D4Science Infrastructure - Task #899

Task # 896 (Closed): Please create a testing cluster for couchdb

New VM for the couchdb dev cluster haproxy frontend

Oct 06, 2015 05:26 PM - Andrea Dell'Amico

Status:	Closed	**Start date:**	Oct 06, 2015
Priority:	High	**Due date:**	Oct 16, 2015
Assignee:	Andrea Dell'Amico	**% Done:**	100%
Category:	System Application	**Estimated time:**	0.00 hour
Target version:	CouchDB Deployment		
Infrastructure:	Development, Pre-Production		

Description

Possibile names:
couchdb-d-d4s.d4science.org
couchdb-gcube-d-d4s.d4science.org

History

#1 - Oct 06, 2015 05:28 PM - Andrea Dell'Amico

- Subject changed from New VM for the couchdb dev cluster to New VM for the couchdb dev cluster haproxy frontend

- Description updated

#2 - Oct 06, 2015 05:29 PM - Andrea Dell'Amico

- Description updated

#3 - Oct 08, 2015 04:49 PM - Luca Frosini

- Tracker changed from Support to Task

- Due date set to Oct 16, 2015

#4 - Oct 21, 2015 03:36 PM - Luca Frosini

- Priority changed from Normal to High

#5 - Oct 22, 2015 05:50 PM - Andrea Dell'Amico

- Status changed from New to In Progress

The VM hostname is accounting-d-d4s.d4science.org

#6 - Oct 22, 2015 05:54 PM - Andrea Dell'Amico

- Assignee changed from _InfraScience Systems Engineer to Andrea Dell'Amico

- % Done changed from 0 to 40

I'm going to install haproxy with a failover configuration. The preferred node will be couchdb01-d-d4s.d4science.org

#7 - Oct 23, 2015 10:31 AM - Luca Frosini

- Related to Task #1226: Migrate databases from accounting-d4s.d4science.org to couchdb01-d-d4s.d4science.org added

#8 - Oct 23, 2015 10:32 AM - Luca Frosini

- Related to deleted (Task #1226: Migrate databases from accounting-d4s.d4science.org to couchdb01-d-d4s.d4science.org)

#9 - Oct 23, 2015 10:42 AM - Andrea Dell'Amico

- Status changed from In Progress to Feedback

- % Done changed from 40 to 80

haproxy is running with a plain load balancing configuration.

Only http and not https for now. We have certificates for the production nodes only.

#10 - Oct 23, 2015 01:30 PM - Andrea Dell'Amico

- % Done changed from 80 to 90

https is enabled on the dev haproxy server. The certificate is the one generated for the production host, so expect some warnings.

http is still enabled, after the testing phase the http requests will be redirected to https.

#11 - Oct 23, 2015 05:25 PM - Luca Frosini

The proxy seems not working properly
Using the proper username and password hidden here by XXX for security reason I have the right behaviour interrogating directly the couch installation:

```
$ ADMIN_HOST="http://XXXX:XXXXX@couchdb01-d-d4s.d4science.org:5984"
$ curl -X GET $ADMIN_HOST
{"couchdb":"Welcome","uuid":"bab79b78679999cb9a8c500d116c67ab","version":"1.6.1","vendor":{"version":"14.04","
name":"Ubuntu"}}

$ ADMIN_HOST="http://XXXX:XXXXX@couchdb02-d-d4s.d4science.org:5984"
$ curl -X GET $ADMIN_HOST
{"couchdb":"Welcome","uuid":"d9d072547ff335b88104c9219f9027d9","version":"1.6.1","vendor":{"version":"14.04","
name":"Ubuntu"}}
```

Using the same credentials for proxy server I obtained no answer.

```
$ ADMIN_HOST="http://XXXX:XXXXX@accounting-d-d4s.d4science.org"
$ curl -X GET $ADMIN_HOST
```

Trying to create a new user I had:

```
$ curl -HContent-Type:application/json -vXPUT $ADMIN_HOST/_users/org.couchdb.user:test --data-binary '{"_id":
"org.couchdb.user:test","name": "test","roles": [],"type": "user","password": "ASAP"}'

* Hostname was NOT found in DNS cache
*   Trying 146.48.123.24...
* Connected to accounting-d-d4s.d4science.org (146.48.123.24) port 80 (#0)
* Server auth using Basic with user 'admin'
> PUT /_users/org.couchdb.user:test HTTP/1.1
> Authorization: Basic YWRtaW46YmV0dGVyX3RoYW5fbm90aGluZw==
> User-Agent: curl/7.38.0
> Host: accounting-d-d4s.d4science.org
> Accept: */*
> Content-Type:application/json
> Content-Length: 93
>
* upload completely sent off: 93 out of 93 bytes
< HTTP/1.1 302 Found
< Cache-Control: no-cache
< Content-length: 0
< Location: https://accounting-d-d4s.d4science.org/_users/org.couchdb.user:test
< Connection: close
<
* Closing connection 0
```

