25,262 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-cell2
[DEBUG] 2015-10-05 07:18:25,262 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-start
[DEBUG] 2015-10-05 07:18:25,262 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-testudo
[DEBUG] 2015-10-05 07:18:25,263 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-dv.test.004
[DEBUG] 2015-10-05 07:18:25,263 (ObjectListHarvestTask:call:192) placed on hzSyncObjectQueue- Task-urn:node:mnTestFLYNN-dv.test.006

So, it looks to me like sync is working for FLYNN (and still failing for FLYNN2), so I think this Apache config did the trick. The pid you mentioned below is now sync’d on the CN: https://cn-dev-2.test.dataone.org/cn/v2/meta/start . Note that replication ensued, and replicas succeeded on mnDevUCSB2 and mnDevUNM2, but it failed on mnTestFLYNN2 (due to the SSL issues I suspect).

Soooo, this works, but it’s not a global fix. My thought here is that we need to disable SNI support on the CNs programmatically using (-Djsse.enableSNIExtension=false) so that when they encounter MNs that don’t pass along serverName information, they’ll still be able to connect over SSL. I’m re-opening #6787 and cc’ing Jing on this so he’s aware of the issue.

#6 - 2015-10-05 16:33 - Chris Jones

- % Done changed from 30 to 100

- Status changed from In Progress to Closed

Dave pointed out that SNI can have practical benefits, so we're just going to require the ServerName setting for all CNs and MNs. I'll close this again.

#7 - 2016-01-14 17:57 - Robert Waltz

- Related to Story #7586: LogAggregation fails for MN in production with handshake alert added