The same http request made directly to couchdb01 terminated successfully:

```
$ curl -HContent-Type:application/json -vXPUT $ADMIN_HOST/_users/org.couchdb.user:test --data-binary '{"_id":
"org.couchdb.user:test","name": "test","roles": [],"type": "user","password": "ASAP"}'

* Hostname was NOT found in DNS cache
*   Trying 146.48.123.50...
* Connected to couchdb01-d-d4s.d4science.org (146.48.123.50) port 5984 (#0)
* Server auth using Basic with user 'admin'
> PUT /_users/org.couchdb.user:test HTTP/1.1
> Authorization: Basic YWRtaW46YmV0dGVyX3RoYW5fbm90aGluZw==
> User-Agent: curl/7.38.0
> Host: couchdb01-d-d4s.d4science.org:5984
> Accept: */*
> Content-Type:application/json
> Content-Length: 93
>
* upload completely sent off: 93 out of 93 bytes
```

```
< HTTP/1.1 201 Created
* Server CouchDB/1.6.1 (Erlang OTP/R16B03) is not blacklisted
< Server: CouchDB/1.6.1 (Erlang OTP/R16B03)
< Location: http://couchdb01-d-d4s.d4science.org:5984/_users/org.couchdb.user:test
< ETag: "1-1178079f6b93e03eba97a405405e9e59"
< Date: Fri, 23 Oct 2015 15:24:38 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 84
< Cache-Control: must-revalidate
<
{"ok":true,"id":"org.couchdb.user:test","rev":"1-1178079f6b93e03eba97a405405e9e59"}
* Connection #0 to host couchdb01-d-d4s.d4science.org left intact
```

#12 - Oct 23, 2015 05:40 PM - Luca Frosini

The interesting thing is that Futon works perfectly. Maybe just a matter of configuration made explicitly just to make futon working?
https://accounting-d-d4s.d4science.org/_utils/

#13 - Oct 27, 2015 03:25 PM - Luca Frosini

- Target version changed from zz - Accouting Facility to CouchDB Deployment

#14 - Oct 28, 2015 03:06 PM - Luca Frosini

The problem was related to my error:
I used

```
$ ADMIN_HOST="http://XXXX:XXXXX@accounting-d-d4s.d4science.org"
```

instead of

```
$ ADMIN_HOST="https://XXXX:XXXXX@accounting-d-d4s.d4science.org"
```

Note http*s* in the url. Using **https** and using -k option with curl (to accept all certificates) seems working properly.

I have now to test it if java code works with our certificates. If it does not work we should deactivate https on haproxy for dev cluster.

#15 - Oct 28, 2015 03:15 PM - Andrea Dell'Amico

Or you can produce a new keyring that contains the INFN CA cert. We did the same for the portals.

#16 - Oct 28, 2015 03:19 PM - Luca Frosini

Unfortunately we can't. Accounting is a library that run on all ghn

#17 - Oct 28, 2015 06:00 PM - Luca Frosini

I confirm that in dev we can't enable **https** until we can obtain a valid certificate.
javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching accounting-d-d4s.d4science.org found.

The alternative is renaming the proxy hostname with tha name of an unused host we already own a globally recognized certificate:

I'm going to test the production now

#21 - Oct 28, 2015 06:46 PM - Luca Frosini

Dev haproxy seems working now on http. Thank you

#23 - Oct 29, 2015 12:03 PM - Luca Frosini

I Confirm that also using java code there is the same security issue with the certificate of accounting-d4s.d4science.org.

```
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
    at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
    at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1904)
    at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:279)
    at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:273)
    at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1446)
    at sun.security.ssl.ClientHandshaker.processMessage(ClientHandshaker.java:209)
    at sun.security.ssl.Handshaker.processLoop(Handshaker.java:913)
    at sun.security.ssl.Handshaker.process_record(Handshaker.java:849)
    at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1023)
    at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1332)
    at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1359)
    at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1343)
    at sun.net.www.protocol.https.HttpsClient.afterConnect(HttpsClient.java:559)
    at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnectio
n.java:185)
    at sun.net.www.protocol.http.HttpURLConnection.getOutputStream(HttpURLConnection.java:1092)
    at sun.net.www.protocol.https.HttpsURLConnectionImpl.getOutputStream(HttpsURLConnectionImpl.java:250)
    .......
Caused by: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpat
h.SunCertPathBuilderException: unable to find valid certification path to requested target
    at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:385)
    at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:292)
    at sun.security.validator.Validator.validate(Validator.java:260)
    at sun.security.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:326)
    at sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:231)
    at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:126)
    at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1428)
    ... 38 more
Caused by: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path
 to requested target
    at sun.security.provider.certpath.SunCertPathBuilder.engineBuild(SunCertPathBuilder.java:196)
    at java.security.cert.CertPathBuilder.build(CertPathBuilder.java:268)
    at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:380)
    ... 44 more
```

#24 - Oct 29, 2015 12:39 PM - Andrea Dell'Amico

It seems that the Terena CA that was used by GARR is not operating anymore (see [[[https://www.terena.org/activities/tcs/]]]), now this kind of certificates offering is running under another initiative: [[[http://www.geant.org/TCS/Pages/default.aspx]]] (note that the site is plain http :-))

My expectation was that is these situations the old CA cert should live for a while, but I was wrong.

#25 - Oct 29, 2015 02:42 PM - Luca Frosini

- Status changed from Feedback to Closed

- % Done changed from 90 to 100

So I think this ticket can be closed now. We will open a new one for such an issue.